

Information Security Management Systems (ISMS)

–

A comparison between ISO 27001 and ISM3

The necessity for a comprehensive management framework for Information Security and the two standards, which are used for building the same. The focus is on ISO 27001, which has a compliant/Not compliant approach and ISM3, which has a significantly different approach, based on maturity levels.

Author

Anup Narayanan, CISA, CISSP
2nd Floor, Melka Tower, Cheruparampath Road, Kadavanthra, Kochi,
Kerala, India
anup@anupnarayanan.org

Abstract.

The term ISMS is in circulation amongst senior level business decision makers and Information Technology implementers for the past few years, as the realization that there is a need for a comprehensive approach towards Information Security has set in. Approaching Information Security from a technical perspective does provides security for one area of the organization, viz. Wireless Network, Perimeter, Desktops etc. The big question, which the Information Security community is trying to answer, is – “How to integrate the stand-alone security solutions under one common framework and integrate it with the business goals of the organization”.

The Information Security community has answered this question by developing frameworks (standards), which can be used to develop a comprehensive Information Security Management framework. Significant amongst them have been ISO 27001, which has evolved into ISO 27001. ISO 27001 has a controls-oriented approach, which has a “security” or “no security”. In significant contrast to this Information Security Management Maturity Model, referred to as ISM3 (pronounced ISM cubed) adopts a process-oriented approach towards Information Security. ISM3 does not aim at absolute security unlike ISO 27001. ISM3 looks at security, as a component that has to grow over a period of time and that is not possible to have absolute 100% security.

Information Security: A Business Case

Information generates and sustains organizations in today's global business landscape. The challenge facing organizations is security of intellectual information and the assets containing this information. This challenge is further enhanced by the trans-national nature of businesses, whereby organization exchanges information between one another, either as a form of business outsourcing or transfer of information between clients and customers etc.

Organizations started to respond to these challenges by implementing technical measures to protect conduits of Information and storage devices. Though they proved sufficient initially, as businesses evolved new threats surfaced, significant amongst them being "Inside Information Theft", "Social Engineering", "Leakage of Intellectual Information through non-technical channels" etc.

This realization has shifted the focus from viewing Information Security as a technical solution to a management motivated organizational culture.

The advent of Information Security Management Systems (ISMS)

Developed nations are today at the forefront of developing and defining standards in Information Security, significant amongst them being COBIT, ISO 27001, ISM3 etc. The primary purpose of this standard is to provide a single framework for effective Information Security management. This includes in general,

- Having a vision defining the importance of Information Security from a business perspective.
- Integrating technical and non-technical security approaches.
- Planning and implementing solutions.
- A method for continuous improvement.
- Adequate documentation.
- Steps to ensure continuity of business.

A significant change in outlook which standards have brought about can be summarized below,

- An organization stands to lose it's chance for good business with intelligent customers if they do not pay attention to

Information Security or rather see it as an area purely concerning the IT department.

- The realization that customers need assurance that there is adequate protection for critical information.

The catalyst for this change in approach has been standards and guidelines. The current international standards in Information Security such as ISO 27001 and ISM3 works around the principle of ISMS. These standards approach Information Security in a top-down manner, with the initiatives towards an ISMS set and supported by the senior management and implemented by the lower rungs of the organization.

Comparison of ISM3 and ISO 27001 for the purpose of designing, deploying and maintaining ISMS integrated to business goals.

An analysis of ISM3 and ISO 27001 would best start with a basic overview of the underlying principles of the standard and the reasons as to why they were established. ISO 27001 has found considerable adoption with around 1500 organizations certified since its inception. But a significant hurdle to adoption of ISO 27001 is its stress on a risk analysis and building ISMS around the same. The fact is that there is no proven standard or reproducible method to do a risk analysis, which guides an organization on the security measures they should implement or how much to spend on security.

ISM3 works on a concept of the need for Information Security coming from within the business. By aligning security processes with business requirements, the impact of incidents can be reduced and security investments directed at the areas of more returns.

ISO 27001 – A brief description

ISO 27001 has its origins from a code of good practice published by the UK Department of Trade and Industry in 1989, which slowly evolved into BS7799. ISO 27001 is a set of guidelines, which can be used by an organization to design, deploy and maintain ISMS.

ISO 27001 consists of a set of guidelines, which can be used to implement the ISMS. The organization designs a scope for developing

the ISMS, and selects the controls, which fits into the scope and reject some of the controls, which are not required. The process of certification involves an auditor deputed by a certification body examining the scope of work and the justification for choosing/ignoring controls and the effectiveness of the same.

ISM3 – A brief description

ISM3 (pronounced ISM cubed) offers a paradigm shift in designing and deploying Information Security Management Systems. The principal author of the standard is Vicente Aceituno Canal¹. Vicente designed ISM3 to provide a framework for Information Security Management that can be used both at an entry level by small organizations and at a sophisticated level by major organizations as part of their governance assurance processes. ISM3 is based on maturity levels, so that an organization can choose a level, which fits their needs, and move towards it.

The base for ISM3 is built from best ideas of management systems and controls from ISO 9000, ITIL, CMMI and ISO 27001. Apart from ISO 27001, ISM3 is the only Information Security standard that is accreditable. The major difference between ISO 27001 and ISM3 is that the second has four maturity levels, while ISO 27001 takes a compliant/non-compliant approach. ISM3 is based on maturity levels, so that an organization can choose a level, which fits their needs, and move towards it. A brief overview of these levels is presented below in Table 1.

Maturity Level	Description
ISM3 Level 0	This level is not recommended.
ISM3 Level 1	This level should result in significant reduction in risks from technical threats, for a minimum investment in essential ISM processes. This level is recommended for organizations with low information Security Targets in low risk environments.
ISM3 Level2	This level should result in further risk reduction from technical threats for a moderate investment in ISM processes.

¹ Vicente Aceituno Canal can be reached at Vicente@isecom.org

	This level is recommended for organizations with normal Information Security targets in normal risk environments.
ISM3 Level 3	<p>This level should result in the highest risk reduction from technical threats, for a serious investment in Information Security processes.</p> <p>This level is recommended for organizations with high Information Security targets in high-risk environments.</p>
ISM3 Level 4	<p>This level should result in the highest risk reduction from technical and internal threats, for a serious investment in Information Security processes.</p> <p>This level is recommended for organizations affected by specific requirements (such as utilities, financial institutions and organizations sharing or holding sensitive information) with high Information Security targets in normal or high-risk environments.</p>

Table 1. A description of maturity levels used by ISM3.

A joint analysis of ISM3 and ISO 27001

A comparison between the key differentiating factors with respect to ISM3 and ISO 27001 is presented below.

The approach:

ISO 2700 has a compliant/ non-compliant approach built around Controls. The focus is on implementing controls to mitigate risks. This provides an easy framework from an implementation perspective. The disadvantage is that this approach is not suitable from a Management perspective, as they may find "Controls" difficult to understand. Management would like it if Security is aligned to business goals.

ISM3 has a process-oriented approach towards Information Security which focuses on the business goals of the organization. This is best illustrated with the following example.

Example - The primary business goal of any organization is to be profitable. To attain this, resources have to be utilized to the maximum. A threat to this could be viruses, which would infect systems and reduce the number of man-hours.

ISM3 would approach this situation with the following manner - – “The number of man-hours lost due to virus attacks should be less than 10 per annum”. This is a classic example of defined (attainable) security and the performance of the ISMS can be measured against this target. If the organization achieves this target, they can redefine the targets towards more stringent ones and raise the level of security. This approach is easy for the management to understand.

With respect to ISO 27001, it would be a controls oriented approach, whereby the standard states whether there exists a control to prevent malicious software. The task of the auditor is to check whether this control is working properly or not and whether any weaknesses has been identified and rectified. This approach focuses only on controls and not the performance of the business due to the controls/.

Measuring the performance of the ISMS

ISO 27001 does not metrics to check the performance of the ISMS. The task of the auditor is to look at the proper functioning of controls. In essence, the concept of shifting from one level of security to another is absent. The organization's focus is always on getting the controls to work fine. Over a period of time this becomes a monotonous task as there is not end goal to aim for.

ISMS follow “Levels of Maturity”. An organization can start Information Security implementation at a level, which is comfortable for the organization, and move upwards. At each level a set of defined goals are formulated and achievement of these goals are mandatory for moving on to the next level.

Ease of understanding

ISO 27001 is more auditor friendly than management friendly, since Security Targets are not based on business goals, but derived from a risk

analysis framework. Key decision makers of an organization would find it difficult to understand and appreciate technical matter such as risk analysis reports. Further, when the Information Security team approaches the management with a list of controls, Management cannot understand the concept of “controls” very well and they would prefer a “return of investment approach” on information security.

ISM3 is easy to understand from a business perspective as the Security Targets are defined from the perspective of overall business goals and not from a Risk Analysis report per se. This is easy for the management to understand.

Do ISO 27001 and ISM3 complement each other?

Implementation of ISM3 processes complements ISO 27001 in a significant manner. For the Information Security Practitioner ISM3 is a tool to implement a business oriented ISMS and further the ISMS can be certified as per ISO 27001.

Summary

It is necessary for standards to complement each other in order to ensure that businesses are conducted in a robust manner aided by secure information storage, transfer and processing. ISO 27001 and ISM3 differ in approach, but the end objective of both standards is to ensure a comprehensive Information Security Management System. ISO 27001 stresses on Risk Assessment, the drawback of which tends towards a lack of alignment with security investments and absence of direct alignment to business needs. Both these factors are an important component for effective Information Security management. ISM3 aims to address these problems by aligning Information Security with business goals.

Acknowledgment

I would like to thank Vicente Aceituno Canal for encouraging me to review ISM3 and for his guidance in making clear to me the principles behind it.

References

Standards

ISM3, <http://www.isecom.org/projects/ism3.shtml>

ISO 27001-2: 2002, <http://www.bsi-global.com>

ISO/IEC 17799:2000, <http://www.17799.com>

COBIT, <http://www.isaca.org>

CMMI, <http://www.sei.cmu.edu/cmmi/>

Information from Websites

ISECOM – www.isecom.org

“Security Standards” –

<http://infosecuritymag.techtarget.com/2002/mar/iso17799.shtml>