How to Cite:
Mohammed, T. J., & Jasim, N. A. (2022). Designing a model to protect documented information according to the integration of some international standards (ISO 27001: 2013) (ISO 10013: 2021): A case study. *International Journal of Health Sciences*, *6*(S3), 10684–10697. https://doi.org/10.53730/ijhs.v6nS3.8376

Designing a model to protect documented information according to the integration of some international standards (ISO 27001: 2013) (ISO 10013: 2021): A case study

Taha Jassim Mohammed
College of Administration and Economics, Al-Mustansiriya University, Iraq.
Email: tahajassim1989@uomustansiriyah.edu.iq

Nagham Ali Jasim
College of Administration and Economics, Al-Mustansiriya University, Iraq
Email: nagam_aja@uomustansiriyah.edu.iq

***Abstract*---**The research aims to apply a proposed model to diagnose the gap between the actual reality of the work of the Oil Exploration Company and the protection of information security according to some provisions of the international standard ("ISO 27001: 2013,") and the international standard ("ISO 10013:2021 "). The company has due to the limited measures taken to protect the security of the information documented in it, and in order to reach the scientific facts, the case study approach was adopted, and the checklist was used. As for the statistical analysis methods, the arithmetic mean and percentage of application and documentation were used, and the proposed model showed a gap in the reality of the actual application and documentation of the company under study, which was at a rate of (36%) as somewhat medium rate due to the existence of a bank of documented oil information, the first of its kind in the oil sector performance level.

***Keywords*---**designing, protect documented, integration, international standards.

Introduction

The tremendous development in the digital information systems and their application, and the widespread spread of the strategy of relying on computer networks in the automation work and the preservation of documented information have led to an increase in information security challenges. These

challenges pose a danger, threat, loss of confidence and a burden on the company in case the information security system fails to maintain the confidentiality and integrity of documented information security. Yet, the oil and gas sector is the main source of the Iraqi economy, as it participates by (90%) of the total gross domestic product, which prompts us to pay attention to documented oil information. Based on the foregoing, the research addresses the integration between the requirements of some provisions of the two international standards (ISO 27001: 2013) (ISO 10013: 2021), in an attempt to find out the extent of application of the requirements and guidelines of the two standards and the possibility of adopting them and adhering to their standards in the Oil Exploration Company. The research consists of three sections, the first section deals with the protection of documented information and the second topic deals with the two international standards ISO 10013:2021)) (ISO 27001:2013), while the third topic deals with the practical side of the research.

Methodology of research

The research problem

The researchers relied on personal interviews in the initial survey with officials and heads of a number of departments in the Oil Exploration Company, and it was found that there are real risks to which the company is exposed, represented in limited measures to protect the security of information documented in it. They expose the company to problems due to the nature of its work represented in providing services to its clients in the form of geochemical, geophysical and geological studies.Thus, the researchers believe that there is a need to apply some measures to provide the desired protection for documented information in all its preservation methods, and this is what is provided by the integration between some requirements of the international standard (ISO 27001: 2013) and the guidelines of the documented information system (ISO 10013: 2021), and thus the research problem revolves which will be formulated in the form of questions as follows:

- Is it possible to prepare a unified model to combine the requirements of the standard specification (ISO 27001: 2013) and the instructions of the documented information system (ISO 10013:2021) to protect the documented information system in the researched company?
- What are the extents of application of the proposed model and is there a gap in the application in the research sample?
- What are the strengths, weaknesses and obstacles facing the protection of documented information security in the researched company?

The importance of the study

The study is important because, it

- is a study that guides the company in question to improve and protect the security of its documented information.
- diagnoses strengths and weaknesses in order to provide appropriate recommendations to bridge that gap.

- addresses the reasons for the weak protection of the documented information in the researched company and fills the gap to improve the information provided to the beneficiaries.

Research Objectives

The study aims at:

- preparing and formulating a unified form to combine the requirements of the standard specification (ISO 27001: 2013) and the guidelines of the documented information system (ISO 10013:2021) to protect the documented information system in the researched company.
- Determining the levels of application of the proposed model.
- Diagnosing the gap and identify the most influential reasons for embodying the gap by presenting the strengths, weaknesses and obstacles facing the protection of documented information security in the researched company.

The research plan

The company wishes to develop its quality system in line with the requirements of the international standard (ISO 27001:2013) and the guidelines of the international standard (ISO 10013:2021), so it must define and apply the processes in it to ensure a continuous control over the information and protect its security. This secures the interdependence between the processes and control the interaction between them.

Figure 1 shows the procedural scheme of the research, which shows the lines followed in how to reach the desired results

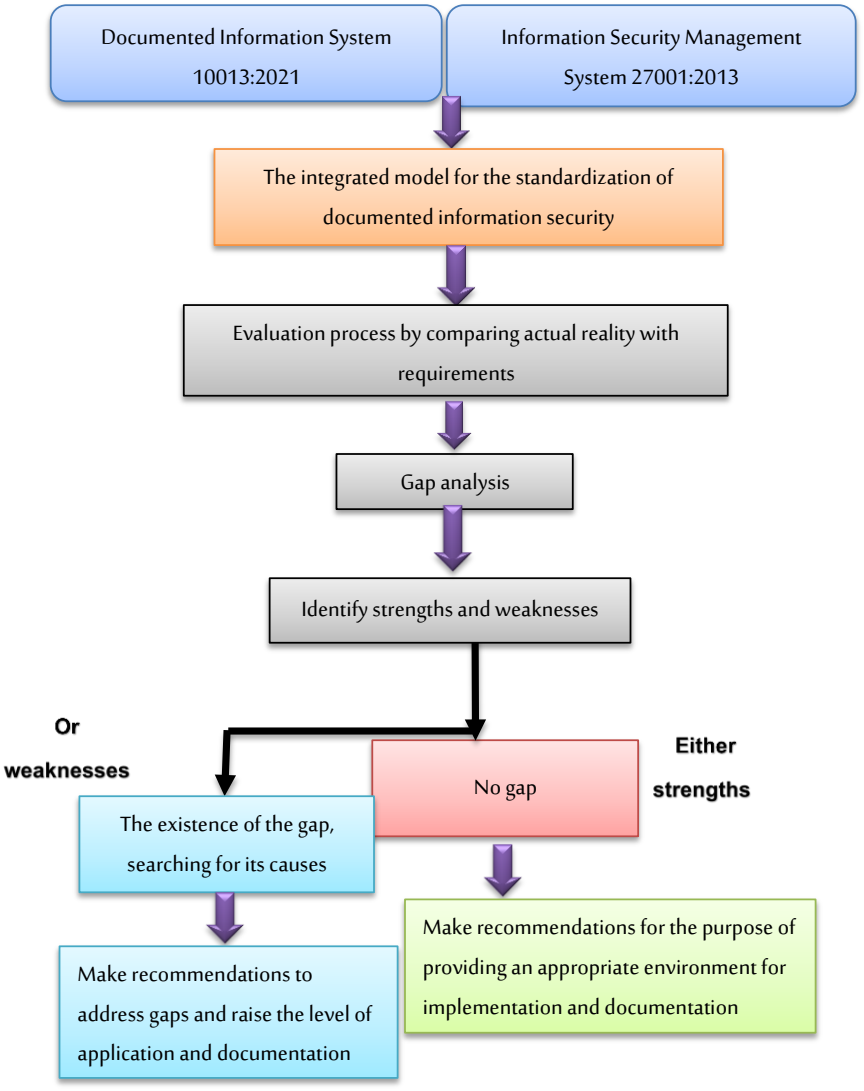

Figure 1. The procedural scheme of the research

Research hypotheses

The research stems from a basic premise, "What is the contribution of the application of protecting some of the provisions of the two standards to maintaining the security of documented information in the Oil Exploration Company?

Research Limits

- Spatial limits: This research was conducted in the Iraqi National Oil Company / Oil Exploration Company at its headquarters in Baghdad.
- Temporal limits: The research period took (8 months) from 1/9/2021 to 1/5/2022.

Some previous studies

Previous studies on the International Standard (ISO 27001:2013)

Table 1
Previous studies

No	Study name and date	Study Title	The study Problem	Objectives of the study	The most important conclusions
	(Attia & Mohamed, 2020)	The role of the external auditor in assessing the security of information technology systems in the light of the specification (ISO 27001:2013) an applied research on a sample of private banks	The necessity of periodically examining and evaluating the security of data and information systems by senior managements in banks and the extent to which they apply information security procedures and policies in light of the standard specification (ISO/IEC27001:2013).	1- Introducing information technology and highlighting the information technology and banking systems used.	The research sample banks did not achieve all the requirements and standards of the standard (ISO/IEC 27001) and the presence of weaknesses, as well as the presence of a defect in the security of information technology, which requires standing and studying them and taking the necessary measures to address them.
2	(Syreyshchikova, Pimenov, Mikolajczyk, & Moldovan, 2019)	"Information Safety Process Development According to ISO 27001 for an Industrial Enterprise" "	Violation of information security of the company "JSC "K.	2- Introducing the International Organization for Standardization and International Standards and Specifications that it issues, including (ISO/IEC27001:2013).	The main results of the research are:
3	(Kadhem, 2018)	Requirements for the application of	The study problem can be expressed through the following question:	1- Development of the information security process.	1- Ensuring that data is available to

		the international standard ISO 27001: 2013 for the implementation of government contracts			authorized users
4	(Candiwan & Priyadi, 2016)	"Analysis of Information Security Audit Using ISO 27001:2013 & ISO 27002:2013 at IT Division -X Company, In Bandung, Indonesia"	(Does the Contracts Department have an acceptable level of information security management system by adopting the international standard ISO 27001:2013)?	2- Developing an information security methodology through risk management for the information security process.	2- Ensuring the confidentiality of the organization's information.

There are no previous studies available on the international standard ISO 10013:2021 (to the knowledge of the researcher).

Theoretical framework of the research

The first topic: the protection of documented information
Documented information

Documented information can be defined as a form of documents or media, and these documents may be in the form of (paper, electronic or optical computer disk, image, basic sample or any other physical medium)("ISO 9001 :2015,"). As defined by the International Standard ISO 10013:2021:1), it is the information required to be controlled and maintained by the organization and the medium that contains it. Documented information can be used for communication, to provide objective evidence or to exchange knowledge. It enables the organization's knowledge and experience to be maintained and can generate value to support improvement of products or services. It is the information that must be kept as evidence that the achieved results or activities are being carried out as planned. It can be structured and generated in a variety of ways based on the needs of the organization and other factors such as leadership, desired outcomes of the management system, context (including legal and regulatory requirements), and stakeholders. Therefore, we can say that documented information is that type of information taken from an official source such as government websites or official organizations and does not belong to any personal opinions as it is the primary source of information that provides real, documented information that makes the individual able to make correct decisions about them, unlike random sources. Documented information shall be in any kind of media such as paper or electronic sample, photographs, maps and other physical media.

Information security

Information security science investigates theories and strategies to protect documented information from threats to it and from attacking activities. It is all

the necessary means, tools and procedures to be provided to ensure the protection of information from internal and external dangers(S. S. Hassan, 2020). It also means preserving the information in any information system from the risks of loss and damage, or from the risks of incorrect use, whether intentional or spontaneous(Maghribi, 2016). The term information security is broad and includes the protection of information from accidental or intentional misuse by persons inside or outside the organization. It is the primary tool that any organization can use to combat downtime-related threats(Simanjuntak, 2022). The concept of information security includes all procedures and measures that cover all aspects of computer security. More broadly, it represents the protection of data and information sources from intentional and unlawful interference with them, especially in the security and strategic areas. Therefore, information security must be maintained on an ongoing basis to track, monitor and audit the information environment(Jassim, Al-Zahir, & Khazraji, 2022).

Elements of information security

Information security depends on three basic elements that must be present in the information that requires protection(A. F. a. Hassan & Muhammad, 2020):

- Confidentiality: It is the ability to maintain the confidentiality of information by preventing unauthorized access to information, whether it is stored on a physical medium or sent through means of communication.
- Information integrity and content integrity: Ensuring the preservation of information content and its integrity from tampering, modification or corruption, by preventing access to this content through illegal interference.
- Availability and Availability of Information: Ensuring the availability of information and the ability to provide it and make it available in a timely manner through authorized persons, and ensuring that these persons will not be prevented from using or accessing information.
- Non-disavowal: this means the inability of the accused to deny the crime committed against information security, and it is intended to ensure that the person who breached information security or its sites does not evade, and deny that s/he is the one who did this behavior(Al-Hasaniah, 2020).

Means of protecting documented information security

Information security represents a set of mechanisms, procedures, tools and products that are used to prevent or reduce risks and threats to computers, networks, information systems and their rules, as follows(Yassin, 2014):

- Antivirus programs: They are the software that is used to detect and remove all types of malicious software and work to completely erase them from the system because of the threats that this software has that may affect the security of the information contained in the organization(Abdul-Razzaq, 2007).
- Firewall programs: This category of programs works to secure the ports on the computer through which applications can access Internet services, and in many cases the user is not aware of the open ports on the system, which allows forgetting to secure and protect these ports. Firewall programs act as

a filter that prevents malware from reaching devices through this open window (Titi, 2010).

- Encryption: Encryption is the science used to preserve the security and confidentiality of information. It is not possible to know the content of the information sent by anyone other than the person to whom that information was sent and who owns the key to decrypt it, noting that if that information reaches other people, they cannot take advantage of it or even understand its meaning(Bidgoli, 2021). If you want to protect and hide your messages and files from prying eyes, you can encrypt them. Encryption obfuscates the contents of a file so that you cannot read it without the correct decryption key. There are different ways to encrypt messages. You can switch the order of characters, replace characters with other characters, or insert or remove characters(Cummings & McCubbrey, 2010).

The second topic: international standards
International Standard ISO 10013:2021

Despite the expenses and commitment involved in the ISO certification, it gives great external and internal benefits. The external benefits come from the advantage of the products that will be sold compared to companies that do not have the ISO certificate. Therefore, many companies seek to obtain this certificate to enjoy the competitive advantage that it provides. Internal benefits come from the increase in profitability of ISO certified companies, where registered companies reported a (48%) increase in profitability and a (76%) improvement in marketing(Krajewski, Ritzman, & Malhotra, 2021). More than 1.6 million ISO certificates have been granted to companies in (201) countries, including (30,000) certificates in America to do business worldwide and have been included in the ISO guide(Sartor, Orzes, & Moras, 2019).

Implementing and maintaining the requirements of the chosen standard may prove to be a burden in terms of costs and additional paperwork without any compensating benefits. Therefore, ISO registration should not only be required to meet the contractual requirements of major customers or for marketing purposes, but rather adopt the requirements of this system as an integrated project preceded by an internal quality audit of the existing quality management system by a qualified auditor. This will determine the initial status of the company's quality management system and enable management to assess the amount required for qualification and meeting its requirements, as well as knowing the amount of the gap between the current reality and what the organization aspires to be in the future(Dale, Bamford, & van der Wiele, 2016).

The international standard ISO 10013 is the international standard for documented information (documentation) is a specification (guidance) that helps the organization that intends to implement management systems (such as the quality management system, environmental management system, etc.) in preparing its documented information and how to respond to the requirements contained in those specifications. This standard went through several stages to reach this version, which, despite the existence of previous versions, is considered the first version. In 1995, the Guiding Standard 10013:1999 was issued, entitled "Guiding Principles for the Development of Quality Manuals", and then followed

by another version in 2001 as well. The first version was considered because it took a different curve from its predecessor, and the version was ISO/TR 10013:2001, entitled “Guidelines for Documenting the Quality System.” It is noted that the 2001 version was in the form of a technical report. Therefore, the 2021 version was considered the first real version, being more focused. It has comprehensive details and was issued by the International Organization for Standardization as an international specification ISO 10013:2021 entitled "Quality management systems - Guidelines for documented information". The international specification ISO10013:2021 aims to guide public and private companies to obtain documented information (documentation of information) and find appropriate ways to preserve it as well as maintain and reuse it. Among these benefits that the organization obtains are the following (ISO 10013,2021): -

- Demonstrate compliance with legal and regulatory requirements.
- Make information readily available to all organizational levels so that they can better understand the interrelationships.
- Communicate the organization's commitment to quality to the relevant stakeholders.
- Helping people understand their role within the organization and thus providing a basis for work performance expectations.
- Providing objective evidence that the specified requirements have been met.
- Addressing risks and opportunities to improve organizational performance, product or service compatibility, and customer satisfaction. We must make it clear that with the issuance of the ISO 9001 specification version 2015, the use of the name “procedures” has been terminated and has been replaced by “documented information” or “documenting information,” which are the documents that the company or institution needs as a limit. Minimum if it wants to be compliant with (ISO 9001:2015).

International Standard ISO 27001:2013

The International Organization for Standardization (ISO), and through cooperation with the International Electrotechnical Commission, has developed a series of specialized specifications for information security, namely (ISO 27001), which is called information security management systems. This gives a general model for the application, operation and improvement of information security management systems(ISMS)(Al-Khaled, 2018). This international standard has been prepared to provide the requirements for establishing, implementing and maintaining an information security management system continuously. The adoption of an information security management system is a strategic decision for the company. The application of the system in the company is affected by its needs, objectives, security requirements, organizational processes used, and the size and structure of the company; The Information Security Management System maintains the confidentiality and integrity of information availability through the application of the risk management process and gives confidence to the concerned parties that the risks are managed appropriately (ISO 27001,2013).

The specification is also a useful model for establishing, implementing, monitoring, reviewing, maintaining and improving an information security management system (ISMS). It is understandable and can be applied anywhere in

the world. It also is consistent, coherent, contains best practices, experiences and expertise worldwide and is technically neutral. It is designed for implementation in any organization(Calder, 2011).

The third topic - the practical side

This topic focuses on the diagnosis and analysis of the gap using the seven-way Likert scale according to weights from (0) the lowest weight to (6) the highest weight (Al-Khatib, 2008). Some of the main and sub-items have been adopted in building the checklist for the requirements of the international standard (ISO 27001: 2013) and the guidelines of the international standard (ISO 10013: 2021). Gaps will also be found in the company according to the following equations(Al-Moussawi, 2020; Ibrahim, 2021).

- Equation (1) Arithmetic mean = sum of (weights * their frequencies) / sum of frequencies
- Equation (2) The percentage of conformity = (weighted arithmetic mean) / value of the highest weight in the scale
- Equation (3) The size of the gap for each item in the checklist = 1- Percentage of match

Discussing the results

Table 2
Results of the two international standards checklist

No	Requirement name	Estimated Arithmetic mean (average)	Percentage of application and documentation	Gap size for requirement	Application level
1	Create and update information	3.83	%64	%36	and documentation
2	Documented	2.72	%45	%55	Partially Applied Fully Documented
3	Automated workflow	2	%33	%67	Partially Applied Partially Documented
4	Protection	6	%100	%0	Partially Applied Partially Documented
5	keep and dispose	4	%66	%34	Fully Applied Completely Documented
6	Information security awareness	4	%66	%34	Completely

					undocumented
7	Procedures for dealing with information security risks	3.75	%62.5	%37.5	Completely undocumented
8	Handling information security risks	4.5	%75	%25	Partially applied, fully documented
The sum total of the evaluation results		30.8	%511.5	%288.5	
The upper limit of the application and complete documentation of the requirement		6	%100		
Assumed total sum of application and full documentation		48			
The amount of the gap in the application and documentation of the total requirements		17.2			
The ratio of the total actual results to the total assumed results		%64			
Percentage of the gap in the application and documentation of the international standard		%36			

Based on the results of Table (2), it was found that the actual percentage of application and documentation in the Oil Exploration Company was (64%), which reflects the existence of a gap between the model and the reality of the application and actual documentation of the company in question, which was at a rate of (36%), which is a somewhat medium ratio due to The existence of a bank of documented oil information, the first of its kind in the oil sector .The lowest percentage of application and documentation of the requirement (protection of documented information security) was an evaluation rate of (67%), which reflects the weakness of interest in protecting documented information security for the researched company, while the largest percentage of conformity with the international standard was for the requirement (retention and disposal), which reflects the efficiency and effectiveness of the company in preparing a guide The quality (operational) of its operations, as well as the unique description of the good and service it provides, represented in the exploration of oil and gas exclusively throughout Iraq, and the efficiency and accuracy of the methods of retention and disposal of documented information for the researched company.

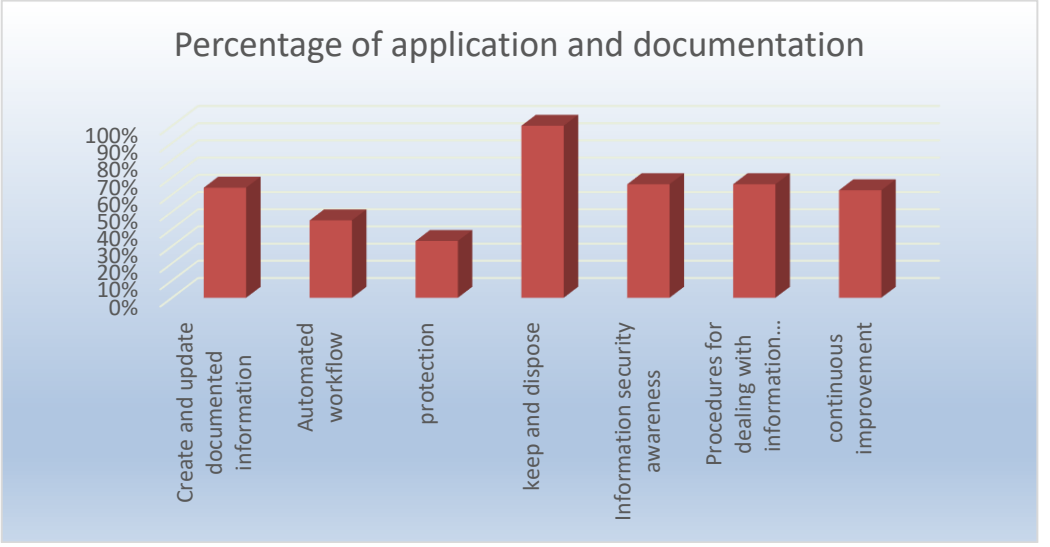

Figure 2. Percentage of application and documentation of some clauses of the two international standards

Conclusions

This part reviews the conclusions reached by the researchers by analyzing the results of the practical side of the research as follows:

- The company shows the importance of creating and updating documented information by identifying the individuals responsible for creating documented information by issuing administrative orders to form main and subsidiary committees by the Human Resources Management Department
- The company does not have a unified electronic system that contains the details of contracts and sales, as well as the failure to build an electronic system for the unified automated workflow for the circulation of all reports and the statement of work details in the company through a unified database.
- The company does not use modern methods to avoid exposure to documented information security risks related to cyber security.
- The company relies on the Documents Preservation Law No. (37) of (2016) in the retention and disposal of documented oil information.
- The company is not obligated to hold specialized training courses to educate employees about the risks of documented information security.
- The company's management deals with information security risks and with the risks resulting from them by forming a higher committee to manage documented information security.

Recommendations

- We recommend the use of electronic documentation of administrative orders issued to individuals responsible for creating and updating the information documented by the Human Resources Management Department.

- We recommend a unified electronic system that contains the details of contracts and sales. We also recommend the necessity of building an electronic system for the unified automated workflow to circulate all reports and show the work details in the company through a unified database.
- Introducing modern work methods to protect documented information in the company to avoid exposure to documented information security risks related to cybersecurity is preferable.
- Adopting the unified form of the two state standards in preparing the company to obtain the international standards certificate for the management of documented information security.
- The company can conduct specialized training courses to educate employees about the risks of documented information security. We recommend preparing a brochure for all the activities and tasks of the company's departments and bodies, in which it shows in detail and accurately the daily work steps from beginning to end for all the company's operations and its various activities.
- We recommend the adoption of the principle of accurate documentation of all information, and work to classify it in the electronic authentication system and not to neglect the documentation of errors and cases of breach to benefit from them in future risk analysis.

References

Abdul-Razzaq, J. S. T. (2007). Electronic Documents in Indicators and Information Coders, -. *Journal of the College of Education*(4). Retrieved from https://www.iasj.net/iasj/pdf/4171fd7b5335cf18

Al-Hasaniah, I. S. (2020). *Management Information Systems; Information management in the era of digital organizations* (3 ed.). Amman - Jordan: Al-Warraq Publishing and Distribution Corporation.

Al-Khaled, S. M. (2018). *Trends in Information Security and Security: The Importance of Cryptographic Techniques*: Obeikan Publishing.

Al-Khatib, S. K. (2008). *Total Quality Management and ISO Contemporary Introduction* (1 ed.). Baghdad - Iraq: Jaafar Al-Asami Library.

Al-Moussawi, A. S. A. (2020). *Evaluation of the requirements for implementing the international standard ISO 45001:2018 for an occupational health and safety management system - a case study in a Wasit textile and weaving factory.* Al-Mustansiriya University, College of Administration and Economics.

Attia, R. F., & Mohamed, M. E. (2020). The role of the external auditor in assessing the security of information technology systems in light of the standard specification (27001). *Journal of Accounting and Financial Studies, 15*(51).

Bidgoli, H. (2021). *Management information systems* (10 ed.): published Cengage Learning Canada.

Calder, A. (2011). *Implementing information security based on ISO 27001/ISO 27002*: Van Haren.

Candiwan, M., & Priyadi, Y. (2016). Analysis of Information Security Audit Using ISO 27001: 2013 & ISO 27002: 2013 at IT Division-X Company, In Bandung, Indonesia. *International Journal of Basic and Applied Science, 4*(04), 77-88.

Cummings, M., & McCubbrey, D. J. (2010). *Management information systems for the information age*: McGraw-Hill Irwin.

Dale, B. G., Bamford, D., & van der Wiele, T. (2016). *Managing quality: An essential guide and resource gateway*: John Wiley & Sons.

Hassan, A. F. a., & Muhammad, J. T. (2020). Digital Information Security and Ways to Protect It Under Current Legislations. *The Egyptian Journal of Information Sciences, 7*(1). Retrieved from https://www.youtube.com/watch? http://jesi.journals.ekb.eg/article_90110.html

Hassan, S. S. (2020). Methods for Archiving and Preserving Digitized Records. *The Arab Journal of Information Sciences, 7*(2). Retrieved from https://jesi.journals.ekb.eg /article_160400.html

Ibrahim, I. A. A. (2021). *The Possibility of Implementing the Quality Management System for Electoral Organizations ISO 540001: 2019 in the Independent High Electoral Commission.* (Master). University of Baghdad, College of Administration and Economics.

ISO 9001 :2015. In.

ISO 10013:2021 In.

ISO 27001: 2013. In.

Jassim, N. A., Al-Zahir, B. A. M., & Khazraji, A. (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 & Decision Sciences, 25*.

Kadhem, A. F. (2018). *the requirements for the application of the international standard ISO 27001 2013: for the implementation of government contracts / a case study in the Ministry of Commerce.* (Master). Al-Mustansiriya University, College of Administration and Economics TAAD.

Krajewski, L. J., Ritzman, L., & Malhotra, M. (2021). Operations Management: Processes and Supply Chains (10 uppl.). *Harlow: Pearson Education Limited*.

Maghribi, M. A.-F. (2016). *Management Information Systems* (1 ed.). Amman - Jordan: Dar Al-Jinan for Publishing and Distribution.

Sartor, M., Orzes, G., & Moras, E. (2019). ISO 14001. In *Quality Management: Tools, methods, and standards*: Emerald Publishing Limited.

Simanjuntak, M. (2022). PEMANFAATAN TEKNOLOGI INFORMASI DAN KOMUNIKASI PADA E-BUSINESS. *E-Business: Inovasi di Era Digital*, 33.

Syreyshchikova, N. V., Pimenov, D. Y., Mikolajczyk, T., & Moldovan, L. (2019). Information Safety Process Development According to ISO 27001 for an industrial enterprise. *Procedia manufacturing, 32*, 278-285.

Titi, K. M. (2010). *Knowledge Management Challenges, Techniques and Solutions* (1 ed.). Amman - Jordan: Dar Al-Hamid for Publishing and Distribution.

Yassin, N. A. (2014). *Cloud computing for libraries, solutions and applications* (1 ed.). Cairo: Dar Al-Shorouk.

Rinartha, K., Suryasa, W., & Kartika, L. G. S. (2018). Comparative Analysis of String Similarity on Dynamic Query Suggestions. In *2018 Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS)* (pp. 399-404). IEEE.

Suryasa, I. W., Rodríguez-Gámez, M., & Koldoris, T. (2021). Get vaccinated when it is your turn and follow the local guidelines. *International Journal of Health Sciences*, *5*(3), x-xv. https://doi.org/10.53730/ijhs.v5n3.2938