Information Security Management Systems

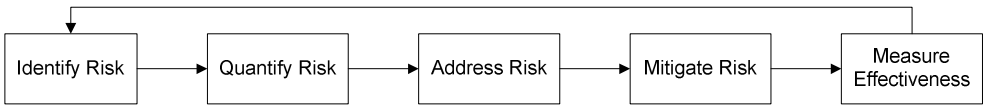
Prasanna Ramakrishnan, CISSP

Introduction

Information security has always been looked upon as a necessary evil by business people and management. One of the biggest challenges for INFOSEC professionals has been to sell security to management. Some of the recent events like the 9/11, the big blackout in northeast, virus/worm attacks etc., have really brought information security to the work table of the Government, management and other decision makers. On the same token, information security is no good until it is effectively managed and controlled. This paper makes an attempt to discuss the concepts of Information security management systems (ISMS)

Information security process

Information security is a *process* and not a *product*. The process is intended to identify and minimize risk to acceptable levels. It should be iterative and should be managed.



The process of Information Security

Why information security is difficult?

Information security is no different from a typical network infrastructure or server infrastructure. It is only as good as the brains that put it together. However, it is very difficult to show a tangible value on information security infrastructure until after the actual hit occurs and losses are incurred. Hence, in today's world, most of information security is a 'reactive' phenomenon as opposed to being a 'proactive' phenomenon.

Information Security Management System (ISMS)

ISMS is a proactive approach to continuously and effectively manage, at a high level, information security including people, infrastructure and businesses. The goal is to reduce risks to manageable level, while taking into perspective both business goals and customer expectations. ISMS is not specific to an industry. The beauty is that the concepts from ISMS can be applied with little modifications to make it relevant to a specific industry. ISMS is not a specific virus update, or a patch or a firewall rule set, but it is the common sense behind what needs to go where. Many enterprises already have significant investment in information security products such as firewalls and anti-virus. ISMS maximizes the efficient use of all the organizational resources.

ISMS and relevant standards

ISMS is not a standalone concept. It has its derivatives from various different international bodies and

standards. Included are:
ISO 17799/BS17799 - ISO17799 is for the IT security industry, what ISO 9000 is for the TQM industry. It attempts to protect the quality of the C,I,A of information.
ISO 13335 – Guidelines for management of IT security
GASSP – Generally accepted system security principle.

Recently, ISSA is initiating an effort in the development and maintenance of the Generally Accepted Information Security Principles (GAISP). ISMS fits nicely into all these buckets.

Designing ISMS

The first step in designing an ISMS is to select the framework within which the ISMS will function. The framework will depend on the type of industry or the need to go for certification (such as BS7799)

Terminology

There should be a consistent use of terminologies in the entire ISMS infrastructure so that there is no room for confusion. In addition, the definitions to terminologies should be concise and clear. For example, a 'standard' is defined as requirement that supports the policy and can be measured, whereas a 'guideline' is defined as a best practice recommendation on how to meet requirements.

Authorization and ownership

Before starting to build and implement an ISMS, all the stakeholders should be identified and the authorization agreed upon. Authorization exists in multiple levels such as authorization to adopt the policies, standards etc., authorization to change the policies, standards etc. There should also be a documented authorization process in place.

The environment

It is always helpful to understand the environment and the space in which the enterprise is working in to effectively design an ISMS. It is beneficial to know if the ISMS will ultimately satisfy a marketing requirement or a legal requirement for the enterprise. Some additional information on the environment that can be gathered could be:

- An org chart of the enterprise
- Is management centralized or decentralized?

Building ISMS

Building an ISMS involves many steps. While performing each step, inputs from all the stakeholders identified above should be included and results discussed to reach an agreed upon path. A *security manual* serves as the central repository for ISMS. This manual will be maintained by the Chief security officer and usually considered a confidential document. The various steps involved in building an ISMS are:

Step – 1: Risk Assessment

An industry accepted security risk assessment should be done. The goal is to identify assets, threats, vulnerabilities and controls to mitigate risks. Some risks will be accepted and management approval should be attained on this.

Step – 2: Top down approach

Security is a management issue and not just an IT issue. Hence it is critical that top management plays an important role in building an ISMS. Management should have the overall ownership of ISMS. Management should encourage a culture within the enterprise to follow security principles.

Step – 3: Functional roles

Once management's approval is attained, functional roles will have to be identified. Depending on the type and size of the enterprise, the roles can vary in type and number. A chief information security officer should be identified who solely owns the ISMS. Other functional roles could include Data stewards, Security awareness trainers etc.

Step - 4: Write the Policy

The security policy is a document that states the enterprise's information security strategy at a high level. The language in the policy is derived from the risk assessment. Details should be avoided in a policy. In order to make the policy acceptable to all stakeholders, the wording in the policy should be at a high level and align nicely with the enterprise's business priorities and goals.

Step – 4: Write the Standards

Standards are *definite requirements* that an enterprise should put forth for everybody to follow. The standards should support the security policy and be measurable. It is good practice to document what the penalties are when standards are not met

Step – 5: Write the guidelines and procedures

Guidelines are *recommended ideas* for an enterprise. They can also be termed as 'nice to haves'. It should be noted that the effectiveness of an enterprise's security management will not be measured by the guidelines present. There, usually, are no penalties for not following the guidelines. However, there can be some incentives if the enterprise follows the guidelines.

Procedures are *step by step description* on how to meet the standards or guidelines so that the policy is supported. Procedures are usually targeted at the system level people who actually implement the control.

Controls

The need for controls is an outcome of the risk assessment process. Once the need for controls is decided, the choice of control is done based on a cost-benefit analysis of the asset it is protecting and the control's cost itself. In ISMS, controls can be software, hardware, person or a process. In a good ISMS, they should be implemented and used for their intended purposes only.

Maintaining an ISMS

Everything in Information security should be an iterative process. ISMS is no different. An ISMS is built with a snapshot of information and may become outdated or obsolete, rendering the ISMS ineffective. A yearly audit of the ISMS is suggested. The audit should reveal the following:

- Are the controls online and performing their intended functions?
- Are there any new risks identified that need to be addressed?
- Do the policy, standards, guidelines and procedures need to be changed or updated?
- Identify gaps between what was set forth in the ISMS manual and what the practice is

The audit can be done in house or by a third party.

Practical examples of ISMS

Information security took a gigantic dimension with the publication of the PDD 63 for protecting US's critical infrastructure. Since then there has been a slue of regulations and requirements from various organizations that apply to various industries. The goal of all these regulations is one: hold management responsible for information security and encourage them to show 'due diligence' in protecting their assets.

HIPPA

Health Insurance Portability and Accountability Act, applies to the health care industry and attempts to put forth requirements and guidelines to protect the privacy of common individuals, when it comes to dealing with hospitals, doctors, pharmacies etc. HIPPA addresses the same topics, ISO 17799 addresses in its 10 domains, with an emphasis on privacy of information.

GLBA and BITS

Gramm Leach Bliley act applies to the banking and financial industry and addresses privacy of information in that industry. GLBA has four steps as

- Identify and assess the risks that may threaten customer information.
- Develop a written plan containing policies and procedures to manage and control these risks.
- Implement and test the plan.
- Adjust the plan on a continuing basis to account for changes in technology, the sensitivity of customer information, and internal or external threats to information security.

This reflects nicely with the steps in designing an ISMS.

BITS is a financial round table that is serving as a strategic brain trust for all financial institutions. As demonstrated in the BITS *Security Assessment Expectation Matrix* document, BITS has recognized the value of ISO17799, mapping segments of the BITS framework to the various ISO17799 control areas. Hence an ISO17799 based Information Security Management System (ISMS) can easily integrate into the BITS framework

FERC/NERC SMD NOPR

Federal Energy Regulatory commission/North American Reliability council are the governing bodies for the energy utilities in North America. Their recently published cyber security guidelines references ISO-17799 when it comes to controls in many areas such as access controls, physical security, and others.

Finally…..

ISMS attempts to achieve 'due diligence' on the part of management to mitigate business risks. It is common sense to say that the most secure piece of hardware is one that is turned off and does not have a power connection to it. However, this isn't practically feasible. Many enterprises boast of possessing the latest and greatest security/network technology. However, the entire infrastructure is rendered ineffective if there is no good security management in place. Not long ago, Information security management was considered an expensive add-on. However, it is not illogical to conclude that the recent disastrous events and few regulations that followed will make enterprises consider ISMS at a more

serious level.