Information Security Management System

Sahar Al-Dhahri
King Abdulaziz University
Collage of Computing and Information Technology
Saudi Arabia

Manar Al-Sarti
King Abdulaziz University
Collage of Computing and Information Technology
Saudi Arabia

Azrilah Abdul Aziz, PhD
King Abdulaziz University
Collage of Computing and Information Technology
Saudi Arabia

ABSTRACT
The ISO27001 is an information security management system (ISMS). It is helps the organizations to manage the security of assets. However, the ISO27001 is the best-known standard providing requirements for an information security management system (ISMS). In 2015, based on ISO survey, ISO/IEC 27001 saw a 20% increase to 27,536 certificates worldwide [13]

Keywords
Information Security, Information Security Management, Total quality management, Information security, Incremental approach

1. INTRODUCTION
Information Security determines as the process of protecting information and information assets, to preserving confidentiality, integrity, and availability of information (ISO17799, 2004). It is a major issue for businesses, their clients and the public. From 1997 to 2001, U.S. organizations spent over $2.5 trillion on information technology, nearly double the amount than the previous five years. According to the paper the personal information has four dimensions (Sinha and Gillies, 2011):

1. Operational value: personal information is a sensitive asset for the organization and needs to be preserved to ensure it is safe**.**
2. Individual value: using people's personal data leads to important risks, so information need to be handle with care, and respect people's privacy.
3. Value to others: when an organization undermined a legitimate purpose to use the personal information of the users, it should being handled according to the data protection principles. On other case, it could harm the people and embarrassment the organization.
4. Societal value: Society legislates give the right to privacy a legislative basis such as the EU directive 95/46/EC7, (European Parliament, 1995) enshrined in UK law as the Data Protection Act (1998), and alternative legislation outside the EU.

2. TOTAL QUALITY MANAGEMENT
The current management systems are derived from the work of W. Edwards Demming and the related world of Total Quality Management (TQM). Although it initially considers relevant only to a production environment, the concepts have been successfully applied to many other environments include organization's security (Carlson et al., 2008).The integration between TQM "Deming's 14 points" and organizations security directly affect the success or lack of the organization's security

2.1 Risk Management
Risk management defined as "the process of identifying vulnerabilities and threats within the framework of an organization, as well as producing some measurements to minimize their impact over the informational resources".
According to Pavlov and Karakaneva (2011]) is the combination of activities which aim to protect the organization assets cost effectively based on the organization's missions or objectives. Risk management contains two processes:

1. Risk Analysis: is the process of identifying the influence factors over the information security.
2. Risk Assessment has four main outcomes:
   a) Determine the threats;
   b) Prioritization of these threats according to the risk levels;
   c) Define controls and protection measures;
   d) Development plan for these measures implementation.

2.2 Information Security Components
According to Hong et al., (2003) the components for any information security architecture are:

1. Organization and infrastructure security
2. Policy, standards and procedures security
3. Baselines and risk assessments security
4. Awareness and training program security
5. Compliance security Fomin et al.,(2008) addressed the low adoption for the international standard ISO/IEC 2700 on information security management especially in academia field. The basic barriers to standard's adoption are high cost on money and time.

2.3 Information Security Incidents
1. Vulnerability: is a weakness of one or more assets which may attacked by a threat.
2. Threats: is a potential unwanted incident that may harm to a system or organization**.**

3. INFORMATION SECURITY MANAGEMENT SYSTEM
Information Security Management System include (Carlson et al., 2008):

a. Risk management: based upon metrics of confidentiality, integrity, and availability.

b. TQM applied: based upon metrics of efficiency and effectiveness.

c. A monitoring and reporting model: based upon abstraction layers.

d. A structured approach: contains people, process, and technology.

e. An extensible framework from which to manage information security compliance.

Information Security Management System provide requirements for establishing, implementing, maintaining and improving an information security management system. This adoption is a strategic decision for an organization which influenced by the organization's needs and objectives, security requirements and scaled based on the organization's needs. The information security management system is applying a risk management process to protect the confidentiality, integrity, and availability of information. ISMS can be used by internal and external parties and describes by ISO/IEC 27000. It provides a catalog of controls that can be implemented for ISMS.

3.1 Information Security Management System Components

ISMS involves the following essential components (see Figure 1):

a. Management principles

b. Resources

c. Personnel

d. Information security process

Fig 1: Information Security Management System Components (Source: http: //www. isaca.org)

3.2 Information Security Management System Domains

The Information Security Management System standard comprises of 11 security areas, 39 controls objectives, and 133 controls**.** Following Table is a list of the Domains and Control Objectives [15]:

Table 1: Information Security Management System Domains

Domains	Objective
Security policy	Provide management direction and support for information security
Organizational Security	Manage information security within the organization.
Asset Management	Achieve and maintain appropriate protection of organizational assets.
Human Resources	Details any personnel issues like training, responsibilities, and how employees responded to security incidents.
Physical and Environmental Security	prevent unauthorized physical access
Communications and Operations Management	Ensure the correct and secure operation of information processing facilities.
Access Control	To control access to information.
Information System Acquisition, Development & Maintenance	Ensure that security is an integral part of information systems.
Information Security Incident Management	Ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.
Business Continuity Management	Maintenance of essential business activities during adverse conditions, from coping with major disasters to minor, local issues
Compliance	Avoid breaches of any security requirements.

3.3 ISO/IEC 27001

In 1987, the ISO 9000 standards were first published, then revised in 1994 and 2000 (ISO, 2000). Therewith, ISO introduced the management system standards (MSS), for example, the ISO 14001 Environmental Management System (EMS), and the ISO/IEC 27001 Information Security Management (ISMS) standards. The three management system standards similar to each other (Fomin et al., 2008). ISO/IEC 27001 developed to protect the organizations' information assets, "the 'life-blood' of all businesses" (Humphreys, 2005). ISO/IEC 27001 introduces the "Plan-Do-Check-Act" (PDCA) model which aims to establish, implement, monitor and improve the effectiveness of an organization's ISMS. The PDCA has four phases as shown in

Fig 2: The ISMS Plan-Do-Check-Act cycle (Al-Ahmad Mohammad, 2013)

1. Plan: establish security policy, objectives, processes and procedures to managing risk and improving information security
2. Do: implement and operate the security policy, controls, processes and procedures.
3. Check: monitor and measure process performance against security policy, objectives and practical experience
4. Act: maintaining and improving based on the results of the management review, to achieve continual improvement of the ISMS

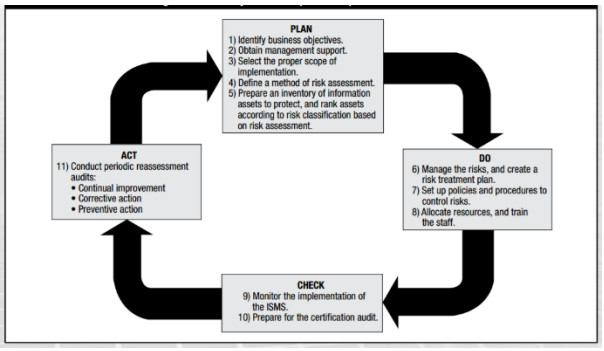

Fig 2: The ISMS Plan-Do-Check-Act cycle (Source: http: //www. isaca.org)

3.4 The ISO27001 STANDARD

The International Organization for Standardization (ISO) has declared standards for information security management systems (ISMS) including the standard ISO/IEC 27001 "Information Technology - Security Techniques - Information Security Management Systems - Requirements" (ISO, 2005a).There is no one way that can guarantee 100% of information security, but the ISO 27000 has many of standards to decide which an information security management system (ISMS) can be certificated (Sinha and Gillies, 2011). These standards are (see Table 2):

Table 2: The ISO27001 STANDARD

Year	Standards
1989	UK DTI publish a users' code of practice for information security
1993	BS PD 003: A code of practice for information security management
1995	BS7799-1 A code of practice evolved from BS PD003
1998	BS7799-2 A certification standard for an information security management system.
1999	BS7799-1 and BS7799-2 aligned: the subsequent ISO17799 and ISO27002 standards are based on this version of BS7799-1.
2002	BS7799-2 is modified to incorporate the Plan-Do-Check-Act cycle, in order to align it with ISO9001. This version formed the basis for the subsequent ISO27001 release in 2005
2005	ISO code of practice published for information security management as ISO17799 (June).
2005	ISO certification standard for an information security management system published as ISO27001 (October).
2007	ISO17799 renumbered to ISO27002: note that the 1 and 2 numbering is now reversed when compared with BS7799.

The total number of certified organizations worldwide for ISO/IEC 27001 is now 27, 536 increasing of 20% over 2014 (Fig 3: ISO/IEC 27001 Certification Worldwide). While the information technology sector dominates the certification list, with 40% of certified organizations being in that business area.

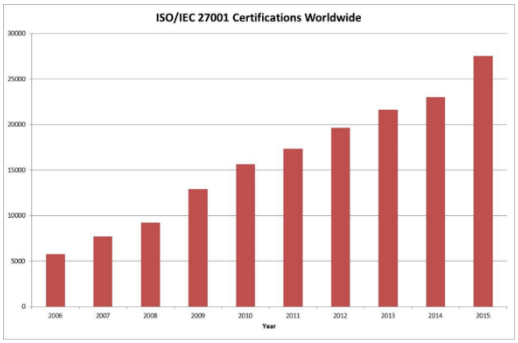

Fig 3: ISO/IEC 27001 Certification Worldwide (Source: http: //www. certikit.com)

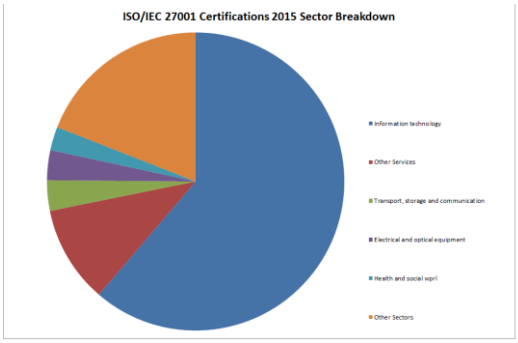

Fig 4: ISO/IEC 27001 Certification Sectors (Source: http: //www. certikit.com)

4. BENEFITS OF ISO27001

The ISO27001 helps the organizations to manage the security of assets. However, the ISO27001 is the best-known standard providing requirements for an information security management system (ISMS)

1. Increased business efficiency
2. Reduced operational risk
3. Ensure that information security is rationally applied
4. Assurance to business partners & clients via certification which used as a marketing initiative
5. Security awareness amongst employees and managers

Figure 5: BENEFITS OF ISO27001 (Source: http://www. .bsigroup.com.eu)

5. INFORMATION SECURITY MANAGEMENT SYSTEM FRAMEWORK

The information security management system (ISO 27001, 2005) is an integral part of the organization's management system and business culture. This system contains the organization structures, planning, politics, processes, and resources. In ISMS development include six steps (see Fig 6: Information Security Management System Developing Process (Source: **http://www.enisa.europa.eu**):

1. Define the Security Policy
2. Define the ISMS Scope
3. Risk Assessment
4. Risk Management
5. Select the Appropriate Controls
6. Statement of Applicability

In steps 3 and 4, the Risk Assessment and Management process, frame the core of the ISMS. The two processes transform the guidelines of security policy and the objectives of ISMS into particular plans to decrease the threats and vulnerabilities. However, steps 5 and 6 related to the operative actions for technical implementation, maintenance, and control of security measurements. Appropriate controls are derived from existing sets of controls or mechanisms for information security standards

5.1 Risk Management Processes

This process of the risk management includes five processes:

1. Risk Assessment: covering of three steps: risk identification, risk analysis, and risk evaluation to understand the impact of the risk and decide the best measures to face them.
2. Risk Treatment is the selecting and implementing of measures to modify risk. Risk treatment measures include avoiding, optimizing, transferring or retaining risk.
3. Monitor and Review are measuring the efficiency and effectiveness of the risk management of the organization processes.
4. Risks Communication a process to exchange information about risk between the decision-maker and other stakeholders inside and outside an organization.
5. Risk acceptance is the decision to accept a risk by the responsible management of the organization. the options are:
    a. reduce: lower the risk
    b. transfer: offload the risk by placing it on other entity
    c. accept: the risk is acceptable based on the benefit;
    d. ignore: choose not to reduce, transfer or accept the risk - this is equivalent to accepting the risk

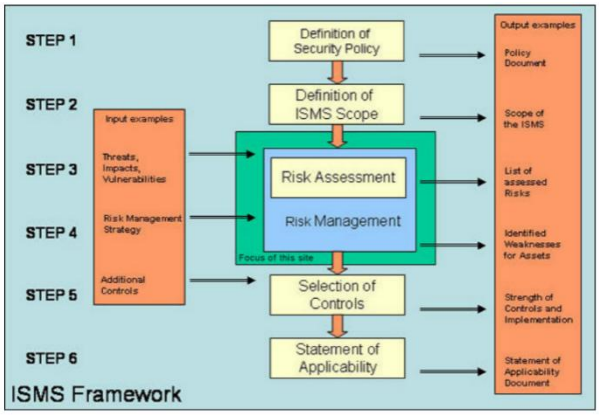

Fig 6: Information Security Management System Developing Process (Source: http://www.enisa.europa.eu)

5.2 Risk Assessments Challenges

According to Al-Ahmad Mohammad (2013) the challenges to Information Security Risk Assessments:

1. Absence of senior management commitment & support
2. Absence of appropriate policies for information security risk management
3. Disintegrated GRC efforts
4. Improper assessments management
5. Assets ownership is either undefined or unpracticed
6. Limitations of existing automated solutions
7. Existence of several IT risk assessment frameworks

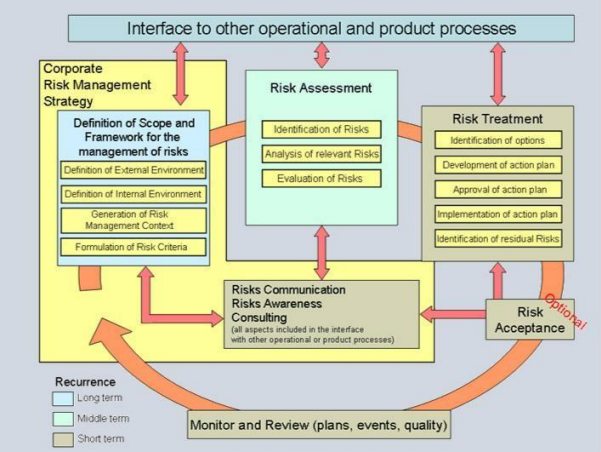

Fig 7: Risk Management Process (Source: http://www.enisa.europa.eu)

6. INFORMATION SECURITY MANAGEMENT SYSTEM CHALLENGES

We have already examined the primary risk assessment challenges in an organization. Here we will explore the challenges related to nature of the Information Security Management (Ashenden, 2008):

1. Structural, process and boundary challenges
   The 21st century forces the Information Security management to face the runny business environment. There are hard boundaries that are breaking down the Information Security such as (geographical, physical and logical)
2. The human challenge
   Hackers spend time to discover vulnerabilities more than Information Security practitioners, and humans are difficult to manage in the context of Information Security
3. Changing Organizational Culture
   We need to have a better understanding of the social aspects of the organization's security; especially the human element. Unluckily, humans are not machines. We do not get the same information is input and processed in the same way then the result that is output will be the same time after time.

7. ACKNOWLEDGMENTS

We would like to express our sincere thanks and gratitude to our supervisor Dr. Azrilah AbdulAziz who has helped us on this work.

8. REFERENCES

[1] ENISA (European Network and Information Security Agency), "Risk Management /Risk Assessment " (available on-line at http://www.enisa.europa.eu/rmra)

[2] Walid Al-Ahmad and Bassil Mohammad. Addressing information security risks by adopting standards. International Journal of Information Security Science, 2(2):28_43, 2013.

[3] Tom Carlson, HF Tipton, and M Krause. Understanding Information Security Management Systems. Auerbach Publications Boca Raton, FL, 2008.

[4] Vladislav V Fomin, H Vries, and Y Barlette. Iso/iec 27001 information systems security management standard: exploring the reasons for low adoption. In Proceedings of The third European Conference on Management of Technology (EUROMOT), 2008.

[5] Kwo-Shing Hong, Yen-Ping Chi, Louis R Chao, and Jih-Hsing Tang. An integrated system theory of information security management. Information Management & Computer Security, 11(5):243_248, 2003.

[6] Ted Humphreys. State-of-the-art information security management systems with iso/iec 27001: 2005. ISO Management Systems, 6(1), 2006.

[7] G Pavlov and J Karakaneva. Information security management system in organization. Trakia Journal of Sciences, 9(4):20_25, 2011.

[8] Madhav Sinha and Alan Gillies. Improving the quality of information security management systems with iso27000. The TQM Journal, 23(4):367_376, 2011.

[9] The ISO Survey of Management System Standard Certi_cations 2015 http://www.iso.org/iso/the_iso_survey_of_management_system_standard_certi_cations_2015.pdf (Accessed: 11 December 2016).

[10] ISO/IEC 17799 (2005) _Information technology - Security techniques - Code of practice for information security management_.

[11] ISO/IEC 27001(2005) _Information technology - Security techniques - Information security management systems _ Requirements_.

[12] Debi Ashenden. Information security management: A human challenge? Information security technical report, 13(4):195_201, 2008.

[13] I. (n.d.). The ISO Survey of Management System Standard Certifications 2015. Retrieved December 2, 2016, from http://www.iso.org/iso/the_iso_survey_of_management_system_standard_certifications_2015.pdf

[14] S. (n.d.). Security Incident Management. Retrieved December 10, 2016, fromhttps://ito.hkbu.edu.hk/pub/is_newsletter/professional/Issue_12_SecurityIncidentMgt/IssueIT12_1.htm

[15] Information Security Management System ISO 27001:2005. (2015). Retrieved December 2, 2016, from http://www.tuv-nord.com/, http://www.tuv-nord.com/cps/rde/xbcr/tng_in/Product_Information_27001.pdf