Information Technology Security

Management

Information technology security management can be defined as processes that support

enabling organizational structure and technology to protect an organization’s IT operations

and assets against internal and external threats, intentional or otherwise.

1. **Information Security Management Standards**

A range of standards are specified by various industry bodies. Although specific to an

industry, these standards can be used by any organization and adapted to its goals. Here we

discuss the main organizations that set standards related to information security management.

**Federal Information Security Management Act**

National Institute of Standards and Technology (NIST) has specified guidelines for implementing the Federal Information Security Management Act (FISMA). This act aims to provide the standards are :

* Standards for categorizing information and information systems by mission impact
* Standards for minimum security requirements for information and information systems
* Guidance for assessing security controls in information systems and determining security control effectiveness
* Guidance for certifying and accrediting information systems

The “FederavInformation Security Management Framework Recommended by NIST” sidebar describes the risk management framework as specified in FISMA. The activities specified in this framework are paramount in implementing an IT security management plan.

**Federal Information Security Management Framework Recomended by NIST**

* **Step 1 : Categorize**

In this step, information systems and internal information should be categorized based on impact.

* **Step 2 : Select**

Use the categorization in the first step to select an initial set of security controls for the information system and apply tailoring guidance as appropriate, to obtain a starting point for required controls.

* **Step 3 : Supplement**

Assess the risk and local conditions, including the security requirements, specific threat information, and cost/benefit analyses or special circumstances. Supplement the initial set of security controls with the supplement analyses.

* **Step 4 : Document**

The original set of security controls and the supplements should be documented.

* **Step 5 : Implement**

The security controls you identified and supplemented should be implemented in the organization’s information systems.

* **Step 6 : Assess**

The security controls should be assessed to determine whether the controls are implemented correctly, are operating as intended, and are producing the desired outcome with respect to meeting the security requirements for the system

* **Step 7 : Authorize**

Upon a determination of the risk to organizational operations, organizational assets,

or individuals resulting from their operation, authorize the information systems.

* **Step 8 : Monitor**

Monitor and assess selected security controls in the information system on a

continuous basis, including documenting changes to the system.

**International Organization for Standardization**

Other influential international bodies, the International Organization for Standardization(ISO) and the International Electrotechnical Commission (IEC), published ISO/IEC 17799:2005. These standards establish guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an

organization. The objectives outlined provide general guidance on the commonly accepted

goals of information security management.

**Other Organizations Involved in Standards**

Other organizations that are involved in information security management include The Internet Society and the Information Security Forum . These professional societies

have members in the thousands. The Internet Society is the organization home for the groups responsible for Internet infrastructure standards, including the Internet Engineering

Task Force (IETF) and the Internet Architecture Board (IAB). The Information Security Forum is a global nonprofit organization of several hundred leading organizations in financial

services, manufacturing, telecommunications, consumer goods, government, and other

areas. It provides research into best practices and advice, summarized in its biannual

Standard of Good Practice, which incorporates detailed specifications across many areas.

1. **Information Technology Security Aspects**

The various aspects to IT security in an organization that must be considered include the following:

• Security policies and procedures

• Security organization structure

• IT security processes

Processes for a business continuity strategy

Processes for IT security governance planning

• Rules and regulations

**Security Policies and Procedures**

Security policies and procedures steps are essential for implementing IT security management: authorizing security roles and responsibilities to various security personnel; setting rules for expected behavior from users and security role players; setting rules for business continuity plans; and more. The security policy should be generally agreed to by most personnel in the organization and should have the support of the highest-level management. Some important issues included in most security policies are :

* Access control standards.
* Accountability
* Audit trails
* Backups
* Disposal of medi
* Disposal of printed matter
* Information ownership
* Managers’ responsibility
* Equipment
* Communication
* Work procedures and processes

**Security Organization Structure**

Various security-related roles need to be maintained and well defined. These roles and their brief descriptions are described here :

* End User
* Executive Management
* Security Officer
* Data/Information Owners
* Information System Auditor
* Information Technology Personnel
* System Administrator

**IT** **Security Processes**

To achieve effective IT security requires processes related to security management. These processes include business continuity strategy, processes related to IT security governance planning, and IT security management implementation.

Processes for a Business Continuity Strategy

As is the case with any strategy, the business continuity strategy depends on a commitment from senior management. The Disaster Recovery Institute International (DRII) associates eight tasks with the contingency planning process. They are as follows:

* Business impact analysis, to analyze the impact of outage on critical business function operations.
* Risk assessment, to assess the risks to the current infrastructure and the incorporation of safeguards to reduce the likelihood and impact of disasters.
* Recovery strategy identification, to develop a variety of disaster scenarios and identify recovery strategies.
* Recovery strategy selection, to select the appropriate recovery strategies based on the perceived threats and the time needed to recover.
* Contingency plan development, to document the processes, equipment, and facilities required to restore the IT assets.
* User training, to develop training programs to enable all affected users to perform their tasks.
* Plan verification, for accuracy and adequacy.
* Plan maintenance, for continuous upkeep of the plan as needs change.

Processes for IT Security Governance Planning

IT security governance planning includes prioritization as its major function. This helps in utilizing the limited resources of the organization. Determinin priorities among the potential conflicting interests is the main focus of these processes. This task includes budget setting, resource allocation, and, most important, the political process needed to prioritize in an organization.

Rules and Regulations

An organization is influenced by rules and regulations that influence its business. In a business environment marked by globalization, organizations have to be aware of both national and international rules and regulations. We give more details on some rules and regulations here:

* The Health Insurance Portability and Accountability Act (HIPAA) requires the adoption of national standards for electronic healthcare transactions and national identifiers for providers, health insurance plans, and employers.
* The Sarbanes-Oxley Act of 2002 (SOX) requires companies to protect and audit their financial data.
* State Security Breach Notification Laws (California and many others) require businesses, nonprofits, and state institutions to notify consumers when unencrypted “personal information” might have been compromised, lost, or stolen.
* The Personal Information Protection and Electronics Document Act (PIPEDA) supports and promotes electronic commerce by protecting personal information that is collected, used, or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions.
* The Computer Fraud and Abuse Act, or CFAA (also known as Fraud and Related Activity in Connection with Computers), is a U.S. law passed in 1986 and intended to reduce computer crimes.