Journal of Information Systems Engineering and Management
2026, 11(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The Contribution of Internal Auditing to Improving the Efficiency of the Information Security System Under ISO 27001 Standard

KHELLADI Radhia [a], CHEBLAL ALI [a] , NADHIR CHEBROU [a] , Salmi Mohamed [a]

a r.khelladi@univ-boumerdes.dz (University M'hamed Bougara of Boumerdes _ ALGERIA).
a a.cheblal@lagh-univ.dz (Amar Telidji University of Laghouat_ ALGERIA).
a nadirchabrou@gmail.com (University of EL-OUED_ ALGERIA).
a salmimoh615@gmail.com (Center University Aflou _ ALGERIA).

ARTICLEINFO

Received:12 Nov 2025
Accepted: 27 May 2026
Published: 07 July 2026

ABSTRACT

This study aims to highlight the contribution of internal auditing to improving the efficiency of information security management systems. It utilizes ISO/IEC 27001as a framework for assessing an organization's compliance with security controls and identifies the role of auditing in identifying vulnerabilities and enhancing information governance. To achieve this, a descriptive-analytical approach was employed to establish a foundation for understanding, along with a case study for practical application. The study concludes that internal auditing is an effective strategic tool for improving the efficiency of information security systems, and that ISO/IEC 27001 is a comprehensive and essential framework for establishing an effective information security system.

Keywords: Internal auditing, information security system, ISO/IEC 27001, efficiency.

Introduction:

In light of the rapid changes and increasing challenges facing the business environment, economic institutions are in dire need of effective mechanisms to ensure the integrity and transparency of their operations, which in turn supports their ability to achieve their stated objectives. Digital transformation is accelerating, and cyber threats are on the rise, making information a vital asset upon which institutions rely to conduct their business and make strategic decisions.

Consequently, the need has arisen to strengthen information protection mechanisms and ensure its confidentiality, integrity, and availability. This has made information security a fundamental pillar of business continuity. In this context, internal auditing emerges as an effective tool to ensure compliance with information security standards, evaluate the effectiveness of adopted controls, and mitigate associated risks.

Internal auditing aims to provide assurances that add value to the organization and improve its performance. The internal auditor contributes to protecting the organization's assets, ensuring the

.

accuracy of financial and operational information, and promoting compliance with regulations. Its importance increases when linked to assessing the organization's adherence to the Information Security Management System (ISMS) according to ISO/IEC 27001, which represents the international reference framework for establishing a comprehensive policy for information protection and managing related risks.

This study will examine the contribution of internal auditing to improving the information security system under the ISO/IEC 27001 standard at the National Institute of Geophysics in Algeria. This will be achieved by conducting an internal audit at various stages, identifying weaknesses and strengths, and proposing the necessary improvements to maintain the information security system at this organization.

Research Problem:

The internal audit methodology relies on risk analysis, which involves identifying and assessing risks, then implementing procedures to determine their causes and provide recommendations. Internal auditing is thus used to evaluate the information security management system with the aim of improving it. Therefore, the following main research question can be posed:

To what extent does internal auditing contribute to improving the efficiency of the information security system under the ISO/IEC 27001 standard at the National Geophysical Institute of Algeria?

Sub-questions:

The following sub-questions stem from the main research problem:

- What is the current state of the information security system implemented at the National Geophysical Institute of Algeria?
- What methodology does the internal auditor use to improve the information security system at the National Geophysical Institute of Algeria?

Research Hypotheses:

To address the main research problem and as a preliminary answer to the sub-questions, the following hypotheses were formulated:

- The information security system at the National Geophysical Institute suffers from some weaknesses that may affect its efficiency.
- The internal auditor at the National Geophysical Institute relies on a structured methodology that includes risk analysis, execution of audit tasks, provision of recommendations, and follow-up on their implementation. Research Objectives:

The main objective of this study is to determine the extent to which internal auditing contributes to improving the efficiency of information security management systems in organizations.

In addition, the following objectives are also pursued:

- Highlighting the importance of having an effective information security management system in organizations.
- Defining the role of the internal audit function in identifying weaknesses in the information security system.
- Proposing mechanisms to enhance the contribution of internal auditing to protecting information assets.

.

Journal of Information Systems Engineering and Management
2026, 11(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Research Significance: The significance of this research stems from its focus on a vital topic in the business environment: information security. By linking it to the internal audit function, which is considered an effective control tool, the research aims to highlight the role that internal auditing can play in improving the efficiency of information security management systems within organizations, particularly in light of the continuous increase in cyber risks and threats.

Methodology Used in the Study:

Given the nature of the study and in line with its subject matter, and to achieve its objectives and desired results, a combination of descriptive and analytical methods was employed. Information was gathered from various sources, including books, journals, and relevant Arabic and foreign scientific studies and research, in addition to professional guidelines and standards issued by international organizations.

For the applied aspect, a case study was used, relying on interviews as research tools, along with observation and documentary analysis.

Previous Studies: To the best of our knowledge, there are few studies that directly address the contribution of internal auditing to improving the efficiency of information security systems. Therefore, some previous studies related to the research variables will be presented:

First Study: (Sarah, 2022-2023).

This study aimed to determine the contribution of internal auditing to improving and managing risks in the institutions under study. This was achieved by answering the research question: To what extent does the internal auditor contribute to risk management processes in Algerian public institutions? The descriptive, analytical, and case study methods were adopted. Among the findings of the study is that: the internal auditor provides risk management consulting, but it is not within their role to conduct risk management itself, which falls under the responsibilities of general management.

Second Study: (Basma and Saeeda Tayeb, 2018).

This study aimed to highlight the ISO 27001 standard, considered the most important international standard in information security systems, and its significant role in protecting organizational assets, especially at a time when information has become the primary source of power and authority.

This study concluded that: ISO 27001 is considered a basis for evaluating information security management, serving as a system assessment document. It is also a comprehensive standard for building an effective information security system, whereby the organization studies and understands the risks related to its information and then builds an integrated information security system that mitigates these risks and is continuously scalable based on a clear and reliable methodology.

What distinguishes this study from previous studies: This study is distinguished by several aspects that make it different from previous studies, the most important of which is the direct link between the two variables, internal auditing and the information security system, which is a topic that has not been addressed in depth previously, as most studies focus on each field separately. This study seeks to clarify how internal auditing can be an effective tool and contribute to improving the efficiency of the information security system, in light of the use of the ISO 27001 standard as a reference framework.

Study model:

.

Journal of Information Systems Engineering and Management
2026, 11(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Dependent variable **Independent variable**

Intermediate variable

Standard ISO/IEC 27001

First: The Conceptual Framework of Internal Auditing.

Internal auditing is a management function that aims to review and evaluate the operational and financial activities within an organization to ensure compliance with policies and procedures, and to achieve objectives efficiently and effectively. It also contributes to enhancing transparency and reducing risks through a systematic approach to evaluating and improving the effectiveness of control processes.

1. Definition of Internal Auditing

The definitions of internal auditing have addressed numerous aspects, varying according to the issuing bodies and parties. Despite the formal differences between these definitions, they all converge on the same objective. The most important of these definitions are listed below:

The international definition adopted by the International Institute of Internal Auditors (IIA) on June 29, 1999, and endorsed by the Board of Directors of the French Institute of Internal Auditors (IFACI) on March 21, 2000, translates as follows: "Internal auditing is an independent and objective activity that provides an organization with assurance regarding its control over its operations, advises on their improvement, helps create added value, and assists the organization in achieving its objectives through the systematic and methodological evaluation of risk management, control, and governance processes, and provides recommendations to enhance their effectiveness." (SCHICK, Jacques VERA, & Olivier BOURROUICH-PAREGE, 2014)

It can also be defined as an evaluation function integrated into the internal control system, exercised independently and by delegation, linked to a functional department (financial, administrative, or... An independent department, internal audit assesses the accuracy and regularity of an organization's procedures and information. Its mission is to ensure the protection of the organization's assets and resources and to evaluate the effectiveness and performance of its information systems. (BOUDIA & Ali DEBBI, 2020, p. 3)

Internal auditing is the process of evaluating and confirming the effectiveness and efficiency of operations and is one of the effective means of internal control. It helps ensure that the established control mechanisms are applied and sufficient to achieve operational efficiency, guarantee the accuracy of accounting data, protect the organization's assets and funds, and verify that its employees follow the policies, plans, and administrative procedures set for them. (Ibrahim, 2016, p. 19)

According to the Committee of Organizations Sponsoring the Integrated Internal Control Framework (COSO), internal auditing is: "A process influenced by the organization's board of directors, designed to give reasonable assurance about the organization's achievement of its objectives in the following areas: operational efficiency and effectiveness, reliance on financial reports, and compliance with applicable laws and activities." (Lazan, 2016)

From this, we see that internal auditing has evolved to include: (Al-Wardat, 2017)

• Services Preventive: This refers to the procedures established by the internal auditor to ensure the protection of assets and property from theft and embezzlement.

• Evaluative Services: These encompass the procedures and methods employed by the internal auditor to measure and assess the effectiveness of internal control systems implemented within the organization.

.

• Constructive Services: These involve assisting the internal auditor in providing relevant data to improve the organization's administrative, financial, and production systems.
• Remedial Services: These include the procedures, recommendations, and methods used by the internal auditor to correct identified errors or recommendations included in their audit report for rectifying errors and addressing deficiencies in various systems.
• Examination and Evaluation: This involves determining the accuracy of financial, operational, and administrative information, etc., and relies on the accuracy, validity, and legality of the documents.
• Analysis: This relies on financial analysis tools, comparisons, and results analysis.
• Compliance: This refers to the extent to which the organization's operations adhere to established administrative policies and implement processes according to established systems or decisions.
• Evaluation: This assesses the effectiveness of data and plans in achieving objectives.
• Report: This includes observations on the audited activities and details any problems encountered. The challenges facing the organization, their causes, weaknesses, and even strengths.

From the above, it can be concluded that internal auditing is an independent and objective activity within an organization, aimed at examining and evaluating various processes and systems to ensure their effectiveness and integrity. It also contributes to strengthening the internal control and risk management system by providing recommendations that help improve performance and ensure the achievement of the organization's objectives.

2. Objectives of Internal Auditing:

The objective of internal auditing is defined by Standard 2100 – Nature of the Work – which states that the primary task of internal auditing is to evaluate and contribute to the improvement of governance, risk management, and control processes. This evaluation must be conducted in a systematic and rigorous manner (auditors, 2017). Therefore, the objective of auditing is to evaluate corporate governance, risk management, and internal control processes. The objectives of internal auditing are defined in the International Standards for the Professional Practice of Internal Auditing (ISAs 2110 – Governance), 2120 – Risk Management, and 2130 – Control, as detailed below:

• Governance:

With regard to governance, internal audit aims to assess and provide appropriate recommendations to improve the organization's governance processes for strategic and operational decision-making, monitor risk management and control processes, and promote appropriate ethical and value standards within the organization. The auditor also informs stakeholders about risk and control information, coordinates activities and information exchange between the board of directors, external auditors, and internal auditors, and evaluates whether the organization's information systems governance supports its strategies and objectives. Furthermore, the auditor assesses the implementation and effectiveness of the organization's ethical objectives, programs, and activities. (auditors, 2017, p. 19)

• Risk Management:

With regard to risk management, internal audit aims to assess whether the organization's objectives are consistent with and contribute to the achievement of its mission. Significant risks are identified and assessed, and the chosen risk management methods are ensured to be appropriate and consistent with the organization's risk tolerance. The collection and communication of risk-related information within the organization is also ensured to enable employees, management, and the board of directors to fulfill their responsibilities in a timely manner. (auditors, 2017, p. 19) (2017, p. 20)

• Control:

The audit also aims to assess the suitability and effectiveness of the chosen control system. This is to ensure the achievement of the organization's strategic objectives, the reliability and integrity of financial and operational information, the efficiency and effectiveness of processes and programs, compliance with laws, regulations, rules, and procedures, and the protection of assets. (auditors, 2017, p. 21)

.

Journal of Information Systems Engineering and Management
2026, 11(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

3. Stages of the Internal Audit Process

The internal audit process is carried out through three basic stages (Bertin, 2013):

• Preparatory Stage:

This stage aims to prepare all preparatory work before moving to implementation. It requires the auditor to be able to read, focus, and understand in order to gain a complete knowledge of the organization, to identify where useful information is located, and the parties who can help in obtaining it. This is a necessary and important stage that must be initiated. International Standard on the Professional Practice of Internal Auditing (ISA) No. 2200 specifies the necessity of preparing a plan for each task by defining its scope, timeframe, and the resources required for its implementation. The steps of this stage are:

- The order The assignment: This is the mandate granted by management to the internal audit department and takes the form of a written document to inform officials and all parties involved in the audit process of its commencement.
- Study phase: In this phase, the auditor develops a detailed, risk-based program to prioritize the task in line with the organization's objectives. This is based on gathering information that enables the auditor to understand the subject of the audit and gain an initial overview of the department being audited.
- Risk assessment: After studying and analyzing the information, the auditor prepares a table containing strengths and weaknesses, ranking risks according to their degree of impact on the organization. This table allows for the preparation of the guidance report, which defines the scope of the audit and focuses on tasks with a high degree of risk. Following this, the work plan is prepared and presented to management for approval.

• Implementation phase:

In this phase, the internal auditor goes into the field to conduct the audit. This phase begins with an introductory meeting, followed by the commencement of fieldwork. - Opening Meeting: This meeting takes place at the premises of the activity to be audited. It is held between the audit team and the head of the activity being audited. The meeting covers several points, including focusing on the overall objectives of the audit, reviewing and analyzing the introductory report and discussing it, setting dates and identifying the individuals the auditor will interact with, determining the logistical requirements for the engagement, reviewing the field procedures during the audit process, and recording the conclusions of this meeting in the minutes.

- Fieldwork: This is the official launch of the audit process, involving the implementation of the work program in the field. The International Standards for the Professional Practice of Internal Auditing (ISAs) stipulate several standards regarding this, such as Standard 2300 - Engagement Execution - "The auditor must identify, analyze, evaluate, and document sufficient information to achieve the objectives of the engagement," Standard 2320 - Analysis and Evaluation - "The internal auditor must base their conclusions and findings on a range of appropriate analyses and evaluations," and Standard 2340 - Engagement Supervision - "Audit engagements must be under appropriate supervision to ensure the achievement of objectives, guarantee quality, and develop the team's competencies." At this stage, interviews, tests, comparisons, and other auditing techniques are conducted to gather sufficient evidence to achieve the mission objectives. Interview summaries are then compiled into an "interview report."

• Conclusion Phase: After obtaining all the necessary information and completing the fieldwork, the internal auditors return to their offices to prepare a draft report. This draft is then presented and discussed at the closing meeting for approval, along with the presentation of observations and findings. Once approved, the report is finalized and sent to all relevant parties. The steps of this phase are as follows:

- Draft Internal Audit: At the beginning of the conclusion phase, the report is a draft because it is not yet complete, has not been approved, and has not yet been presented to the audited entity.
- Closing Meeting: This meeting is attended by the same individuals who participated in the initial meeting. The key points of the initial draft are presented, discussed, and approved. This meeting is based

.

on a set of principles: everything written in the report must be discussed with the individuals whose work was audited, and all supporting documents and evidence must be presented without reservation. The auditor must also provide recommendations, ranking them according to their importance.

- Issuance of the Final Report: After discussing and approving the initial draft of the report, it becomes final. Regarding this report, International Standards for the Professional Practice of Internal Auditing (ISA) 2420 – Quality of Reporting – stipulate that "reports must be accurate, objective, concise, constructive, complete, and timely." The internal auditor must disclose either a state of compliance, if the audited entity has adhered to all applicable international rules, conduct, and standards, or a state of non-compliance, if the entity has violated them.

Second: The Conceptual Framework of the Information Security Management System and ISO 27001 Standard

In light of the increasing threats targeting information assets, the need to adopt effective information security management systems has become paramount. The international standard ISO 27001 serves as the reference framework for developing, implementing, and maintaining an integrated system that ensures the confidentiality and integrity of information. Before discussing the information security management system, we will define the concept of an information system.

1. The Concept of an Information Security Management System

Before discussing an information security management system, let's define an information system, information security, and information security management.

1.1. Definition of an Information System

There are several definitions of an information system, depending on the researcher's perspective. It has been defined as "a system composed of a set of interconnected components (parts, information, people, equipment, and procedures) that work together harmoniously through a series of organized processes (collection, storage, processing, and analysis), presenting outputs and results in various forms of information (reports, figures, graphs, and charts), so that the results are provided to the system's users in a way that supports and serves their decisions, facilitates their work, and enables them to plan and control the organization's activities" (Nadia, 2010/2011). It has also been defined as: "An information system is an environment containing a number of elements that interact with each other and with their surroundings in order to collect and process data, produce and disseminate information to those who need it for decision-making" (Al-Sagh, 2003). Furthermore, it has been defined as: "An organized set of resources: physical, software, human, data, and procedures that allow for the collection, processing, and storage of information (in the form of data, text, images, sound, etc.) within and between organizations" (Bourliataux, 2003). (Cyril Gallitre & Yvers Roy, 2008).

From these definitions, we conclude that an information system is a framework within which resources (human and material) are coordinated to transform inputs (data) into outputs (information) to achieve the organization's goals.

1.2. Definition of Information Security:

Information security refers to the protection and security of all resources used in information processing. This includes securing the organization itself, its employees, the equipment used, and the information media containing the organization's data. This is achieved by following numerous protection procedures and methods that ultimately ensure the integrity of the information, which is a precious asset that the organization must protect (Daoud, 2000).

1.3. Concept of Information Security Management:

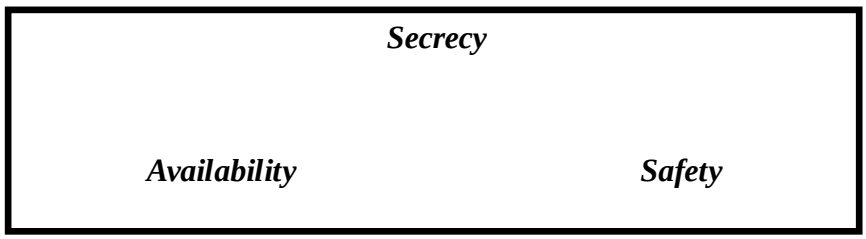
This is a series of administrative activities aimed at protecting and securing information assets within the organization and its information system. The assessment of access to this information may vary from one

.

Journal of Information Systems Engineering and Management
2026, 11(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

organization to another (autres, 2012). Through information security management, organizations strive to achieve the CIA triad, which includes: confidentiality and privacy, integrity, and security. Content (integrity), availability, and accessibility are the essential characteristics that information must possess to be considered valuable. (Younes) The following figure illustrates this:

Figure (01): Dimensions of Information Security Management



Source :(https://sarasecurit.wordpress.com, s.d.)

These three dimensions can be explained as follows (Sahrawi, 2020):

• Confidentiality: This dimension provides the organization with complete confidentiality for all information, even if the information is small and simple.

• Integrity and Safety: The ISO 27001 standard provides a benchmark for protecting and maintaining the integrity of information and its processing methods. This ensures business continuity and recovery in the event of disasters.

• Availability: This refers to the availability of restricted information. Using ISO 27001 to protect the information system assures the organization that only authorized users can access this information and its assets. This makes information security management a manageable task.

1.4. Definition of an Information Security Management System:

An information security management system is defined as: "A part of a comprehensive management system, based on a methodology for managing activity-related risks, and aimed at establishing, implementing, operating, monitoring, reviewing, maintaining, and improving information security" (Lachapelle). 2. Introduction to the ISO 27001 Information Security Management Standard

Given the increasing reliance of organizations on information systems to operate their processes, it has become essential to secure these systems by implementing internationally recognized standards, foremost among them ISO 27001, which will be introduced in this section.

2.1. Introduction to ISO 27001

ISO/IEC 27001, or officially ISO/IEC 27001:2005, is an international standard issued by the International Organization for Standardization (ISO) in October 2005 and subsequently revised in 2013 to become ISO/IEC 27001:2013. This international standard was developed to provide a model for establishing, implementing, operating, monitoring, auditing, maintaining, and improving an Information Security Management System (ISMS).

(Information security, s.d.) An Information Security Management System (ISMS) refers to the systematic methodology by which an organization ensures the security of sensitive information. ISMS is designed according to risk management processes and encompasses people, processes, and IT systems. This solution can be beneficial for organizations of all sectors and sizes that value the confidentiality of their information (https://www.iso.org/fr/standard/27001, s.d.).

.

Journal of Information Systems Engineering and Management
2026, 11(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

The ISMS standard provides a model based on a business risk approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving information security to achieve organizational goals (Younes, p. 72).

Establishing ISMS policies is based on a risk management approach. Policy definition begins with understanding the business environment and assessing resources and processes to identify potential information security risks. After identifying risks, the organization evaluates each risk, assesses its potential impact, and develops risk management strategies with extensive participation from management and employees. Since the environment and business processes vary from one organization to another, the identified risks and the strategies developed will also differ. Any organization, whether for-profit or non-profit, private or public, small or large, can implement the standard, provided it obtains accreditation from the International Organization for Standardization (Ben Mohammed H., 2023).

2.2. ISO 27001 Requirements:

Implementing the Information Security Management System (ISMS) is a step towards building effective information security by adhering to the following requirements (Ben Mohammed, 2023, pp. 185-186):

• Defining the ISMS in light of the organization's information systems specifications in terms of size, sources, and types, within the framework of the organization's regulatory and legislative needs.

• Developing an ISMS strategy that outlines the procedures and steps necessary for implementing this system.

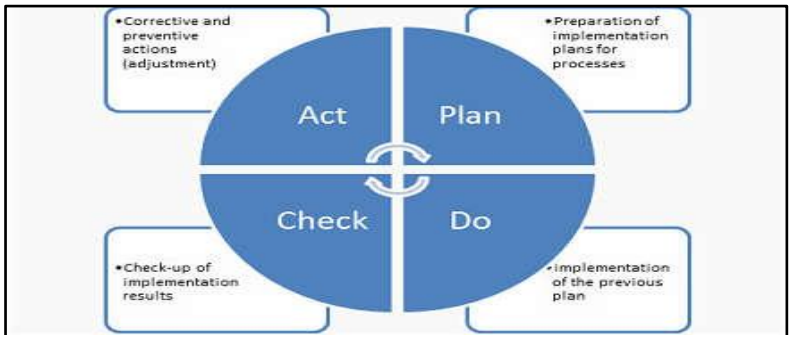
• Identifying and detecting risks using an appropriate methodology, and differentiating between risks that threaten information security to ensure the effective use of available resources.

• Evaluating risk mitigation options and selecting appropriate control objectives.

• Obtaining management approval and commencing implementation. The effective implementation of the ISO 27001 standard provides management with the means to control information security while reducing operational risks arising from inaccurate information and the risk of information leaks (Sahrawi, 2020, p. 436).

To manage information security issues within an organization, the Information Management System (ISMS) uses the PDCA model, which stands for: Input = Information Security Requirements and Expectations, and Output = Managed Information Security (Managed Information Security), as illustrated in the following figure:

Figure (02): PDCA (plan–Do–Check–Act) form



Source: (Younes, p. 72).

In the Plan phase, policies and objectives related to the Information Security Management System (ISMS) are established to achieve results consistent with the organization's policies and objectives.

.

Journal of Information Systems Engineering and Management
2026, 11(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

In the Do phase, the ISMS policy, controls, and procedures are implemented.
In the Check phase, process performance, objectives, and practical experience are measured, and results are reported.
In the final Act phase, corrective and preventive actions are taken based on the results of the internal ISMS audit, management audit, or other relevant information to ensure the continuous improvement of the system.

2.3. Dimensions of the ISO 27001 Information Security Management Standard:

The dimensions of the ISMS consist of the following elements (Youssef & et al., 2009, p. 423):

• Security Policy: This dimension documents the ISMS objectives to help the organization provide appropriate support and guidance.
• Information Security Organization: This enables the organization to control all its information through a set of policies, procedures, security tasks, and responsibilities. • Asset Management: By providing appropriate protection for assets;
• Human Resources Security: To mitigate risks arising from human error;
• Physical and Environmental Security: Contributes to securing physical areas (information processing facilities) and the work environment within the organization for effective information security management;
• Operations and Communications Management: This encompasses the facilities for secure delivery, secure management of daily operations, and data and network operations;
• Controlling Employee Access to the Information System: This is a key dimension in protecting the organization's information and safeguarding it from network breaches;
• Emergency Management: By establishing an effective communication system between different organizational levels to address emergencies and identify weaknesses in information security management;
• Business Continuity Management: This dimension allows for appropriate flexibility to address natural disasters, failures, and unforeseen disruptions, thus ensuring the continuity of information security activities;
• Compliance: This dimension defines contractual obligations, organizational security policy requirements, system audit processes, and security procedures.

Third: Internal Audit of the Information Security Management System.

• Human Resources Security: To mitigate risks arising from human error;
• Physical and Environmental Security: This dimension contributes to securing physical areas (information processing facilities) and the work of security personnel.
• Internal Audit of the Information Security Management System Auditing an Information Security Management System (ISMS) is a cornerstone of ensuring the effectiveness and efficiency of management systems in organizations. It aims to assess the extent to which processes and controls comply with established standards and policies within the context of information security and the ISO 27001 standard, which represents the international framework for information security management. Internal auditing becomes a pivotal tool for verifying the ISMS's conformity to the standard's requirements. This section will explore the relationship between these elements.

1. Definition of an Information Security Management System Audit

An information security management system audit is defined as: "A procedure that allows for the evaluation of the overall level of an information system. It may provide confirmation of the availability of the information system, data integrity, and access security, and provides evidence that allows us to know who accesses, when, and to which data or application." (Lachapelle)

.

Journal of Information Systems Engineering and Management
2026, 11(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

"An information security management system audit, according to the international standard ISO/IEC 27001, is a systematic and continuous protection of organizational assets, especially information and databases." (Faihan) Based on the preceding definitions, an Information Security Management System (ISMS) audit is a systematic, independent, and reliable process designed to assess the conformity and effectiveness of an organization's ISMS against the requirements of the international standard ISO/IEC 27001 or other internal standards. The audit aims to ensure that the system achieves its objectives of protecting the confidentiality, integrity, and availability of information, and that it is effectively managed and improved.

2. Scope of an ISMS Audit

An ISMS audit aims to provide management with reasonable assurance about the level of information security risks related to the organization's operations. Information security encompasses both logical and physical security, including access control to systems and machine rooms. This is achieved through (Khalida, 2020):

• Identifying and assessing the importance of the organization's assets;
• Analyzing the threats and risks the organization may face, as well as its vulnerabilities;
• Making a decision that defines the organization's risk management posture and the resulting security measures and procedures.

3. Information Security Management System (ISMS) Audit Procedures

The methodology for auditing an Information Security Management System (ISMS) is essentially the same as the steps involved in an internal audit. Furthermore, to conduct an IMS audit, it is essential to use a framework to define the audit objectives, which can be categorized into general and specific objectives. The most widely recognized and used framework in the field of IMS is the ISO 27000 series of standards.

The audit objectives are as follows:

3.1. General Objectives

The most common general objectives are (Yende, 2018):

• Identifying the organization's information assets: These include computer hardware, software, and databases. Therefore, effective and appropriate management procedures are necessary.
• Identifying risks: Appropriate management mechanisms must be in place to monitor vulnerable areas. This monitoring should be carried out by the RSSI (Resource Security Officer).
• Assessing threats: The RSSI is responsible for identifying the main risks associated with the various areas of the information system. These threats should be documented. • Impact Assessment: The Information Systems Security Officer (ISSO) must map the risks associated with the information system. This allows for the development of attack scenarios and the assessment of vulnerabilities.
• Control Assessment: This involves evaluating access control mechanisms, data encryption, and the disaster recovery plan.

3.2. Specific Objectives

Specific objectives are determined based on the audit client's interests and expectations, best practices in information security (such as those presented in ISO 27002: Good Practice Guide), or a combination of both.

IV. Field Study at the National Geophysical Institute

The preceding concepts and procedures were applied to the National Geophysical Institute in Algeria through an internal audit of the institute's information security system. This involved conducting interviews, analyzing documents, and observing the process.

1. Introduction to the National Geophysical Institute's Information Security System:

.

Journal of Information Systems Engineering and Management
2026, 11(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The National Geophysical Institute's information system comprises fourteen (14) applications developed internally by developers from the Digitalization and Information Systems Directorate and one (1) application acquired from an external vendor (BIG-Finance).

Table No. (01): Presentation of the current status of information technology applications used in the institution.

N°	Application	Domaine d'utilisation	Date mise en service	Nombre
01	BIG-Finance	Comptabilité générale	2011	63
02	IMMOBILISATION	Gestion des immobilisations	Juillet 2005	77
03	GRH	Gestion administrative, paie, etc.	Juin 2013	304
04	PRODUCTION	Production DES et DHT	Janvier 2014	67
05	FACTURATION	Facturation client	Janvier 2014	150
06	PRESTATION	Gestion des fournisseurs	Janvier 2014	321
07	ACHAT	Passation des marchés	Février 2014	188
08	FISCALITE	Fiscalité	Février 2014	11
09	QHSE	Management, décisionnel	Janvier 2015	158
10	T-BORD	Décisionnel	Janvier 2015	14
11	STOCK	Gestion des stocks multi magasins	Décembre 2015	373
12	COURRIER	Administration	Janvier 2016	3
13	GMAO	Gestion de la maintenance	Octobre 2016	182
14	JURIDIQUE	Affaires juridiques	Décembre 2016	16
15	Assurances	Gestion des sinistres	Aout 2018	21

Source: (October 2021)

Of the fourteen applications integrated into the National Geophysical Institute's information system, four are interconnected with the BIG-Finance accounting application, as shown in the following table :

Table 2: Applications Interconnected with BIG-Finance.

Applications	Nature des opérations interfacées
Facturation	Enregistrement des opérations de facturation (DES,DHT, DTS et DCDEV)
Stock	Enregistrement des entrées et sorties de stocks de PDR, consommables, Fournitures de bureau, Ravitaillement, Carburant et Médicaments
Immobilisation	Enregistrement des amortissements
GRH	Enregistrement des opérations de la paie

Source: (October 2021)

2. Methodology Used to Evaluate the Information Security Management System at the National Institute of Geophysics.

The methodology adopted for evaluating the Information Security Management System at the National Institute of Geophysics will be presented, consisting of the following steps:

2.1. Preparation for the Information Security Management System Audit:

The audit was conducted at the Digitalization and Information Systems Directorate, located at the National Institute of Geophysics in Boumerdès. The facility has a computer room with computers and a communications network, and stores data on various media. The audit was carried out as detailed below:

The preparation phase allowed for:

- Identifying the area to be audited;
- Identifying and assessing the risks and the controls implemented to manage them;

.

Journal of Information Systems Engineering and Management
2026, 11(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

- Preparing a table of risks and the controls implemented to manage them.

It should be noted that ISO 27001 was used as a reference for setting the requirements for the Information Security Management System, and ISO 27002 as a guide to good practices. The task was prepared as follows:

• Preliminary Study:

The preliminary study was conducted based on:

- Interviews with officials from the Digitalization and Information Systems Directorate.
- Review of collected documents, such as operating procedures and methods, the organizational structure, job descriptions, etc.

• Risk Assessment:

The main information security risks were identified during the preliminary study, as shown in the following table:

Table No. (03): Risk Assessment

Risks	Field
− -Differences between structures in the field of information security (viewpoint, method of understanding, how to apply)	***Information security policy***
-Diffused responsibilities. -Weak information security management activities. -Inadequate risk and threat management.	***Information security organization***
− - Improper installation of IT equipment (cramped offices, lack of ventilation, etc) − -Improper connection of electrical equipment (risk of overload, electric shock, etc.). − -Substandard electrical network posing a threat to the facility. − -Risk of flooding and dampness (rainwater, leaks in water pipes, etc.).	***Asset management, physical and environmental security, and data storage***
Information systems are down. Data transmission is disrupted.	***Information networks***
− - Risk of data manipulation. − -Risk of breach of professional confidentiality.	***Human resources and communications security***
− - Internally acquired or developed applications that do not meet user needs. − -Difficulty in maintaining information systems. − -The presence of source code containing malicious code.	***Acquisition, development and maintenance of information systems***
− - Lack of preparedness to face potential risks. − -Inadequate control and protection measures against cyber risks. − -User account impersonation. − -Data breaches. − -The information system is not protected against computer viruses.	***Operational Management***
− -Disruption/stoppage of activity in the event of a cyber incident. − -Difficulty resuming activity after a major incident.	***Information security incident management and business continuity***
− Difficulty in gathering, analyzing, and reporting information. − Impact on the decision-making process.	***Information system***

Source: (Prepared by researchers based on information obtained from the organization).

.

Journal of Information Systems Engineering and Management
2026, 11(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

• Mission Objectives:
The mission objectives were defined based on the aforementioned risks and are as follows:
 Information Security Policy:
- Ensure the existence of a formal and publicly available information security policy.
- Ensure the policy aligns with the organization's objectives.
 Information Security Organization:
- Evaluate the organization's information security structure.
- Verify the existence of appropriate procedures for addressing information security.
- Ensure the availability of the necessary human and material resources for information security management.
- Ensure regular security audits and reviews are conducted.
 Asset Management, Physical and Environmental Security, and Data Storage:
- Ensure that computer equipment and all data storage equipment are properly identified and installed in suitable locations (dedicated offices, workshops) and protected from physical and environmental hazards (humidity, flooding, etc.).
- Ensure that computer equipment is supplied with electricity in accordance with standards and that all equipment is equipped with surge protection devices. - Ensure the electrical network is constructed according to standards and does not pose a risk to the IT installations.
- Ensure that the drinking water and industrial water networks do not pose a risk to the IT installations.
- Ensure that any threats are identified and the necessary measures are taken.
 IT Networks:
- Ensure the network architecture is reliable and accessible to facilitate any intervention on the IT network.
- Ensure that IT network security is ensured by providing the necessary human and material resources.
- Ensure that IT networks are protected against various threats.
 Human Resources and Communications Security:
- Ensure that data manipulation risks are identified and that measures are implemented to control them.
- Verify the existence of an information security code of ethics for employees with access to information.
 Acquisition, Development, and Maintenance of Information Systems:
- Ensure the availability of database-related schemas and assess their security level.
- Ensure that source code is reviewed by individuals other than the developers to ensure it is free of malicious code. - Ensure that source code is secure by addressing technical vulnerabilities through the integration of security code.
 Operational Management:
- Ensure that risks (intrusions, attacks, malware) are identified and contained.
- Evaluate the implemented control and protection procedures.
- Evaluate application access controls.
- Ensure that antivirus software is secure and up-to-date.
 Information Security and Business Continuity Incident Management:
- Verify the existence and implementation of incident management procedures.
- Verify the existence of an information security incident management plan to ensure business continuity.
 Information System:
- Verify the existence of a dedicated information security system.
- Verify the existence of information security data analytics and reports.
• Work Program:
Prepared based on the audit objectives, the work program aims to define, distribute, plan, and monitor the audit activities as detailed in Table 4 below:

Table 4: Work Program

Auditing tools	Area/Objectives of Audit
	Information security policy
− Interview	− -Ensure that a formal and publicly available information security policy is

.

– Documentary Analysis	in place. – Ensure that the policy aligns with the organization's objectives.
Information security organization	
Interview -Documentary Analysis	– Assess the organization of the information security aspect. – Verify the existence of appropriate procedures for addressing information security. – Ensure the implementation of the necessary human and material resources for managing information security. – Ensure that security audits and reviews are conducted periodically.
Asset management, physical and environmental security, and data storage	
– Interview – Documentary Analysis – Observation	– Ensure that computer equipment and all data storage equipment are correctly identified and installed in their appropriate locations. – Ensure that the computer equipment is supplied with electricity according to standards and that all equipment is equipped with surge protection devices. – Ensure that the electrical network is constructed according to standards and does not pose a risk to the computer installations. – Ensure that any threats are identified and appropriate action is taken.
Information networks	
–Interview –Documentary Analysis -Observation	– Ensure the network infrastructure is reliable and accessible to facilitate any intervention on the information network. – Ensure that information network security is maintained by providing the necessary human and material resources. – Ensure that information networks are protected against various threats.
Human resources and communications security	
– Interview – Documentary Analysis – Observation	– Ensure that data manipulation risks are identified and that measures are in place to control them. – Verify that an information security code of ethics is in place for employees with access to information.
Acquisition, development and maintenance of information systems	
– Interview – Documentary Analysis	– Ensure the availability of database-related schemas and assess their security level. – Ensure that source code is reviewed by individuals outside the developer team to verify it is free of malicious code. – Ensure that source code is secure by addressing technical vulnerabilities through the integration of security measures.
Operational Management	
– Interview – Documentary Analysis – Observation	– Ensure that risks of breaches and attacks have been identified and contained. – Evaluate the implemented security and protection measures. – Assess application access controls. – Ensure that antivirus software is secure and up-to-date.
Information security incident management and business continuity	

.

Journal of Information Systems Engineering and Management
2026, 11(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

− Interview − Documentary Analysis	− Verify the existence and implementation of incident management procedures. − Verify the existence of an information technology incident management plan to ensure business continuity.
Information system	
−Interview −Documentary Analysis	− Verify the existence of a dedicated information security system. − Verify the existence of information security data analytics and reporting.

Source: (Institution).

2.2. Execution of the Task
Information Security Management System Audit:
The phase of executing the internal audit task at the National Geophysical Institute included conducting tests and documenting audit observations:
• Audit Tests: These consisted of:
 Performing the verification processes included in the work program;
 Preparing audit summaries, including test cover sheets;
 Gathering information and compiling evidence to support the audit observations.
• Audit Observations:
The identified deficiencies were documented on the observations form and presented to the relevant department heads for initial approval.
These forms collectively constitute the audit report, which will be presented at the conclusion of the audit task through data presentation and analysis.
2.3. Conclusion Phase
The conclusion phase of the task was dedicated to presenting and analyzing the data, culminating in the preparation of the audit report. This report included the most important observations noted during the task execution phase, highlighting strengths and areas for improvement. However, some verification processes necessitated the involvement of an expert in the electrical field.
• The positive points identified:
- The existence of a formal information charter, regularly updated and distributed to employees, clearly defining their rights and responsibilities regarding the use of information systems, in addition to the rules that must be respected in the field of information security.
- The existence of a confidentiality agreement signed by employees of the Digitalization and Information Systems Directorate, which enhances the protection of sensitive information.
- Complete control over data backup operations, through daily and weekly backups of all system databases.
- Control of risks associated with the electrical grid, through the provision of essential physical equipment (such as redundant power supply, the use of a high-capacity uninterruptible power supply, and a generator).
- Installation of security software, antivirus programs, and data protection systems such as a firewall.
- Development and testing of a plan for business recovery after a major incident. • Improvement Areas:
The improvement areas include correcting the deficiencies identified in several regions, as detailed below:
- Asset Management, Physical and Environmental Security, and Data Storage:
Defect #1: Network and Electrical Installations Threat to IT Equipment.

.

Journal of Information Systems Engineering and Management
2026, 11(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Severity Level: High

Event:

- Some circuit breakers supply power to several offices simultaneously, which contain IT equipment (desktop computers, printers, etc.).
- The electrical connections for some cabinets (e.g., first floor, north side) were incorrectly installed and pose a risk, as three electrical connections were made to a single neutral wire (serial connection).

Cause:

- Failure to adhere to established standards during the network and electrical installation.
- Insufficient resources available to the teams during the electrical installation.

Fault #2: Flooding Risk in the Instrument Room

Risk Level: High

Event:

- The instrument room of the Seismic Processing Directorate in Boumerdès is located in the basement of the building, making it constantly vulnerable to flooding.

Cause:

- Inadequate assessment of flood and natural disaster risks.
- Inadequate risk control measures.
- The instrument room is unsuitable for the equipment and activities carried out there.

Fault #3: Lack of Data Backup and Archiving for Some Directorates

Risk Level: High

Event:

- Unlike the previously mentioned interconnected application databases, which are regularly backed up and archived on disk and tape arrays, the Headquarters Directorate only benefits from the storage of data from the shared space (if available), and for a period not exceeding one month, without any actual or permanent data archiving.

Reason:

- Limited data storage capacity.
- Lack of analytical studies to identify data storage needs and provide appropriate solutions.
- Underestimation of the risks of losing unarchived data, exposing it to damage or loss.
- Human Resources and Communications Security:

Fault #4: Absence of an information security ethics code within the organization and failure to enforce confidentiality agreements.

Severity Level: High

Event:

- The organization lacks an information security ethics code. Furthermore, the information usage charter does not adequately address confidentiality and data manipulation.

Reason:

- Deficiencies in information security culture and underestimation of associated risks.
- Weak coordination between departments within the organization and failure to share best practices (such as adherence to confidentiality and the professional code of conduct).
- Operational Management:

Fault #5: Users removing antivirus software.

Severity Level: High Event:

- Some users remove their antivirus software, claiming it improves internet connection quality (speed). As a result, computers are used without any protection.

Reason:

- Underestimating information security risks.

.

Journal of Information Systems Engineering and Management
2026, 11(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

- Users' disregard for the Information Usage Charter.
- Difficulty for the Digitalization and Information Systems Directorate staff to monitor all computer equipment.
- Information System:

Fault No. 6: Information System
Severity Level: Moderate
Event:
- The statistics compiled by the Digitalization and Information Systems Directorate regarding information security are limited to indicators provided by the system, such as: detected attacks, controlled attacks, spam, violations of the Information Usage Charter, etc., without conducting a deeper analysis of the data, such as: sources of attacks, causes of malfunctions, severity of incidents, etc.

Reason:
- Information related to the source of incidents is not retained.
- There is no clear and officially approved methodology for identifying and assessing risks. 3. Study Results

Following the audit conducted at the Digitalization and Information Systems Directorate level, which began with a preparatory phase including a preliminary study, the development of a risk assessment, and the identification of objectives to be achieved through a work program, the audit task was carried out. This task involved identifying and presenting the strengths and weaknesses observed. The most significant findings will be presented, along with the key recommendations based on the submitted study.
3.1. Findings: - Difficulty in identifying the source of electrical faults, necessitating the disconnection of power to all offices connected to the same circuit breaker during intervention.
- The existence of risks to the health and safety of employees as a result of these faults.
- The potential for damage to IT equipment due to electrical problems.
- The existence of a risk stemming from the use of high-energy-consumption devices.
- The possibility of overloading the electrical network, which could lead to a fire.
- A high risk of damage to IT equipment and loss of sensitive data.
- Limited data storage capacity.
- The lack of widespread use of shared spaces for storing and exchanging information between different departments. - Lack of awareness among operational departments regarding the importance of data backup, coupled with the absence of feasibility studies to assess actual needs and appropriate solutions.
- Underestimation of the risks of losing unarchived data and a failure to address them seriously.
- Inadequate oversight of risks associated with professional confidentiality and the potential for information manipulation.
- Exposure of IT equipment to threats due to a lack of protection, posing a risk to the organization's information network security.
- Inadequate collection and analysis of information security statistics.
- Insufficient knowledge of the organization's actual performance in the field of information security.

3.2. Recommendations and Suggestions:
After presenting all the findings, and based on the above, and in cooperation with the internal auditor of the organization under study, as well as the electrical expert for the same organization, the following recommendations and suggestions can be offered:
- Updating the electrical grid and its associated facilities, and addressing all previously identified technical issues.

.

- Taking the necessary preventive measures to mitigate the risks of floods and natural disasters. - Relocate the IT equipment room to a more secure location when necessary to enhance the protection of IT equipment.
- Increase data storage capacity at the Digitalization and Information Systems Directorate to meet growing needs.
- Expand the use of shared spaces for storing and exchanging information among all directorates and work teams.
- Conduct a comprehensive assessment of directorates' data deletion needs and propose appropriate and effective solutions.
- Develop and implement a code of conduct for information security for all users.
- Raise user awareness about the risks of disabling security software and emphasize the prohibition against removing antivirus programs.
- Ensure automatic updates for security software are enabled on all IT equipment within the organization.
- Document technical incident data and their causes, and prepare periodic statistics for analysis and utilization.
- Adopt a clear methodology for identifying and assessing risks regularly and systematically.

Based on the findings and recommendations, it can be concluded that internal auditing, while existing as an independent and effective function within the organization, requires greater methodological and technical support to ensure a high level of information security. Therefore, the contribution of internal auditing to improving the efficiency of the information security management system remains, but it requires organizational will and greater investment in tools, methodologies, and preventive analysis to ensure effective compliance with the ISO/IEC 27001 standard and to achieve effective protection of information assets.

Conclusion

This study falls within the research that seeks to highlight the role of internal auditing in improving the efficiency of information security management systems, in light of the technological and informational challenges facing the contemporary business environment, especially in institutions that rely heavily on digital information systems, and within the framework of the international reference standard ISO/IEC 27001.

The study began with a central problem: "To what extent does internal auditing contribute to improving the efficiency of the information security system at the National Geophysical Institute?" This problem was addressed through a theoretical framework that covered the basic concepts of internal auditing and information security, followed by a practical field application at the National Geophysical Institute.

Hypothesis Testing:

The results of the hypothesis testing largely confirmed the theoretical framework of the study, proving that:
- First Hypothesis: The applied study confirmed the existence of several actual weaknesses in the information security system, such as:
• Limited data storage capabilities.
• Lack of in-depth analysis of cyberattacks.
• Lack of a formal methodology for risk assessment.
-: The hypothesis is accepted.
- Second hypothesis: The field study showed that the organization does indeed apply a clear internal audit methodology, divided into four main stages: preparation, execution, conclusion, and follow-up. The process begins with risk analysis and the preparation of a detailed audit program, followed by the collection of evidence in the field, and then the drafting of the final report and the presentation of recommendations.
-: The hypothesis is accepted.

The findings can be summarized as follows:

.

- There is a structured internal audit within the organization, but its role still faces challenges in terms of the tools and technical methodologies adopted.
- There is an absence of a formal and continuous methodology for assessing information security risks at the organizational level.
- There are shortcomings in the analysis of cyberattacks and information incidents, with reliance on superficial reactions without in-depth study.
- There are tangible technical threats, such as power outages, that threaten the information infrastructure and employee safety.
- There are limited storage capacities, which may lead to the loss of sensitive and strategic data.
- There is weak digital coordination between departments, resulting from the ineffective use of shared digital spaces. The absence of a strategic vision for information security leaves the organization vulnerable to recurring risks without thorough analysis or continuous improvement.

All these findings confirm that internal auditing has the potential to play a pivotal role in enhancing the efficiency of the information security management system, but it requires structural development, greater integration with information security teams, and the use of advanced analytical tools based on artificial intelligence and data analytics.

References

1. auditors, T.i. (2017). Cadre de reference internationale des pratiques professionnelles de laudit interne-*Edition. 19.*
2. *autres, K. M. (2012). Evaluation of information security management system success factors: case study of municipal organizations. African journal of bussiness management, 06(14), p. 498.*
3. *bertin, E. (2013). Manual comptabilite and audit. Edition bertin, 556.*
4. *BOUDIA, M., & Ali DEBBI. (2020). The internal contribution in the internal control lamelioration. Research economics and managers, 14(03), p. 03.*
5. *Bourliataux, S., Cyril Gallitre, & Yvers Roy. (2008). System information de gestion. Paris: Paris.*
6. *cybersecurity and privacy protection — Information security management systems — Requirements (third edition), https://www.iso27001security.com/. Information security.*
7. *https://sarasecurit.wordpress.*
8. *https://www.iso.org/fr/standard/27001*
9. *Khalida, B. (2020). Lapport to the Internet in the lamelioration of the information management system.*
10. *Lachapelle, E. (s.d.). Introduction to standard ISO 27001.06.*
11. *SCHICK, P., JACQUES VERA, & OLIVIER BOURROUICH-PAREGE. (2014). Audit internal references for risks. Dunod: Paris.*
12. *Yende, R. G. (2018). Support for downloading system information.*
13. *Ethar Abdulhadi Al-Faihan. Evaluating the Information Security Management System at the Iraqi Commission for Accounts and Information Technology according to the international standard ISO/IEC 27001:2013. Journal of Economic and Administrative Sciences, 21(86).*
14. *Iman Sahrawi et al. (2020). The Spread of the ISO 27001 Information Security Management System Application in Business Organizations: An Evaluation Study for the Period 2006-2007. Afaq Ilmiya Journal, 12(02).*
15. *Boulfrakh Sara. (2022-2023). The Role of Internal Auditing in Risk Management in Algerian Institutions (Doctoral Dissertation). Faculty of Economic, Commercial and Management Sciences, Setif: Ferhat Abbas University Setif 1.*
16. *Hajim Al-Tai Youssef et al. (2009). Quality Management Systems in Production and Service Organizations. Amman, Jordan: Dar Al-Yazouri for Publishing and Distribution.*
17. *Hassan Taher Daoud. (2000). Computers and Information Security. Riyadh: General Administration for Printing and Publishing.*
18. *Khalaf Abdullah Al-Wardat. (2017). Internal Auditing: Between Theory and Practice. Jordan: Al-Warraq Foundation for Publishing and Distribution.*
19. *Ru'a Younis. (n.d.). A Study of the Reality of Information Systems Security Management in Syrian Institutions. Al-Baath University Journal, 39(31).*

.

20. *Imad Abdul Wahab Al-Sagh. (2003). Information Systems and Their Components. Amman: Dar Al-Thaqafa for Publishing and Distribution.*
21. *Fatima Ahmed Ibrahim. (2016). Factors Affecting the Quality of Internal Audit Reports in Palestinian Ministries and Governmental Institutions Operating in the Gaza Strip (Master's Thesis). 19. Faculty of Commerce, Islamic University, Gaza: Islamic University - Gaza.*
22. *Kahoul Basma, and Saeeda Tayeb. (2018). The Importance of Using the International Standard ISO 27001 for Information Systems Management. Al-Mustaqbal Journal for In-Depth Economic Studies, 01(01).*
23. *Lounis Nadia. (2010/2011). The Impact of Information and Communication Technology on Activating Business Operations in Institutions (Unpublished Master's Thesis). 12. Faculty of Economic, Commercial and Management Sciences, Algiers: University of Algiers 3.*
24. *Prepared by the researchers based on information obtained from the institution.*
25. *Prepared by the researchers based on information obtained from the institution.*
26. *From the institution's documents (Institutional Information System Analysis Project Report, October 2021).*
27. *From the institution's documents (Institutional Information System Analysis Project Report, October 2021).*
28. *Huda et al. Ben Mohamed. (2023). International Standards for Information Security Management. Journal of Research and Studies.*
29. *Huda Ben Mohamed. (2023). International Standards for Information Security Management. Journal of Research and Studies.*
30. *Haya Marwan Ibrahim Lazhan. (2016). The Effectiveness of the Role of Internal Auditing in Evaluating Risk Management According to the COSO Framework (Master's Thesis). 17. Faculty of Commerce, Islamic University, Gaza: Islamic University - Gaza.*

.