The role of information systems controls in reducing cybersecurity risks

in the Government Sector

Field Study - Central Financial Control Authority - Syria

The fourteenth competition organized by the Arab Organization of Supreme Audit Institutions

Accounting for Scientific Research in the Field of Control

Prepared by: Abeer Zarak

Central Financial Control Authority - Aleppo Branch

The Syrian Arab Republic

2024

Research Summary

The role of information systems controls in reducing cybersecurity risks in the government sector.

The research addresses the challenges imposed by technological development on the government sector, as many information systems and infrastructures connected to networks are exposed to the risk of breaches and attacks. Since monitoring information systems is considered an essential part of cybersecurity strategies, there is a need to monitor information systems in terms of their effectiveness in performing activities as well as ensuring their cybersecurity.

Focusing on operational and financial transaction processing in the government sector, the research aims to identify the role of control exercised by the Central Agency for Financial Control over information systems in reducing cybersecurity risks through the control practices it carries out, in addition to its evaluation of the internal control system within the information systems environment in the government sector.

The research dealt with the theoretical aspects of the components and elements of information systems, the concept and importance of information security, the concept of cybersecurity, the requirements for achieving it, and its risks. It also shed light on the importance of control as a vital tool for enhancing cybersecurity in the government sector.

Based on the relevant theoretical aspect and previous studies, the research objectives were as follows:

A questionnaire was prepared to achieve the following: The first hypothesis related to the role of demographic variables of the research sample individuals (gender, age, job title, academic qualification, years of job experience). The second hypothesis focused on questions about the control of information systems, which was divided into two axes:

• The role of internal control systems in the information systems environment in reducing cybersecurity risks in the government sector.

• The role of the Central Agency for Financial Control over information systems in limiting cybersecurity risks in the government sector.

The questionnaire was applied in the field with inspectors of the Central Agency for Financial Control branch in Aleppo Governorate. The research concluded that there were no fundamental differences with statistical significance in the answers of the research sample individuals regarding demographic variables. However, regarding the role of control over information systems in reducing cybersecurity risks, the following findings were made:

In the first axis, it was found that there is a significant role in reviewing the structure and framework of internal controls and statistically evaluating internal control by inspectors of the Central Agency for Financial Control.

In the second axis, it was found that there is no statistically significant role for the control practices carried out by the Central Agency for Financial Control over information systems in reducing cybersecurity risks in the government sector.

The research recommended several measures, including:

Enhancing training and professional development by organizing advanced and specialized training courses in the field of cybersecurity for all employees of the Central Agency for Financial Control.

Preparing and distributing guidance manuals with detailed explanations of roles, responsibilities, and specific procedures to be followed in the field of information systems control and cybersecurity.

Recruiting cybersecurity experts to coordinate efforts and provide technical support to the agency’s members in their tasks.

Table of Contents

Methodological Structure of the Research

Introduction:

One of the challenges imposed by the new world order in the current century is the tremendous scientific and technological development and the development of the role of technology in managing the work of institutions, until it became not limited to, but rather managing the institution by recording data, analyzing information, and performing mathematical operations for full management.[1]

The issue of information security and integrity is considered one of the most important issues of the era, as the success of any institution has become largely dependent on the information it possesses. However, many types of information, systems, and networked infrastructure are vulnerable from time to time, as they face various types of information breaches and are exposed to criminal activities (hackers) that disrupt their services and destroy their property. Hacker attacks vary between parties, locations, and times, using continuously renewed and developed penetration tools and mechanisms.[2]

With the emergence of modern technologies in information systems and digital technology, and the increasing number of companies that are present on websites and use them in their digital transactions, benefiting from them in their operational, production, and sales aspects, and even in collecting their revenues, their systems, operations, and activities have become exposed to many risks, threats, and challenges, including cybersecurity threats. This includes the loss and damage of data, systems, networks, and even private and sensitive information assets, manipulation, and disruption. This may cause companies to incur large costs and losses, undermine confidence, and thus the topic of cybersecurity has emerged, which includes information security on computer devices and networks, including the processes and mechanisms through which computer equipment, information, and services are protected from any unintended or unauthorized interference or

[1] Al-Hilali, Al-Hilali Al-Sharbiny (2020). "Journal of Educational Technology and Digital Education," Egyptian Society for Technological Development, Volume 1, Issue 1, p. 3.
[2] Al-Samhan, Mona Abdullah (2020). "Requirements for Achieving Cybersecurity for Administrative Information Systems at King Saud University," *College Journal of Education*, Issue 111, p. 1.

disruption. Therefore, cybersecurity has become a fundamental pillar in all organizations, institutions, and even countries that may face wars.[3]

Questions have been raised about the methods of monitoring and ensuring trust in electronic systems and electronic sites, especially the security of electronic sites dedicated to exchanging information related to e-government and beneficiary parties, and there is still doubt and fear regarding the adequacy of the security precautions designed to protect data sent over the electronic network. The question is raised about how the auditor obtains proof regarding the production of records that include all the operations that occurred between distant parties on the Internet. As a result of the growth of e-government, the units that deal with it are moving towards immediate data operations, reflected in accounting in the form of immediate, paperless data entry, and the invisible operation of accounting data. This leads to the development of government control methods to adapt to immediate systems. In order for the auditor to achieve the control objective efficiently and effectively, it has become necessary for the auditor to be fully familiar with electronic data operation systems, emerging problems in the systems environment, and the latest procedures and methods.[4]

The rapid and continuous changes in the business environment have increased the importance of information systems and internal control. Modern information systems must focus on data management and providing the necessary information to operate the business effectively. Internal control systems cannot function without the support of information systems. When an external auditor reviews the structure and framework of internal control, they will assess the control cycle of the information systems.

This will lead the auditor to study and evaluate the information systems in use, highlighting the relationship between information systems, internal control, and the auditor's procedures (control processes).[5]

[3] **Ali, Haya Jamal Hashem** (2023). "A Proposed Procedural Approach to Measure the Extent of the External Auditor's Response to Cyber Risks in the Client's Facility," *Scientific Journal of Financial and Commercial Studies and Research*, Faculty of Commerce, Damietta University, Vol. 4, No. 2, p. 2.

[4] **Al-Khasawneh, Reem Aqab** (2010). "Evaluation of Government Control Procedures in Light of the Application of E-Government in the Hashemite Kingdom of Jordan," *An-Najah University Journal of Research*, Volume 9/24, p. 2692.

[5] **Jassim, Adhraa Diaa** (2020). "The Role of Information Systems and Internal Control in Enhancing the Independence of Supervisory Work," *Journal of Administration and Economics*, Issue 126, p.186

In order for auditors to achieve control objectives, they must understand how to protect systems from various threats and have a good understanding of information systems, their capabilities, and the risks they face. [6]

Based on the above, the researcher sought to:

Understand the role of information systems control exercised by the Central Agency for Financial Control in reducing cybersecurity risks in the government sector. For this reason, the researcher divided the research into two parts:

- A: A part related to the theoretical aspect
- B: A part related to the practical analytical aspect of the study.

The general framework of the research was determined to give the reader a complete idea of the research problem, its questions, hypotheses, objectives, importance, limits, difficulties, and previous studies. The researcher addressed the theoretical aspect.

The research topic consists of two chapters as follows:

- Chapter One: Control of Information Systems
- Chapter Two: The Nature of Cybersecurity

The second part was devoted to the field study, where it dealt with the method and procedures specific to this research, and the research methodology, community, sample, tools, and sources of obtaining information were explained. Then, the results and recommendations were presented.

[6] Deban, Abdul Latif, 2004, Accounting Information Systems and Information Technology, p. 71

1. Research Problem:

Information technology and networking in government agencies, in light of the rapid technological development entering and the trend toward e-government and automation of administrative and financial work, have led to the adoption of information systems in various sectors to manage their daily operations. As a result, cyber risks have increased significantly. These risks include cyber threats such as cyber-attacks, data breaches, and malware, which can cause:

- Huge financial losses
- Loss of trust among customers
- Damage to the reputation of institutions

With the expansion of the use of Internet services globally, and the spread of its use in Syria in particular, the emergence of e-commerce and e-government, and reliance on Internet services in many aspects, the negative side of using the Internet has appeared with the emergence of new types of crimes arising from this service, called “cybercrime”, which includes acts of piracy, espionage, violation of privacy, and information theft.[7]

Therefore, there was an urgent need for international cooperation to reduce these cybercrimes and protect information security by exchanging expertise and cooperating to find legal and technical means to confront the dangers that threaten information security.

The public sector is more vulnerable to cyber-attacks due to:[8]

1. **Rich Data Repositories:** Public sector organizations often hold vast amounts of sensitive data, including citizen data, government secrets, financial records, etc. This data is of great value to cybercriminals for various purposes such as identity theft, financial fraud, or espionage.

[7] **Al-Fawal, Issam** (2020). "Evaluating the Potential of Investment in Implementing an Information Security Management System in the Syrian Services and Communications Sector," *Ministry of Higher Education, Higher Institute of Business Administration*, Project Prepared for a Master’s Degree in Business Administration, Executive Management, p. 2.

[8] **Dodd, Vivek** (2024). "Cyber Risks in the Public Sector," *Skillcast*, May 2024. https://www.skillcast.com

2. **Critical Infrastructure**: Many public sector organizations manage critical infrastructure such as water supplies, transportation systems, and healthcare facilities. Disruption of these systems, being destroyed or damaged through cyber-attacks, could lead to widespread chaos and disruption.

3. **Political Motives:** Public sector organizations are government institutions, which may make them targets for politically motivated cyber-attacks. Hacker groups or state-sponsored actors may target government agencies to disrupt operations, spread propaganda, or steal information, because they are sensitive to political influence.

4. **Budget Constraints:** Public sector organizations often operate with limited cybersecurity budgets compared to their private sector counterparts. This may result in outdated or insufficient cybersecurity infrastructure, making them more vulnerable to cyberattacks.

The list of priorities of internet and information technology experts, along with cybersecurity, continues to guide the efforts of companies in combating information crimes and cyberattacks. In addition, legal measures and legislation are being implemented to protect victims of these crimes. Electronic threats and risks remain a significant concern for many countries, security agencies, and internet users worldwide.

In the first half of 2022, approximately 2.8 billion malware attacks occurred worldwide, and 236.1 million ransomware attacks were reported in 2023. [9]This highlights the urgent need for effective measures to reduce these risks, as controlling information systems is a crucial part of cybersecurity strategies. It is essential to monitor information systems to ensure their effectiveness in performing operational activities and processing transactions, as well as ensuring their cybersecurity. Financial security threats in the government sector have become increasingly complex and recurring.

[9] Lebanon<https://al-akhbar.com

Therefore, it has become imperative for government institutions to proactively protect electronic systems and networks from attacks and electronic threats, to monitor networks, servers, and applications for potential security threats, and to respond to them promptly to ensure the integrity of sensitive data, operations, and information.

The problem of the study is summarized in the lack of sufficient knowledge of the role of information systems control exercised by the Central Agency for Financial Control in reducing cybersecurity risks in the government sector.

Based on the above, the research problem can be posed with the following question:

Does the information systems control exercised by the Central Agency for Financial Control play a role in reducing cybersecurity risks in the government sector?

The following two questions branch out from it:

1. Is there a role for internal control and the internal control system in the information systems environment in limiting and reviewing the structure of internal control, and its evaluation by the Central Agency for Financial Control in reducing cybersecurity risks in the government sector?
2. Is there a role for the oversight exercised by the Central Agency for Financial Control over information systems in reducing cybersecurity risks in the government sector?

2. **Research Objectives:**

The main objective is to determine the role of the oversight exercised by the Central Agency for Financial Control over information systems in reducing cybersecurity risks in the government sector. This objective can be divided into the following sub-objectives:

1. Clarifying the role of oversight exercised by the Central Agency for Financial Control over information systems in reducing internal control system and cybersecurity risks through the control mechanisms it uses, in addition to its assessment of internal control within the information systems environment in the government sector.
2. Studying the concept of cybersecurity and identifying its risks.

3. Identifying weaknesses in current control operations in light of the results from field reality, which may help in raising the level of performance, and may also provide an incentive to offer more specialized training programs.
4. Identifying training needs and submitting proposals for training programs that help employees of the Central Agency for Financial Control acquire the skills and knowledge necessary to monitor information systems effectively.
5. Providing recommendations to improve information systems control practices in a way that contributes to enhancing cybersecurity in the government sector.
6. Fulfilling the researcher's desire to delve deeper into the topic of information systems control and cybersecurity and to identify the different types of cyber threats and risks facing information systems, with the aim of enriching the researcher's academic and professional knowledge.

3. The Importance of the Research:

This research is of particular importance, given the increase in cyber threats targeting the government sector in light of rapid technological development and the emergence of so-called electronic wars and cyberattacks. These threats may lead to serious legal and financial risks for institutions that rely on information systems in their work. With the increasing reliance of the government sector on digital technology, enhancing cybersecurity becomes an urgent necessity to protect data and ensure business continuity. Therefore, the increasing risks impose the need for the Central Agency for Financial Control to develop strategies that align its performance with the modern environment. This research aims to emphasize the importance of controlling information systems to reduce cybersecurity risks by defining the components that auditors must assess to monitor and protect systems from threats and breaches.

4. **Research Hypotheses:** The research hypotheses aim to answer the questions raised in the study problem, as follows:

First Hypothesis:

There are no statistically significant differences for demographic variables (gender, age, job title, academic qualification, years of job experience) regarding questions related to the role of information systems oversight in reducing cybersecurity risks in the government sector.

Second Hypothesis:

There is no statistically significant role for information systems oversight in reducing cybersecurity risks in the government sector.

The following two sub-hypotheses branch out from it:

1. There is no statistically significant role for internal control and the internal control system in reviewing and assessing the structure and organization of information systems to reduce cybersecurity risks in the government sector, based on a review of the structure of international control and its evaluation by the Central Agency for Financial Control
2. There is no statistically significant role for the control exercised by the Central Agency for Financial Control over information systems in reducing cybersecurity risks in the government sector.

5. Research limits:

Spatial boundaries: The Central Agency for Financial Control, Aleppo Branch.

Temporal boundaries: The period of time it took to complete the research, from 02/01/2024 to 06/30/2024.

6. Research methodology:

Regarding the theoretical aspect:

The researcher relied on the descriptive analytical approach by reviewing references and research from electronic websites to achieve the study's objectives, as well as previous related periodicals and studies.

Regarding the practical aspect:

The researcher relied on the statistical questionnaire as a tool to prove or deny the research hypotheses. The questionnaire was applied in the field at the branch of the Central Agency for Financial Control in Aleppo Governorate, where the opinions of the research sample members were surveyed using a questionnaire designed based on the relevant theoretical aspect and previous studies for the purpose of collecting primary data that serves the research, in order to know the role of control over information systems in reducing cybersecurity risks in the government sector.

Data were collected, analyzed, and hypotheses tested using statistical methods and software (SPSS 18).

7. Research community and sample:

The research community consists of the inspectors of the Central Agency for Financial Control in Syria, numbering about 950 inspectors. A sample was drawn from the inspectors of the Central Agency for Financial Control in Aleppo Governorate, numbering 105, and the visa inspectors were excluded, as they do not perform auditing work related to information systems.

A total of 77 questionnaires were distributed to the research sample, and 69 forms were recovered, of which 65 were valid and statistically analyzed.

8. Research difficulties:

One of the most important difficulties the researcher faced during the preparation of the research was the lack of references discussing the topic of oversight carried out by the supreme financial oversight bodies over information systems and cybersecurity. Given the novelty of the subject, reliance was placed, to some extent, on websites.

9. Previous studies:

1. Reem Aqab Al-Khasawneh's study from 2009 entitled "A Framework for Evaluating the Audit Bureau's Control in the Hashemite Kingdom of Jordan in Light of the Application of E-Government: [10]

The study aimed to highlight the impact of e-government on government oversight, clarify the new challenges facing government oversight, draw the attention of the auditor in the Audit Bureau to the challenges that require the auditor to have sufficient knowledge of e-government technologies and the problems related to the environment of that technology, and identify the latest procedures and methods in the field of government oversight of e-government operations.

The study reached a set of results, including:

- The legal and professional publications of the Audit Bureau do not meet the requirements of government auditing in light of the application of e-government.
- The Audit Bureau does not have auditing methods compatible with the government auditing environment in light of the application of e-government.d
- The employees of the Audit Bureau do not possess the technical and cognitive skills required for government auditing in the context of e-government application.

2. Reem Aqab Al-Khasawneh's 2010 Study titled "Evaluation of Government Control Procedures in Light of the Application of E-Government in the Hashemite Kingdom of Jordan":

The study aimed to identify the procedures of the Audit Bureau in the Hashemite Kingdom of Jordan in light of the application of e-government. The research addressed a set of procedures and proposed steps for government oversight. The research concluded that the Audit Bureau does not have appropriate oversight procedures for the government oversight process, and that there are deficiencies in the standards of government auditing in the Hashemite Kingdom of Jordan. Furthermore, there are no procedures for implementing the government oversight

[10] **Al-Khasawneh, Maryam Aqab** (2009). "A Framework for Evaluating the Audit Bureau's Control in the Hashemite Kingdom of Jordan in Light of the Application of E-Government," *PhD Thesis*, Arab Open University for Graduate Studies, Jordan.

process in the field of government systems. The study recommended the need to develop appropriate audit procedures in light of e-government.[11]

3. **Salim Muslim Al-Hakim's 2010 Study titled "The Possibility of Controlling Automated Accounting Information Systems of Public Institutions of an Economic Nature by Inspectors of the Central Agency for Financial Control in Syria":**

The study aimed to identify the possibility of evaluating the automated internal control structure by the inspectors of the agency when auditing economic institutions that use automated accounting information systems, according to the standards of control over information systems in a manner consistent with the ongoing developments. The research recommended including laws for controlling public institutions that require auditors to conduct control over accounting information systems to align with the advancements in public institutions in Syria in the field of information technology. Additionally, the study recommended raising awareness among the inspectors of the agency about the necessity of conducting control over information systems and using the latest control methods to achieve this.[12]

4. **Amana Muhammad Mansour's 2021 Study titled "The Impact of Cybersecurity on Internal Control and its Reflection on Economic Unity":**

This is an exploratory study that surveys the opinions of a sample of auditors and accountants from the Ministry of Higher Education and Scientific Research. The study aimed to identify the importance of cybersecurity through its impact on internal control and the value of the economic unit by adopting the Information Technology Governance Framework (COBIT).

The most important conclusions reached by the research indicate general acceptance and agreement on the existence of a relationship between the dimensions and requirements of cybersecurity, modern frameworks of internal

[11] **Al-Khasawneh, Reem Aqab** (2010). "Evaluation of Government Control Procedures in Light of the Application of E-Government in the Hashemite Kingdom of Jordan," *An-Najah University Journal of Research*, Volume 24, Issue 9.

[12] **Al-Hakim, Salim Muslim** (2010). "The Possibility of Controlling the Automated Accounting Information Systems of Public Institutions of an Economic Nature by Inspectors of the Central Agency for Financial Control in Syria," *Damascus University Journal of Economic and Legal Sciences*, Volume 26, Issue 1.

control, and the value of the economic unit. The researcher recommended that the economic unit adopt effective means for the continuous evaluation of internal control to maintain information security by relying on modern frameworks of internal control. This approach would help prevent methods of hacking electronic systems and attempts to manipulate their information.[13]

5. **Hanan Haroun Farid's Study (2022) titled "The Proposed Role of the Auditor in Instilling Confidence in the Cybersecurity Risk Management Report and Its Impact on the Significance of Financial Statements":**

The study aimed to demonstrate the auditor's role in instilling confidence in the cybersecurity risk management report and its impact on the significance of financial statements, enabling the auditor to keep pace with the rapid changes in the business environment. The study concluded that there is a significant impact of the importance of disclosing the cybersecurity risk management report and a significant effect of the proposed role of the auditor on the financial statements.[14]

6. **Hiba Gamal Ali's Study (2023) titled "A Proposed Procedural Approach to Measuring the Extent of Response by the External Auditor to Cyber Risks in the Client Facility":**

The study aimed to develop a proposed procedural approach to measure the external auditor's response to cyber risks in the client's facility in the Egyptian environment. The study concluded that the assessment of cybersecurity risks depends on audit processes that analyze and evaluate a set of predetermined controls across various topics related to cybersecurity. It demonstrated a significant positive effect of cybersecurity attack risks in the client's facility on the work of the external auditor and a significant positive correlation between the management of cybersecurity risk disclosures and the proposed procedural approach for the external auditor's work. The study reached several results and recommendations, the most

[13] **Mansour, Amina Muhammad** (2021). "The Impact of Cybersecurity on Internal Control and Its Reflection on the Economic Unit: A Survey Study," *Journal of Management and Economics*, Issue 127, March.

[14] **Farid, Hanan Haroun** (2022). "The Proposed Role of the Auditor in Instilling Confidence in the Cybersecurity Risk Management Report and Its Impact on the Significance of Financial Statements," *Future Institute for Specialized Technological Studies*, Volume 13, Issue 4.

important of which is to include cybersecurity risks as part of the auditor's assessment of an organization's IT risks in the facility.[15]

7. **Jahan Adel Amirhom's 2012 Study: "The Impact of Internal Audit Quality on Reducing Cybersecurity Risks and Its Implications for Rationalizing Investor Decisions":**

The study aimed to identify and analyze the most effective internal audit practices in reducing cybersecurity risks and their impact on rationalizing investors' decisions. The study concluded that stakeholders can only monitor cybersecurity operations with the assistance of internal audits. The study recommended that internal auditors should enhance their qualifications and that the internal audit department must submit independent reports to the Board of Directors and the Audit Committee, focusing specifically on cybersecurity risks.[16]

<u>What Distinguishes the Current Research from Previous Studies:</u>

Although there are many studies that have addressed the control of information systems and cybersecurity from the perspective of the external auditor, studies focusing on the control of information systems and cybersecurity by supreme financial audit institutions remain very limited (to the best of the researcher's knowledge). This research gap highlights an area of deficiency in current literature, which this study aims to address. While existing studies primarily focus on the mechanisms and methods of external audits, there is a significant need for a deeper understanding of the role of supreme financial audit institutions in overseeing and protecting information systems from cyber threats in the entities under their supervision.

[15] **Ali, Heba Gamal Hashem** (2023). "A Proposed Procedural Approach to Measure the Extent of the External Auditor's Response to Cyber Risks in the Client's Facility," *Scientific Journal of Financial and Commercial Studies and Research*, Faculty of Commerce, Damietta University, Vol. 4, No. 2.

[16] **Amirhom, Jihan Adel** (2022). "The Impact of Internal Audit Quality in Reducing Cybersecurity Risks and Its Repercussions on Rationalizing Investors' Decisions," *Journal of Financial and Business Research*, Volume 23, Issue 3.

10. Research Outline:

The research consists of the methodological structure and three chapters as follows:

Chapter One: Information Systems Monitoring

- Topic One: supervision
- Topic Two: Definition of Information Systems and Their Components

Chapter Two: Cybersecurity

- Topic One: The Concept of Information Security
- Topic Two: The Nature of Cybersecurity

Chapter Three: The Field Study

This chapter includes the design of the field study, conclusions, and recommendations.

11. Search Terms:

1. **Information System:** An information system is a set of resources and components that are interconnected with each other to store, process, and deliver information in a regular manner. It produces useful information that helps users perform the functions assigned to them, providing the necessary information at the appropriate time and in the appropriate manner.

2. **Cybersecurity:** Cybersecurity refers to the prevention of damage to computers, electronic communication systems, electronic communication services, and wired communications. It involves their protection and restoration, including the information contained within them, to ensure its availability, integrity, authentication, and confidentiality.

Chapter One: Information Systems Control

Section One: Control

- **Financial Control:**

The development and diversification of businesses, along with the increasing complexity of administrative functions, have created an urgent need for financial control. This necessity has grown particularly with the evolution of government operations, the increase in government responsibilities, and the complexities of organizational structures. Additionally, the significant progress required for executing financial tasks has called for the development of effective control procedures and systems to ensure the smooth operation of businesses.[17]

Financial control plays a critical role in preserving public funds and monitoring the individuals responsible for implementing laws and regulations, ensuring compliance with professional financial instructions and rules currently in effect.[18]

Financial control serves as a guiding compass for financial performance within government agencies. It acts as a vital tool for achieving oversight of the public sector through various procedures, which aim to maximize the use of state financial resources and safeguard them. This is achieved through effective control mechanisms, adherence to governance standards, and the proper utilization of government budgets to achieve desired outcomes.

In essence, financial control involves the processes of supervision, inspection, and review conducted by an authority with the legal right to oversee activities within the entity under its supervision.

The purpose is to ensure the appropriate use of public funds for their designated purposes, compliance with relevant laws, regulations, and instructions, and the detection of violations. It also includes identifying means to address these violations to prevent their recurrence in the future. Ultimately, financial control ensures the health, safety, and professional integrity of collection and spending operations.

[17] **Al-Sayed, Alaa** (2005). A Proposed Framework for Developing the Performance of Financial Control at the Islamic University, Gaza, Palestine, p. 19.

[18] **Al-Mutairi, Youssef Muhammad** (2020). The Impact of Financial Control of the Kuwaiti Audit Bureau on Activating Governance Standards in Entities.

- **Central Agency for Financial Control:**

The Central Agency for Financial Control is an independent oversight body affiliated with the Prime Minister. Its primary objective is to provide effective supervision of state funds and monitor the financial performance of executive, administrative, and economic entities, ensuring they fulfill their financial responsibilities.

The Central apparatus holds responsibility for auditing and inspecting accounts. It exercises legality control, accounting control, and adequacy control, complemented by investigative and inspection tasks.

The Central apparatus for Financial Control fulfills its mandate over various authorities, ministries, departments, and organizations, including the General Authority for Administrative Affairs and its affiliated entities, as well as entities with an economic nature. Its operations encompass auditing and reviewing in compliance with the provisions outlined in Decree No. 64 of 2003. Furthermore, the agency conducts inspections either autonomously, at the request of public institutions, or based on explicit information provided by informants.[19]

- **Internal Control:**

The internal control function, underpinned by an electronic operating system, plays a pivotal role across nations committed to implementing robust oversight mechanisms as a cornerstone of governance and accountability. By ensuring the credibility of the data used in supervisory processes, internal control mechanisms significantly contribute to achieving strategic objectives.[20]

Organizations endeavor to establish internal control systems to safeguard their assets, ensure operational integrity, and maintain adherence to managerial policies and directives. These systems are particularly crucial in addressing the evolving demands of information technology and advancing professional practices.[21]

[19] ***Decree No. 64 of 2003***, Central Financial Control Agency Law

[20] **Lotfy, Amin Al-Sayed Ahmed** (2007). *Modern Developments in Auditing*, University House, Cairo, Egypt, p. 3.

[21] **Al-Zayoud, Ayman Hassan Ali** (2022). "The Effectiveness of Internal Control and Its Application in Light of the Electronic Operating System from the Point of View of Employees at Sahab Municipality," *Arab Journal of Scientific Publishing*, Issue 42, p. 726.

An internal control system supported by an electronic operating framework shields institution from potential risks and serves as a vital resource for delivering accurate, timely information to facilitate managerial decision-making. Consequently, the ongoing enhancement of internal control processes is imperative, as these mechanisms form the backbone of organizational information systems and management strategies.[22]

Internal control is defined as all procedures and mechanisms employed within public administrative bodies to ensure the accuracy and validity of accounting data and reports, as well as adherence to policies aimed at safeguarding the public interest. This encompasses respecting laws, achieving predefined objectives, and ensuring that financial appropriations allocated in the budget are spent for their intended purposes. Furthermore, sound management of public funds necessitates the imposition of internal control on the administration.

This type of control extends across all stages of implementing expenditure and revenue operations. The American Institute of Certified Public Accountants (AICPA) defines the internal control system as: the organizational framework, coordination methods, and standards implemented within an entity to protect its assets, monitor and review accounting data, ensure its accuracy and reliability, enhance operational efficiency, and promote adherence to established administrative policies. [23]

Internal control represents one of the most essential tools for performance oversight in the public sector. It is a critical mechanism employed by supreme oversight bodies to evaluate and ensure disciplined performance, thereby fostering financial and administrative reforms within modern government units. Studies have highlighted that auditors must determine the extent of their testing based on the internal control system, especially considering the transition from detailed audits to more streamlined approaches.[24]

Auditors are also required to assess the internal control system and the administrative review mechanisms, utilizing the evaluation results to design audit plans, develop programs, and select methodologies. Furthermore, auditors evaluate

[22] **Damarey, Stephanie** (2007). *Execution and Control of Finances*, Gualino Editor, p. 115.

[23] **Mohamed Amin, Walid Ibrahim** (2018). "An Analytical Study of the Role of the Supreme Audit Bodies in Developing Internal Control Systems to Reduce Financial Corruption in Government Units, Libya," *Scientific Journal of Commercial and Environmental Studies*, Suez Canal University, Volume 9, Issue 2, p. 8.

[24] **Al-Jabri, Mohamed** (2014). "Evaluating the Role of the Internal Auditor in Improving the Internal Control System of Accounting Information Systems in Insurance Companies in Yemen," *Master's Thesis*, Sana'a University, Yemen, p. 29.

the accounting framework, verify the integrity of the information derived from it, and review the reports of the Board of Directors, regulations, and related documentation. Internal control plays a pivotal role in producing financial statements with a high degree of transparency, disclosure, and credibility.[25]

[25] **Abdul Hassani, Waad Hadi** (2016). "External Opinion Polls and Their Impact on Internal Performance Evaluation," *ResearchGate*, https://www.researchgate.net, p. 3.

Section Two: Definition of information systems and their components

Information systems play a significant role in our lives overall and in most types of systems specifically. They are utilized in various institutions, including banks, stock markets, the General Electricity Company, the General Water Company, the General Telecommunications Company, and higher education.

The growing reliance on information systems is largely due to the distribution of workplaces and branches across distant geographical locations and the need to coordinate their operations. This has created a demand for systems that can manage information and facilitate its exchange with ease, accuracy, and cost-efficiency.[26]

These systems form the backbone of an institution, delivering essential information. With advancements in technology across all domains, information systems are now primarily built on technological principles, integrating processes from input to processing, and ultimately generating outputs and feedback.[27]

Computers, software, and data represent the foundational elements of an information system within the digital environment of an organization. Computers may be connected via communication devices and services in networks involving terminals, other accounts, or specific communication tools. These networks can take various forms, such as local area networks (LANs), private networks serving the administrative interests of an organization (e.g., intranets), wide area networks (WANs), extranets, or even global networks like the Internet. External communication links can also enable individuals with suitable technological means to access these systems.

Many information networks combine internal and external elements. Communication networks may include data systems as well as telephone and fax modems. Additional devices, such as printers, can be connected to computers and communication equipment. Software includes operating systems and application programs specifically designed for particular clients or government organizations. These may be installed directly onto computers or stored on external media such as CD-ROMs

[26] **Addas, Dahya Saket Ghassan** (2020): I italicized the book title for consistency with citation formatting. I also used "pp. 19-20" for a range of pages, which is the standard way to refer to multiple pages.

[27] **Maqrani, Qaddour** (2016): I added quotation marks around the thesis title and italicized "Master's Thesis" to clarify the document type. Additionally, I formatted the name of the university and the faculty for clarity and consistency.p.10

or other digital storage devices. Paper-based, documentary, portable, and electronically readable evidence supports the operation of these systems.

Both hardware and software, along with their maintenance and usage, form the foundation of information systems and applications in the digital environment. These systems aim to store, process, retrieve, and transfer data and information to targeted users. Together, these diverse and interrelated components create the information system in the digital environment.[28]

1. Definition of Information Systems

Definitions of information systems vary in their wording but align in their core meaning.

Among the most notable are:

- **An information system** is a set of resources and components that are interconnected in a structured way to produce valuable information. It facilitates the processing, storage, and delivery of information to users at the appropriate time and in an appropriate manner, supporting them in performing their designated functions.[29]

- **Information systems** are a collection of elements (individuals, equipment, procedures, and data) that are interconnected and interact cohesively through a set of systematic processes (e.g., collection, storage, processing, and analysis). They display outputs in various formats, such as reports, forms, charts, and graphs, delivering these results to the system's beneficiaries in ways that support decision-making, streamline operations, and enable effective planning and monitoring of organizational activities.[30]

[28] **Abirat, Muqaddam Houari, Miraj** (2022). "Security Risk Management and Information Transparency of Information Systems in the Digital Environment," *University of Laghouat, Algeria*, p. 1.

[29] **Qasim Abdul Razzaq Muhammad** (2008). *Computerized Accounting Information Systems*, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, p. 19.

[30] **Al-Ubaidi, Fatima Naji** (2012). "The Risks of Using Computerized Accounting Information Systems and Their Impact on the Effectiveness of the Auditing Process in Jordan," *Published Thesis for Master's Degree in Accounting*, p. 16.

- The researcher believes that information systems focus on studying, designing, developing, and managing computer systems to support the collection, storage, and retrieval of information. These systems aim to enhance institutional performance by simplifying administrative processes and providing accurate, timely information for improved decision-making, efficiency, and effectiveness.

Second: Elements of Information Systems

The system consists of three main parts:

A - Inputs: Inputs are everything that comes from outside the system and enters it. The system's inputs are different resources determined based on the objectives that the system seeks to achieve from these resources (human resources, machines, raw materials, capital, administrative information, etc.).

B - Processing: It is the mechanism for dealing with inputs and converting them into outputs, where specific operations are carried out on the system's resources (inputs). These are the various transformation operations that lead to converting these inputs into the objectives to be achieved by the system, or what are called outputs.

C - Outputs: These are the results of the processing process that exit the system. They represent everything that results from this system in the form of tangible or intangible goods or information.

- Inputs and outputs can be easily defined and explained, but the processing mechanism varies from system to system.
- The inputs of one system can be the outputs of another system, and vice versa.

In order for the system to work properly and effectively, a fourth element must be added to the system's components, which is monitoring the system's performance in all its stages—feedback.

Monitoring (feedback) represents the corrective actions and directives accompanying the stages of the system's work. These actions are taken into consideration when developing plans, considering the nature of changing conditions and their impact on the plans, operations, and objectives of the system. They are preventive and remedial processes.[31]

[31] Maqrani, 2016, previously cited reference, p. 6.

Therefore, in all information systems, information is managed starting with the users of the information. It is then converted into inputs, processed, and converted into outputs. All of this happens under control mechanisms across all stages.

It can be said that the work of the information system is to maintain a permanent ability to interact with data, provide information at the required time, ensure safe access to it through reliable channels, deliver services to information sites, and ensure that the user is not exposed to any restrictions preventing access.

Third: Components of Information Systems

1. Devices and Equipment: This includes all physical devices and materials used in operating the information system.

It encompasses:

- Computer Systems: Representing the central operating unit and secondary storage media.
- Complementary Devices: Such as mice, keyboards, monitors, and printers.
- Media: Tangible objects on which data is recorded, including paper, optical discs, and magnetic discs.

2. Software: Includes all kinds of instructions for operating and processing data.

3. Human Element: Divided into:
   - End Users: Individuals who directly use the system or its outputs processed by third parties.
   - Automation Specialists: Individuals responsible for operating and developing the system.
4. Database.
5. Networks.

Fourth: The Importance of Information Systems[32]

1. Performing Large-Scale and Fast Digital Calculations: Enables the storage of vast amounts of information and data in a compact and easily accessible location.
2. Improving Decision-Making: Provides communication channels that help enhance scrutiny and securely exchange information.
3. Reducing the Occurrence of Crises: Achieved through future-oriented information technology.
4. Speed in Printing and Editing: Facilitates the rapid processing of information and data.
5. Increasing the Added Value: The value of information is measured by the extent to which the resulting benefit outweighs the cost of preparation. It also reduces the time required to obtain information.[33]

The use of information technology improves the quality of work through ease of communication, high accuracy, cost reduction, time and effort savings, risk mitigation, and support for the development of new products or services. This is achieved alongside the presence of a security system capable of protecting this information. Additionally, it contributes to strengthening the competitive position of institutions and organizations.

Technology enables organizations to reconsider their management and operational approaches to achieve integrated management. Simultaneously, it reduces human errors and risks while eliminating spatial and temporal barriers. It plays a significant role in advancing essential areas that are indispensable in the lives of individuals, institutions, and nations.[34]

[32] **Al-Marri, Rashid Muhammad** (2022). "The Impact of Information Technology on the Security System and Internal Control," *Journal of Jurisprudential and Legal Research*, January, pp. 1319–1320.
[33] **Al-Sudairy, Muhammad bin Ahmed bin Turki** (2012). *Administrative Information Systems*, King Saud University, p. 23.
[34] Nour El Houda Chabou 2021, The Role of Modern Communication Technology in Improving Public Service, Master's Thesis, Algeria,

University of Arab Ben Mahdi Oum El Bouaghi, p. 31

Chapter Two: Cybersecurity

When examining the concept of cybersecurity, it is essential to first understand the concept of information security and distinguish between the two, as a comprehensive understanding of information security provides the foundation for protecting information and technical systems from various threats.

The primary distinction between cybersecurity and information security lies in the type of data and information each seeks to protect. Cybersecurity focuses exclusively on ensuring the security of electronic information, whereas information security encompasses the protection of information in all its forms—whether paper-based, electronic, or otherwise.

Thus, information security represents a broader and more comprehensive field, addressing the protection of all types of data, including those covered by cybersecurity.[35]

[35] https://horizons-edu.com

Section One: The Concept of Information Security

Information is a major resource for an organization and a key source of its success, due to its role in increasing the efficiency and effectiveness of various administrative activities within the organization. Accurate information that is readily available and flows quickly to the organization's management will help it perform many tasks and functions, including planning, organizing, directing, decision-making, and monitoring. It also facilitates the optimal exploitation of resources and controls their use.

Therefore, while it is essential for any organization to have access to information, this alone is not sufficient to solve the challenges it faces. The information must be organized within a system that facilitates its timely retrieval.[36]

Information systems have been developed to manage the vast amount of data: storing, processing, and distributing it in a way that ensures the availability of accurate and relevant data for the institution at all administrative levels and within the various subsystems. This enables the institution to improve its performance and enhance its decision-making efficiency.

Information is an essential element of any organization's operations, and therefore, it must be continuously protected, with its associated risks effectively managed according to modern standards and principles.

Information Security is concerned with safeguarding information from threats and attacks to ensure business continuity, minimize losses, and increase the chances of success and profitability.[37]

[36] **Hussein, Skfali, Marwa, Maqlatni** (2020). "Management Information Systems and Their Impact on Employees' Job Performance: Case Study of the Agricultural and Rural Development Bank, Qalma Agency," *Master's Thesis in Facilitation Sciences, Business Administration*, University of May 8, Qalma, p. 2.

[37] **International Organization for Standardization and International Electrotechnical Commission** (2010). *National Information Center Technical Department Quality and Development Division Standards Unit, Operating Systems Standards Committee, Confidentiality and Assurance Standard Code of Practice for Information Security Management*, ISO 27002, p. 6.

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) define information security from several perspectives:

- Academically, it is the field that studies the theories and strategies for protecting information from threats and attacks.
- Technically, it involves the means, tools, and procedures required to safeguard information from both internal and external dangers.

- Legally**,** it is the study of methods and measures to protect the confidentiality, integrity, and availability of information, as well as combat activities that attack it or exploit its systems to commit a crime.

Basic Principles of Information Security:[38]

Organizations seek to achieve information systems security by achieving the following trinity:

1. **Confidentiality**: This ensures that information is not disclosed or accessed except by authorized persons, whether it is stored on a physical medium or transmitted through communication means.
2. **Availability**: This ensures the continuous operation of the information system with all its components and the ongoing ability to interact with it. It also ensures the provision of services and information to its users upon request without any delay and without the users being prevented from using or accessing it.
3. **Integrity of the content**: This ensures that the information content is complete and correct and has not been modified, destroyed, or tampered with at any stage of processing or exchange, whether illegally, intentionally, or accidentally.

[38] **Janulevicius, Justinas** (2016). *Op. Cit.*, p. 12., **Van der Meer, Jeroen** (2012). "Multi-Criteria Decision Model Inference and Application in Information Security Risk Classification," *Master's Thesis in Computational Economics*, Erasmus School of Economics, Erasmus University Rotterdam, p. 12.

Other principles have also been added, such as:

- **Non-repudiation**: This means that the person who performed an action related to the information or its locations (such as sending, modifying, or receiving) cannot deny their responsibility or the fact that they took that action.
- **Authentication or identity verification**: This involves verifying the identity of the person attempting to use the information and determining whether or not they are the authorized user permitted to handle that information.

Information Security Components:[39]

With the increasing reliance on the electronic environment in storing, processing, and transferring information, Internet security, the security of electronic devices, networks, and communications through which information is stored, processed, and transferred electronically, has become a major component of information security. In addition to this, the following are key components of information security:

- Physical Security: The protection of resources, property, and buildings, and the prevention of unauthorized access to them.
- Individual Security: The protection of individuals who have access to information.
- Operational Security: The protection of system operations performed by authorized personnel.
- Business Continuity Plans: These are intended to develop plans to overcome the effects of security incidents and resume normal work after an incident.
- Data Security: Ensuring the confidentiality, integrity, and availability of data.

[39] **National Institute of Standards and Technology** (2016). *Internal Report 7621, Revision 1*, p. 2., **Idem** (2016). *Internal Report 7621, Revision 1*, p. 3.

Information Systems Security Threats:[40]

There are many challenges that affect the proper performance of information systems functions, including:

1. **Rapid Technological Developments:** The increasing technical problems, changing environmental events, human weaknesses, and the unsuitability of current social, political, and economic institutions to successive changes complicate the task of tracking the threats and risks facing information systems, whether arising from intentional or unintentional actions and behaviors, which can come from both internal and external sources.
2. **Technical Factors Leading to System Failures:** The technical factors that contribute to the failure of information systems are numerous and varied, and sometimes they may be difficult to comprehend.
3. **System Errors:** Errors resulting from the misuse of hardware and software, latent errors, as well as overload or operational problems.

4. **Viruses:** Viruses often enter the system through infected software, worms, or logic bombs, which are some of the technical means used to disable the system, distort it, damage, or corrupt its data and various functions.
5. **Serious environmental events** include fires, earthquakes, floods, electrical storms, and extreme heat waves. As for adverse natural equipment conditions, they may result from breaches of natural security measures, such as power outages, misuse of air conditioning devices, water leakage, or direct neglect in designated areas. The great diversity of information system users, including differences in awareness, training, and varying interests, may lead to difficulties related to information security and its systems.

In addition to users choosing simple passwords for information systems that are easy to remember and verify, users may also share identification codes and passwords,

[40] **Abirat** (2022). *Op. Cit.,* p. 12.

leaving control and access ports open on security sites, which exposes them to hacking.

Errors and breaches may occur in the collection, processing, storage, transmission, and deletion of data and information. Failure to create alternative and backup copies of critical files and software compounds the negative effects of errors and breaches. This may expose the organization to expenses and losses related to the time, effort, and money spent in re-creating them. Intentional misuse of the system, unauthorized access, deliberate sabotage, destruction, fraud, or theft are serious risks and threats that affect the life of the system and the organization that owns it. A significant portion of the threats facing information systems comes from external sources. Conversely, individuals who have been granted authorized access to the system may also pose significant threats.

Therefore, it is necessary[41] to conduct a systematic assessment of the information system's security to develop and implement effective security practices, by examining the security of the information systems to determine the effectiveness of the security measures taken, and working to adopt appropriate protection solutions and reduce the risks that may affect the system. On the safety of information systems, it is therefore necessary for public administrations and institutions to update their information systems by conducting information systems security audits.

[41] https://www.dgssi.gov.ma

Section Two: The Nature of Cybersecurity

The study of cybersecurity has become one of the innovations of the technological and digital development that we have been experiencing in the world recently. The developed world in all its parts is witnessing a great development that we cannot ignore in any way. However, there is another dark side to this digital development, which can make major countries, companies, and commercial and economic institutions vulnerable to hacking. Perhaps this is one of the reasons for the importance of studying cybersecurity, which works to protect data, networks, and electronic systems from attacks and hacking that could destroy them and their stability.[42]

Cybersecurity has become an increasing focus for organizations, and the COVID-19 pandemic has highlighted cyber risks for every type of organization with remote work, the expansion of enterprise systems into work environments using video conferencing software, and the addition of personal devices and Wi-Fi networks.

In a study conducted by the Government Accountability Office (GAO) entitled *Urgent Action is Needed to Address the Cybersecurity Challenges Facing the Nation*, four major cybersecurity challenges were addressed through ten proposed actions to solve the problems. The challenges include: developing a cybersecurity strategy, strengthening federal systems, protecting critical infrastructure, protecting sensitive data, and ensuring data privacy.[43]

Some developing countries have also sought to take similar measures to ensure cybersecurity. These countries have faced some problems, including the lack of a comprehensive cybersecurity initiative, insufficient support, and the absence of educational initiatives capable of keeping pace with developments in the field of communications and information technology. This has been reflected in the decline in the level of cybersecurity, and Internet users in these countries have become more vulnerable to cyberattacks and crimes.[44]

[42] Al-Samhan, 2020, previously cited reference, p. 4

[43] https://governmenttechnologyinsider.com by Jackie Davis August 16.2018

[44] Kortjan & Solms, 2013, p.291

In 2013, the US retail giant Target suffered a data breach, in which credit and debit card details and personal data of 70 million customers were stolen from the company's databases, with total damages estimated at more than $18 billion.[45]

In 2022, cybersecurity topped the list of critical risks in the European Union Internal Audit Institutes [46](ECIIA) report, and the Positive Technologies Cyber Threat Landscape report indicated that government entities in the Middle East are prime targets for cybercriminals, with 22% of all cyberattacks targeting government departments. Experts estimate that 78% of cyberattacks on businesses in the Middle East target computers, servers, and network equipment. Cybercriminals hack systems by deploying malware, exploiting vulnerabilities to steal confidential information, or disable devices. Attacks in the Middle East are most notorious for using spaces that delete files on compromised devices.[47] Following the cyberattack on Leicester City Council, where documents were revealed, including rental data due to a ransomware attack by the INC Ransom Group, it has become clear that government agencies are prime targets for cybercriminals, in addition to similar attacks on NHS Dumfries and Galloway, indicating a worrying trend that requires immediate attention.[48]

Hence, the need to understand what cybersecurity is and identify its risks.

The word "cyber" is derived from the Latin word *cyber*, meaning imaginary or virtual. Cyber is a term used to describe the space that includes computer networks, communication and information systems, and remote-control systems. It means everything related to or connected to computers, information technology, and virtual reality, from which the terms *cyber* and *cybernetics* were derived.

Cybernetics is often defined as the study of communication and control in living organisms and machines.[49]

The word "cyber" refers to electronic systems and everything related to electronic computer networks, Internet networks, and other applications, such as Facebook,

---

[45] **Kosen, Didibe and Ho Ngzi Lu, Abraham** (2021). "Cyber Risks in the Public Sector," *IMD*, May 2021, www.imd.org, p. 45.

[46] **ISACA** (2022). "ISACA Journal, Volume 3," www.isaca.org/resources/isaca-journal/issues/2022/volume-3/.

[47] **Ad-Dawra**. www.ad-dawra.com.

[48] **Mah6at.net**. "Cyber Risks in the Public Sector," May 2024, Vivek Dodd, www.mah6at.net.

[49] **Al-Azzizi, Hani Muhammad Khalil Ibrahim** (2023). "The International Legal System for Combating Cyber Risks," *Contemporary Egypt*, Issue 549, p. 469.

WhatsApp, and other applications, as well as services through which money is transferred on the Internet, online services, and many other services in all life applications around the world.[50]

Al-Samhan defines cybersecurity as taking the necessary measures to protect cyberspace from cyberattacks through a set of means used technically, organizationally, and administratively to prevent unauthorized access to electronic information and prevent its illegal exploitation. Thus, it aims to maintain the continuity of systems and the information available in them, and protect them with all privacy and confidentiality by following the necessary measures and procedures to protect data.[51]

The National Institute of Standards and Technology defines cybersecurity as the prevention, protection, and restoration of computers, electronic communication systems, and electronic and wired communication services, including the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.[52]

It is also known as information technology security or computer security, i.e. protecting information, equipment, devices, computers, computer resources, communication devices, and the information stored therein from unauthorized access, use, disruption, modification, or disclosure.[53]

It is defined as the process of protecting information by addressing threats to information that is processed, stored, and transmitted by information systems interconnected between networks.[54]

[50] https://www.mahbat.net

[51] **Al-Samhan** (2020). *Op. Cit.*, p. 9.

[52] **Coussin, Didier and Ho Ngzi Lu, Abraham** (2021). "Cyber Risks in the Public Sector," *IMD*, May 2021, www.imd.org.

[53] **SIS** (n.d.). www.sis.gov.eg.

[54] **Their Emir** (2022). *Op. Cit.*, p. 337.

In light of the above, cybersecurity is a set of strategies, technologies, and practices that aim to protect electronic systems, networks, computers, and information from cyberattacks. This includes protecting the confidentiality, integrity, and availability of information, preventing unauthorized access, detecting the illegal exploitation of information or digital resources, and ensuring business continuity by providing preventive measures and procedures necessary to address increasing cyber threats.

1. Concepts related to cybersecurity:

- **Cyberspace:** Cyberspace is defined as the virtual computer world, or the electronic means used to facilitate communication over the Internet. Cyberspace includes a large computer network consisting of several sub-computer networks spread throughout the world. [55]

  The International Telecommunication Union defined cyberspace as: the physical and non-physical field that consists of and results from elements such as computers, networks, software, information computing, electronic content, transmission data, and digital control. [56]
- **Cybercrime:** The use of a computer as a tool to achieve illegal goals, such as committing fraud, stealing identity or intellectual property, or violating privacy. [57]
- **Cyberattack**: A deliberate attempt by an individual or organization to hack into an individual's or organization's information system. The person carrying out such attacks often seeks to gain a benefit from attacking the other party and disrupting their network.

  Cyberattacks occur daily, some of which are discovered and some of which are still undetected. Attackers often target vulnerable electronic systems and demand a ransom in exchange for their return or non-disruption, which results in the loss of huge sums of money for the companies and individuals who are victims.[58]

[55] https://mawdoo3.com
[56] The International Telecommunication Union, ITU Toolkit for Cybercrime Legislation, Geneva, 2010,p12
[57] Michael Aaron Dennis, May, 2024, https://www.britannica.com
[58] https:mawdoo3.com 2021 Qusay Abu Shama, December 12

In a 2016 study by Rolf Weber, which aimed to identify legislative measures to protect information security in the Internet environment through the Internet of Things, the study concluded that the speed of change, technological development, and the development of attackers' methods require new approaches to protect information in the Internet environment. Every computer connected to the Internet is under threat from these crimes, with many vulnerabilities that facilitate these attacks. This necessitates urgently enhancing information security in the Internet environment, as well as having innovative flexibility to confront these attacks.

2. **Cybersecurity Patterns:** [59]
   - Network security: The practice of securing a computer network from intrusive and opportunistic elements, whether targeted attackers or malware.
   - Application security: Focuses on keeping software and hardware free from threats. A compromised application could provide access to data intended to be protected. Successful security implementation begins at the initial design stage before the software or hardware is deployed.
   - Information security: Protects the integrity and privacy of data, whether in storage or during transmission.
   - Operational security: Includes the processes and decisions that handle data assets and ensure their protection.

Risks that threaten cybersecurity:

The concept of cybersecurity risks refers to electronic threats and attacks that disrupt the technological systems of institutions and their electronic services. These risks not only harm the technologies and devices of institutions, but they also incur losses and damage their reputation.

According to the International Association of Insurance Supervisors (IAIS), cyber risks are defined as: any risks arising from the use and transmission of electronic data, including technology tools such as communication networks. It also includes physical damage and fraud committed through misuse of data, as well as any responsibility arising from the storage of data and the availability and integrity.[60]

[59] Al-Samhan, 2020, previously cited reference, p. 14

[60] IAIS. (2018), "Draft Application Paper on Supervision of Insurer Cybersecurity", in IAIS (Ed.). IAIS,

Cybersecurity risks can be divided into two main groups:[61]

A. Performance risks: These are associated with the application of modern information technology tools, reflecting the failure of these tools to perform their intended tasks and achieve the desired results.

B. Security risks, which include three basic types:

1. **Physical security breaches:** These involve the penetration of physical components of the infrastructure on which a company relies for its IT services. Examples include searching through the company's infrastructure waste, such as floppy disks or electronic network devices, that may contain information or passwords crucial for completing a breach. Additionally, "wave espionage" refers to using specialized devices to capture all wireless signals from the IT system, such as sound waves.

2. **Employee-related protection breaches:** These are linked to internal and external risks arising from employee behavior within the company. Examples include piracy of pre-existing software, violations of security permissions due to weak internal controls, and social engineering. Social engineering exploits employee relationships and positions to gain unauthorized access to information or embezzle it.
3. **Breaches of information and communication security**: This category includes attacks such as unauthorized copies of data and the use of secret data transmission channels. It also includes attacks on software, such as viruses, traps, and back doors.

[61] Shehata, Mr. Shehata, 2022, Towards an effective role for the internal auditor in managing cybersecurity risks in companies listed on the Egyptian Stock Exchange, Scientific Journal of Financial and Administrative Studies and Research, Volume Thirteen, Issue Two, p. 28

The study by Jehan Adel Ibrahim further divides cyber risks into three categories: cyber risks related to confidentiality, cyber risks related to integrity, and cyber risks related to performance continuity. These three types of cyber risks have direct and different impacts on organizational objectives. For instance, business disruptions prevent operations, leading to revenue loss. Fraud results in immediate financial losses, while investigation into breaches takes time. Data breaches not only take time to resolve but also cause reputational damage and legal costs.

In general, the risk of losing customer trust following cyberattacks is particularly high in the financial sector, where financial institutions rely heavily on customer trust, directly affecting their decisions.[62]

4. Types of Cybercrimes:[63]

1. **Electronic blackmail**

2. **Identity theft or impersonation:** This is a form of fraud that occurs when an individual uses another person's personal identification information, such as their name, passport number, ID card, credit card details, online account information, or photo, without consent. This stolen information is used to commit fraudulent activities, steal money or credit cards, or damage the victim’s reputation. For example, this can involve opening bank accounts, obtaining loans, or conducting illegal business by impersonating the victim or using their credit card for unauthorized purchases or cash withdrawals.

3. **Online phishing:** This type of fraud typically involves the theft of users' personal data, such as login details, passwords, phone numbers, and credit card information. Cybercriminals create a fake website resembling a legitimate one, then send a link to this fake site via email, pretending to be a trusted entity such as a company or bank. The victim is encouraged to click the link and input their sensitive information. This data can later be used for fraud or

[62] Their Emir, 2022, previously cited reference, p. 339

[63] https://isf.gov.ib Cyber Risk Awareness Guide

unauthorized account access. It may also lead to the installation of malicious programs on the victim's devices, which aids hackers in stealing information or sabotaging operations.

4. **Hacking Devices and Data:**

This category involves unauthorized access to or attempts to breach electronic data belonging to individuals, private companies, or government institutions. The purpose can be to steal, destroy, or manipulate data, often including sensitive information about citizens, customers, employees, or intellectual property.

5. **Ransomware and Data Encryption:**

Ransomware involves encrypting critical data or entire devices, preventing access until the victim pays a ransom, often in untraceable digital currencies such as Bitcoin. Hackers typically demand this ransom in exchange for decrypting the data and restoring access.

6. **Business Email Fraud:**

This type of crime targets companies that conduct financial transactions, particularly those working with international suppliers. Criminals gain access to the email accounts of executives or financial officers through phishing or hacking. They create email addresses similar to those of authorized personnel or hack into original addresses, deceiving employees into processing fraudulent financial transfers. Such activities often lead to significant monetary losses.

5. Cybersecurity Risk Management: [64]

Cybersecurity risk management refers to the set of technical, organizational, and administrative measures aimed at preventing unauthorized use, misuse, or recovery

[64] Yaqoub, Ibtihaj Ismail et al., 2022, A proposed indicator for accounting disclosure of cyber risks in the Iraq Stock Exchange according to international requirements, an experimental study, Journal of Financial, Accounting and Administrative Studies, Volume 9, Issue 1, pp. 1407-1408

of electronic information and associated systems. Its purpose is to ensure the availability and continuity of information systems while enhancing data protection, confidentiality, and privacy.

The National Cybersecurity Strategy in Iraq defines cybersecurity risk as the potential threat and vulnerabilities within the country's cyberspace that could harm the security of information systems and critical infrastructure. These risks arise due to cyber threats and weaknesses in cloud infrastructures.

The National Institute of Standards and Technology (NIST) has released the updated version 2.0 of its Cybersecurity Framework, a framework that provides a way for organizations to better understand, manage, and mitigate cybersecurity risks. The framework is intended to help all organizations manage and mitigate risks and is no longer limited to organizations operating in critical infrastructure, which was its original target audience. The Cybersecurity Framework focuses on a set of core functions: identification, protection, detection, response, recovery, and governance, which includes strategic decision-making related to cybersecurity at the enterprise level. [65]

Accounting and auditing play an important role in managing cybersecurity risks, as they are emerging risks that lead to huge financial losses as well as reputational and operational risks, by building an effective cybersecurity risk management system (similar to an internal control system) by conducting the necessary tests for the effectiveness of cybersecurity control elements and by selecting standard reference points for technology controls within the organization.

The American Public Accounting Oversight Board (ACAOB) has prioritized future cybersecurity risks as it works to address cybersecurity risks in the audit process and has issued guidance to help auditors understand and mitigate these risks. The Board recommends that auditors assess the risks of their IT systems and implement

[65] httsp://www.barikat.com.tr

controls to protect against cyber threats, and that auditors periodically test their IT systems to ensure their effectiveness. [66]

6. Requirements for Achieving Cybersecurity:[67]

1. Determining the work procedures in information networks: They must be clear and specific in what is allowed or not allowed in relation to information security on the network.
2. Providing the necessary mechanisms to implement work policies: There must be clarity and precision regarding how to implement these policies and determine the penalties that will be imposed in the event of a breach.
3. Human resources: It is necessary to focus on assigning the management and operation of information networks to competent human elements, trained and qualified to deal with modern techniques and technology, and not to allow any room for amateurs to tamper with the capabilities of government agencies.
4. Updating the original status of network equipment: The original status of equipment connected to information networks must be changed periodically as a precautionary measure, which helps prevent hacking.
5. Monitoring: It is necessary to ensure the provision of continuous and accurate monitoring and follow-up of information activities on the network.
6. Providing a type of monitoring and follow-up of information activities: This must be conducted in an accurate and permanent manner, with the aim of discovering any suspicious activities or abnormal movements within the network and working to avoid worsening conditions.
7. Good selection of network points' locations: It is necessary to be precise when selecting connection points to information networks, ensuring these points are in secure locations and protected from hacking.
8. Data encryption: Data on the network must be encrypted to secure information, using globally recognized and trusted programs. Authentication and encryption protocols must also be employed.

[66] https://fastercapital.com

[67] Al-Qatani, Salem bin Saeed Al-Anzi Hamoudin Muhammad 2011, Exchange of Information between Security Agencies in the Kingdom of Saudi Arabia: A Field Study, PhD Thesis, College of Graduate Studies, Naif Arab University for Security Sciences, Saudi Arabia.

9. [68]Endpoint Security: Employees often use publicly owned laptops and mobile devices, which are common targets for cyberattacks. Endpoint security solutions can help prevent and remediate malware infections and other cyber threats on these devices.

10. Internet of Things (IoT): Critical infrastructure is typically operated and controlled by IoT devices, which can pose significant risks to government cybersecurity due to unpatched vulnerabilities and other factors. IoT devices must be carefully managed to ensure they are not infected with malicious botnets or used as access points for organizational networks.

7. The Importance of Oversight in Enhancing Cybersecurity Measures

The Joint Inspection Unit report on the 2021 study of cybersecurity in the organizations of the United Nations system in Geneva indicated that internal and external oversight bodies in the organizations of the United Nations system were concerned with cybersecurity issues, even if there were no specific references in their mandates to the subject itself. The inspectors came across several examples of institutional improvements to the cybersecurity framework in the participating organizations that resulted from oversight recommendations, such as the creation of the position of Chief Information Security Officer, recommendations for training, and the development of an operational roadmap.

The report noted that audit and oversight committees addressed cybersecurity issues as part of their mandate covering central risk management and not in the context of IT governance and communications. These committees adopted the topic of cybersecurity not merely to support management but to inform legislative and administrative bodies of cybersecurity risks, enabling them to contribute to mitigating

[68] https://www.checkpoint.com Cyber Security Cyber Hub

the risks facing organizations and ensuring that all oversight bodies add maximum value from a cybersecurity perspective. The report indicated that it is necessary for the work of oversight staff to be guided by the knowledge and experience of cybersecurity experts within the organization, and for this knowledge and experience to be channeled into that work. [69]

Abu Musa's 2004 study on external auditors (New Challenges for Auditing E-Business external auditors) aimed to clarify the challenges facing external auditors in the e-business environment and provided guidance on how to audit it. The most important auditing standards affected by the electronic environment were presented, namely: the standard for planning the audit process, the standard for collecting and evaluating evidence, auditor independence, adequate training, and examining the internal control system. The study concluded that external auditors must understand how modern technology affects the auditing process and must obtain sufficient knowledge and skills to deal with the electronic environment. Additionally, planning the audit process has become a critical task requiring great attention from auditors.

The review of IT systems, controls, and monitoring processes has become a central theme of audits conducted by Supreme Audit Institutions (SAIs) as a natural result of the reliance on IT systems to support government and public sector organizations. These systems must protect the organization's data and assets while supporting financial and other specific missions and objectives

Technological advances have increased risks and vulnerabilities, as well as the growth of technical systems and networks. Web-based information has increased the security risks facing government organizations. The COVID-19 pandemic has also created unprecedented challenges for government organizations, which need to continue carrying out their missions while ensuring that their employees can do their work safely and effectively.

These trends, combined with the increasing sophistication of hackers and others with malicious intent, increase the risk of sensitive data being compromised. Ineffective protection of an organization’s systems and networks can impede the delivery of critical services. As such, each new vulnerability must be identified, the risks

[69] https://www.unjiu.org

assessed in terms of likelihood and impact, mitigated according to the organization's risk appetite, and controlled where appropriate.

The International Organization of Supreme Audit Institutions (INTOSAI) has issued Guidance 5100 as a comprehensive framework for conducting information systems audits within the INTOSAI framework, and its contents can be applied to the planning, implementation, reporting, and follow-up stages of the audit process.[70]

Therefore, it can be said that the oversight carried out by the supreme financial audit institutions over information systems should play a vital role in enhancing cybersecurity.

8. The role of the auditor in monitoring information systems to enhance cybersecurity:

When starting the audit process, the auditor must assess the risks, which is an important part of the audit planning. Auditing standards indicate that the auditor is required to understand the business risks that may lead to the risks of errors or material misstatements in the financial reports. Therefore, cybersecurity risks are an area of risk that is no less important than business risks and cannot be ignored.[71]

The auditor and the reviewer must conduct an examination of the institution's internal control system in order to be able to form a clear and correct opinion about the institution. [72]

The auditor must do the following:[73]

1. **Cybersecurity Risk and Controls Assessment:**
   Auditors should assess the organization's cybersecurity risks and controls as part of their audit. This includes assessing the audited entity's risk management practices, information security policies, and information technology controls to determine whether they are adequate to mitigate cybersecurity threats and protect the organization's data and financial systems.

[70] INTOSAI Development Initiative Guide to IT Auditing Supreme Audit Institutions, 2022 pp. 1-3
[71] Ali 2023, previously cited reference, p. (4)
[72] Lotfi, 2007, previously cited reference, p. 411
[73] htts://gridlex.com/the impact of cybersecurity risks on the audit process in accounting

2. **Assessing the Impact on Financial Reporting:**
   Cybersecurity incidents can have a significant impact on an organization's financial reporting, potentially resulting in errors or inaccuracies in financial statements. Auditors should consider the potential financial implications of cybersecurity breaches, such as the cost of remediation efforts, potential fines, damages, and reputational damage, and assess whether these matters have been accurately calculated and disclosed in the organization's financial statements.
3. **Identifying Fraud and Manipulation:**
   Cybersecurity threats can also create opportunities for fraud and manipulation of financial data. Auditors must be vigilant when detecting and investigating potential fraudulent activities or irregularities resulting from cybersecurity incidents. This may include analyzing data for unusual patterns, corroborating information with external sources, and interviewing management and employees to gather evidence and insights.
4. **Ensure Compliance with Regulations:**
   The increasing prevalence of cybersecurity risks has led to the introduction of various regulations and guidelines aimed at protecting sensitive data and ensuring the integrity of financial reporting. Auditors must ensure that organizations comply with these regulations, such as the General Data Protection Regulation, evaluate the policies and procedures taken by the audited entities by verifying the existence of clear and updated cybersecurity policies and procedures, monitor compliance with national and international security standards and policies, and verify the existence of data recovery procedures and disaster recovery systems.[74]

The audit function in information systems includes examining all components of the system, represented by workers, hardware, software, and databases.

These components integrate with each other to achieve the goal of the audit as follows:[75]

[74] Hunton, James, et al, 2021, Business and Audit RISKS Associated with ERP SYSTEMS: knowledge Differences Between information systems audit specialists and financial auditors, p1-5
[75] Obstacle, Al-Rida, 2008, Auditing in the Light of Accounting Information Systems, a working paper within the global events of the Association of Accountants

First: **Supervision of Workers**, which deals in particular with:

1. Insisting on granting the employee their annual leave.
2. Verifying the presence of passwords and specialized monitoring programs that do not allow anyone to access any information.
3. [76]Auditing manual controls, such as separation of duties between system users and scheduling for system users, including production and programmers, data entry operators, network administrators, and the like.
4. Ensuring the rotation of tasks among operations staff.
5. Verifying the existence of cybersecurity training and awareness programs for employees, and ensuring that employees understand their roles and responsibilities in protecting information.

Second: **Monitoring of Devices**, which includes the following:

1. Choosing a secure location for the devices.
2. Determining the list of employees allowed to use the computer.
3. Keeping backup copies of important files and records in a safe place.
4. Insuring the devices.
5. Focusing on existing controls to protect assets and ensure data integrity, such as adequate fire prevention, water detection, and physical security controls.[77]

Third: **Software Control** through:

1. Verifying the program accreditation procedures.
2. Conducting a sudden review of the program during operation and not relying on evaluating the outputs only.
3. Ensuring that the program outputs are in line with the goal for which it was designed.
4. Reviewing reports, including system performance metrics.
5. Reviewing the infrastructure of the entity subject to supervision to ensure that the necessary protection measures are implemented, such as firewalls, intrusion detection systems, and antivirus software.[78]

[76] Hunton, James, et al, 2021, p1-5 op. cit.
[77] Hunton, James, et al, 2021, 21-5 Reference above
[78] Hunton, James, et al, 2011-5 op. cit.

6. Auditing controls that monitor the recording of system error messages and the re-running of cancelled (expired) programs, which would contribute to maintaining data integrity.

Fourth: **Database Control:**
The auditor must audit the database as it contains the basic and confidential data of the organization, so it must be protected from misuse, especially since the cost of redesigning another database is very expensive. A comprehensive risk analysis should be conducted to identify gaps and weaknesses in information systems, assess the impact of risks, and ensure that plans are in place to respond to them.

Upon completion of the audit process, a report must be prepared that includes the audit results, provides recommendations for improvement, follows up on the implementation of the recommendations, and evaluates their impact on reducing risks, which contributes to building a strong and sustainable infrastructure in the government sector.

9. Adapting the Audit Process to Address Cybersecurity Risks:[79]

1. **Developing Cybersecurity Expertise:**
   Auditors must develop expertise in cybersecurity risk management and controls to effectively assess an organization's exposure to cybersecurity threats. This may include obtaining specialized certifications, such as Certified Information Systems Auditor, attending training courses, and staying up-to-date on emerging trends and best practices in cybersecurity.
2. **Leveraging Technology and Data Analytics:**
   Auditors can leverage technology and data analytics tools to enhance their ability to identify and assess cybersecurity risks.
3. **Collaborating with IT and Cybersecurity Professionals:**
   Given the complexity of cybersecurity risks, auditors may need to collaborate with IT and cybersecurity professionals to gain the expertise and insights needed to assess an organization's cybersecurity controls and risk management practices. This may include engaging external experts to address the challenges posed by cybersecurity threats.

[79] htts://gridlex.com/ the impact of cybersecurity risks on the audit process in accounting

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

   A risk-based audit approach can help auditors prioritize their efforts and resources in areas most exposed to cybersecurity risks. This includes identifying and assessing the most critical systems and processes in the organization, determining the likelihood and impact of potential cybersecurity incidents, designing audit procedures to address these risks, leveraging technology and data analytics, and collaborating with specialists to do so.

Chapter Three: Field Study

To achieve the research objectives and prove its hypotheses, the researcher relied on two main sources for data collection:

1. Primary Sources:

The researcher collected the primary data by using a questionnaire as the main research tool. It was specifically designed for this purpose based on previous studies, where the variables under investigation were explored to address the analytical aspects of the research.

2. Secondary Sources:

In addressing the theoretical framework of the research, the researcher referred to secondary data sources, including books, research papers, journals, theses, and publications from websites related to the research topic.

Second: Research Community and Sample

1. Research Community:

The research community consists of inspectors from the Central Agency for Financial Control in Syria, numbering approximately 950 male and female inspectors. A sample of this community was selected, specifically inspectors from the Aleppo branch of the Central Agency for Financial Control, for the sake of efficiency in data collection and ease of communication.

2. Research Sample:

The sample was taken from the Aleppo branch of the Central Agency for Financial Control. The questionnaire was distributed to 77 male and female inspectors. The researcher used a facilitated random sampling method to select the sample, and 69 questionnaires were returned, with 65 being valid for analysis.

Third: Research Tool

A questionnaire was designed to achieve the objectives of this research, based on previous studies, similar studies, and the theoretical framework of the research. It was directed to the inspectors at the Central Agency branch in Aleppo. The questionnaire was divided into the following sections:

- The demographic characteristics axis, also known as the personal data axis of the research sample, included the following variables: gender, age, job title, academic qualification, and years of work experience.
- The axis evaluating the internal control system and internal controls consisted of 15 statements or questions.
- The axis assessing the supervisory practices of the Central Agency for Financial Control contained 13 statements or questions.

Thus, the total number of questionnaire statements was 28, with responses following the five-point Likert scale as shown in the following table:

Table No. (1) Five-point Likert Scale

Ranking	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Points	1	2	3	4	5

Fourth: Stability of the Research Tool (Reliability):

The reliability test was conducted on the research sample using the Alpha Cronbach coefficient. The reliability of the measurement tool refers to the internal consistency between its statements. The reliability of the tool has two aspects: the first is the stability of the scale, meaning the same results should be obtained if the variable is measured several times. The second aspect of reliability is objectivity, meaning that the same degree of consistency should be obtained regardless of the person who applies the test or the person who designed it. The value of the Alpha Cronbach correlation coefficient ranges between 0 and 1. For the scale to be considered reliable, the minimum value of the coefficient must be no less than 0.70[80]. Table No. (2) shows the results of the Alpha Cronbach coefficient analysis for each axis (section) of the questionnaire.

[80] Darq, Omar, The Impact of Organizational Justice Management on Work Stress Management (2007), Master's Thesis in Business Administration, University of
Ain Shams Faculty of Commerce Ain Shams, p. 91

Table (2) Cronbach's Alpha Coefficient for Questionnaire Axes

No.	Axis Text	Number of Paragraphs	Cronbach´s coefficient value	Reliability assessment	Rang
1	Evaluation of the internal control system and internal Control	15	0,702	Middle	2
2	Central Agency for financial control´s regulatory practices	13	0,795	Middle	1
--	All axes	28	0,812	High	--

We note from **Table No. (2)** that the value of the Alpha Cronbach coefficient for the questionnaire ranges between 0.702 for the axis related to the evaluation of the internal control system and internal control, and 0.795 for the axis related to the control practices of the Central Agency for Financial Control. This indicates that the coefficient values for the questionnaire axes are greater than 0.70, which signifies that the research tool demonstrates internal consistency between its phrases. Additionally, the total coefficient value for the entire questionnaire is 0.812, which is considered high and indicates a good degree of stability for the questionnaire, confirming that it is valid for measuring its intended purpose.

Field Framework and Statistical Processing

The researcher completed and analyzed the questionnaire using the SPSS 18 statistical program and conducted the appropriate statistical tests to serve the research objectives and validate or refute the hypotheses. The questionnaire was applied to a sample of 65 individuals representing the studied community of approximately 950 individuals, meaning that the sample size constitutes 6.7% of the community size.

The following table shows the distribution of sample members according to their personal data:

Table No. (3) Distribution of Research Sample Individuals According to the Variables of Gender, Job Title, and Academic Qualification

Gender	Total	Percentage %	Job title	Number	Percentage	Academic qualification	Number	Percentage
Males	44	67,7	Assistant inspector	6	9,2	Bachelor	6	9,2
Females	21	32,3	Inspector	26	40,0	Bachelor	26	40,0
--	--	--	Senior inspector	33	50,8	Master´s	33	50,8
The Total	65	100	The total	65	100	The Total	65	100

The table was prepared by the researcher based on the outputs of the SPSS statistical program.

Table No. (4) Distribution of research sample members according to the variables of age and years of experience

The age	Number	Percentage	Years of experience	Number	Percentage
21-30	0	0	Less than a year	2	3,1
31-40	25	38,5	1-5	5	7,7
41-50	22	33,8	6-10	18	27,7
Older than 50	18	27,7	11-15	9	13,8
--	--	--	More than 15	31	47,7
The total	65	100	The total	65	100

The table was prepared by the researcher based on the outputs of the SPSS statistical program.

- The results of the hypothesis test for demographic variables indicate that there are no statistically significant differences between the responses of the research sample to questions related to the role of information control systems in reducing cybersecurity risks in the government sector based on the demographic characteristics of the sample. A one-way ANOVA was conducted to determine whether there are statistically significant differences in the responses of the research sample to questions regarding the role of information control systems in mitigating cybersecurity risks in the government sector, considering the following characteristics of the research sample.

1. By Gender:

Table No. (5) below presents the results of the One-Way ANOVA, analyzing the responses of the research sample members based on the gender variable.

Table No. (5): Results of the One-Way ANOVA

Source of Variation	Sum of Squares	Degrees of Freedom (df)	Mean Squares	F Value	Significance Level (Sig)	Statistical Significance
Between Groups	0.181	1	0.181	1.272	0.264	Insignificant
Within Groups	8.964	63	0.142			
Total	9.145	64				

Prepared by the researcher based on the results of the statistical analysis of the questionnaire.

From the table above, it can be observed that the value of the significance level (Sig) is 0.264, which is greater than the assumed threshold of 0.05 (5%). This indicates that there are no statistically significant differences in the responses of the research sample members to the questions concerning the role of information systems control in reducing cybersecurity risks in the government sector based on the gender variable.

2. By Job Title:

Table No. (6) below presents the results of the One-Way ANOVA, analyzing the responses of the research sample members based on their job title.

Table No. (6): Results of the One-Way ANOVA

Source of Variation	Sum of Squares	Degrees of Freedom (df)	Mean Squares	F Value	Significance Level (Sig)	Statistical Significance
Between Groups	0.61	2	0.31	2.23	0.12	Insignificant
Within Groups	8.53	62	0.14			
Total	9.15	64				

Prepared by the researcher based on the results of the statistical analysis of the questionnaire.

From the table above, it can be observed that the value of the significance level (Sig) is 0.12, which is greater than the assumed threshold of 0.05 (5%). This indicates that there are no statistically significant differences in the responses of the research sample members to the questions concerning the role of information systems control in reducing cybersecurity risks in the government sector based on the job title variable.

3. According to Age:

Table No. (7) below presents the results of the One-Way ANOVA, analyzing the responses of the research sample members based on the age variable.

Table No. (7): Results of the One-Way ANOVA

Source of Variation	Sum of Squares	Degrees of Freedom (df)	Mean Squares	F Value	Significance Level (Sig)	Statistical Significance
Between Groups	0,16	2	0,08	0,55	0,579	Insignificant
Within Groups	8,99	62	0,15			
Total	9,15	64				

Prepared by the researcher based on the results of the statistical analysis of the questionnaire.

From the table above, it can be observed that the value of the significance level (Sig) is 0.579, which is greater than the assumed threshold of 0.05 (5%). This indicates that there are no statistically significant differences in the responses of the research sample members to the questions concerning the role of information systems control in reducing cybersecurity risks in the government sector based on the age variable.

4. According to Academic Qualification:

Table No. (8) below presents the results of the One-Way ANOVA, analyzing the responses of the research sample members based on their academic qualifications.

Table No. (8): Results of the One-Way ANOVA

Source of Variation	Sum of Squares	Degrees of Freedom (df)	Mean Squares	F Value	Significance Level (Sig)	Statistical Significance
Between Groups	0,05	2	0,025	0,18	0,836	Insignificant
Within Groups	9,09	62	0,146			
Total	9,15	64				

Prepared by the researcher based on the results of the statistical analysis of the questionnaire.

From the table above, it can be observed that the value of the significance level (Sig) is 0.836, which is greater than the assumed threshold of 0.05 (5%). This indicates that there are no statistically significant differences in the responses of the research sample members to the questions concerning the role of information systems control in reducing cybersecurity risks in the government sector based on the educational qualification variable.

5. According to Years of Experience:

Table No. (9) below presents the results of the One-Way ANOVA, analyzing the responses of the research sample members based on their years of experience.

Table No. (9): Results of the One-Way ANOVA

Source of Variation	Sum of Squares	Degrees of Freedom (df)	Mean Squares	F Value	Significance Level (Sig)	Statistical Significance
Between Groups	0,48	4	0,12	0,83	0,514	Insignificant
Within Groups	8,67	60	0,14			
Total	9,15	64				

Prepared by the researcher based on the results of the statistical analysis of the questionnaire.

From the table above, it can be observed that the value of the significance level (Sig) is 0.514, which is greater than the assumed threshold of 0.05 (5%). This indicates that there are no statistically significant differences in the responses of the research sample members to the questions concerning the role of information systems control in reducing cybersecurity risks in the government sector based on the years of experience variable.

From the previous results, it is clear that there are no statistically significant differences in the answers of the research sample members regarding the role of information systems control in reducing cybersecurity risks in the government sector (evaluation of the internal control system, internal control, and the control practices of the Central Agency for Financial Control) according to all sample characteristics. Therefore, we accept the null hypothesis stating that there are no statistically significant differences in the responses of the research sample members regarding the questions related to the role of information systems control in reducing cybersecurity risks in the governmental sector, versus rejecting the alternative hypothesis that there are fundamental differences with statistical significance between the answers of the research sample regarding the role of information systems control in reducing cybersecurity risks in the government sector according to the characteristics of the research sample.

The results of testing the hypothesis of the original research variables, which state that: There is no statistically significant role for information systems control in reducing cybersecurity risks in the government sector. The following two sub-hypotheses branch out from this hypothesis:

1. There is no statistically significant role for the internal control system and internal control in the information systems environment in reducing cybersecurity risks in the government sector based on the review of the structure and framework of internal control and the evaluation of internal control by the Central Agency for Financial Control.

The results were as shown in the following table

Table no. (10) Response of the research sample individuals regarding the evaluation of the internal control system and internal control

		Verification degree							
No.	Statement	Strongly Agree (n/%)	Agree (n/%)	Neutral (n/%)	Disagree (n/%)	Strongly Disagree (n/%)	Arithmetic Mean	Relative Importance	Approval Level
1.	Provides access controls to data and information to reduce the risk of hacking, misuse, and destruction of sensitive information.	2 (3.1%)	20 (30.8%)	20 (30.8%)	20 (30.8%)	3 (4.6%)	2.97	10	Neutral
2.	Keeps backup copies of important files and records in a safe place on a regular basis.	29 (44.6%)	9 (13.8%)	17 (26.2%)	8 (12.3%)	2 (3.1%)	3.85	6	Agree
3.	Internal IT controls ensure confidentiality, integrity, validity, and availability of data.	3 (4.6%)	9(13.8%)	29 (44.6%)	20 (30.8%)	4 (6.2%)	2.80	11	Neutral
4.	Implements basic security measures such as strong, unpredictable passwords that include numbers, upper/lower case letters, and symbols.	19 (29.2%)	34 (52.3%)	10 (15.4%)	1 (1.5%)	1 (1.5%)	4.06	4	Agree
5.	Academic staff are adequately trained in safe file-handling techniques.	54 (83.1%)	6 (9.2%)	5 (7.7%)	0 (0.0%)	0 (0.0%)	4.75	1	Strongly Agree

6.	Conflicting functions (e.g., accounting vs. treasury tasks) are separated for system users.	3 (4.6%)	5 (7.7%)	7 (10.8%)	5 (7.7%)	0 (0.0%)	4.60	2	Strongly Agree
7.	An authorized list of employee names is maintained for system usage.	43 (66.2%)	14 (21.5%)	5 (7.7%)	2 (3.1%)	1 (1,5%)	4.48	3	Strongly Agree
8.	The cybersecurity department, if any, is independent of the IT department.	1 (1.5%)	7 (10,8%)	9 (13.8%)	39(60%)	9 (13.8%)	2.26	14	Disagree
9.	Update old hardware and unsupported software versions as they pose significant risks to the organization's data and operations.	8 (12.3%)	12(18.5%)	33(50.8%)	7(10.8%)	5(7.7%)	3.17	9	Neutral
10.	There are surveillance cameras to detect any intruder and they are maintained periodically.	5 (7.7%)	40(61.5%)	14(21.5%)	5(7.7%)	1(1.5%)	3.66	7	Agree
11.	Choose a secure location for the devices.	12 (18.5%)	9 (13.8%)	38(58.5%)	4(6.2%)	2(3.1%)	3.38	8	Neutral
12.	Use of hardware and software that helps increase control of network access, such as antivirus	11 (16.9%)	43 (66.2%)	8(12.3%)	0(0.0%)	3(4.6%)	3.91	5	Agree
13.	Update antivirus software regularly	6 (9.2%)	4 (6.2%)	33(50.8%)	15(23.1%)	7(10.8%)	2.80	11	Neutral
14.	Setting controls for data confidentiality, encryption, and access only by authorized persons	3 (4.6%)	8(12.3%)	29(44.6%)	19(29.2%)	6(9.2%)	2.74	12	Agree
15.	Data transfer from one location to another is done over secure, unhackable transmission channels	5 (7.7%)	8(12.3%)	22(33.8%)	23(35.4%)	7(10.8%)	2.71	13	Agree
	Evaluation of the internal control system and internal control							**3.476**	**Agree**

It is clear from Table No. (10) above that the level of agreement is good, as the total arithmetic mean value for all the statements of this axis reached 3.48, which indicates the possibility of achieving cybersecurity through evaluating the internal control system and internal control by the Central Agency for Financial Control. Most of the

responses lean towards the approval of the research sample members regarding the axis statements, which would help achieve cybersecurity in public entities subject to control. The data in the previous table highlight the most important statements that received the highest ranking among the axis statements, which are listed in order:

1. Do not share passwords with others (Phrase No. (5)) with an average approval rate of 4.60.
2. Separation of conflicting functions of system users, such as separating accounting tasks from cashier tasks (Statement No. (6)), with an average approval of 4.60.
3. The existence of a list of the names of employees authorized to use the system (Statement No. (17)), with an average approval of 4.48.
4. Applying basic security measures such as having strong passwords that include numbers, uppercase and lowercase letters, and unpredictable symbols, and changing them regularly (Statement No. (4)), with an average approval of 4.06.
5. Using devices and software that help increase control over access to the network, such as anti-virus software (Statement No. (12)), with an average approval rate of 3.91.
6. Keeping backup copies of important files and records in a safe place periodically (Statement No. (2)), with an average approval rate of 3.85.
7. The presence of surveillance cameras to detect any intruder and their periodic maintenance (Phrase No. (10)), with an average approval of 3.66.

The level of agreement for the previous statements ranges between "agree" and "strongly agree," which indicates that there is a statistically significant role for control in the information systems environment in reducing cybersecurity risks in the government sector. Therefore, we reject the null hypothesis that there is no statistically significant role for the internal control system and internal control in the information systems environment in reducing cybersecurity risks in the government sector. This conclusion is based on the review of the structure and framework of internal control and the evaluation of internal control by the Central Agency for Financial Control, in exchange for accepting the alternative hypothesis.

The results of the analysis indicate that the research sample members believe that the internal systems and internal control in the entities subject to supervision are sufficient in themselves, if activated in the appropriate manner, to achieve an acceptable level of cybersecurity. This may reflect the belief that the problem lies not in the systems themselves, but in their implementation and monitoring.

2). There is no statistically significant role for the oversight exercised by the Central Agency for Financial Control over information systems in reducing cybersecurity risks in the government sector, as the results are as follows:

It is shown in the following table.

		Verification degree							
No.	**Statement**	**Strongly Agree (n/%)**	**Agree (n/%)**	**Neutral (n/%)**	**Disagree (n/%)**	**Strongly Disagree (n/%)**	**Arithmetic Mean**	**Relative Importance**	**Approval Level**
1.	Ensure that information systems are able to provide appropriate evidence for the audit process.	2 (3.1%)	9 (13.8%)	27 (41.5%)	21(32.3%)	6(9.2%)	2.69	8	Neutral
2.	Evaluating and monitoring the extent of the entity subject to control's commitment to providing appropriate procedures related to data security and preserving it from damage or distortion and the procedures followed for the safety of the information system.	6(9.2%)	14 (21.5%)	21 (32.3%)	22(33.8%)	2(3.1%)	3.00	5	Neutral
3.	Ensure effective use of firewalls and antivirus software to protect systems from the introduction of malicious or unauthorized software.	0(0.00%)	5(7.7%)	5(7.7%)	45(69.2%)	10 (15.4%)	2.08	13	Disagree
4.	Ensuring the effective use of encryption, including maintaining confidentiality and security when sending data and information over the network and preventing misuse through encryption technology.	2(3.1%)	3(4.6%)	21 (32.3%)	17(26.2%)	22 (33.8%)	2.17	12	Disagree

5.	Monitoring the compliance of the entities subject to control in processing data in accordance with applicable laws and regulations and compliance with cybersecurity legislation.	3(4.6%)	12 (18.5%)	28(43.1)	12(18.5%)	10 (15.4%)	2.78	6	Neutral
6.	Ensure the ability to retrieve operational documents from electronic document files such as documents stored online or in electronic systems.	1(1.5%)	9 (13.8%)	32 (49.2%)	8(12.3%)	15 (23.1%)	2.58	9	Disagree
7.	Give the inspector the authority to view all information in the database.	0(0.0%)	3(4.6%)	50 (76.9%)	6(9.2%)	6(9.2%)	2.77	7	Neutral
8.	Auditing it to ensure the integrity of the outputs and the absence of duplication or repetition by taking a sample and calculating it manually to obtain a single result.	7(10.8%)	47(72.3 %)	8(12.3%)	3(4.6%)	0(0.0%)	3.89	1	Agree
9.	Ensure that the protection devices are in good condition and fill them periodically, such as the fire protection devices.	6(9.2%)	36 (55.4%)	20 (30.8%)	3(4.6%)	0(0.0%)	3.69	2	Agree
10.	Ensure that systems and procedures are in place to address identified errors and deviations.	13(20%)	4(6.2%)	14(21.5 %)	29(44.6%)	5(7.7%)	3.14	4	Neural
11.	Ensure that business continuity plans and disaster recovery procedures are established and effective.	2(3.1%)	0(0.0%)	21(32.3 %)	30(46.2%)	12(18.5%)	2.23	11	Disagree
12.	Ensure that critical operations are authorized by at least two authorized employees.	10(15.4%)	26(40%)	15(23.1 %)	7(10.8%)	7(10.8%)	3.38	3	Neutral
13.	Ensure that the program's outputs are consistent with the intended purpose for which it was designed.	0(0.0%)	1(1.5%)	19(29.2 %)	44(1.5%)	67.7(1.5%)	2.31	10	Disagree
	Central Agency for Financial control´s regulatory practices							2.82	Neutral/Disagree

It is clear from Table No. (11) that the level of approval is very low, as the total arithmetic mean value for all the statements in this axis reached 2.82 (neutral), which is closer to disagreement. This indicates the impossibility of achieving cybersecurity in public entities through the control practices carried out by the Central Agency for Financial Control. The majority of the research sample members tend towards neutrality or disagreement with the control practices carried out by the Central Agency for Financial Control.

Results indicating neutrality or disagreement can be interpreted as research sample members not being fully informed about policies and procedures related to cybersecurity, or the lack of clarity regarding the policies and procedures to be followed. It may also suggest that research sample members do not understand their responsibilities or roles in implementing and monitoring cybersecurity practices in regulated entities, or they may lack sufficient knowledge or awareness of the importance of cybersecurity and the procedures required to achieve it.

Looking at Table No. (11), we find that only two phrases out of thirteen received the highest approval ratings (8-9), while the rest of the statements ranged, as mentioned, between neutrality and disagreement. This indicates that there is no statistically significant role for the control practices carried out by the Central Agency for Financial Control on information systems in reducing cybersecurity risks in the government sector. Therefore, we accept the null hypothesis that there is no statistically significant role for the control practices carried out by the Central Agency for Financial Control on information systems in reducing cybersecurity risks in the government sector, in contrast to rejecting the alternative hypothesis that there is a significant role.

Statistically, the control practices carried out by the Central Agency for Financial Control on information systems in reducing cybersecurity risks in the government sector.

Possible reasons for the results can be explained as follows:

1. Difficulties in implementing cybersecurity policies and procedures due to complexities or lack of support.

2. Lack of training, guidance, and knowledge to deal with cybersecurity risks effectively.
3. Inadequate technical skills related to cybersecurity among the research sample members.
4. Lack of resources within the central agency, whether in terms of technology or human expertise, to enhance cybersecurity in the government sector.
5. Lack of clarity regarding the specific role of the central agency in the field of cybersecurity, or conflict of roles between the central agency and other entities concerned with cybersecurity.
6. The lack of clear and specific policies and procedures for the tasks of the research sample individuals regarding cybersecurity.

Recommendations:

1. Implementing periodic verification and auditing procedures for information systems in entities subject to control to ensure compliance with cybersecurity standards and take the necessary corrective measures.
2. Enhancing training and professional development by organizing advanced and specialized training courses in cybersecurity for all employees of the Central Agency for Financial Control, organizing internal awareness campaigns to enhance employees' understanding of the importance of cybersecurity and how to contribute to achieving it, and developing skills and knowledge of the latest cybersecurity technologies and challenges.
3. Holding interactive workshops to raise awareness and exchange experiences among members of the Central Agency for Financial Control.
4. Forming joint working groups between the Central Agency for Financial Control, government agencies, and entities concerned with cybersecurity to exchange knowledge and expertise on best practices in cybersecurity.
5. Preparing and distributing detailed guidelines explaining the specific roles, responsibilities, and procedures that must be followed in the field of monitoring information systems and cybersecurity, and encouraging the agency's employees to participate in developing these guidelines, which enhances their sense of responsibility and commitment to implementation.

6. Establishing key performance indicators to measure the effectiveness of practices and procedures followed by the Authority's employees in the field of cybersecurity.
7. Conducting periodic evaluations to review performance, identify areas that need improvement, and implement corrective plans when necessary.
8. Updating the guidelines and procedures specified for the tasks of the Central Agency's employees with regard to cybersecurity in the entities subject to supervision to ensure they keep pace with the latest threats and developments.
9. Encouraging members of the Central Agency for Financial Control to attend conferences and seminars related to cybersecurity to learn about the latest developments and innovations.
10. Employing experts specialized in the field of cybersecurity within the Central Agency for Financial Control to coordinate efforts and provide technical support to the agency's personnel in their tasks.
11. Exchanging best practices between INTOSAI and ARBOSAI members to improve information systems oversight and cybersecurity in the government sector.

Arabic references:

- Hilali, Hilali Al-Sharbiny (2020). *Journal of Educational Technology and Digital Education*, Egyptian Society for Technological Development, Volume 1, Issue 1.
- Ali Haya Gamal Hashem (2023). "A proposed procedural approach to measure the extent of the external auditor's response to cyber risks in the client's facility." *Scientific Journal of Financial and Commercial Studies and Research*, Faculty of Commerce, Damietta University, Vol. 4, No. 2.
- Al-Samhan, Mona Abdullah (2020). "Requirements for Achieving Cybersecurity for Administrative Information Systems at King Saud University." *Journal of the College of Education*, Issue 111.
- Jassim Adhraa Diaa. "The role of information systems and internal control in enhancing the independence of supervisory work." *Journal of Administration and Economics*, Issue 126.
- Al-Fawal, Issam (2020). "Evaluating the Potential of Investment in Implementing an Information Security Management System in the Syrian Services and Communications Sector." Ministry of Higher Education, Higher Institute of Business Administration, Project Prepared for a Master's Degree in Business Administration, Executive Management.
- Al-Khasawneh, Reem Aqab (2009). "A Framework for Evaluating the Audit Bureau's Control in the Hashemite Kingdom of Jordan in Light of the Application of E-Government." PhD Thesis, Arab Open University for Graduate Studies, Jordan.
- Al-Khasawneh, Reem Aqab (2010). "Evaluation of government control procedures in light of the application of e-government in the Hashemite Kingdom of Jordan." *An-Najah University Journal for Research*, Volume 9/24.
- Ahmed Mustafa Jabbar (2021). "Internal Control System in Light of Electronic Operation and Its Impact on Performance Evaluation in Banks." Master's Thesis, Near East University, Nicosia.
- Al-Hakim, Salim Muslim (2010). "The possibility of controlling the automated accounting information systems of public institutions of an economic nature by inspectors of the Central Agency for Financial Control in Syria." *Damascus University Journal of Economic and Legal Sciences*, Volume 26, Issue 1.

- Al-Marri, Rashid Muhammad (January 2022). "The Impact of Information Technology on the Security System and Internal Control."
- Mansour, Amina Muhammad (2021). "The impact of cybersecurity on internal control and its reflection on the economic unit: A survey study." *Journal of Administration and Economics*, Issue 127, March.
- Maqrani, Qaddour (2016). "Evaluation of the extent of the contribution of electronic information systems security in reducing information systems risks: A case study of the Algerian Telecommunications Corporation." University of Kasdi Merbah, Ouargla, Algeria, Faculty of Economics, Commerce and Management Sciences, Department of Management Sciences, Master's thesis.
- Al-Sayed, Alaa (2005). "A proposed framework for developing the performance of financial control." Islamic University of Gaza, Palestine.
- Al-Mutairi, Yousef Muhammad (2020). "The Impact of Financial Control of the Kuwaiti Audit Bureau on Activating Governance Standards in Government Entities." *Journal of the College of Economics and Political Science*, Volume 21, Issue 3.
- Decree No. 64 of 2003, including the Central Financial Control Agency Law.
- Al-Zayoud, Ayman Hassan Ali (2022). "The Effectiveness of Internal Control and its Application in Light of the Electronic Operating System from the Perspective of Sahab Municipality Employees." *Arab Journal of Scientific Publishing*, Issue 42.
- Muhammad Amin Walid Ibrahim (2018). "An analytical study of the role of supreme audit bodies in developing internal audit systems to reduce financial corruption in government units, Libya." *Scientific Journal of Commercial and Environmental Studies*, Suez Canal University, Volume 9, Issue 2.
- Al-Jabri, Muhammad (2014). "Evaluating the role of the internal auditor in improving the internal control system of accounting information systems in insurance companies in Yemen." Master's thesis, Sana'a University, Yemen.
- Addas, Dahha; Saket, Ghassan (2020). *Banking Information System*, Publications of the University of Aleppo, Syria, Faculty of Economics.
- Abirat, Muqaddam; Houari, Maraj (2022). "Security Risk Management and Information Transparency of Information Systems in the Digital Environment." University of Laghouat, Algeria.

- Qasim Abdul Razzaq Muhammad (2008). *Computer Accounting Information Systems*, Dar Al Thaqafa for Publishing and Distribution, Amman, Jordan.
- Al-Ubaidi, Fatima Naji (2012). "The risks of using computerized accounting information systems and their impact on the effectiveness of the auditing process in Jordan." A published thesis to obtain a Master's degree in Accounting.
- Al-Sudairy, Muhammad bin Ahmed bin Turki (2012). *Management Information Systems*, King Saud University.
- Nour El Houda Shabou (2021). "The Role of Modern Communication Technology in Improving Public Service." Master's Thesis, University of Arab Ben Mahdi Oum El Bouaghi, Algeria.
- Hussein Skfali, Marwa Maqlatni (2020). "Management Information Systems and Their Impact on Employees' Job Performance: Case Study of the Agricultural and Rural Development Bank, Qalma Agency." Master's Thesis in Facilitation Sciences, Business Administration, University of May 8, Qalma.
- International Organization for Standardization and International Electrotechnical Commission (2010). *National Information Center Technical Department Quality and Development Division Standards Unit, Operating Systems Standards, Confidentiality and Security Committee Standard Code of Practice for Information Security Management*, ISO 27002.
- Amirhom, Jihan Adel (2022). "The impact of internal audit quality in reducing cybersecurity risks and its repercussions on rationalizing investors' decisions." *Journal of Financial and Commercial Research*, Volume 23, Issue 3.
- Al-Azzizi, Hani Muhammad Khalil Ibrahim (2023). "The International Legal System for Combating Cyber Risks." *Contemporary Egypt*, Issue 549.
- Shahata, Mr. Shahata (2022). "Towards an effective role for the internal auditor in managing cybersecurity risks in companies listed on the Egyptian Stock Exchange." *Scientific Journal of Financial and Administrative Studies and Research*, Volume Thirteen, Issue Two.
- Yaqoub, Ibtihaj Ismail et al. (2022). "A Proposed Indicator for Accounting Disclosure of Cyber Risks in the Iraq Stock Exchange According to International Requirements: An Experimental Study." *Journal of Financial, Accounting and Administrative Studies*, Volume 9, Issue 1.

- Al-Qahtani, Salem bin Saeed; Al-Arabi, Hamoudin Muhammad (2011). "Information Fairness among Security Agencies in the Kingdom of Saudi Arabia: A Field Study." PhD Thesis, College of Graduate Studies, Naif Arab University for Security Sciences, Saudi Arabia.
- INTOSAI Development Initiative (2022). *Guide to IT Auditing Organizations Audit*, Supreme.
- Lotfy, Amin Al-Sayed Ahmed (2007). *Modern Developments in Auditing*, Alexandria University House.
- Obstacle, Al-Rida (2008). "Auditing in the Light of Accounting Information Systems." A working paper within the global activities of the Syrian Association of Certified Public Accountants, Syria.
- Dora, Omar (2007). "The Impact of Organizational Justice Management on Work Stress Management." Master's Thesis in Business Administration, Ain Shams University, Faculty of Commerce, Ain Shams.
- Diban, Abdel Latif (2004). *Accounting Information Systems and Information Technology*.
- Mr. Alaa (2005). "A proposed framework for developing the performance of financial control at the Islamic University of Gaza, Palestine."

Foreign reference:

- Stephanie Damarey (2007). *Execution et control des finances*, Gualino Editeur.
- Janulevicius, Justinas (2016). *Op. cit.*
- Van der Meer, Jeroen (2012). "Multi-criteria decision model inference and application in information security risk classification." Master Thesis of Computational Economics, Erasmus School of Economics, Erasmus University Rotterdam.
- National Institute of Standards and Technology (2016). *Internal Report 7621, Revision.*
- Hunton, James, et al. (2021). "Business and Audit RISKS Associated with ERP Systems: Knowledge Differences Between Information Systems Audit Specialists and Financial Auditors."
- IAIS (2018). "Draft Application Paper on Supervision of Insurer Cybersecurity." In IAIS (Ed.).
- The International Telecommunication Union (ITU) (2010). *ITU Toolkit for Cybercrime Legislation*, Geneva.
- Kortjan, N., & Solms, R. (2013). "Cybersecurity education in developing countries: A South African perspective." Lecture notes of the Institute for Computer Sciences, Social Informatics, and Telecommunications Engineering.

Websites:

- Abdul Hassani, Waad Hadi (2016). "External Control and Its Impact on Evaluating the Performance of Internal Control." *ResearchGate*. https://www.researchgate.net
- Vivek Dodd (2024). "Cyber Risks in the Public Sector." *Skillcast*. https://www.skillcast.com
- *Al-Akhbar* (Lebanon). https://al-akhbar.com
- *Horizons-edu.com*. https://horizons-edu.com
- *DGSSI* (Morocco). https://www.dgssi.gov.ma
- *IMD*. https://www.imd.org
- Denibeh Kosin and Abraham Ho Ngzi Lu (2021). "Cybersecurity Risks." https://www.isaca.org/resources/isaca
- *Ad-Dawra*. https://www.ad-dawra.com
- *Mah6at.net*. https://www.mah6at.net
- *SIS*. https://www.sis.gov.eg
- *Mawdoo3*. https://mawdoo3.com
- Michael Aaron Dennis (2024). *Britannica*. https://www.britannica.com
- *ISF*. https://isf.gov.lb
- *Barikat*. https://www.barikat.com.tr
- *FasterCapital*. https://fastercapital.com
- Qusay Abu Shama (December 12). "Cyber Risk Awareness Guide." https://gridlex.com
- *Checkpoint* (Cybersecurity / Cyber Hub). https://www.checkpoint.com
- *UNJIU*. https://www.unjiu.org
- *Government Technology Insider*. https://governmenttechnologyinsider.com

Survey

About a research titled:

The Role of Information Systems Control in Reducing Cybersecurity Risks in the Government Sector

Prepared by researcher Abeer Zarak

Through this questionnaire, the researcher aims to:

- Measure the role of information systems oversight carried out by the inspectors of the Central Agency for Financial Control, in addition to the procedures carried out by the departments of the entities subject to oversight (through the inspector's assessment of the internal control system and internal control) in reducing cybersecurity risks in the government sector. Cybersecurity is a modern concept that expresses the security of networks, information systems, all data, information, and devices connected to the Internet and the risks associated with losing private and sensitive information, tampering with, and damaging data, systems, and networks.

Please tick (✔) in the appropriate box for your choice:

Personal Data

1. **Gender**:
   ☐ Male
   ☐ Female
2. **Job Title**:
   ☐ Assistant Inspector
   ☐ Inspector
   ☐ Senior Inspector
3. **Age**:
   ☐ 21-30 years
   ☐ 31-40 years
   ☐ 41-50 years
   ☐ More than 50 years
4. **Academic Qualification**:
   ☐ Bachelor's Degree
   ☐ Master's Degree
   ☐ Doctoral Degree (PhD)
   ☐ Master's Degree in Supervision
5. **Years of Experience**:
   ☐ Less than 1 year
   ☐ 1-5 years
   ☐ 6-10 years
   ☐ 11-15 years
   ☐ Over 15 years

The first axis: Evaluating the internal control system and internal control in the information systems environment in reducing cybersecurity risks in the government sector based on reviewing the structure and framework of internal control and evaluating it by the Central Agency for Financial Control.

When you review, test, and evaluate the internal control system and internal control in the information systems environment, what is the degree of your agreement with the following statements:

Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1. Provides access controls to data and information to reduce the risk of hacking, misuse, and destruction of sensitive information.	☐	☐	☐	☐	☐
2. Keeps backup copies of important files and records in a safe place on a regular basis.	☐	☐	☐	☐	☐
3. Internal IT controls relating to data confidentiality, integrity, validity, and availability have been adopted by the audited entity.	☐	☐	☐	☐	☐
4. Implements basic security measures such as having strong passwords that include numbers, upper- and lower-case letters, and unpredictable symbols, and changing them regularly.	☐	☐	☐	☐	☐
5. Does not share passwords with others.	☐	☐	☐	☐	☐
6. Separates conflicting functions of system users, such as separating accounting duties from cashier duties.	☐	☐	☐	☐	☐
7. Has a list of the names of employees authorized to use the system.	☐	☐	☐	☐	☐
8. The cybersecurity department, if any, is independent of the IT department.	☐	☐	☐	☐	☐
9. Updates old devices and unsupported software versions as they pose significant risks to the organization’s data and operations.	☐	☐	☐	☐	☐

10. The presence of surveillance cameras to detect any intruder and their periodic maintenance.	☐	☐	☐	☐	☐
11. Choose a secure location for devices.	☐	☐	☐	☐	☐
12. Use hardware and software that helps increase control over network access, such as antivirus.	☐	☐	☐	☐	☐
13. Update antivirus software regularly.	☐	☐	☐	☐	☐
14. Setting controls for data confidentiality, encryption, and accessibility only by authorized persons.	☐	☐	☐	☐	☐
15. Data transfer from one location to another is done over secure, unhackable transmission channels.	☐	☐	☐	☐	☐

The Second Axis: The Role of the Oversight Exercised by the Central Agency for Financial Control Over Information Systems in Reducing Cybersecurity Risks in the Government Sector:

When evaluating the oversight exercised by the Central Agency for Financial Control over information systems, what is the degree of your agreement with the following statements?

Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1. Ensures that information systems are able to provide appropriate evidence for the audit process.	☐	☐	☐	☐	☐
2. Evaluates and monitors the extent of the entity subject to oversight's commitment to providing appropriate procedures related to data security and preserving it from damage or distortion.	☐	☐	☐	☐	☐
3. Ensures the effective use of firewalls and antivirus programs to protect systems from the introduction of malicious software or unauthorized access.	☐	☐	☐	☐	☐
4. Ensures the effective use of encryption, including maintaining confidentiality and security when sending data and information over the network and preventing misuse through encryption technology.	☐	☐	☐	☐	☐
5. Monitors the compliance of the entities subject to supervision in processing data in accordance with applicable laws and regulations and compliance with special legislation.	☐	☐	☐	☐	☐
6. Ensures the ability to retrieve operational documents from electronic document files, such as documents stored online or in cybersecurity systems.	☐	☐	☐	☐	☐
7. Grants the inspector the authority to view all information in the database and audit the database to ensure the integrity of the electronic outputs.	☐	☐	☐	☐	☐
8. Ensures there is no duplication or repetition by taking a sample and calculating it manually to obtain a single result.	☐	☐	☐	☐	☐

Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
9. Ensures the validity of protection devices and conducts periodic checks, such as fire protection devices.	☐	☐	☐	☐	☐
10. Ensures that the audited entity conducts a comprehensive inventory of all information systems equipment.	☐	☐	☐	☐	☐
11. Ensures that systems and procedures are in place to address detected errors and deviations.	☐	☐	☐	☐	☐
12. Ensures that business continuity plans and disaster recovery procedures are in place and effective.	☐	☐	☐	☐	☐
13. Ensures that critical operations are authorized by two or more employees according to their authority levels.	☐	☐	☐	☐	☐