Guidelines[1] on Information Technology Security

Introduction

The State Bank of Pakistan recognizes that financial industry is built around the sanctity of the financial transactions. Owing to the critical role of financial institutions for a country and the extreme sensitivity of their information assets, the seriousness of IT Security and the ever-increasing threats it faces in today's open world cannot be overstated. As more and more of our Banking Operations and products & services become technology driven and dependent, consequently our reliance on these technology assets increases, and so does the need to protect and safeguard these resources to ensure smooth functioning of the financial industry.

State Bank is, therefore, setting down guidelines for IT Security through the understanding and addressing off the following areas:

- Commitment to IT Security
- IT Security
- IT Security Risk Management
- IT Security Policy Development
- IT Security Awareness & Training
- IT Security Team
- Contingency & Disaster Recovery Planning

These guidelines are meant to help the Banks/DFIs achieve adequate levels of IT Security.

Purpose and Nature

The objective of this document is two fold – to increase IT Security awareness of the Banks/DFIs, and secondly to provide them with guidelines to formulate an effective institution-wide information technology security framework in order to protect their valuable financial and technical assets. These guidelines will provide a starting point to set practices and procedures in place that will eventually reduce the likelihood of internal or external attack on IT resources and also limit the damage caused by an inadvertent or malicious incident.

Commitment to IT Security

A clear commitment and direction towards IT Security, is required from the banks/DFIs' senior management. Each bank/DFI 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 & modifying the IT policy to cope with the IT risks, documenting IT issues & initiatives and monitoring the performance.

The committee should be a mix of senior management, key business units' heads and IT function's senior officers. It should meet regularly. The minutes of the meetings of the

[1] These guidelines should be read in conjunction with the introduction along with the glossary, which contains an explanation of the abbreviations and other terms used in these guidelines.

IT Steering Committee should be properly drawn up and periodically presented to the Board of Directors and Senior Management.

IT Security

In today's world, the banking industry relies heavily on Information systems. Banks/DFIs must, therefore, understand existing internal and external threats, such as unauthorized access to critical financial data, service interruptions, impersonating clients and theft or alteration of information. When an institution performs financial transactions, it is very prone to such types of risk. The risk control mechanism and security policies are evolved within the organization to restrict this risk to an acceptable level. IT Security is, therefore, about mitigating/minimizing risk.

Risk Management

The success of an IT Security program depends on its effective risk management. With risk management, a bank/DFI 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:

- **Identification of System / Areas**

  As a first step, it is recommended that the organization 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. Banks may also consider to assign ownership within their respective organizations for identified technology and related assets with clear responsibilities to protect them.

- **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.

- **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

IT Security Policies are critical to any organization 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.

IT Security policies should follow a defined process – it is recommended that polices should be approved by the Board of Directors, disseminated and enforced, monitored and revised by Management/Board of Directors, compiled to and signed-off by the users. Revisiting IT Security policies and procedures helps identify any weak points from the previously implemented security measures and facilitates updated risk assessment for the organization. IT Security is, therefore, an ongoing process.

Awareness & Training

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 i.e. notify the management of any incident that appears to compromise security.

IT Security Team

To successfully implement IT Security, a lot of coordination work is required from both 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

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 & Disaster Recover Planning

Business continuity planning and disaster recovery planning are vital activities that ensure availability of resources to businesses in an event of disaster. The first step is to consider the potential impact of each type of disaster or event. The 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

To ensure the adequacy of the adopted security plan and procedures and the effectiveness of the implemented controls, banks/DFIs should opt for a third party IT

security audit. In order to build the confidence and trust in the industry and the clients, it may be appropriate for the banks/DFIs to go for internationally recognized certifications.

Conclusion

A completely secure, zero risk system is one which has zero functionality. Latest technology high-performance automated systems bring with them new risks in the shape of new attacks, new viruses and new software bugs, etc. IT Security, therefore, is an ongoing process. Proper risk management keeps the IT Security plans, policies and procedures up to date as per new requirements and changes in the computing environment. To implement controls to counter risks requires policies, and policy can only be implemented successfully if the top management is committed. And policy's effective implementation is not possible without the training and awareness of staff.

GLOSSARY

Access
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
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
The process of developing a plan to restore information technology operations in the event of a disaster.

Impersonation
An attempt to gain access to an IT system by posting as an authorized user.

Information Asset
A component or part of the total information system to which the 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
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 related processes; the accountability of the information stored, processed or transmitted; and the availability of systems and services.

Malicious Incident
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 (c) government property or information.

Risk
Intuitively, the adverse affects 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. There is no standard definition.

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

Sensitivity
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
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
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.