Attachment 4

Baseline Security Standard for Information Security Management

Assurance Level 1

Version 1.0

PART I: Introduction

Foreword

Driven by business objectives, such as increasing revenue and customer base, many organisations are embracing ICT-enabled solutions to provide richer online services to their client base. These very services have driven many banks and other organisations to interconnect via common communications and information processing infrastructure.

In terms of security posture, organisations in Sri Lanka represent a spectrum of capabilities. However, just as the strength of a chain lies with its weakest link, so does the strength of information security in the financial services sector lie with its weakest member, which in turn poses a threat to all other members, which may potentially lead to financial fraud.

The Central Bank of Sri Lanka (CBSL), the Sri Lanka Computer Emergency Readiness Team | Co-ordination Center (Sri Lanka CERT|CC) and the Sri Lanka Banks' Association (SLBA) worked towards the establishment of the Baseline Security Standard for Information Security Management (BSS), based on the globally recognized ISO 27000 series of international Standards for information security. The implementation of the Standard will be supervised by CBSL and the subsequent revisions to the Standard will be proposed by Bank Computer Security Incident Response Team (Bank CSIRT) to CBSL for consideration.

1. Fundamentals

1.1. Information Security Management

The preservation of the Confidentiality, Integrity and Availability of information by the appropriate and systematic application of security controls to manage the risk of exposure to a threat, which arises due to the existence of vulnerabilities in information assets.

1.2. Information Security Risk Management

Information security risk management is the systematic approach to ascertaining the impact and likelihood of an information asset being exposed to a threat.

This Standard assumes the application of ISO 27005, to assign risk ratings to information assets which fall within the scope of the Information Security Management System of the Organization concerned.

1.3. Security Considerations

All organisations are required to derive their security requirements to conform to the laws in Sri Lanka including the regulatory requirements set by the respective regulators and the international best practices adopted globally. Additionally, security requirements are also governed by the business objectives set by the board of directors and the senior management of the organization. The BSS is developed taking into consideration the requirements set in these Standards, with a view towards increasing the level of conformance with such requirements. Significant changes to these requirements will be reflected in the revised versions of the BSS.

1.3.1. Legal Requirements

All organisations are liable to comply with the laws applicable in this regard including the Computer Crimes Act No. 24 of 2007, the Electronic Transactions Act No.19 of 2006, Payment Devices Frauds Act No. 30 of 2006, and Intellectual Property Act No. 36 of 2003 of which any violations amounts to an offence.

1.3.2. Regulatory Requirements

Local industry regulations/directives set forth by the CBSL and other regulatory bodies must be complied with.

1.3.3. International Standards

In order to be recognized as competent online/e-banking service providers, organizations need to comply with internationally recognized industry specific security standards, such as PCI-DSS.

1.3.4. Information Security Objectives

Information Security objectives must be identified supporting fulfillment of key business objectives within the framework of the information security policies, statutory requirements, other requirements and business processes.

2. Terms and Definitions

The following terms and definitions are applicable throughout this document.

2.1. Asset

Anything that has value to the organization.

[ISO/IEC 13335-1:2004]

2.2. BSS

Baseline Security Standard on Information Security Management.

2.3. Control

Means managing risk through policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management or legal nature.

2.4. Fraud

Wrongful or criminal deception intended to result in financial or personal gain.

2.5. Guideline

A description that clarifies what shall be done and how to achieve the objectives set out in policies.

[ISO/IEC 13335-1:2004]

2.6. IEC

International Electrotechnical Commission.

2.7. ISO

International Organization for Standardization.

2.8. Information System

Any information processing system, service or infrastructure, or the physical locations housing them.

2.9. Information Security

Preservation of confidentiality, integrity and availability of information. Other attributes such as authenticity, accountability, non-repudiation and reliability can also be involved.

2.10. Information Security Event

An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

[ISO/IEC Technical Report 18044:2004]

2.11. Information Security Incident

A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

[ISO/IEC Technical Report 18044:2004]

2.12. Malicious Codes

Programs that cause undesirable effects to the Information Systems. Examples of malicious codes include computer viruses, network worms, Trojan horses, logic bombs, spyware etc.

2.13. Organizations

Financial institutions who are members of Bank CSIRT.

2.14. Outsourcing

An agreement between a licensed bank and a third party ‘service provider’, whereby the service provider performs an activity, function or process connected with the operations of a licensed bank.

[Banking Act Directions No. 2 of 2012]

2.15. Policy

Overall intention and direction as formally expressed by the Board/Senior management.

2.16. PCI-DSS

Payment Card Industry – Data Security Standard.

2.17. Risk

A combination of the likelihood of an event and its impact.

[ISO/IEC Guide 73:2002]

2.18. Risk analysis

Systematic use of information to identify sources of risk and to estimate the level of risk.

[ISO/IEC Guide 73:2002]

2.19. Risk assessment

Overall process of risk analysis and risk evaluation.

[ISO/IEC Guide 73:2002]

2.20. Risk Evaluation

Process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

[ISO/IEC Guide 73:2002]

2.21. Risk Management

Coordinated activities to direct and control an organization with regard to risk.

[ISO/IEC Guide 73:2002]

2.22. Risk Treatment

Process of selection and implementation of measures to modify risk.

[ISO/IEC Guide 73:2002]

2.23. Service Provider

'Includes the Head Office, parent institution, another branch or related company of a Licensed Commercial Bank or Licensed Specialised Bank, or an unrelated institution, whether located in Sri Lanka or elsewhere.

[Banking Act Directions No. 2 of 2012]

2.24. Third Party

A person or body corporate that is recognized as being independent of the parties involved, as concerns the issue in question.

[ISO/IEC Guide 2:1996]

2.25. Threat

A potential cause of an unwanted incident, which may result in harm, damage to a system or an organization.

[ISO/IEC 13335-1:2004]

2.26. Vulnerability

A weakness of an asset or a group of assets that can be exploited by one or more threats.

[ISO/IEC 13335-1:2004]

3. Applicability of BSS

This section defines the applicability and preservation of this document.

3.1. Scope

This Standard is applicable to all Information Security Management Systems used within organisations who are members of the Bank CSIRT, as well as personnel handling such information and information systems, both internal and third party.

3.2. Structure

Part I of the Standard addresses the ownership and management of this document, its structure, scope of applicability and recommended risk management methodologies.

Part II of the Standard introduces fourteen (14) main security domains to be considered within the current version of this Standard.

3.3. Maintenance

This document is to be reviewed in six (6) months from the time of introduction, and the result is to be published as Version 2 in case if changes are made, otherwise revision status remains unchanged with the date of reviewed. Bank CSIRT shall take responsibility for this task in consultation with the CBSL. Adoption of each subsequent version will provide improved information security management.

3.4. Implementation

Expected implementation period for Version 1 is 12 months from the time of introduction of the standard.

4. Risk Management

Risk management is a fundamental component of any cost effective information security management system.

4.1. Risk as a basis for Information Security Management

Assets contain vulnerabilities due to weak design, production, implementation, handling, management and a host of other activities. These vulnerabilities may be exploited to give rise to threats. The combination of the likelihood of a threat being realized and the impact of that exposure is called risk, and is an important measure of the relative urgency and need to impose control measures to mitigate that risk.

4.2. Risk Treatment and Security Controls

Adoption of BSS and its successive revisions, will introduce security controls which would mitigate identified risks.

4.3. Guidelines for Risk Management

Risk Management shall be done in accordance with ISO 27005:2011.

4.4. Associated Documents and Activities

The establishment of Guidelines, policies , procedural manuals, schemes and templates by the respective organisations will aid the implementation of the BSS.

PART II: Security Domains

1. Organization of Information Security Management

Objective: To introduce a structured approach to managing information security by defining security roles and assigning responsibilities and making available the necessary resources and authority to perform activities to enhance the Information Security Management System of the organization.

Scope: Applicable to all personnel handling information and information assets within the Information Security Management System of the organization.

1.1. Management Commitment to Information Security

1.2. Management shall establish a clear information security policy direction across the organization on par with its business strategies and objectives. Such policies shall be approved by the Board of Directors or senior management of the organization or the head/Regional Office, as the case may be. These management activities include regular review and amendments depending on the evolving ICT, security, legal, regulatory and audit environments. The management shall provide adequate resources and assign security roles and responsibilities to achieve the above.

1.3. Information Security Risk Assessment

Risk assessments shall identify, quantify and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. Results of risk assessment should guide and determine the appropriate management action and priorities for managing information security risk and for implementing controls selected to protect against these risks. The information security risk assessments shall have a clearly defined scope and should be performed periodically to address changes in the security requirements.

1.4. Information Security Risk Treatment

Risk treatment decision shall be made after following the risk assessment.

1.5. Information Security Coordination

Information Security shall be coordinated by authorized representatives with required technical skills from different parts of the organization with relevant roles and responsibilities assigned to them. This function shall be executed in compliance with information security policy of the organization.

1.6. Allocation of Information Security (IS) Responsibilities

Allocation of IS responsibilities shall be clearly defined in accordance with the information security policy. These responsibilities shall adequately address the ways and means for identification of IS assets and delegation of responsibilities, level of protection required and necessary documentation.

Confidentiality or non-disclosure agreements shall reflect the institutional needs for information security and protection from unauthorized access using legally enforceable terms. Such agreements shall be included in employment and outsourcing arrangements.

1.7. Communication with Authorities

Organizations shall have procedures in place that define who and how to communicate with external authorities in reporting IS incidents and related events.

1.8. Communication with Special Interest Groups

Appropriate contacts with special interest groups, IS forums and professional bodies shall be maintained.

1.9. Independent Review of Information Security

Respective IS policies, procedures and control objectives shall be reviewed at planned intervals and as and when significant change of ICT infrastructure occurs within the organization.

2. Information Security (IS) Policy

Objective: To provide management direction and support for information security in accordance with business, legal and regulatory requirements. IS Policy Document.

The IS policy document shall state the management commitment and set out the approach for managing information security defining overall objectives, scope and the importance of security and commitment to comply with legal and regulatory requirements.

2.2. Review of the IS Policy Document

IS policy document shall be reviewed in planned regular intervals and when significant ICT infrastructure changes occur within the organization. All reviews shall be properly documented and retained.

2.3. Administration and implementation of the IS Policy Document

Policy administration shall be assigned to an appropriate division or department of the organization, with an appointment of an Information Security Officer to be responsible for the implementation with identified procedures and methodologies.

3. Third Parties

Objective: To maintain the security of the organization's information, information processing facilities and information assets that are accessed, processed, communicated to or managed by third parties.

3.1. Identification of Risk Related to Third Parties

Risk to organization's information, information systems and assets from business processes involving third parties shall be identified and appropriate controls shall be implemented before granting access to such third parties.

3.2. Addressing Security when Dealing with Customers

All identified security requirements shall be addressed before giving customers access to the organization's information and information assets.

3.3. Addressing Security in Third Party Agreements

Respective agreements with third parties shall cover all relevant information security requirements and shall ensure that there is no misunderstanding between the respective third party and the organization.

3.4. Service Delivery

Intended service delivery by third parties shall be covered with a Service Level Agreement (SLA) that includes and clearly describes the measures taken to ensure information security, the service to be provided, expected level of service, performance criteria, escalation procedures for problem resolution, respective liabilities of the third party and involvement of sub contractors by third parties and conditions for termination.

3.5. Monitoring and Review of Third Party Services

Services rendered by the third party in accordance with the SLA shall be monitored closely and shall be reviewed in planned intervals by the appropriate internal division or department of the organisation. Third parties are required to adhere to the information security requirements of the organizations even after the expiry of their service contracts.

4. Information Asset Management

Objective: To achieve and maintain appropriate level of protection of organization's information assets.

4.1. Inventory of Information Assets

All information assets shall be clearly identified and an inventory of all such information assets shall be recorded and maintained. This asset inventory shall include all information required for recovery from a disaster.

4.2. Information Asset Classification

Information classification guidelines of the organization shall be published in the information security policy document to support the asset owner who shall classify the information to indicate the need, priorities, and expected level of protection when handling the information. Appropriate set of procedures for labeling information shall be developed and implemented in accordance with the classification guidelines of the organization (Refer Section 77 of the Banking Act, No 30. of 1988, as amended)

4.3. Acceptable use of Information Assets

Rules for acceptable use of information and assets shall be identified, documented, implemented and reviewed periodically. These rules shall be followed by employees, contractors and third parties for the acceptable use.

5. Human Resource Security

Objective: To ensure that employees, contractors, service providers and third party users understand their roles and responsibilities to reduce the risk of theft, fraud and unauthorized use of facilities.

5.1. Definition of Roles and Responsibilities

Organization's information security policy shall clearly define the roles and responsibilities of every user or user group.

5.2. Security Screening

Background screening checks for all candidates especially for sensitive job holders for employment, contractors, service providers and third party users shall be carried out.

5.3. Terms and Conditions of Employment

As part of employment or service contract, all employees, contractors, service providers and third parties (users) shall agree and sign the terms and conditions of the employment contract. All contractual documents shall include reference and acceptance to the Information Security Policy.

5.4. Management Responsibilities

Management shall require all users to apply security in accordance with established policies and procedures of the organization. They shall be properly briefed on their roles and responsibilities prior to granting access to information systems.

5.5. Information Security Awareness, Education and Training

Regular updates to this policy and changes to ICT infrastructure shall be communicated to all users. Appropriate technical and user training to carry out their duties shall be provided to respective officers on regular basis.

5.6. Breach of Security and Penalties

There shall be formal and defined disciplinary procedure/s for investigation of information security incidents or breaches.

5.7. Termination Formalities

Responsibilities for performing employment termination or change of employment, including changes to user access rights shall be clearly defined and assigned. Such responsibilities and duties still valid after termination of employment shall be included into respective agreements.

5.8. Return of Information Assets

All users shall return/declare organization's information assets including logical access information in their possession upon termination of their employment, contract or agreement.

5.9. Revocation of Access Rights

Upon termination or changes of the employment status or third party contract, access to information, information systems and information processing facilities shall be removed or changed with immediate effect.

6. Operations Security

Objective: To protect from unauthorized access, damage and interference to organization's premises, information and operations.

6.1. Information Processing Sites

Appropriate security perimeters shall be implemented and maintained in good order to protect areas, equipment, both on-site and off-site and network cabling that contain information and information processing facilities from natural or manmade disasters.

6.2. Equipment Maintenance

Equipment shall be maintained in good working order to ensure its continued availability and integrity. Those deployed for critical operations shall be covered with annual maintenance and support agreements with the vendor.

6.3. Documented Operating Procedures

Operating procedures shall be documented, maintained and made available for all users on need to know basis. If there is a significant change to the ICT infrastructure and systems, relevant documents must be updated to reflect such changes/ modifications.

6.4. Segregation of Duties

Duties and areas of responsibility shall be segregated to reduce unauthorized access, modification and misuse of organization's information and systems giving due consideration to specific job functions.

6.5. Change Management

Changes to information systems and information processing facilities shall be attended in a controlled manner adhering to industry accepted good practices. Duties and areas of responsibility shall be segregated to reduce instances for unauthorized access, modifications and misuse of organization's information system assets.

6.6. Separation of Development, Test and Operational Facilities

Development, test and production operations shall be separated to reduce the unauthorized access, misuse and changes to the operational systems

6.7. Capacity Management

Use of resources shall be monitored, tuned and projected to capture future growth and capacity requirements to ensure the required level of performance is maintained for continuity of operations.

6.8. System Acceptance

Acceptance criteria for the implementation of in-house developed applications, acquisition of application software or major upgrades shall be in place and appropriate system tests shall be carried before moving for live operations.

6.9. Controls Against Malicious Codes

Detection, prevention and recovery controls to protect against malicious codes shall be in place along with appropriate user awareness programmes.

6.10. Information Backup

Appropriate backup policy shall be implemented to ensure the availability of critical, sensitive and other required information to be used in a contingency situation. These backup copies of information systems and procedures shall be tested regularly.

6.11. Information Handling Procedures

Proper procedures shall be in place to prevent unauthorized disclosure, modification and removal/disposal of media used to store information of the organization.

6.12. Security of System Documentation

System documentation shall be stored securely to protect against unauthorized access.

6.13. Information Exchange Policies and Procedures

Proper procedures shall be designed and in place to protect information from interception, copying, modification, misuse, and destruction. Policies and procedures shall be designed and in place to protect information associated with the interconnection of business information systems giving due consideration to address known vulnerabilities in managing information sharing.

6.14. Audit Logging

Audit logs that record user activities, exceptions and information security events shall be maintained with proper care for designated periods as per the audit and legal requirements.

6.15. Monitoring System Use and Protection of Log Information

Systems shall be monitored to review administrator, operator and fault logs and information security events (if any) shall be recorded. These logs shall be used to ensure that information system problems are identified and addressed.

6.16. Clock Synchronization

The system time stamps of all information systems shall be synchronized with an agreed, standard time source.

7. Communications Security

Objective: Prevention of unauthorized interception from accessing telecommunication networks in an intelligible form, while delivering content to the intended recipients. This shall cover crypto security, transmission security, emission security and physical security of information and its processing facilities and transmission mechanisms implemented in the organization.

7.1. Oversight of Critical Infrastructure by the Board or Delegated Authority

Regular reviews of development and continued maintenance of security control infrastructure for the safeguard of electronic banking systems shall be conducted. This shall include the establishment of authorization privileges, logical and physical access controls to maintain appropriate boundaries and restrictions on both internal and external user activities.

7.2. Network Security Management

To ensure the protection of information in networks and the protection of the supporting infrastructure.

7.3. Network Controls

Capability of users connecting to the organization's local area or wide area network shall be restricted in accordance with the access control policy of the organization. Groups of network services, users and information systems shall be separately maintained in the network to access those resources in accordance with the information security policy of the organisation.

7.4. Mobile Computing and Communications

The information security policy shall cover the appropriate security measures to protect against the risks of using mobile computing and communication facilities.

7.5. User Authentication for External Connections

Appropriate authentication methods shall be used to control access by remote users. Physical and logical access to diagnostic and configuration ports shall be controlled.

7.6. Equipment Identification in Networks

Automatic equipment creation and identification shall be considered as a means to authenticate connections from specific locations and equipment.

7.7. Network Connection Control

For shared networks that extend the boundaries of the organization, the capability of users to connect to the network shall be controlled in accordance with the access control policy of the organization.

7.8. Network Routing Protocol

Routing controls shall be in place for networks to ensure that network connections and information flows do not breach the access control policy of the organization.

8. Physical and Environmental Security

Objective: To prevent unauthorized physical access, damage, and interference to the organization's premises, information and information system assets.

8.1. Physical Security Perimeter

Appropriate security perimeters (barriers such as walls, card controlled entry points, manned information processing facilities) shall be implemented to protect areas that contain information systems and information processing facilities.

8.2. Physical Entry Controls

Only authorized personnel are allowed to enter into information processing facilities with proper access control mechanisms. A register shall be maintained to record access by visitors entering such areas and they shall be accompanied always by an authorized officer.

8.3. Securing Offices, Rooms and Facilities

Physical security for offices, sites, rooms and facilities shall be properly designed and implemented.

8.4. Protection from External and Environmental Threats

Physical protection against damage from natural or manmade disaster shall be designed and implemented.

8.5. Working in Secured Areas

Physical protection and guidelines for working in secured areas shall be designed, implemented and made available to respective officers on a regular basis.

8.6. Public Access, Delivery and Loading Areas

Access points such as delivery and loading bays where unauthorized personnel may enter the facilities shall be controlled and isolated from the information processing facilities where possible.

8.7. Utilities

All equipment shall be protected from failure of power and air conditioning, fire and other disruptions caused by failures in supporting utilities.

8.8. Cabling Security

Power and telecommunication cables carrying data and information services shall be protected from interception or damage.

9. Access Control

Objective: Access to information, information systems, facilities and business processes shall be on the basis of organisation's business and security requirements.

9.1. Access Control Policy

An access control policy shall be established, documented, and reviewed based on the business and security requirements.

9.2. User Access Management

Formal procedures shall be in place to provide access to authorized officers while denying access to unauthorized officers. Management shall review the user access rights in regular intervals using a formal procedure.

9.3. User Identification and Authentication

There shall be a formal user creation and deactivation procedure in place when granting and revoking access to information systems.

9.4. Password Management Systems

Allocation of passwords and password governing rules shall be established in the security policies of the organization. Users are required to follow good security practices in selection and use of passwords.

9.5. Session Timeout/Limitation of Connection Time

Termination of active sessions is required when the respective work is completed. Users shall ensure that unattended equipment has appropriate protection from unauthorized access.

10. Internet and E-mail Security

Objective: A secure and well structured framework shall be established to ensure the effective use of email and internet facilities.

10.1. Electronic Messaging and Internet

The corporate email and Internet connections are primarily for official use only. Procedures shall be in place to authenticate the identity and authorization of customers providing facilities for Internet banking.

10.2. Online Transactions

Procedures shall be in place to ensure the implementation of adequate segregation of duties within the organization for systems and databases that shall use transaction authentication methods to ensure non-repudiation and shall establish accountability for internet banking transactions. Organizations shall maintain comprehensive audit trails and logs and shall employ appropriate cryptographic techniques, specific protocols or other security controls to ensure the confidentiality of customer internet banking data.

10.3. Publicly Available Information

Organization shall ensure that they provide correct and appropriate level of information to its customers through different media, electronically as well as in printed form.

11. Information Systems Acceptable Use

Objective: Formal procedures shall be established to prevent unauthorized user access and compromise or theft of information, and information processing facilities.

11.1. Authorization Process for Information Systems

Allocation and revocation of access rights, to information systems and information services shall be handled using controlled and secure mechanisms. Management shall review user access rights in regular intervals using a formal procedure.

11.2. Media Handling

A secure framework has to be established by the management to ensure that electronic and printed media are used, managed and disposed by authorized officers as per the agreed policies of the organization.

11.3. Use of System Utilities

Use of system utilities shall be restricted to authorized officers and controlled to ensure that the intended service is delivered.

11.4. Clear Desk and Clear Screen Policy

A clear desk policy for printed and removable storage media and a clear screen policy for information processing facilities shall be adopted in accordance with the information classification guidelines of the organization.

12. Information Security Incident Management

Objective: Formal incident reporting and escalation procedures shall be in place. These procedures shall be made available to all relevant stake holders.

12.1. Reporting Information Security Incidents

Information security events shall be reported through appropriate management channels as quickly as possible. A formal reporting procedure shall be implemented together with an incident response and escalation procedure setting the action to be taken.

12.2. Reporting Security Weaknesses

All employees, contractors or third party users of information systems and services are required to note and report observed or suspected security weaknesses in the systems or service delivery.

12.3. Responsibilities and Procedures

Management responsibilities and procedures shall be established to ensure quick, effective and orderly response to information security incidents. These procedures shall cover analysis and identification of the incident, contents, planning and implementation of corrective measures to avoid future recurrence.

12.4. Learning from Information Security Incidents

There shall be mechanisms in place to enable types, volumes and costs of information security incidents to be quantified and monitored.

12.5. Collection of Evidence

Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the requirements on evidence as set out in the relevant jurisdiction(s).

13. Acquisition, Development and Maintenance of Information Systems

Objective: To ensure that information security management is an integral part of information systems.

13.1. Information Security Requirements Analysis and Specification for Software and Hardware

Information security requirements shall be identified, justified, agreed and documented as part of the implementation and overall business case for an information system.

13.2. Correct Processing in Applications

To prevent errors, losses, unauthorized modifications or misuses of information, appropriate controls shall be implemented at data input, processing and output stages.

13.3. Message Integrity

Requirements for ensuring authenticity and protecting message integrity in applications shall be identified and implemented.

13.4. Control of Operational Software

Formal procedures for controlling operational software in production environments shall be in place to minimize the risk of corruptions. Use of pirated software shall be prohibited and compliance to the acts and laws pertaining to intellectual property in Sri Lanka must be maintained.

13.5. Protection of System Test Data

System testing shall be carried out in a separate test environment to avoid unauthorized access to production databases and these test results and test scripts shall be retained for control /audit purposes.

13.6. Access Control to Program Source Code

Access to source code shall be restricted. Source code of purchased software packages that are deployed for critical operations should be kept with an escrow agent based on the policy adopted by respective organisation.

13.7. Change Control Procedures

Formal change control procedures shall be in place to control the implementation of changes to information systems.

13.8. Technical Review of Applications After Operating System Changes

Review of application controls and integrity checks shall be conducted to ensure that the changed computing environment has not compromised the internal controls.

13.9. Restrictions on Changes to Software Packages

Modifications to software packages must be discouraged and shall be used without modification. If modifications are required, the risk of in-built controls and integrity processes shall be evaluated with the vendor's technical support.

13.10. Information Leakage

Possibilities for information leakages shall be prevented at all times.

13.11. Outsourced Software Development

When software development is outsourced, licensing arrangements shall be established respecting the intellectual property rights. Outsourced software development shall be monitored and supervised by the organization.

13.12. Technical Vulnerability Management

Timely information about technical vulnerabilities of information systems being used shall be obtained. The organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

13.13. Control of Technical Vulnerabilities

Technical vulnerability controls shall be implemented through effective and systematic measurements to ensure the hardware and software are functioning as intended.

14. Business Continuity Management

Objective: To counteract with the interruption to business and to protect critical business processes from the effects of major failures of information systems and facilities or disasters and to ensure their timely resumption within tolerable time frames.

14.1. Preparation and Approval for Business Continuity Plans (BCP)

A single framework of enterprise wide business continuity plan shall be maintained to ensure all plans are consistent, addressing information security requirements and identifying priorities for testing and maintenance. BCP shall be prepared on the basis of business impact analysis that is conducted giving due considerations to business operations of the organization. BCP shall be approved by the Board of Directors or Senior management of the organization or the Head/Regional office as the case may be.

14.2. Business Continuity and Risk Assessment

Events that can cause interruptions to business processes and facilities shall be identified, along with the probability and impact of such interruptions and their consequences for information security.

14.3. Including Information Security in the Business Continuity Management Process

A managed process shall be in place for business continuity throughout the organization that addresses the information security requirements needed for the entire organization's business continuity.

14.4. Developing and Implementing BCP including Information Security

Plans shall be developed, documented, maintained and reviewed regularly to ensure the restoration of business operations.

14.5. Testing, Maintenance and Revision of BCP

Business continuity plan shall be tested and updated regularly to ensure that they are up to date and effective. These tests should ensure that all members of the recovery, operational and other relevant teams are aware of the plan, their role for business continuity and information security.

End of BSS Version 1