International Journal of Business Management and Economic Review

Vol. 7, No. 01; 2024

ISSN: 2581-4664

MEASURING AND ANALYZING THE REALITY OF IMPLEMENTING THE INFORMATION SECURITY MANAGEMENT SYSTEM IN ACCORDANCE WITH ISO 27001:2022- CASE STUDY AT THE VEHICLE REGISTRATION SITE IN BAGHDAD AL-HUSSEINIYAH

Hakeem Abdul Wahid Muhammad
Imam Al-Kadhum College, Baghdad, Iraq

http://doi.org/10.35409/IJBMER.2024.3550

ABSTRACT

The research addresses the possibility of organizations implementing an information security system in accordance with standard specification (ISO 27001:2022). The standard is important in enhanc-ing the reputation of organizations and generating competition to ob-tain accreditation from granting bodies. The research aims to Assess the actual reality of information security management system requirements by (ISO 27001:2022), In addition to diagnosing the size of gap in General Traffic Directorate- vehicle registration site in Bagh-dad al-husseiniyah. The research reveals weaknesses in the application of the information security management system and identifies aspects of documentation in a way that contributes to the possibility of developing an improvement plan. The research relied on a case study through carefully collecting data by the author based on a checklist designed based on the requirements of (ISO 27001:2022), in addition to conducting personal interviews with several administrative leaders in the General Traffic Directorate- vehicle registration site in Baghdad al-husseiniyah. The research problem included weak implementation of the information security management system and failure to meet the requirements of (ISO 27001:2022) which negatively affected the work of the information security system. The results of research show a total non- conformity rate of (68%).The most prominent recommendations are the need to pay attention to implementing, maintaining, and improving the information management system.

Keywords: International Standard (ISO 27001: 2022), information security management system, Procedures to improve.

1. INTRODUCTION

Information is of great importance to all organizations. It is considered one of their basic resources and best methods are used to protect and preserve it. ISO 27001:2022 is one of the best systems for implementing information security management. It is applied to ensure the implementation of an effective information security system because it creates an appropriate work environment characterized by appropriate attention and good handling of information. (Hashim, 2019) Indicates that concept of information security is to maintain the confidentiality, integrity and availability of information by implementing a set of controls through information security management systems and include procedures, organizational structures, processes, policies, devices and programs to protect information assets. He pointed out the need to define, implement, review and improve these controls to ensure the achievement of the organization's information security goals and objectives. An information security system is defined as a set of technical controls, policies, and procedures used to prevent unauthorized individuals from accessing to handle information or harming the physical aspect of information systems

Vol. 7, No. 01; 2024
ISSN: 2581-4664

(Razikin & Soewito, 2022). (Ding et al., 2021) defines it as protecting the organization's information from misuse, failure, unauthorized access, or destruction. The information security system is based on four axes: data, technology, operations, and individuals. (Ali & Ismail, 2019) indicated in a study conducted in one of the fertilizer manufacturing companies that there is safe information that is obtained in a timely manner because it applies standard (ISO 27001). The results of the study (Kabro & Kazem, 2019) con-ducted in the contracts department of one of the Iraqi ministries indicated that implementing the (ISO 27001) standard requires support and successful planning by senior leadership. (Attiya & Muhammad,2020) pointed out in a study conducted in several Iraqi private banks that there are weaknesses in application of the information security system in Iraqi private banks and the need for the presence of information security specialists to align the systems and policies applied with requirements contained in (ISO 27001:2022). (Podrecca et al., 2022) conducted a study in (143) companies in the United States to analyze the relationship between obtaining certification and performance, and it became clear that protecting information represents a challenge in a business environment characterized by increasing digitization and communications. Hence the importance of conducting studies and research in organizations that deal with information on an ongoing basis. This research aims to diagnose the size of the gap and weak points, evaluate the actual reality of the requirements of (ISO 27001:2022), and provide action procedures to improve the weak points. The problem in this research stemmed from the weak availability of the requirements of (ISO 27001:2022) and the lack of interest in applying and documenting indicators and items (ISO 27001:2022) in the General Traffic Directorate- vehicle registration site in Baghdad Al-Husseiniyah, which led to the creation of a group of Gaps that require improvement through diagnosing weaknesses in the application of the information security management system.

2. LITERATURE REVIEW

2.1 Implementing An Information Security Management System

Many successful organizations seek to implement an information security system by implementing the provisions of specification (ISO 27001:2022) for the purpose of protecting information from various risks and threats and maintaining the confidentiality, integrity and availability of this information (Kamariza, 2017). There are several reasons indicated by (Abbas, 2018) that push organizations to implement an information security management system, which are as follows:

- Customer Confidence: Customer confidence increases in organizations that implement and maintain information security systems.
- Compliance & Regulation: The desire of organizations to implement legislation and practical practices to protect data and avoid its misuse.
- Internal Effectiveness: Organizations' desire to manage information securi-ty more effectively.
- External Risks: The need for organizations to better manage their infor-mation security in light of general business risks.

Implementing an information security system achieves a set of goals that organizations seek to achieve through the accuracy, security and safety of all information system processes and sources. (Gupta et al., 2023), and information can be preserved and its goals achieved by limiting the possibility of allowing unauthorized persons to access the information (Alsmadi et al., 2018), and the objectives can be clarified as follows:

Vol. 7, No. 01; 2024
ISSN: 2581-4664

• Integration of information to protect against tampering and sabotage through methods provided by database systems.

• The information must be available to users who are authorized to access it. The integrity of the information is worthless if this information is not available.

• Maintaining complete confidentiality of information for people other than legally authorized individuals, even if the information is simple, including personal, military, and other information.

• Information users authorization, meaning it determines what can be done with the information and the system. It is a privilege for them and is part of the organizations policy.

• Accountability, preventing any tampering with information, and confronting information security risks, as well as taking legal measures if this happens.

• Information privacy by restricting random access, as information security policies play an important role in protecting and preserving personal information and how this information is collected and processed.

2.2 Requirements For Building An Information Security System

Management commitment and identifying the persons responsible for system security are among the requirements for implementing an information security system in accordance with the ISO 27001 standard. (Muhammad et al., 2023) indicates the necessity of estimating the costs of establishing an information security system and estimating potential losses, The requirements of the information security system can be explained as follows (Muhaisen & Hammoud, 2015):

• Determine the scope of the information security system in terms of size, types, and organizational needs.

• Develop a strategy consisting of a set of steps and procedures necessary to implement the system.

• Identify risks and distinguish between their types that threaten information security.

• Obtaining approval from senior management to implement the system.

• The implementation phase begins with preparing an implementation statement that explains the documentation, monitoring objectives, reasons and controls for selection and exclusion.

3. METHODOLOGY

The evaluation of information security management system is conducted in accordance with the international standard (ISO 27001:2022) at General Directorate of Traffic- vehicle registration site in Baghdad Al-Husseiniyah. where we build a checklist in accordance with the standards of the specification, which are: (Scope, Normative references, terms and definitions, context Organization, leadership, planning, support, operation, performance evaluation, improvement). Documents are reviewed, data is verified, and personal interviews are conducted with those responsible for implementing the system to ensure the accuracy of the information. Table (1) shows the evaluation and measurement process according to the seven-point scale, which shows the extent to which the standards are applied and documented.

Vol. 7, No. 01; 2024

ISSN: 2581-4664

Table 1: Evaluation according to requirements of standard (ISO 27001:2022)

Requirements according to the standard(ISO27001:2022)(	Non-conformity & undocumented	Conformity Partial &	Conformity Partial Partial &	Conformity Partial & documented	Conformity & undocumented	Conformity & Partial	Conformity & documented
	Value 0)(	Value 1)(	Value 2)(	Value 3)(	Value 4)(	Value 5)(	Value 6)(
1. Scope	intended to be applicable to all organizations, regardless of type, size or nature.						
2. Normative references	The following documents are referred in (ISO27001:2022)						
3. Terms and definitions	The organization is working to understand terms and definitions contained in the standard (ISO27001:2022).						
4. Context of the organization							
4.1. Understanding organization and its context				√			
4.2.Understanding needs and expectations of interested parties				√			
4.3. Determining scope of the information security management system.						√	
4.4.1. The organization shall , maintain and continually improve an information security.	√						
5. Leadership							
5.1.1. Determine information security policy and objectives.		√					
5.1.2. Integrate information security management system requirements into its operations.				√			
5.1.3. The organization provides the resources required for the system		√					
5.2. Information security policy			√				
5.3. Organizational roles, responsibilities and authorities			√				
6. Planning							

Vol. 7, No. 01; 2024
ISSN: 2581-4664

6.1.1. Actions to address risks and opportunities			√				
6.1.2.1. information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information.			√				
6.1.2.2. compare the results of risk analysis with the risk criteria and prioritize the analysed risks for risk treatment			√				
6.1.3.1. The organization shall define and apply an information security risk treatment process.		√					
6.1.3.2. formulate an information security risk treatment plan and obtain risk owners' approval.			√				
6.2.1. The organization shall establish information security objectives at relevant functions and levels.				√			
6.2.2. The information security objectives shall be consistent with the information security policy be measurable be communicated be updated as appropriate be available as documented information.				√			
6.3. organization determines the need for changes to the information security management out in a planned manner.		√					
7. Support							
7.1. Resources					√		
7.2. Competence			√				
7.3. Awareness			√				
7.4. Communication		√					
7.5.1. Documented information		√					
7.5.2. When creating and updating documented information, organization must ensure that: identification and description (e.g. a title, date, number)and format (e.g. language, software version,) and review.		√					

Vol. 7, No. 01; 2024
ISSN: 2581-4664

7.5.3. Control of documented information			√				
8. Operation							
8.1. Operational planning and control			√				
8.2. Information security risk assessment		√					
8.3. Information security risk treatment		√					
9. Performance evaluation							
9.1. Monitoring, measurement, analysis and evaluation.			√				
9.2.2. Internal audit programme			√				
9.3.2. Management review inputs			√				
9.3.3. Management review results		√					
10. Improvement							
10.1. The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.				√			
10.2.1. When a nonconformity occurs, organization shall react to the nonconformity, take action to control and correct it; deal with the consequences.			√				
10.2.2. evaluate need for action to eliminate causes of nonconformity, in order that it does not recur.		√					
10.2.3. make changes to the information security management system, if necessary.			√				

4. DATA ANALYSIS

After conducting the evaluation process, we analyze the checklist by using statistical methods, such as the weighted arithmetic average, in order to extract the Conformity rates for each standard and extract the gaps for following standards (organizational context, leadership, planning, support, operation, performance evaluation, improvement). As shown in Table (2) and Figure (1). The first three standards of the specification were not addressed, which are (Scope, Normative references, terms and definitions) as they are guiding standards for organizations to clarify the scope of application and use of the document (ISO:27001:2022), as explained in Table No. (1).

Vol. 7, No. 01; 2024
ISSN: 2581-4664

Table 2: Conformity rates and non-conformity rates

Requirements according to the standard(ISO27001:2022)	Weighted mean	Percentage of conformity	Gap size
Context of the organization	2.8	46%	54%
Leadership	1.8	30%	70%
Planning	2	33%	67%
Support	1.85	31%	69%
Operation	1.3	22%	78%
Performance evaluation	1.75	29%	71%
improvement	2	33%	67%
Total	**1.9**	**32%**	68%

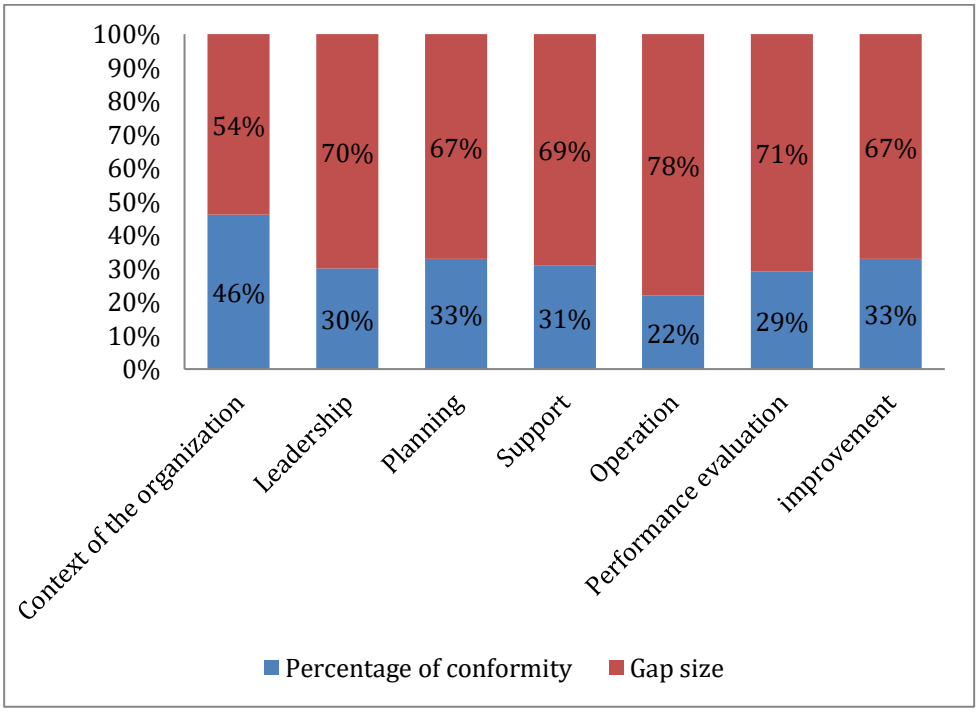

Figure 1: Conformity rates and non-conformity rates

It is clear from the results that there are large gaps between actual reality of General Directorate of Traffic- vehicle registration site in Baghdad Al-Husseiniyah and requirements of information security management system. Accordingly, we are preparing (an information security management system improvement plan) as in Table (3), which includes work procedures in accordance with the requirements of the international standard (ISO 27001:2022). We prepare these procedures through field coexistence in the organization (research scope) and recording the experiences that

Vol. 7, No. 01; 2024
ISSN: 2581-4664

officials and workers have about its information security system with, the aim of improving the low vulnerabilities that are monitored during the assessment, and that correspond to the weight (0, Non-conformity and not documented) and to the weight (1, partial conformity and not documented), according to the seven-point scale used in the checklist shown in Table (1). these procedures are considered appropriate solutions to meet the requirements of the specification and attempt to improve performance.

Table 3: Procedures to improve the information security management system

Procedures to improve the information security management system	
4. Context of the organization	**procedures**
4.4.1. The organization shall , maintain and continually improve an information security	• Spreading the culture of implementing the information security system • The Quality Assurance Division trains individuals to implement the system • Internal audit work in accordance with the requirements of the specification • Correcting non-conforming cases and improving performance • Working on using continuous improvement systems for the system
5. Leadership	**procedures**
5.1.1. Determine information security policy and objectives.	• Documenting and publishing the followed policy • Announcement of the policy • Urging employees to understand the policy and adhere to it • Notifying the parties concerned about it • Periodic and continuous follow-up
5.1.3. The organization provides the resources required for the system	• Form a team to identify the required resources • Identify and arrange resources according to importance • Seeking to provide resources related to implementing the system • Optimal use of resources • Ensure the effectiveness of the application according to the new resources • Sustainability and preservation of resources
6. Planning	**procedures**
6.1.3.1. The organization shall define and apply an information security risk treatment process.	• Establishing instructions indicating the risks, their types, and the priority in dealing with them

Vol. 7, No. 01; 2024
ISSN: 2581-4664

	• Determine the methods by which treatment is carried out • Determine the resources required • Identifying those responsible for follow-up • Setting a time limit for addressing risks
6.3. organization determines the need for changes to the information security management out in a planned manner.	•Follow up on the organization's basic plans and understand their details •Follow up on the basic changes in the organization, including structure, strategies and systems •Studying changes to information security systems and the need for them • Studying the available alternatives according to ISO27001:2022 •Implementation, follow-up and testing of results
7. Support	**procedures**
7.4. Communication	• The organization determines the parties with which it should be communicated, whether they are internal or external. • Determine appropriate means of communication. • Identify those authorized to communicate. • Documenting communication processes, storing information, and continuous follow-up.
7.5.1. Documented information	• Identifying the administrative authorities for documentation and those authorized to do so • • Determine the type of documents that are stored according to the information security system • Save documents in a safe way and also save information electronically • Make backup copies for safekeeping • updating documented information the organization shall ensure appropriate: identification and description (e.g. a title, date, number)and format (e.g. language, software version,) and review.
7.5.2. When creating and updating documented information, the organization must ensure that: identification and description (e.g. a title, date, number)and format (e.g. language, software version,) and review	
8. Operation	**procedures**
8.2. Information security risk assessment	•The organization must identify information security risks and plan for them in advance •Evaluate information according to

Vol. 7, No. 01; 2024
ISSN: 2581-4664

8.3. Information security risk treatment	importance • Determine a time period for evaluation • Proposing changes made by the organization • Proposing alternatives to address risks • Providing the necessary resources and capabilities for treatment • Evaluating solutions and their compatibility with the information security management system • Maintain information and document it well
9. Performance evaluation	**procedures**
9.3.3. Management review results	• Establishing a system audit and review team Determine a plan for the review • • Review and audit work is divided according to tasks, including cases of non-conformity, feedback, results of monitoring and improving the system and achieving goals. • Preparing follow-up reports and the progress of audits • Trying to establish corrective procedures for observations and providing support to workers in reviewing the system
10. Improvement	**procedures**
10.2.2.evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur.	• Identifying non-conformities accurately • Classifying cases into minor violations or major non conformities. • Develop a plan to eliminate cases of non-conformity that includes preparing the necessary resources, time, and stakeholders within the organization •Implementing appropriate treatments according to the requirements of the specification. • Identifying the people responsible for follow-up

5. CONCLUSIONS

Through results of the research, it appears to us that there is a weakness in availability of information security system requirements, and presence of large gaps in the items of the standard specification (ISO 27001: 2022) in General Traffic Directorate- Vehicle Registration Site in Baghdad Al-Husseiniyah. The percentage of gaps reaches 78% in the operational item and 71% In performance evaluation item. vehicle registration website lacks the capabilities that would help it

Vol. 7, No. 01; 2024
ISSN: 2581-4664

implement the standard effectively. There is a lack of interest in documentation which is an essential part of the application. There is negligence in implementing, maintaining and constantly improving the information security management system, and the policy and objectives were not well defined, and strategic direction was not taken into account, as well as weakness Management review in cases of non-conformity. Therefore, the research recommends the necessity of providing many requirements for the information security system in the General Traffic Directorate- Vehicle Registration Site in Baghdad Al-Husseiniyah, and the necessity of applying the work procedures mentioned during this research and taking an active interest in implementing and constantly improving the information security management system.

REFERENCES

Abbas, Z. S. (2018).Evaluation of the information security management system in accordance with the international standard (ISO 27001: 2013) and its impact on business excellence by adopting the European model standards: case study in the General Company for Electronic Systems. Master thesis, Administrative Technical College, Iraq.

Ali, R. A**.,** & Ismail, I. F. (2019). Measuring the possibility of applying the ISO 27001 standard: a case study in the General Company for Southern Fertilizers Manufacturing. *Gulf Economic Journal*, *35*(40).
https://search.emarefa.net/ar/detail/BIM-977732-27001

Alsmadi, I., & Burdwell, R., & Aleroud, A., & Wahbeh, A., & Al-Qudah, M. A.,& Al-Omari, A. (2018), Practical Information Security, Switzerland, 6.
https://link.springer.com/book/10.1007/978-3-319-72119-4

Attia, R. F., & Mohamed, M. I. (2020). The role of the external auditor in assessing the security of information technology systems in light of (ISO/IEC 27001): Applied research on a sample of private banks. *Journal of Accounting and Financial Studies, 15* (51).
https://www.iasj.net/iasj/download/39a8926d90fa0a86

Dhillon, G., & Smith, K., & Dissanayaka, I. (2021). Information systems security research agenda: Exploring the gap between research and practice. *Strategic Information Systems, 30*(4),16.
https://doi.org/10.1016/j.jsis.2021.101693

Ding, Y., & Wu, Z., &Tan, Z., & Jiang, X. (2021). Research and application of security baseline in business information system. *Procedia Computer Science*, *22*(183), 631. https://doi.org/10.1016/j.procs.2021.02.107

Gupta, B., & Gaurav, A., & Panigrahi, P. (2023). Analysis of security and privacy issues ofinformation management of big data inB2B based healthcare systems. *Journal of Business Research*, *162*(2).
https://doi.org/10.1016/j.jbusres.2023.113859

Hashem, Y. S. S. (2019). Diagnosing the size of the gap between the actual reality and the requirements of the information security management system according to ISO/IEC 27001:2013: a case study in the Ministry of Interior. Master thesis, Administrative Technical College, Iraq,(19).

ISO/IEC. (2022). International Organization for Standardization International Electrotechnical Commission :(ISO/IEC 27001:2022) . Information security management systems . Fifth edition, Geneva, Switzerland.
https://www.iso.org/standard/27001

Vol. 7, No. 01; 2024
ISSN: 2581-4664

Kamariza, Y. (2017). Implementation of information security policies in public organizations. Master Thesis, Jonkoping University, Sweden, 5.
http://hj.diva-portal.org/smash/record.jsf?pid=diva2%3A1154975
Kapro, R. Y., & Kathem, E. F.(2019). Possibility of using ISO 27001: 2013 in the implementation of government contracts quality standards: case study in the Ministry of Commerce Contracts Section. *Journal of Administration and Economics*,*37*(121).
https://admics.uomustansiriyah.edu.iq/index.php/admeco/article/view/291
Kavak, A., & Odabas, H. (2023). The impact of information securitymanagement guide utilization on technological and institutionalinformation security measures inuniversity libraries in Turkiye. *The Journal of Academic Librarianship*,*49*(6),5. https://doi.org/10.1016/j.acalib.2023.102800
Muhaisen, H. N., & Hammoud, A. K. (2015). Evaluation of information security management systems in the Information Technology Department according to ISO 27001. *Iraqi Journal of Science and Technology*, *6*(2).
https://www.iasj.net/iasj/download/29defdf488d02314
Muhammad, A. R.,& Sukarno, P.,& Wardana, A. A..(2023). Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning. *Procedia Computer Science*, *217*(23),1407. https://doi.org/10.1016/j.procs.2022.12.339
Podrecca, M., & Culot,G.,& Nassimbeni, G., & Sartor, M. (2022). Information security and value creationThe performance implications of ISO/IEC27001. *Computers in Industry*,142.
https://doi.org/10.1016/j.compind.2022.103744
Razikin, K.,& Soewito, B. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. *Egyptian Informatics Journal*,*23*(3),384.
https://doi.org/10.1016/j.eij.2022.03.001