ANNEXURE

INFORMATION SYTEMS SECURITY GUIDELINES FOR THE BANKING AND FINANCIAL SECTOR'

Chapter 1

Introduction

1.1 The information and the supporting processes, the computer systems and the networks, used for generating, storing and retrieving information and the human beings are important business assets of every organisation. The confidentiality, integrity and availability of information is essential for any financial organisation to maintain its competitive edge, cash-flow, profitability, legal compliance and commercial image. The application of Information Technology has brought about significant changes in the way the banking and the financial organisations process and store data. The telecommunication networks have played a catalytic role in the expansion and integration of the Information Systems, within and among the organisations, facilitating data accessibility to different users. This has made it imperative for each organisation to put in place adequate security controls to ensure data accessibility to all the authorised users, data inaccessibility to all the unauthorized users, maintenance of data integrity and implementation of safeguards against all security threats to guarantee information and information systems security across the organisation. This makes it necessary for each organisation to define, document, communicate, implement and audit Information Systems (IS) Security.

1.2 The information systems and the networks of the organisations are increasingly faced with security threats from a wide range of sources including computer-assisted fraud, espionage, sabotage, vandalism etc. The sources of damage such as the computer viruses, computer hacking and denial of service attacks have become more common, more ambitious and increasingly sophisticated in the networked environment. The ever-growing dependence of the organisations on the information systems has made them more vulnerable to such security threats. At the same time, the interconnection between the public and the private networks and the sharing of the information assets/ resources have increased the difficulty of ensuring security for information and the information systems. The trend to distributed computing has significantly contributed to the complexity in security controls.

1.3 The maintenance of information security relates to the preservation of the confidentiality, integrity and availability of information, as described hereunder**:**

(a) Confidentiality of information relates to authorised access only to information and the controls put in place to ensure the same.

(b) Integrity of information relates to the safeguarding of the accuracy and the completeness of information including the associated processing methods.

(c) Availability of information means the accessibility to information, as and when required, by the authorised users only.

1.4 Each organisation has to identify its security requirements, which can be facilitated by addressing the following :

a) Risk Assessment to identify the threats to information and information assets. Their vulnerability to security threats and the likelihood of the occurrence of such threats. The potential impact of such threats on the business of the organisation.

b) The legal, statutory, regulatory and contractual requirements, which an organization, its trading partners, contractors and service providers have to comply with.

c) The principles, objectives and requirements for information processing, which an organisation may have developed to support its business operations.

1.5 The security controls to be put in place require to be identified by a methodical

assessment of risks. The expenditure on the security controls need to be balanced against the business hardships, which are likely to result from security failures. The risk assessment techniques require to be applied to the whole organization or only parts thereof including individual information systems, specific components of such systems or services. In fact, risk assessment is a systematic consideration of the business hardships, likely to result from security failure, togetherwith the potential consequences of the loss of confidentiality, integrity or availability of information and the information assets and the realistic likelihood of the occurrence of such failure in the light of the prevailing threats and vulnerabilities vis-à-vis the security controls currently implemented in the organisation.

1.6 The results of this assessment will help guide and determine the appropriate management action, the priorities for managing the information and the information systems security risks and for implementing security controls, selected to protect the organisation against such risks. The process of assessing the risks and the selection of the security controls may require to be performed a number of times to cover different parts of the organization or the individual information systems and services. It is also important to carry out periodic reviews of the security risks and the implemented security controls in view of new threats and vulnerabilities and to confirm that the security controls in place are effective and appropriate. The reviews will require to be performed at different levels of depth, depending on the results of the previous assessments and the changing levels of risk, which the management of the organisation is prepared to accept. The risk assessments will require to be carried out first at a high level for prioritising the information and the information assets in the areas of high risk and then, at a more detailed level to address specific risks.

1.7 Many information systems in operation in an organisation may not have been designed to be sufficiently secure. Further, the level of security, which can be achieved through the application of technology, could also be limited and therefore, it requires to be supported by appropriate **management policies and procedures**. The selection of the security controls requires careful and detailed planning. The management of information and information systems security will require **participation by all the employees in an organisation**. It will also require **participation from the third parties such as the suppliers, vendors, customers and shareholders**. The organisation **may also have to turn to specialist advice** in the matter of information systems security, as and when required. The information systems security could be achieved by implementing a suitable set of controls **which consists of policies, practices, procedures, organisational structures, hardware and software functions.** Each organisation has to establish these controls to ensure that its security requirements are met.

1.8 The Board of Directors/Management of each organisation has the responsibility for ensuring appropriate corporate policies, which set out the management responsibilities and the control practices for all the areas of information processing activities. A well-defined corporate security policy has to be put in place and periodically reviewed and amended, as required, under the approval of the Board of Directors/Management of the organisation.

1.9 The management of risks is central to the organisation in the banking and financial sector. These organisations manage risks through prudent business practices, contractual arrangements with third parties, obtaining insurance coverage and use of appropriate security mechanisms. These organisations have now been increasingly dependent on the Information Technology (IT) for the efficient conduct of business, which necessitates growing levels of information systems security within the organisations. **This report contains the guidelines for building up an "Information Systems Security Programme"**

by an organisation in the banking and financial sector.

The objectives of this report are :

a) to provide a structure for the information systems security ;

b) to provide a guide to security controls, procedures and practices ; and

c) to be consistent with the existing and emerging needs of information systems security.

1.10 The objective is to produce a comprehensive document to facilitate the creation of effective security for ensuring confidentiality, integrity and availability of information and the information systems by the banking and financial organisations. However, the **recommendations in this document should be considered as the bare minimum security requirements only and it is suggested that the banking and the financial organisations may have to endeavour to strengthen the same continuously in view of the ever increasing complexity in security threats to information and information systems.**

Chapter 2
Executive Summary

2.1 The Board of Directors/Managements of the banks and the financial organisations are responsible for putting in place effective security controls for protecting information assets, as the confidentiality, integrity, authenticity and timely availability of such information is of paramount importance to business operations. It is, therefore, critical for such organisations to protect the information and information systems from unauthorised disclosure, modification, replication, destruction and access. Built-in safeguards and controls should be put in place to save information and the information systems from the unauthorised persons, hackers etc.

2.2 The business operations in the banking and the financial sector would be increasingly dependent on computerised information systems in future. It has now become impossible to separate technology from the business of the banks/financial organisations. The growing use of the personal computers and their networking in the financial sector has necessitated their integration in a Local Area or Wide Area Network environment. In many organisations, most of the work is still done on the standalone personal computers and those integrated with intra-city networks including LANs than on large mainframe systems. The security controls for these computer systems and networks are not as developed as the security controls available for the mainframe systems. On account of the phenomenal growth in the use of IT and IT based applications by these organisations in their day-to-day operations, the need for putting in place the security controls for all the information systems has grown tremendously. The information systems security has, therefore, assumed great importance for the commercial success of an organisation, as the survival of the organisation depends on the speed, accuracy and reliability of the flow of information within the organisation vis-à-vis its customers.

2.3 The security controls are required to minimise the vulnerability to unauthorised use of the information and the information systems. However, such controls may have to be consistent with the degree of exposure of such systems and the information and the impact of loss to the organisation on account of unauthorised access and misuse, including accidental misuse, of such systems and information. The unauthorised including accidental misuse of the information may result in financial loss, competitive disadvantage, damaged reputation, improper disclosure, law suits and non-compliance with the regulatory provisions etc. **Structured, well defined and documented security policies, standards and guidelines lay the foundation for good information systems security and are the need of the hour.**

2.4 No threat becomes obsolete. Further, new threats surface from time to time. The financial sector has witnessed rapid changes in the volume and the value of transactions and

the introduction of the most modern and secured methods for the delivery of services to the customers. Still better information systems are being introduced at frequent intervals. Further, the banking and the financial sector is now poised to countenance various developments such as Internet banking, e-money, e-cheque, e-commerce etc., which have been made possible by the revolutionary researches and discoveries in Information Technology and its applications and the future promises to remain challenging. Constant developments of far reaching implications dictate constant vigilance and necessitate sound information systems security programme. Constant Vigilance and the extensive and proper implementation of the information systems security programme in an organisation are the minimum requirements for the organisation's competitiveness and continued contribution to economic growth.

Chapter 3

Ensuring Security In Bankig and Financial Sector - Implementation of Information Systems Security Programme

3.1 The acceptance of ethical values and adoption of security control measures may have to be communicated by the highest level of the organisation (Board of Directors) to its management and staff. The prudential control over the information assets of an organisation constitutes a sound business practice. The protection of the information on the key business processes is critical for protecting the business processes, which are very critical to an organisation. Therefore, the security requirements should be carefully examined at each stage of the business process in the organisation.

3.2 The development, maintenance and monitoring of an information systems security programme requires wholehearted participation by the functionaries in various disciplines in an organisation such as business operations, audit, insurance, regulation compliance, physical security, training of personnel and their deployment, legal etc. There has to be close co-ordination between the business manager and the information systems security manager. The maintenance of the Information systems security is basically a team effort and it is the responsibility of each and every individual in an organisation to ensure its proper implementation and observance.

3.3 The information systems security programme should include an organisation-wide information systems security policy and a statement containing the following :

a) a statement that the organisation considers information in any form to be an important asset;

b) an identification of risks ;

c) the requirements/procedures/processes for the implementation of the security controls and practices;

d) an assurance that the information assets are protected and that the organisation continuously endeavours to beef up the security controls/measures against the ever increasing threats thereagainst;

e) a well-defined procedure on the responsibilities of each manager, employee and the related third parties for the maintenance of information systems security; and

f) a commitment to security awareness and education among the employees in the organisation irrespective of cadres and grades.

In addition to the above, the information systems security programme must also deal with the following :

a) At the apex level, a Senior Executive should be responsible for Information Systems Security. He will be assisted by one or more officer(s) to be responsible for the information systems security programme in each of the offices/locations of the

organisation. If so required, there may be an Information Systems Security Department in each organisation to address various issues such as the development of the Information Systems Security Policy, updation of the Information Systems Security Guidelines on an on-going basis, provision of consultancy and information on information systems security requirements, maintenance of centralised security functions etc. Further, the System Administration responsibilities should, among others, relate to the implementation of the security controls, compliance with the information systems security guidelines, management of day-today security functions etc.

b) Identification of individuals to be responsible for the protection of information assets at each office/location of the organisation or as warranted;

c) Classification of information assets and specifications of the appropriate levels of security for each class of information assets;

d) Implementation of an awareness/education programme to ensure that the employees and the related third parties are aware of and observe their respective responsibilities for the maintenance and continuation of information systems security in the organisation;

e) Reporting of information systems security incidents and provision for their resolution;

f) Preparation of written (comprehensively documented) plans and procedures for business resumption/continuity following disasters;

g) Identification of the procedures and the processes for addressing exceptions or deviations from the information systems security policy document ;

h) Co-ordination and co-operation among the various disciplines in the organisation such as technical, operational, audit, insurance and regulatory compliance ;

i) Laying down precisely the responsibilities to ensure compliance with and to assess soundness and comprehensiveness of the information systems security programme on a continuous basis ;

j) Review, updation and upgradation of the information systems security programme in the light of new threats and technology on a continuous basis ; and

k) Preparation of the audit records, where necessary and the monitoring of the audit trails for the detection of uncharacteristic behaviour of individuals and activities.

3.4 The Information Systems Security Managers will serve as the supervisors and have to, therefore, monitor the successful implementation of the Information Systems Security Policy within their work-areas. This makes them key players in the information systems security programme. It is, therefore, essential that each Information Systems Security Manager should:

a) understand, support and abide by the organisation's information systems security policy, standards and directives ;

b) ensure that the employees and the related third parties understand, support and abide by the information systems security policy, standards and directives;

c) implement information systems security controls, consistent with the requirements of business and prudent business practices, obtaining in the organisation ;

d) create a positive atmosphere that encourages employees and the third parties to report information systems security concerns/ incidents to the Information Systems Security Manager immediately;

e) participate in the information systems security communication and awareness programme ;

f) apply sound business and security principles in preparing the exception requests;

g) define realistic business and security principles in preparing exception requests;

h) define realistic business "need-to-know" or "need-to-restrict" criteria to implement and maintain appropriate access controls and identify and obtain resources, necessary to implement these tasks ;

i) ensure that information systems security reviews are undertaken, whenever required, by the concerned functionaries. The circumstances that should trigger such a review illustratively include the following :

? material/large loss from a security failure ;

? appearance of bugs in the software all of a sudden;

? preparation of an annual report to the Board of Directors and Audit Committee (relevant authority as per the systems and procedures in the organisation) ;

? acquisition of a financial organisation ;

? purchase or upgradation of computer systems, either hardware or software, or both ;

? introduction of a new financial product ;

? appointment of a new external processing third party ; and

? discovery of a new threat or a change in an existing threat's direction, scope or intent.

3.5 All business information should have an identified "owner' and the ownership of information should be established as per the procedures laid down therefor in this document. The 'owner' of the information should also be responsible for :

a) classification of information or information processing systems under his control;

b) defining the security requirements for his information or information processing systems ;

c) authorizing access to information or information processing systems under his control ;

d) informing the Information Systems Security Officer of the access rights ; and

e) keeping the information on access rights up-to-date.

3.6 The employees and the third parties such as the suppliers, vendors, contractors and shareholders (if any) should:

a) understand, support and abide by the information security policies, standards and directives of the organization and the associated business unit;

b) be aware of the security implications of their actions ;

c) promptly report any suspicious behaviour or circumstances, which may threaten the integrity of the information and/or information assets ; and

d) keep the organisation's information confidential. This especially applies to the contractors, vendors and suppliers with several organisations being their customers. This includes internal confidentiality requirements as per the terms and conditions relating to Confidentiality, specified in the Service Agreement/ Employment Contract, signed by the organisation with them.

3.7 Legal Function :

Each organisation has to ensure compliance with the legal requirements and keep track of the modifications/additions to the legal requirements, as prescribed by the concerned authorities. Each organisation will have to take care of the following :

a) monitor changes in the law through legislation, regulation and settled court cases that may affect the information systems security programme of the organisation;

b) review contracts concerning employees, customers, service providers, contractors, vendors and any other third party to ensure that the legal issues relating to information systems security have been duly taken care of ;

c) render advice with respect to the security breach incidents ; and

d) develop and maintain procedures for handling security threats including the preservation of evidence thereof etc.

3.8 Information Security Officers :

An Information Security Officer could be a senior official or a group of officials entrusted

with the design, development, implementation and maintenance of the Information Systems Security Programme for protecting the information and the information assets of the organisation. There could be one or many information security officers in an organisation, as warranted by the size and spread of the organisation. In case of the need for many information security officers, every organisation should have a Chief Information Security Officer with supervisory, administrative and regulatory powers in regard to the other information security officers in the organisation.

The information Security Officer/s will have to:

a) manage the overall information systems security programme in the organisation;

b) be responsible for developing the Information Systems 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 ;

c) assist business units in the development of specific standards or guidelines that meet the information security policies for specific products within the business unit. This requires working with the business managers to ensure that an effective process for implementing and maintaining the security controls is in place ;

d) ensure that, when exceptions to the information security policy are necessitated, the risk acceptance process is completed and the exceptions are reviewed and re-assessed periodically ;

e) remain current/up-to-date on the threats against the information assets. Attending information security meetings, reading trade publications and participation in work groups are some of the ways to stay current/up-to-date with the developments in the field of information systems security ;

f) 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 ;

g) understand the business processes of the organisation, so as to provide appropriate security protection ;

h) apply management and organizational skills and knowledge of the business in the execution of their duties ;

i) encourage the participation of the managers, auditors, insurance staff, legal experts and the staff members from other disciplines, who can contribute to the information systems security programme;

j) review audit and examination reports dealing with the information security issues and ensure that they are placed before the Board of Directors/Management of the organisation at pre-determined intervals. The information security officer should be involved in the formulation of the management's response to the audit findings and follow-up to ensure that the security controls and procedures, as required, are implemented within the stipulated time frame ;

k) confirm that the key threats to the information assets have been defined and understood by the management of the organisation ;

l) assume responsibility or assist in the preparation and distribution of an appropriate warning system of potentially serious and imminent threats to the organisation's information assets e.g. outbreak of computer virus etc. ;

m) co-ordinate or assist in the investigation of security threats or other attacks on the information assets ;

n) assist in the recovery of information and information assets from such attacks; and

o) assist in responding to the security issues relating to the customers including the letters of assurance and suitable replies to the questions on information systems security, as and when raised by the customers.

3.9 Information Systems Security Administration :

Each business unit and information systems manager should lay down the need-to-know access privileges for the users within his business domain and communicate the same to the users. These access privileges should be documented. Further, these documented privileges should be reviewed periodically and changes should be made as and when deemed appropriate.

3.10 Each information access control system should have one or more Information Systems Security Administrator(s), appointed to ensure that the access control procedures are being monitored and enforced continuously. The Information Systems Security Administrator should:

a) be responsible for maintaining accurate and complete access control privileges, based on the instructions from the information resource owner and in accordance with any applicable internal policies, directives and standards, laid down therefor;

b) remain informed by the appropriate manager/s whenever the service of the employees is terminated or they are transferred or retire or are on leave or when have joint responsibilities, if any ;

c) monitor selected users with high-level access privileges and remove such privileges immediately, when such privileges are no longer required ;

d) 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 the availability of information and the information systems. These unusual activities, whether intentional or accidental, must be brought to the attention of the information resource owner for investigation and resolution;

e) ensure that each information 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 the user's gaining access to the information system by utilizing an established/properly chosen authentication technology;

f) make periodic reviews on access to information systems by the users and report to the appropriate information resource owner ; and

g) ensure that the audit trail is collected, protected and available, whenever required.

3.11 The activities of the Information Systems Security Administrator/s (ISSA) have to be reviewed by an independent party, appointed by the management of the organisation for the purpose, on a routine basis.

3.12 Risk Acceptance :

The business managers will have to abide by the information systems security policy, standards and directives, issued by the organisation. If any business manager believes that the circumstances or any particular situation prevents him from operating within the laid down information systems security policy, standards and directives, he/she should either :

a) undertake steps to observe compliance, as required, as soon as possible, under proper intimation to the information systems security officer ; or

b) seek an exception from the information systems security officer, based upon risk assessment of the special circumstances/situations involved.

3.13 The Information Systems Security Officer will have to participate in the preparation of the compliance plan or exception request for submission to the appropriate authority in the organisation for decision/approval. The Information Systems Security Officer will also have to consider changes to the information systems security programme, whenever the exception procedure reveals situation/ s, which had not been previously addressed.

3.14 Insurance :

In planning the information systems security programme, the Information Systems Security Officer and the business manager should consult the insurance department and if possible, the

insurance service provider. This will result in a more effective information systems security programme.

3.15 The insurance service provider/s may require that certain controls, say conditions prior to liability or conditions precedent, will have to be met before a claim could be honoured. The conditions prior to liability often deal with the proper observance of the information systems security controls. Since these security controls must be in place for, among others, insurance purposes, they should be incorporated into the organisation's information systems security programme. Some controls may also require to be warranted i.e. to be shown to have been in place continuously since the implementation of the information systems security programme. The coverage of business interruption and that of the errors and omissions, in particular, will have to be integrated with the information systems security programme.

3.16 Audit :

Internal audit is an independent appraisal function, established within an organization, to examine and evaluate its activities, as a service to the organization. The objective of internal auditing is to assist the members of the organization in the effective discharge of their responsibilities. To this end, internal auditing furnishes with the analyses, appraisals, recommendations, counsel and information concerning the activities reviewed, so that necessary corrective/preventive action could be taken to ensure that the activities of the organisation continue, conforming to the procedures/guidelines/prescriptions, as laid down therefor.

The auditors of information systems security should :

a) evaluate and test the security controls, implemented for the confidentiality, integrity and availability of the information and the information assets against internationally accepted standards;

b) engage in an on-going dialogue with the Information Systems Security Officer and others, associated with the security of the information and the information assets, to bring in appropriate perspectives to the identification of threats, risks and adequacy of the security controls and procedures in place, both for the existing and the new products/assets ;

c) provide the management of the organisation with objective reports on the condition of the controlled environment in respect of the security for information and information assets and recommend changes, improvements etc., if any, which can be justified by the need and the cost-benefit criteria therefor ; and

d) specify the retention and review of the audit trail information.

3.17 Where the audit review function relating to the information systems security is combined with such other functions, the management of the organisation is required to put appropriate system/procedure in place, so that the conflict of interest on account of the conduct of the combined activities could be either eliminated or minimised. Further, the Information Systems Audit has to be performed by persons with suitable skills/expertise therefor, say CISA (Certified Information Systems Auditor) or CISSP (Certified Information Systems Security Professionals) personnel.

3.18 Regulatory Compliance :

The Regulatory Authorities concern themselves principally with the issues of safety, soundness and compliance with the laws and regulations. One measure for the safety and soundness is the control system, the organisation has put in place, which facilitates the availability of/access to information to the authorised persons only in the organisation and protects the same from unauthorized modifications, disclosures and destruction.

The Regulatory Compliance Officer/s will have to work with the Information Systems Security Officer/s, business managers, risk control managers and the Information Systems

Auditors to ensure that the regulatory requirements for the information systems security are understood and implemented. The Regulatory Compliance Officer/s will have to remain current/up-to-date on the new technologies or methodologies, which may come under the subject of regulation.

3.19 Disaster Recovery Planning :

An important part of an Information Systems Security Programme is a comprehensively documented plan to ensure the continuation of the critical business operations of the organisation in the event of disruption. A disaster recovery plan outlines the roles and responsibilities under such situations and the system/procedures to be adopted for business continuity.

3.20 The disaster recovery is that part of the business resumption plan which ensures that the information and the information processing facilities are restored to their normal operating conditions as soon as possible after disruption. The disaster recovery plan should include the following:

a) listing of business activities which are considered critical, preferably with priority rankings, including the time frame, adequate to meet business commitments ;

b) identification of the range of disasters that must be protected against ;

c) identification of the processing resources and locations, available to replace those supporting critical activities ;

d) identification of personnel to operate information processing resources at the disaster recovery site;

e) identification of information to be backed up and the location for storage, as well as the requirement for the information to be saved for back-up purpose on a stated schedule and compliance therewith;

f) information back-up systems being capable of locating and retrieving critical information in a timely fashion ; and

g) agreements entered into with the service providers/contractors/ vendors for priority resumption of services under the terms and conditions specified therefor therein.

3.21 The disaster recovery plan will have to be tested as frequently as necessary, as per the terms and conditions specified therefor in the agreement/ s with the service providers/contractors/vendors, to find problems, if any in the execution of the plan as also to keep the personnel trained therefor and in the operation of the back-up system. The record of each of these exercises should be documented, submitted to higher-ups and preserved. A periodic re-evaluation of the disaster recovery plan, to ascertain that it still serves the purpose, will have to be undertaken. A minimal frequency for both the testing of the disaster recovery plan and the re-evaluation exercise of its appropriateness/suitability will require to be specified by the Organisation. The agreement/s with the service providers/contractors/vendors will have to include the terms and conditions for switch-over to the primary system on the resolution of the problems thereat. Further, if the implementation of the disaster recovery plan requires close co-ordination among various service providers/contractors/vendors, the terms and conditions, warranting close co-ordination & co-operation among them, will have to be specified in each relevant agreement, setting out the obligations to be met by each of the service providers/contractors/vendors including the penalties/punitive measures in case of non-compliance.

Chapter 4

Information Systems Security Awareness Programme and Third Parties

4.1 The goal of an Information Systems Security Awareness Programme is to promote

information systems security awareness among all concerned. The programme is meant to influence in a positive manner the employees' approach towards Information Systems Security. The security awareness, among all concerned, requires to be addressed on an on-going basis.

4.2 The success of any Information Systems Security Programme is directly related to the Information Systems Security Officer's ability to gain support and commitment from all categories of employees within the organization. The failure to gain this support reduces the programme's effectiveness. There should be clear directions from the Board of Directors/Management of the organisation regarding the Information Systems Security Programme including the role and responsibility of different functionaries/individuals in the organisation.

4.3 The Information Systems Managers will have to be made aware of the exposure, risks and loss potential as well as regulatory and audit requirements. To function properly, the Information Systems Security Programme must achieve a balance between the security controls and accessibility to information and the information assets. Both the staff and the management must be made aware of this requirement. It will have to be ensured that the users are given sufficient access to perform their required official functions. However, they should never be given unrestricted access.

4.4 The Information Systems Security Programme must be so structured and documented as to support the work environment to which it applies. The Information Systems Security staff must not operate in a vacuum. They must understand the business objectives, the internal operations and the organizational structure of the institution to be able to protect information and information systems better and to periodically advise the organisation in the matter. By working in co-ordination with the other groups in the organisation, a co-operative spirit would evolve, which will benefit one and all in the organisation and the organisation itself.

4.5 External Service Providers :

The Organisation will have to ensure that the externally provided critical services such as data processing, transaction handling, network service management, maintenance and software development and modifications, if any, receive the same levels of security controls and information protection as the data processed / activities performed within the organisation itself. The agreement entered into with the service providers/contractors/vendors will have to, among others, contain terms and conditions to satisfy the following requirements:

a) the external service provider must in all cases abide by the security policies and standards adopted by the Organisation ;

b) the third party reports i.e. the reports prepared by the service provider, should be available to the Information Systems Security Manager alongwith the relevant departments/divisions/wings in the Organisation ;

c) the internal auditors from the Organisation shall have the right to conduct an audit of the procedures and security controls, adopted by the Service Provider, for ensuring conformity to the procedures and security controls, as specified by the Organisation ; and

d) Escrow arrangements for all such products, both hardware and software, in the country or as the case may be, whose ownership can not be transferred to the Organisation.

4.6 An independent financial review of the service provider requires to be conducted by the specialists in the Organisation before entering into a contract with the Service Provider. If expertise/skills are not available in-house for the purpose, the review should be conducted with out-sourced expertise/skills under well documented terms and conditions.

4.7 No business should be transacted with a service provider unless a letter of assurance is obtained stating that the required information security controls and procedures are in place

with the service provider. The Information Systems Security Officer should examine the Service Provider's information systems security programme to determine if it is in conformity with that of the organisation. Any inaccuracy/ies or inadequacy/ies should be resolved either through negotiation with the service provider or by the risk acceptance process within the organisation.

4.8 In addition to the information systems security requirements, the contract/ s with the service provider/s will include the confidentiality clause and clear assignment of liability for loss resulting from information security lapses, if any, for which the service provider is solely responsible.

4.9 Internet Service Provider :

The Internet has made spectacular progress in the coverage of geographical area and subscribers across the world. However, this networking environment is associated with new types of risk to the banking and financial sector. The Internet is the world-wide collection of inter-connected networks. It uses Internet Protocol (IP) to link various physical networks into a single logical network. The risks of a public network such as the Internet are many because security was never a design consideration during its evolution and therefore, needs to be retro-fitted. The security features, provided by the operating systems and applications ensure better protection than the one that is added later on. The following are, among others, the major security risks/concerns, which the operating systems alone may not be able to address and specific security applications such as firewalls, Intrusion Detection System etc. will, therefore, have to be implemented therefor.

a) Address spoofing which allows someone to impersonate and thereby, making the messages untrustworthy.

b) Integrity of the message being threatened by the ability to change the contents of the message, either while in transit or after it has reached the recipient-destination.

c) Theft of information where the original message is left unaltered, but information such as credit card numbers etc. is stolen.

d) Denial-of-service-attacks where persons are able to flood an Internet node with automated mail messages, called spamming, which may eventually shut down the Internet node.

4.10 Internet Connectivity : There are several ways through which one can have Internet connectivity. The first is to have a direct connection to the Internet from a computer through Serial Line Internet Protocol (SLIP) connection or a Point-to-Point Protocol (PPP) connection. Both these methods cause the greatest risks to the Organisation's internal network/s because they provide a Peer-to- Peer connection. In other words, the systems and/or networks outside the organisation become a part of its internal network/s and enjoy access to any of the organisation's network resources, unless prevented through security barriers such as Proxy Servers, Firewalls etc. The second method is to procure a connection from an Internet Service Provider who will provide access to the Internet. However, the external systems/networks will have connectivity with the Systems of the Internet Service Provider only and not with the internal network/systems of the Organisation.

4.11 Selection of Internet Service Provider : While selecting an Internet Service Provider for Internet connectivity, the factors such as the safeguards/ security measures, deployed by the Internet Service Provider to prevent access by the external systems to the organisation's internal network/systems must be duly considered in addition to the cost requirements for such connectivity. Some Internet Service Providers offer complete turnkey operations, where all the security equipment/products are operational at their sites and are managed by them. Under such circumstances, they monitor the security violations, if any and alert the subscriber-organisations to such incidents. The agreement between the Internet Service Provider and the Subscribers governs the relationship between them.

4.12 Before procuring the Internet connectivity from the Internet Service Provider, the Organisation should conduct a thorough review of the Internet Service Provider to ascertain the details of access to the computer systems and the firewall, which provide the gateway to the Organisation's internal network/s. It should be ensured that only the barest minimum of the Internet Service Provider's staff have access to these computer resources and that such access privileges are closely monitored by the Internet Service Provider on a regular basis. If the Organisation does not have the necessary in-house skills to conduct the review, the services of a third party with suitable skills and expertise for the purpose and not related to the Internet Service Provider, may be engaged to conduct the security review concerning the Internet Service Provider and the organisation must ask for a written report of the findings from the third party, which the Organisation should use to negotiate changes with the Internet Service Provider before entering into the required agreement for obtaining Internet connectivity.

4.13 Penetration Attempt – Regular Penetration-Prevention Exercise:

The use of a third party to test the information systems security of the organisation by attempting penetration into the Information Systems, with the knowledge and consent of the appropriate official/s of the organisation, could be considered as a penetration-prevention exercise for ensuring adequacy of the information systems security programme in place and taking necessary steps to plug loopholes, if any. Such an exercise has to be carried out at regular intervals to ensure the adequacy of the information systems security programme. As the computer systems become more and more complex, the security requirements will become increasingly harder to maintain. The use of such a third party can help find specific points of weakness in an organisation's Information Systems Security Programme. While adopting this methodology, the Organisation will have to duly consider the following :

a) The Organisation should enter into an agreement with the selected third party, which must contain, among others, the terms and conditions for confidentiality of information and prohibitive penalties/ liabilities in the event of breach of agreement by the third party. Further, the terms and conditions will have to also ensure that the third party unfailingly advises the organisation about the emerging security concerns during the currency of the agreement/contract.

b) The organisation should not rely solely on the third party's report on the findings of the penetration exercise to review and address the shortcomings in its Information Systems Security Programme.

The Organisations should endeavour to develop necessary in-house skills/expertise for the purpose also.

4.14 Electronic Money :

Recent advancements in the smart card technology and cryptography have enabled the organisations to issue tokens which are capable of storing and exchanging value. The organisation should consider the following and take necessary action before participating in the Electronic Money Programme.

4.14.1 Disclosure: How much information is to be made available to the customers and how? Compliance with the regulatory requirements, if any, in regard to the issues of liability, refund policy in case of loss, malfunction or theft, privacy expectations and other similar issues.

4.14.2 Capacity: How much can be stored in a token ? Can the token be refilled ? How are limits to be enforced ? Compliance with the requirements in place.

4.14.3 Privacy: Restrictions on the collection of information for marketing purposes on the purchase by the customers and compliance therewith.

4.14.4 Law Enforcement Concerns : Measures taken/provisions put in place to prevent money laundering, which may be facilitated by an unlimited value refillable, untraceable,

anonymous electronic cash system and compliance therewith.

4.14.5 Record Keeping: If the electronic money is to be refundable, the Electronic Money System will have to be capable of tracing the transactions and compliance with the methodology put in place therefor including the maintenance of records to facilitate refund. Compliance with the privacy, accountability and legal requirements is in place.

4.15 Cryptographic Operations :

4.15.1 Threats against confidentiality and integrity of information can be countered/minimised by the implementation of appropriate cryptographic controls. Cryptographic controls such as encryption and authentication require that certain materials such as the cryptographic keys remain secret. One or more facilities that generate, distribute and account for the cryptographic materials may be required to support cryptographic controls.

4.15.2 The facilities providing the management of the cryptographic materials must 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.

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

4.15.4 Supply of cryptographic materials to customers should be done in a manner that minimizes the possibility of any compromise. The customers should be made aware of the importance of the security measures for the cryptographic materials. The inter-operation between a customer's correspondent's and the Service Provider's cryptographic systems should only be allowed under a fully documented letter of assurance and confidentiality of information.

4.15.5 The quality of security, delivered by the cryptographic products, depends on the continued integrity of these products. Both hardware and software cryptographic products require integrity protection, consistent with the level of security they are intended to provide. The use of appropriately certified integrated circuits, anti-tamper enclosures and key zeroing make hardware systems some what easier to protect than software. Where circumstances allow, software cryptographic products may be used. The features that enhance system integrity such as self-testing should be employed to the maximum possible extent.

4.15.6 The cryptographic products, their implementation/use and the systems/ procedures/methodologies therefor may be subject to varying governmental regulations relating to import and export and such regulations will have to be complied with.

4.16 Privacy/Confidentiality :

4.16.1 The financial organisations possess some of the most sensitive information about individuals and organizations. The 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 may raise concerns about the adequacy of the privacy protection measures adopted by the Organisation.

4.16.2 The financial organisations should review all privacy laws and regulations which involve credit information.

4.16.3 The organisation should continuously update itself on the developments/ changes relating to the national privacy legislation, either through its law offices, industry sources or other independent information sources. In addition, the organisations, which have international operations, need to be aware of the applicable regional, international and other privacy laws and regulations and necessary compliance therewith.

4.16.4 The organisations should review their business operations from time to time to assess whether the information on their customers and employees are adequately protected. The

organisations will have to put in place specific policies and procedures concerning how the information is gathered, used and protected. These policies and procedures should be made known to the relevant employees/ customers. The privacy policies and procedures of the organisations should address the following requirements:

a) Collection of information to ensure that only information, which is relevant and accurate to an identified business need, is to be collected.

b) Provision for appropriate access controls including decision on who should have access to information and the extent of accessibility, quality control to avoid errors in data entry or processing and protection against inadvertent and unauthorized access.

c) Sharing of information through pre-determined procedures, use of the information for the purposes relevant to the reasons for its original collection and ensuring that such sharing of information does not lead to new opportunities for unauthorized privacy invasion by other parties.

d) Methodology adopted for the storage of information to ensure that it occurs in protected fashion to disallow unauthorized access.

e) Notification of the use of the information and the availability of procedures which allow the person, whose information is being held, to correct errors and to raise objections, if any, over the use of the information or any part thereof.

f) Secure destruction of information, when no longer needed.

4.16.5 In addition, the methodology adopted for monitoring the collection, use and storage of information, either electronic or in any other form, must meet the legal requirements. The organisation will also require to develop a privacy audit. This audit will evaluate how well the organisation is achieving privacy protection and explore ways by which Information Technology can address the privacy concerns.

Chapter 5

Security Controls and Procedures/Methodologies

5.1 The security controls to be adopted, among others, to ensure the availability of information, the information processing resources and to prevent unauthorized modifications, disclosures or destruction of information, are mentioned hereunder:

a) Classification of Information

b) Access Control

c) Audit Trails

d) Change Control Mechanism

5.2 The assessment of the vulnerabilities in the Information System Resources and the risks which arise therefrom are an integral part of any Information Systems Security programme. The process of risk assessment is a method for formulating the policies and selecting the safeguards to protect information and information system assets from security threats occurring through the vulnerabilities, inherent in the personnel, facilities and equipment, communications, applications, environmental conditions, operating systems and applications. The risk assessment should be done by assessing the security threats relating to the above vulnerabilities and based on the impact of the occurrence, assigning a high, moderate or low risk to the particular vulnerability. In this way, the possibility and the magnitude of monetary loss, productivity loss and embarrassment to the organisation can be minimized. It is important that the organisation addresses all the known threats prudently/judiciously. The implementation of the security controls, the execution of the

insurance policy and the recognition and acceptance of the risks are preferable to ignoring the security threats, existing and the likely future ones.

5.3 Classification of Information :

5.3.1 Not all information in an organisation requires maximum level of security control. The methodology for identifying which information requires comparatively lower, middle and higher level of security control should be implemented. Information can be classified on the basis of its criticality and sensitivity to business operations.

5.3.2 The criticality of information is the requirement that the information be available when and where required for the continuity and survival of business operations. The criticality of the information is directly related to the criticality of the processes accessing the information. The contingency/disaster recovery programme provides classification of the processes. The same categorisation/ classification should be applied to information also. The information which is classified as 'CRITICAL' requires certain controls to ensure its availability with integrity, whenever required.

On the basis of criticality, Information could be broadly classified as under :

ESSENTIAL :

Information or information processing capacity/asset, whose loss would cause severe or irreparable damage to the organisation.

IMPORTANT:

Information or information processing capacity/asset, whose loss would cause moderate, but recoverable damage to the organisation.

NORMAL :

Information or information processing capacity/asset, whose loss would represent minor disruption in the business operations of the organisation.

5.3.3 Information sensitivity is specified in very broad terms as a measure of how mishandling of such information may impact the organisation. The question which may be addressed while categorizing sensitive information is, "What is the possible impact on the organisation of unauthorized modifications, disclosures or destruction of the information and what is the probability of the occurrence with such sort of impact ?" The areas to consider, while evaluating the impact, include the effect on the organisation's credibility, profitability and customer confidence as well as compliance with the regulatory and legal requirements.

5.3.4 The following procedure may be adopted for the classification of information. The primary reason for classifying the information is to communicate the management's expectations of how the employees are required to handle the same. If a document, file or database contains various classifications, it must be according to the highest category of information classification it contains. The classification of any information may also change during the useful life of that information. It is, therefore, required that the change in the classification of information has to be an authorised one.

HIGHLY SENSITIVE:

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

SENSITIVE:

Information which, if mishandled, may cause significant damage to the organisation. It is sensitive to both internal as well as external exposure. Examples may include internal personnel information, customer information and departmental budgets or staffing plans.

INTERNAL:

Information, which is sensitive to external exposure only and any unauthorised disclosure would cause embarrassment or difficulty to the organisation. Examples may include internal memos, telephone books and organizational charts.

PUBLIC :

Information which has been expressly approved for release to the public. Note that the public information never originates as 'PUBLIC', but is re-classified as such when it is released. Examples are the annual report, other publications and new products.

5.4 Business Requirements & Access Control Policy :

Access to information and business processes require to be controlled on the basis of business and security requirements. The access control system, required to be put in place, should be in conformity with the policies for information dissemination and authorization in the organisation. The business requirements for access control should be defined and documented. The access control rules and rights for each user or group of users should be clearly stated in an access policy statement. The users and the service providers should be given a clear statement of the business requirements to be met by access controls. The access control policy should take into account of the following:

a) security requirements of individual business applications;

b) identification of all information related to the business applications and the methodology for handling, controlling such information ;

c) policies for information dissemination and authorization e.g. the need-to-know principle, security levels and classification of information;

d) consistency between the access control and the policies for information classification of different systems and networks;

e) relevant legislation and any contractual obligations regarding the protection of access to data or services ;

f) standard user access profiles for common categories of job;

g) management of access rights in a distributed and networked environment which recognizes all types of connections available ; and

h) Implementation of Intrusion Detection System.

While specifying the access control rules, the following points should be considered :

a) Differentiation between the rules which must always be enforced and the rules which are optional or conditional.

b) Establishment of the rules based on the premise of "What must be generally forbidden unless expressly permitted" rather than that of "Everything is generally permitted unless expressly forbidden".

c) Changes in the information labels which are automatically initiated by the information processing facilities and those which are initiated at the discretion of a user.

d) Changes in the user permissions which are automatically initiated by the information system and those which are initiated by a system administrator.

e) Rules which require the approval of the system administrator or that of other appropriate authority/ies before execution and those which do not.

5.4.1 User Access Management :

Formal procedures should be put in place to control the allocation of access rights to the information systems and/or services. The procedures should cover all stages in the life-cycle of user access i.e. from the initial registration of new users to the final de-registration of users, who no longer require access to information systems and services. Special attention has to be paid, where appropriate, to the need-to-control the allocation of privileged access rights, which allow such users to override the system controls.

5.4.2 User Registration :

There should be a formal user registration and de-registration procedure for granting access to all multi-user information systems and services. The access to the multi-user information systems and services should be controlled through a formal user registration process, which should include the following :

a) Use of unique User Ids, so that the users can be linked to and be made responsible for their actions.

b) Use of Group Ids to be permitted where they are suitable for the work to be carried out.

c) Checking that the user has authorization from the system owner for the use of the information systems and/or services.

d) Checking that the level of access granted is appropriate to the business purpose and is consistent with the organisation's information systems security policy.

e) Giving users a written statement containing their respective access rights.

f) Requirement for the users to sign statements indicating that they understand the conditions of access.

g) Ensuring that no service provider provides access, if any, until the authorization procedure has been completed.

h) Maintenance of a formal record of all persons registered to use the information systems and/or services.

i) Immediate removal of access rights of the users who have changed jobs or left the organization.

j) Periodic checking for the redundant User Ids and Accounts and removal thereof.

k) Ensuring that the redundant User Ids are not issued to the other users.

l) Inclusion of terms and conditions in the staff contracts and the service provider contracts, which specify sanctions/penalties if unauthorized access is attempted by the staff or the service providers.

Each organisation should gradually introduce Identity Mapping, Role–based Approach and Single Sign-on.

5.4.3 Privilege Management :

The allocation and use of privileges (any feature or facility of a multi-user information system which enables the user to override the operating system or application controls) should be restricted and controlled. Inappropriate use of such system privileges is often found to be a major contributory factor to the failure/breach of the inforrmation systems security. Multi-user systems should have the allocation of privileges controlled through a formal authorization process. The authorisation process should include the following :

a) The privileges associated with each system product e.g. operating system, database management system and each application and the categories of staff to which they need to be allocated should be identified.

b) Privileges should be allocated to the individuals on a need-to-use basis and on an event-by-event basis i.e. the minimum requirement for performing their functional role only, when needed.

c) An authorization process and a record of all privileges allocated should be maintained. Privileges should not be granted until the authorization process is complete.

d) The development and the use of the system routines should be promoted to avoid the need to grant privileges to the users.

e) Privileges should be assigned to a different User Id from those used for normal business use.

5.4.4 Logical Access Control & Identification of Users :

It is the collection of all controls, used to ensure that only authorized persons will have access to information and/or information processing facilities for which they are authorized. The identification of the users focuses on the individuals. In some circumstances, a group of users may be required to share an identification and password. Under such circumstances, the local management must assume any responsibility arising from this shared use. When such a decision is taken, the term "individual user" may be interpreted to also include a group of users. Each organisation shall decide on the length of the password depending upon the class

of information under access. Further, the period for expiration of the password could be dependent upon the User privileges. All User Accounts in the system will be associated with an applicable, informative full name and description. Guest Account, if any, will require to be disabled. Temporary passwords to Users will be conveyed to such Users in a secure manner. The passwords will conform to the password construction standards. The passwords will have to be difficult to guess and unique to each User. To identify individual users of information and/or information processing facilities, the following procedure may be followed :

a) assign a unique user identification sequence (USERID) to each individual user of the information processing systems ;

b) hold each individual user accountable for all the activities performed under his USERID ; and

c) require that each use of an USERID be traceable to the individual who logs on to the information system.

To ensure that the unused or unneeded USERIDs are not used in an authorised manner, the following procedure may be followed :

a) suspend rights associated with an USERID after 'N' days of non-use (suggestion 'N'=number of days to be as decided by the organisation) and delete the USERID after 'N' days of suspension (suggestion 'N'=number of days to be as decided by the organisation). If it be so that the USERIDs are used quarterly only or as the case may be, longer time limits may require to be fixed. It will have to be ensured that the rights should remain suspended between the scheduled actions/ uses ; and

b) revoke the privileges assigned to the separated or transferred employees' USERIDs, immediately on their transfer, separation, dismissal or retirement.

5.4.5 Authentication of Users :

All the users including the technical support staff such as the operators, the network administrators, the system programmers, the database administrators and the system administrators should have a unique identifier (user ID) for their personal and exclusive use, so that the activities can subsequently be traced. User Ids should not give any indication of the user's privilege level e.g. manager, supervisor etc. In exceptional circumstances, where there is a clear business benefit, the use of a shared user ID for a group of users or a specific job can be used. Approval by the management/concerned authority should be documented for such cases. Additional controls may be required to maintain accountability. Bio-metric authentication technologies that use the unique characteristics or attributes of an individual can also be used to authenticate the user's identity.

Users may be internal or external to the organisation. The provision for the authentication of the user's identity requires the use of either static or dynamic passwords. The static passwords are those that are memorized by the user. They authenticate a person by something the person knows. The 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.

5.4.5.1 Password Management System : A good 'Password Management System' should ensure the following :

a) enforce the use of individual passwords to maintain accountability;

b) allow users to select and change their own passwords, where appropriate, and include a confirmation procedure to allow for input errors;

c) enforce a choice of quality passwords ;

d) force the users to change temporary passwords at the first log-on, where the users select the passwords ;

e) maintain a record of the previous user passwords, say, for the previous 12 months and prevent re-use of such passwords for a reasonable period of time;

f) non-display of the password on the screen when being entered;

g) store password files separately from the application system data;

h) store passwords in encrypted form using a one-way encryption algorithm; and

i) alter the vendor's/supplier's default passwords, following the installation of the hardware/software.

j) In case of Web based applications, http POST may be used for obtaining information from the users, which could be sensitive, personal or may compromise with the security of the applications.

5.4.5.2 USE OF STATIC PASSWORD : To ensure proper authentication using a static password, the following steps, among others, should be taken:

a) users to report known or suspected password compromises immediately ;

b) passwords to be chosen by the user ; and

c) assignment of an initial password that is to be changed by the new or the reinstated user on the first use thereof.

5.4.5.3 To minimize the chances that someone may acquire or guess a password, the following steps should be taken:

a) use of a minimum password length of 6 characters ;

b) change of the passwords at least once in 'N' days (suggestion 'N'=number of days as decided by the organisation) and enforcement by suspension of the USERID, if passwords are not changed ;

c) availability of distress passwords for sensitive operations. A distress password is a pre-arranged password, different from an user's usual password that is used to signal that the user is being forced or has to access the system under duress/abnormal circumstances;

d) passwords not to be shared, available or known to others, including the system administrator ;

e) instruction to the users not to choose passwords which can be easily guessed i.e. names or part of names, phone numbers, dates, common words or numbers. Use dictionary checking to restrict selection, if available. A dictionary, enhanced with organizational terminologies, would provide better checking ;

f) passwords to include both alphabetical and numeric components ;

g) no writing down of the passwords. Alternatively, the passwords may be subject to the handling procedures used for lock combinations ; and

h) protection of the password by encryption during transmission. The encryption mechanisms, which prevent successful replay of the encrypted passwords, should be used. However, mailing of passwords in uncontrolled and insecure environment should be strictly prohibited.

5.4.5.4 Maintenance of Static Password Integrity : To ensure the continued integrity of the static passwords, the following steps should be taken:

a) to use the current password prior to allowing a new password to become effective;

b) to prevent re-use of the user's last 'N' passwords (suggestion 'N'= number of passwords to be as decided by the organisation) ;

c) to prohibit change of password within 'N' days of previous change (suggestion 'N'= number of days to be as decided by the organisation) ;

d) to store passwords under irreversible encryption ; and

e) to prohibit the display of passwords on input, reports or other media.

5.4.5.5 Use of Dynamic Password System : To ensure proper authentication using dynamic password systems, the following steps should be taken :

a) to select authentication tokens that require either an user-changeable personal identification number (PIN) or the activation of biometric data ;

b) an user's PIN is different from the USERID ;

c) to prohibit the token PINs from being shared ;

d) the minimum token PIN length to be of 'N' characters (suggestion 'N'= number of characters to be decided by the organisation) ;

e) the length of the generated password be of minimum 'N' characters (suggestion 'N'= number of characters to be decided by the organisation) ;

f) the randomly generated passwords be used only once ;

g) the generated passwords can not be easily guessed ;

h) the keys and the other information 'CRITICAL' to authentication be encrypted within the token and on the validating system ;

i) the security tokens be resistant to tampering and duplication ;

j) the token gets locked after 'N' invalid PIN entries (suggestion 'N'= number of invalid attempts to be decided by the organisation) ;

k) to maintain an inventory control on security tokens ;

l) the employees sign for security tokens on a form which contains details of the acceptable uses and the consequences for misuse ;

m) to recover dynamic tokens from the employees upon reassignment or termination. Alternatively, to ensure termination of the access rights, associated with the token assigned to such employees ; and

n) to consider the use of bio-metric features with security tokens.

5.4.6 Limiting Sign-on Attempts :

The following should be implemented for detecting unauthorized sign-on attempts:

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

The following should be implemented to limit the opportunity for unauthorized attempts to sign-on to a system :

a) To suspend the USERID after a maximum of 'N' repeated unsuccessful log-on attempts (suggestion 'N'= number of unsuccessful log-ons to be as decided by the organisation).

b) To set authentication time limit at 'N' minutes (suggestion 'N'=number of minutes to be decided by the organisation) and to terminate the session if the time limit is exceeded. In both the cases, users should be informed of the failure to sign on, but not the reason therefor.

5.4.7 Unattended Terminals :

The following steps should be implemented to prevent unauthorized use of a terminal connected to a system :

a) Identification and authentication process to be repeated after a specified period of inactivity before work can be continued on the terminal.

b) Use of one-button lock-up system, force button or shut-off sequence to be activated when the terminal is left alone.

c) All users and contractors should be made aware of the security requirements and procedures for protecting unattended terminals as well as their responsibilities for implementing such protection.

d) Termination of the active sessions when finished, unless they can be secured by an appropriate locking mechanism e.g. a password protected screen saver.

e) Log-off to the mainframe system, when the session is finished and not just switch-off the PC or terminal.

f) Inactive terminals in high risk locations, e.g. public or external areas outside the organization's security management or serving high risk systems, should shut down after a defined period of inactivity to prevent access by unauthorized persons. This time-out

facility should clear the terminal screen and close both application and network sessions after a defined period of inactivity. The time-out delay should reflect the security risks of the area and the users of the terminal.

g) A limited form of terminal time-out facility can be provided for some PCs which clears the screen and prevents unauthorized access but does not close down the application or network sessions.

5.4.8 Access Control Features & Operating System :

Information and information processing resources are protected when systems, supporting multiple users, are in use, the access control software that is capable of restricting the access of each individual to only those information resources for which the individual is authorised, requires to be specified and used. Security facilities at the operating system level should be used to restrict access to computer resources. Administration Account should be used for Administration purpose only and not for general purpose. These facilities should be capable of the following :

a) Identification and verification of the identity and if necessary, the terminal or location of each authorized user.

b) Recording of successful and failed system accesses.

c) Provision for appropriate means for authentication.

d) Provision (where appropriate) for restricting the connection time of the users.

e) Use of the access control methods, such as challenge-response, if these are justified on the basis of the business requirements and risk.

f) Control of user access to information and application system functions in accordance with the established access control policy.

g) Provision of protection from unauthorized access for any utility and/ or operating system software that is capable of overriding system or application controls.

h) Non-compromise of the security of the other systems with which information resources are shared.

i) Provision for access to information to the owner only, other authorized individuals or authorised users.

5.4.9 Information Access Restriction :

Users of application systems, inclusive of the technical support staff, should be provided with access to information and the application system functions in accordance with the established access control policy, based on the individual business application requirements. Application of the following controls should be considered for implementing information access restrictions.

a) Provision for menus to control access to application system functions.

b) Restriction of users' knowledge of information or application system functions which they are not authorized to access with appropriate editing of user documentation.

c) Control of the access rights of the users, e.g. read, write, delete and execute.

d) The outputs from the application systems, handling sensitive information, contain only the information that is relevant to the use of the output and is sent only to authorized terminals and locations, including periodic review of such outputs to ensure that redundant information is removed.

5.4.10 Automatic Terminal Identification :

Automatic terminal identification should be considered to authenticate connection to specified locations and to portable equipment. Automatic terminal identification is a technique that can be used, if it is important that the session can only be initiated from a particular location or computer terminal. An identifier in or attached to the terminal can be used to indicate whether a particular terminal is permitted to initiate or receive specific transactions. It may be necessary to apply physical protection to the terminal and to maintain

the security of the terminal identifier.

5.4.11 Terminal Log-on Procedures :

Access to information services should be attainable through a secure log-on process. The procedure for logging into a computer system should be designed to minimize the opportunity for unauthorized access. The log-on procedure should, therefore, disclose the minimum of information about the system in order to avoid providing an unauthorized user with unnecessary assistance. A good log-on procedure should :

a) not display system or application identifiers until the log-on process has been successfully completed ;

b) display a general notice warning that the computer should only be accessed by the authorized users;

c) not provide help messages during the log-on procedure that could aid an unauthorized user;

d) validate the log-on information only on completion of all input data.
If an error arises, the system should not indicate which part of the data is correct or incorrect ;

e) limit the number of unsuccessful log-on attempts allowed (the number of such log on attempts to be as decided by the organisation) and consider:

i. recording unsuccessful attempts;

ii. forcing a time delay before further log-on attempts are allowed or rejecting any further attempts without specific authorization; and

iii. disconnecting data link connections;

f) limit the maximum and minimum time allowed for the log-on procedure. If exceeded, the system should terminate the log-on; and

g) display the following information on completion of a successful log-on

i. date and time of the previous successful log-on;

ii. details of any unsuccessful log-on attempts since the last successful log-on.

In case of application software, the system should authenticate the User ID and User Password.

5.4.12 Use of System Utilities :

Most computer installations have one or more system utility programs that might be capable of overriding system and application controls. It is essential that their use is restricted and tightly controlled. The following controls should be considered :

a) use of authentication procedures for system utilities;

b) segregation of system utilities from application software;

c) limitation of the use of system utilities to the minimum practical number of trusted, authorized users;

d) authorization for ad hoc use of systems utilities;

e) limitation of the availability of system utilities;

f) logging of all the uses of system utilities;

g) defining and documenting the authorization levels for system utilities; and

h) removal of all unnecessary software based utilities and system software.

5.4.13 Limitation of Connection Time :

Restrictions on connection time should provide additional security for high risk applications. Limiting the period during which terminal connections are allowed to computer services reduces the window of opportunity for unauthorized access. Such a control should be considered for sensitive computer applications, especially those with terminals installed at the

high risk locations e.g. public or external areas that are outside the organization's security management. The examples of such restrictions may include:

a) use of pre-determined time slots e.g. for batch file transmissions or regular interactive sessions of short duration; and

b) restricting the connection time to normal office hours if there is no requirement for extended-hours of operation.

5.4.14 Warning :

To warn unauthorized users of the possible consequences of their actions, to display a warning screen, prior to completing sign-on, that makes it clear to the users that unauthorized access, if any, will be deemed illegal only, resulting in the prosecution of such unauthorised users, as prescribed under Law.

5.4.15 External Users :

In addition to the controls listed above, the internal network of the organisation will require to be closely controlled/guarded in regard to the access granted to the users from outside the organisation. To protect against unauthorized access by the external users, it is to be ensured that all the traffic, external to the organisation's network, pass through a properly configured firewall.

5.4.16 Audit Trails :

The audit trails are records of activity, used to provide a means for restructuring events and establishing accountability. The audit trail information is essential for investigation of the incidents/problems. The controls, useful in the audit trail process, are described hereunder. To deter and provide early detection of unauthorized activity, the following steps should be implemented :

A) To provide an audit trail for the computer systems and manual operations when:

a) SENSITIVE or HIGHLY SENSITIVE information is accessed ;

b) network services are accessed ; and

c) special privileges or authorities such as the security administration commands, emergency USERIDs, supervisory functions etc., overriding the normal processing flow, are used.

B) To include in the audit trail as much of the following as is practical:

a) user identification ;

b) functions, resources and information used or changed ;

c) date and time stamp (including time zone) ;

d) work-station address and network connectivity path ; and

e) specific transaction or program executed.

C) To provide an additional real time alarm of significant security-related events for all computer systems having on-line capabilities for enquiry or update, containing information as under :

a. access attempts that violate the access control rules ;

b. attempts to access functions or information not authorized ;

c. concurrent log-on attempts ; and

d. security profile changes.

D) To investigate and report suspicious activity immediately.
E) To ensure that management reviews the audit trail information on a timely basis, usually daily.
F) To investigate and report security exceptions/violations and unusual occurrences.
G) To preserve the audit trail information for an appropriate period of time for business requirements.
H) To protect the audit trail information from deletion, modifications, fabrications or re-sequencing by use of digital signature.

5.4.17 Sensitive System Isolation :

Sensitive systems might require a dedicated (isolated) computing environment. Some application systems are sufficiently sensitive to potential loss and they require special handling. The sensitivity/criticality may be such that the application system requires to run on a dedicated computer system or that it should share resources with other trusted application systems only. The following may be considered for addressing such requirements:

a) The sensitivity of an application system should be explicitly identified and documented by the application owner.

b) When a sensitive application is to run in a shared environment, the other application system/s with which it will share resources should be identified and agreed with the owner of the sensitive application.

5.4.18 Monitoring of System Use - Procedures and Areas of Risk :

Procedures for monitoring the use of information processing facilities should be established. Such procedures are necessary to ensure that the users perform only those activities, for which they have been authorized. The level of monitoring required for individual facilities should be determined by a risk assessment which should include the following :

a) Authorized Access including details as under :

? the user ID;

? the date and time of key events;

? the types of events ;

? the files accessed; and

? the program/utilities used.

b) All Privileged Operations as under :

? use of supervisor account;

? system start-up and stop; and l

? I/O device attachment/detachment.

c) Unauthorized Access Attempts as under :

? failed attempts;

? access policy violations and notifications for network gateways and firewalls; and
? alerts from proprietary intrusion detection systems.

d) System Alerts or Failure as under :

? console alerts or messages;

? system log exceptions; and

? network management alarms.

5.4.19 Risk Factors :

The result of the system monitoring activities should be reviewed regularly. The frequency of the review should depend on the risks involved. The risk factors, as under, should be considered in this regard :

a) the criticality of the application processes ;

b) the value, sensitivity or criticality of the information involved ;

c) the past experience of system infiltration and misuse; and

d) the extent of system interconnection (particularly public networks)

5.4.20 Operator logs :

Operational staff should maintain a log of their activities. Logs should include the following:

a) system starting and finishing times;
b) system errors and corrective action taken;
c) confirmation of the correct handling of data files and computer output; and
d) the name of the person making the log entry.

Operator logs should be subject to regular, independent checks against operating procedures.

5.4.21 Fault Logging :

Faults should be reported and corrective action taken. Faults, reported by the users regarding the problems with the information processing or communication systems, should be logged. There should be established rules and procedures for handling the reported faults which, among others, should include:

a) review of the fault logs to ensure that faults have been satisfactorily resolved;
b) review of corrective measures to ensure that controls have not been compromised and that the action taken is fully authorized.

5.4.22 Logging and Reviewing of Events :

A log review involves understanding the security threats faced by the information systems and the manner in which such threats may arise. System logs often contain a large volume of information, much of which is extraneous to security monitoring. There should be a documented plan for the volumes of information to be logged, rotation of log files, back-up archival of log files, encryption of log files and retention/disposal of log data. To help identify significant events for security monitoring purposes, the copying of appropriate message types automatically to a second log, and/or the use of suitable system utilities or audit tools to perform file interrogation should be considered. When allocating the responsibility for log review, a separation of roles should be considered between the person(s) undertaking the review and those whose activities are being monitored. Particular attention should be given to the security of the logging facility because any susceptibility to tampering thereof i.e. modifications, fabrications etc., can lead to a false sense of security. Security controls should aim to protect the logging facilities against unauthorized changes and operational problems including:

a) the logging facility being de-activated:

b) alterations to the message types that are recorded;

c) log files being edited or deleted; and

d) log file media becoming exhausted and either failing to record events or overwriting itself.

5.4.23 System Clock Synchronization :

The correct setting of computer clocks is important to ensure the accuracy of audit logs,

which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence. Where a computer or communications device has the capability to operate a real-time clock, it should be set to an agreed standard, e.g. Universal Co-ordinated Time (UCT) or local standard time. As some clocks are known to drift with time, there should be a procedure that checks for and corrects any significant variation.

Chapter 6

Software and Security Controls

Software, used in the financial sector, needs high integrity. Since software is intangible i.e. not visible or capable of existing in multiple copies or in various forms without the user's intervention, the control of software poses challenges different from those relating to the control of equipment (hardware). The following controls should be exercised for the protection of software and the information that is processed by the software. In general, access to live data or software should be justified and authorized. The work which is carried out should be monitored or recorded and validated and signed off by the authorized personnel, who understand the underlying business application/s. The results should be reported to the designated authority and filed in the security unit.

6.1 System software :

System software is that set of instructions which functions as the central control for the computer system. Special attention should be paid to the control of this software, which, among others, includes manipulation of this software allowed and other security controls in the system.

To ensure the integrity of system software, the following steps should be taken:

a) To apply the most stringent access controls to system software and their handling facilities.

b) To apply the highest Human Resource standards in selecting personnel for systems software operation and maintenance.

6.2 Memory Resident Programs :

To prevent loss of integrity because of the presence of memory resident programs i.e., those programs that allow seemingly normal processing to take place, but retain ultimate control over the functions of the processing resources, periodic inspection of the software installed to ascertain, whether any unauthorised software has been inserted, should be performed. Further, special attention should be paid to the detection of the memory resident programs.

6.3 Applications :

Applications are specific sets of software designed to accomplish one or more functions, such as funds transfer, billing, logical access control etc. A business application serves the basis for using the computation power of the computer systems. To prevent unavailability or unauthorized modifications, disclosures or destruction of information, the following steps should be taken.

a) To integrate the application security with the operating system access control facility in such a manner that the USERIDs and the passwords are maintained by the operating system control facility and not the application system. This facilitates centralized and standardized USERID and password management as well as more efficient audit and reporting functions.

b) To 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 in such a manner that the "least possible privilege" can be granted to an individual to perform the job.

c) Consistent access controls on information that is replicated on multiple platforms.

d) Application controls identify specific accountabilitiy with an user/ USERID through USERID/time/date stamp.

e) To incorporate information ownership into the system. The ownership may be accountable on a group or individual level.

f) To consider location control methodology that applies additional restrictions at specific locations.

g) Dual control capabilities for CRITICAL transactions such as money movement transactions.

h) The applications, not under the control of a database management system, to meet requirements listed under the databases.

i) To log and report violation (modifications/alterations/amendments) of the messages, when they exist.

6.4 Application Testing :

Application testing is the checking of new or modified processing systems to ensure that the systems work properly. To protect sensitive or highly sensitive customer information from disclosure or inappropriate processing during application testing, the following steps should be implemented.

To establish and communicate a policy that controls the use of production information during application testing and uses access control to limit to appropriate personnel the renaming and restoration of the production files.

Alternatively,

a) To depersonalise 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.

b) To dispose of production information used in testing, in either case.

c) To require use of physically separate environments for operational and development systems.

6.5 Availability of Application Software Code :

To ensure that source code is available for debugging or enhancement, the following steps should be taken :

a) To establish procedures to maintain the most current version of the programs written by the organisation's staff and contractors.

b) To consider an escrow arrangement for the application software code under due agreement for the purchased application software for which source code is not available.

6.6 Change Management :

To maintain the integrity of software when changes are made, the established change control procedures should be followed.

6.7 Databases :

A database is a collection of information that may be retrieved according to one or more criteria. It is dealt with in this document as a special case of software application. To protect databases from unauthorized modification or destruction and to maintain the integrity of information stored in the databases, the following steps should be taken :

a) To ensure that the database management systems have controls, so that all updating and retrieval of information preserve information integrity with respect to transaction

control and system failure.

Concurrency control is required for shared databases.

b) All accesses to information be controlled as specified by an Information Systems Security Administrator.

c) To 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.

6.8 Artificial Intelligence (AI) :

The applications, which use AI techniques, should include controls, specific to that technology and the following steps should be taken :

a) To secure all knowledge bases used by inference engines or similar AI processing techniques and ensure a regular review thereof for accuracy and effectiveness.

b) To place limits of the automatic decision making ability of AI systems or AI sub-systems of conventional applications to ensure that vital decisions are approved.

c) To place controls on the information used in the training of neural networks based applications.

d) To monitor the stability of neural network based applications for effectiveness.

e) To build all AI systems within programmed decision enclosures to ensure that the control of decision making is kept within reasonable limits according to the information being processed or the impact of the decisions made.

6.9 Defective Software :

To minimize the probability of latent defects in software, the following steps should be taken :

a) To select vendors with a good reputation, a proven record and sufficient resources or insurance to cover the damages, which may result from the use of their software.

b) To install and operationalise quality assurance program for all software.

c) All software to be fully documented, tested and verified.

6.10 Unlicensed Software :

To prevent litigation or embarrassment, caused by use of software that is not licensed or beyond the license granted by the vendor, the following steps should be taken.

a) To use only licensed or authorized software.

b) To maintain evidence that license agreements are being fully met.

This can include an inventory system, physical control of master copies of software and periodic auditing of the information systems.

6.11 Protection against Malicious Software :

Software and information processing facilities are vulnerable to the introduction of malicious software such as computer viruses, network worms, Trojan horses and logic bombs. Users should be made aware of the dangers of unauthorized or malicious software and the Information System Security Managers should, where appropriate, introduce special controls to detect or prevent its introduction. It is essential that precautions are taken to detect and prevent computer viruses on personal computers.

6.11.1 Controls against Malicious Software :

The detection and prevention controls to protect against malicious software and appropriate user awareness procedures should be implemented. The protection against malicious software should be based on security awareness, appropriate system access and change management controls. To protect the integrity of information and the information systems from modifications, disclosures or destruction by malicious software, the following steps should be taken:

a) To establish a virus detection and protection procedure, to be continuously reviewed

and revised, conforming to the emerging requirements and to implement the same across the organisation.

All software acquired by the organisation should be checked by the virus detection procedure prior to installation and use.

b) To establish the management procedures and responsibilities to deal with the virus protection on systems, training in their use, reporting and recovering from virus attacks.

c) To distribute instructions on the detection of viruses to all the users.

Evidence such as sluggish performance or mysterious growth of files should alert the users to a problem that must be reported to the information system security manager immediately on occurrence thereof.

d) To establish a written policy on downloading, acceptance and use of freeware and shareware including the flexibility to prohibit this practice, if deemed necessary.

e) To establish a formal policy requiring compliance with software licences and prohibiting the use of unauthorized software.

f) To authenticate software for highly CRITICAL applications using digital signature. Failure to verify would indicate potential problem/ s and the software should not be used until the source of the problem is identified and properly dealt with.

g) To establish a formal policy to protect against risks associated with obtaining files and software either from or via external networks or on any other medium, indicating what protective measures should be taken.

h) To install and regularly update the anti-virus detection and repair software to scan computers and media, either as a precautionary control or on a routine basis.

i) To conduct regular reviews of the software and data content of systems supporting critical business processes. The presence of any unapproved files or unauthorized amendments should be formally investigated.

j) To establish a policy and procedure for checking the diskettes and other such media, brought in from outside the organisation's normal purchasing programme. To check any files on electronic media of uncertain or unauthorized origin or files received over untrusted networks for viruses before use.

k) To check any electronic mail attachments and downloads for malicious software before use. This check may be carried out at different places e.g. at electronic mail servers, desktop computers or when entering the network of the organization.

l) To establish appropriate business continuity plans for recovering from virus attacks, including all necessary data and software backup and recovery arrangements.

m) To establish procedures to verify all information relating to malicious software and ensure that warning bulletins are accurate and informative. The Information Systems Security Managers should ensure that qualified sources, e.g. reputed journals, reliable Internet sites or anti-virus software suppliers are used to differentiate between hoaxes and real viruses. The users of the information systems should be made aware of the problem of hoaxes and the action to be taken on receipt thereof.

To ensure recovery of the processing capabilities following a virus infection, the following steps should be taken :

a) To retain the original back-up copy of all software and hold the same until such time as the original software is no longer in use.

b) All data is backed up regularly.

6.12 Software provided to Customers :

Financial organisations may provide software to their customers for the purpose of serving the customers better or to interact with a customer for various purposes. To prevent unauthorized destruction or modifications of the software distributed to the customers, the following steps should be taken :

a) To create a secure and 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 master copies of the customer software. Alternatively, it has to be ensured to restore the copying hardware and software to a "diskette creation state" prior to the creation of each session.

b) To obtain a written statement from the vendor/s of the software, which is being provided to the customers, binding such Vendor/s that the respective vendors are making their best efforts to protect the software against viruses and other unwanted codes and undertake to continuously upgrade such software with virus detection/protection measures, as required.

To protect the organisation against the claims of negligence due to the use of the software provided by the organisation, the following steps should be taken :

a) All software controls, applicable to the organisation's software, also apply to the software provided to the customers. The organisation should also develop control requirements and guidelines for all the departments issuing software to the customers. This should include the software developed within the organisations, third-party software that may be legally distributed to customers and a combination of both internally developed and third-party software "packages."

b) To execute an agreement with the customers to whom software is provided specifying, among others, each party's responsibilities, security requirements, indemnity for the organisation, limits on liability, compliance with environmental conditions and implementation of access controls at each customer site/s and instructions/procedures for use of the software.

c) To maintain sufficient documentation to prove that the software, provided by the organisation, was not the cause of viruses or other malicious codes, if encountered subsequently.

6.13 Software to interface with Customers :

The growth of computerisation and connectivity in banking operations may lead to the customers communicating with the financial organisations through commercial banking packages, ushering in the era of on-line banking facilities. On account of the growing pressure of competition and the need for the competitive edge in operations, the banks may have to provide on-line banking services to the customers. To limit the liabilities or losses which may arise on account of on-line banking, the following steps should be taken :

a) The liability/ies for the security breaches are, among others, clearly specified in the agreement/s with the banks.

b) To specify, among others, the role and responsibilities of the customers, availing of on-line banking facilities, under the terms and conditions, the organisation has set out for rendering such services.

c) The security policies of the service provider/s are compatible with that of the banks and financial organisations.

6.14 Security Controls and System Documentation :

Systems documentation may contain a range of sensitive information e.g. description of the application processes, procedures, data structures, authorization processes etc. The following security controls should be considered to protect the system documentation from unauthorized access.

a. System documentation should be stored securely.

b. The size of the access list for access to system documentation should be kept to a minimum and authorized by the system/ application owner.

c. System documentation held over a public network or supplied through a public

network should be appropriately protected.

6.15 Exchange of Information and Software :

Exchanges of information and software between organizations should be controlled and be in conformity with the relevant legislations. Such exchange/s should be carried out on the basis of written agreements. Procedures and standards to protect information and media in transit should be established. The business and security implications, associated with electronic data interchange, electronic commerce and electronic mail and the requirements for security controls therefor, should be considered.

6.15.1 Information and Software Exchange Agreement :

Agreements including software escrow agreements, where appropriate, should be established for the exchange of information and software (whether electronic or manual) between the organizations. The security controls, specified in such an agreement, should reflect the sensitivity of the business information involved. Agreements on security conditions should consider the following :

a) management responsibilities for controlling and notifying transmission, despatch and receipt ;

b) Procedures for notifying sender, transmission, despatch and receipt;

c) minimum technical standards for packaging and transmission ;

d) courier identification standards ;

e) responsibilities and liabilities in the event of loss of data ;

f) use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected;

g) information and software ownership and responsibilities for data protection, software copyright compliance and similar considerations;

h) technical standards for recording and reading information and software; and

i) any special controls such as the cryptographic keys that may be required to protect sensitive items.

6.14 Applets, JAVA and Software from External Sources :

The Internet Service Providers may download software to their customers. However, care should be taken to preclude such software as is introduced into the organisation's domain without the specific request therefor or the express consent of the organisation. JAVA, a computer language, specifically aimed at creating applications that can be remotely accessed and run, also represents a path for software, not requested by a customer, to become resident in a computer.

To prevent the entry of unauthorized software into the organisation's systems, the following steps should be taken :

a. To provide connectivity to the Internet with the required security safeguards, as required for the conduct of business.

b. To install firewall including proxy server between the Internet and the internal network of the organisation.

c. Either the firewall includes virus scanning or that any executable file is virus scanned before it is introduced to the organisation's network.

d. To include, among others, liability clauses in any contract/ agreement entered into with such Internet Service Providers.

Chapter 7

Computer Systems and Security Controls

The computer Systems are at the centre of the information systems security policy. The computation power, provided by these systems, allows the organisations more flexibility and processing capability than ever before. The complex array of computer capabilities offers both operational advantages and at the same time, raises security concerns also. The following controls, among others, will require to be implemented to protect the integrity of the computer systems which include, among others, mainframes, mini-computers, microcomputers, laptops, notebooks, palmtops, servers, workstations and personal computers in use in the organisation.

7.1 Physical Protection :

Physical barriers to information and information processing resources can serve to control access. The "fortress computer centre" is becoming increasingly rare. However, there may be circumstances, when physical controls may be adequate. The following steps will require to be taken to protect the computer systems and the central information processing centres from physical damage:

a) To choose the site/s for the information processing centres away from the flight paths, geological fault lines, power lines, potential terrorist targets etc.

b) To define a security perimeter around the central processing facilities as a basis for physical controls.

c) To limit physical access strictly to the authorized personnel. A record of entry and exit should be kept. Positive identification should be made prior to any entry. All staff should be instructed to challenge or report unrecognised or unauthorized persons.

d) To implement an inventory or property control program.

e) To monitor the movement of all computer resources/components/ parts from the organisation's sites.

f) To build rooms or areas containing information processing equipment which conform to all building and fire codes of the local jurisdiction and to the manufacturer's specifications.

g) To provide adequate air-conditioning for cooling of the equipment i.e. for maintenance of room temperature and humidity at levels, specified by the manufacturer/s under the worst-case conditions.

h) To provide clean and adequate power supply. The installation of the uninterrupted power supply (UPS), generators and execution of agreements with the related parties/agencies for priority restoration of such services should be done.

i) To provide adequate fire and water protection.

j) To have engineering diagrams which have been reviewed for single-point-of-failure and evaluated for ways to eliminate those failures.

k) To prohibit storage of hazardous or combustible material within the perimeter of the processing site/s.

l) To consider an intermediate holding area for deliveries to the processing rooms.

m) To escort visitors, if any, within the premises at all times.

n) The building and the computer equipment meet the insurer's requirements.

7.2) The following steps will require to be implemented to protect the personal computers, when used off-site:

a) To prohibit the use of the personal computers off-site unless virus controls have been installed.

b) The personal computers are not left unattended in the public places.

c) The personal computers are carried as hand luggage while travelling.

d) To prohibit the use of the personal computers off-site unless they have adequate

access protection controls, commensurate with the classification of the information.

e) To apply all other controls as appropriate.

f) All the manufacturer's instructions regarding the protection of the computer equipment are followed.

7.3 Logical Access Control :

The logical access control for all the computer systems will be implemented to prevent unauthorized modifications, disclosures or destruction of information residing in the computer systems.

7.4 Change Control :

The established change control procedures will be followed to ensure the maintenance of the integrity of the computer systems and that of information, as and when changes are made.

7.5 Maintenance of Equipment :

The following steps will require to be followed to ensure the integrity of the security controls in place during the maintenance of the equipment :

a) Allow modifications to be made only by authorized personnel within the established maintenance procedures.

b) The testing of the security controls in place, both before and after the maintenance service.

c) Maintain a record of all faults or suspected faults.

d) Appropriate virus checks are made.

e) Tamper-protection of the components which store sensitive information.

7.6 Casual Viewing :

Privacy shields may be installed to minimize the disclosure of SENSITIVE or HIGHLY SENSITIVE information on the computer terminals.

7.7 Emulation Concerns :

To ensure that all appropriate controls are implemented, it is required to ensure that the controls which apply to a specific transaction or process should also apply to the computer systems which support that transaction or process.

7.8 Business Continuity :

The organisation should include computer systems as part of the contingency and disaster recovery plan to ensure that the organisation can continue to function in case of major disruption, caused by natural disasters, power failures or other factors.

7.9 Audit Trails :

The maintenance of the audit trails is essential to ensure quality of security controls.

7.10 Disposal of Equipment :

The following steps will require to be implemented to prevent the disclosure of sensitive information :

a) To check all equipment containing storage media for sensitive information prior to disposal.

b) To perform a risk assessment on the damaged equipment to determine if it should be destroyed, repaired or discarded. The process of destruction should be defined, if it has to be discarded.

c) To ensure that the storage media goes through a secure erasure procedure prior to disposal.

Chapter 8

Change Control Mechanism

8.1 To protect the integrity of the information processing systems, a change control procedure is essential. The change control procedures will relate to hardware changes, software changes and changes in manual procedures. The change control procedure will also have to address emergency changes. To prevent unauthorized changes in the production environment, a change control procedure that manages all changes, regardless of the magnitude, whether scheduled or emergency, will require to be established. The following steps should be implemented to ensure that the change control procedure, put in place, remains effective:

a) Establish a formal change request and the authorization process therefor.
b) Establish a test and system acceptance procedure for each change.
c) All changes are scheduled and fully documented.
d) All changes have viable back-up procedures, well defined and documented, to take care of failure during or after the implementation of the change.
e) Virus checks are made before and after the implementation of the changes.

8.2 Emergency Problems :

The following steps will be taken to ensure maintenance of integrity of the computer systems during emergencies:

a) Allow emergency fixes only to resolve production problems.
b) Return to normal change procedures expeditiously.
c) Emergency support personnel to document the changes implemented.
d) Review all emergency changes.

Chapter 9

Network and Security Controls

A network is the collection of information processing and communication resources, which enable the computer systems or the individuals to access and transmit information. Networks may be as simple as two personal computers connected to each other or as complex as a world-wide, multi-organisational funds transfer network. Access to both internal and external network and services should be controlled. This is necessary to ensure that the users who have access to networks and network services do not compromise the security of these network services by ensuring;

a. appropriate interfaces between the organization's and the public networks, with adequate security controls in place ;
b. appropriate authentication mechanisms for the users and the equipment; and
c. control of users access to the information services.

9.1 Policy on Use of Network and Network Services :

Insecure connections to network services can affect the whole organization. Users should only be provided with direct access to the services that they have been specifically authorized to use. This control is particularly important for network connections to sensitive or critical business applications or to users in high-risk locations e.g. public or external areas that are outside the organization's security management and control. A policy should be put in place concerning the use of the networks and the network services. This policy should cover the following :

a. the networks and network services which are allowed to be accessed;
b. authorization procedures for determining who is allowed to access which networks and network services;

c. management controls and procedures to protect the access to network connections and network services ;

d. consistency with the access control policy of the organisation ;

e. enabling network services for business reasons only ;

f. the removal or disabling of the unused or unwanted network services ;

g. documented procedures including all critical parameter settings, scripts and configuration files for installation and operationalisation of a network operating system ;

h. regular updation of the security related software ;

i. identification of the types of information which need to be logged ;

j. limiting the Users to a single concurrent session ;and

k. preventing IP Spoofing – all in-bound IP packets with a source address originating from the organisation's internal network and all out-bound IP packets with source addresses other than the internal network to be dropped.

9.2 Enforced Path :

The path from the user terminal to the computer service may need to be controlled. Networks are designed to allow maximum scope for sharing of resources and flexibility of routing. These features may provide opportunities for unauthorized access to business applications or unauthorized use of the information facilities. Incorporating controls that restrict the route between a user terminal and the computer services, the user is authorized to access e.g. creating an enforced path, can reduce such risks. The objective of an enforced path is to prevent any user selecting routes outside the route between the user terminal and the service, that the user is authorized to access. This requires the implementation of a number of controls at different points in the route. The principle is to limit the routing options at each point in the network through predefined and authorised routes, as described hereunder:

a. allocating dedicated lines or telephone numbers:

b. automatically connecting ports to specified application systems or security gateways;

c. limiting menu and sub-menu options for individual users;

d. preventing unlimited network roaming;

e. enforcing the use of specified application systems and/or security gateways for external network users;

f. actively controlling allowed source to destination communications via security gateways e.g. firewalls;

g. restricting network access by setting up separate logical domains e.g. virtual private networks, for user groups within the organization; and

h. ensuring consistency between the requirements for an enforced path and the access control policy.

9.3 User Authentication for External Connections :

External connections provide a potential for unauthorized access to business information e.g. access by dial-up methods. Therefore, access by remote users should be subject to authentication. There are different types of authentication methods, some of these provide a greater level of protection than others e.g. methods based on the use of cryptographic techniques can provide strong authentication. It is important to determine on the basis of risk assessment the level of protection required. This is needed for the appropriate selection of an authentication method. Authentication of remote users can be achieved using eg. a cryptographic based technique, hardware tokens or a challenge/ response protocol. Dedicated private lines or a network user address checking facility can also be used to provide assurance about the source of connections. Dial-back procedures and controls e.g. use of dial-back modems, can provide protection against unauthorized and unwanted connections to an organization's information processing facilities. This type of control authenticates the users

trying to establish a connection to an organization's network from remote locations. When using this control, an organization should not use network services which include call forwarding or, if they do, they should disable the use of such features to avoid weaknesses associated with call forwarding. It is also important that the call back process includes ensuring that an actual disconnection on the organization's side occurs. Otherwise, the remote user could hold the line open pretending that call back verification has occurred. Call back procedures and controls should be thoroughly tested for this possibility.

9.4 Node Authentication :

A facility for automatic connection to a remote computer could provide a way of gaining unauthorized access to a business application. Connections to remote computer systems should, therefore, be authenticated. This is especially important if the connection uses a network that is outside the control of the organization's security management. Node authentication can serve as an alternative means of authenticating groups of remote users, where they are connected to a secure, shared computer facility.

9.5 Remote Diagnostic Port Protection :

Access to diagnostic ports should be securely controlled. Many computers and communication systems could be installed with a dial-up remote diagnostic facility for use by the engineers. If unprotected, these diagnostic ports provide a means of unauthorized access. They should, therefore, be protected by appropriate security mechanism e.g. a key lock and procedure to ensure that they are only accessible by an arrangement between the manager of the computer services and the hardware/software support personnel requiring access.

9.6 Segregation of Networks :

Networks are increasingly being extended beyond the traditional organizational boundaries, as business partnerships are formed that may require the interconnection or sharing of information processing and networking facilities. Such extensions might increase the risk of unauthorized access to already existing information systems that use the network, some of which might require protection from other network users because of their sensitivity or criticality. In such circumstances, the introduction of controls within the network to segregate groups of information services, users and information systems, should be considered. One method of controlling the security of large networks is to divide them into separate logical network domains e.g. an organization's internal network domains and external network domains, each protected by a denied security perimeter. Such a perimeter can be implemented by installing a secure gateway i.e. firewall, between the two networks to be interconnected to control access and information flow between the two domains. This gateway should be configured to filter traffic between these domains and to block unauthorized access in accordance with the organization's access control policy and on the basis of cost and performance impact of incorporating suitable network routing or gateway technology .

9.7 Network Connection Control :

Access control policy requirements for shared networks, especially those extending across organizational boundaries, may require the incorporation of controls to restrict the connection capability of the users. Such controls can be implemented through network gateways that filter traffic by means of pre-defined tables or rules. The restrictions applied should be based on the access policy and requirements of the business applications and should be maintained and updated accordingly. The applications to which restrictions should be applied are as under :

a) electronic mail;

b) one-way file transfer;

c) both ways file transfer ;

d) interactive access; and

e) network access lined to method of day or date.

9.8 Network Routing Control :

Shared networks, especially those extending across organizational boundaries, may require the incorporation of routing controls to ensure that computer connections and information flows do not breach the access control policy of the organisation. This control is often essential for networks shared with third party users. Routing controls should be based on the positive source and destination address checking mechanisms. Network Address Translation (NAT) is a very useful mechanism for isolating networks and preventing routes to propagate from the network of one organization into the network of another.

9.9 Security of Network Services :

Network services may have unique or complex security characteristics. Organizations using network services should ensure that a clear description of the security attributes of all services used is provided.

9.10 Network Controls :

A range of controls is required to be implemented to achieve and maintain security in computer networks. Network managers should implement controls to ensure the security of data in networks and the protection of the connected services from unauthorized access. For the purpose. the following steps should be taken :

a) Operational responsibility for networks should be separate from computer operations, where appropriate.

b) Responsibilities and procedures for the management of remote equipment, including equipment in user areas, should be established.

c) Special controls should be established to safeguard the confidentiality and integrity of the data passing over public networks and to protect the connected systems.

d) Special controls should also be established to maintain the availability of the network services and the computers connected.

9.11 Network Integrity :

The following steps will require to be taken to prevent the capture of a session during accidental or intentional communication line drops.

a) Provide network controls for the detection and reporting of dropped communications lines and timely termination of all associated computer sessions.

b) Re-authentication when the line drops occur.

9.12 Access Control :

The communication access requires to be granted only on a need-to-use basis to protect against modifications, destruction or disclosures of information through unauthorized access or use of the communication facilities.

9.13 Dial-in :

Dial-in is the capability to access information processing resources via public or private networks. The following steps require to be implemented to ensure that access control is not compromised through misuse of the dial-in facility.

a) Establish a policy setting out the conditions under which dial-in is permissible. Dial-in phone numbers should not be published or provided to other employees or third party.

b) Implement, where business needs dictate, additional controls such as, card/token based authentication devices, security modems etc. which can provide password and dial-back controls or remote computing software that can provide password controls.

9.14 The following steps require to be taken to ensure that dial-in by the vendors, customers etc. (if such facility has been made available to them) does not compromise the

security controls in place.

a) Execute a written agreement/contract with the vendors, suppliers, customers etc. identifying their respective role and responsibilities regarding security including the penalties in the event of breach of contract by such parties.

b) Establish a procedure which requires the intervention of an authorized employee to enable a dial-in access session. It must be ensured to disable the dial-in session on completion thereof .

c) Review the activity log of each such third party session.

9.15 Network Equipment :

The following steps require to be taken to prevent unauthorized use or interruption of the network equipment :

a) Control access to network equipment by logical access controls.

b) Locate network equipment in physically secure environment.

c) Wiring of the closets to be physically secure with only authorized personnel being permitted access.

d) Route cabling underground or through conduits.

e) Maintain an inventory of network equipment.

9.16 Change Control Procedure :

It should be ensured to limit the network changes to those made in accordance with the established change management procedures to preserve the integrity and availability of information and information resources during changes to the network.

9.17 Connection with other Networks :

The following steps require to be implemented to ensure that the information system security is not compromised because of the security problems in networks external to the organisation:

a) Specific authorization is obtained from the Information Systems Security Manager, prior to establishing connection with the external networks, which are outside the security management of the organisation. Further, policies and procedures, well documented, require to be established, to be followed for connection with the external networks.

b) The security policy of the service provider of the external network verifiably be as strong as the organisation’s security policy for its network.

9.18 Network Monitoring :

The following steps require to be taken for monitoring the network with the use of monitoring devices to protect against information disclosures, modifications or destruction :

a) Implement the use and storage controls over the devices, which monitor or record information being transmitted over a network (e.g. protocol analysers and other diagnostic equipment).

b) The employees are made aware, as part of the terms and conditions of employment as also by way of the management’s directives in this regard, that the use of the organisation’s information processing assets constitute consent to monitoring the same also.

9.19 Protection during Transmission :

The following steps should be taken to protect sensitive and highly sensitive information from disclosure during transmission:

a) Encrypt sensitive and highly sensitive information during electronic transmission.

b) Protect passwords by encryption during transmission.

To detect corruption or modification of highly sensitive information during transmission, it is required to authenticate the information with digital signature and the same has to be verified at the destination.

9.20 Network Availability :

It is required to protect the network equipment by use of Uninterrupted Power Supplies (UPS) to protect against information loss in situations, where power fluctuations or outages occur.

9.21 The following steps require to be taken to protect against the destruction or modifications of information residing in the network resources:

a) Establish and enforce a periodic back-up of information on network resources.
b) Test the recovery of the backed-up data periodically.

It requires to be ensured that the Disaster Recovery Plan includes disaster recovery in respect of the network services also to protect against losses due to the unavailability of the network resources.

9.22 Audit Trails :

Audit trails will require to be maintained to ensure continuity in the quality of security controls.

Chapter 10

Separation of Development and (Production) Operational Facilities and Information Handling and Back-up

10.1 Development and Test activities, co-existent with the Operational activities, can cause serious problems e.g. unwanted modifications of the files or the system environment, resulting in system disruption/failure. Where development and test staff have access to the operational system and its information, they may be able to introduce unauthorized and untested code or alter operational data. On some systems, this capability could be misused to commit fraud or introduce untested or malicious code. Untested or malicious code can cause serious operational problems. Developers and testers may also pose a threat to the confidentiality of the operational information.

10.2 Separating the development, test and operational facilities from one another is essential to achieve segregation of the roles and responsibilities involved and to ensure non-interference of the development and testing activities with the operational facilities. This will reduce the risk of accidental change or unauthorized access to operational software and business data. The level of separation among the operational, test and development environments should be decided as necessary. A similar separation should also be ensured between the development and the test functions, as it is also important to maintain a known and stable environment in which to carry out the test activities and at the same time, preventing inappropriate developer access. Rules and procedures for the transfer of software from the development to operational status should be well defined and documented. The following controls should be considered for separating the development, test and operational facilities.

a) Development and operational software should, where possible, be resident in different domains or directories and use different computer processors.
b) Development and testing activities should be separated as far as possible.
c) Compilers, editors and other system utilities should not be accessible from the operational systems, when not required and the availability thereof to be ensured after completion of due authorisation process.
d) Different log-on procedures should be used for operational and test systems to reduce the risk of errors. Users should use different passwords for these systems and the menus should display appropriate identification messages.
e) Development staff may have access to operational passwords, where controls are in place for issuing such passwords and that too, for supporting the operational systems

only. Security controls should ensure that such passwords are changed or withdrawn after their use for the specific purposes is over.

10.3 Information Handling Procedures :

Rules and procedures should be established for the handling and storage of information, consistent with its classification relating to documents, computing systems, networks, mobile computing etc., in order to protect such information from unauthorized disclosures or misuse, considering the following :

a) Vulnerabilities of information in office systems e.g. recording phone calls or conference calls, confidentiality of calls, storage of faxes and opening & distribution of mails ;

b) Policy and appropriate controls to manage information sharing e.g. the use of corporate electronic bulletin boards ;

c) Restricting access to diary information relating to selected individuals e.g. staff working on sensitive projects ;

d) Suitability or otherwise of the system to support business applications, such as communicating orders or authorizations ;

e) Categories of staff, contractors or business partners, allowed to use the information systems and services and the locations from which they may be accessed ;

f) Restricting the use of selected facilities to specific categories of users only ;

g) Identification of the status of the users e.g. employees of the organization or those of the contractors, service providers etc. in directories for the benefit of other users;

h) Retention and back-up of information held on the information systems ;

i) Sensitive/Highly Sensitive documents (hard copy) to be marked accordingly on each page and the pages to be numbered

j) Fallback requirements and arrangements therefor .

10.4 Information Back-up :

Back-up copies of the essential business information and software should be taken regularly. Adequate back-up facilities should be provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Back-up arrangements for individual systems should be regularly tested to ensure that they meet the requirements of business continuity plans. The following steps should be considered for the purpose.

a. A minimum level of back-up information, togetherwith accurate and complete records of procedures, should be stored in a remote location, easily accessible and to be turned to in case of disaster at the main site.

b. Back-up information should be given an appropriate level of physical and environmental protection, consistent with the standards applied at the main site. The controls applied to media at the main site should be extended to cover the back-up site.

c. Back-up media should be regularly tested, where practicable, to ensure that they can be relied upon for emergency use when necessary.

d. Restoration procedures should be regularly checked and tested to ensure that they are effective and that they can be completed within the time, allotted in the operational procedures for recovery.

e. The retention period for essential business information and also any requirement for archiving copies, to be permanently retained, should be determined on the basis of business requirements and compliance with legal and regulatory requirements.

10.5 Housekeeping :

To maintain the integrity and the availability of the information processing and communication services, appropriate rules and procedures should be established for taking

back-up copies of data and rehearsing their timely restoration, logging events and faults and where appropriate, monitoring the system environment.

Chapter 11

Security Controls and Media Handling

Media should be controlled and physically protected to prevent damage to assets and interruptions to business activities. Appropriate operating procedures should be established to protect documents, computer media (tapes, disks, cassettes), input/output data and system documentation from damage, theft and unauthorized access.

11.1 Security Controls for Media in Transit :

Information can be vulnerable to unauthorized access, misuse or corruption during physical transport e.g. while sending media through the postal service or courier. The following controls should be applied to safeguard the computer media while being transported between sites.

a) Reliable transport or couriers should be used. A list of the authorized couriers should be agreed with management and a procedure to check the identification of couriers implemented.

b) Packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with manufacturers' specifications.

c) Special controls should be adopted, where necessary, to protect sensitive information from unauthorized disclosures or modifications, which should include the following:

- ? use of locked containers ;
- ? delivery by hand;
- ? tamper evident packaging (which reveals any attempt to gain access); and
- ? in exceptional cases, splitting of the consignment and dispatch by different routes.

11.2 Management of Removable Computer Media :

Procedures should be established for the management of removable computer media such as tapes, disks, cassettes and printed reports, considering the following :

a. If no longer required, the previous contents of any re-usable media, to be removed from the organization, should be erased.

b. Authorisation should be required for all media, to be removed from the organization and a record of all such removals to be maintained.

c. All media should be stored in safe and secure environment in accordance with the manufacturers' specifications.

d. All procedures and authorization levels should be documented.

11.3 Disposal of Media :

Media should be disposed of securely and safely, when no longer required. Sensitive information could be leaked to outside persons through careless disposal of media. Procedures should be established for the secure disposal of media, considering the following:

a) Media containing sensitive information should be stored and disposed of securely and safely e.g. by incineration or shredding or emptied of data for use by another application within the organization.

b) The following list identifies the items that might require secure disposal :

- ? paper documents;
- ? voice or other recordings;
- ? output reports;
- ? one-time-use printer ribbons;
- ? magnetic tapes;

? removable disks or cassettes;

? optical storage media (all forms including the manufacturer's software distribution media);

? program listings;

? test data; and

? system documentation.

c) There may be organizations which offer collection and disposal services for papers, equipment and media. Care should be taken to select suitable contractors for the purpose with adequate controls and experience.

d) Disposal of sensitive items should be logged, where possible, in order to maintain an audit trail.

When accumulating media for disposal, consideration should be given to the aggregation effect, which may cause a large quantity of unclassified information to become more sensitive than a small quantity of classified information.

Chapter 12

Telecommuting/Teleworking, Mobile Computing and Security Controls

12.1 Telecommuting/Tele-working is generally thought to be working from home or from a fixed location outside the organization, using communications technology. A virtual office can be anywhere that is an extension of the workplace. Telecommuting equipment may include phone, fax and computers, usually laptops or desktops. The telecommuters benefit through the reduction in commuting costs, time and the avoidance of stress and fatigue. The policy of allowing the individuals to work from their homes or a fixed location outside the traditional office may be beneficial to the organisation also. However, care should be taken to determine if the functions performed by such employees can be properly carried out away from the traditional office.

12.2 All the security controls, listed in this document, apply to the telecommuting environment also. In addition, Human Resource issues also arise in respect of the employees who telecommute. Further, care has also to be taken with respect to the remote access to information resources of the organisation. Suitable protection of the telecommuting / teleworking site should be in place against the security hazards e.g. theft of equipment and information, unauthorized disclosures of information, unauthorized remote access to the organization's internal systems or misuse of facilities. It is important that telecommuting/teleworking is both authorized and controlled by the management of the organisation and that suitable arrangements are put in place for this way of working.

12.3 Organizations should consider developing policy and procedures and standards to control teleworking activities, authorizing teleworking activities only if they are satisfied that appropriate security arrangements and controls are in place and that these comply with the organization's information systems security requirements.

12.4 To prevent loss of control over the personal computers and the systems to which they may be connected because of capture through remote access software, it should be ensured that the remote access software is not allowed to remain resident on the computer systems. It should be loaded only as required, with specific concurrency from both the parties at the time and then be removed when the session is completed. At that time, complete disk scan should be done to check for viruses, including any diskettes used in the session.

12.5 The security issues concerning telecommuting/teleworking should be addressed as under :

a) Allow an employee to telecommute only after consideration is given to the employee's interpersonal skills, communication skills and ability to work in an unsupervised environment.

b) Establish and distribute a clear written policy on telecommuting.

c) Ensure that any employee, who wishes to telecommute, executes a written agreement with the organisation, which addresses the following issues :

? Equipment to be used: bank's or employee's

? Phone lines: separate or employee's

? Maintenance of the equipment

? Cost and reimbursement

? Supervision

? Liability for personal injury, fire, etc.

? Physical and logical access controls to include protection of equipment, information (transmitted or stored), hardcopy, backup of information, disposal of hardcopy and diskettes and protection of networks.

12.6 The physical and logical security requirements of the teleworking site should be addressed, considering the existing physical security arrangements for the building and the local environment vis-a-vis the requirements, as under ;

the proposed teleworking environment; o the communications security requirements, taking into account the need for remote access to the organization's internal systems, the sensitivity of the information that will be accessed and passed over the communication link and the sensitivity of the internal systems; and the threat of unauthorized access to information or resources from other people using the accommodation e.g. family and friends.

12.7 In addition to the above security controls and arrangements, the following should also be considered in this regard :

a) Provision of suitable equipment and storage furniture for the teleworking activities;

b) Definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the teleworker is authorized to access;

c) Provision of suitable communication equipment, including methods for securing remote access;

d) Rules and guidance on family and visitor access to equipment and information;

e) Procedures for back-up and business continuity;

f) Audit and security monitoring ;

g) Revocation of authority, access rights and the return of the equipment when the teleworking activities cease or as decided by the organisation.

12.8 Mobile Computing :

12.8.1 When using mobile computing facilities e.g. notebooks, palmtops, laptops and mobile phones, special care should be taken to ensure that the business information is not compromised. Policy should be established that takes into account the risk of working with mobile computing facilities, particularly in unprotected environment. The policy should include the requirements for physical protection, access controls, cryptographic techniques, back-ups and virus protection. The policy should also include rules and advice on the connectivity of the mobile computing facilities to the networks and the guidance on the use of these facilities in public places. Care should be taken while using the mobile computing facilities in public places, meeting rooms and other unprotected areas, outside the organization's premises. Adequate security controls should be in place e.g. use of cryptographic techniques, to prevent unauthorized access to or disclosures of the information, stored and processed by these facilities.

12.8.2 It is important that when such facilities are used in public places, care is taken to avoid the risk of overlooking by unauthorized persons. Procedures against malicious software should be in place and be kept up to date. Equipment should be available to enable quick and easy back-up of information. These back-ups should be given adequate protection against safety hazards e.g. theft or loss of information.

12.8.3 Suitable protection should be given to the mobile computing facilities, connected to networks. Remote access to business information and information systems across public network using mobile computing facilities should take place only after successful identification and authentication of the user under suitable access control mechanisms in place.

12.8.4 Mobile computing facilities should be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centres and meeting places. Equipment carrying important, sensitive and/or critical business information should not be left unattended and, where possible, should be physically locked away or special locks should be used to secure the equipment.

12.8.5 Training should be arranged for the staff using mobile computing facilities to raise their awareness about the additional risks to business operations, which may result from this way of working and the security controls which will have to be implemented.

Chapter 13

Voice, Telephone and related Equipment and Security Controls

13.1 Information is carried frequently by voice media. Security controls require to apply to voice as well as the carrier/medium of transmission of the voice. This applies to the voice related information, used in the conduct of business only and does not cover social conversation. The organisations which utilize the Voice Mail Systems will be 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 Systems Security Administrator to be involved in the review and implementation of appropriate controls, offered by the vendor in order to reduce or eliminate these exposures. Controls which should be used to protect voice and related information are discussed hereunder.

13.2 Access to Voice Mail system :

To preserve the integrity of information residing on Voice Mail and to limit expenses and liability for unauthorized use of Voice Mail services, the access to Voice Mail service should be controlled with physical controls and with logical access controls, as discussed in this document.

13.3 Private Branch Exchange (PBX) :

A PBX is an internal switch for attached telephone units within an organisation that usually supports connections to outside telephone lines and may also support electronic switching of information to the 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 disclosures, modifications or destruction, the following steps should be implemented:

a) Maintain close liaison with the PBX supplier and the network service providers concerning frauds and other problems.

b) Provide physical access controls that restrict access to the PBX to authorized individuals only.

c) Protect any maintenance or administrative ports that are accessible via remote dial-up

with passwords meeting the access control criteria, as discussed in this document. This may require secure call-back or challenge/response procedures.

d) Produce an audit trail of all the administrative and maintenance accesses.

e) Change all default password settings immediately upon installation of a PBX.

f) Follow the approved change control procedures, documenting all changes, as discussed in this document.

g) Use call accounting software.

h) Prevent access to local "hot numbers" or other expensive services.

i) Follow the least privilege on the setting up of facilities for particular extensions e.g. deny international access unless explicitly authorized.

13.4 Spoken Word :

To educate the employees to the sensitivity of information being discussed regardless of the circumstances, it should be ensured to advise the employees periodically 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 the persons who are party to the conversation or the meeting are aware of the sensitivity of the information.

13.5 Interception :

It may be easy to intercept the cellular and the cordless telephonic conversations. To protect against interception of highly sensitive information during telephonic conversations, the following steps should be taken :

a) Consider encrypting the telephone calls in which highly sensitive information will be discussed.

b) Prohibit the use of the cordless or the unencrypted cellular telephones for the transmission of HIGHLY SENSITIVE information, except in emergencies.

13.6 Business Continuity :

To ensure the continued availability of the Voice Mail and telephone services, it should be ensured to include the continuation of the telephone and the Voice Mail services as part of the contingency and disaster recovery plans of the organisation.

13.7 Documentation :

To preserve a record of telephone transaction requests and to prevent action on unauthenticated requests, it should be ensured to verify the requests for transaction, received from outside the organisation via telephone or Voice Mail or by call back, using the Cryptographic Authentication or other means, as approved under the Information Systems Security Programme. However, the telephone transaction requests which are part of the business activities, traditionally conducted over the telephones, such as foreign exchange or arbitrage, should be conducted on the recorded telephone lines. The recordings should be retained at least as long as and as required under the statute of limitations for any legal action or crime that may arise from the transactions in question.

13.8 Voice Response Units (VRU) :

The Voice Response Units may be used as a means to allow the 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 etc. To provide a high degree of assurance that the accounts will only be accessed by the true owners and no one else, the following steps should be taken:

a) Use of the customer selected Personal Identification Numbers (PINs). The PINs, used in a low risk application and which may not require encryption, should be limited to that application only.

However, normal security practice requires encryption.

b) Notify to all the account owners the PIN selection process.

c) Provide the ability to the owner to block the account from service/ operation.

e) Protect the customers' PINs after they are acquired by the VRU, the PINs, once received by the VRU, should be encrypted prior to validation by the VRU or any other system to which such PINs may be transmitted.

f) Limit the opportunity for unauthorised attempts to sign on to the system, it should be ensured to allow the 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 behaviour could be identified.

13.9 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 a sophisticated totally paperless image processing system with image files transmitted via e-mail. Where possible in an organisation to prevent unauthorised access, the use of a Central Fax Server should be considered. The following controls should be implemented.

13.9.1 Modification :

To prevent possible payment on fraudulently altered facsimile images, it should be ensured to have independent verification by prearranged method of the authenticity of the source and the contents of such transaction requests, received via facsimile or image system, prior to action being taken.

13.9.2 Repudiation :

To prevent false claims of the communication of messages or for the denial of message delivery, it should be ensured to apply non-repudiation controls such as digital signatures.

13.9.3 Misdirection of Messages :

To reduce the disclosure of sensitive or highly sensitive information through misdirected facsimile transmission, it should be ensured to exercise care in dialing fax numbers. A check of the fax display of the identity of the receiver should be done. To detect fax messages which were misdirected and to assist in the retrieval of information, it should be ensured to display warning notices on the fax coversheets to the effect that the message is meant for the addressee only, for his information and use and that the use of the message by any other party will be deemed illegal and shall be punishable under law.

13.9.4 Disclosure :

To prevent disclosure of information during transmission, it should be ensured to encrypt fax and image transmissions carrying highly sensitive information. To prevent disclosure of information by unauthorised viewing of unattended facsimile equipment, the following steps should be taken :

a) Locate the facsimile machines and the image processing terminals within areas under physical access control.

b) Prohibit fax transmissions carrying sensitive or highly sensitive information, unless it is verified by independent means that a properly authorized person is present at the receiving terminal.

c) One method of doing this is to send the cover sheet only, wait for telephonic acknowledgement of its receipt and then to resend the entire package using the redial button on the fax device.

d) Classify and label the documents in the image systems or received via fax using the same criteria used for paper documents.

Documents should bear markings appropriate to their classification.

e) The use of cellular facsimile raises potential disclosure concerns.To protect against disclosure of fax sent via cellular connection, the transmission of cellular fax of sensitive or highly sensitive information should be prohibited, unless encryption is in use.

13.9.5 Business Continuity :

To ensure against business interruption due to loss of image systems, it should be ensured to include image systems and fax capability as part of the contingency and disaster recovery plan.

13.9.6 Denial of Service :

To minimize the loss of service caused by junk fax or unsolicited and unwelcome messages, it should be ensured to block disclosure of fax numbers outside the organisation, except on a need-to-know basis. It should be adopted as a practice that the fax lines that the organisation may want to establish for its business should not be used for other purposes.

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

Chapter 14

Electronic Mail and Security Controls

14.1 Electronic Mail (e-mail) is store and forward message system for transporting information between two or more parties. The e-mail was originally developed to support informal communications over the computer systems. It has now been integrated with the word processing systems, so that a sender can compose a formal letter and have it instantly transmitted. The e-mail may also incorporate digitised voice, messages and images. It may operate over public or private networks. It is being used for business communications, replacing traditional forms of communication such as telex and letters. The e-mail differs from traditional forms of business communications by, for example, its speed, message structure, degree of informality and vulnerability to unauthorized actions. The following controls should be implemented to protect e-mail :

14.1.1 Authorized Users :

To ensure that only authorized users access e-mail, it should be ensured to restrict access to e-mail facility by logical access control, as discussed in this document. E-mail facility will have to be used as approved by the organisation and necessary steps to be taken to ensure the same.

14.1.2 Physical Protection :

To prevent modifications, disclosures or destruction of information and information processing capabilities through access to equipment providing e-mail services, it should be ensured to restrict physical access to information processing resources providing e-mail services to those personnel necessary for the operation of the system. A record of the entry and exit to the facility should be maintained.

14.1.3 Integrity of Transactions :

To prevent unauthorized transactions or repudiation of transactions, it should be ensured to obtain independent verification of authenticity as to the source and content, prior to the completion of such transactions requested via e-mail.

14.1.4 Disclosure :

To protect against the disclosures of sensitive or highly sensitive Information, using the same criteria as used for the paper documents, it should be ensured to prohibit the transmission of highly sensitive information over e-mail, unless encrypted. To minimize the chances of wrong delivery and the consequences thereof, the following steps should be taken :

a) The e-mail messages carrying sensitive or highly sensitive information be checked for correct addressing and routing information. Use of warning messages, similar to those as in case of fax, should be considered.

b) Select public network providers from those who provide protection against wrong delivery.

14.1.5 Business Continuity :

To ensure business continuation in case of loss of e-mail service, it should be ensured to include the continuation of e-mail service as part of the contingency and disaster recovery plan, as discussed in this document.

14.1.6 Message Retention :

To ensure that the messages, required for business and regulatory reasons, are safely stored and easily retrievable, it should be ensured to implement a record retention programme, appropriate to business and regulatory requirements. To ensure that the messages archived can be properly reconstructed and authenticated, the public key certificates or authentication keys, used during the processing of such messages, should be archived.

14.1.7 Message Reception :

To ensure that all the messages are received and action taken thereon, the senders should ensure that their messages are received and read. The organisation should consider using an automated status checking facility for the purpose.

14.2 Policy on Electronic Mail :

Policy should be established regarding the use of electronic mail, including the following:

a) attacks on electronic mail e.g. viruses, interception;

b) protection of electronic mail attachments;

c) guidelines on when not to use electronic mail;

d) employee responsibility not to compromise the company e.g. sending defamatory electronic mail, use of electronic mail for harassment etc.;

e) use of cryptographic techniques to protect the confidentiality and integrity of electronic messages ;

f) retention of messages which, if stored, could be discovered in case of litigation; and

g) additional controls for vetting messaging which cannot be authenticated.

14.3 Paper Documents :

Cheques and currency notes are outside the purview of the discussion in this sub-section. Much of the information used for decision making is first captured on paper. The pre-printed forms such as deposit slips, loan applications and memoranda of telephone transfer requests are useful for a variety of financial operations. Regulators also require certain reports to be submitted in writing. The following controls should be used for protection of paper resources.

14.3.1 Modification :

To prevent the modifications of information, received or stored on paper documents, the following steps should be taken :

a) Prohibit the use of pencils or other erasable implements for the preparation of documents, used as source for payments, loans or other transactions.

b) Require the use of erasure detection paper for high value documents.

c) Reject document as source document for any transaction that contains Strike-outs,

correction fluid marks or typed over text, unless such corrections or additions are initialled/authenticated by all the signatories to the document.

14.3.3 Viewing :

To protect against unauthorized viewing of sensitive or highly sensitive information on documents, it should be ensured to make the employees aware of the importance of information security. Leaving paperwork containing sensitive or highly sensitive information open to view by others should be pointed out as an example of an unacceptable security practice.

14.3.4 Storage Facilities :

To ensure the safe storage of documents containing critical, sensitive or highly sensitive information. However, such information remaining open to view should be pointed out as an example of an unacceptable security practice.

14.3.5 Destruction :

To ensure that information is not disclosed because of improper disposal of the documents, the following steps should be taken :

a) The sensitive or highly sensitive documents are securely destroyed.

b) Establish a policy covering the destruction of records. The type of record, its sensitivity, statutory limitations and other applicable regulations should be used to determine a destruction date. This policy should be reviewed periodically.

Chapter 15

Firewall - A Security Control Measure

15.1 The increased use of the Internet has simultaneously made computer technology more useful and at the same time, more risky. The universal connectivity, which is nothing short of a miracle, also presents unprecedented risks/opportunities for attack. Any person with a computer can subscribe to an Internet service provider and become a true network "node." As a result, there is no control over who can be on the Internet or what they are using it for. There is, therefore, a need to protect systems on the Internet from against both known and unknown assaults from a vast pool of attackers/hackers. This protection is generally provided in the form of a Firewall. A Firewall is defined as a collection of electronic components placed between two networks that collectively have the following properties:

a) All traffic from inside to outside and vice-versa must pass through the firewall.

b) Only authorized traffic, as defined by the information systems security policy, will be allowed to pass through the firewall.

c) The firewall is itself immune to penetration.

A well-designed firewall protects the organisation's network against attacks from sources external to its network and the network to which it is connected by the firewall. The attacks from within the organisation's network or from its communicating partner/s will require to be addressed by other security services.

15.2 The firewalls require to be designed for the following considerations :

15.2.1 Strong Authentication and Identification :

A high degree of confidence of knowing with whom an organisation has been dealing is required. "Know your Customer" could be a regulatory requirement and must precede any authorization to conduct business. The ability to identify who is using a system is required to prevent unauthorized use as also to assist in the investigation of attacks.

15.2.2 Audit and Archival Requirements :

The organisations are required by regulation to maintain certain records. The activity through a firewall will often contain information which must be archived to prove that the

transactions had taken place. Auditable security-related events must also be properly captured.

15.2.3 Non-repudiation :

Payment instructions will require to be sufficiently protected to support a collection action.

15.2.4 Availability :

Unless a service can be reliably offered, it should not be offered. The frustration of the customer over the banking systems which do not work on demand, on the introduction of Information Technology based products, may result in loss of business.

15.2.5 Confidentiality of Records :

The confidence that the banking organisation's records will remain protected is a customer's assumption. Loss of this confidence will result in loss of business. Further, it can be presumed that causing embarrassment to a big organisation is a powerful motivator to the hacker community.

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

15.2.6.1 Design Axioms : The following basic requirements should be complied with.

a) Any interface of the internet to the organisation's networks must be properly controlled.

b) IP packets will be exchanged between the organisation's network and the Internet through connection/s established through the firewall.

c) Traffic is exchanged through the firewall at the application layer only.

d) Organisation's hosts, which support incoming service requests from the public Internet, will sit "outside" any firewall with suitable security controls, preferably in a DMZ zone, separate from the internal 'trusted network'.

e) Firewall systems will be implemented to work within the constraints of internal network routing.

15.2.6.2 The technical features to be met are as under :

a) The firewall must enforce a protocol discontinuity at the transport layer.

b) The firewall must hide the structure of the protected network.

c) The firewall must provide an audit trail of all communications to or through the firewall system and will generate alarms when suspicious activity is detected.

d) The firewall system must use a "proxy server" to provide application gateway function through the firewall.

e) The routes through the firewall must be statically defined.

f) The firewall must not accept session initiation from the Public Internet.

g) The firewall system must defend itself against direct attack.

h) The firewall must be structured, so that there is no way to bypass any firewall component.

j) The firewall must include an application "launch server" to support application connections from the user systems to Internet services.

k) The firewall must deny all in-bound and out-bound services unless specifically permitted.

l) The firewall must be so configured as to log all reports on daily, weekly and monthly basis. Software tools or such utilities to be used for programatically summarising the log entries or the associate actions with the log file entries.

m) The firewall administrator will have to be notified of security alarms by e-mail, pager or other means. The alarms, among others, may relate to 'N' failed attempts to connect to any service port within a time span of 'N' minutes, 'N' consecutive failed attempts to utilise Proxy Services etc. The failed attempts to be directly logged into the firewall

system.

15.2.6.3 The Proxy Server, configured on the firewall, should have the following features:

a) The proxy server acts as an application gateway.

b) The proxy server hides Internet details of the protected network from the public Internet.

c) The proxy server does not switch any network level packets. d) The proxy server logs all activities in which it is involved. e) There are no user accounts on the proxy server itself.

15.2.6.4 The 'Launch Server' should have the following features :

a) The launch server houses only client applications.

b) User logins on the launch server must be different from the user's "home account."

c) The launch server should be based on a different hardware and software platform than on the user "home" systems.

Chapter 16

Implementation of Cryptographic Controls

The growth in information technology has made the traditional methods of controlling information much more challenging. The popularisation and extensive use of cryptographic devices has provided the financial organisations with the opportunity to maintain high level of security in business operations, while reaping benefits from the increased use of Information Technology. The organisations should bear the following factors in view while taking decision on the selection, use and evaluation of their cryptography-based controls.

16.1 Cryptographic Controls :

Cryptographic systems and techniques should be used for the protection of the confidentiality, authenticity and integrity of information that is considered at risk and for which other security controls do not provide adequate protection.

16.2 Policy on the Use of cryptographic Controls :

Making a decision as to whether a cryptographic solution is appropriate should be seen as part of a wider process of assessing risks and selecting security controls. A risk assessment should be carried out to determine the level of protection that information should be given. This assessment can then be used to determine whether a cryptographic control is appropriate, what type of control should be applied and for what purpose and which business process. An organization should develop a policy on its use of cryptographic controls for protection of its information. Such a policy is necessary to maximize benefits and minimize the risks of using cryptographic techniques and to avoid inappropriate or incorrect use. When developing a policy for the purpose, the following should be considered :

a) the management approach towards the use of cryptographic controls across the organization including the general principles under which business information should be protected;

b) the approach to key management, including methods to deal with the recovery of the encrypted information in the case of lost, compromised or damaged keys;

c) Roles and responsibilities e.g. who is responsible for :

l the implementation of the policy; and l the key management;

d) how the appropriate level of cryptographic protection is to be determined; and

e) the standards to be adopted for the effective implementation throughout the organization (which cryptographic solution is used for which business process).

16.3 Encryption :

Encryption is a cryptographic technique that can be used to protect the confidentiality of information. It should be considered for the protection of sensitive or critical information.

Based on a risk assessment, the required level of protection should be identified, taking into account the type and quality of the encryption algorithms and the length of the cryptographic keys to be used. When implementing the organization's policy on cryptography, consideration should be given to the regulations and national restrictions that might apply to the use of cryptographic techniques in different parts of the world and to the issues of trans-border flow of encrypted information. In addition, consideration should also be given to the controls that apply to the export and import of cryptographic technology. Specialist advice should be sought to identify the appropriate level of protection, to select suitable cryptographic products that will provide the required protection and the implementation of a secure key management. In addition, legal advice may need to be sought regarding the laws and regulations that might apply to the organization's intended use of encryption.

16.4 Applying Encryption :

16.4.1 What to Encrypt?

Information requiring confidentiality protection should be encrypted if

a) the information will be appearing outside the direct control of the organisation;

b) the information is to be stored or transported on removable media; and

c) the information is to be transmitted over telephone, fax or computer networks.

Information not requiring confidentiality protection should not be separately encrypted.

16.4.2 How to Encrypt ? :

Several issues will have to be considered to determine how best to encrypt. These issues relate to hardware versus software encryption products, end-to-end or local encryption, placement in the OSI model and key management issues.

16.4.2.1Hardware Versus Software Encryption Products :

Encryption products exist in either hardware or software form. Hardware devices can be stand-alone devices which attach to a communications port or an electronic equipment with in-built microcircuit. Software encryption products can be individual products which encrypt any file which may be sent or can be integrated into other applications. The hardware encryption products should be used to address the following requirements :

a) when assurance is required that the encryption product is operating as specified ; and

b) whenever possible.

The software encryption products should be used to address the following requirements :

a) the cost as a major factor ;

b) assurance that the encryption product operates as specified ; and

c) compensating controls can verify that the software is operating as specified. For example, customers who will not accept additional hardware in their systems may request cryptographic services within a software package. In this case, a certain amount of assurance can be achieved, if these applications communicate with the hardware cryptographic devices.

16.4.2.2 End-to-End, Link or Local Encryption:

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

a) significant communications exist between the facilities;

b) other controls protect information within a building or campus ; or

c) controls are in place to ensure that information in need of protection will be routed over the designated links.

The end-to-end encryption should be used to address the following requirements :

a) communication between one or more central facilities and individual users ;

b) a small number of users are involved within a given enterprise ;

c) protection is required end-to-end ; or

d) link encryption is not warranted.

The encryption should be used in local mode to address the following requirements :

a) information is to be protected in storage by an individual user ; or

b) key management prevents unauthorized use of the encryption facility.

16.4.2.3 The Open Systems Interconnection (OSI) Layer :

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

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

The encryption capability should be placed at Layer 2 when link encryption is specified.

The encryption capability should be placed at Layer 4 when all traffic from a given terminal is to be encrypted.

The encryption capability should be placed at Layer 6 when encryption is to be treated as a service to be called from multiple applications.

The encryption capability should be placed at Layer 7 when the protection of an application is specified.

16.4.3 Who Controls Encryption ? :

Organisations employing encryption must determine who can control the use of the encryption services. Encryption is a two-edged sword. It can protect the organisation's information. It can also assist a dishonest employee in stealing the organisation's assets or holding a database at ransom. To ensure that encryption is properly controlled, the following steps should be implemented :

? To establish corporate policies on the use and control of encryption.

? To limit control of encryption services to the most trustworthy individuals in the organisation.

? To establish positive organisational control over all cryptographic keying material.

? To ensure that no single individual can access keys or change keys to a value chosen by that individual.

? To ensure proper key management.

16.4.4 Physical and Logical Security of Encryption Products :

The organisation has to ensure that proper physical and logical security controls, as discussed

in this document, are applied to cryptographic products.

16.4.5 Choice of Encryption Algorithms :

To ensure the highest quality of encryption, the algorithms contained in ISO developed standards or such other standards, accepted internationally, should be considered for use by financial organisations.

Chapter 17

Digital Signatures - A Security Control Measure

17.1 Why Digital Signatures are required ?

As the information processing systems are automated, it is observed that the paper based documents are being stored and processed in electronic form. Documents in electronic form facilitates rapid processing and transmission and thereby improves the overall efficiency of the information systems and the business processes. However, approval of a written document has traditionally been indicated by written signatures. There is a need for an electronic equivalent to the written signatures, which would be recognized to have the desired legal status. Merely digitizing the written signatures - converting the signature into a series of numbers - is not an acceptable alternative, since the digitized signatures bear no relationship to the data that is being signed.

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

Digital signatures provide a means of protecting the authenticity and integrity of the electronic documents. For example, they can be used in electronic commerce where there is a need to verify who has signed an electronic document and to check whether the contents of the signed document have been changed in transit. Digital signatures can be applied to any form of document being processed electronically e.g. they can be used to sign electronic payments, funds transfers, contracts and agreements.

Digital signatures can be implemented using a cryptographic technique based on a uniquely related pair of keys, where one key is used to create a signature (the private key) and the other to check the signature (the public key). Care should be taken to protect the confidentiality of the private key. This key should be kept secret, since anyone having access to this key can sign documents e.g. payments, contracts, and thereby forging the signature of the owner of that key. In addition, protecting the integrity of the public key is important. Consideration needs to be given to the type and quality of the signature algorithms used and the length of the keys to be used. Cryptographic keys used for Digital signatures should be different from those used for encryption. When using Digital signatures, consideration should be given to any relevant legislation that describes the conditions under which a digital signature is legally binding.

Non-repudiation services should be used where it might be necessary to resolve disputes about the occurrence or the non-occurrence of an event or action e.g. dispute involving the use of a digital signature on an electronic contract or payment. They can help establish evidence to substantiate whether a particular event or action has taken place e.g. denial of sending a digitally signed instruction using electronic mail. These services are based on the use of encryption and digital signature techniques.

17.2 How to generate Digital Signatures?

Security architectures have emerged, based on public key cryptography, that facilitate authentication via digital signature implementation in smart cards or PCMCIA (Personal Computer Memory Card Industry Association) cards. These cards contain the private key associated with the individual. Thus, the transactions 'signed' with the private key can be validated by anyone with access to the individual's public key. This provides a close association between a document and an individual who possesses the authority to bind the organisation to the contents of a document. Furthermore, these cards can also contain secret encryption keys used in symmetric encryption operations. As with tokens, card systems should provide PIN number entry services. To assure that the digital signatures, used by the organisation, deliver proper non-repudiation, the following steps should be taken:

a) Limit the signature authority to those individuals who have been authorised/entrusted to bind the organisation.

b) Use digital signature standards, accepted by ISO or by competent national authorities.

c) The parameters and the keying materials are properly generated and used.

17.3 Certification :

A digital signature is a value derived from the message being signed by an appropriate cryptographic algorithm and the 'secret' key half of an asymmetric key pair. Any party who holds the 'public' half of the key pair can verify that the holder of the 'secret' key half was the party signing the message. The party verifying must have some assurance that the 'public' key half is indeed the one associated with the signing party. This assurance is accorded by the Certification Authorities, mutually trusted third parties, who can cryptographically bind an individual to his 'public' key. The Certification Authorities can exist in a hierarchy. All that is required is for both the parties to a transaction to have at least one common authority in its set of relationships, the Certification Authorities could be different with proper agreement between them for facilitating, among others, cross verification. If the two parties have identified a common Certification Authority, that authority's public key must be well known or delivered with integrity protection to preclude system compromise.

17.4 Legal standing of Digital Signatures :

The Information Technology Act, 2000 recognises the legal validity of digital signatures for the purpose of authentication and non-repudiation. The parties conducting business under a pre-existing contract may suitably modify the same and use digital signature for the purpose of authentication and non-repudiation.

17.5 Certificate (Key) Management :

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

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

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

17.5.1 Protection of Cryptographic Keys :

The management of cryptographic keys is essential to the effective use of cryptographic techniques. Any compromise or loss of cryptographic keys may lead to a compromise of the confidentiality, authenticity and/or integrity of information. A management system should be in place to support the organization's use of the two types of cryptographic techniques, which are as discussed hereunder :

a) secret key techniques, where two or more parties share the same key and this key is used both to encrypt and decrypt information.

This key has to be kept secret since anyone having access to it is able to decrypt all information being encrypted with that key or to introduce unauthorized information.

b) Public key techniques, where each user has a key pair, a public key (which can be revealed to any one) and a private key (which has to be kept secret). Public key techniques can be used for encryption and to produce digital signatures.

All keys should be protected against modifications and destruction and secret and the private keys need protection against unauthorized disclosures. Cryptographic technique can also be used for this purpose. Physical protection should be used to protect equipment used to generate, store and archive keys.

17.5.2 Standards, Procedures and Methods :

A key management system should be based on an agreed set of standards, procedures and secure methods for :

a) generating keys for different cryptographic systems and different applications;

b) generating and obtaining public key certificates;

c) distributing keys to intended users, including how keys should be activated when received;

d) storing keys, including how authorized users obtain access to keys;

e) changing or updating keys including rules on when keys should be changed and how this will be done;

f) dealing with compromised keys;

g) revoking keys including how keys should be withdrawn or deactivated e.g. when keys have been compromised or when a user leaves an organization (in which case keys should also be archived);

h) recovering keys that are lost or corrupted as part of business continuity management e.g. for recovery of encrypted information;

i) Archiving keys e.g. for information archived or backed up;

j) Destroying keys; and

k) Logging and auditing of key management related activities.

17.5.3 In order to reduce the likelihood of compromise, keys should have defined activation and deactivation dates, so they can only be used for limited period of time. This period of time should be dependent on the circumstances under which the cryptographic control is being used and the perceived risk. Procedures may need to be considered for handling legal requests for access to cryptographic keys e.g. encrypted information may need to be made available in an unencrypted form as evidence in a court case.

In addition to the issue of the securely managed secret and private keys, the protection of the public keys should also be considered. This problem is addressed by the use of a public key certificate. These certificates should be produced in a way that uniquely binds the information related to the owner of the public/private key pair to the public key. It is, therefore, important that the management process that generates these certificates can be trusted. This process is normally carried out by a Certification Authority, which should be a recognized organization

with suitable controls and procedures in place to provide the required degree of trust.
The terms and conditions of the service level agreements or contracts with external suppliers of cryptographic services e.g. with a Certification Authority, should cover issues of liability, reliability of services and response time for the provision of services.

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

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

To ensure that the non-repudiation service is properly used, the following steps should be taken :

a) Address non-repudiation in the overall information security policy for the organisation.

b) Select personnel who may be authorized to digitally sign the messages in the same manner as the selection of personnel who may sign paper documents of a similar nature.

c) Select a Certification Authority with extreme care.

d) Establish a Certification Authority for the organisation.

17.6 Choice of Algorithm :

To ensure proper digital signature operation, it should be ensured to allow only ISO specified algorithms or those accepted internationally, to be used.

17.7 Generation of Cryptographic Keys :

To ensure that the cryptographic keys are not predictable, the following steps should be taken :

a) Generate sector keys using random or pseudo random generation techniques, such as found in ISO or in those other internationally accepted standards.

b) Consider central generation using a single high-quality random or pseudo random source and to monitor for continuing quality of output.

To assure that the asymmetric keys are properly generated, the required tests for the primality or other requirements that yield low probability of error should be performed.

17.8 Distribution of Cryptographic Keys :

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

17.8.1 Distribution of Secret Keys :

The Keys which must be kept secret include symmetric keys and the secret 'private' key in asymmetric crypto-systems. To protect cryptographic keys during distribution, it should be ensured to observe all the requirements of ISO or such other internationally accepted products for the transport of keys.

17.8.2 Distribution of Public Keys :

To ensure the validity of the public keys in an asymmetric crypto system, the following steps should be taken ;

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

b) Enforce the use of the key certificates.

17.9 Storage of the Cryptographic Keys :

Another area of concern is the storage of the back-up copies of the keys in use including the future and the discontinued keys. Both require the ability to protect these keys from disclosures or substitution, but, at the same time, must also be available for access and audit by the authorized personnel. To ensure safe storage and retrieval of the cryptographic keys, it should be ensured to enforce the requirements of ISO security standards or such other internationally accepted standards for the storage and archiving of the keys.

17.10 Public Key Certification and Standards :

To ensure that asymmetric-algorithm based crypto systems deliver the full measure of security for which they are intended, the following steps should be taken:

a) The use of a Certification Authority which operates using ISO approved standards or such other nationally approved standards.

b) Address the issues of liability in service contract with external Certification Authorities.

c) Reference to the Certificate Revocation Lists (CRLs) periodically or before transactions involving amounts in excess of a given limit.

d) Incorporate certification service with data recovery services.

Chapter 18

Certification Authorities(CA)/Trusted Third Parties (TTP)

18.1 Many markets have recognized the need for enhanced security services, provided by an entity, mutually trusted by the other entities. These services range from increasing trust or business confidence in specific transactions to provision for the recovery of information for which encryption keys are not otherwise available to authorized entities. Trusted Third Parties (TTP) are the vehicles for the delivery of such services. For the banking and financial services industry, TTP technology offers a vehicle by which an organisation can deliver assurances between its sub-divisions, between itself and its customers and between itself and its correspondent organisations. An organisation may choose to set up an internal TTP function or subscribe to an external provider for TTP services. The banking and financial organisations desiring to use the TTP services should consider the following :

18.1.1 Assurance :

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

a) Trust : Is the TTP organized, controlled and regulated in such a way that its operation can be relied upon, checked and verified?

b) Accreditation : Is the TTP accredited by the recognized national, regional or international groups?

c) Compliance : Is the TTP operating in compliance with accepted industry standards and all relevant regulations?

d) Contract : Is there a legally binding contract in place covering the provisions of the service and addressing of all the issues in this list? Are there contracts with co-operating TTPs which also address these concerns?

e) Liability : Is there a clear understanding as to the issues of liability? Under what circumstances is the TTP liable for damages? Does the TTP have sufficient resources or insurance to meet its potential liabilities?

f) Policy Statement : Does the TTP have a security policy covering technical,

administrative and organizational requirements?

18.2 Services of a TTP :

The services which a TTP can provide include as under :

a) Issue of Digital Certificates

b) Key Management for symmetric crypto-systems

c) Key Management for asymmetric crypto-systems

d) Key Recovery

e) Authentication and Identification

f) Access Control

g) Non-repudiation

Key recovery is the ability of the TTP to recover either mathematically or through secure storage or through other procedures, the proper cryptographic key used for encryption of information using the organisation's information processing resources. This function would assure an organisation that it can always have access to information within its information processing resources. Such recovery services may be essential in disaster recovery.

18.3 Network of TTPs :

A network of co-operating TTPs require to be developed before the full potential of the TTPs can be realized. The competition between the TTPs may reduce cost at the risk of offering reduced levels of service or assurances. However, the confidence in the organisation and the financial services sector has to be preserved.

18.4 Legal Issues :

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

Liability for the misfeasance, malfeasance or non-feasance of the TTP including direct and consequential damages must also be fully understood and agreed upon. The TTP must have adequate financial reserves or insurance to meet any liability.

Banking and financial organisations in many jurisdictions are obliged to protect the privacy rights of their customers, especially the safeguarding of the personal data. These obligations are sometimes at odds with the requirements under law relating to access to information. The contract with an external TTP or the operating procedures of an internal TTP should address both these concerns.

Chapter 19

Business Continuity Planning Framework/Disaster Recovery Planning (DRP)

19.1 A business continuity management process should be implemented to reduce the disruption, caused by disasters and security failures (which may be the result of, for example, natural disasters, accidents, equipment failures and deliberate actions) to an acceptable level through a combination of preventative and recovery controls. The consequences of disasters, security failures and loss of service should be analyzed. Contingency plans should be developed and implemented to ensure that business processes can be restored within the required time-scales. Such plans should be maintained and practiced to become an integral part of all other management processes. Business continuity management should include controls to identify and reduce risks, limit the consequences of damaging incidents and

ensure the timely resumption of essential operations.

A single framework of business continuity plans should be maintained to ensure that all plans are consistent and to identify priorities for testing and maintenance. Each business continuity plan should specify clearly the conditions for its activation, as well as the individuals responsible for executing each component of the plan. When new requirements are identified, the established emergency procedures e.g. evacuation plans or any existing fallback arrangements, should be amended as appropriate. A business continuity planning framework should consider the following :

a) the conditions for activating the plans which describe the process to be followed (how to assess the situation, who is to be involved, etc.) before each plan is activated;

b) emergency procedures, which describe the actions to be taken following an incident which jeopardizes business operations and/ or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities e.g. police, fire service and local government;

c) fall back procedures which describe the actions to be taken to move essential business activities or support services to alternative temporary locations and to bring business processes back into operation in the required time-scales;

d) resumption procedures which describe the actions to be taken to return to normal business operations;

e) a maintenance schedule which specifies how and when the plan will be tested and the process for maintaining the plan;

f) awareness and education activities which are designed to create understanding of the business continuity processes and ensure that the processes continue to be effective;

g) the responsibilities of the individuals, describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.

Each plan should have a specific owner. Emergency procedures, manual fallback plans and resumption plans should be within the responsibility of the owners of the appropriate business resources or processes involved. Fallback arrangements for alternative technical services such as the information processing and communications facilities should be carried out in co-ordination with the service providers/contractors/ suppliers under written agreement/contract, setting out the roles and responsibilities of each party for meeting the emergency situations as also the imposition of penalties including legal actions, to be initiated by the organisation against the service providers/contractors/suppliers in the event of non-compliance/non-co-operation on their part.

19.2 Business Continuity Management Process :

There should be a managed process in place for developing and maintaining business continuity throughout the organization. It should bring together the following key elements of business continuity management.

a) understanding the risks the organization is facing in terms of their likelihood and their impact, including an identification and prioritization of critical business processes;

b) understanding the impact which interruptions are likely to have on the business (it is important that solutions are found that will handle smaller incidents as well as serious incidents that could threaten the viability of the organization) and establishing the business objectives of the information processing facilities;

c) Considering the purchase of suitable insurance which may form part of the business continuity process;

d) Formulating and documenting a business continuity strategy consistent with the agreed business objectives and priorities;

e) Formulating and documenting business continuity plans in line with the agreed strategy;

f) Regular testing and updating of the plans and processes put in place; and

g) The management of business continuity is incorporated in the organization's processes and structure.

19.3 Business Continuity and Impact Analysis :

Business continuity should begin by identifying the events that can cause interruptions to business processes e.g. equipment failure, flood and fire. This should be followed by a risk assessment to determine the impact of those interruptions (both in terms of damage scale and recovery period). Both of these activities should be carried out with full involvement from owners of business resources and processes. This assessment considers all business processes and is not limited to the information processing facilities. Depending on the results of the risk assessment, a strategic plan should be developed to determine the overall approach to business continuity. Once this plan has been created, it should be approved by management.

19.4 Writing and Implementing Business Continuity Plans :

Plans should be developed to maintain or restore business operations in the required time scales following interruption to, or failure of, critical business processes. The business continuity planning process should consider the following:

a) identification and agreement of all responsibilities and emergency procedures;

b) implementation of the emergency procedures to allow recovery and restoration in required time-scales. Particular attention needs to be given to the assessment of the external business dependencies and the contracts in place;

c) documentation of the agreed procedures and processes ;

d) Appropriate education of staff in the agreed emergency procedures and processes including crisis management;

e) Testing and updating of the plans.

Examples of situations that might necessitate updating the plans include the acquisition of new equipment or the upgradation of the operational systems and changes in :

a) personal;

b) addresses or telephone numbers;

c) business strategy ;

d) location, facilities and resources;

e) legislation;

f) contractors, suppliers and key customers;

g) processes - new/withdrawn ones; and

h) risk (operational and financial)

19.5 Testing, Maintenance and Re-assessment of Business Continuity Plans :

19.5.1 Testing the Plans :

Business continuity plans may fail on being tested, often because of incorrect assumptions, oversights or changes in equipment or personnel. They should, therefore, be tested regularly to ensure that they are up to date and effective. Such tests should also ensure that all members of the recovery team and other relevant staff are aware of the plans. The test schedule for business continuity plans(s) should indicate how and when each component of the plan should be tested. It is recommended to test the individual components of the plans(s) frequently. A variety of techniques should be used in order to provide assurance that the plan(s) will operate in real life. These should include:

a) table-top testing for various scenarios (discussing the business recovery arrangements using example interruptions) ;

b) simulations (particularly for training people in their post-incident/ crisis management roles);

c) technical recovery testing (ensuring information systems can be restored effectively);

d) testing recovery at an alternate site (running business processes in parallel with recovery operations away from the main site) ;

e) tests of supplier facilities and services (ensuring externally provided services and products will meet the contracted commitment); and

f) complete rehearsals (testing that the organization, personnel, equipment, facilities and processes can cope with interruptions).

The techniques can be used by any organization and should reflect the nature of the specific recovery plan.

19.5.2 Maintenance and Re-assessment of the Plans :

Business continuity plans should be maintained by regular reviews and updates to ensure their continuing effectiveness. Procedures should be included within the organization's change management programme to ensure that business continuity matters are appropriately addressed. Responsibility should be assigned for regular reviews of each business continuity plan. The identification of changes in business arrangements, not yet reflected in the business continuity plans, should be followed by an appropriate update of the plan. This formal change control process should ensure that the updated plans are distributed and reinforced by regular reviews of the complete plan. **C**onsideration should be given to the possibility of degradation of media used for storage of records. Storage and handling procedures should be implemented in accordance with manufacture's recommendations.

Where electronic storage media are chosen, procedures to ensure the ability to access data (both media and format readability) throughout the retention period should be included, to safeguard against loss due to future technology change. Data storage systems should be chosen such that the required data can be retrieved in a manner acceptable to a court of law e.g. all records required can be retrieved in an acceptable timeframe and in an acceptable format. The system of storage and handling should ensure clear identification of records and of their statutory or regulatory retention period. It should permit appropriate destruction of records after that period if they are not needed by the organization.

To meet these obligations, the following steps should be taken within an organization.

a) Guidelines should be issued on the retention, storage, handling and disposal of records and information.

b) A retention schedule should be drawn up identifying essential record types and then the period of time for which they should be retained.

c) An inventory of the sources of key information should be maintained.

d) Appropriate controls should be implemented to protect essential records and information from loss, destruction and falsification.

19.6 Business Continuity :

To ensure that vital business records are not lost through destruction or loss of paper documents, the paper documents and the media storage should be included as part of the contingency and disaster recovery plan, discussed in this document.

19.7 Preservation of Evidence :

To ensure that transaction source documents can be located when needed, the following steps should be taken :

a) The 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.

b) The use of electronic article surveillance for areas containing a concentration of documents that are processed frequently by several authorised personnel.

19.8 Labelling :

To further identify documents with HIGHLY SENSITIVE information, the organisation should establish a policy for the labelling of the documents. However, while deciding on the policy, the organisation should keep in view the factors whether the benefits of providing the notice of sensitivity are outweighed by the cost of doing so.

19.9 Forged Documents :

To prevent the acceptance of forged documents, the organisation should train the personnel, responsible for the processing of value-bearing documents or documents, which are used as the basis of transactions, to refer the documents to their supervisor immediately, if any irregularity is detected or suspected.

19.10 Output Distribution Schemes :

There is a trend to replace the paper documents such as reports, prospectuses and statements with on-line access to computer systems and in the event of the adoption of such a system/practice in the organisation, it has to be ensured that all the relevant controls, as discussed in this document, apply to these computer systems.

19.11 Microfilm and other Media Storage :

The 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.

19.11.1 Disclosure :

To procure greater security for HIGHLY SENSITIVIE information stored on magnetic media, it is to be ensured to encrypt the storage media containing HIGHLY SENSITIVE information or to physically protect the media from unauthorized access or removal. To prevent the disclosure of sensitive or HIGHLY SENSITIVE information on microfilm or microfiche, it is to be ensured to attach labels indicating the highest classifications of information that is stored on a microfilm or microfiche. This label should be clearly visible.

19.11.2 Destruction :

To prevent destruction or disclosure of information through unauthorized removal of storage media, it is to be ensured to 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.

19.11.3 Business Continuity :

To ensure the continued availability of the information stored on microfilm, microfiche or mass storage media, it is to be ensured to include microfilm, microfiche and mass storage media as part of the contingency and disaster recovery plan, as discussed in this document.

19.11.4 Environmental :

To prevent the destruction of information through loss of storage media due to environmental problems, it is to be ensured to provide adequate fire protection and environment control for storage sites.

Chapter 20

Disaster Recovery Planning and Cryptographic Disasters

Disaster Recovery Planning (DRP), also called business resumption/continuity planning, is an on-going requirement in any financial organisation. Its main purpose is to assure that the business functions continue to function during and after disasters, such as fire, flood, power failures, disruption in operations etc. DRP and cryptography interact in two basic ways in the

matter.

20.1 Disaster Cryptography :

From the DRP perspective, the cryptographic facilities such as the key management centres and the Certification Authorities are one class of functions which must be brought back on-line following disruption. It has to be ensured that the keying material remains secure while it is made available at the backup sites. For example, the keys for MAC of fund transfer messages may be replicated and securely stored at a back-up site. Split knowledge and dual control could be adequate. However, the back-up site for a Certification Authority should use a separate certification root, since the integrity of the signature system derives from the non-disclosure of the root key outside of the Certification Authority's key generation device. The continued operation of the cryptographic facilities must be part of the organisation's DRP.

20.2 Cryptographic Disasters :

DRP must also cover how to deal with the events caused by or complicated by the cryptographic services, especially unforeseen failures. For example, an organisation may have implemented a state-of-the-art access control system. However, there might have been noticed clear signs of an intruder in the system. One possibility could be that the cryptography facilities have failed. DRP must contain clear instructions regarding how to handle such situations from the point of view plugging the loopholes in the system and containing damage, if any.

The Information Systems Security and the Disaster Recovery Programme of an organisation must address cryptographic threats, at least in generic form and implement the following steps therefor :

a) Establish a system for regular monitoring of the information processing system for abnormal behaviour ;

b) Establish the procedures to be followed for determining the cause of the abnormal behaviour and guidelines on how to respond to a threat, intruder etc.;

c) Establish the procedures for dealing with the failure of any cryptographic control; and

d) The availability of the cryptographic services, keying material and other related services following business interruption.

Chapter 21

Financial Services/Products and Security Controls

21.1 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.

Financial Card Associations, as a corporate policy, maintain their own minimum security standards for financial organisations and contractors. In addition to those security programs, organisations using financial transaction cards should employ the controls listed below.

21.1.1 Physical Security :

To protect against the destruction, disclosures or modifications of transaction card information during the processing stages, it is to be ensured to locate the local facility in an area regularly, patrolled by the public law enforcement services and by fire protection services. Further, it is also to be ensured that the local facility should be protected by an intrusion (detection) alarm system with auxiliary power.

21.1.2 Insider Abuse :

To prevent fraudulent transactions being made through access to card information, the following steps should be taken :

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

b) Keep the production and issuing function for cards physically separate from the production and issuing function for PINs.

21.1.3 Transportation of PINs :

To prevent losses through the use of PINs having been intercepted by unauthorised persons, it is to be ensured to handle the PINs, Personal Identification Number (PIN) Management and Security, as appropriate and required.

21.1.4 Personnel :

To prevent the assignment of unsuitable personnel to credit card processing duty, it is to be ensured to conduct credit and criminal record checks for all employees handling embossed or unembossed cards.

21.1.5 Audit :

To ensure the integrity of control and audit information, it should be ensured that the controls and audit logs are maintained for the printed plastic sheets, plates, embossing and encoding equipment, signature panel foil, honograms, magnetic tape, semi-finished and finished cards, simple cards, information on cardholder account numbers and equipment for disposal of waste.

21.1.6 Enforcement :

To ensure continued compliance with the security standards and the maintenance of the Audit Control Logs, it should be ensured to appoint at least one person to serve as the prime security officer responsible for performing the security functions.

21.1.7 Prevention of Counterfeit Card :

To prevent information, disclosed on the sale of drafts from being used to produce counterfeit magnetic stripe cards, it should be ensured to encode cryptographic check digits on the magnetic stripe and validate these digits on as many transactions as possible. To prevent the intercepted information, if any, from being used to produce counterfeit cards, it should be ensured to use the physical Card Authentication Method (CAM) to validate the authenticity of cards.

21.2 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 which are generally associated with the tellers. These devices may be located inside an organisation's buildings, attached to the outside of any such buildings or be away from the organisation's office.

Additional precautions should be taken to reduce robbery and vandalism to the machines e.g. through installation of CCTV etc. The manufacturers of these devices and the ATM network providers supply general public security guidelines for the use of ATMs. These guidelines should be kept in view while deciding on the location of ATM and use thereof.

21.2.1 User Identification :

To provide assurance to the authorised users of the ATMs, the following steps should be taken:

a) Require the use of Personal Identification Numbers (PINs) to activate the ATM.

b) Educate the users to understand that the maintenance of the secrecy of the PIN is their responsibility.

To prevent unauthorized transactions, caused by guessing the PIN of a card being used by an

unauthorized person, it should be ensured to limit the number of attempts for the entry of a PIN to three attempts only. Further, the mechanism should be such that the card used in such an attempt should be captured, so that the owner of such a card could be contacted to ascertain the nature of the problem.

21.2.2 Authenticity of Information :

To prevent the unauthorized modification of the information transmitted to and from the ATMs, it should be ensured to use a Message Authentication Code (MAC) for each such transmission.

To prevent unauthorized modifications, destruction or disclosures of information residing in an ATM, it should be ensured that the physical access controls to the interior of the ATMs are consistent with the physical protection controls to the containers of currency.

21.2.3 Disclosure of Information :

To prevent the unauthorized use of ATMs or the Point of Sale Terminals through the unauthorized disclosure of information, the following steps should be taken:

a) Encrypt within the ATM or to use smart card for introducing any PIN into the ATM prior to transmisison.
b) Consider encrypting all information transmitted from the ATM.
c) Manage PINs in accordance with relevant International standards.

21.2.4 Fraud Prevention :

To detect and prevent fraudulent use of the ATMs such as the kitting schemes, empty envelope deposits and disallowed transactions, the following steps should be taken:

a) Limit the number of transactions and the amount of funds which can be withdrawn per day per account.
b) Balance the ATM under dual control daily.
c) Install video cameras at the site for capturing the images of all the users of the ATM.
d) Maintain the operation of the ATMs on-line i.e. the ATMs should have the ability to check the account balances prior to the completion of the transaction.

If on-line operation is not possible, it should be ensured to establish more stringent card issuance requirements which would be used for on-line operation of the ATM.

21.2.5 Maintenance and Service :

To prevent unauthorized access to information during the maintenance and the servicing of the ATMs, the following steps should be taken :

a) ATMs as placed “out of service” to customers, prior to any maintenance being performed.
b) Establish dual control procedures for the servicing of the ATMs involving opening of the vault.

21.3 Electronic Funds Transfers :

In addition to the security issues relating to Electronic Funds Transfers, as discussed under various clauses in this document, this sub-clause reexamines the probable threats and the required controls, as under, from the perspective of fund transfer applications, independent of the technology used.

21.3.1 Unauthorised Source :

To prevent loss through the acceptance of a payment request from an unauthorized source, it should be ensured to authenticate the source of messages requesting funds transfer, using a security procedure, as specified in the customer or correspondent agreement. The Cryptographic Authentication should be implemented, whenever feasible. Digital signature should be used. Successful decryption of a message may be used to establish the authenticity of the source of the message.

21.3.2 Unauthorized Changes :

To prevent an improper payment due to changed message contents, whether intentional or accidental, it should be ensured to 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 should be used.

21.3.3 Replay of Messages :

To prevent an unauthorized repeated payment caused by a replayed message, it should be ensured to use and verify unique message identification. Further, this identification should be included in any authentication performed.

21.3.4 Retention of Record :

To preserve evidence that may be needed to prove authorization in making a payment, it should be ensured to record the messages requesting for transfer of funds regardless of the media used to transmit the messages. The material messages to prove authentication including the supporting cryptographic material should be preserved, as required for the purpose.

21.3.5 Legal Basis for Payments:

To ensure that payments are being made in accordance with a signed agreement. It should be ensured to see that the agreement for the EFT is quickly standardised with the provision for change control to take care of the future growth.

21.4 Cheques :

The Cheques, also known as Negotiable Orders of Withdrawal or Drafts, which are written orders directing a bank to pay money. Several new approaches to the processing of cheques raise security concerns to be addressed by the financial organisations. The use of the Cheque Image and Cheque Truncation are techniques which raise security concerns. The transmission and use of the cheque image should be done under encryption and digital signature.

21.5 Electronic Commerce :

Electronic commerce, the provision of financial services over the Internet, is an emerging area of security concerns in the business operations of the financial organisations. Whether the financial services over the Internet are provided directly or with the assistance of a service provider, all usual security concerns must be addressed. Some security areas, which may be of special concern, are discussed hereunder :

21.5.1 New Customers :

The requirement to “Know Your Customer” poses several challenges when the services are delivered through the cyberspace. While it may be desirable to advertise the services using a Homepage or other electronic medium, a personal visit to a financial organisation’s place of business should be insisted for the opening a new account. Normal customer qualification procedures should be observed.

21.5.2 Integrity Issues :

Each transaction should be protected to ensure the identification of the user, authenticity of the user, authenticity of the message, confidentiality of sensitive information and the non-repudiation of instructions. The Transaction requests should be digitally signed, using a key authenticated for the purpose by the Organisation’s Certification Authority. This will provide the required assurance that the user is identified, the integrity of the message contents is maintained and the user is legally bound to his or her actions. It should be ensured that the Account Numbers, PINs or other information which, if revealed, may allow unauthorized use of an account, should be protected with encryption and digital signature.

21.6 Electronic Money :

To prevent against attacks on electronic money systems, the following steps should be taken:

a) Employ devices to ensure tamper-protection against analysis and unauthorized changes.

b) Employ cryptographic authentication of devices and transactions.

c) Employ cryptographic protection for data confidentiality and integrity.

To detect attacks against an electronic money system, the following steps should be taken :

a) Collect the transaction details for verification of financial and security data.

b) Connection with the central system, at least periodically, to collect and verify the transaction logs.

c) Limit the transferability of the stored-value balances to minimise fraud.

d) Analyse payment flow statistics on a regular basis.

e) Maintain suspicious/invalid card lists and make them available to the merchants.

To contain overall security, the following steps should be taken :

a) Establish strict manufacturing and software development procedures.

b) Have contract for third-party security evaluation of components and procedures.

c) Clearly define the responsibilities of all the participants.

d) Strictly control the initialisation, personalization and distribution of the devices.

e) Audit the system regularly.

21.6.1 Duplication of Devices:

To prevent the duplication of devices and to protect information on the software and hardware design, the following steps should be taken:

a) Employ the devices, whose essential parts are physically protected against optical and electrical reading.

b) Logically protect secret data in the token through encryption.

To detect the duplication of devices, the following steps should be taken :

a) Register the devices.

b) Assign a unique identification number and cryptographic key to each device.

c) Authenticate each transaction.

d) Monitor devices whenever connected to the central operator.

To contain losses due to duplicated devices, the following steps should be taken:

a) Publish the list of suspicious/invalid cards and make list available to the merchants.

b) Permit the blocking of devices from the central system.

To provide additional protection due to duplication threats, the following steps should be taken :

a) Separate the manufacturing process from the intialization, personalization and distribution of the devices.

b) Establish a separation of duties with each organisation.

c) Have contract for third-party security evaluation of the devices.

21.6.2 Alteration or Duplication of Data or Software :

To protect against alteration or duplication of data or software, the following steps should be taken :

a) Store data and software in tamper-resistant devices.

b) Monitor tamper-evidence.

c) On-line authorization or detection of suspicious messages.

d) Have the ability to block devices from the central system.

e) Allow the loading of the security software from the central system.

To detect duplication of electronic notes, the central verification of such notes should be ensured.

To prevent or detect creation of unauthorized electronic notes, the following steps should be taken :

a) Establish a system to ensure that the electronic notes are cryptographically certified by the issuer.

b) Establish a system to ensure on-line verification.

To prevent or detect unauthorized creation of transactions, the following steps should be taken :

a) Establish a system to ensure that the transactions are digitally signed by a key unique to device.

b) Establish a system to ensure on-line authorization of transactions.

c) Authentication of the devices.

d) Verify the transaction sequence numbers.

e) Maintain shadow accounts.

f) Establish a system to regularly monitor unusual payment patterns.

To protect or detect unauthorized alteration of the operating system software or static data, the following steps should be taken :

a) Store critical software and data in physically protected memory and to logically protect the same with encryption.

b) Establish a system to ensure to create and verify software checksums.

To prevent or detect unauthorized alteration of the electronic value balance, the following steps should be taken :

a) Modification of the balance is performed only by the authorized devices.

b) Maintain shadow balance.

21.7 Alteration of Messages :

To prevent unauthorized modification of messages, the following steps should be taken :

a) Have challenge-response mechanisms to initiate transactions.

b) Use of the derived sessions key to exchange messages.

c) Verify the message integrity by hash.

d) Authenticate messages by digital signature.

To detect unauthorized modification of messages, the following steps should be taken :

a) Verify the electronic signatures.

b) Verify transaction sequence numbers.

d) Verify time-stamps.

21.8 Replay or Duplication of Transactions :

To prevent or detect the replay or duplication of transactions, the following steps should be taken :

a) Use of unique session keys. **b) U**se of PIN for load and deposit truncations. **c) V**erify the transaction sequence numbers. **d) V**erify the time-stamps. **e) M**aintain shadow balances. **f) E**stablish a system to regularly monitor unusual payment patterns.

21.9 Theft of Devices :

To prevent theft of devices and to contain losses from theft, the following steps should be taken :

a) Use of PIN for load transactions.

b) Polling of cards.

c) Establish a system to allow the users to lock cards with PIN.

d) Establish a system to allow the cards to be blocked by the issuer.

e) Set transaction or card value limits.

21.10 Repudiation :

To prevent truncations from being repudiated, the following steps should be taken:

a) Establish a system for the issuer to log transactions.

b) Allow the cardholder to check the number of transactions from the card.

c) Time-stamping and sequence numbering of the transactions.

d) Establish a system to ensure that the merchant and the client cryptographically sign the transactions.

e) Employ a reputable Certification Authority.

21.11 Malfunction :

To protect against loss due to malfunction, the following steps should be taken :

a) Structure the protocols such that the transactions are either successfully carried out or cancelled.

b) Establish a system for the cards and the devices to log any errors detected.

c) Set a maximum number of errors after which the card will be forced to connect to the central operator.

21.12 Cryptographic Issues :

To prevent theft of cryptographic keys, the following steps should be taken :

a) Employ tamper resistant devices.

b) Generate secret keys in secured environment.

c) Encryption of any secret key, which is transported over the network or to use asymmetric crypto systems for the purpose.

To protect against the consequences of theft, the following steps should be taken :

a) Maintain the list of the compromised keys.

b) Allow for periodic and emergency change of keys.

c) Establish expiration date for all keys.

d) Employment of strict key management.

e) Third party evaluation of the crypto systems implemented.

f) Subject the system to external audit.

g) Use published algorithms.

21.13 Criminal Activities :

To detect criminal activities and to contain damage from such activities, the following steps should be taken :

a) Uniquely identify truncations.

b) Establish a system to ensure digital signature of truncations.

c) Verify and authorize load or payment transactions on-line.

d) Force the devices to interact with the banking system. **e) I**nvestigate specific payment patterns. **f) S**et limits for transferability of value. **g) S**et limits for truncations.

h) Establish a system for the devices, holding value, to be registered and linked to an account.

i) Establish a system to know your customer.

j) Establish a system to check the criminal records of the customers and merchants

(wherever possible and relevant).

k) Establish a system to monitor organisations participating in electronic money systems.

21.14 Miscellaneous :

No matter how carefully one plans, there is always a security concern that is not obvious until it becomes a problem. The Steganography is one such security concern, which should be addressed as discussed hereunder :

21.14.1 Steganography - Covert Channels :

Steganography is the hiding of information within another media. It is a practice that can be traced back in history. With the advent of bandwidth, multimedia transfers of digitised pictures, movies, sound bites etc. raise the possibility of moving information of all sorts through a covert channel.

While many existing financial applications may make efficient use of bandwidth, leaving little redundancy for covert transmission, new technologies may introduce the opportunity for steganographic activity. The existence of a vehicle for covert channel exposes the organisation to several concerns. Among them are the unauthorized release and transmission of business information, unauthorized loading of malicious code into the processing system etc.

To prevent the use of steganographic tools on the organisation's information processing system, the organisation should employ digital signatures, wherever possible, to detect changes in graphic, voice and multimedia files. It should be ensured that the digital signatures are applied before the opportunity to apply the steganographic tools. The organisation should also implement the following steps in this regard.

a) Maintain strict configuration control on all the information processing platforms.

b) Conduct periodic checking for the presence of steganographic tools.

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

Chapter 22

Compliance with Legal Requirements

The design, operation, use and management of the information systems should be subject to the statutory, regulatory and contractual security requirements to avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements. Advice on specific legal requirements should be sought from the organization's legal advisers or suitably qualified legal practitioners.

All relevant statutory, regulatory and contractual requirements should be explicitly defined and documented for each information system. The specific controls and individual responsibilities to meet these requirements should be similarly defined and documented.

Chapter 23

Intellectual Property Rights

To minimize concerns over the intellectual property rights to software, a written policy on intellectual property rights should be adopted. The employees and the contractors involved in the development of the software should be made aware of this policy.

23.1 Copyright :

Appropriate procedures should be implemented to ensure compliance with legal restrictions

on the use of material in respect of which there may be intellectual property rights such as copyright, design rights or trade marks. Copyright infringement can lead to legal action which may involve criminal proceedings.

Legislative, regulatory and contractual requirements may place restrictions on the copying of proprietary material. In particular, they may require that only material that is developed by the organization or that is licensed or provided by the developer to the organization can be used.

23.2 Software Copyright :

Proprietary software products are usually supplied under a license agreement that limits the use of the products to specified machines and may limit copying to the creation of back-up copies only. The following controls should be considered.

a) publishing a software copyright compliance policy which defines the legal use of software and information products;

b) issuing standards for the procedures for acquisition of software products;

c) maintaining awareness of the software copyright and acquisition policies and giving notice of the intent to take disciplinary action against staff who breach them ;

d) Maintaining appropriate asset registers;

e) Maintaining proof and evidence of ownership of licenses, master disks, manuals, etc;

f) Implementing controls to ensure that any maximum number of users permitted for using the software is not exceeded;

g)Carrying out checks that only authorized software and licensed products are installed;

h)Providing a policy for maintaining appropriate licence conditions; i) Providing a policy for disposing of or transferring software to others; j) Using appropriate audit tools;

k)Complying with terms and conditions for software and information obtained from software vendors and public networks ; and

l) Network Management Software or Server Management Software should be used to detect unauthorised software in the network.

Chapter 24

Review of Information Systems Security policy and Technical Compliance

The security of the information systems should be regularly reviewed to ensure compliance of the information systems with the organizational information systems security policy and standards. Such reviews should be performed against the appropriate security policy and the technical platforms and the information systems should be audited for compliance with security implementation standards.

24.1 Compliance with the Information Systems Security Policy :

Information Systems Security Officers and the Business Managers should ensure that all security procedures within their area of responsibility are carried out correctly. In addition, all the areas within the organization should be considered for regular review to ensure compliance with the information systems security policy and standards. This should include the following:

a) information systems ;

b) systems providers;

c) owners of information and information assets;

d) users;

e) Third Parties ; and

f) management.

Owners of the information systems should support regular reviews of the compliance of their systems with the security policy, standards and any other security requirements, put in place by the organisation.

24.2 Technical Compliance Checking :

Information systems should be regularly checked for compliance with security implementation standards. Technical compliance checking involves the examination of the operational systems to ensure that the hardware and software controls have been correctly implemented. This type of compliance checking requires specialist technical assistance. It should be performed manually (supported by appropriate software tools, if necessary) by an experienced system engineer or by an automated software package which generates a technical report for subsequent interpretation by a technical specialist.

Compliance checking also covers, for example, penetration testing, which might be carried out by independent experts, specifically contracted for this purpose. This can be useful in detecting vulnerabilities in the system and for checking how effective the controls are in preventing unauthorized access due to these vulnerabilities. Caution should be exercised in case success of a penetration test could lead to a compromise of the security of the system and inadvertently exploit other vulnerabilities.

Any technical compliance check should only be carried out by or under the supervision of competent, authorized persons.

Chapter 25

System Audit Considerations

There should be controls to safeguard operational systems and audit tools during system audits to maximize the effectiveness of and to minimize interference to/ from the system audit process. Protection is also required to safeguard the integrity of the information systems and prevent misuse of the audit tools.

25.1 System Audit Controls :

Audit requirements and the activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruption to the business processes. The following should be observed :

a) Audit requirements should be agreed with the appropriate management.

b) The scope of the checks should be agreed and controlled.

c) The checks should be limited to read-only access to software and data.

d) Access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed.

e) IT resources for performing the checks should be explicitly identified and made available.

f) Requirements for special or additional processing should be identified and agreed.

g) All accesses should be monitored and logged to produce a reference trail.

h) All procedures, requirements and responsibilities should be documented.

25.2 Protection of System Audit Tools :

Access to system audit tools i.e. software or data files, should be protected to prevent any possible misuse or compromise. Such tools should be separated from development and operational systems and not held in tape libraries or user areas, unless given an appropriate

level of additional protection.

Chapter 26

Human Resources

The work force is one of the most important assets of any organisation and more particularly, of a financial organisation. In a service sector, where quality management is accorded top priority, the human resources are of critical importance for the success of the organisation. The organisations in the banking and financial sector should encourage their employees to acquire, develop and sharpen Information Systems skills.

Human resources are essential ingredients in any successful information security programme. They are the first line of defence, helping to make the technology function as it should, sensing security breaches signals and helping in creating security awareness to succeed.

It is equally correct that the staff members also commit computer crimes. They can misuse the technology. The organisations should optimally mobilize their human resources to build up the required level of security in all areas of the organisation, while developing techniques to minimize the opportunities for people to commit security breach related crimes.

Certain positions in an organisation may be sensitive due to the imminent sharing of sensitive information or "key area" because of certain privileges, associated with the position. The selection of personnel for such positions should be through rigorous screening.

The controls, listed below, represent the controls relating to the employees, which an organisation should apply.

26.1 Awareness :

To educate employees in their information security duties and to impress upon them the importance of information security, the following steps should be taken:

a) Inform all the directors, officers, managers, employees and contractors that information in any form is an asset of the organisation and shall only be used to conduct official business.

b) Establish, as part of the information security programme, the communications and awareness programme to create awareness among the employees of the importance and the seriousness of information security in the organisation.

c) Establish the policies that assign and enforce responsibilities for information security issues. The employees should be made aware of the fact that the security violations may invite disciplinary measures by the organisation.

d) The employees understand their responsibilities.

To further minimize risk of loss, a "clear desk" policy for papers and diskettes should be established and implemented. Any material not in use should be properly destroyed.

26.2 Management :

To utilize the managers as a part of the sound information security awareness programme, the following steps should be taken:

a) Encourage the managers to treat information security concerns of the employees seriously in order to encourage their participation.

b) Encourage the managers to make the employees security conscious as also aware of the sensitivity of the information they use on the job.

c) Encourage the managers to be aware of unusual behaviour by the employees and seek assistance from the human resource department in the matter.

d) Consider the effects of setting employment and management policies.

e) Make the managers and the employees aware of the downsizing, merger or acquisition plans and have a proper mechanism to counteract destructive rumours.

26.3 Unauthorized use of Information Resources :

To prevent disclosures, destruction or modifications of information through unauthorized use of information resources, the policies covering the authorised uses of the personal computers and other information resources should be made available to all personnel in the organisation. The policy on the removal of information or equipment from the premises should be clearly spelt out and adhered to.

26.4 Hiring Practices :

To ensure that hiring practices are consistent with the information security programme, the organisation should employ prudent hiring practices including periodical checking for possible security exposure.

26.5 Policy on Ethical Behaviour :

To avoid conflict of interest and to ensure ethical behaviour, the following steps should be taken :

a) Establish an ethics policy consistent with the information security programme of the organisation.

b) Monitor compliance with special attention to employees in sensitive positions.

26.6 Disciplinary Policy :

To ensure that the employees understand the consequences of any deviation from the security policy or standards, adopted by the organisation, a written disciplinary policy should be established.

26.7 Fraud Detection :

To assist in detecting on-going defalcation, if any, the following steps should be taken :

a) Every year, when employees are away on leave for a sufficiently long period, say one/two weeks, as per the policy on leave of the organisation, the USERIDs of the employees should be suspended during this time. The persons replacing such employees should notify the management of the security-related abnormalities, if any, observed in respect of the employees on leave.

b) Perform unannounced rotation of the personnel involved in sensitive or highly sensitive activities from time to time.

c) Implement strong controls over the fire-end points through which embezzlers may use to remove the proceeds of fraud. These endpoints are official cheques, wire transfers, credit to account or avoidance of debits, cash and items of value, received or delivered.

26.8 Know your Employee :

To assist the employees in handling personal problems that might result in possible information security exposures, the organisation should periodically interact/share some of the personal problems of these employees to infuse the required level of confidence in them.

26.9 Former Employees :

To prevent unauthorized access by former employees, the following steps should be taken :

a) Terminate all access that an employee possessed immediately on dismissal, retirement, resignation or other forms of permanent departure. The USERID, assigned to the employee, should not be re-issued.

b) Retrieve all identification, badges, keys, access control tokens and other security-related items as well as the equipment supplied by the organisation.

GLOSSARY OF TERMS

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

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

? 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.

Audit : Function which seeks to validate that controls are in place, adequate for their purposes and report inadequacies to the 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 the facilities has taken place.

Authentication : Process which seeks to validate identity or to prove the integrity of the 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 at the production site.

Bio-metrics : Methods of authenticating the identity of a person by measurement/ identification/matching of some physical characteristics, such as fingerprint, retinal pattern or voice.

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

Card Authentication Method : Concept which allows unique machine-reading/ identification of a financial transaction card and which prevents copying of the 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 sort code (the instructions the programmer writes).

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

Control : Measure taken to assure the integrity and quality of 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, as generated under ISO with a cryptographic key distributed under ISO or inferred through successful decryption of a message, encrypted under ISO with a key distributed under ISO.

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 organisation and the customer.

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

Digital Signature : Value which can serve in place of a handwritten signature. Normally, a digital signature is the function of the contents of the message, the identity of the sender and some cryptographic information.

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.

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

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

Electronic Money : The scheme under which value is created, stored or transferred in an electronic form. Conceptually, it is a replacement for coins and currency.

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

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

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

Freeware : Software made generally available, which does not require a license agreement for use thereof.

Guideline : Recommendation for information security controls to be implemented against given threats. 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. 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 organisation to make decisions, move funds, set rates, advance loans, process transactions and the like. This definition includes software components of the processing system.

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

Information Resources : Equipment which is used to manipulate, communicate or store information whether they are inside or outside the organisation. 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.

Key : Cryptographic key, as discussed in this document.

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

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

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.

Modification of Information : The unauthorized or accidental change in information, whether detected or undetected.
Need-to-Know : Security concept which limits access to such information and information processing resources as are 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 in business operations.
Risk : Possibility of loss due to occurrence of one or more threats to information. This is 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 of communications, interfacing with file storage or printing facility.
Shareware : Software which is generally available and which carry a moral, though not a legal, obligation for payment.
Sign-on : Completion of identification and authentication of an 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 acceptance practices to meet a particular defined policy.
2. A document published by a standards setting body, which provides industry wide methods of performing certain functions.

Stored Value Card : A token which is capable of storing and transferring electronic money.
Tamper Evident Packaging : Protective packaging which will preserve an indication of attempts to access its contents.
Threat : Condition which may cause information or information processing resources to be intentionally or accidentally lost, modified, exposed, made inaccessible or otherwise affected to the detriment of the organisation.
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.
USER ID : A character string which is used to uniquely identify each user of a system.

REFERENCES

Voice Mail : Systems which record and retrieve voice messages.

1. Technical Report - Banking and related Financial Services - Information Security Guidelines - ISO TR 13569
2. Information Security Management - Code of Practice for Information Security Management - BS 7799-1:1999
3. Information Technology Security Guidelines - September, 1999 -Infocomm Development Authority of Singapore

4. IT Governance Institute - CoBIT - Control Objectives - July, 2000
5. IT Governance Institute - CoBIT - Management Guidelines - July, 2000
6. Information Technology Act, 2000 dated the 17th October, 2000 –Government of India
7. Information Technology (Certifying Authorities) Rules, 2000 dated the 17th October, 2000 – Government of India