Implementation of ISMS and its Practical Shortcomings

Alpana Kakkar, Ritu Punhani,
Dr. S. Madan, Prof. D. Jain

International Research Journal
ISSN 1839-6518
Vol. 2, No. 1, 2012
82800201201205

Implementation of ISMS and its Practical Shortcomings

Alpana Kakkar,
Ritu Punhani,
Dr. S. Madan
Prof. D. Jain

International Research Journal
ISSN 1839-6518
Vol. 2, No. 1, 2012
82800201201205

Implementation of ISMS and its Practical Shortcomings

Abstract

Information security has been a global issue and challenge from many years. Protection of vital information of the organization has always been a huge challenge for all as millions of intruders put continuous efforts to get access to this information. The information whether stored in physical form on papers or in electronic form in computers, is the most critical element of any successful business and its high values make it the focused target of intruders. Organizational data face threats from external as well as internal factors of the organizations and there is no surprise that organizations implement security measures for their data assets in their premises and networks. Companies spend huge efforts, time, and money on the security of their crucial data and make best possible efforts to keep their data confidential and private yet face losses at many places due to limitations of their security systems.

This white paper highlights some most common practical shortcomings in the security systems of the companies.

Information Security Management System (ISMS)

An information security management system (ISMS) is a set of policies concerned with the management of security of information crucial in business success. The governing principle behind ISMS is that an organization should design, implement and maintain a coherent set of policies, processes and systems to manage and control the risks to its data assets, and herby ensuring acceptable levels of security risks to its information resources.

"ISMS" is known as an initiative from the UK Department of Trade and Industry in 1995 and originally its main objective was to provide a code of practice to information security practitioners. ISMS concern itself with the security of information whether in physical or logical form and focuses on three areas *(quote from ISO/IEC 13335-1:2004)*:

i. **Confidentiality:** The property that information is not made available or disclosed to unauthorized individuals, entities, or processes;
ii. **Integrity:** The property of safeguarding the accuracy and completeness of assets;
iii. **Availability:** The property of being accessible and usable upon demand by an authorized entity.

These three areas are commonly known as "CIA".

ISMS is never a one-time effort or investment, rather is a continuous cycle of planning, implementation, assessment, and improvement as shown in Figure-1.

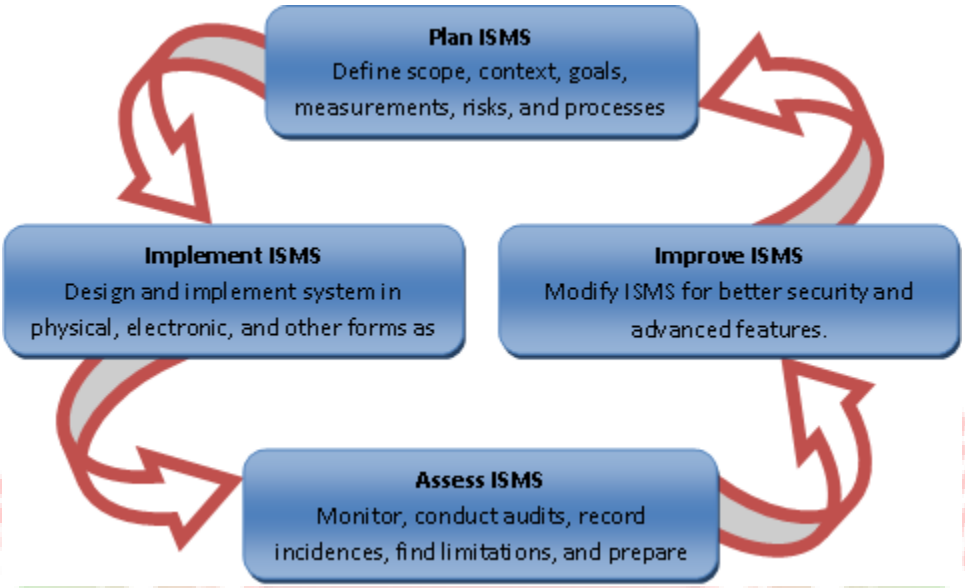

Figure 1: ISMS Life Cycle

Need of ISMS

Increasing number of security breaches and information leaks causing huge business losses have increased organizational concerns over adoption of effective ISMS.

An ISMS empowers an organization with a mechanism to systematically manage the risks to its information security. By establishing the ISMS, the organization can determine the necessary security levels, mitigation plans and distribute its assets based on its own assessment of associated risks in addition to technical countermeasures against each individual issue.

The major need of ISMS in an organization is to manage the risk to information security and minimize the losses due to any breach or incidence. It provides the organization an improved security system for its vital information assets. ISMS enforces the implementation the mechanism of providing the relevant information to and only to relevant levels of accesses. It herby enforces the organizations to understand different levels of access-requirements of the information and relevancy of access by an internal or external resource. This not only allows a detailed understanding of value of the information but also avoids confusions or misunderstanding by flow of irrelevant information on different access levels.

ISMS helps the organization in developing an understanding of the business drivers and strategies within the organisation and identifying the key threats and perils related to these activities. It helps in analysing the security implications of the network topology, the key security

components of the network design, and the security characteristics of key applications related to external connections and business activities. Figure-2 shows ISMS as a 3-phase process implementation addressing to different actions or objectives:

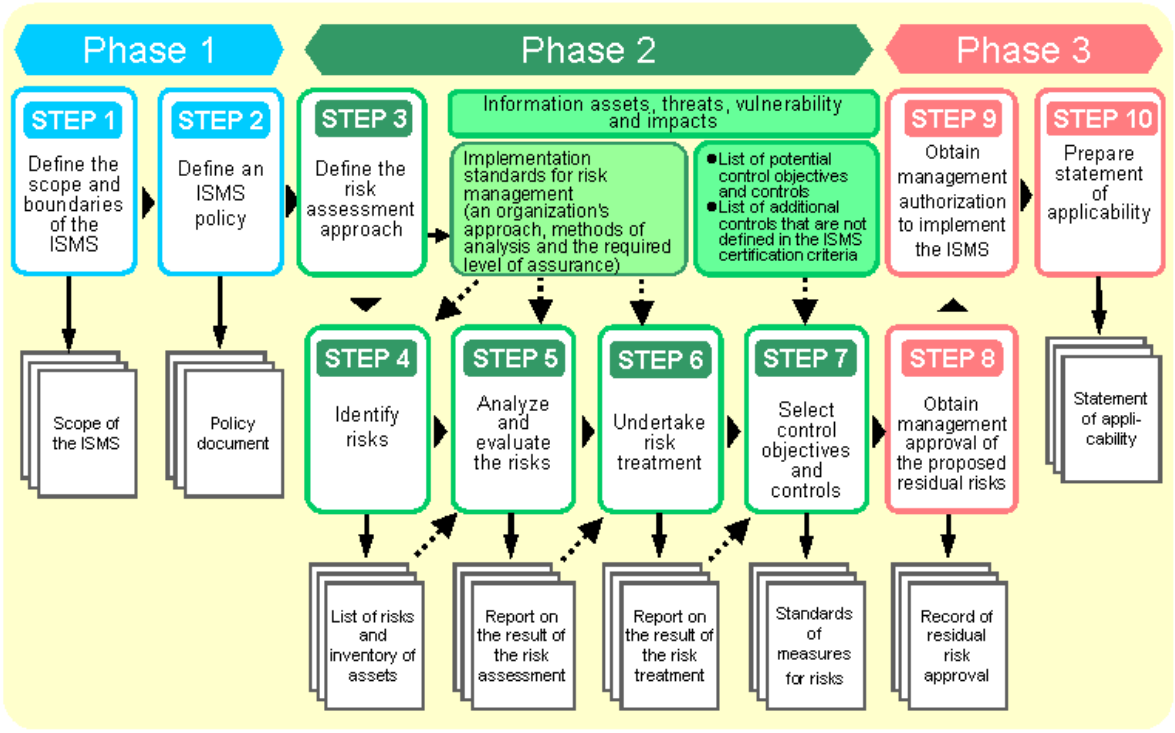

Figure 2: 3-Phase ISMS Process
(source: http://www.isms.jipdec.jp/en/isms/frame.html)

Shortcomings in ISMS

Selection and implementation of ISMS in an organization has many inbuilt complexities as well as limitations, some of which are studied and discussed herein below:

1. An ISMS is a set of policies, defined for information security measures in the organization, which are implemented through people and technology. The definition of the scope of these policies and hereby the scope of ISMS is a crucial step. Many organization choose too limited scope of ISMS to minimise its complexity, but in fact they also loss the effectiveness of it by doing so.
2. Focus of ISMS should be Information Security benefits to the organization. But many organizations implement ISMS with the focus of certifications and showing off to their customers. This diversion from core focus of ISMS leads to a big risk of loosening the effectiveness of ISMS.

3. Management must also understand that benefits never come free of charges. ISMS attract costs of implementation as well as maintenance. A proper planning and cost-benefit-ratio analysis would however give rational benefits.
4. Before depending on ISMS, an organization must understand that effectiveness and benefits of ISMS are very much dependent on people factors. It relies on awareness and interest of people or the organization in making the ISMS effective.
5. In many organizations, people hesitate to take responsibility of security due to fear of mistakes and failures. Management must understand that the changes never come overnight and it takes time in implementing and showing the effectiveness of ISMS in the organization. Proactive actions however give better results.
6. Awareness and training about ISMS policies, procedures, and benefits is the key of success of ISMS. It needs active participation of people of the organizations at all levels including from administration, housekeeping staff, executives, engineers, team leaders, managers, directors, and owners etc. the benefits of ISMS must be sold to and accepted by all participating people of the organization.
7. ISMS although is people driven, yet includes a complex technical system also. Selection of technology and technical systems for implementation of ISMS in the organization is a dominating factor in its success. This decision includes the analysis of cost, practical feasibility, technical feasibility, effectiveness, needs and benefit etc.
8. After implementation of the selected ISMS, another crucial thing is its assessment and improvement. ISMS Assessment criteria would in fact assess its effectiveness as well as the benefits gained from it. The assessment is expected to be comprehensive, well focused, and objective in nature. A comprehensive listing meticulously identifies assets most prone to security violations so that plans can be developed to mitigate risks occurring to them. It is essential for carrying out a thorough risk assessment. In studies, it has been surprisingly found that many organisations have not fully assessed the impact that external and internal threats can have on data protection while some have not even defined an acceptable level of risks that they can take should a security breach occur.
9. The frequency of Assessments and Audits is another crucial factor in effectiveness of ISMS. Too early audits will incur unnecessary costs and also will give less time for improvements. And too late assessments will give late results and the system may face risks of security breaches. An adequate frequency of the audits should be defend and complied as per the need and severity of the security system. Skipping of the audits on set frequency is another big risk to the effectiveness of ISMS.
10. Improving the ISMS as per the audit results is also very important. Delayed improvement means no improvement and timely improvement can mean to achievement to true benefits of ISMS. Many organizations lack in timely improvement in ISMS policies and technologies which in fact is a big risk to their information security.

Conclusion

ISMS is crucial for information security of an organization. ISMS is complex, incurs cost and efforts, takes time in giving results, and needs improvements in multiple cycles. ISMS is people driven and its success depends of participation of people and their awareness and interest in it. ISMS has its inbuilt complexities and shortcomings due to people and technology dependency. Timely actions and proactive approaches can give better results and lesser shortcomings of ISMS and improve information security in organizations.

References

i. Albert Caballero (2009), *Computer and Information Security Handbook*, Morgan Kaufmann Publications Elsevier Inc p. 232 ISBN 978-0-12-374354-1
ii. *An Introduction to BS7799*, DOI: http://gtechindia.org/jsp/BS7799TrivandrumSPIN.ppt
iii. Craig S Wright, SANS Darling Harbour (2005) *Implementing an Information Security Management System (ISMS) Training process*, Global Information Assurance Certification Paper taken from the GIAC directory of certified professionals, SANS Institute; DOI: http://www.giac.org/paper/g2700/39/implementing-information-security-management-system-isms-training-process/107335
iv. *History of 7799*, DOI: http://www.gammassl.co.uk/bs7799/history.html
v. Inger Nordin (2003), *Information Security Management System (ISMS) – Introduction*, DOI: http://www.ivpk.lt/dokumentai/prezentacijos/08%20Information%20Security%20Management%20System%20-%20Introduction.ppt
vi. Inger Nordin (2003), *Implementation of an ISMS - A process approach*, DOI: http://www.ivpk.lt/dokumentai/prezentacijos/09%20Information%20Security20Management%20System%20-%20Implementatio.ppt
vii. MAKINO Tsutomu (2012), *How to Establish an ISMS Management Framework*, JIPDEC , DOI: http://www.isms.jipdec.jp/en/isms/frame.html
viii. Shamsuddin Abdul Jalil, Rafidah Abdul Hamid (2003),*ISMS Pilot Program Experiences: Benefits, Challenges & Recommendations*, DOI: http://www.cybersecurity.my/data/content_files/11/23.pdf
ix. The National ICT Security and Emergency Response Centre (NISER) (2012), *NISER'S ISMS PILOT PROGRAMME EXPERIENCES: COMMON SHORTCOMINGS IN ISMS IMPLEMENTATION*, DOI: http://www.cybersecurity.my/data/content_files/11/24.pdf

Certificate of Recognition

This certificate is awarded to

Alpana Kakkar

in recognition of his / her contribution

"Implementation of ISMS and its Practical Shortcomings"

to Vol. 02, No. 01, 2012 *of*

IARS International Research Journal

08 FEB 2012

Editor in Chief

Certificate of Recognition

This certificate is awarded to

Ritu Punhani

in recognition of his / her contribution

"Implementation of ISMS and its Practical Shortcomings"

to **Vol. 02, No. 01, 2012** *of*

International Research Journal

08 FEB 2012

Editor in Chief