Presentation a Framework to Increase Information Security in Organizations

Hamid Mehdi
Department of Computer, Andimeshk Branch, Islamic Azad University, Andimeshk, Iran
Hamidmehdi@gmail.com

Abstract
Nowadays, one of the most important problems in Variety organizations to maintenance and transmission information is security. The most of organization has tried to use from known standard to meet against different risks. One of the standard problems to use in organizations is standard complexity for using. Any standard has different steps to implement at organizations. Hence, some organizations do not try to implement information security standards. In This article it has been tried to present a new simple standard to implement in organizations that results show suitable performance and drop complexity.

Keywords: Information, framework, Security, Standard, ISO/IEC, MIQ

I. Introduction

There many different information security standards to decrease risk in organization or any places what information is important. For example, it can be mentioned:

- ISO/IEC 27000 — Information security management systems — Overview and vocabulary
- ISO/IEC 27001 — Information security management systems — Requirements. The older ISO/IEC 27001:2005 standard relied on the Plan-Do-Check-Act cycle; the newer ISO/IEC 27001:2013 does not, but has been updated in other ways to reflect changes in technologies and in how organizations manage information.
- ISO/IEC 27002 — Code of practice for information security management
- ISO/IEC 27003 — Information security management system implementation guidance
- ISO/IEC 27004 — Information security management — Measurement

Any standards have some problems (Siponen et al, 2009) and way to execution which this point causes some organizations (Veiga, 2007) search standards and thy find easy standard to implement. Standards can protect information against danger (Sowa et al, 2009) and can safe transmission. Also standards can safeguard employees and all resource at organization. These factors cause organization go to implement standard to decrease information security. So some standards has been tried to improve them solve to increase performance (Savola,2007)(Humphreys,2007)
II. ISO/IEC 27001:2005


The standard contains 11 domains:

1- Security policy - management direction
2- Organization of information security - governance of information security
3- Asset management - inventory and classification of information assets
4- Human resources security - security aspects for employees joining, moving and leaving an organization.
5- Physical and environmental security - protection of the computer facilities
6- Communications and operations management - management of technical security controls in systems and networks
7- Access control - restriction of access rights to networks, systems, applications, functions and data
8- Information systems acquisition, development and maintenance - building security into applications
9- Information security incident management - anticipating and responding appropriately to information security breaches
10- Business continuity management - protecting, maintaining and recovering business-critical processes and systems
11- Compliance - ensuring conformance with information security policies, standards, laws and regulations

Most organizations have a number of information security controls. However, without an information security management system (ISMS), controls tend to be somewhat disorganized and disjointed, having been implemented often as point solutions to specific situations or simply as a matter of convention. Security controls in operation typically address certain aspects of IT or data security specifically; leaving non-IT information assets (such as paperwork and proprietary knowledge) less protected on the whole. Moreover business continuity planning and physical security may be managed quite independently of IT or information security while Human Resources practices may make little reference to the need
to define and assign information security roles and responsibilities throughout the organization.
III. The PDCA Cycle

![PDCA Cycle](image.png)

Figure 1. The PDCA Cycle

The 27001:2005 adopts the process model “Plan-Do-Check-Act” (PDCA) which is applied to the structure of all the processes in ISMS.

Plan:
Establish the policy, the ISMS objectives, processes and procedures related to risk management and the improvement of information security to provide results in line with the global policies and objectives of the organization.

Do:
Implement and exploit the ISMS policy, controls, processes and procedures.

Check:
Assess and, if applicable, measure the performances of the processes against the policy, objectives and practical experience and report results to management for review.

Act:
Undertake corrective and preventive actions, on the basis of the results of the ISMS internal audit and management review, or other relevant information to continually improve the said system.

IV. Proposed framework

One of the most implementation problems is complexity in separating task for every part. In this article we presented a novel way to separate in order to decrease implementation of complicity. Table I shows standard detailed which it has been called MIQ. In this manner we divided three parts: Implementation, management, QoS. The first phase; management includes Security policy, Organization of information security, Asset management and Information security incident management. In this part it has been tried to gather all action related to management.

The second phase is implementation which this part includes: Human resources security, Physical and environmental security, Communications and operations management, Access control and Information systems acquisition. In this part it has been tried to gather action related to standard implementation. Also the third phase is QoS. This part includes Business continuity management and Compliance which it has been tried to assess quality of service about implementation by standard checking.
The main gold from classification of standard decreases execution complexity. When many of organizations want to implement a standard they have to analyze standards and then decide to implement a standard. Now, this standard did that time they need to analyze and define any parts. So, they need just implementation.

### TABLE I
**MIQ STANDARDS PARTS**

| Security Management | 1- Security policy - management direction  
|                     | 2- Organization of information security - governance of information security  
|                     | 3- Asset management - inventory and classification of information assets  
|                     | 4- Information security incident management - anticipating and responding appropriately to information security breaches  
| Implementation      | 1- Human resources security - security aspects for employees joining, moving and leaving an organization.  
|                     | 2- Physical and environmental security - protection of the computer facilities  
|                     | 3- Communications and operations management - management of technical security controls in systems and networks  
|                     | 4- Access control - restriction of access rights to networks, systems, applications, functions and data  
|                     | 5- Information systems acquisition, development and maintenance - building security into applications  
| QOS                 | 1- Business continuity management - protecting, maintaining and recovering business-critical processes and systems  
|                     | 2- Compliance - ensuring conformance with information security policies, standards, laws and regulations  

Also, it can be seen in figure 1 to execution sequence.

![MIQ Standard Diagram]

**Figure 1. MIQ Standard**

V. **Conclusion**

Nowadays, we live in the world that information faces to different dangers, robberies, misuses, etc. One of the most important methods to prevention these dangers is information security. This is important that any organizations must have a information security standard so that they become sure from information when transferring.

In this paper it has been tried to present a novel standard according to existing standard to decrease execution complexity. This standard is quick and easy in execution, which all of organizations can use them easily and they increase information security.

**Acknowledgement**

This research was supported by the Islamic Azad University, Andimeshk Branch.

**References**


iii. Poole, Vernon.(2007).information security management and IT audit/why the emerging ISO 27000 series are vital for business resilience.


