# The Role of Information Systems Auditing in Enhancing Cybersecurity Within Organizations

**Chikh abdelkader** *
Laboratory of Enterprise Economics and Applied Management,
University of Hadj Lakhdar Batna 1- Algeria
**Abdelkader.chikh@univ-batna.dz**

**Lazhar khaldi**
Mouloud Mammeri University – Tizi-Ouzou (Algeria),
**lazhar.khaldi@ummto.dz**

Received: 03/08/2025 Accepted: 26/08/2025 Date de publication: 22 /11/2025

**Abstract:**

In light of the rapid digital transformation taking place globally, information systems have become a strategic necessity within organizations, making them increasingly vulnerable to cyber threats. This study aims to analyze the relationship between information systems auditing and cybersecurity, and to assess the effectiveness of such auditing as a control tool for detecting vulnerabilities, evaluating risks, and enhancing regulatory compliance.

A descriptive-analytical approach was adopted, supported by a field study involving a sample of chartered accountants, certified public accountants, internal auditors, and administrative staff in organizations based in the Wilaya of Batna. Data were collected through structured questionnaires and statistically analyzed to test the research hypotheses.

The findings reveal that information systems auditing significantly contributes to improving the cybersecurity posture of organizations by supporting security policies, reducing system vulnerabilities, and enhancing compliance. The results also indicate a high level of awareness among organizations regarding the importance of this type of control.

**Keywords**: Information Systems, Information Systems Auditing, Cybersecurity, Security Vulnerabilities.

**Jel Classification Codes :** M42, L86.

* Corresponding author.

**Introduction:**

The world is currently undergoing a comprehensive digital transformation that has affected all vital sectors, leading to an increasing reliance on information systems in managing administrative, financial, and service operations. Despite the advantages of this shift, it has been accompanied by a significant rise in cyber threats targeting data confidentiality, system integrity, and service continuity. In this context, cybersecurity has become an urgent necessity—not limited to technical aspects alone but extending to administrative and control dimensions, most notably information systems auditing.

Various reports indicate that many organizations struggle to detect vulnerabilities and respond to cyberattacks due to the absence of effective control mechanisms. Within this framework, information systems auditing serves as a central tool for evaluating the effectiveness of security controls, analyzing risks, and ensuring compliance with adopted policies and standards. Through this tool, organizations can strengthen their defense infrastructure and develop more flexible and effective strategies to counter threats.

The need for this type of auditing is even more pronounced in organizations pursuing digital transformation, where information becomes a strategic asset that must be protected. While some entities have already begun implementing periodic audit practices, the greatest challenge lies in linking audit findings to actual improvements in cybersecurity posture—an issue this study aims to explore by assessing its realism and practical impact.

**Problem Statement:**

Based on the above, the main research question can be formulated as follows:

**What is the role of information systems auditing in enhancing cybersecurity within organizations?**

From this main question, the following sub-questions are derived:

- To what extent are organizations aware of the importance of information systems auditing as a control tool?
- How can information systems auditing contribute to identifying and addressing security weaknesses in information systems?
- Is there a statistically significant relationship between the quality of information systems auditing and the organization's ability to respond to cyber risks?

**Research Hypotheses:**

- There is a high level of awareness among the surveyed organizations regarding the importance of information systems auditing.
- There is a high level of awareness among the surveyed organizations regarding the importance of cybersecurity.
- There is a statistically significant relationship between information systems auditing and cybersecurity in the surveyed organizations.
- Information systems auditing has a statistically significant impact on cybersecurity in the surveyed organizations.

**Significance of the Study:**

The significance of this study lies in its focus on a critical aspect of the digital work environment by linking two fundamental domains—auditing and cybersecurity. The goal is to highlight the strategic role of technical oversight in mitigating digital risks and fostering a culture of security governance.

**Objectives of the Study:**

- To explore the fundamental concepts of both information systems auditing and cybersecurity.
- To identify the relationship between auditing mechanisms and the level of security in information systems.
- To demonstrate the extent to which auditing contributes to the identification of vulnerabilities and risk analysis.
- To evaluate organizational compliance with security standards through auditing practices.
- To provide recommendations for aligning auditing functions with information security in a comprehensive manner.

**Research Methodology:**

The study adopts a descriptive-analytical approach through the review of relevant literature and previous studies. In addition, a structured questionnaire was used to collect data from a sample comprising chartered accountants, certified public accountants, internal auditors, and administrative staff from various organizations in the Wilaya of Batna. The collected data were then statistically analyzed to test the research hypotheses.

**Section One: The Nature of Information Systems Auditing**

**First: The Concept of a System**

**1. Definition of a System**

The term "system" refers to a set of components or elements that work together in a coordinated and organized manner, according to specific procedures and rules, to achieve a particular objective or a group of objectives. **(Al-Jajawi, T. M. A., & Al-Jubouri, F. A. M, 2013, p. 10)**

**2. Components of a System**

A system consists of a set of parts or subsystems that are functionally related and interact with each other to achieve common goals. These components include: **(Sayad, Sabah, 2018/2017, pp. 09-10)**

- **Inputs:** All elements, data, and information that enter the system, whether originating from the organization's internal environment or external surroundings.
- **Processes:** All operations, functions, and activities performed on the inputs to transform them into outputs.
- **Outputs:** The results of processing and transformation, which may take the form of products, services, information, or other deliverables.
- **System Boundaries:** Each system has internal and external environments, with boundaries separating the two. These boundaries can be physical or intangible. Their significance lies in the design phase, where elements belonging to the system are distinguished from those that do not.
- **Control:** Aims to monitor all operations taking place within the system.
- **Feedback:** Refers to the process of retrieving information to compare it with predefined standards and objectives in order to identify deviations.

**Second: Information Systems**

**1. Definition of Information Systems**

There are various definitions of information systems, with one of the most prominent being: "An information system is an organized set of resources—hardware, software, personnel, data, and procedures—that enables the collection, processing, and storage of information in the form of data, text, images, sound, etc., within and across systems." **(Chantal Morley, Jean Hugues, Bernard Leblanc, 2008, p. 48)**

**2. Types of Information Systems**

Scholars and researchers have proposed various classifications of information systems. Some categorize them based on management level, while others use functional criteria. According to administrative levels, information systems can be classified into three main types, ascending from the lowest level to the highest: **(Abdelwahid, A. S. I. , 2015, pp. 36-38)**

- **Operational Level Systems:** These support operational managers and assist them in performing basic activities and business transactions. Their primary function is to monitor routine operations.
- **Management Level Systems:** These support middle management in monitoring, supervising, decision-making, and performing various administrative tasks.
- **Strategic Level Systems:** These assist senior executives in formulating strategies and addressing strategic issues within and outside the organization.

**Third: Information Systems Auditing**

1. **Definition of Information Systems Auditing**

Information systems auditing is the process of collecting and evaluating audit evidence to determine whether a computer-based system contributes to safeguarding assets, ensuring data integrity, managing resources efficiently, and achieving organizational objectives. **(eli, N., & Behaz, J. , 2024, p. 158)**

2. **Objectives of Information Systems Auditing**

The primary objectives of information systems auditing include: **(Mabsout & Saleh, 2013, p. 08)**

- **Protection and Security of IS Resources and Assets:** This involves safeguarding all infrastructure elements of information systems, such as hardware, software, files, data, system documentation, and operation manuals, as well as protecting specialized human resources. Loss or damage to any of these components can adversely impact the organization.
- **Data Integrity and Maintenance:** Since data are the core resource of information systems, they must be accurate, complete, current, and valid. Auditing prevents data fraud and manipulation, thereby enhancing credibility and integrity through examination of input controls, processing routines, and system logic.
- **System Efficiency and Effectiveness:** Auditors assess system strengths and weaknesses to ensure the effectiveness of implemented systems and the quality of their outputs, along with user interaction. They also evaluate the extent to which system capabilities are fully utilized.
- **Information Systems Security and Integrity:** Auditing ensures that proper security and management procedures are in place and are followed by system administrators, operators, and maintenance staff. It often results in recommendations to improve information security and system performance.
- **Assessment of Software and Asset Management Controls:** Organizations must have strong controls for handling software as valuable assets, including procurement, installation, licensing, and maintenance.
- **Evaluation of IS Risk Management:** A comprehensive risk management program enhances decision-makers' confidence. The auditor evaluates risks related to IS management and provides necessary recommendations. Common risks include hardware and software failures, exposure to malware, and data storage device damage.

3. **Types of Information Systems Auditing**

Several authorities have categorized IS audit types. According to Lawless & Goodman, audit procedures follow three structured approaches: **(https://ar.wikipedia.org , 2025)**

- **Technological Innovation Audit:** Focuses on risks associated with new or ongoing projects, evaluates the organization's competence with selected technologies, and examines market positioning.
- **Comparative Innovation Audit:** Evaluates the innovation capabilities of the audited company and compares them to competitors, including a historical review of product innovation.
- **Technological Functions Audit:** Assesses current and required technologies in the organization.

Other classifications define five audit domains:

- **Systems and Applications:** Evaluates the adequacy and control of systems to ensure accurate, timely, and secure data input, processing, and output.
- **Information Processing Facilities:** Assesses the control environment of processing facilities to ensure data is handled accurately and efficiently, even under disruptive conditions.
- **Systems Development:** Ensures that systems under development align with organizational goals and conform to established development standards.
- **IT Management and Enterprise Architecture:** Reviews organizational structures and procedures to ensure a controlled and effective information processing environment.
- **Client/Server, Telecommunications, Intranet, and Extranet:** Evaluates the presence and effectiveness of telecommunications controls between clients and servers, including networks.

Some authorities reduce IS auditing to two major types:

- **General Control Audit**
- **Application Control Audit**

**4. Steps of Information Systems Auditing**

Auditing IS involves reviewing all system components: **(Ziyad Abdel-Halim et al, 2011, p. 37)**

- **Personnel Controls:**
  - Separation of duties
  - Mandatory annual leave for employees
  - Password enforcement and access control software
- **Hardware Controls:**
  - Secure physical location of equipment
  - Restriction of access to authorized personnel
  - Backup of critical files stored in secure locations
  - Insurance coverage for hardware
- **Software Controls:**
  - Approval procedures for new software
  - Validation of control groups within software
  - Surprise audits during software operation
  - Random use of approved software during data processing
- **Database Controls:**

It is essential to protect organizational databases for the following reasons:

  - Computer files are not human-readable and require controls for accessibility.
  - They contain critical and confidential organizational data that must be protected from misuse.
  - They store large volumes of data vulnerable to power outages or fluctuations.
  - Databases are considered valuable assets and should be protected like other organizational assets.

**Section Two: Cybersecurity**

With the massive expansion in the use of technology and the growing reliance on information systems across various sectors, cybersecurity has become one of the most significant challenges facing modern institutions. The digital transformation has given rise to increasingly diverse and complex cyber threats, necessitating the implementation of effective mechanisms to protect data and systems from breaches, leaks, and various forms of cyberattacks.

**1. Definition of Cybersecurity and Its Importance in Institutions**

**1.1 Definition of Cybersecurity**

Cybersecurity refers to the protection of sensitive information, data, and computer systems from hackers, cybercriminals, and malicious software. The primary objective is to ensure the confidentiality, integrity, and availability of data and to safeguard digital information from unauthorized manipulation or exploitation. **(Bouarafa, Oussama, 2025, p. 02)**

**1.2 The Importance of Achieving Cybersecurity**

The ultimate goal of cybersecurity lies in the ability to withstand intentional and unintentional threats, respond to incidents, and recover from them, thereby minimizing the risk of harm or damage resulting from the disruption or misuse of information and communication technology. This includes protecting networks, computers, software, and data from attacks, damage, or unauthorized access.
This need has become even more pressing with the emergence of cyber warfare among major powers, signaling the decline of traditional wars that relied on heavy weaponry and the rise of digital warfare.

Cybersecurity revolves around three core principles: **(Matrouh & Ouniss,, 2022, p. 224)**

- **Confidentiality**: Controlling access to data and ensuring it is only available to authorized individuals.
- **Integrity**: Maintaining the accuracy and consistency of data, protecting it from tampering or theft.
- **Availability**: Ensuring systems, services, and data are accessible and operational whenever needed by the organization and its clients.

In today's interconnected world, all stakeholders benefit from robust cybersecurity measures. The significance of cybersecurity can be summarized as follows:

- Safeguarding information, ensuring its integrity, and preventing unauthorized tampering.
- Ensuring the availability of data when required.
- Protecting devices and networks from breaches, creating a secure environment for data.
- Identifying system vulnerabilities and addressing them proactively.
- Utilizing and developing open-source tools to meet cybersecurity objectives.
- Providing a secure digital work environment over the internet.

- Preventing unauthorized access to networks.
- Enhancing the protection of information and ensuring business continuity.
- Strengthening stakeholders' trust in the organization.
- Accelerating the retrieval of confidential data in case of a cybersecurity breach.

**2. Types of Cybersecurity**

Given the various definitions of cybersecurity, it can be categorized into several types, including: **(Tawfiq & Morsi, 2022, p. 767)**

- **Network Security**: Focused on protecting computer systems from attacks originating within or outside the network. Key tools include firewalls, which act as barriers between internal and external systems, and email security solutions.
- **Application Security**: Protects data related to specific applications on a computer through measures like password protection, authentication processes, and security questions to verify user identity.
- **Cloud Security**: Refers to the protection of data stored in cloud computing platforms. As cloud storage becomes more popular than local storage, the need to secure cloud-based data has grown significantly.
- **Operational Security (OpSec)**: Involves managing risks associated with internal cybersecurity operations. Risk management experts develop contingency plans for potential breaches and train employees on best practices to mitigate threats.

**3. Cybersecurity Threats**

Cybersecurity threats are vast and constantly evolving. They can generally be classified into four main categories: **(Hamidi & A. Taylib, 2022, p. 10)**

- Threats targeting computer networks.
- Threats aimed at breaching systems to destroy software or data.
- Threats utilizing computers as tools in attacks.
- Threats exploiting stored data without authorization.

Common types of cybersecurity threats include: **(Sanaa & Abdullah , 2024, p. 819/820)**

- **Malware**: One of the most widespread cyber threats, created by hackers to disrupt or damage users' computers. It typically spreads through phishing emails or seemingly legitimate downloads and can be used for financial gain or politically motivated attacks.
- **Viruses**: Self-replicating programs that attach to clean files and spread throughout a computer system, infecting files with malicious code.
- **Trojans**: Malware disguised as legitimate software. Cybercriminals trick users into installing Trojans, which then damage or steal data.

- **Spyware**: Software that secretly records user activity, often used to obtain sensitive information like credit card details.
- **Ransomware**: Encrypts user data and demands payment in exchange for restoring access.
- **Adware**: Advertising software that can also serve as a vector for malware.
- **Botnets**: Networks of malware-infected computers that criminals use to perform tasks online without the user's consent.
- **SQL Injection**: A type of cyberattack that allows attackers to manipulate databases using malicious SQL queries, often resulting in unauthorized access to sensitive data.
- **Phishing**: A deceptive method where cybercriminals send fake emails posing as legitimate organizations to trick recipients into revealing sensitive information.
- **Denial-of-Service (DoS) Attacks**: Involve overwhelming a system, server, or network with traffic to disrupt legitimate access and operations, effectively crippling the organization's digital infrastructure.

**Section Three: The Relationship Between Information Systems Auditing and Cybersecurity**

In light of the growing cyber threats, information systems auditing is no longer limited to evaluating technical efficiency. It now plays a pivotal role in supporting and enhancing cybersecurity within organizations. Effective auditing can uncover vulnerabilities and security loopholes, and ensure the organization's compliance with established security standards and policies.

**1. The Role of Auditing in Risk Assessment**

Risk assessment is an essential component of risk management practices in organizations worldwide. It involves identifying threats and vulnerabilities across the organization's assets and operations. This is a crucial task for the cybersecurity team, as each weakness must be addressed—whether by eliminating the risk, mitigating it, transferring it, or accepting it—but it cannot be ignored. **(Hassan Mohammed Al-Hussein, 2022, p. 29)**

Audit activities must assess institutional risks related to governance, operational processes, and information systems in terms of: (Sarah Polfrakh, 2023, p. 113)

- Achieving the organization's strategic objectives
- Reliability and credibility of financial and operational data
- Operational effectiveness and efficiency
- Asset protection
- Compliance with laws, regulations, policies, procedures, and contractual obligations

Auditors are also expected to assess the organization's cybersecurity risks and controls as part of the audit process. This includes evaluating the entity's risk management practices, information security policies, and IT

controls to determine whether they are adequate to mitigate cybersecurity threats and protect financial data and systems.

**2. Auditing's Contribution to Identifying Security Vulnerabilities and Enhancing the Security Posture**

Security vulnerabilities often stem from software or hardware flaws. When attackers become aware of these vulnerabilities, they exploit them using specialized software known as **"Exploits."** The act of exploiting these vulnerabilities is referred to in cybersecurity as an **"Attack."** (Osama Hossam El-Din,, 2017, p. 20)

Cyber audits help identify weaknesses in information systems, network infrastructure, and the organization's security protocols. Through a comprehensive review of existing security measures, audits reveal potential entry points for cyberattacks, enabling organizations to prioritize and address these vulnerabilities promptly. **(Mahmoudi Amhamed, 2024, p. 29)**

Moreover, cyber auditing reinforces security measures by exposing flaws in existing controls and updating security policies, thereby reducing the risk of cyberattacks. **(Mahmoudi Amhamed, 2024, p. 30)**

**3. The Role of Auditing in Ensuring Regulatory Compliance**

The growing prevalence of cybersecurity risks has led to the establishment of numerous regulations and guidelines aimed at protecting sensitive data and ensuring the integrity of financial reporting. Auditors must verify that organizations comply with such regulations—such as the General Data Protection Regulation (GDPR)—by assessing whether: **(Abeer Zarq, 2022, p. 42)**

- Clear and up-to-date cybersecurity policies and procedures are in place
- There is adherence to national and international cybersecurity standards and frameworks
- Disaster recovery and data restoration procedures are well established

**4. Adapting the Audit Process to Address Cybersecurity Risks**

**1. Developing Cybersecurity Expertise:**

Auditors must enhance their knowledge of cybersecurity risk management and control frameworks to assess an organization's exposure to cyber threats effectively. This may include earning specialized certifications (e.g., Certified Information Systems Auditor - CISA), attending training programs, and staying informed of emerging trends and best practices in cybersecurity. **(https://gridlex.com, 2025)**

3. **Leveraging Technology and Data Analytics:**

   Auditors can use advanced technological tools and data analytics to strengthen their capacity to detect and evaluate cybersecurity risks.

4. **Collaborating with IT and Cybersecurity Specialists:**

   Given the complexity of cybersecurity risks, auditors may need to collaborate with IT and cybersecurity professionals to gain the necessary expertise and insights for evaluating cybersecurity controls and risk

management practices. This could also involve engaging external experts to address specific challenges posed by cybersecurity threats.

**5. Adopting a Risk-Based Audit Approach:**

A risk-based audit approach helps auditors prioritize their efforts and allocate resources to areas most vulnerable to cybersecurity threats. This involves:

- Identifying and evaluating the organization's critical systems and processes
- Assessing the likelihood and potential impact of cybersecurity incidents
- Designing audit procedures that address these specific risks
- Using data analytics and technological tools
- Working in close coordination with specialists to ensure effective risk coverage

## Section Four: Field Study

### 1. Study Methodology, Population, and Sample

#### 1.1 Study Methodology

The choice of methodology is not arbitrary; it is determined by the nature of the research topic and the study's objectives. Since the present research aims to investigate the role of information systems auditing in enhancing cybersecurity within institutions—and the targeted population includes certified accountants, statutory auditors, internal auditors, and administrators from various institutions in the Wilaya of Batna—the study falls within the scope of descriptive research. Therefore, the **descriptive analytical method** was adopted as the most appropriate approach to achieve the objectives of this research.

Accordingly, we employed the descriptive analytical approach to verify the research hypotheses, as the nature of the topic necessitated its use. This method was applied to describe and analyze the role of information systems auditing in enhancing cybersecurity within organizations.

#### 1.2 Study Population and Sample

The study population refers to a group of individuals or elements that share one or more characteristics that distinguish them from others and upon which the research is conducted. In this study, the population consists of certified accountants, statutory auditors, internal auditors, and administrators working in several institutions in the Wilaya of Batna.

Due to the difficulty in reaching all potential respondents within the targeted institutions, **a non-probability purposive sampling** method was adopted. Consequently, **50 questionnaires** were distributed, and **42 valid responses** were collected and deemed suitable for statistical analysis.

**2. Questionnaire Reliability Test**

After collecting and organizing the responses, the data was analyzed statistically using **Cronbach's Alpha coefficient** to test the internal consistency and reliability of the questionnaire across all its dimensions. The results obtained are presented in the following table:

**Table (01): Cronbach's Alpha Reliability Coefficient**

| Dimension | Number of Items | Cronbach's Alpha |
|---|---|---|
| Information Systems Auditing | 8 | 0.671 |
| Cybersecurity | 9 | 0.845 |
| Relationship Between IS Auditing and Cybersecurity | 20 | 0.881 |
| Overall Reliability | 27 | 0.784 |

**Source:** Prepared by the researcher based on SPSS output.

From the table, it is evident that the **overall Cronbach's Alpha coefficient** is **0.784**, while the coefficients for the individual dimensions of the study range from **0.671 to 0.881**. As all values exceed the threshold of **0.6**, this indicates that the data collection instrument used in the present study (i.e., the questionnaire) demonstrates a **high level of internal consistency and reliability**, and is therefore suitable and dependable for use in the main empirical research.

**Third: Normality Test**

To verify whether the study variables follow a normal distribution, the Kolmogorov-Smirnov and Shapiro-Wilk tests were applied. The results are presented in Table (02):

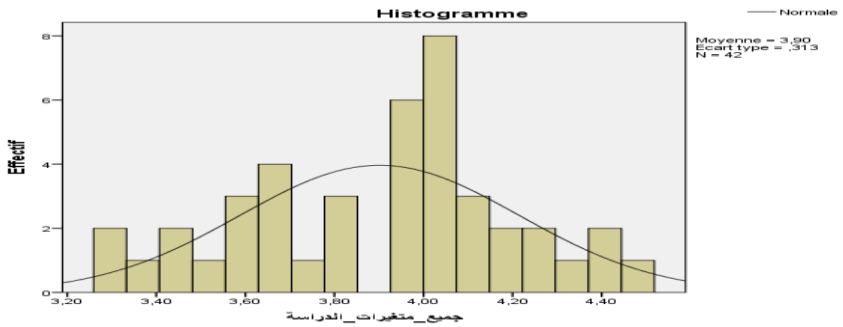
**Table (02): Normality Test Results**

| Dimension | Kolmogorov-Smirnov | df | Sig. | Shapiro-Wilk | df | Sig. |
|---|---|---|---|---|---|---|
| All Study Variables | 0.127 | 42 | 0.088 | 0.963 | 42 | 0.193 |

**Source:** Prepared by the researcher based on SPSS output.

As shown in the table above, the significance level (Sig.) for all the variables combined in the study is 0.088 according to the Kolmogorov-Smirnov test and 0.193 according to the Shapiro-Wilk test. Since both values are greater than the significance threshold of 0.05, this indicates that the data follows a normal distribution. Accordingly, it is statistically appropriate to proceed with the parametric tests in testing the research hypotheses.

**Figure (1): Normality Test**




**Source:** Prepared by the researcher based on SPSS output.

**Fourth: Presentation and Analysis of Respondents' Answers**

The analysis of respondents' answers regarding the study variables is presented through the arithmetic mean of each item, the corresponding dimension, and the overall dimension.

**1: Presentation and Analysis of Respondents' Answers Regarding Information Systems Auditing**

The analysis of respondents' answers regarding information systems auditing is presented through the arithmetic mean of each item, the corresponding dimension, and the overall dimension.

**Table (03): Arithmetic Mean and Standard Deviation for the Information Systems Auditing Variable**

| No. | Statement | Mean | Std. Deviation | Level of Agreement | Rank |
|---|---|---|---|---|---|
| 1 | Institutions use modern technologies in information systems auditing. | 4.31 | 0.563 | Very High | 2 |
| 2 | Periodic audits are conducted on information systems in institutions. | 4.62 | 0.539 | Very High | 1 |
| 3 | Information systems auditing is an effective tool to detect system vulnerabilities. | 4.02 | 0.869 | High | 4 |
| 4 | Auditors possess the necessary competencies to detect security risks in information systems. | 3.74 | 1.061 | High | 6 |
| 5 | Information systems auditing includes a comprehensive evaluation of all system components. | 4.12 | 0.803 | High | 3 |
| 6 | Information systems auditing contributes to identifying security issues before they escalate. | 3.67 | 1.004 | High | 7 |
| 7 | Information systems auditing is an effective tool to ensure compliance with international security standards. | 3.57 | 1.107 | High | 8 |
| 8 | There are clear plans to update information systems auditing technologies in institutions. | 3.79 | 0.813 | High | 5 |
| | **Overall – Information Systems Auditing** | **3.98** | **0.477** | **High** | — |

**Source:** Prepared by the researcher based on SPSS outputs.

**Interpretation:**

The table above shows that the arithmetic mean for the practice of information systems auditing is 3.98, which corresponds to a high level of agreement as it falls within the range [3.4—4.2[. This indicates that the respondents generally agree at a high level regarding the importance of information systems auditing in the institutions under study. The standard deviation is 0.477, which is less than 1, indicating an acceptable level of dispersion in the sample's responses regarding this dimension.

**2: Presentation and Analysis of Respondents' Answers Regarding Cybersecurity**

The analysis of respondents' answers concerning cybersecurity is presented through the arithmetic mean for each statement, the corresponding dimension, and the overall dimension.

**Table (04): Arithmetic Mean and Standard Deviation for the Cybersecurity Variable**

| No. | Statement | Mean | Std. Deviation | Level of Agreement | Rank |
|---|---|---|---|---|---|
| 1 | Cybersecurity is one of the key pillars for ensuring business continuity and protecting digital assets in institutions. | 3.79 | 0.717 | High | 7 |
| 2 | Cybersecurity is a shared responsibility among all employees, not only IT personnel. | 3.90 | 0.759 | High | 2 |
| 3 | Effective cybersecurity practices require continuous investment in modern tools and technologies to detect cyber threats. | 3.90 | 0.726 | High | 1 |
| 4 | Cybersecurity is not limited to protective tools but also involves staff awareness on how to prevent attacks. | 3.95 | 0.825 | High | 3 |
| 5 | Implementing cybersecurity practices contributes to building trust between the organization and its clients. | 3.64 | 0.932 | High | 9 |
| 6 | Institutions rely on integrated strategies involving prevention, detection, and response to improve cybersecurity. | 3.88 | 0.942 | High | 5 |
| 7 | Cyber threats are constantly evolving, requiring institutions to regularly update their cybersecurity strategies. | 3.83 | 0.762 | High | 4 |
| 8 | Cybersecurity measures directly impact the protection of personal data and prevent data leakage. | 3.69 | 0.643 | High | 8 |
| 9 | Cybersecurity in institutions requires close collaboration with audit and review teams to ensure compliance with security standards. | 3.79 | 0.682 | High | 6 |
| | **Overall – Cybersecurity** | **3.82** | **0.523** | **High** | — |

**Source:** Prepared by the researcher based on SPSS outputs.

**Interpretation:**

As shown in the table above, the arithmetic mean for the level of attention to cybersecurity is **3.82**, which indicates a **high level of agreement**, as it falls within the range [3.4—4.2[. This reflects that the respondents generally agree on the importance of cybersecurity in the institutions under study. The **standard deviation is 0.523**, which is **less than 1**, indicating an acceptable level of variation in the respondents' answers regarding this dimension.

**3: Presentation and Analysis of Respondents' Answers Regarding the Relationship Between Information Systems Auditing and Cybersecurity**

The analysis of respondents' answers regarding the relationship between information systems auditing and cybersecurity is presented through the arithmetic mean for each statement, the corresponding sub-dimension, and the overall dimension.

**Table (05): Arithmetic Mean and Standard Deviation for the Variable of the Relationship Between Information Systems Auditing and Cybersecurity**

| No. | Statement | Mean | Std. Deviation | Level of Agreement | Rank |
|---|---|---|---|---|---|
| 1 | Information systems auditing helps conduct a comprehensive and accurate assessment of cyber risks within the organization. | 3.93 | 0.640 | High | 3 |
| 2 | The results of information systems audits are used to develop effective strategies for improving the security posture. | 3.93 | 0.712 | High | 4 |
| 3 | Information systems auditing contributes to the early detection of security vulnerabilities that may be exploited in attacks. | 3.90 | 0.692 | High | 7 |
| 4 | Regular auditing enhances the organization's ability to respond swiftly to cyber threats. | 3.95 | 0.764 | High | 2 |
| 5 | Information systems auditing supports compliance with cybersecurity-related regulations and laws. | 3.88 | 0.832 | High | 9 |
| 6 | Audit reports serve as a primary reference in cybersecurity-related decision-making. | 3.93 | 0.838 | High | 5 |
| 7 | An effective auditing system facilitates monitoring the organization's adherence to approved security policies and procedures. | 3.90 | 0.617 | High | 6 |
| 8 | Information systems auditing promotes transparency in cybersecurity management within the organization. | 3.90 | 0.932 | High | 8 |
| 9 | Reviewing security controls through auditing helps reduce the likelihood of future breaches. | 3.71 | 0.835 | High | 10 |

| No. | Statement | Mean | Std. Deviation | Level of Agreement | Rank |
|---|---|---|---|---|---|
| 10 | Audit results help identify and address security gaps in accordance with recognized standards and regulations. | 4.07 | 0.808 | High | 1 |
| | **Overall – Relationship Between IS Auditing and Cybersecurity** | **3.91** | **0.537** | **High** | — |

**Source:** Prepared by the researcher based on SPSS outputs.

**Interpretation:**

As shown in the table above, the arithmetic mean for the relationship between information systems auditing and cybersecurity is **3.91**, indicating a **high level of agreement**, as it falls within the range [3.4–4.2[. This suggests that respondents generally agree to a significant extent on the existence of a strong relationship between IS auditing and cybersecurity in the institutions under study. The **standard deviation of 0.537** is **less than 1**, which indicates an **acceptable level of dispersion** in the respondents' answers regarding this dimension.

**5: Testing the Study Hypotheses**

The study hypotheses are tested below using the appropriate statistical tests.

**1: Testing the First Hypothesis**

The first hypothesis states that:

**"There is a high level of awareness within the institutions under study regarding the importance of information systems auditing."**

This hypothesis is tested using the **One-Sample T-Test**, and the results are presented in Table (06).

**Table (06): Testing the First Hypothesis**

| Variable | Mean | Std. Deviation | Calculated T | Tabulated T | Significance Level (Sig.) |
|---|---|---|---|---|---|
| Information Systems Auditing | 3.98 | 0.477 | 13.295 | 2.01 | 0.000 |

**Source:** Prepared by the researcher based on SPSS outputs.

**Interpretation:**

The analysis of the above table shows that the **calculated T value (13.295)** is greater than the **tabulated T value (2.01)**, and the result is **statistically significant** at a **significance level of 0.000**, which is less than the adopted threshold of 0.05.

Moreover, the **mean score of 3.98** falls within a **high level**, which confirms that the respondents strongly agree on the importance of information systems auditing.

Accordingly, the **first hypothesis is accepted**, which states that:

**"There is a high level of awareness within the institutions under study regarding the importance of information systems auditing."**

**2: Testing the Second Hypothesis**

The second hypothesis states that:

**"There is a high level of awareness within the institutions under study regarding the importance of cybersecurity."**

This hypothesis is tested using the **One-Sample T-Test**, and the results are presented in Table (07).

**Table (07): Testing the Second Hypothesis**

| Variable | Mean | Std. Deviation | Calculated T | Tabulated T | Significance Level (Sig.) |
|---|---|---|---|---|---|
| Cybersecurity | 3.82 | 0.523 | 10.154 | 2.01 | 0.000 |

**Source:** Prepared by the researcher based on SPSS outputs.

**Interpretation:**

The analysis of the table above reveals that the **calculated T value (10.154)** exceeds the **tabulated T value (2.01)**, and the result is **statistically significant** at a **significance level of 0.000**, which is lower than the accepted threshold of 0.05.

Additionally, the **mean value of 3.82** indicates a **high level of agreement**, suggesting that the respondents recognize the importance of cybersecurity.

Therefore, the **second hypothesis is accepted**, which states that:

**"There is a high level of awareness within the institutions under study regarding the importance of cybersecurity."**

**3: Testing the Third Hypothesis**

The third hypothesis states that:

**"There is a statistically significant relationship at the ($\alpha \leq 0.05$) significance level between information systems auditing and cybersecurity within the institutions under study."**

This hypothesis was tested using the **One-Sample T-Test**, and the results are presented in **Table (08).**

**Table (08): Testing the Third Hypothesis**

| Variable | Mean | Std. Deviation | Calculated T | Tabulated T | Significance Level (Sig.) |
|---|---|---|---|---|---|
| Relationship between Information Systems Auditing and Cybersecurity | 3.91 | 0.537 | 10.996 | 2.01 | 0.000 |

**Source:** Prepared by the researcher based on SPSS outputs.

**Interpretation:**

The analysis of the table above shows that the **calculated T value (10.996)** is greater than the **tabulated T**

**value (2.01)**. Moreover, the **significance level (Sig.) is 0.000**, which is **less than the adopted threshold (0.05)** in the current study, indicating statistical significance.

In addition, the **mean value of 3.91** reflects a **high level of agreement** among the respondents.

Therefore, the **third hypothesis is accepted**, which states that:

**"There is a statistically significant relationship at the ($\alpha \leq 0.05$) significance level between information systems auditing and cybersecurity within the institutions under study."**

**4. Testing the Fourth Hypothesis**

The fourth hypothesis states:

**"There is a statistically significant impact at the significance level ($\alpha \leq 0.05$) of information systems auditing on cybersecurity within the institutions under study."**

The results of the simple linear regression test are shown in **Table (09)** below:

**Table (09): Results of the Simple Linear Regression Test for the Fourth Hypothesis**

| Independent Variable | Dependent Variable | R (Correlation Coefficient) | $R^2$ (Coefficient of Determination) | Calculated T | Tabulated T | Sig. Level |
|---|---|---|---|---|---|---|
| Information Systems Auditing | Cybersecurity | 0.543 | 0.295 | 4.092 | 2.01 | 0.000 |

**Source:** Prepared by the researcher based on SPSS outputs.

**Interpretation:**

The **calculated T value (4.092)** is greater than the **tabulated T value (2.01)**, and the **significance level (0.000)** is lower than the study's adopted threshold (0.05), indicating that the result is statistically significant.

There is a **positive and statistically significant correlation** between the independent variable (information systems auditing) and the dependent variable (cybersecurity), with a **correlation coefficient (R) of 0.543**, meaning 54.3% of the variation in cybersecurity practices can be explained by information systems auditing. Additionally, the **coefficient of determination ($R^2 = 0.295$)** indicates that 29.5% of the changes in cybersecurity levels are attributable to information systems auditing, while the remaining percentage is due to other factors.

Accordingly, the **fourth hypothesis is accepted**, confirming that:

**"There is a statistically significant impact at the ($\alpha \leq 0.05$) significance level of information systems auditing on cybersecurity within the institutions under study."**

**Conclusion**

In light of the growing challenges posed by the modern digital environment, **cybersecurity has become a strategic priority** for institutions. This has necessitated the integration of effective oversight tools, most notably **information systems auditing**.

The present study aimed to **analyze the relationship between information systems auditing and the level of cybersecurity** within organizations, through a field study conducted on a sample of economic institutions in the Wilaya of Batna.

The study was guided by a central research question:

**"What is the role of information systems auditing in enhancing cybersecurity within institutions?"**

This was further subdivided into a series of sub-questions and four primary hypotheses, tested using a **descriptive-analytical methodology** and appropriate **statistical tools**. The main findings are summarized as follows:

**Key Findings:**

- **First Hypothesis:** There is a high level of awareness among the institutions under study regarding the importance of information systems auditing. ⟶ **Confirmed.**
- **Second Hypothesis:** There is a high level of awareness among the institutions under study regarding the importance of cybersecurity. ⟶ **Confirmed.**
- **Third Hypothesis:** There is a statistically significant relationship between information systems auditing and cybersecurity. ⟶ **Confirmed.**
- **Fourth Hypothesis:** Information systems auditing has a statistically significant impact on cybersecurity. ⟶ **Confirmed.**

**Most Notable Results:**

- Information systems auditing is an **effective tool for enhancing cybersecurity** within institutions.
- The institutions studied **demonstrated a high level of awareness** of the importance of cybersecurity as part of their overall strategic priorities.
- There is a **direct and strong relationship** between the quality of audit practices and the level of information security.
- Information systems auditing serves as a **crucial gateway for developing cybersecurity policies** and guiding security strategies.
- Auditing contributes significantly to **identifying system vulnerabilities**, **assessing compliance**, and **supporting informed security-related decision-making**.

**Recommendations:**

Based on the findings of the study, the following recommendations are proposed:

- Foster a culture of **information systems auditing** as part of organizational governance and cybersecurity frameworks.
- Conduct **regular audits** that encompass both technical and administrative aspects of information systems.
- Establish **specialized audit teams** that combine accounting expertise with cybersecurity knowledge.
- Link audit outcomes with **cybersecurity improvement plans**.
- Continuously update **security policies and procedures** in response to audit findings and emerging risks.

- Encourage **academic research and professional training** in the area of integrating information systems auditing and cybersecurity.

**Bibliographie**

1. Al-Jajawi, Talal Mohamed Ali & Al-Jubouri, Fouad Abdul Mohsen. (2013). Accounting Information Systems and Their Effectiveness in Light of the Strategic Role of Business Organizations. Ktab INC.

2. Sayyad, Sabah. (2017/2018). Information Systems and Their Impact on the Competitiveness of Algerian Enterprises. Master's Thesis, Faculty of Economic Sciences, University of Oran 2.

3. Morley, Chantal, Hugues, Jean & Leblanc, Bernard. (2008). "UML 2 pour l'analyse d'un système d'information" (4th ed.). Dunod, France.

4. Abdelwahid, Aan Said Ibrahim. (2015). Information Security Policies and Their Relationship with the Effectiveness of Management Information Systems at the Palestinian University – Gaza Strip. Master's Thesis, Al-Azhar University, Faculty of Economics and Administrative Sciences.

5. Nacer, Teli & Behaz, Djilali. (2024). The Contribution of Information Systems Audit Standards to Strengthening Corporate Governance. "Al-Muqri Journal of Economic and Financial Studies", Vol. 8, No. 2.

6. Mabsout, Hawaria & Saleh, Elyas. (2013). Auditing and its Role in Evaluating the Effectiveness of Information Systems in the Organization. *Journal of Economic Sciences*, Vol. 8, No. 8.

7. Wikipedia (Arabic). Retrieved on April 29, 2025, at 17:30 from: [https://ar.wikipedia.org](https://ar.wikipedia.org).

8. Ziyad Abdel-Halim et al. (2011). Information Systems in Control and Auditing. Dar Al-Maisarah for Publishing, Distribution and Printing, Amman, Jordan.

9. Bouarafa, Oussama. (February 3, 2025). "Concepts of Cybersecurity."

10. Matrouh, Wafa & Ouniss, Ibtissam. (2022). The Repercussions of the COVID-19 Pandemic and Its Impact on Achieving Cybersecurity in Algeria. "International Journal of Social Communication", Abdelhamid Ben Badis University – Mostaganem, Vol. 09, No. 02.

11. Tawfiq, Salah El-Din Mohamed & Morsi, Sherine Eid. (2022). Requirements for Achieving Cybersecurity in Egyptian Universities in Light of Digital Transformation from the Perspective of Faculty Members. "The Educational Journal", Issue 105, November 23.

12. Hamidi, Hayat & Talib, Nassima. (2022). A Conceptual Introduction to Cybersecurity. "Madar Journal of Digital Communication Studies", Vol. 02, No. 02, November.

13. Al-Shdeifat, Sanaa Ahmad Abdullah. (2024). Cybersecurity and the Protection of Data and Information in the Departments of the Municipality of Manshiyat Bani Hassan. "Journal of Human and Natural Sciences", Vol. 05, No. 01.

14. Al-Hussein, Hassan Mohamed. (2022). "Fundamentals of Cybersecurity". Aleppo, Syria.

15. Boulefrah, Sarah. (2023). The Role of Internal Audit in Risk Management in Algerian Institutions. Doctoral Thesis, Ferhat Abbas University – Setif 1, Faculty of Economic Sciences.

16. Zarraq, Abeer. (2024). The Role of Information Systems Control in Reducing Cybersecurity Risks in the Public Sector. Central Authority for Financial Control – Aleppo Branch, Syrian Arab Republic.

17. Hossam El-Din, Osama. (2017). "Introduction to Cybersecurity 0.2". Kingdom of Saudi Arabia, September 19.

18. Mahmoudi, Mhamed. (2024). Cyber Information Systems Control. Audit Council.

21. GRIDLEX. (2025). "The Impact of Cyber Security Risks on the Audit Process in Accounting", April 28, 2025, 23:46. Available at: [https://gridlex.com](https://gridlex.com).