CENTRAL BANK OF SOLOMON ISLANDS
Financial Market Supervision Department

Prudential Guideline No.13
On Information Technology Security Risk Management

Applicability

1. The Prudential Guideline is applicable to Financial Institutions (FI) licensed and deemed licensed by the Central Bank of Solomon Islands (CBSI).

Purpose of Prudential Guideline

2. The Prudential Guideline aims to provide FIs with a minimum framework for information technology security risk management (ITSRM), to ensure financial institutions increase IT Security awareness, to protect and safeguard its information assets.

3. The Prudential Guideline also aims to provide FIs with guidelines to formulate an effective Institution-wide information technology security framework in order to protect FIs' valuable financial and technical assets.

4. This guideline provides minimum set practices and procedures aimed at reducing the likelihood of internal or external attack on IT resources and also limit the damage caused by an inadvertent or malicious incident.

5. The key requirements include:

    a. Commitment to IT Security;
    b. IT Security;
    c. IT Security Risk Management;
    d. IT Security Policy Development;
    e. IT Security Awareness and Training;
    f. IT Security Team;
    g. Incident Management;
    h. Contingency and Disaster Recovery Planning; and
    i. Information System Audit and Certifications

Definition

6. As used in this Prudential Guideline, the following terms, unless otherwise clearly indicated by the context, have the meanings specified below:

    "Access" – means a specific type of interaction between a subject or entity and an object or resource which results in a flow of information from one to another or in the subject or entity changing the observable properties of the object or resource. For example, the logging on to a computer system, for the purpose of gaining entry to a word processing application or gaining entry to stored information.

"Attack"- means the act of aggressively trying to bypass security controls on an IT system or network. The fact that the attack is made does not mean it will succeed. The success depends on the vulnerability of the system, network or activity and the effectiveness of safeguards in place.

"Disaster Recovery Planning"- means the process of developing a plan to restore information technology operations in the event of a disaster.

"Impersonation"- means an attempt to gain access to an IT system by posing as an authorized user.

"Information Asset"- means a component or part of the total information system to which the IT department directly assigns a value to represent the level of importance to the "business" or operations/operational mission of the department, and therefore warrants an appropriate level of protection. Assets types include: information, hardware, communication equipment, firmware, documents/publications, environmental equipment, people/staff, infrastructure, goodwill, money, income, organizational integrity, customer confidence, services and organizational image.

"IT Security"- means the protection resulting from an integrated set of safeguards, designed to ensure the confidentiality of information electronically stored, processed or transmitted; the integrity of the information and relate processes; the accountability of the information stored, processed or transmitted; and the availability of systems and services.

"Malicious Incident"- means an adverse event associated with an IT system(s): (a) that is a failure to comply with the departmental security regulations or directives; (b) that results in suspected or actual compromise of classified information or government property or information.

"Risk"- means adverse effects that can result if vulnerability is exploited or if a threat is actualized. In some contexts, a risk is a measure of the likelihood of adverse effects or the product of the likelihood and the quantified consequences.

"Security Incident"- means an adverse event associated with an IT System(s): (a) that is a failure to comply with IT department security regulations or directives; (b) that results in suspected or actual compromise of classified information or government property or information.

"Sensitivity"- means the characteristic of a source, which implies its value or importance to an organization, or the injury, or harm that could result from its deliberate or inadvertent discloser, modification, loss or denial.

"Potential Threat"- means any potential event or act that could cause one or more of the following to occur: unauthorized disclosure, destruction, removal, modification or interruption of sensitive or critical information, assets or services. A threat can be natural, deliberate or accidental.

"Vulnerability"- means a quantifiable, threat-independent characteristic or attribute of any asset within a system boundary or environment in which it operates and which increases the probability of a threat event occurring and causing harm in terms of confidentiality, availability, and or integrity, or increases the severity of the effects of a threat event if it occurs.

Commitment to IT Security

7. A clear commitment and direction towards IT Security, is required from the FIs' senior management. Each FI should ideally set up an IT Steering Committee with the objective of overseeing effective use of IT resources to support business objectives, identifying significant IT related risks, providing guidance in designing and modifying the IT policy to cope with the IT risks, documenting IT issues and initiatives, and monitoring the performance.

8. At the minimum, the committee should comprise of senior management, key business units' heads, and IT function's senior officers. The committee should meet regularly. The minutes of the meetings of the IT Steering Committee should be properly drawn up and periodically presented to the Board of Directors or its proxy and Senior Management.

IT Security

9. Each FI must mitigate in its ITSRM existing internal and external threats such as unauthorised access to critical financial data, service interruptions, impersonating clients and theft or alteration of information.

10. When a FI performs financial transactions, it is prone to risks listed in Paragraph 9. The risk control mechanism and security policies must be within the FI's legal arm's length and restrict this risk to an acceptable level.

IT Security Risk Management

11. The success of an IT Security program depends on its effective risk management. With risk management, a FI can identify, assess, measure, monitor risks, and take appropriate steps to reduce them. For any effective risk management program, the following vital steps must be followed in the prescribed order:

    a. **Identification of IT System:** As a first step, it is recommended that the FI carries out a detailed exercise to identify all systems, technology, and related assets that are involved in support of critical business processes, and prioritize them with a business value (in terms of the information they process and the cost associated with them) for ease of decision-making and accurate and realistic assessment. FIs should also consider to assign ownership within their respective organizations for identified technology and related assets with clear responsibilities to protect them.

    b. **Risk Assessment and Re-assessment:** Risk assessment helps to determine the vulnerability as well as the potential threats (and their consequences) to the identified information systems. Risk needs to be assessed from all aspects of IT Security including physical, environmental, administrative, and technical. It

should also identify threat sources and potential vulnerabilities, the likelihood of the occurrence of an event that will exploit that vulnerability and the resulting adverse impact of that event. Risk re-assessment should be a continuing process.

c. **Risk Mitigation:** Risk-reducing controls should be in place that mitigate or eliminate the identified risks and protect the organization's mission at the lowest cost, with minimal adverse impact to the business objectives. The recommended procedural and technical security controls have to be evaluated and prioritized considering the operational impact of the risks, feasibility of the mitigation controls and their cost benefit analysis.

IT Security Policy Development

12. IT Security Policies are critical and its security infrastructure since these in reality provide a "risk-control" mechanism and are developed in response to known risks. Security objectives can only be met in setting up a workable and organization-wide security policy. For efficient and effective IT Security, security policy and programs should be aligned to the business objectives. It is essential that the policies be structured as lightweight as possible, without missing any important issue. One way to achieve this is to split the whole master policy framework into a number of smaller policies and arrange them in a hierarchical, but coherent, manner.

13. IT Security policies should follow a defined process and that such process should be documented in IT Policies. Such policies should be approved by the Board of Directors or its proxy and vigorously enforced. They should be disseminated to authorized IT users for familiarity. They should also be revised periodically by Management and Board of Directors or its proxy board. Periodic review of IT Security policies and procedures helps identify any gaps from the previously implemented security measures and facilitates updated risk assessment for the organization. IT Security is, therefore, an ongoing process.

Awareness and Training

14. Awareness and training programs are crucial to IT Security since they ensure that users are aware of the risks to IT systems and the policies in place to protect those systems, that the users pay attention to the system and notify the management of any incident that appears to compromise security.

IT Security Team

15. To successfully implement IT Security, a lot of coordination work is required from both the technical side and the business side. It is recommended that a team be formed of a competent mix of experienced technical and business human resources with a thorough appreciation and understanding of IT Security issues. This team would streamline the IT Security related process and procedures, including incident response and management and should report to the IT Steering Committee.

Incident Management

16. IT Security Program will manage and mitigate the IT security risk, but even then exploitation of vulnerabilities can happen to the most well prepared organizations. When such an adverse event occurs, a proper plan must be in place to respond to the contingency. IT Incident management is responsible for incident response planning by covering every reasonable contingency scenario. It includes the definition of an incident response team and the steps (process) to take during an incident.

Contingency and Disaster Recovery Planning

17. Business continuity planning and disaster recovery planning are vital activities that ensure availability of resources to businesses in an event of disaster. As a first step, FIs should identify and document a potential impact of each category or type of disaster or event. Such a contingency and disaster recovery plan must then be maintained, tested, and audited by the internal auditors to ensure that it remains appropriate to the needs of the organization.

Information System Audit and Certifications

18. To ensure the adequacy of the adopted security plan and procedures and the effectiveness of the implemented controls, FIs should opt for a third party IT security audit. In order to build the confidence and trust in the industry and the clients, it should be appropriate for the FIs to go for internationally recognized certifications.

Reporting Requirements to the CBSI

19. Each financial institution must submit to the CBSI a copy of their IT security risks to enable effective oversight of performance of IT security management function in meeting its stated objectives. The reporting should include but not limited to the following:
    a. risk profile(s);
    b. exposure analysis;
    c. progress against strategy;
    d. incident analysis;
    e. system capacity and performance analysis;
    f. recovery status;
    g. infrastructure and software analysis;
    h. audit findings and ageing reports; and
    i. fraud analysis.

Implementation

20. Financial institutions have a transition period of (90) calendar days from the effective date to complete the following:
    a. Report on their compliance with this Prudential Guideline.
    b. Submit to CBSI a plan and timeframe for rectifying areas of non-compliance with this Prudential Guideline.

Enforcement and Corrective Measures

21. A FI, which fails to comply with the requirements contained in this Prudential Guideline or to submit certain reports to the CBSI, which are materially inaccurate, will be considered in breach of violation of this guideline and therefore, shall be subject to a monetary penalty.

22. The CBSI shall pursue any or all corrective measures as provided in section 16 of the Financial Institutions Act 1998 (as amended) to enforce the provisions of this Prudential Guideline including:
    c. Issuance of an order to cease and desist from the unsound and unsafe practices and
    d. Action to replace or strengthen the management of the financial institution.

Effective Date

23. The effective date of this Prudential Guideline is July 1, 2018.

Issued this 16th day of April 2018.

Governor Denton Rarawa
Central Bank of Solomon Islands