DIAGNOSING THE CURRENT INFORMATION SYSTEMS SECURITY DEPARTMENT IN THE INFORMATION TECHNOLOGY DEPARTMENT ACCORDING TO THE INTERNATIONAL STANDARD (ISO / IEC 27001: 2013)

Nagham Ali Jassim, Al-Mustansiriya University
Basmal Abdel Moneim Al-Zahir, Officer at the Ministry of Interior
A Hamad Makki Khazraji, Director of the Department of Total Quality Management and Institutional Development

ABSTRACT

IT systems and networks of information are vulnerable to threats resulting from the breach or attempt to obtain data or reports, records and files that contain the information, which is available to persons, designated in the Ministry of the Interior. This is because of its inherent specificity associated with work and the concern of the attempted destruction by the authorities that aim to misuse the information. The importance of research stems from the importance of the application of the standard because the information protection means the protection of the human resource in the Ministry of the Interior and protects all those who are working on this information. It also protects them from loss and damage and access to it to get benefits from it by any person whose aim is to disrupt the order or sabotage. Thus, it is required to manage it with the best methods of protection adopted globally. The research aims to diagnose the gap between the information security system in the department according to the international standard ("ISO / IEC 27001 ", 2013). It also aims to identify the gap using Likert Sibai scale. The size of the gap has reached the largest gap in the size of the requirement of leadership represented by about 49% and matching 51% due to lack of establishment of information security policy in the section.

Keywords: Information Systems, Technology

INTRODUCTION

The developments in the information continuously and steadily change working methods. It became the process of transmission of information across local and international networks and computers of routine matters. It is one of the features of the current. Despite its clarity in facilitating business requirements and developing methods, it maintains the confidentiality and the integrity of information security demand. Whatever they run, may be vulnerable to penetration and leakage. So this technology is double - edged sword. Thus, the organization aims to protect it, so we dealt, in this research, with evaluation system of information security in the IT department in the Interior Ministry, according to International standard("ISO / IEC 27001 ", 2013). The researchers used a checklist according to Likert's scale of seven items to identify the gap and then determine the strengths and weaknesses of the application to reach the most important conclusions and recommendations.

METHODOLOGY

First: The Problem of Research

Citation Information: Jassim, N.A., Al-Zahir, B.A.M., & Khazraji, A.H.M. (2022). Diagnosing the current information systems security department in the information technology department according to the international standard (ISO / IEC 27001: 2013). *Journal of Management Information and Decision Sciences, 25*(S2), 1-7.

It has become a necessity to adopt regulations for the protection of information in the Department of Information Technology in the Ministry of Interior because of the danger and threat to the human resources. It is also poses a threat to all those who work on this information. Thus, protecting it from accessible from other parties aimed at sabotage and keeping the confidentiality and integrity of information security provide a means of protection for those who work on it. Thus, the researchers aim to show the importance of the application of the system of information security management in accordance with the international standard ("ISO / IEC 27001 ", 2013). Also, the ministry aims to implement it. Accordingly, the problem can be expressed by formulating the following question: -

What is the size of the gap for the system of information security management in the IT Department of Information, Ministry of the Interior and Information Security Management System in accordance with the standard ("ISO / IEC 27001 ", 2013)? Also, what is the importance of evaluating it performance to improve it ?.

Second: The Importance of Research

The work is an attempt to link the actual reality of the information security management system in the Information Technology Department - Ministry of Interior and the requirements of the this standard ("ISO / IEC 27001 ", 2013). This helps to manage and reduce the risks related to information by following the best security controls to achieve the management of safe and high-privacy information assets.

Third: Research Objectives

For the purpose of reaching the best results by diagnosing the actual reality of the Information Security Department and knowing the extent to which the provisions ("ISO / IEC 27001 ", 2013) can be applied. This work also measures the gap between the actual reality of the Department of Information Security in the Information Technology Department at the Ministry of Interior. This is to identify and understand the mechanism of action and continuously improve to face with current and future challenges.

Fourth: Research methodology

This work is a case study method. It applies the checklist of personal interviews using Sibai Likert scale according to item measurement. The items are fully implemented and fully documented, fully implemented and documented partially, fully implemented and undocumented, implemented in part fully documented, implemented and documented partially , implemented and partially documented, not implemented and not documented. This scale is used to measure the extent of compliance with the implementation and actual documentation of the requirements of the standard with scores starting from 0-6 in row.

Fifth: A brief history of the Information Technology Department

The Information Technology Department is one of the departments of the General Directorate of Human Resources Management within the Administrative and Financial Agency of the Ministry of Interior. This department carries out several tasks that reflect the Ministry's policy in the extent of institutional development in line with recent work directions aimed at computerizing information on human resources. It also aims to quit the paperwork stage, where it has been persistent. The section in question is to create information databases based on sustainable electronic systems, as well as its role in reducing red tape and administrative bureaucracy.

Citation Information: Jassim, N.A., Al-Zahir, B.A.M., & Khazraji, A.H.M. (2022). Diagnosing the current information systems security department in the information technology department according to the international standard (ISO / IEC 27001: 2013). *Journal of Management Information and Decision Sciences, 25*(S2), 1-7.

Second: The theoretical part

Information Security Management System (ISMS)

First: The standard for Information Security (ISO27001) Requirements

The concept of information security includes all procedures and measures that cover all aspects of computer security (Kolaly, 2005). More broadly, it represents the protection of data and information sources from deliberate and unlawful interference with it, especially in the security and strategic areas. Therefore, information security needs to be maintained continuously to track, monitor and audit the information environment (Cazemier, 2009). It represents protecting information systems from unavailable access, authorized use, disruption or destruction(Andress, 2011). It protects information from threats, reducing risks and preventing damage to business (Laudon & Laudon., 2005). The most important aspect is the security policy, which should be continuously developed to prevent penetration (Calder, 2009). The information security policy is sometimes called the document (Peltier, Peltier, Justin, & Blackley, 2005) in which it specifies the scope of security that the organization needs to provide the necessary protection and submits the document to support the implementation of the information security policy that the administration follows("ISO / IEC 27002," 2013). It is described as the central nervous system for information security and there must be three basic pillars or represent the principles of information security (Integrity, Availability, Confidentiality (Arnason & Willett, 2007). Therefore, organizations search for different methods and means of starting the security of information for this by the International Standards Organization (ISO). It develops a new series specialized in information security, namely "ISO / IEC 27001 " 2013). The so-called information security management systems (requirements, standard) provide the organization with a common model for the implementation, operation and improvement of information security systems (ISMS). Also, the effective application of ISO27001 is that it provides senior management and means of for monitoring and control of information security while reducing the risks of work arising from the lack of access to accurate information required (Al-Jubouri, 2011). It also reduces the risk of information leakage and the application of the organization standard that will ensure the security of their information officially to communicate with the customer and the legitimacy (legal). In some cases, information security is the decisive factor for people to send their information to the party that requests it and to maintain complete confidentiality about sending information (Doomun, 2008). This satisfies the requirements of the stakeholders of the organization (al-Karim & Al-Rubaie, 2013) as the following figure shows which is adopted from IEC27003 (2010).

Citation Information: Jassim, N.A., Al-Zahir, B.A.M., & Khazraji, A.H.M. (2022). Diagnosing the current information systems security department in the information technology department according to the international standard (ISO / IEC 27001: 2013). *Journal of Management Information and Decision Sciences, 25*(S2), 1-7.

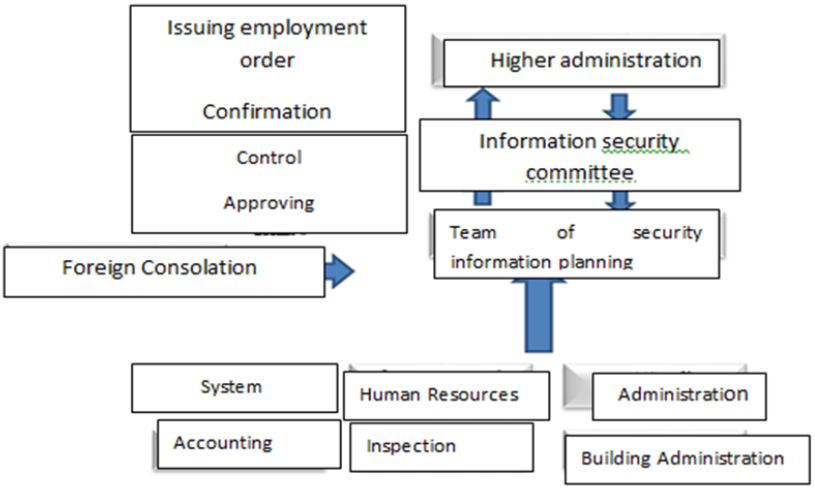

FIGURE 1
AN EXAMPLE OF AN ORGANIZATIONAL STRUCTURE THAT CREATES (ISMS)

Second: The emergence and development of the standard for information security management (ISO27001)

The standard (ISO27001) adopted, since its inception on the British specification (BS779). It was produced in 1995 and which was the result of a joint initiative of the British commercial and industrial sector. It represented a base of practices for the Information Technology Protection Department, which produced a solution that adopted a framework for implementing standards for information protection and was called Specifications for Information Protection Management Systems. It is an evaluated and certified system directed at managing information protection systems (Sewuster, 2011).

Also, the international standard was established (ISO27001) in 2005 as a rule of practice that takes its directives and recommendations from the International Standard (ISO17799: 2000) which was the British equivalent (BS7799).

ISO27001 can be considered as a basis for evaluating the integrated information protection management system (ISMS). Another version of the specification management information and new amendment security (2013) were produced in 2013. It improved the previous release of the year (2005). It introduced improvements to security controls within the specification ("ISO / IEC 27001", 2013) to ensure that the standard remains effective and is able to deal with today's dangers . Table (1) presents a comparison of items between the two versions according to the direction each item is aimed at .

Table 1
COMPARISON BETWEEN THE ITEMS OF THE TWO VERSIONS OF THE STANDARD ("ISO / IEC 27001", 2013).

ISO / IEC27001: 2005	("ISO / IEC 27001 ", 2013)
4.1Understanding the organization and its context	8.3Precautions
4.2 Understanding the needs and expectations of interested parties	5.2.1 Define and address legal, regulatory, and security contractual requirements
4.3 Determine the scope of the information security management system	4.2.1 Scope Determination and Boundaries 4.2.3 Ensure that the range remains sufficient
4.4 Information Security Management System	4.1 General Requirements
5.1 Measurement d of commitment and	5.1 Management commitment
5.2 Policy	4.2.1 Define a policy ISMS
5.3Organizational roles , responsibilities and authorities	5.1 Establish roles and responsibilities for a of the information
6.1Procedures for addressing risks and opportunities	8.3 Precautions

Citation Information: Jassim, N.A., Al-Zahir, B.A.M., & Khazraji, A.H.M. (2022). Diagnosing the current information systems security department in the information technology department according to the international standard (ISO / IEC 27001: 2013). *Journal of Management Information and Decision Sciences, 25*(S2), 1-7.

6.1.2 Information security risk assessment	4.2.1 Definition of Risk Assessment Approach 4.2.1 Identifying risks 4.2.1 Risk analysis and assessment
6.1.3 Addressing Information Security Risks	4.2.1 Identifying and evaluating risk treatment options 4.2.1 Choosing monitoring and control objectives to address risk 4.2.1 Obtaining management's assessment of the proposed residual risks 4.2.1 Initialization of a Statement of Applicability 4.2.2 Formulating a Risk Management Plan
6.2Information security objectives and planning to achieve them	5.1 Ensure that goals and plans (ISMS) Has been established
7.1Resources	4.2.2 Resource management ISMS 5.2.11 Provision of Resources
7.2Efficiency	5.2.2 Training, awareness and competence
7.3Awareness	4.2.2 Implement training and awareness programs 5.2.2 Training, awareness and competence
7.4Communications	4.2.2 Communicate with measures and improvements 5.1 Communicate with the organization
7.5Documented Information	4.3 Documentation of Requirements
8.1Operational Planning and Control	4.2.2 Operations management ISMS
8.2Information security risk assessment	4.2.3 Review risk assessment for planned periods.
8.3Addressing information security risks	4.2.2 Implement the risk treatment plan 4.2.2 Application of controls

This Table is taken from ISO / IEC 27001 mapping guide . (2013). Uk, milton keynes: mk58pp.8

Fourth: The Benefits of Obtaining the Standard Certificate of "ISO / IEC 27001" 2013)

There are several reasons that push the organization to obtain the certificate in order to get several benefits(Fuleihan & Gharib, 2015):

1. Credibility and increased confidence.
2. Improving the partnership (working with the partner).
3. Increase the confidence of customers and stakeholders.
4. Regulation and protection of the trading partner.
5. A certificate stating that the organization is qualified and complied with all applicable laws and instructions.
6. Differentiate between competitors and obtain instructions at low costs.

Third: The Practical Part

First: Diagnosing the actual reality of the information system

Table illustrates the assessment of the reality of the availability of the requirements of the information security management system. It also shows the analysis of the gap between the actual reality of the information security management and the requirements of the standard ("ISO / IEC 27001", 2013) in the Information Technology Department of the Ministry of the Interior.

It is clear from the results of the checklist in Table that the level of implementation and documentation of the item is the context of the organization. The percentage was (68%) and the size of the gap (32%) for the following reasons:

- The existence of a partial implementation of the information security management system mechanism according to the specification ("ISO / IEC 27001 ", 2013) lacking documentation.
- There are no documented steps to establish an information security management system according to the specification of the standard("ISO / IEC 27001 ", 2013), despite the application of this system and the lack of a well thought out and documented plan for the maintenance of the system.

Citation Information: Jassim, N.A., Al-Zahir, B.A.M., & Khazraji, A.H.M. (2022). Diagnosing the current information systems security department in the information technology department according to the international standard (ISO / IEC 27001: 2013). *Journal of Management Information and Decision Sciences, 25*(S2), 1-7.

- This is due to the fact that the department has a documentation system that includes following up administrative orders, analyzing and collecting data of all employees of the Ministry's formations. However, the system does not integrate with the terms of the standard ("ISO / IEC 27001 ", 2013). In addition, there is no manual for the information security management system.

Table Driving requirement checklist

The checklist in Table shows the level of implementation and documentation of the leadership item with (51%) compliance (49%) size of the gap)49%. The possible causes of this could:

- The information security management system does not meet the requirements of the standard ("ISO / IEC 27001 ", 2013).
- The absence of a written information security policy approved by the higher management in accordance with the specification ("ISO / IEC 27001 ", 2013).

Table Planning requirement checklist

Table shows that the level of implementation and actual documentation of the items requiring with (39%) examination of the requirement and (7%) size of the gap. This is due to the application and the overall documentation of the item.

- This could be caused because of the lack of documentation of the procedures in the operations of (ISMS), the risks, opportunities, and undesirable effects are not documented.
- Neither a standard for performing risk assessments was documented nor a realistic probability of risk occurrence.
- There is no fully documentation of the types of control necessary to implement information security risk treatment.

According to the above table, the level of implementation and actual documentation of item is (2.10). This is followed by examining the requirement of monitoring, measuring, analysis and evaluation in the department (98%) and the gap size (2%). This is could be attributed to the lack of documentation and the mismatch.

Second: A summary of the final results for measuring the implementation gap of the information security management system in the department according to the specification("ISO / IEC 27001 ", 2013)

Table summarizes the results of measuring the gap between the reality of the information security management system in the general section of electronic systems and the articles of the specification ("ISO / IEC 27001 ", 2013).

Table (2) A summary of the results of the level of implementation and documentation of the requirements of the international standard in the Information Technology department ("ISO / IEC 27001 ", 2013):

Table 2
A SUMMARY OF THE RESULTS OF THE LEVEL OF IMPLEMENTATION AND DOCUMENTATION OF THE REQUIREMENTS OF THE INTERNATIONAL STANDARD IN THE INFORMATION TECHNOLOGY DEPARTMENT

T	Titles of requirements according to the standard:("ISO / IEC 27001 ", 2013)		Evaluation scores for application and actual documentation		
	Requirement number	The name of the requirement	Arithmetic mean Weighted (adjusted)	Percentage to match	Gap size (%)
1	4	The sum total of the organizational context requirement items	4,1	68 %	32 %
2	5	The total sum of the driving requirement items	3.1	51%	49%

Citation Information: Jassim, N.A., Al-Zahir, B.A.M., & Khazraji, A.H.M. (2022). Diagnosing the current information systems security department in the information technology department according to the international standard (ISO / IEC 27001: 2013). *Journal of Management Information and Decision Sciences, 25*(S2), 1-7.

3	6	The total sum of the lines of the planning requirement	5,6	%93	7 %
4	7	The total sum of the support requirement items	5.9	98%	2%
5	8	The total sum of the operational planning and control requirements	5. 2	86 %	14 %
6	9	The total sum of the items of the measurement, analysis and evaluation requirement	5.6	9 3 %	7 %
7	10	The total number of items for the Corrective Action and Continuous Improvement Requirement	5.9	98%	2%
8	The total sum of the evaluation results		5.1	8 3 %	1 7 %

Table (9) shows that there is a gap between the actual reality, implementation and documentation in the IT section and the articles of the specification. The gap was 71% and the implementation and documentation was 38% compared to the international standard where the items (support operational planning, control, measurement, analysis and evaluation and efficiency) recorded the highest ratios. However, the items (understanding of the organization and its context and leadership and commitment) recorded lower ratios, thus requiring the department to reinforce the positive aspects and remove the negative aspects.

CONCLUSIONS AND RECOMMENDATIONS

First: The Conclusions

1. The interest of the Ministry of Interior's administration is to implement quality management systems at work. It called for the importance of implementing information security management systems in it because there is no documented and certified information security management system policy.
2. Despite the high financial allocations in the Ministry of the Interior, it suffers from a lack of availability of the necessary resources from the maintenance of equipment and computers to manage its information security system.
3. The Information Technology Department needs to implement a high-precision security information management system and provides a special guide for the information security management system.
4. There is no information security management system in the technology department according to international standards.
5. The existence of continuous good training has prevented a breach of the system in the department although the electronic systems are still incomplete attention to them.

Second: Recommendations

Based on the conclusion above, this work recommends the following:

1. Developing a policy for the Information Technology Department and approving it by the private authorities. It is available for all employees to view and work on according to an ISO application approved for managing the information system.
2. Providing the necessary resources for the maintenance of computers and equipment based on a good financial allocation for the importance of continuously protecting information systems. This could be done in accordance with the latest global systems.
3. Preparing a special guide for information security management that aims to clarify and create a high-confidential security environment in order to maintain the confidentiality of work in the ministry and prevent any breaches.
4. The ministry must approve correspondence with the concerned authorities to obtain a certificate ("ISO / IEC 27001", 2013) to prevent the risks that can occur as a result of the importance of the work environment in which it operates**.**
5. The awareness of higher managements of the importance of security training to avoid the occurrence of breaches needs to develop a methodology for continuous auditing of the information security system and a permanent assessment of the strengths and weaknesses of the system.

Citation Information: Jassim, N.A., Al-Zahir, B.A.M., & Khazraji, A.H.M. (2022). Diagnosing the current information systems security department in the information technology department according to the international standard (ISO / IEC 27001: 2013). *Journal of Management Information and Decision Sciences, 25*(S2), 1-7.

REFERENCES

Al-Jubouri, N.I. (2011). Protecting the security of information systems, A case study in Al-Rafidain Bank. *Tikrit Journal of Administrative and Economic Sciences, 21*(7).

al-Karim, N.A.A.L.A., & Al-Rubaie, K.H. (2013). Information security and confidentiality and their impact on competitive performance: An applied study in the Iraqi general insurance companies and al-hamraa al-ahlia insurance company, *Journal of Accounting and Financial Studies, 8*(23).

Andress, J. (2011). *The Basics of information security: Understanding the Fundamentals of InfoSec in theory and practice* (1 ed.): The Elsevier Inc stock.

Arnason, S.T., & Willett, K.D. (2007). *How to achieve 27001 certification: An example of applied compliance management*: CRC Press.

Calder, A. (2009). *Implementing Information Security based on ISO 27001 / ISO27002-Amanagement Guide* (2 ed.). London: Van Haran Publishing.

Cazemier, J. (2009). *The Basics of Information Security– A Practical Handbook*: Monika Vroege- Pokrzywa.

Doomun, M. R. (2008). Multi-level information system security in outsourcing domain. *Business Process Management Journal*.

Fuleihan, A. A. H. A., & Gharib, A. H. A. (2015). Evaluation of the Information Security System in the Iraqi Computer and Information Authority according to the international standard (ISO27001; 2013). *86*(21).

IEC27003, I. (2010). Information technology- Security techniques Information security management system implementation guidance: Geneva.

ISO / IEC 27001 (2013). In *International Standard - Information technology- Information security management systems- Requirements (2 nd ed.)*.

ISO / IEC 27002. (2013). In *Information technology - Security techniques - Code of practice for information security controls* Geneva: ISO

Kolaly, M. A., (2005). *Concepts of Information Technology*. UK: Cheltenham Courseware Ltd.

Laudon, K., & Laudon., J.P. (2005). *Management Information System* (6 ed.). New Jersey: Prentice - Hill

Peltier, T., Peltier, J., & Blackley. (2005). *Information security fundamentals* (1 ed.). United States of America: Auerbach - Puplication.

Sewuster, P. (2011). *Information security in practice: the Practice of using ISO 27002 in the Public Sector* (Master Unpublished).

Received: 30-Dec-2021, **Manuscript No.** JMIDS-21-5603; **Editor assigned:** 02-Jan-2022, **PreQC No.** JMIDS-21-5603 (PQ); **Reviewed:** 15-Jan-2022, **QC No.** JMIDS-21-5603; **Revised:** 23-Jan-2022, **Manuscript No.** JMIDS-21-5603 (R); **Published:** 30-Jan-2022

Citation Information: Jassim, N.A., Al-Zahir, B.A.M., & Khazraji, A.H.M. (2022). Diagnosing the current information systems security department in the information technology department according to the international standard (ISO / IEC 27001: 2013). *Journal of Management Information and Decision Sciences, 25*(S2), 1-7.