International Journal of Engineering Sciences Paradigms and Researches (IJESPR)
(Vol. 41, Issue 01) and (Publishing Month: April 2017)
(An Indexed, Referred and Impact Factor Journal)
ISSN (Online): 2319-6564
www.ijesonline.com

Information Security Management System (ISMS) Implementation Challenges

Ammar Hajo Mohamed[1], Bashier Suliman Elbashier[2], Mwada El-tahir Alsubki[3] and Huwaida Tagelsir Ibrahim Elshoush[4]

[1]ammarhajo05@gmail.com, [2]bashiersuliman@gmail.com, [3]mwdaalsubki@yahoo.com and [4]hetlshoush@uofk.edu
Khartoum University, Sudan

Publishing Date: April 03, 2017

Abstract

The information security became very important issue for all types of companies and individuals for many years. ISMS (information security management system) needs to be enforcing to guarantee the security for companies or people information's and transactions. The implementation process may face many challenges that can prevent ISMS providing the main security roles CIA (confidentiality, integrity, availability) of information to those companies or people. Companies offered great effort, time and money to assure that their data is secured**.** So this paper would focus on the challenges and propose new ways to accommodate those challenges. In addition to negotiation of some ISO rules in information security.

Keywords: *Risk Assessment, Security Management, ISMS.*

1. Introduction

ISMS is a set of policies concerned with the management of information security of information crucial in business success. The governing principle behind ISMS is that the organization should design, implement and guarantee coherent set of rules, policies, principles, processes and systems to manage and control risks to its data assets, and ensuring acceptable levels of security risks to its information resources [8].The ISMS provides security by focusing in three main security areas ''CIA'' [9] as defined as follow:

Confidentiality: means that the information is not available for disclosures.

Integrity: the property that guarding against improper modification of information.

Availability: access of information is available for authorized users only.

The ISMS is never been completed, it always needs improvement in cyclic way to accommodate the new intruders, The ISMS is a quality management system, using the: plan – do – check – act [PDCA] cycle as illustrated in figure 1

- **Plan**

Establish strategy, policy, objectives, targets, processes and procedures to manage risk and improve cyber security in accordance with business needs, strategy, policies and objectives [4].

- **Do**

Identify and classify assets, conduct risk assessment, implement and operate controls to manage cyber security risks in a manner consistent with overall business risks [4].

- **Check**

Monitor and review the performance and effectiveness of the ISMS, using objective measurement [4].

- **Act**

Review outcomes and performance indicators or benchmarking findings, and act accordingly to continually improve the ISMS [4].

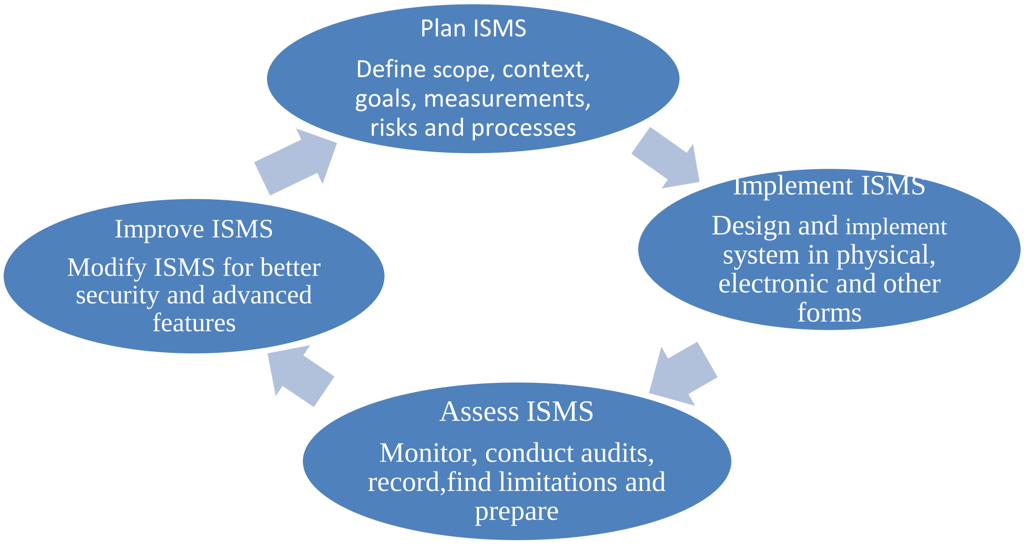
Plan ISMS
Define scope, context, goals, measurements, risks and processes
Implement ISMS
Design and implement system in physical, electronic and other forms
Assess ISMS
Monitor, conduct audits, record,find limitations and prepare
Improve ISMS
Modify ISMS for better security and advanced features

Figure 1: ISMS Life Cycle

ISMS must ensure business continuity and its plans are in place to counteract interruptions to business activities and to protect critical business processes from the effects of major incidence or disasters. These plans are subject to regular testing to validate their effectiveness [4].

2. ISMS Needs

- Due to increased numbers of security breaches and information leaks causes system lose the organizational concern to gain effective ISMS has increased.
- An ISMS provides an organization with mechanism to systematically manage risks to its information security. By establishing ISMS the organization can determine the necessary security levels, mitigation plans and distribute its assets based on its own assessments of associated risks.
- The most important need of ISMS in an organization is to manage risks to an information security and minimize the losses due to any breach or incidence.
- ISMS enforce organization to understand different levels of access requirements of information and relevancy of access by internal and external resources [8].

3. ISMS Challenges and Proposed Solutions

The challenges that faced ISMS must beconsidered seriously and taken under control to be solved; that helps the security specialist in organization to enforce the ISMS rules. In this section most of these challenges are negotiated and have been solved, as follows

[C: challenge, S: solution**]**

C: Lack of senior management's commitment [10]

S:Senior management in organization don't give high attention to implement ISMS and pay less interest to its practice, as security specialist, your major is to convince the top management about the importance of system and its advantages in protecting organization data and information.

When the organization implements ISMS, its benefits and percentage of advantage - (highlighted) - must be written in clear document and understandable way; this is to add more logic and influence.

C: Scope issues: insufficient, inaccurate, or even completely inappropriate, many organizations choose limited scope of ISMS to minimize its complexity [8].

S: The organization must determine sufficient, appropriateand accurate scope for implement ISMS (do not choose limited scope or inappropriate in order to reduce the challenges of implementation).

C: Awareness and expertise of employees: many organizations face the challenge of ensuring that all employees are aware of the applicable policies such as activating screensavers, firewalls, and virus detection systems, just to name a few [8].

S: Training the employees for ISMS and how to use security tools in an organization, when any additional tool is added to security system, you had to explain and train the employees for using this tool, to ensure proper use of that tool.

C: Implementation flaws: flaws such as open firewalls, routers with default passwords, deactivated security measures are quite often the result of a lack of awareness or expertise of employees [10].

S: Use high security restriction for tools to secure system such as password or biometric system for each employee and avoid use of default password (make sure that default account and passwords are switched off) [3].

C: No risk assessment: could result in spending resources in areas that are important, but ignoring those areas that are more important.

S: Use risk management process which is planned to present a standardized risk management process [10].

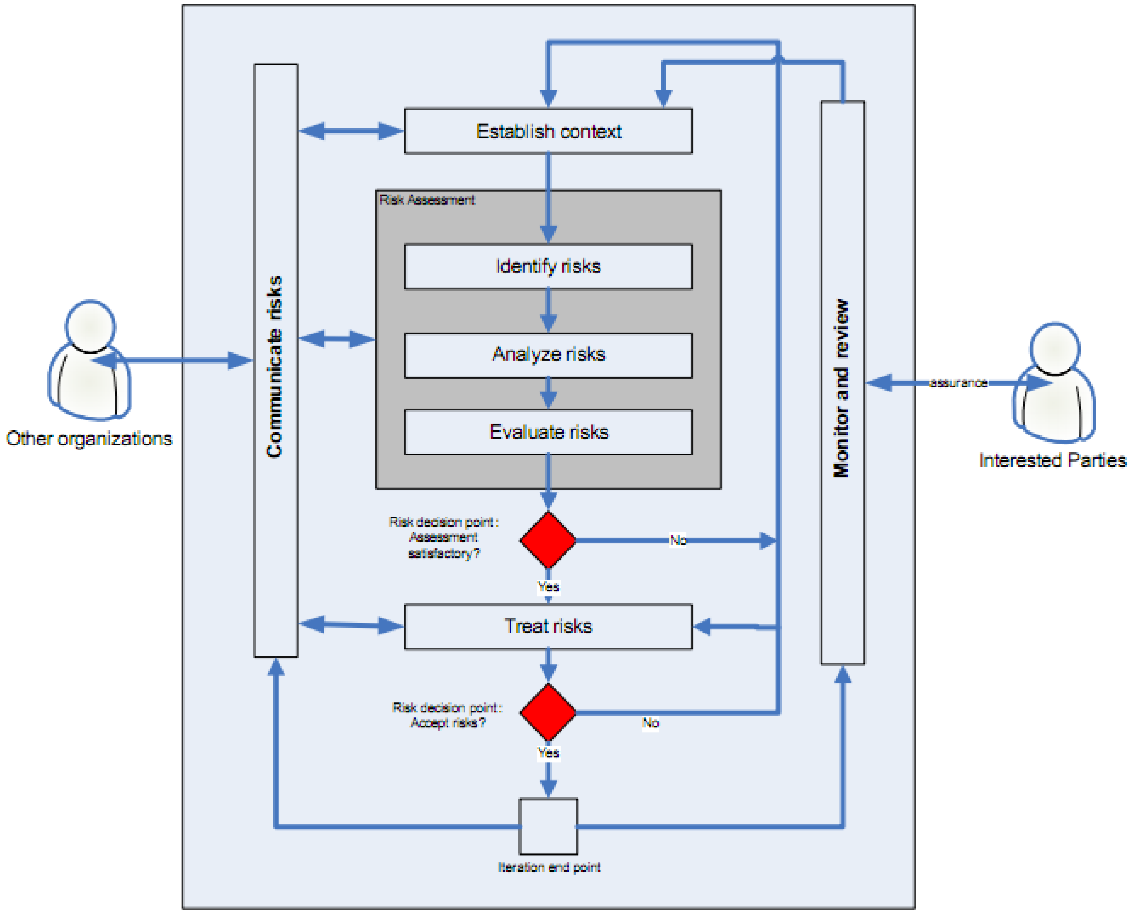

Figure 2: The Risk Management Process [6]

C: Insufficient resources: organizations are constantly in the process of allocating resources; the challenge for many organizations is the proper/correct allocation of resources [8].

S: Security specialists must ensuresufficient resources before starting implementing ISMS and allocation resources in proper way.

C: Inadequate, insufficient asset classification: many organizations are lacking the clear, concise classification of information (e.g. public, internal use only, confidential, secret, top secret). This leads to inconsistency in the implementation [8].

S: Classify the assets and information in a correct way (public, internal use only, restricted, confidential, secret, top secret) by security department.

'**Top secret**' applied to information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security [2].

'**Secret**' applied to information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security [2].

'**Confidential**' information has significant value for an organization, and unauthorized disclosure or dissemination could result in severe financial or reputational damage to organization.

‘**Restricted**’ information is subject to controls on access, such as only allowing valid logons from a small group of staff. Restricted information must be held in such a manner that prevents unauthorized access.

‘**Internal use**’ information can be disclosed or disseminated by its owner to appropriate members of an organization, partners and other individuals, as appropriate by information owners without any restrictions on content or time of publication.

‘**Public**’ information can be disclosed or disseminated without any restrictions on content, audience or time of publication [5].

C: Increased cost: by implementing ISMS, it will definitely cause an increase in the cost incurred especially when implementing the controls identified to mitigate the known risks [11].

S: Adequate budget to allocate the fund and/or resources to implement ISMS and ensure that the budget available in company account.

C: Inadequate knowledge as to approach: many organizations still do not have how on proper ISMS implementation and they may not have personnel who are qualified subject matter experts in the area. Thus this may lead to the delay or avoidance on the implementation [8].

S: When organization needs to implement ISMS, and does not have insufficient information about how to implement it. The organization lets this task to security specialists in it. If there are no security specialists in an organization, it may gain help from known person who is expert in security.

C: Fear of mistake: In many organizations, people hesitate to take responsibility of security due to fear of mistakes and failures [11].

S: When implement ISMS in the first time faces some errors and challenges, and in the act phase of the ISMS life cycle the errors are corrected. Person does not fear from any kind of mistakes occur when implement an ISMS.

C: 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 losing the effectiveness of the ISMS [10].

S: Focus of ISMS should be Information Security benefits to the organization.

4. ISO Certificate

An ISO 27001 based information security management system (ISMS) is a set of integrated processes that govern the management of security program policies and procedures.

It is a time-proven international standard of best practices published by the international organization for standardization (ISO) for establishing, maintaining, and improving security programs for all organizations.

The latest version of this standard was published in 2013, and its full title is now ISO/IEC 27001:2013. The first revision of the standard was published in 2005, and it was developed based on the British standard BS 7799-2. The current valid version is ISO/IEC 27001:2013 [1].

Following table [1] comparing between ISO 27001:2005 and ISO27001:2013

Table 1: Comparison between ISO 27001:2005 and ISO27001:2013

ISO 27001:2005	*ISO 27001:2013*
Structure The specification is spread across 5 clauses, which approach the ISMS from a managerial perspective. 1. Information security management system 2. Management responsibility 3. Internal ISMS audits 4. Management review of the ISMS 5. ISMS improvement	**Structure** The specification is spread across 7 clauses, which do not have to be followed in the order they are listed. 1. Context of the organisation 2. Leadership 3. Planning 4. Support 5. Operation 6. Performance evaluation 7. Improvement
Process The standard clearly states that it follows the PDCA (Plan-Do-Check-Act) model.	**Process** The standard does not specify any particular process model. The standard requires that a process of continual improvement is used.
Risk assessments The risk is the "combination of the probability of an event and its consequences". The organisation identifies risks against assets. The asset owner determines how to treat the risk, accepting residual risk.	**Risk assessments** The risk is the "effect of uncertainty on objectives", which may be positive or negative. Business and contractual obligations may be identified and implemented before the risk assessment is conducted.
Documentation The standard recognises two forms: documents and records. Documents include policies, procedures, process diagrams, etc. Records track work completed, audit schedules, etc.	**Documentation** The standard makes no distinction between documents and records. Documents and records are subject to the same control requirements.
Measuring effectiveness There is a requirement to define how to measure effectiveness of controls and how those measurements will be assessed. The organisations must identify their own measurement and monitoring regime in order to prove the efficacy of the ISMS.	**Measuring effectiveness** The standard requires a process for measuring effectiveness of the ISMS, its processes and controls. It specifies the requirements for measurement. The standard sets requirements for a process for defining the measurement and monitoring regime.
Certification ISMS can be certified by any accredited certification organisation. Certification against ISO 27001:2005 is likely to remain valid for up to 3 years, even after ISO 27001:2013 certification has begun.	**Certification** There is currently no accredited certification programme.

5. Benefits of Certification [1]

- Reduced operational risk.
- Increased business efficiency.
- Assurance that information security is being rationally applied.
- Security awareness amongst staff and managers.
- Certification can also be used as marketing initiative, assurance to business partners & clients.
- A valuable framework for resolving security issues.
- Enhancement of client confidence & perception of your organization.
- Enhancement of business partners' confidence & perception of your organization.

- Provides confidence that you have managed risk in your own security implementation.
- Enhancement of security awareness within an organization.
- Assists in the development of best practice.
- Can often be a deciding differentiator between competing organizations.

6. Conclusion

ISMS is important for information security of organizations. ISMS is complicated, sustains cost and pains. It takes very long time in giving desired result, and requires improvement in periodic way. ISMS is people driven and its implementation success depends on collaboration of people and their awareness, expertise and interest in it.ISMS has many implementation challenges and complexities. Proposed solutions for challenges can help to improve security of organization.

References

[1] https://www.iso.org/iso/home/standards/management-standards/iso27001.htm [accessed 5 march 2017].

[2] https://usmilitary.about.com/cs/generalinfo/a/security.htm[accessed 1 march 2017].

[3] H. T. Elshoush, Advanced Topics in Information Security, Department of Computer Science, University of Khartoum – Sudan, 2015.

[4] Government Framework on Cyber Security, Information Security Management Framework (ISMF), Government of South Australia, 2014, pp: 32-33.

[5] J. Perkins, Information Security - Information Classification, p.8, 2013.

[6] Amarachi A. A, Okolie S.O and A jaegbu. C, Information Security Management System: Emerging Issues and Prospect, p.5, 2013.

[7] IT Governance Ltd, Comparing ISO 27001:2005 to ISO 27001:2013, pp: 2-6, 2013.

[8] A. Kakkkar, R. Punhani, S. Madan, D. Jain, Implementation of ISMS and its practical shortcomings, International Research Journal, Vol.2, No.1, 2012, pp:3-6.

[9] W. Stallings, Cryptography and Network Security principles and Practice, 5th edition**,** Prentice Hall**,** 2011, p.11.

[10] F. Pattinson, Certifying Information Security Management Systems, 2007, pp: 3-10.

[11] S Jalil, Shamsuddin Abdul, and Rafidah Abdul Hamid. "ISMS Pilot Program Experiences: Benefits, Challenges & Recommendations." (2003).