Volume-01, 2019

E-ISSN: 2582 – 7502
JS International Journal of Multidisciplinary Research (JSIJMR)
www.jconsortium.com/index.php/JSIJMR
www.jsu.edu.in

Practical Shortcoming in Implementation of Information Security Management Systems

*1Jain, Deepak, 2Kakkar, Alpana, 3Punhani, Ritu, 4S, Madan

*1Amity College, Florida, USA
2,3Amity University, Noida, India

ARTICLE DETAILS

Article History
Originally the manuscript is published in IARS' International Research Journal, Vol. 2 No.1 2012 with title "Implementation of ISMS and its Practical Shortcomings". IARS' International Research Journal is Double Blind Peer Reviewed International Journal publishing Multidisciplinary Research Articles since 2011 on Semiannual Frequency, having 7+ Impact Factor as per Citation data from Google-Scholars. The current version has been updated with the latest findings on the work and with appropriate permissions from IARS for using previous content.

Keywords
Information Security, ISMS, ISO27001

ABSTRACT

Information security has always been a global challenge and has gone even tougher with the revolutionary updates in technologies and easier reach to the information in digital form. Protection of vital information about business and persons (staff, vendors, and customers) has always been a big challenge for organizations from every market segment. Companies have been spending a big part of their revenue on ensuring information security and many international standards have been defined for this. Yet, the challenge is continuously increasing and so is the budget spent on it.

This white paper highlights some most practical shortcomings in the security systems common for multiple market segments.

1 Introduction

An information security management system (ISMS) is defined as a set of policies, procedures, formats, and guidelines focused towards the management of security of vital information of a business. The three basic components of Information Security are defined as 'CIA' of the information that stands for 'Confidentiality', 'Integrity', and 'Availability' of the information.

The governing principle behind ISMS is that any organization from any business segment manages a set of information that is vital for its existence in the market and is vital for its competitors or rivals to kill its business and hereby the organization is expected design, implement and maintain a coherent set of policies, processes, and guidelines in its management systems to manage, minimize, and control the risks confidentiality, integrity, and availability of its data assets, and herby ensuring acceptable levels of security risks to its information resources.

2 Explaining CIA

2.1 Confidentiality

The property that information is not made available or disclosed to unauthorized individuals, entities, or processes is called confidentiality of information.

2.2 Integrity

The property of safeguarding the accuracy and completeness of assets is meant to integrity of information.

2.3 Availability

The property of being accessible and usable upon demand by an authorized entity is termed as availability of information.

3 ISMS Life Cycle

ISMS is never a one-time effort or investment, rather this is a continuous effort and a life cycle including planning, implementation, assessment, and improvement. The ISMS Lifecycle has been explained briefly in Figure-1.

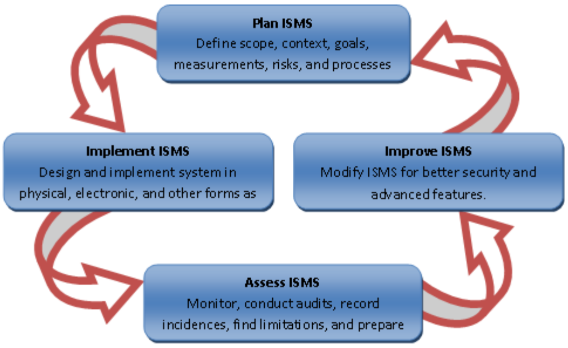
Plan ISMS
Define scope, context, goals, measurements, risks, and processes
Implement ISMS
Design and implement system in physical, electronic, and other forms as
Improve ISMS
Modify ISMS for better security and advanced features.
Assess ISMS
Monitor, conduct audits, record incidences, find limitations, and prepare

Figure 1: ISMS Life Cycle

4 Practical Shortcomings of ISMS

Selection and implementation of an Information Security Management System in an organization can have multiple inbuilt complexities as well as limitations. Based on the limitations of financial supports, infrastructure, human resources, nature of work, geographical location, political environment, and many more factors that influence the nature, vitality, and distribution of information, the organization can have different levels of risks to different information.

During this research, based on different factors, multiple practical limitations of ISMS in different organizations and market segments have been observed and noted, some of which are studied and discussed herein further.

4.1 Shortcoming in Focus of ISMS

Focus of ISMS should be securing the vital business Information from its misuse and organizations must align their policies and procedures towards the same goal. But many organizations have been found to be focused on respective Standard Certifications (like ISO27001, PCI-DSS, GDPR, etc.) and in a focus of certification, they usually loose the core focus of their ISMS mainly due to lost focus in identification of vital information.

4.2 Shortcoming in Scoping ISMS

Information Security Management System (ISMS) is a set of policies, procedures, formats, and guidelines defined for ensuring security measures for vital information of the organization. These systems are implemented through people and technology resources of the organization. The definition of the scope of these policies and hereby the scope of ISMS is crucial for success of ISMS in an organization. Many organizations are found to choose a too limited scope of ISMS to minimize its complexity, but in fact they neglect the effectiveness of it by doing so. Many organizations are found to choose on selective departments which are only customer facing, and other supporting departments are kept out from scope. This is to be understood that Information Security is like a Chain, that can be considered only as strong as its weakest link.

4.3 Shortcoming of Management Commitment

ISMS demands a commitment of top management of the organization towards information security and effectiveness of ISMS in the organization. The Management needs to accept that benefits never come free of charges. ISMS attract costs of implementation as well as maintenance. Investment of resources and efforts is required for ISMS infrastructure. Appropriate planning and cost-benefit-ratio analysis would however give rational benefits.

4.4 Shortcoming of People Commitment

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.

In many organizations, people can be seen hesitating to take responsibility of security due to fear of mistakes and failures. A supporting environment from senior management can help in improving this scenario.

Shamsuddin Abdul Jalil and Rafidah Abdul Hamid mention in their research 'ISMS Pilot Program Experiences: Benefits, Challenges & Recommendations' (source https://www.cybersecurity.my/data/content_files/11/23.pdf) that fear and resistance to changes in organizational procedures is one of the major shortcomings in effectiveness of ISMS of an organization.

Although, the awareness trainings about ISMS can help in improving the things and encouraging people to come forward for initiatives towards strengthening ISMS. Regular ISMS Training needs active participation of people at all levels and departments of the organization including from administration, housekeeping staff, executives, engineers, team leaders, managers, directors, and owners etc.

4.5 Other Common Shortcomings

In different other studies, many generic level shortcomings have been observed by the ISMS Internal Auditors and External Subject Matter Experts while performing audits in multiple organizations.

Increased cost of implementation of an effective ISMS due to increased complexities of information systems, and easier reach to digital data on internet. Allocation of adequate budget for the same is a practical challenge for finance.

Knowledge and expert guidance about effective process of implementation of ISMS is another common shortcoming. PDCA (Plan Do Check Analyze) seems to be very common approach but its effective implementation with the required focus is one of the commonly observed shortcomings.

5 Conclusion

ISMS is crucial for information security of any organization in any business segment. ISMS is complex, incurs cost and efforts, demands commitments, takes time in giving results, and needs improvements in multiple cycles. There are no debates about benefits of ISMS for any organization, but its effectiveness is people driven and needs continuous commitment from top management till last level of workforce.

6 Acknowledgement

All rights of republishing have been received from IARS-Researth/Curie (IARS' International Research Journal, published by International Association of Research Scholars). Amity College – Florida has provided guidance for editing of content along with the efficient team of IARS' Press, Australia. Other references have been acknowledged in the text of the paper.

7 References

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

[2]. An Introduction to BS7799, DOI: http://gtechindia.org/jsp/BS7799TrivandrumSPIN.ppt

[3]. 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

[4]. Inger Nordin (2003). "Implementation of an ISMS - A process approach". URL: http://www.ivpk.lt/dokumentai/prezentacijos/09%20Information%20Security20Management%20System%20-%20Implementatio.ppt

[5]. Inger Nordin (2003). "Information Security Management System (ISMS) – Introduction". URL: http://www.ivpk.lt/dokumentai/prezentacijos/08%20Information%20Security%20Management%20System%20-%20Introduction.ppt

[6]. Shamsuddin Abdul Jalil and Rafidah Abdul Hamid (2019). Cyber Security Malaysia. URL: https://www.cybersecurity.my/data/content_files/11/23.pdf

[7]. MAKINO Tsutomu (2012), How to Establish an ISMS Management Framework, JIPDEC, DOI: http://www.isms.jipdec.jp/en/isms/frame.html

[8]. Punhani, R., Kakkar, A., & Jain, D. (2012). Implementation of ISMS and its Practical Shortcomings. IARS' International Research Journal, 2(1). Retrieved from https://researth.iars.info/index.php/curie/article/view/19

[9]. Rana, A., Nigam, U., & Jain, D. (2012). Insider Threats: Risk to Organization. IARS' International Research Journal, 2(1). Retrieved from https://researth.iars.info/index.php/curie/article/view/18

[10]. 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

[11]. 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