# REVIEW ON INFORMATION SECURITY MANAGEMENT

Madhavi Dhingra
Asst. Prof., Amity University Madhya Pradesh
Email: madhavi.dhingra@gmail.com

**Abstract**

**Currently, all organizations have to tackle the issue of information security. The paper deals with various aspects of Information Security Management (ISM), including procedures, processes, organizational structures, policies and control processes. Introduction of Information Security Management should be a strategic decision. The concept and implementation of Information Security Management in an organization are determined by the corporate needs and objectives, security requirements, the processes deployed as well as the size and structure of the organization. The implementation of ISM should be carried out to the extent consistent with the needs of the organization.**

**Keywords: information security; information security policy; asset management of organization; business continuity management; management of intrusion**

## 1. Introduction

An information security management system (ISMS) is a set of policies concerned with information security management or IT related risks. Security management is becoming a strategic, tactical and operational objective of almost any enterprise or organization. In the public sector, the development of e-government applications becomes possible only if IT-risks are correctly managed.

## 2. Security Management

Security management involves user authentication and identity management, digital rights management and data integrity, certificate management for Public Key Infrastructures (PKI).

User authentication is the starting point of making IT-systems more secure. It is also one of the most critical weaknesses of many internet-based systems, since attackers often try to get access to the system by using the identity of another user. Password identification is no longer considered as being secure, so alternatives must be searched. Most of the present approaches rely on strong authentication, combining a secret the user knows, with something he holds (for instance some portable memory device). On the other hand, experiences in biometrics have not been fully satisfying until now. As a consequence, it is important to explore new means of authentication and to evaluate the efficiency of these approaches. Very often authentication is only done at the entry point of an IT-system. Today this is no longer sufficient, since an attacker could get access to any point of the IT-system; so it is important to generalize the authentication model to all interactions between hard- or software components. Therefore completely new approaches in system design and threat modelling are needed.

Authentication is only as strong as the user management processes and these rely on efficient identity policies. Identity management has become an active research topic since the events of 9-11 and the subsequent growing awareness of the dangers of terrorism. All countries now have the problem of correctly identifying each member of the society, as the old identification schemes are outdated. The Luxembourg national personal identity number for instance is based on the date of birth and the sex of the identified person. This is no longer in accordance with the modern requirements of protection of personal data, where there should be no information leaking from the identification data.

One way of authentication and identity management relies on the use of a Public Key Infrastructure. Such a highly secure infrastructure requires very important investments and an excellent technical, organizational and legal know-how. Therefore it is essential to explore new business cases for these infrastructures, which cannot survive in selling only identity certificates.

## 3. Information Security Cycle

ISO/IEC 27001:2005 therefore incorporated the "Plan-Do-Check-Act" (PDCA), or Deming cycle, approach:

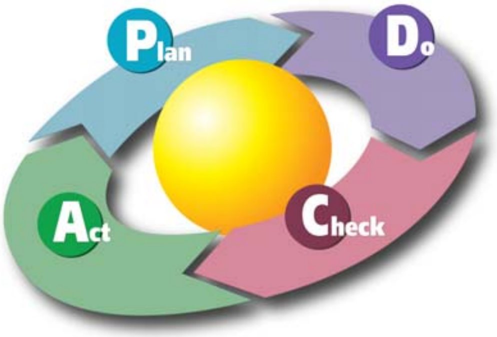

Figure 1: PDCA or Deming Cycle used by ISMS Standards

- The Plan phase is about designing the ISMS, assessing information security risks and selecting appropriate controls.
- The Do phase involves implementing and operating the controls.
- The Check phase objective is to review and evaluate the performance (efficiency and effectiveness) of the ISMS.
- In the Act phase, changes are made where necessary to bring the ISMS back to peak performance.

ISO/IEC 27001:2005 is a risk based information security standard, which means that organizations need to have a risk management process in place. The risk management process fits into the PDCA model given above.

## 4. Need for an Information Security Management System

Security experts say:

- information technology security administrators should expect to devote approximately one-third of their time addressing technical aspects. The remaining two-thirds should be spent developing policies and procedures, performing security reviews and analyzing risk, addressing contingency planning and promoting security awareness;
- security depends on people more than on technology;
- employees are a far greater threat to information security than outsiders;
- Security is like a chain. It is only as strong as its weakest link;
- the degree of security depends on three factors: the risk you are willing to take, the functionality of the system and the costs you are prepared to pay;
- Security is not a status or a snapshot, but a running process.

These facts inevitably lead to the conclusion that security administration is a management issue, and not a purely technical issue.

The establishment, maintenance and continuous update of an ISMS provide a strong indication that a company is using a systematic approach for the identification, assessment and management of information security risks.

## 5. Critical factors of Information Security Management System ISMS

Confidentiality: Protecting information from unauthorized parties.

Integrity: Protecting information from modification by unauthorized users.

Availability: Making the information available to authorized users.

A company will be capable of successfully addressing information confidentiality, integrity and availability (CIA) requirements which in turn have implications:

- business continuity;
- minimization of damages and losses;
- competitive edge;
- profitability and cash-flow;
- respected organization image;
- legal compliance

Large organizations, banks and financial institutes, telecommunication operators, hospital and health institutes and public or governmental bodies have many reasons for addressing information security very seriously. Legal and regulatory requirements which aim at protecting sensitive or personal data as well as general public security requirements impel them to devote the utmost attention and priority to information security risks.Under these circumstances, the development and implementation of a separate and independent management process - namely an ISMS - is the only alternative.

The development of an ISMS framework based on ISO/IEC 27001:2005 entails the following six steps:

- Definition of security policy,
- Definition of ISMS scope,
- Risk assessment (as part of risk management),
- Risk management,
- Selection of appropriate controls
- Statement of applicability

## 6. Issues in Information Security Management System

There are three main problems which lead to uncertainty in information security management systems (ISMS):

1. Dynamically changing security requirements of an organization -Rapid technological development raises new security concerns for organizations. The existing security measures and requirements become obsolete as new vulnerabilities arise with the development in technology. To overcome this issue, the ISMS should organize and manage dynamically changing requirements and keep the system up-to-date.

2. Externalities caused by a security system
Externality is an economic concept for the effects borne by the party that is not directly involved in a transaction. Externalities could be positive or negative. The ISMS deployed in an organization may also cause externalities for other interacting systems. Externalities caused by the ISMS are uncertain and cannot be predetermined before the ISMS is deployed. The internalization of externalities caused by the ISMS is needed in order to benefit internalizing organizations and interacting partners by protecting them from vulnerable ISMS behaviors.

3. Obsolete evaluation of security concerns
The evaluations of security concerns used in ISMS become obsolete as the technology progresses and new threats and vulnerabilities arise. The need for continuous security evaluation of organizational products, services, methods and technology is essential to maintain an effective ISMS. The evaluated security concerns need to be re-evaluated. A continuous security evaluation mechanism of ISMS within the organization is a critical need to achieve information security objectives. The re-evaluation process is tied with dynamic security requirement management process discussed above.

## 7. Conclusion

The chief objective of information security management is to implement the appropriate measurements in order to eliminate or minimize the impact that various security related threats and vulnerabilities might have on an organization. In doing so, information security management will enable implementing the desirable qualitative characteristics of the services offered by the organization (i.e. availability of services, preservation of data confidentiality and integrity etc.). By preventing and minimizing the impacts of security incidents, ISMS ensures business continuity, customer confidence, protect business investments and opportunities, or reduce damage to the business.

References

1. Humphreys, Edward (8 March 2011). "Information security management system standards". Datenschutz und Datensicherheit : 7–11.
2. Jo, Heasuk; Kim, Seungjoo; Won, Dongho (1 January 2011). "Advanced information

security management evaluation system". KSII Transactions on Internet and Information Systems 5(6): 1192–1213.

3. Caballero, Albert. (2009). "14". Computer and Information Security Handbook. Morgan Kaufmann Publications. Elsevier Inc. p. 232. ISBN 978-0-12-374354-1.

4.Ma, Qingxiong; Schmidt, Mark B.; Pearson, Michael (2009). "An integrated framework for information security management". Review of Business 30 (1): 58–69. Retrieved 26 October 2013.

5. Abbas, Haider; Magnusson, Christer; Yngstrom, Louise; Hemani, Ahmed (1 January 2011). "Addressing dynamic issues in information security management". Information Management & Computer Security 19 (1): 5–24.