

# Assessment of Information Security Risk Management System based on ISO/IEC27005 in the Independent High Electoral Commission: A Case Study

Firas Raheem Younis Alazzawi<sup>1</sup>

College of Administration and Economics - University of Baghdad/Iraq

[Firas.alazzawi@coadec.uobaghdad.edu.iq](mailto:Firas.alazzawi@coadec.uobaghdad.edu.iq)

## Abstract

The current research aims to study the extent to which the Independent High Electoral Commission applies to information security risk management by the international standard (ISO / IEC27005) in terms of policies, administrative and technical procedures, and techniques used in managing information security risks, based on the opinions of experts in the sector who occupy positions (General Manager The directorate, department heads and their agents, project managers, heads of divisions, and those authorized to access systems and software). The importance of the research comes by giving a clear picture of the field of information security risk management in the organization in question because of its significant role in identifying risks and setting appropriate controls to manage or get rid of them, flexibility in setting controls at work and gaining the confidence of stakeholders and customers that their data is protected. Compliance with controls gives the organization the confidence of customers that it is the best supplier and raises the level of ability to meet the requirements of tenders and then get new job opportunities, which encouraged addressing this topic by focusing on the basic standards of this specification and trying to study these standards and identify the most critical problems that this prevents its application in the commission understudy in particular. The Independent High Electoral Commission/National Office in Baghdad was chosen as a site to conduct the research, and the approach of the case study and applied research was followed and through field coexistence, observations, interviews, access to documents and information extracted from records and documents in order to determine the extent of the gap between the Information Security Department of the commission in question and the system that the specification came with, analyzing the causes of the gaps and developing solutions, and considering the research was extended to the checklists prepared by the International Standardization Organization, and for the purpose of data analysis, the heptagonal scale was used in the checklists to measure the extent to which the implementation and actual documentation conform to the requirements of the specification, while determining the weights for the answers to the questions contained in the checklists by allocating a specific weight to each paragraph of the scale. The research used two statistical methods, the percentage and the weighted mean to express the extent of application and documentation of the specification paragraphs above and relied on the statement of the main reasons for surgery in the emergence of those gaps. The results that were reached showed several reasons that prevented the application of information security risk management, in the light of which treatments were developed that would reduce the gaps that appeared, the most important of which are: that the Commission did not adopt a clear and documented strategy to address risks, and that information security risk management ineffective and completely secured from external and internal threats. There was also interest in documenting fixed Hardware and portable Hardware represented by computers used at the headquarters of the directorate, servers and small computers used as workstations in divisions and departments and their connection to senior management, as well as laptops and personal digital assistants, which showed a gap attributed to the total undocumented application of Hardware (automatic data processing), processing accessories, and electronic media), while the application was partially and undocumented for other electronic media, including disk drives, printers, paper, and documents.

## Keywords

Information Security Risk Management System, ISO/IEC27005: 2018, the Independent High Electoral Commission.

**To cite this article:** Alazzawi F, R, Y. (2021). Assessment of Information Security Risk Management System based on ISO/IEC27005 in the Independent High Electoral Commission: A Case Study. Review of International Geographical Education (RIGEO), 11(5), 4633-4656. Doi: 10.48047/rigeo.11.05.339

**Submitted:** 07-11-2020 • **Revised:** 10-02-2021 • **Accepted:** 15-03-2021

## Introduction

The rapid growth in recent years in information and communication technology and the increasing pressures to reduce costs and improve quality in business performance and reduce errors that occur during the performance of the daily business has led to the increased use of computer information systems in public and private organizations. The current use of these systems has become a prerequisite for these organizations. A computer information system means any computer system that stores, stores, manages, and transmits personal and organizational information, according to the sector. Therefore, information security is one of the most critical challenges facing these systems, as the data and information of business processes stored in these systems are among the most confidential data, which requires protection. Recording electronic business process information exacerbates the risks of unauthorized access to and disclosure of data. The illegal disclosure of information leads to the occurrence of the affiliates of these organizations in serious problems. Computer information systems in organizations face various forms of internal and external threats that can cause various damages, as well as their negative impact on the organization's operations, information assets, individuals, organizations, and local research fields. Therefore, information security plays a critical role in the organization's continuity, reducing threats to its operations and protecting the confidentiality, transparency, and availability of information. The primary objective of information security is to adopt correct control procedures to eliminate or reduce the effects of various threats related to the security of the organization and organizational weaknesses. However, the main question is how to implement information security in organizations effectively and economically? The answer is Information Security Risk Management (ISRM). Information security risk management is a structured and continuous process aimed at diagnosing, assessing, and reducing some types of risks, as well as achieving an appropriate risk appetite. It is an essential element for the success of information security programs at the organization level for the following reasons. First, information security risks are characterized by their instability over time and their variation in the organization's circumstances, the degree of development of the information system, the changes it is going through, new users, and so on. It is one of the methods used to reduce the adverse effects of risks on the organization. Second, risk management provides organizations with the possibility to focus on the resources of high-risk areas and manage them using correct and measurable methods with reasonable risk reduction. Third: One of the elements of the success of the information security program is the cost-benefit analysis of the application of information security control. A risk management mechanism is used in carrying out this rigorous analysis. The Independent High Electoral Commission is one of the most critical state institutions because of its sensitive role in organizing fair elections that express the will of the people, given that the political rights of the citizen take the most attention, in addition to the seriousness of its role and the great responsibility placed on its shoulders. Therefore, ensuring the security of information in these systems is of fundamental importance in the Ministry. However, the computerized information systems of the organization concerned with the research have faced significant challenges in recent years, and to reduce the general costs of its activities, the reform plan has been implemented as part of its central policies. This required it to link its information systems programs, including its electronic records and entries, via the Internet. However, access to the public Internet dramatically increases the risk of unauthorized access to information. At the same time, some results proved that there are no specific rules about the confidentiality of its operations information in the electronic systems adopted in it. Also, the computer information system in Iraq, and because of the crises it is going through and security breaches, has been exposed in recent years to dangers within cyberspace. The research attempts to delve into the risks of information security in the organization concerned with the research. The importance of managing these risks in reducing and minimizing their effects, as well as the degree of effectiveness of information security programs, as well as the status of risk management in them, in order to provide the resulting results a comprehensive vision of the status of risk management and its role in policies Information security in the Independent High Electoral Commission, and will also assist researchers and policymakers interested in managing information security risks in the Commission. For the reasons mentioned above, which crystallized to give the starting point for conducting the current research, the research sought to answer the following questions: What is the extent of the application of international standards for information security and the methods, procedures, and methods of evaluating and upgrading them to a level that preserves rights and trust in the Directorate and its procedures? To what extent does the Commission own an information security management system and its compatibility with the information security risk management by the specification (ISO/ IEC27005: 2018), which in turn raises the level of its information security and then obtains the certificate of conformity to the aforementioned international standard from the donors? What is the size of the gap between the

actual reality of information security risk management in the Commission and information security risk management by the aforementioned international standard? This research was accomplished based on the case study method, as the necessary data and information were collected through field coexistence at the research site and the mechanism of work of its information systems, documents, It approved procedures, as well as conducting direct personal interviews with the relevant experts in the organization in question. The delegation, The researcher faced many challenges during carrying out the current research, including the difficulty of obtaining information and data from the organization under investigation for fear of confidentiality of information, the lack of sources and references and the difficulty of obtaining them, and finally, the limited period for the completion of the research, which amounted to three months, which led to an intensification of effort to complete the research.

## Methodology

### Research Problem

The present era is known as the information age and the era of absolute openness and transparency. As a result, protecting sensitive and precious information has become one of the most complex matters facing senior officials in the governmental and private sectors. When trying to implement traditional protection, it is costly and hinders the flow of business, and puts it in conflict with the current of progress and development that requires it to put all its information is saved on paper in computerized databases connected with other computers, which exposes its information to threats (malware, data leakage, hacking, data exposure, ... and others). Therefore, the reality of the information space has become unsafe because of the threats that organizations are exposed to, whether internal or external, which made them strive to adopt specific standards for information security policies, to draw up a methodology for applying the concept of information security, starting with identifying assets and analyzing the risks surrounding the organization and ending with the conclusion and extraction Security controls to reduce those risks. The International Organization for Standardization (ISO) has adopted a unified standard for defining and defining the management of information technology security, such as (ISO/IEC 13335), after which the "Implementation Guide for Information Security Management" (ISO/IEC17779) appeared, and other versions of these standards followed, namely the specification (ISO/IEC27005) whose focus was on information security risk management. The security risks and threats have shown in the weak adoption of the organization under consideration of the trends of information security risk management, including the international standard (ISO27005), as it faced many risks and threats when practicing its activities, which varied between fire and unauthorized procedures), information leakage and manipulation of its contents, as well as The absence of inclusion of clear policies and strategies for information security in its information systems, not to mention the shortcomings in the application of the security policies, followed in them. Based on the preceding, the following research problem can be formulated: What is the availability of international standards for managing information security risks and the methods, procedures, and methods for evaluating and upgrading them at a level that preserves rights and confidence in the Directorate and its procedures? What is the reality that the Commission under consideration possesses a management system for information security risks that is compatible with the information security risk management by the international standard (ISO/IEC27005), which in turn raises the level of its information security and obtains a certificate of conformity with the international standard (ISO/IEC27005) Who are the donors? What is the size of the gap between the actual reality of information security risk management in the researched directorate and information security risk management according to the international standard (ISO/IEC27005)? To what extent can proposed mechanisms be presented to reduce the gap between the reality of information security risk management in the Commission researched and the process of managing information security risks according to the aforementioned international standard? The answer to these questions will focus on the current research towards the interpretation and determination of the requirements associated with the mentioned specification.

### Research Importance

The importance of the research appears through its connection to an area of vital importance to society in general, and the Independent High Electoral Commission in particular, as well as an attempt to link the reality of information security risk management in the commission with the international standard (ISO/IEC27005) and is represented in the research's contribution to achieving scientific benefit

process through the following aspects: The research provides a new basis for information security risk management in the organization under study. The research represents an essential step towards the possibility of qualifying the researched organization for registration to grant a certificate of conformity to manage information security risks if it is made a mandatory specification by the International Organization for Standardization. They demonstrate the importance of managing information security risks for the directors of the Commission's departments by assuming a certain level of risk, analyzing risks, and mastering risk management techniques to avoid and avoid them before they occur and mitigate their severity. Identify the basic requirements to achieve the framework and the information security risk management process in the investigated commission according to the international standard (ISO/IEC27005).

## Research Objectives

The research aims to achieve the following objectives: Getting acquainted with the most prominent international standards for information security risk management and the methods, procedures, and methods for its evaluation Upgrading it to a level that preserves rights and confidence in the organization its procedures. Diagnosing the extent to which the commission under consideration possesses a management system for information security risks that is compatible with the management of information security risks according to the international standard (ISO/IEC27005) in preparation for the development of a curriculum and an action plan for the implementation of the international standard (ISO/IEC27005) in the commission in question, and then obtaining Conformity certificate from donors—diagnosing the gap between the actual reality of information security risk management in question and the requirements of information security risk management by the international standard (ISO/IEC27005) by not conforming to the requirements, which helps to achieve compatibility with them to reduce that gap as much as possible. Develop proposed mechanisms to reduce the gap between the reality of information security risk management in the research commission and the information security risk management process by the aforementioned international standard.

## Research Method

In a case study method, through field experience, observations, interviews, documents, and information obtained from records and documents, the researcher was able to determine the extent of the gap between the Information Security Department in the Independent High Electoral Commission/National Office and the system that the specification came with, analyzing the causes of the gaps and developing solutions.

## Literature Review

### The nature of information security risk management and related terminology

In some cases, the word "risk" means "threat" or vice versa. In other words, either of the words "risk and threat" may replace the other without changing the meaning for people who are not specialized in information security. The terms "vulnerability", "threat and danger", and "vulnerability" may be used to express the same thing, although they each have a different meaning in information security science, and none is a substitute for the other. Therefore, before starting the study of information risk management, it is necessary to define each of these terms accurately and know its meaning and the relationship it has with other terms.

### Vulnerability

It does not mean the possibility of a risk occurring, but rather the degree of weakness or defect in the information system, which can be exploited to cause damage to the system. Damage to the system. In other words, it is the three-dimensional relationship between the expected damage, the endangered asset, and the risk itself (Dunlop, Chechak, Hamby & Holosko, 2021). Among the weaknesses are the following: Loss of maintenance program documentation due to theft due to weak use controls. The loss here is the damage that occurred, and documenting the lost program is the original at risk, theft is the same risk, and the weakness of user controls is the degree of exposure. Adjusting the balance in an account in one of the institutions through illegal intervention to implement

a transaction, the account is damage that occurs due to the lack of controls Secure the traffic of messages in the network. Adjusting the balance here is the damage that occurred, the account is the asset at risk, and illegal interference is the risk. The lack of controls to secure the passage of messages in the network is the degree of exposure. Backup tapes lost the database for notifying stores in a fire accident is damage that occurs due to insufficient Emergency plans Damage here is the loss of tapes, backup tapes and perhaps the database itself is the original at risk, and the risk, of course, is fire. The degree of exposure is the inadequacy of emergency plans, a service, or a small program that is not secured on one of the central servers and can be exploited by programs Intrusion An operating system or application software that is out of date with the latest security updates Unspecified. Insecure WAN connectivity Open ports in firewalls Lax physical protection, whether centralized or administrative, allows anyone to enter data centers and regions. Sensitive, automated, or weak passwords are used to access servers and network peripherals (Szczepaniuk, Szczepaniuk, Rokicki, & Klepacki, 2020). Here, it can be said that in order to calculate the degree of exposure accurately, the assets and areas of risk in the organization must be examined, and interviews should be conducted with managers and employees who are familiar with the daily procedures and operations that are implemented in the organization. The organization presents a great deal with the risks that were previously identified in the stage of identifying the potential risks. Appropriate countermeasures must be taken to protect the organization's assets, which we call risk management, and reduce its impact.

### **Threat**

Any object or component that constitutes a potential exposure to information or systems. In other words, it is any person or tool that identifies a point of weakness, such as any of the previous weaknesses, and then uses it against the organization or another person. 2015), and among the manifestations of the threat are the following: an intruder who can enter the network through one of the firewall ports, a process or program that can access data in violation of information security policies, various natural threat sources, an employee who makes fatal mistakes that lead to the disclosure or corruption of confidential data.

### **Risk**

The risk that a threat agent will exploit a vulnerability and then penetrate through it. The more ports a firewall has open, the more likely it is that an intruder will exploit one of these ports and illegally enter the network through it. The more the employee is not trained in the processes and procedures, the more likely he will commit critical errors that lead to data loss or destruction (Szczepaniuk et al., 2020). Then it cannot be avoided, and accordingly, it can be said that danger is the link between weakness, threat, and exploitation of existing loopholes on the one hand and the resulting impact on work on the other hand (Miloslavskaya & Tolstoy, 2019). Which can categorize intrusion detection methodologies into three main categories: signature-based detection, anomaly-based detection, and formal protocol analysis (Liao, Lin, Lin, & Tung, 2013)

### **Exposure Data**

A condition of exposure to a loss situation caused by a threat factor. In the event of vulnerability, the organization will be exposed to possible loss or destruction of data, and in the event of lax protection and management of password databases, users' passwords will be vulnerable to capture and then used in illegal ways. If the organization does not use fire detection and prevention systems and put the necessary measures to combat it, it will be vulnerable to the outbreak of a devastating fire (Szczepaniuk et al., 2020). The main concern of any organization should be its data, as it is often a unique resource. Data collected over time can rarely be remembered in the same way, even when this process can be costly and time-consuming. Be careful with applications, especially if the applications are not tailored, and they should come in second place. All data and applications are vulnerable to failure, damage, and theft. While the culprit in hardware destruction is often a natural disaster or spike force, the culprit in software damage is almost always human (Murdoch, 2010).

### **Safeguard**

The existence of different types of dangers and at the same time that many means of protection require the existence of information security management so that it can draw up security policy and

follow up on implementation procedures, as well as evaluate current protection means and fill security gaps so that applications enjoy reliability by the beneficiaries and accuracy in carrying out works (Miloslavskaya & Tolstoy, 2019). Examples of protection include: having strict password management, having security guards for critical and sensitive areas, implementing an access control mechanism at the operating system level, using passwords at the BIOS level, training, and raising information security. The theoretical arrangement of these concepts shows that the presence of the threat factor allows the threat to exploit the existing weakness, which leads to the existence of danger, and the presence of risk harms the resources of the organization, causing the organization to lose. This is countered by the protection system, which is supposed to affect the presence of the threat factor directly. Among this logical order to evaluate these concepts when applied in the organization is the following order: threat, exposure to loss, weakness, antagonists, and finally, danger. The reason for this is that there may be a threat, but the organization will not be subject to lose as long as there is no weakness that can be exploited by the threat factor, and if there is a particular weakness (which is possible), the protection system must be used to confront the risk or reduce its effects. Finally, applying the appropriate protection system will eliminate vulnerability and exposure to loss and thus reduce the risk. It is well known that threat factors cannot be eliminated, but they can be prevented from exploiting vulnerabilities and penetrating through them. When addressing information security risk management, we discover that "risk management" is used in many disciplines and professions. Risk and risk management have been studied in various fields, such as insurance, economics, management, medicine, operations research, engineering, etc., and the list is long. Each field deals with risks in a way that is related to the topic of analysis and then adopts a particular point of view (Aubert, Patry, & Rivard, 2005). This reflects the increasing trend of applying risk management mechanisms in many disciplines and professions, including IT applications. Risk management is an activity directed towards assessing, mitigating, and monitoring risks. Risk management helps answer questions such as whether passing a new database update will increase the chances of vulnerability, whether that secure email system needs to be implemented, and whether purchasing the latest intrusion detection technology will reduce the likelihood that a web server will be compromised. It will successfully attack (Baryannis, Validi, Dani, & Antoniou, 2019). Risk management also represents the process of measuring and evaluating risks and developing strategies to manage them. These strategies include transferring risks to another party, avoiding them, reducing their causal effects, and accepting some or all of their consequences. In addition, it is the administrative activity that aims to control risks and reduce them to acceptable levels. More precisely, it is the process of determining the risks facing the organization, their measurement, reduction, and control (Kharytonov, Kharytonova, Tolmachevska, Fasii, & Tkalych, 2019). From the preceding, it can be said that risk management helps to prioritize issues. The organization prioritizes knowing the most critical issues and handing over the available resources to the most critical area first. It can be very beneficial if the organization has limited resources and cannot address all risk areas immediately and simultaneously. As for information security, it is the organization's entrance to managing and implementing information security such as (controlling the objectives, controls, policies, processes, and procedures of information security independently at the planned times or when significant changes occur in the implementation of security) (Peltier, 2005). Information security is a requirement because technology applied to information may create risks. In general, information may be incorrectly disclosed (i.e., its confidentiality may be compromised), inappropriately modified (i.e., its integrity may be compromised), destroyed, or lost (i.e., its availability may be compromised) (Blakley, McDermott, & Geer, 2001). Effective risk management is also essential to obtaining certification (ISO27001) and maintaining and improving the Information Security Management System (ISMS). The (ISO27001) certification clearly states that the information security management system must comply with the context of the strategic risk management of the organization, and establish criteria by which risks are assessed" and "identify the risk assessment methodology compatible with (Luke, 2019). (ISMS) Information security risk management is characterized as a structured and continuous process aimed at diagnosing, evaluating, and reducing some types of risks, as well as achieving reasonable acceptability of risks. It is an essential component of the success of information security programs at the organization level because information security risks are not stable over time and vary according to the conditions of the organization, the degree of development of the information system, the changes it is going through, new users, and so on. It is one of the ways used to reduce the adverse effects of risks on the organization. Risk management provides organizations with the ability to focus on the resources of high-risk areas and manage them using correct and measurable methods while reducing risks reasonably. In addition, one of the elements of the success of the information security program is the analysis and utility of the application of information security control. The risk management mechanism is used to implement this accurate cost analysis (Zarei & Sadoughi, 2016).

The information security risk management process can be defined by the international standard (ISO27001) in four stages: Plan, act, check and execute. Information Security Risk Management (ISRM) can support an Information Security Management System (ISMS). There is also a similarity between the method of information security risk management and the information security management system (Setiawan, Putra, & Pradana, 2017), as shown in Table (1).

**Table (1)**

The compatibility of the information security management system with the information security risk management process

No.	Information security management (ISM)	Information security risk management (ISRM)
1	Plan	Establishing the Context, Risk Assessment, Developing a risk treatment plan, Risk Acceptance
2	Do	Implementation of risk treatment plan
3	Check	Continual monitoring and review of risks
4	Act	Maintain and improve the information security risk management process

Source: Setiawan et al. (2017)

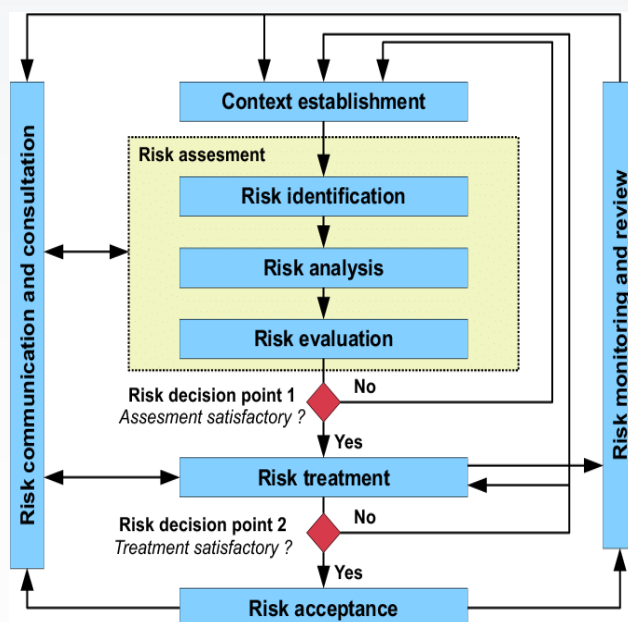
### Information security risk management objectives

Computer information systems in organizations face various forms of internal and external threats that can cause various damages, as well as their negative impact on the organization's operations, information assets, individuals, organizations, and local research fields. Therefore, information security plays a crucial role in the organization's continuity, limiting threats to its operations and protecting the confidentiality, transparency, and availability of its information. The main objective of the Information Security Department is to adopt correct control procedures to eliminate the effects of various threats related to the security of the organization and organizational weaknesses or to work to reduce them (Zarei & Sadoughi, 2016) and to ensure that the organization discovers and identifies information security risks related to information systems. It has to consider the threats and weaknesses experienced by those systems and the impact of this on the work management. The organization also plans to take appropriate initiatives to address the information security risks that have been identified, as well as to address the continuing risks to the information being processed by the organization, as these risks should be addressed by the organization's risk management policy. Achieving the information above security objective depends on the elements: an information security risk management methodology; Information Security Risk Management Policy and Procedures; Information Security Risk Management Process, and Information Security Risk Management Entities (Kiura & Mango, 2017). From the preceding, it can be said that information security risk management presents various objectives, steps, structures, and levels of application. Moreover, information security management includes not only technical, social, and economic aspects but also the prevailing security systems that are relative and depend on the environment in which they are located. Here the process of managing information security risks must be used in the organization as a whole, and any separate part of the organization (such as an administrative unit, physical location or service) or in any information system, existing or planned, or certain aspects of control (such as business continuity planning).

### Information security risk management process

Figure (1) shows how this International Standard applies this risk management. The information security risk management process consists of context establishment (Clause 7), risk assessment (Clause 8), risk treatment (Clause 9), risk acceptance (Clause 10), risk communication and consultation (Clause 11), and risk monitoring and review (Clause 12). As Figure (1) illustrates, the information security risk management process can be iterative for risk assessment and/or risk treatment activities. An iterative approach to conducting risk assessment can increase the depth and detail of the assessment at each iteration. The iterative approach provides a good balance between minimizing the time and effort spent in identifying controls while still ensuring that high risks are appropriately assessed. The context is established first. Then a risk assessment is conducted. If this provides sufficient information to effectively

determine the actions required to modify the risks to an acceptable level, the task is complete, and the risk treatment follows. If the information is insufficient, another iteration of the risk assessment with revised context (e.g., risk evaluation criteria, risk acceptance criteria, or impact criteria) will be conducted, possibly on limited parts of the total scope (see Figure 1, Risk Decision Point 1) (ISO27005: 2011). The effectiveness of the risk treatment depends on the results of the risk assessment. It is possible that the risk treatment will not immediately lead to an acceptable level of residual risk. In this situation, another iteration of the risk assessment with changed context parameters (e.g., risk assessment, risk acceptance, or impact criteria), if necessary, may be required, followed by further risk treatment (see Figure 1, Risk Decision Point 2).



**Figure (1)** Information security risk management process

**Source:** ISO/IEC 27005: 2018, "International Standard Information technology- Information technology - Security techniques - Information security risk management" (3rd ed.), Geneva: ISO Copyright Office. P. (4).

The risk acceptance activity has to ensure residual risks are explicitly accepted by the managers of the organization. This is especially important when the implementation of controls is omitted or postponed, e.g., due to cost. During the information security risk management process, risks and treatment must be communicated to the appropriate managers and operational staff. Even before the treatment of the risks, information about identified risks can be precious to manage incidents and may help to reduce potential damage (ISO27001: 2013). Awareness by managers and staff of the risks, the nature of the controls in place to mitigate the risks, and the areas of concern to the organization assist in dealing with incidents and unexpected events in the most effective manner. The detailed results of every activity of the information security risk management process and from the two risk decision points should be documented (ISO27005: 2011). There are different methodologies for managing information security risks and approaches to analysis) some of which are qualitative, others are in nature. However, these methodologies have a common goal of estimating the value of the overall risk. Information Security Risk Management (ISRM) is not a new area of research. Other mechanisms have been used for some time. Since 1975, Annual Loss Expectancy- ALE has been proposed by the US National Bureau of Standards for measuring IT risk. These forecasts were fundamental, as it was not possible to distinguish between the high or low impact of events. However, after a series of workshops in the 1980s by the US National Bureau of Standards, annual loss forecasts evolved into an iterative process of information security risk management with steps The following are: Requirement's definition, threat analysis, risk measurement, acceptance testing, protection and implementation (Alshareef, 2016). There are also many risks management approaches available, such as (OCTAVE) and (CORAS), which are used in analyzing the risks of qualitative information for information security and information technology. At the same time, quantitative methodologies for information security risk analysis, such as MyRAM and HiLRA, and other relevant risk assessment methods for information security risk management are available. Such as event tree analysis, failure mode and impact analysis, potential risk assessment, human error



analysis, and finally, risk and operation (Khidzir, Mohamed, & Arshad, 2010). Information security risk management consists of six general processes, which are risk identification, analysis, treatment plan, implementation of the treatment plan, and follow-up and control. As shown in Table (2), the practical description of the general process of information security risk management is based on a review of previous studies and literature.

**Table (2)**

Generic Information Security Risk Management Processes and Task Descriptions

No.	Information Security Risk Management Processes	Task/ Action Descriptions
1	Risk Identification	<ul style="list-style-type: none"> <li>• Identify Critical Information Assets</li> <li>• Identify Threats and Vulnerabilities to Critical Information Assets</li> <li>• Identify Security requirements s for Critical Information Assets</li> <li>• Identify Current Security Policies, Practices, and Procedures</li> <li>• Identify Current Technology Vulnerabilities and Threats</li> <li>• Identify Current Organizational Vulnerabilities and Threats</li> <li>• Analyze value for information security risks probability and impact to an organization's ICT services (Evaluate Information Risks).</li> </ul>
2	Risk Analysis	<ul style="list-style-type: none"> <li>• Analyze which risk need to be addressed based on the nature and the organization's general tolerance for information risk (Prioritize Risk and Mitigation Approach)</li> <li>• Develop Protection Strategy (Security Related-practices)</li> <li>• Develop Risk Mitigation Plan (Plan to reduce risks to organization's critical information assets and ICT Services)</li> </ul>
3	Risk Treatment Plan	<ul style="list-style-type: none"> <li>• Develop Action Plan by specifying a set of actions for protection strategy and risk mitigation plan (Action plan, budget, schedule, success criteria, measures to monitor plans, human-resource required to implement action plan)</li> </ul>
4	Risk Treatment Plan Implementation	<ul style="list-style-type: none"> <li>• Execute all action plans according to the schedule and success criteria (as defined in Risk Treatment Plan)</li> <li>• Reprioritize work tasks and schedule to incorporate an action plan (if necessary)</li> <li>• Measures the status of an action plan concerning their schedules and success criteria (Monitor of the progress of action plan)</li> </ul>
5	Risk Monitoring	<ul style="list-style-type: none"> <li>• Indicates the presence of new risks or significant changes to existing risks</li> <li>• Analyzed data tracking of an action plan</li> <li>• Analyzed data tracking of key risk indicators</li> </ul>
6	Risk Control	<ul style="list-style-type: none"> <li>• Decision on changes to an action plan</li> <li>• Decision on identifying new risks</li> <li>• Execute control decision into action</li> <li>• Start of the new risk identification task</li> </ul>

**Source:** Khidzir et al. (2010)

## Results and Discussions

### Gaps analysis of the requirements of the international standard ISO/IEC27005 and the possibility of its application in the Independent High Electoral Commission

With the increasing exposure of organizations to information security threats, decision-makers are constantly forced to pay attention to security issues. Information security risk management provides methods for measuring security by identifying risks, mitigating risks, and assessing risks. Despite proposing a variety of approaches, decision-makers lack Techniques based on sound foundations that show them what they are getting for their investment, as well as whether their investment is effective and does not require deep knowledge in the field of information technology security, and this is what this

paragraph will try to address.

### Graphical representation of matching ratios

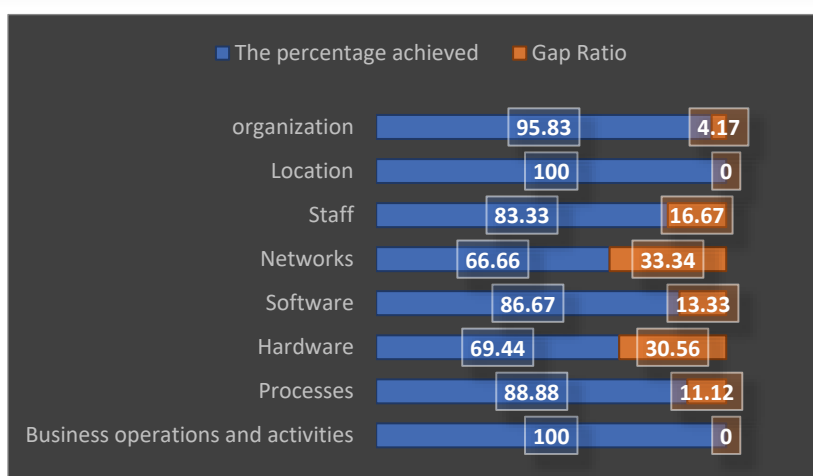
Based on the results of the checklist that showed the level of application and documentation of the requirements of the international standard (ISO/IEC27005), the results of the weighted arithmetic mean (the average) and the percentage of conforming to the main requirements of the international standard will be indicated, as in Table (3).

**Table (3)**

Results of the level of application and documentation of the requirements of the International Standard (ISO/IEC27005) related to the primary and supporting assets of the Independent High Electoral Commission

No.	Requirements according to the addresses on the standard (ISO / IEC27005: 2018)		Ratings for the application of the overall documentation		
	Requirement No.	Requirement Name	achieved degree	The percentage achieved	Gap Ratio
1	B.1.1.1	Business operations and activities	6	100	0
2	B.1.1.2	Processes	5.33	88.88	11.12
3	B.1.2.1	Hardware	4.16	69.44	30.56
4	B.1.2.2	Software	5.2	86.67	13.33
5	B.1.2.3	Networks	4	66.66	33.34
6	B.1.2.4	Staff	5	83.33	16.67
7	B.1.2.5	Location	6	100	0
8	B.1.2.6	organization	5.75	95.83	4.17
9	Total gross for the evaluation results achieved			690.81	109.19
10	The upper limit of the application and complete documentation of the requirement			41.44	100
11	The total sum assumed for the application and complete documentation			6	800
12	The amount of the gap in the application & documentation of the total requirements			48	690.81
13	The percentage of the overall results			6.56	13.64

Table (3) shows that the percentage of the total results of the checklists (primary assets, supporting assets, and their details) has achieved an application and documentation ratio of (86.36%), which is a perfect percentage. However, the non-implementation gap percentage is (13.64%), which prevented achieving a percentage of Full match and documentation.



**Figure (2)** The results of the level of application, documentation, and gaps for the two requirements of information security risk management according to the international standard (ISO/IEC27005) and related to the primary and supporting assets in the Independent High Electoral Commission

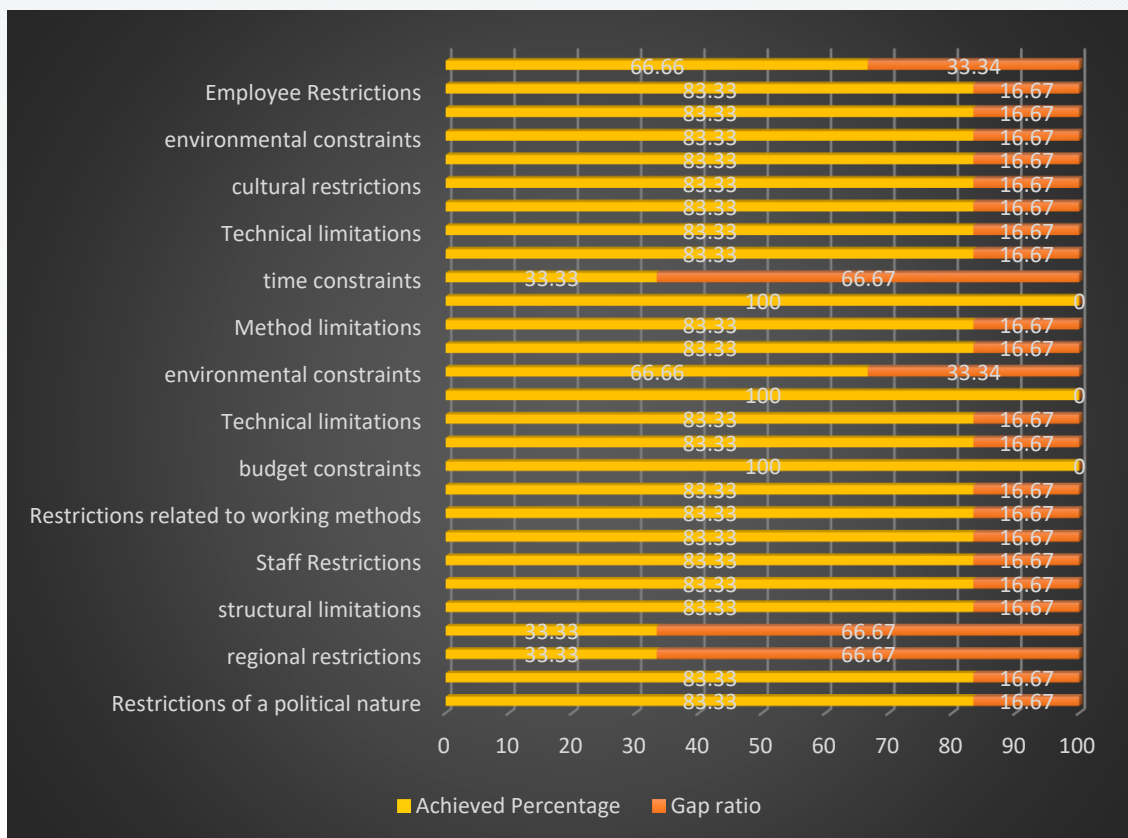
It is clear from Figure (2) that the percentage of application and documentation for all requirements was excellent. However, the reasons for the gap were all requirements that prevented the application and complete documentation of the requirements of the international standard, as the highest gap is in the requirement (B.1.2.3) at a rate of (33.34%), and ends with the two requirements (B.1.1.1, B.1.2.5), which obtained the minor gap with a matching percentage (100%).

**Table (4)**

The results of the application and documentation levels of the constraints of the requirements of the standard (ISO/IEC27005) in the Independent High Electoral Commission

No.	Requirements addresses by (ISO/IEC27005)		Assessment grades for actual application and documentation		
	Requirement No.	Requirement Name	achieved degree	Achieved Percentage%	Gap ratio%
1	A.2.1	Restrictions of a political nature	5	83.33	16.67
2	A.2.2	limitations of a strategic nature	5	83.33	16.67
3	A.2.3	regional restrictions	2	33.33	66.67
4	A.2.4	Constraints arising from the economic and political climate	2	33.33	66.67
5	A.2.5	structural limitations	5	83.33	16.67
6	A.2.6	functional limitations	5	83.33	16.67
7	A.2.7	Staff Restrictions	5	83.33	16.67
8	A.2.8	Constraints arising from the organization's agenda	5	83.33	16.67
9	A.2.9	Restrictions related to working methods	5	83.33	16.67
10	A.2.10	cultural restrictions	5	83.33	16.67
11	A.10.11	budget constraints	6	100	0
12	A.4.1	Restrictions arising from pre-existing operations	5	83.33	16.67
13	A.4.2	Technical limitations	5	83.33	16.67
14	A.4.3	financial constraints	6	100	0
15	A.4.4	environmental constraints	4	66.66	33.34
16	A.4.5	time constraints	5	83.33	16.67
17	A.4.6	Method limitations	5	83.33	16.67
18	A.4.7	regulatory restrictions	6	100	0
19	9.2.1	time constraints	2	33.33	66.67
20	9.2.2	financial constraints	5	83.33	16.67
21	9.2.3	Technical limitations	5	83.33	16.67
22	9.2.4	operational limitations	5	83.33	16.67
23	9.2.5	cultural restrictions	5	83.33	16.67
24	9.2.6	ethical constraints	5	83.33	16.67
25	9.2.7	environmental constraints	5	83.33	16.67
26	9.2.8	Legal restrictions	5	83.33	16.67
27	9.2.9	Employee Restrictions	5	83.33	16.67
28	9.2.10	Limitations of merging new and existing controls	4	66.66	33.34
Total gross for the assessment results achieved			132	2199.91	600.09
The maximum application and complete documentation of the requirement			6	100	100
The total sum assumed for the application & complete documentation			168	2800	2800
The amount of the gap in the application & documentation of the total requirements			36	600.09	2199.91
The percentage of overall results				78.57	21.43

It is noted from Table (4) that the percentage of the total results of the checklists (restrictions affecting the organization and the scope of information security and the modification of risks), has achieved a percentage of application and documentation of (78.57) and a percentage of non-application gap of (21.43) which is a good percentage. However, we must take into account Taking into account the percentage of the gap achieved and working to bridge it. Through the results of Table (3) and (4), the third question has been answered in the research problem, which includes what the size of the gap between the actual reality of information security risk management in the researched directorate and information security risk management is according to the international standard (ISO/IEC27005)?



**Figure (3)** The results of the level of application, documentation, and gaps for the constraints of information security risk management requirements according to the international standard (ISO/IEC27005) in the Independent High Electoral Commission

It is clear from Figure (3) that the percentage of application and documentation for all requirements was good. However, the reasons for the gap for each requirement prevented the application and complete documentation of the requirements of the international standard, as the highest gap is in the requirements (A.2.3, A.2.4, 9.2.1) with a percentage of (66.67), and ends with demands (1.2.11, A.4.3, A.4.7), which got the tiniest gap and with a matching percentage (100%).

**Use Pareto to analyze results**

The Pareto chart is known as (20:80) analysis, meaning the “most influential few” versus the ineffective majority. To perform the Pareto analysis, the data obtained from the checklists must be configured as follows:

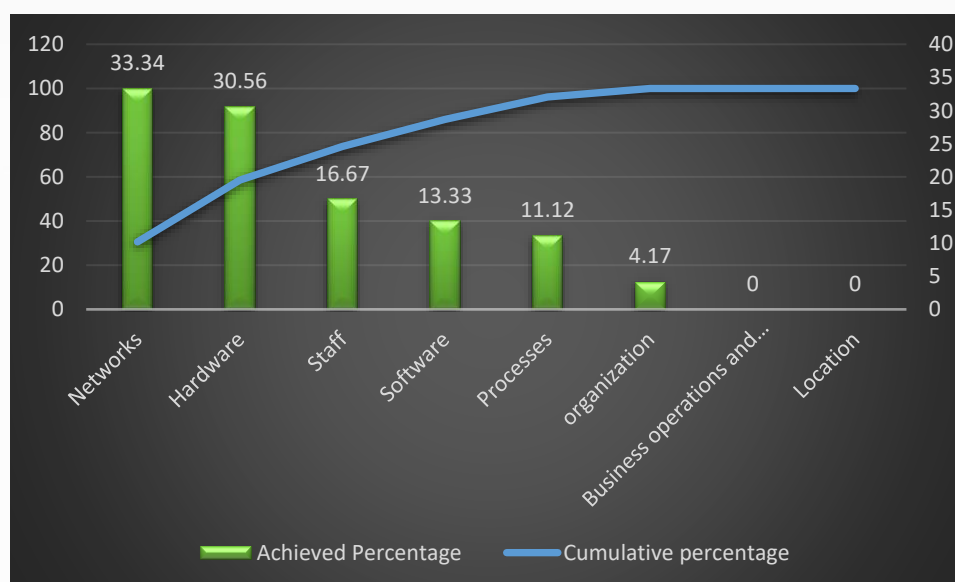
- 1- Arranging the results of the gap ratio for the checklists and for each specification requirement in ascending order.
- 2- Collect the results of the gap ratio and for each specification requirement.
- 3- Extracting the modified percentage using the law (whole part \* 100)
- 4- Extracting the cumulative percentage by taking the value of the modified percentage for the first requirement and counting it the cumulative percentage for the exact requirement, then the cumulative percentage for the second requirement will be from the sum of the cumulative percentage for the first requirement + the gap ratio for the second requirement). Thus the

cumulative percentage is calculated for the rest of the requirements. Through these procedures, the results are as shown in Table (5).

**Table (5)**

Preparing the results of the primary and supporting assets checklists for Pareto analysis

No.	Requirement No.	Requirement Name	achieved degree	Adjusted percentage	Cumulative percentage
1	A.2.1	Networks	33.34	30.53393168	30.53393168
2	A.2.2	Hardware	30.56	27.98791098	58.52184266
3	A.2.3	Staff	16.67	15.26696584	73.7888085
4	A.2.4	Software	13.33	12.20807766	85.99688616
5	A.2.5	Processes	11.12	10.18408279	96.18096895
6	A.2.6	organization	4.17	3.819031047	100
7	A.2.7	Business operations and activities	0	0	100
8	A.2.8	Location	0	0	100
Total gross for the assessment results achieved			109.19	100	



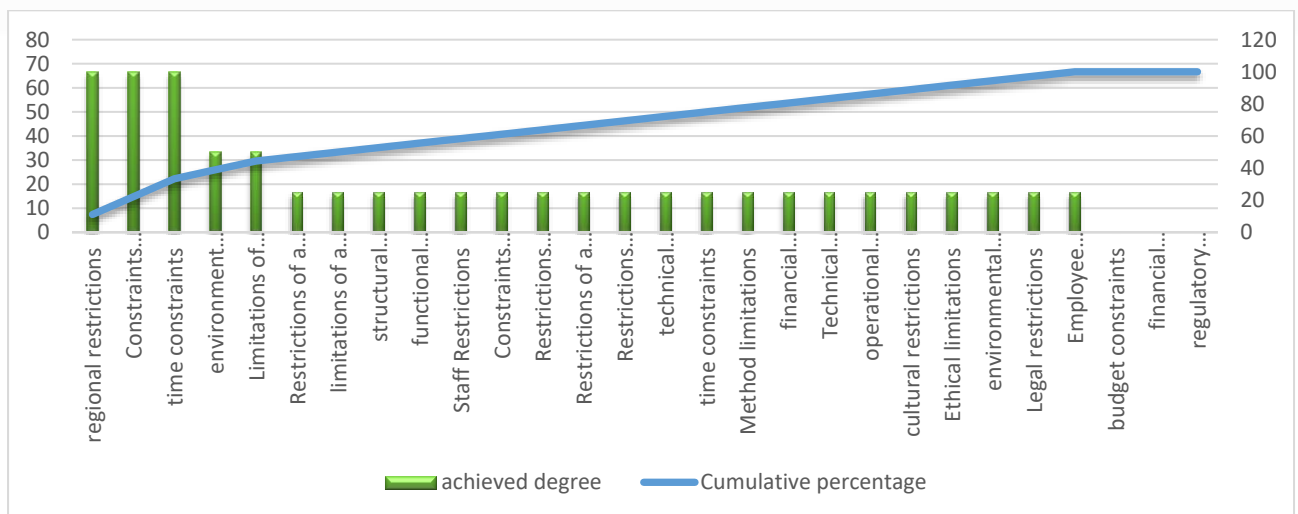
**Figure (4)** Pareto analysis of the gap level of the checklists of primary and supporting assets in terms of identifying the most influential minority in the Independent High Electoral Commission

It can be seen from Figure (4) that the highest gap percentage was achieved in the requirement (B.1.2.3) at a rate of (33.34%), and it ends with the lowest gap percentage that was achieved in the requirement (B.1.2.5) and at a rate of (0%), that is, the application and complete documentation for the requirement.

It is noted from Figure (5) that the highest gap ratio was achieved in the requirement (1.2.3) with a percentage of (66.67), and it ends with the lowest gap percentage that was achieved by the requirement (A.4.7) and at a rate of (0%), that is, the application and complete documentation of the requirement.

**Table (6)**  
Initializing Constraint Checklist Results for Pareto Analysis

No.	Requirement No.	Requirement Name	achieved degree	Adjusted percentage	Cumulative percentage
1	A.2.3	regional restrictions	66.67	11.11000017	11.11000017
2	A.2.4	Constraints arising from the economic climate	66.67	11.11000017	22.22000034
3	9.2.1	time constraints	66.67	11.11000017	33.33000051
4	1.4.4	environment restrictions	33.34	5.555833292	38.8858338
5	9.2.10	Limitations of merging new and existing controls	33.34	5.555833292	44.44166709
6	A.2.1	Restrictions of a political nature	16.67	2.777916646	47.21958374
7	A.2.2	limitations of a strategic nature	16.67	2.777916646	49.99750039
8	A.2.5	structural limitations	16.67	2.777916646	52.77541703
9	A.2.6	functional limitations	16.67	2.777916646	55.55333368
10	A.2.7	Staff Restrictions	16.67	2.777916646	58.33125032
11	A.2.8	Constraints arising from the organization's agenda	16.67	2.777916646	61.10916697
12	A.2.9	Restrictions related to working methods	16.67	2.777916646	63.88708362
13	A.2.10	Restrictions of a cultural nature	16.67	2.777916646	66.66500026
14	A.4.1	Restrictions arising from pre-existing operations	16.67	2.777916646	69.44291691
15	A.4.2	technical limitations	16.67	2.777916646	72.22083355
16	A.4.5	time constraints	16.67	2.777916646	74.9987502
17	A.4.6	Method limitations	16.67	2.777916646	77.77666684
18	A.4.3	financial constraints	16.67	2.777916646	80.55458349
19	9.2.3	Technical limitations	16.67	2.777916646	83.33250013
20	9.2.4	operational limitations	16.67	2.777916646	86.11041678
21	9.2.5	cultural restrictions	16.67	2.777916646	88.88833343
22	9.2.6	Ethical limitations	16.67	2.777916646	91.66625007
23	9.2.7	environmental constraints	16.67	2.777916646	94.44416672
24	9.2.8	Legal restrictions	16.67	2.777916646	97.22208336
25	9.2.9	Employee Restrictions	16.67	2.777916646	100
26	A.2.11	budget constraints	0	0	100
27	9.2.2	financial constraints	0	0	100
28	1.4.7	regulatory restrictions	0	0	100
Total			600.09	100	



**Figure (5)** Pareto analysis of the gap level of constraints identifies the most influential minority in the IHEC.

**Table (7)**

The primary and possible secondary reasons for the gap of the International Standard (ISO/IEC27005:2018)

No.	The main reasons	secondary reasons
1	Absence or lack of technology	Not keeping pace with technological development Weak provision of Hardware and supplies Poor provision of financial allocation
2	Absence of trained staff	Weak staff training Weakness in the provision of resources
3	Limited participation of senior management	Weakness inefficiency lack of awareness Weakness in the communications
4	Lack of accident detection	Weaknesses in the monitoring, measurement, analysis, and evaluation process Weakness in the audit of the information security system
5	Weak organizational ability to respond to security threats	Weakness in handling information security risks Underestimation of information security risks Weakness in the distribution of responsibilities and regulatory authorities
6	Insufficient support for the Independent High Electoral Commission	Weakness in the allocation of resources Weakness in the follow-up
7	Absence of a culture of compliance (strategic goals and business practices)	Not to put information security goals and plans to achieve Underestimation of information security risks Weak adoption of risk and opportunity targeting procedures

Notes from a table (7) Some of the reasons the primary and secondary gap, lack of application and documentation of the requirements of the International Standard (ISO / IEC27005: 2018) which starts from the absence or lack of technology and ending in the absence of a culture of compliance (strategic goals and work practices).

### Assessing and addressing information security risks

The information security risk assessment identifies and diagnoses the related threats and weaknesses that exist (or likely exist) and reveals the potential consequences, and finally prioritizes the derived risks and classifies them according to the risk assessment rules specified in the international standard (ISO / IEC27005: 2018) and as follows:

### The matrix of quantitative and descriptive analysis of the potential impact risks




The risk is measured by multiplying the impact of each threat with the probability of its occurrence, and the result is compared with the matrix shown below, as the matrix classifies the risk from low to medium to high, to determine the priority of the risks that need treatment, and then choose the appropriate method to address it.

**Table (8)**

Quantitative and descriptive risk analysis matrix (probability effect matrix)

Probability	0.90	0.72	0.63	0.45	0.27	0.09
	0.70	0.56	0.49	0.35	0.21	0.07
	0.50	0.40	0.35	0.25	0.15	0.05
	0.30	0.24	0.21	0.15	0.09	0.03
	0.10	0.08	0.07	0.05	0.03	0.01
		0.80	0.70	0.10	0.30	5

**Impact**

-  The threat is high and must be closely monitored by the administration.
-  The threat is moderate and should be followed up by the project manager.
-  The threat is weak and must be followed up by the staff.

**Table (9)**

Threat classification (physical damage) to measure the risk using the (impact-probability) matrix

Threat type	Threat Name	Impact (I)	Probability (P)	Danger (I*P)	Threat class
material damage	Fire	0.7	0.3	0.21	M
	Water damage	0.3	0.3	0.09	M
	Pollution	0.1	0.5	0.05	L
	Big accident	0.7	0.3	0.21	M
	Destroy Hardware or media	0.7	0.3	0.21	M
	Dust, corrosion and freezing	0.5	0.3	0.15	M

It is clear from the results of Table (9) regarding the type of threat (physical damage) that the highest impact ratio was (fire, major accident, destruction of Hardware and media) with an impact ratio (0.7), respectively, while the impact ratio of dust, corrosion and freezing was (0.5), while The effect of damage due to water was (0.3), and finally it was the lowest impact rate of pollution with a value of (0.1), while at the level of probability, the pollution got the highest probability value (0.5), as for (fire, damage due to water, major accident, destruction of Hardware and media, Dust, corrosion and freezing) respectively, they all got a probability of (0.3), as for the level of risk, it got (fire, major accident, destruction of Hardware and media) in the first order and with a rating of (medium threat), as the researcher believes that this percentage of danger It is attributed to its significant impact on the Commission, as it affects construction, assets, Hardware, media and documents, while the second rank was dust, corrosion and freezing, with a risk ratio of (0.15), which made the classification (threat medium), as the researcher believes that this percentage was affected by the value of the impact of the damage caused by corrosion. Documents, documents, hardware, and Hardware obsolescence, and the impact of dullness as for water damage, ranked third, with a risk ratio (0.09), and a medium threat category, as the impact and probability are equal as a result of the precautions and controls in the construction of the commission building and the laying and draining of water pipes as they are visible and monitored. In order to be suitable for human consumption, the pollution came in the last order with a risk ratio (0.05) and a low threat category, as it is noted that the probability of pollution is high while its impact is low, as the probability of pollution is caused by conditions outside the control of the Commission (such as water pollution, exhaust emissions, ... etc.).

**Table (10)**

Classification of threats (natural events) to measure the risk using the (impact-probability) matrix

Threat type	Threat Name	Impact (I)	Probability (P)	Danger (I*P)	Threat class
natural events	climatic phenomenon	0.5	0.3	0.15	M
	seismic phenomenon	0.3	0.1	0.03	L
	Pollution	0.3	0.1	0.03	L
	volcanic phenomenon	0.1	0.3	0.03	L
	meteorological phenomenon	0.7	0.3	0.21	M
	Flood	0.5	0.3	0.15	M

It is clear from Table (10) regarding the type of threat (natural events), which are attributed to threats that humans can only intervene in or foresee in a few. In terms of the impact of natural events, floods took the lead, as the flood got the first order with an impact ratio (0.7) of Where the effect is due to



the destruction it brings to the commission's infrastructure, furniture, documents, and computers. In contrast, the second rank was the impact of the climatic phenomenon, such as high temperature in summer and very cold in winter, at a rate of (0.5), while the third rank was in the level of influence of earthquakes and volcanoes phenomena, stemming from the fact that Iraq is outside the scope of Iraq. The effect, while in the last order, the effect of the meteorological phenomenon was at a rate of (0.1), while the probability of the occurrence of natural events was at a rate of (0.3) for climatic phenomena, meteorology, and flooding, respectively, while the second-order of seismic and volcanic phenomena was at a rate of (0.1), either the level of The risks of natural events were at the forefront of floods with a classification of (medium threat), the level of severity of climatic phenomena on the Commission (0.15) and a threat class (medium), while the level of the severity of natural events represented by (apparent seismicity, volcanic phenomena, and meteorological phenomena), respectively, in the third and last order, with a hazard ratio (0.03) and a half threat (low).

**Table (11)**

Classification of threats (natural events) to measure the risk using the (impact-probability) matrix

Threat type	Threat Name	Impact (I)	Probability (P)	Danger (I*P)	Threat class
loss of basic services	Air conditioning failure	0.5	0.3	0.15	M
	loss in processing capacity	0.7	0.3	0.21	M
	Wireless communication	0.5	0.3	0.15	M
	Hardware failure				

The results of Table (11) regarding the type of threat (loss of essential services) in the Commission show that the threat (loss of capacity Hardware) had an effect value of (0.7), while threats (failure of air conditioning, failure of wireless communication Hardware) came at the level of impact (0.5) respectively, while the threat (failure of air conditioning, failure of wireless communication Hardware) got a probability level of (0.5), respectively, while the probability of losing power Hardware got a percentage of (0.3), so the severity (failure of air conditioning) was, failure of wireless communication Hardware) with a percentage of (0.25) and a threat rating (medium), respectively, while the risk of losing power supply was (0.21) and a threat rating (medium).

**Table (12)**

classify threats (interference due to radiation) to measure the danger using a matrix (Impact-probability)

Threat type	Threat Name	Impact (I)	Probability (P)	Danger (I*P)	Threat class
Disturbance due to radiation	Electromagnetic radiation	0.7	0.3	0.21	M
	heat radiation	0.3	0.3	0.09	M
	Electromagnetic pulses	0.7	0.3	0.21	M

It is clear by reviewing the results of Table (12) regarding the type of threat (interference due to radiation), as the threat (electromagnetic radiation and electromagnetic pulses) had an impact ratio of (0.7), respectively, while the thermal radiation threat obtained a percentage of (0.3) because of the commission far from the stations. On the level of the possibility of the threat emerging, the three threats (electromagnetic radiation, thermal radiation, and electromagnetic pulses) received a percentage of (0.3), respectively, while the level of danger was for (electromagnetic radiation, electromagnetic pulses) with a risk ratio of (0.21) and a class medium threat, respectively. In contrast, the threat (heat radiation) received a risk ratio of (0.09) and a medium threat class.

**Table (13)**

Classification of threats (violation of information integrity) to measure the risk using a matrix (Impact-probability)

Threat type	Threat Name	Impact (I)	Probability (P)	Danger (I*P)	Threat class
Information integrity violation	Interfering signal interception	0.5	0.3	0.5	M
	remote spying	0.8	0.3	0.8	M
	Listen	0.5	0.3	0.5	M
	Media or documents theft	0.8	0.1	0.8	L
	Hardware theft	0.8	0.1	0.8	L
	Return of recycled or discarded media	0.3	0.3	0.3	L
	disclosure	0.8	0.3	0.8	M
	Data from untrustworthy sources	0.7	0.1	0.7	L
	hardware tampering	0.7	0.3	0.7	M
	software tampering	0.7	0.1	0.7	L
	location detection	0.3	0.1	0.3	L

It is clear from the results of Table (13) related to the threat (violation of information integrity) in the Independent High Electoral Commission, the impact value of the threats (remote espionage, media theft or documents theft of Hardware, disclosure) is evident in the first order, with a percentage of (0.8) in the second-order Threats (data from untrustworthy sources, hardware tampering, software tampering) had a percentage of (0.7). In contrast, threats (interception, crosstalk, eavesdropping) got a percentage of (0.5), and in third place, the threat (location detection) got an impact ratio of (0.3). As for the level of threat appearance, the threats (interfering signals, remote espionage, eavesdropping, retrieval of recycled or discarded media, disclosure, tampering with devices) got a percentage of (0.3), while the percentage of threats (media theft or Documents, Hardware theft, data from untrustworthy sources, software tampering, and location detection) at a rate of (0.1) and, respectively, as for the level of danger posed by the threat, the threat (remote espionage, disclosure) ranked first with a rate of (0.24) and classified Medium threat, while the second-order of threat was a threat (manipulation The percentage of threats was (interference signals, eavesdropping) and (0.15) with a medium threat category, while the threats (recovery of recycled or discarded media, theft of media or documents, Hardware theft, data from untrustworthy sources, software tampering, and location detection) respectively, with a percentage (0.09, 0.08, 0.08, 0.07, 0.07, 0.03) and a low threat rating.

**Table (14)**

Classification of threats (technical failures) to measure the risk using the (impact-probability) matrix

Threat type	Threat Name	Impact (I)	Probability (P)	Danger (I*P)	Threat class
technical failures	Hardware crash	0.7	0.5	0.35	M
	Hardware failure	0.8	0.3	0.24	M
	saturation of the information system	0.7	0.3	0.21	M
	Program malfunction	0.8	0.3	0.24	M
	Breach of information system preservation	0.7	0.3	0.21	M

The results of Table (14) for the type of threats (technical failures) to the Commission show that threats (Hardware failure, program failure) have an impact ratio (0.8) and are in the first order, while the second order of threats is (Hardware failure, information system saturation, breach of maintaining the system information) at a rate of (0.7) and, respectively, as for the level of probability of emergence of threats, the threat of Hardware failure was the first with a percentage of (0.5) for the probability of appearance, while threats (Hardware failure, information system saturation, program malfunction, breach of maintaining information system) got a percentage (0.3) and, in order, in terms of the probability of appearing in the commission, and in terms of the level of emergence of

danger, the threat (information failure) got a risk ratio of (0.35) with a medium threat class and in the first order, while the two threats (Hardware failure, and program failure) got the second order. And with a percentage of (0.24) with a medium threat category, while the third rank for the two threats (information system saturation, breach of information system preservation) and with a percentage (0.21), respectively, with a medium rating.

**Table (15)**

Threat classification (unauthorized actions) to measure risk using the (impact-probability) matrix

Threat type	Threat Name	Impact (I)	Probability (P)	Danger (I*P)	Threat class
Unauthorized actions	Unauthorized use of Hardware	0.7	0.3	0.21	M
	Backup software	0.8	0.3	0.24	M
	Use of counterfeit or copied software	0.8	0.3	0.24	M
	data corruption	0.8	0.3	0.24	M
	Unlawful data processing	0.8	0.3	0.24	H

Table (15) shows the threats caused by unauthorized procedures in the High Independent Electoral Commission and their impact. Threats (program backup, use of counterfeit or copied programs, data corruption, illegal data processing) ranked first with a percentage of (0.8), respectively, while the second rank in terms of the impact on the Commission of the unauthorized use of Hardware with a percentage of (0.7), as for the level of the probability of emergence of the threat to the Commission, the illegal processing of data ranked first with a rate of (0.5), while the second rank was for threats (fraudulent copying For the program, the use of counterfeit or copied programs, data corruption, unauthorized use of Hardware) on a percentage of (0.3) and respectively, as for the level of risks generated by threats, it was the first place for illegal processing of data with a risk rate of (0.40) and a threat category (High), while the second rank of threats (fraudulent copying of the program, the use of counterfeit or copied programs, data corruption) was on the second rank, with a risk ratio of (0.24) and a medium and high threat category. Finally, the threat of unauthorized use obtained a risk ratio (0.21) and a medium threat class.

**Table (16)**

Classification of threats (functions Violation) to measure the risk using the (impact-probability) matrix

Threat type	Threat Name	Impact (I)	Probability (P)	Danger (I*P)	Threat class
functions Violation	Usage error	0.7	0.3	0.21	M
	Abuse of rights	0.7	0.3	0.21	M
	falsification of rights	0.7	0.3	0.21	M
	denial of actions	0.5	0.5	0.25	M
	Violation of staff availability	0.7	0.1	0.07	L

By looking at the results of Table (16) related to the type of threat (functions Violation), the impact values for threats (error of use, abuse of rights, forgery of rights, violation of workers' availability) appeared on a percentage (0.7) respectively and in the first order, while the order was The second was at the level of impact on the denial of procedures, with a percentage of (0.5). In terms of the probability of the emergence of these threats, the first order of threat was the denial of actions with a percentage of (0.5), while the second-order of threats was (error of use, abuse of rights, forgery of rights) and at a rate of (0.3). Respectively, as for the threat of violating the availability of workers, it ranked third, with a probability of appearance of (0.1), as shown in table (48) for the level of threats and their classification. While the risk of threats (error of use, abuse of rights, forgery of rights) was (0.21) with a medium risk category, respectively, while the risk of violating the availability of workers was (0.07) with a weak threat category.

## Core assets risk measurement

The value of each asset is determined on a scale from (0 - 4) as shown in the matrix below, and the probability of the threat occurring on a scale that starts with low, then medium, and ends with high, then we determine the weaknesses on a scale consisting of three degrees (low, medium, high), then The values of the assets and the levels of threat and vulnerability related to each type of consequence are matched in the matrix, to determine the size of the risk for each group on a scale between (0-8) degrees, as shown in Table (17).

**Table (17)**

Matrix with the values of pre-selection

	Probability	Low			Medium			High		
		Weaknesses	Low	Medium	High	Low	Medium	High	Low	Medium
Asset	0	0	1	2	0	1	3	2	3	4
Value	1	1	2	3	1	2	4	3	4	5
	2	2	3	4	2	3	5	4	5	6
	3	3	4	5	3	4	6	5	6	7
	4	4	5	6	4	5	7	6	7	8

- Low risk: 0-2
- Medium risk: 3-5
- High risk: 6-8

**Table (18)**

Risk Measurement for primary assets (the impact of business and activities/operations) by using a matrix with predetermined values

Primary assets		Asset Value	Probability (P)	Weaknesses	risk measurement
Business and activities Impact	concluded contracts	1	L	M	2
	Assessments of observers	2	M	M	4
	Oversight office access records	2	L	M	3
Processes	Authorization groups	1	M	M	3
	management accounts	1	L	M	2

It is evident from the results of Table (18) regarding the matrix of the Commission's primary assets and related to the impact of the works, activities, and operations and according to each of its dimensions. The results were clarified as follows:

### Measuring the risk of the primary assets and their impact on business and activities

**(First)** The underlying asset (contracted contracts) shows the possibility of a threat arising from it with a value (1) that expresses a low probability of the threat. At the same time, the weakness faced by the Commission was medium, resulting in this matrix measuring the risk (2), which indicates a low level of risk, as The Commission must be careful when it resorts to concluding contracts with any of the parties, by maintaining the confidentiality and documentation of information.

**(Second)** While the main asset (observers' assessments) shows the possibility of an induced threat with a value of (2), indicating the possibility of a low threat, and with a value of medium vulnerability, the risk measurement was (4), to indicate a medium risk level, and here the Commission should take the observers' views It is documented and preserved as it pertains to the overall work of the Commission and its work evaluation, so that it can invest in strengths, and works to reduce weakness from the point of view of observers, in addition to the fact that this information is confidential, so the Commission must deliberately prevent its access to competitors or other stakeholders.

**(Third)** While the main asset (oversight office) shows the possibility of a threat with a value of (2), it indicates the possibility of a threat with a low probability, and a vulnerability index with a value of

(medium) for the Commission, so that this matrix results in a risk measurement (3), to confirm the emergence of a medium risk If the Commission neglects to document this assessment or makes it open to the stakeholders' information, which requires maintaining the security of information and preventing access to it by other parties in order to invest it in a way that serves their interests.

### Measuring the risk of the primary assets and their impact on operations

**(First)** The primary asset (access records) got the value of the asset (weaknesses) of (1). At the same time, it indicates the probability of the commission facing the threat of (medium) occurrence, while the organization's weaknesses in facing this threat refer to (medium), and by measuring the risk (3) It indicates moderate risks, so the Commission should preserve records from damage and loss, as well as document and store them electronically, and prevent them from being exposed to information, distortion, and loss by parties that take advantage of that situation.

**(Second)** While the matrix for the main asset (authorization groups) showed the value of the asset (weakness points) amounting to (1) indicating the possibility of the commission facing a threat of medium occurrence and confrontation, while weaknesses of the commission appeared (average) when facing a threat, and with a risk measurement indicator (3), indicates that the Commission faces moderate risks, which necessitates setting controls and instructions for those authorized to deal with the Commission's information by preventing the disclosure of secrets and information and preserving them from damage, loss, and disclosure, except with an official authorization that allows them to do so.

**(Third)** As for the primary asset matrix (management accounts), it obtained an asset value (weakness points) that amounted to (1), to indicate the possibility of the commission facing a low-incidence threat and confrontation because the management accounts are made confidential and by decisions that cannot be viewed, and if they are exposed to disclosure It will bear the prominent harm and direct the risk on its own, which exposes it to accountability. In contrast, the matrix showed an indicator of weaknesses (medium) for the Commission, and by measuring the risk (2), it indicates facing a low risk, which draws the administration's attention to its accounts and documents, and is keen on the confidentiality of decisions, contracts and orders.

### Event Scenario Possibility Matrix

The possibility of an incident scenario occurring is given by a threat exploiting a vulnerability with a given possibility. The table sets this probability against the impact of the business related to the accident scenario, where the resulting risks are measured on a scale of (0-8) and as shown in Table (19), and this risk scale can also be mapped to simple, comprehensive risk classification, such as:

- Low risk: 0 -2
- Medium risk: 3-5
- High risk: 6 -8

**Table (19)**

Matrix possibility of event scenario

	The possibility of the event scenario	very low (impossible)	low (unlikely)	Medium (possible)	high (possible)	very high (frequent)
Business Impact	very low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	high	3	4	5	6	7
	very high	4	5	6	7	8

**Table (20)**

Risk Measurement for primary assets (business impact and activities/operations) by using the event scenario potential matrix

primary assets		probability	event scenario possible	risk measurement
business and activities Impact	concluded contracts	L	M	3
	Observer ratings	M	M	4
	Oversight office	L	L	2
Processes	access records	M	M	4
	Authorization groups management	M	M	4
	accounts	L	M	3

Through the researcher's resort to the matrix of the possibility of occurrence of the expected scenario of the primary assets, the results agreed with the results of Table (5) to indicate the accuracy of the analysis, if the results are according to the following:

**First: the primary assets (business and activities impact) and were as follows**

1. Maintaining the security of the information of the concluded contracts showed the possibility of being exposed to a low threat, the possibility of a medium event scenario, and a measure of risk (3), which indicates that the Commission faces a medium risk.
2. While maintaining the security of the observers' assessments, information showed the possibility of being exposed to a medium threat, the possibility of a medium event scenario, and a measure of risk (4), which indicates that the Commission faces a medium risk.
3. While maintaining the security of the information of the Oversight Office showed the possibility of being exposed to a low threat, the possibility of a low event scenario, and a measure of risk (2), which indicates that the Commission faces a low risk.

**Second: The primary assets (the impact of operations) and their results were as follows**

1. Maintaining the security of the access records information showed the possibility of being exposed to a medium threat, the possibility of a medium event scenario, and a measure of risk (4), which indicates that the Commission faces a medium risk.
2. Maintaining the security of the information security of the authorization groups showed the possibility of being exposed to a medium threat, the possibility of a medium event scenario, and a measure of risk (4), which indicates that the Commission faces a medium risk.
3. Maintaining the security of the management accounts information showed a low probability of being exposed to a threat, with the possibility of a medium event scenario and a measure of risk (3), which indicates that the Commission faces a medium risk.

## Conclusions

**In light of the results of the current research, the conclusions drawn can be identified as follows**

It appeared through field visits to the organization concerned with the research that there are some clear goals related to information security and declared in the procedures of the Commission, despite the existence of a written information security policy approved by the Ministry of Electricity and recommended for implementation. Despite the Commission's lack of commitment to the full implementation of the information security policy, its departments are committed to changing the passwords of their main systems every month to prevent any breach that might occur, as well as their interest in archiving their information on multiple storage media inside and outside the Commission to prevent that data from being exposed to any risks. There are no financial allocations for the management of information security in the independent sense. However, each department presents its needs of financial resources from the budget, and according to the known chapters, there is no particular chapter on information security risks and that the commission in question has

its budget. The Commission does not employ cloud computing services, whether public or private, in documenting its data and information, due to the lack of reliability of those services. The Commission uses cheap storage media such as CDs to archive its information and data, as well as hard disks (normal, unsafe (shock and water-resistant), as well as being unencrypted due to their high price. The Commission uses operating systems and free and unlicensed programs that threaten the security of its information. The commission in question did not adopt any written information security risk management strategy approved by the senior management, which reflects the senior management's lack of knowledge of information security, which negatively affected the reality of its management of information security, and even its resort to personal judgments and improvised decisions, which are not based on Sometimes to any documentation mentioned in this area. The Commission showed great interest in documenting the fixed and portable Hardware used at the Commission headquarters from physical assets, which added strengths to be invested in facing threats to weaken its primary assets (operational and informational). At the same time, it was found that there is a weakness in the documented rules and procedures for Hardware, especially In automatic data processing, processing accessories, and electronic media), and weaknesses in the application and documentation of other electronic media, which included (compact and hard disk drives, flash drives, printers, and documents). The commission concerned with research uses the supporting assets (communication networks), which it uses to transfer data and information among its other relevant departments and divisions, with a weakness in the documentation procedures for those devices and systems used by the commission, as it is the one who documents them in terms of purchase and warehouse entry, while Do not document it while working, as modern culture is specifically for public organizations to adopt documentation for every detail of the specification. The Commission complies with the constraints arising from the economic climate, especially in light of the poor level of partial implementation and partial documentation, as a result of the Commission's performance being subjected to drastic changes due to the government financial crises in (2014), which led to a partial halt in the implementation of some developments. The limited interest in the application and documentation of time constraints shows the reason for the weakness of adopting a limited type of time constraints and organizational controls such as the life rate of information in the Commission, as well as the period needed by managers to determine the acceptable duration of exposure to certain risks, as its information becomes obsolete if it is not employed promptly. It was confirmed that the Commission was interested in the complete application of the restrictions of merging the new and current controls, in line with the interest in information security. However, it was not documented, as well as the interdependence between both types of controls, and the reason for the gap is attributed to the fluctuating use between all controls, given Because every officer has his way; And that each method has its advantages and disadvantages in certain use cases. Security management of information security risks is ineffective and not secure solidly and reliably from external and internal threats because the internal audit system is traditional. The unauthorized procedures (illegal data processing) constituted the most prominent threats that led to security breaches, reflecting the most critical risks that the commission under consideration could face. There is nobody specialized in evaluating and measuring information security risk management and documenting the results, in addition to the fact that the Commission remains without tests to secure it from penetration. The commission surveyed's indifference regarding the development of a clear and documented strategy to address risks that includes the four options (modification, retention, avoidance, and risk-sharing) in the danger of the existing situation in the event of the loss of a specialist in this field and the loss of experience, as well as the sharing of responsibility among all in the event the strategy is approved by before senior management.

## References

- Alshareef, N. (2016). A Model for an Information Security Risk Management (ISRM) Framework for Saudi Arabian Organisations. International Association for Development of the Information Society, 365-370. Retrieved from <https://eric.ed.gov/?id=ED571604>
- Aubert, B. A., Patry, M., & Rivard, S. (2005). A framework for information technology outsourcing risk management. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 36(4), 9-28. Doi:<https://doi.org/10.1145/1104004.1104007>

- Baryannis, G., Validi, S., Dani, S., & Antoniou, G. (2019). Supply chain risk management and artificial intelligence: state of the art and future research directions. *International Journal of Production Research*, 57(7), 2179-2202. Doi:<https://doi.org/10.1080/00207543.2018.1530476>
- Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. Paper presented at the Proceedings of the 2001 workshop on New security paradigms. Doi:<https://doi.org/10.1145/508171.508187>
- Dunlop, J. M., Chechak, D., Hamby, W., & Holosko, M. J. (2021). Social Work and Technology: Using Geographic Information Systems to Leverage Community Development Responses to Hate Crimes. *Journal of Technology in Human Services*, 1-29. Doi:<https://doi.org/10.1080/15228835.2021.1931635>
- ISO/IEC 27001:2013, "International Standard Information technology- Information technology - Security techniques - Information security management" (2d ed.), Geneva: ISO Copyright Office.
- ISO/IEC 27005:2011, "International Standard Information technology- Information technology - Security techniques - Information security risk management" (2nd ed.), Geneva: ISO Copyright Office.
- ISO/IEC 27005:2018, "International Standard Information technology. Information technology - Security techniques - Information security risk management", 3rd ed., Geneva: ISO Copyright Office
- Kharytonov, E., Kharytonova, O., Tolmachevska, Y., Fasii, B., & Tkalych, M. (2019). Information Security and Means of Its Legal Support. *Amazonia Investiga*, 8(19), 255-265. Retrieved from <https://amazoniainvestiga.info/index.php/amazonia/article/view/227>
- Khidzir, N. Z., Mohamed, A., & Arshad, N. H. H. (2010). Information security risk management: An empirical study on the difficulties and practices in ICT outsourcing. Paper presented at the 2010 Second International Conference on Network Applications, Protocols and Services. Doi:<http://dx.doi.org/10.1109%2FNETAPPS.2010.49>
- Kiura, S. M., & Mango, D. M. (2017). INFORMATION SYSTEMS SECURITY RISK MANAGEMENT (ISSRM) MODEL IN KENYAN PRIVATE CHARTERED UNIVERSITIES. *European Journal of Computer Science and Information Technology*, 5(2), 1-15. Retrieved from <https://www.eajournals.org/wp-content/uploads/Information-Systems-Security-Risk-Management-ISSRM-Model-in-Kenyan-Private-Chartered-Universities.pdf>
- Liao, H.-J., Lin, C.-H. R., Lin, Y.-C., & Tung, K.-Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1), 16-24. Doi:<https://doi.org/10.1016/j.inca.2012.09.004>
- Luke, I. (2019). Why ISO 27005 risk management is the key to achieving ISO 27001 certification. Retrieved from <https://www.itgovernance.co.uk/blog/why-iso-27005-risk-management-is-key-to-iso-27001>
- Miloslavskaya, N., & Tolstoy, A. (2019). Internet of things: information security challenges and solutions. *Cluster Computing*, 22(1), 103-119. Doi:<https://doi.org/10.1007/s10586-018-2823-6>
- Murdoch, S. (2010). Destructive activism: The double-edged sword of digital tactics. *Digital Activism Decoded: The new mechanics of change*, 137-148. Retrieved from <https://murdoch.is/papers/digiact10destructive.pdf>
- Peltier, T. R. (2005). *Information Security Risk Analysis*, Second Edition: Taylor & Francis. Retrieved from <https://books.google.com.pk/books?id=n8Z1RDjEKa0C>
- Setiawan, H., Putra, F. A., & Pradana, A. R. (2017). Design of information security risk management using ISO/IEC 27005 and NIST SP 800-30 revision 1: A case study at communication data applications of XYZ institute. Paper presented at the 2017 International Conference on Information Technology Systems and Innovation (ICITSI). Doi:<https://www.doi.org/10.1109/ICITSI.2017.8267952>
- Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information security assessment in public administration. *Computers & Security*, 90, 101709. Doi:<https://doi.org/10.1016/j.cose.2019.101709>
- Zarei, J., & Sadoughi, F. (2016). Information security risk management for computerized health information systems in hospitals: a case study of Iran. *Risk management and healthcare policy*, 9, 75-85. Doi:<https://dx.doi.org/10.2147%2FRMHP.S99908>