ISSN:2336-2693 | E-ISSN:2336-4890

# THE IMPACT OF CYBER SECURITY GOVERNANCE IN REDUCING THE RISKS OF ELECTRONIC AUDITING IN JORDANIAN COMMERCIAL BANKS

**Dr. Othman Hussein Othman Othman**
Isra University

**Dr.Mohanad Fayiz**
Al-dweikat, Isra University

**Abstract:**
This study aimed to identify the impact of cybersecurity governance in reducing the risks of electronic auditing. The study population included Jordanian commercial banks. As for the sample, it consisted of (77) respondents who obtained a chartered accountant certificate and worked in the field of auditing the accounts of Jordanian commercial banks. The study followed the descriptive and analytical approach. The study concluded that there is an impact of cybersecurity governance in reducing the risks of electronic auditing in Jordanian commercial banks. A high level of approval was found on the importance of the three criteria (cybersecurity governance strategy, cybersecurity related to human resources, and cybersecurity risk management) in reducing the risks of electronic auditing in Jordanian commercial banks. The study recommended the necessity of auditing the cybersecurity governance strategy or management interview to determine the resource requirements and the method by which they are identified and approved.

Key words: cybersecurity governance, electronic audit risks, Jordanian commercial banks

## Introduction:

The concept of information technology governance and cybersecurity is one of the most prominent concepts introduced by the information revolution and the Internet into the operations of organizations, which emerged as a result of developments in cyber risk technology resulting from the possibility of threats and risks in the information technology environment in which it operates. It is a term that expresses the radical shift in the concepts concerned with providing the means, policies, instructions and practices related to the protection of information.

Cybersecurity governance requires increased capabilities to provide adequate protection for the information that business organizations possess from cyber threats and risks that exist in cyberspace. Therefore, the perspective of cybersecurity governance is the procedures and arrangements related to the use of technology that help secure that protection, given that this type of governance is the future, as many organizations strive to implement cyber risk management that they are likely to be exposed to.

The impact of the use of information technology and cyberspace on the financial and accounting systems and the process of electronic auditing in business organizations resulted in the mandatory entry of this space in the performance of various types of operations. Concepts related to cybersecurity governance emerged that guide, direct and regulate methods of dealing with financial and accounting systems when demonstrating business results in the IT environment.

This study seeks to know the impact of cybersecurity governance in reducing the risks of electronic auditing in Jordanian commercial banks from the point of view of the certified

ISSN:2336-2693 | E-ISSN:2336-4890

chartered accountant, and the consequent support for their contribution to maximizing the value achieved by these banks' practice of their activities. This requires the need to enhance the electronic audit process, and the skills and capabilities of those in charge of it, to provide sufficient assurance to convince the management of the importance and effectiveness of this new concept in the IT environment, and then motivate it to support it.

**The study problem and its questions:**

The increasing work in information technology and the spread of electronic services in cyberspace has led to more risks and threats. The use of this space also caused a revolution in the world of communications, which contributed greatly to increasing the risks and threats that Jordanian banks could be exposed to when carrying out electronic audits of their data included in their financial statements, in a more efficient manner than the usual methods of traditional auditing.

Here lies the problem of this study, as this technological challenge in cyberspace requires that Jordanian commercial banks face it through cybersecurity governance, as it is an effective tool that provides the required protection from attacks that may be exposed to in this space. It has greatly affected the sphere of integration and harmony with the development of information and communication technologies and their legal requirements, especially since cyber-attacks target financial and banking institutions as an attractive target for these complex programs. Therefore, the following question was raised: What is the effect of cybersecurity governance standards in reducing the risks of electronic auditing in Jordanian commercial banks from the point of view of the certified public accountant? And branched out from a number of questions are as follows:

***The first question***: What is the impact of the cybersecurity governance strategy in reducing the risks of electronic auditing in Jordanian commercial banks from the viewpoint of the certified public accountant?

***The second question***: What is the impact of cybersecurity related to human resources in reducing the risks of electronic auditing in Jordanian commercial banks from the point of view of the certified public accountant?

***The third question***: What is the effect of cybersecurity risk management on reducing the risks of electronic auditing in Jordanian commercial banks from the viewpoint of the certified public accountant?

**The importance of study:**

***First***: The theoretical importance: The theoretical importance of this study lies in the fact that it is considered one of the first accounting studies that dealt with the governance of cybersecurity from the point of view of the certified chartered accountant and its effect in reducing the risks of electronic auditing in Jordanian commercial banks from the point of view of the certified public accountant, as the banking sector It is considered one of the important sectors in the Jordanian national economy. This study also comes at a time when Jordanian commercial banks may need to raise awareness of the importance of cybersecurity governance, and thus identify its importance in the practical application of concepts related to this type of governance.

***Second***: Practical importance: This importance comes from the possibility that the Jordanian commercial banks researched could benefit from their findings in a way that helps them

 ISSN:2336-2693 | E-ISSN:2336-4890

implement cybersecurity governance. Also, this study derives its importance from the fact that its results benefit the financial managers and accountants working in Jordanian commercial banks by introducing them to the importance of cybersecurity governance. It also provides an important and contemporary reference that may push many researchers to conduct more new research in this field, through the theoretical literature, previous studies and research tools that have been verified for their validity and stability that can be employed and used in future studies.

**Objectives of the study:**

1- Recognizing the impact of the cybersecurity governance strategy in reducing the risks of electronic auditing in Jordanian commercial banks from the point of view of the certified public accountant.

2- Recognizing the impact of cybersecurity related to human resources in reducing the risks of electronic auditing in Jordanian commercial banks from the point of view of the certified public accountant.

3- Recognizing the impact of cybersecurity risk management in reducing the risks of electronic auditing in Jordanian commercial banks from the viewpoint of the certified public accountant.

**Hypotheses of the study:**

The researcher adopted the following main hypothesis, which reads: There is no statistically significant effect of cybersecurity governance standards in reducing the risks of electronic auditing in Jordanian commercial banks from the point of view of the certified public accountant. The following hypotheses are divided into:

***The first hypothesis***: There is no statistically significant impact of the cybersecurity governance strategy in reducing the risks of electronic auditing in Jordanian commercial banks from the point of view of the certified public accountant.

***The second hypothesis***: There is no statistically significant effect of cybersecurity related to human resources in reducing the risks of electronic auditing in Jordanian commercial banks from the point of view of the certified public accountant.

***The third hypothesis***: There is no statistically significant effect of managing cybersecurity risks in reducing the risks of electronic auditing in Jordanian commercial banks from the point of view of the certified public accountant.

**Model of the study:**

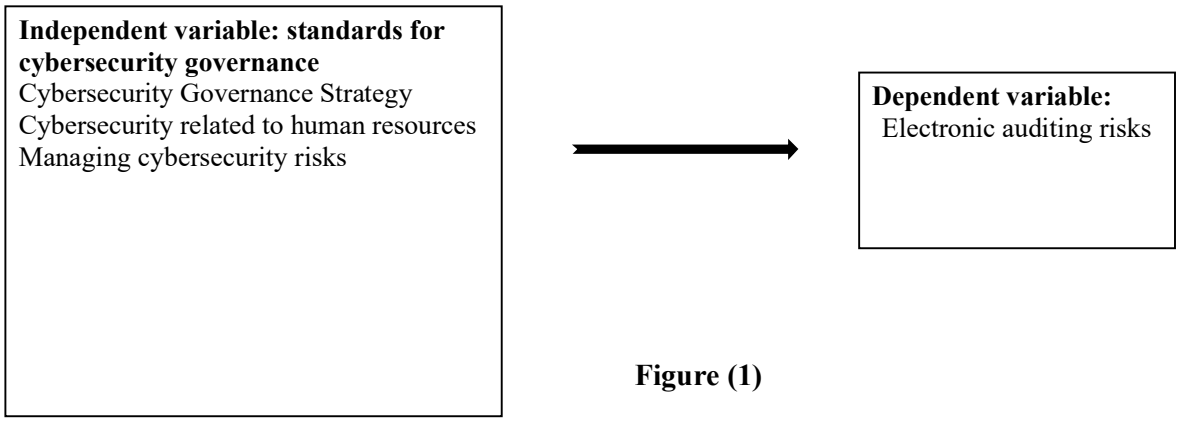


**Figure (1)**

 ISSN:2336-2693 | E-ISSN:2336-4890

Source: The form was prepared by the researcher based on the criteria contained in the instructions for adapting to cyber risks issued by the Central Bank of Jordan in 2018 for auditing cyber risks in information technology.

**Terms of the study:**

Cybersecurity: Maintaining the confidentiality of data and information owned by the bank and its assets, and their integrity within the cyberspace from cyber threats and risks. And that is through the bank providing the means, policies, instructions and practices related to protecting the bank's information (Manual of Instructions for Adaptation to Traffic Risks issued by the Central Bank of Jordan in 2018).

Cybersecurity governance: the arrangements and processes that departments and divisions in the bank establish and their approach to follow. Also, these arrangements and processes are continuously reviewed to implement the management of cyber risks arising from the potential for threats and risks in the information technology environment in which the bank operates (Abu Shanab et al., 2019). It was measured through a number of variables contained in the instructions for adapting to cyber risks issued by the Central Bank of Jordan in 2018 to audit cyber risks in information technology, namely:

1- Cyber Security Governance Strategy: It means giving adequate opportunity to Jordanian commercial banks to implement all measures related to cybersecurity governance with the required speed and accuracy, and clarifying it to the beneficiaries to achieve the maximum benefit from the implementation of this strategy in a way that enables it to be effective and distinct.

2- Cybersecurity related to human resources: it means the types of qualified and trained employees in the field of information technology in Jordanian commercial banks, workers specialized in implementing data collection and analysis operations, program designers, equipment and equipment operators and maintenance workers.

3- Managing cybersecurity risks: it means that Jordanian commercial banks maintain the security of information on the electronic network, and provide protection and maintain the privacy and confidentiality of information from the risks that threaten them or attack them.

The Certified Public Accountant (CPA) is a certification designed by the Institute of Certified Public Accountants in the United States (AICPA) that works to define the scientific content of the certification curriculum. It also recognizes and approves the various curricula issued by publishers and organizes and coordinates the examinations with testing centers all over the United States of America, to give the status of global professional accreditation to those working in the field (Al-Harb, 2015, p.13)

The Cyber Risk Adaptation Instructions Manual: It is a guide issued by the Central Bank of Jordan in 2018 to audit cyber risks in information technology, and aims to provide licensed banks, financial institutions, credit information companies and microfinance companies that are directly subject to the supervision and control of the Central Bank of Jordan. This guide includes a comprehensive and detailed explanation of all areas that banks need when conducting their business in the IT environment.

**The limits of the study:**

1- Temporal limits: The study was completed during the period between (1-12-2020 until 2-15-2021).

2- Spatial limits: Jordanian commercial banks.

3- Human limits: Jordanian certified accountants in auditing the accounts of Jordanian banks.

## The theoretical framework

### Cybersecurity governance:

The degree of organizations 'commitment to implementing the general framework for information technology governance has become one of the most important basic criteria that investors take into account when making their investment decisions, especially in light of economic globalization and intense competition between different organizations to enter financial markets, whether local or global, for investment (Solomon et al, 2013, p: 236).

Hence, organizations that implement IT governance and cybersecurity governance have a competitive advantage to attract capital over those that do not, and their ability to compete in the long term increases. And that is through the transparency that these organizations enjoy in their transactions, accounting and financial auditing procedures, and in all operations of the organization, in a way that supports the confidence of investors, whether local or international, to invest in these organizations. This may lead to a reduction in the cost of capital, as it may result in the end. On achieving greater stability of funding sources (Freeland, 2018, p: 15).

The researcher believes that cybersecurity governance means reviewing the processes related to implementing cyber risk management resulting from the possibility of risks occurring in the information technology environment in which Jordanian commercial banks operate. Thus achieving justice and transparency, granting the right to accountability, and the necessary protection for owners, shareholders, shareholders, and workers' interests, as well as limiting the exploitation of power in other than the public interest, in a manner that leads to the development and development of investments, encouraging their flows, developing savings, maximizing profitability, and providing new job opportunities, . These norms and rules also emphasize the importance of these banks 'commitment to the provisions of the law, and work to ensure a review of financial performance, and the existence of administrative structures that enable management to be held accountable to shareholders.

The following is a review of the three standards related to the general work of cybersecurity governance contained in the instructions for adapting to cyber risks issued by the Central Bank of Jordan in 2018 for auditing cyber risks in information technology, which were adopted as independent variables in the current study, as the existence of these frameworks in security governance The cyber and organizational structure contributes to laying the appropriate foundations and standards for measuring success. This helps the Board of Directors to perform the tasks and responsibilities assigned to them at the level of planning for e-services in the virtual space, leading to the implementation of these tasks and responsibilities, publishing them, measuring the success rate of these services, and achieving maximum satisfaction among the target audience. The following is an overview:

### First: Cybersecurity Governance Strategy:

The use of information technology gives sufficient opportunity to implement governance procedures with the required speed and accuracy, and organizations' use of information technology enables them to be effective and distinguished. It is supposed to define a distinct group of information technology that is unique to it to form competitive advantages that contribute to achieving high performance results. Hence, the business technology strategy imposed a new reality as a result of the adoption of the activities and transactions of organizations on this

ISSN:2336-2693 | E-ISSN:2336-4890

technology, which led to the need to keep pace with this development, and the importance of changing their methods. The traditional methods are developed based on modern technological methods and advanced analytical methods to implement business efficiently and effectively (Deloitte, 2015, p: 4).

The success in implementing a cybersecurity strategy related to providing electronic services is ensured, and after those services are subjected to examining the information effort, this strategy is launched and announced on the Internet. It is worth noting that departments cannot implement a cybersecurity governance strategy and any electronic services on their portal without the department's approval for that, because this would enhance the efficiency and accuracy of performance, reduce the time and cost required to complete transactions, ensure integration and coordination between the various departments and departments and reach better efficiency, transparency and performance. (Al-Muhtadi, 2020, p. 28).

The researcher believes that the strategy of cybersecurity governance means providing electronic services and is clarified to the beneficiaries and employers to enable them to achieve maximum benefit from the implementation of the cybersecurity governance strategy, and to indicate the extent of the ability to exploit the opportunities available to them in the external environment to obtain their needs from scarce resources of value for their continuation in performing its tasks and activities to achieve its planned goals and objectives. In addition, the cybersecurity governance strategy is explained from a technical point of view in order to enable those in charge of developing electronic services to make good use of these services within their approved software. After that, it becomes possible to prepare the technical guide for the short guide for the beneficiaries of the implementation of the cybersecurity governance strategy and its related services, which must be done easily and securely due to the presence of transparency to track performance and provide information to the decision maker.

**Second: Cybersecurity related to human resources:**

This framework is represented by the types of human resources qualified and trained in the field of information technology who are able to deal with cybersecurity risks, workers specialized in the implementation of data collection and analysis operations, program designers, device operators and equipment and maintenance workers, whether related to software maintenance or hardware maintenance. Information, communication technology and cybersecurity depend heavily on human thought, which gives it great importance in developing human resources and building the so-called intellectual capital that is adaptable to changes, circumstances and advanced technology (Zahlan, 2019, p. 255).

Freeland (2018, p: 18) believes that the importance of human resources in information technology increases with the increase in the information available to the organization in making a specific decision, which requires it to pay attention to an important and major aspect in how to convert this enormous information into knowledge and determine where and when to use it. This, in turn, requires advanced information technology that allows it to be logically coherent. This framework also ensured that the Board of Directors would seek the assistance of some qualified and adequately trained personnel in information technology to perform some tasks and responsibilities such as: Government Procedures Engineer, Electronic Services Programming Expert, Web Services Security and Confidentiality Expert, Human and Financial Resources Systems Expert, and the Electronic Mediator Expert.

The researcher believes that cybersecurity related to human resources means that Jordanian

ISSN:2336-2693 | E-ISSN:2336-4890

commercial banks provide human resources and manpower in information technology who are able to use electronic systems, so that they have sufficient skill in using computer equipment and software in order to perform the specific tasks and duties assigned to them, since information and communication technology is widely adopted. Great for this resource.

Third: Cyber Security Risk Management:

Managing cybersecurity risks requires maintaining the security of information on the network. The user needs a special account to access the network, so no one is allowed to access the network unless the user enters the account name and private password in order to be allowed to use the organizations 'data. Consequently, the failure to guarantee the preservation of the privacy of the information and data available within the electronic network, the fear of leakage of information that the owner does not wish to inform others about, and the lack of programs to encrypt the information necessary to transfer it in order to maintain the necessary security and confidentiality are all risks that prevent the application of cybersecurity governance, in addition The limited modernization and development in issuing and disseminating laws, regulations, instructions and procedures used (Al-Muhtadi, 2020, p. 124).

The strategy of managing cybersecurity risks is the means that use information technology that prevents breaches of the accounting system on the Internet, by providing protection and preserving the privacy and confidentiality of information from threats or attacks on it. And that by providing the tools and means necessary to be provided to protect information from internal or external risks, as information security is of great importance because the user needs a special account in order to access the Internet, as he is not allowed to enter the network and is not allowed to use private data In organizations without entering their account name and password (Laudon and Laudon, 2018, p: 88).

The researcher believes that there are aspects that require study and research in managing cybersecurity risks in light of the use of the Internet, and the existence of a set of methods to penetrate the information system. In addition to violating the intellectual rights of individuals and organizations in the electronic world, one of the aspects of information security is the confidentiality and integrity of information, ensuring its survival and not deleting or destroying it.

The concept of electronic auditing

Electronic audit is defined as the process of collecting and evaluating to determine whether the use of the computer contributes to protecting the company's assets, supports the integrity of its data, and effectively achieves its objectives. It uses its resources efficiently to assist the auditor in planning, controlling, and documenting audit work with the means and methods used by management for the purpose of verifying the effectiveness of internal control using information technologies (Al-Omair, 2018, p.30).

Electronic auditing is also defined as that process based on the use of information technologies in order to assist the auditor in planning the audit process, and in a manner that gives the auditor sufficient opportunity to carry out all procedures related to auditing quickly and accurately in a manner that helps the auditor to reach the highest efficiency (Al-Khasawneh, 2013, p.6).

The researcher believes that electronic data auditing is a process carried out by Jordanian commercial banks to exploit modern technology to ensure that financial data have been correctly entered, processed and reported, in a manner that enhances and supports the internal

ISSN:2336-2693 | E-ISSN:2336-4890

audit function in the internal control processes of financial operations and the management of risks associated with them.

**Electronic auditing risks:**

The use of information technologies entails many risks to the audit process, perhaps the most prominent of which are:

1- The use of computers in auditing requires the availability of expertise and skills of the body that conducts the audit process, starting from the planning stage, which may require the use of experts and specialized skills from outside the audit office, in addition to the risks related to the infrastructure that must be provided when using Information technologies such as non-compliance with security and privacy measures (Al-Khalidi, 2015, p. 290).

2- The use of the computer leads to the compilation of all records and data used during the operation process and makes them subject to the control of one operator during the operation process, as this control affects the audit results and leads to the loss of the human element of the ability to trade the financial data and documents related to it, and this leads to the absence The insightful vision, which is often an important factor in discovering mistakes (Al-Khasawneh, 2013, pp. 7-8).

3 - The need to deal with a large amount of financial transactions using the computer during a short period of time, which results from this need the use of automated information systems and arises from it many difficulties facing the electronic audit process for these operations, including failure to process ready-made financial transactions within the required time period and errors caused by the system Ineffective censorship and loss of data due to system failure (Al-Omair, 2018, p.33).

4- Risks related to the necessary applications of information technology, such as insufficient controls over input, processing and output of information, inadequate procedures for securing software security, and the increasing influence of information systems analysts and system software developers. This affects the possibility of conducting monitoring and evaluation processes related to the operating programs of these systems, and the risks related to the environment surrounding the operation of the computerized accounting system, which are the risks that arise due to the environment that represents a defect in the computers used in the application of the system and the programs used in its application. The Basel Committee on Banking Supervision indicated that policies and procedures should be developed to allow risk management to assess these risks, control them and continuously monitor them (Al-Khasawneh, 2013, p. 8).

**Previous studies:**

The study of Nassour (2015) aimed to identify the impact of information technology governance on the quality of financial reports. The field study was conducted in the Syrian banking sector, and it was based on the design of a questionnaire that was distributed to workers in Syrian banks. It was found that there is an impact of information technology governance at the level of its application in these banks collectively, and on the quality of the financial reports prepared in these banks. The study recommended the necessity of applying a model for controlling information technology in the banks under study, and for it to be a tool for preparing financial statements and reports, in a way that reflects positively on the reliability of this

ISSN:2336-2693 | E-ISSN:2336-4890

information.

The study of (Gary, 2016) aimed to demonstrate the importance of controlling information technology and maintaining the security of this technology in light of the risks surrounding this information. The study showed that less than 25% of the organizations that practically conducted the study suffer from several risks related to reasons related to external risks represented by the rules and principles that practically built the organization, which gave a good opportunity for the widespread use of external resources for information technology. The study recommended the necessity of creating information technology governance legislation to alleviate the concerns of investors, users, organizations and customers about the security and confidentiality of information in organizations.

Al-Maghrabi's study, (2018) aimed to identify the influential role of information security governance in reducing the risks of accounting information systems, through a field study of Egyptian companies and banks operating in the virtual village. A survey list was used to collect information from the study sample, which amounted to (125) financial managers and accountants working in Egyptian companies. And it has been shown that the application of information security governance standards has an impact on reducing the risks of accounting information systems. And it has been shown that there are a number of risks to which electronic accounting information systems are exposed, including external risks as a result of threats in the electronic business environment. The study recommended that Egyptian companies and banks operating in the virtual village should pay attention to preparing guides for information technology and pay attention to modern methods of measuring and evaluating the company's performance.

The study of (Wali & Bahl, 2019) aimed to clarify the perceptions of those in charge of providing software services related to information technology security governance and its impact on the quality of service and the security of information provided by companies to clients benefiting from their services. The study was conducted on a sample of (300) respondents. The study showed that companies that provide IT outsourcing services in India and that provide software services have an important and essential impact on the quality of service and the security of information that can be predicted. It was also found that there is a positive impact relationship for the elements of information technology security governance and the quality of information security services. It recommended the necessity of organizing training courses on how to create software services related to information technology security governance due to its impact on the quality of service and the security of information provided by companies to clients benefiting from their services in India.

The study of (Slupska, 2020) dealt with cybersecurity governance as one of the terms used in describing and understanding new technologies that require adherence to ethics and provide adequate protection for the information that organizations possess from cyber threats and risks present in cyberspace. This study is considered one of the descriptive theoretical studies that talked about the governance of cybersecurity, which carries a set of assumptions about the roles and moral obligations to deal with the problems of cybersecurity called the metaphor of electronic warfare that reduces the possibilities of international cooperation in this field by limiting countries to take response policies Act and take proactive action to address the features and characteristics of financial systems in cyberspace. The study recommended the use of alternative metaphors such as health, ecosystem, and architecture that could help provide more cooperation and apply a precise conceptual framework for negotiations to implement the management of cyber risks to

ISSN:2336-2693 | E-ISSN:2336-4890

which they are likely to be exposed.

**What distinguishes the current study from previous studies?**

It is noted through the survey of previous studies, with the exception of the study (Slupska, 2020) that dealt with cybersecurity governance that it dealt with many issues, which focused mostly on many aspects of governance and the important factors of information technology security governance and influencing the publication of financial reports over the Internet in general. Its fields also varied between focusing on examining and demonstrating the comprehensiveness of presenting financial reports on the Internet with knowledge of the influence of a group of factors and characteristics that affect other factors, for example the impact of governance on other financial phenomena. While the current study is distinguished in terms of:

1- Variables: The current study deals with an important aspect of cybersecurity governance standards, namely (cybersecurity governance strategy, cybersecurity related to human resources, management of cybersecurity risks) in reducing the risks of electronic auditing in Jordanian commercial banks, from the viewpoint of the sample. Due to the lack of studies on this topic specifically (cybersecurity governance), this study is a modest contribution to achieving a scientific addition in this field.

2- Objective: Most of the previous studies focused on identifying the general framework of concepts related to e-governance and information technology governance, while the current study attempted to clarify the concepts and aspects related to cybersecurity governance and the risks of electronic auditing as modern concepts that emerged with the great development that occurred in information technology and cyberspace. .

3- Society: This study chose the community of (Jordanian commercial banks) due to the importance of these banks for the Jordanian national economy, as these banks are considered one of the main tributaries of the Jordanian national economy. They also have a great impact on economic and social development, are distinguished by their large size and possess large financial and material assets.

**Study Approach:**

This study is based on the descriptive and analytical approach, as the researcher used a field survey of the study population consisting of Jordanian commercial banks. The inspection unit was chosen from among the Jordanian certified accountants in Jordan who work in the field of auditing the accounts of Jordanian banks in Jordan, whether he is an internal or external auditor of the bank. A questionnaire was designed for this purpose. The descriptive approach was used to deal with and classify the data to describe the phenomenon and the researched community, and the analytical part of it to obtain the results of testing the study hypotheses and arrive at the results through which recommendations can be made.

**Study population and sample:**

The study population includes all Jordanian certified accountants in Jordan. As for the study sample, it was selected from auditors who hold a certified accountant certificate and works in the field of auditing the accounts of Jordanian commercial banks, whether he is an internal or external auditor of the bank as the researcher selected a purposeful sample representing this community in the banks under study. The questionnaires were distributed to them via e-mail because they were inaccessible due to the Corona pandemic, as (100) questionnaires were distributed, and (77) questionnaires were retrieved, representing (77%) of the total number of questionnaires sent,

ISSN:2336-2693 | E-ISSN:2336-4890

which were subjected to statistical analysis.

**Study instrument:**

The researcher reviewed a number of previous studies and literature related to the subject of the study to design a questionnaire that included phrases related to the standards of cybersecurity governance and the risks of electronic auditing. The researcher used the five-point Likert scale: strongly agree (5 points), agree (4 degrees), agree with an average degree (3 degrees), disagree (two points), and strongly disagree (one score). As for the limits adopted by this study when commenting on the arithmetic mean, the researcher has identified three levels (weak, medium, and high) based on the statistical equations related to this aspect.

**Validate the study instrument:**

The researcher conducted a validity test with the aim of ensuring the reliability of the study tool and confidence in its results by presenting the questionnaire to a group of arbitrators, university professors and experts in accounting and statistics to judge the extent of its apparent and logical validity and its validity as a tool for data collection.

**Reliability of the study instrument:**

To ensure the validity of the questionnaire as a tool for collecting the necessary data for the study, the coefficient (Cronbach-Alpha) was used for the internal consistency of the statements of the questionnaire as a whole. It reached (91.8%), which is an appropriate and high reliability rate.

**Data collection methods:**

In this study, two types of information sources were relied on, namely, primary sources and secondary sources, as follows:

First: Primary data: These are data that the researcher relied on through designing a questionnaire that was developed to serve the subject of the study.

Second: Secondary data: These are data obtained from libraries, scientific materials, specialized periodicals, publications and university theses that discuss cyber security governance and the risks of electronic auditing.

**Statistical treatment:**

1- The arithmetic *a*verages, standard deviations, importance and rank were calculated to answer the study questions, and it is related to the degree of the study sample responses to the statements of the questionnaire.

2- Multiple and simple linear regression analysis was used in order to test the effect of all independent variables together and separately on the dependent variable, which is the risks of electronic auditing.

**Field study results**

**First: Descriptive statistics results:**

**1- Results of descriptive statistics for cybersecurity governance strategy questions**

Table (1): Arithmetic means, standard deviations, and the relative importance of a cybersecurity governance strategy

ISSN:2336-2693 | E-ISSN:2336-4890

| No | Statements | Mean | S.D | Level | Rank |
|---|---|---|---|---|---|
| 1 | The bank considers from time to time the development of performance indicators for the cybersecurity governance strategy | 3.706 | .7310 | High | 7 |
| 2 | A cybersecurity governance strategy or management interview is audited to determine resource requirements and the manner in which they are identified and approved. | 3.586 | .7183 | Medium | 10 |
| 3 | The bank takes care to communicate the cybersecurity governance strategy to the departments that ensure the effectiveness of operations | 3.733 | .6224 | High | 6 |
| 4 | The Bank's management is reviewing the minutes of the meetings of the Periodic Organizational Steering Committee for the Cybersecurity Governance Strategy | 3.626 | .8506 | Medium | 9 |
| 5 | The bank is developing a cybersecurity governance strategy in line with its objectives and requirements | 3.946 | .6344 | High | 1 |
| 6 | The bank's management seeks to develop and develop cybersecurity applications | 3.800 | .6576 | High | 4 |
| 7 | The bank is keen to increase cybersecurity capabilities, attract inventions and innovations, and communicate their benefits | 3.893 | .6487 | High | 2 |
| 8 | The systems that support the cybersecurity business strategy are developed and operated | 3.786 | .7586 | High | 5 |
| 9 | The bank has an information technology plan through which the cybersecurity governance strategy is developed, approved, applied and updated | 3.853 | .7107 | High | 3 |
| 10 | The bank is keen to develop the means, methods and processes | 3.706 | .7310 | High | 7 |

 ISSN:2336-2693 | E-ISSN:2336-4890

| No | Statements | Mean | S.D | Level | Rank |
|---|---|---|---|---|---|
| | associated with the cybersecurity governance strategy and related systems | | | | |
| **Cybersecurity governance** | | | **3.770** | | High |

It appears that the responses of the respondents to the statements of the cybersecurity governance strategy and the meansrelated to them came at a high level, as the arithmetic mean reached (3.770). And it ranged between (3.946) and (3.586). The statement "The bank shall develop a cybersecurity governance strategy in line with its objectives and requirements" came first, with an average of (3.946), and a standard deviation of (.63445). The statement which states that "the cybersecurity governance strategy or management interview is audited to determine the resource requirements and the method by which they are defined and approved" came last, with an arithmetic mean of (3.586) and a standard deviation of (.7183). As for the standard deviations, it is noted that they are low, and they indicate that the answers of the study sample are close and similar to a large extent.

**2- Results of descriptive statistics of cybersecurity questions related to human resources**

Table (2): Arithmetic means, standard deviations, and the relative importance of cybersecurity related to human resources

| No | Statements | Mean | S.D | Level | Rank |
|---|---|---|---|---|---|
| 11 | Cybersecurity policies are audited to ensure that they require identifying their current and future needs regarding employees | 3.706 | | High | |
| 12 | The cybersecurity strategic plan is audited to ensure that it includes the requirements of people and resources for current and future needs | 3.506 | | Medium | |
| 13 | Bank management interviews human resources managers to evaluate the mechanism of action of important positions in cases of emergency or long absence | 3.586 | | Medium | |
| 14 | Quality Assurance members are appointed to keep an eye on their work to ensure compliance with policies and procedures related to cybersecurity | 3.733 | | High | |
| 15 | The cybersecurity policy related to human resources is audited to ensure that competency and training | 3.626 | | Medium | |

 ISSN:2336-2693 | E-ISSN:2336-4890

| No | Statements | Mean | S.D | Level | Rank |
|---|---|---|---|---|---|
| | requirements are defined for existing and new employees | | | | |
| 16 | The bank's management is keen on recruiting employees and ensuring that the important aspects of cybersecurity work are presented | 3.936 | | High | |
| 17 | Email and other means are audited to ensure that policies are distributed to employees as they are updated | 3.813 | | High | |
| 18 | Recruitment and training plans are audited to ensure that they reflect the Bank's specific needs | 3.903 | | High | |
| 19 | Policies related to human resources are audited to ensure that they are approved and up-to-date in the context of cybersecurity | 3.786 | | High | |
| 20 | The core training materials through which cybersecurity policies and procedures are communicated to employees are audited | 3.866 | | High | |
| **Cybersecurity related to human resources** | | **3.743** | | | High |

It appears that the responses of the respondents to the articles related to cybersecurity related to human resources and the meansrelated to them came at a high level, as the general arithmetic mean reached (3.743) and ranged between (3.936) and (3.5067). The statement “The bank’s management is keen on recruiting employees and ensuring that the important aspects of cybersecurity are presented” came first, with an arithmetic mean (3.936) and a standard deviation of (.6344). The statement which states that "the strategic cybersecurity plan is audited to ensure that it includes the requirements of people and resources for current and future needs" ranked last, with an arithmetic mean of (3.506) and a standard deviation of (.8442). As for the standard deviations, it is noted that they are low, and they indicate that the answers of the study sample are close and similar to a large extent.

**3- Results of descriptive statistics of cybersecurity risk management questions**

Table (3): The arithmetic means, standard deviations, and the relative importance of managing cybersecurity risks

| No | Statements | Mean | S.D | Level | Rank |
|---|---|---|---|---|---|
| 21 | The bank monitors cybersecurity risks and resources effectively during the achievement of IT goals | 3.653 | .7069 | High | 9 |
| 22 | Training or publication mechanisms such as email, notes, notes are | 3.720 | .6889 | Medium | 7 |

 ISSN:2336-2693 | E-ISSN:2336-4890

| No | Statements | Mean | S.D | Level | Rank |
|---|---|---|---|---|---|
| | scrutinized to ensure that issues related to non-compliance with cybersecurity governance are mentioned. | | | | |
| 23 | The cybersecurity risk management plan or other documentation is audited to ensure that risk management responsibilities are clearly defined | 3.573 | .7198 | High | 10 |
| 24 | Documentation is audited to ensure that cybersecurity risks are part of the overall IT governance framework | 3.746 | .5948 | High | 6 |
| 25 | People responsible for cybersecurity risks are interviewed to determine whether they are adequately costed and appropriate resources provided | 3.706 | .8506 | High | 8 |
| 26 | The Bank's management exercises its supervisory and supervisory role when identifying and measuring cybersecurity risks and developing alternative strategies to face them | 4.000 | .5452 | High | 1 |
| 27 | Documentation is audited to ensure that cybersecurity risks are part of the IT governance framework | 3.853 | .6716 | High | 4 |
| 28 | The bank uses external consultants who are specialized in managing cybersecurity risks | 3.893 | .6487 | High | 2 |
| 29 | Meeting minutes are audited to ensure that new cybersecurity risks are added and analyzed appropriately | 3.813 | .7831 | High | 5 |
| 30 | The extent of adherence to the strategies and policies of cybersecurity risk management in the bank is monitored by the Steering Committee | 3.880 | .7158 | High | 3 |
| **Cybersecurity risk management** | | **3.784** | | | High |

It appears that the responses of the respondents to the items of cybersecurity risk management and the means related to them came at a high level, as the arithmetic mean was (3.784). And it ranged between (4.000) and (3.573). The statement “The bank’s management exercises its supervisory and supervisory role when identifying and measuring cyber security

 ISSN:2336-2693 | E-ISSN:2336-4890

risks and developing alternative strategies to confront them" came in first place with an arithmetic mean of (4,000) and a standard deviation of (.5452). The statement which states that "the cybersecurity risk management plan or any other documents is audited to ensure that the responsibilities for risk management have been clearly defined" came last, with an arithmetic mean of (3.573) and a standard deviation of (.7198). As for the standard deviations, it is noted that they are low, and they indicate that the answers of the study sample are close and similar to a large extent.

**4- Results of descriptive statistics of dependent variable questions: Electronic auditing risks:**

Table (4): The arithmetic means, standard deviations, and the relative importance of electronic auditing risks

| No | Statements | Mean | S.D | Level | Rank |
|---|---|---|---|---|---|
| 31 | Cybersecurity governance provides management with ongoing information to better plan and implement the audit process | 3.516 | .8397 | Medium | 9 |
| 32 | Cybersecurity governance assists in achieving quality in the audit process | 3.333 | .6644 | Medium | 10 |
| 33 | Cybersecurity governance reduces the cost of storing business paperwork | 3.853 | .6083 | High | 3 |
| 34 | Cybersecurity governance gives adequate opportunity to implement all audit procedures quickly and accurately | 3.813 | .7295 | High | 5 |
| 35 | Cybersecurity governance contributes to safeguarding assets and ensures the integrity of financial data | 3.951 | .4932 | High | 1 |
| 36 | Cybersecurity governance enhances the opportunity to carry out an independent and objective audit mission | 3.693 | .6773 | High | 7 |
| 37 | Cybersecurity governance helps an auditor uncover fraud and fraud | 3.853 | .5621 | High | 3 |
| 38 | Cybersecurity governance helps analyze assets, fixed assets, and account balances | 3.893 | .7273 | High | 2 |
| 39 | Cybersecurity governance helps coordinate audit outputs and complete reports in a timely | 3.760 | .6943 | High | 6 |

 ISSN:2336-2693 | E-ISSN:2336-4890

| No | Statements | Mean | S.D | Level | Rank |
|---|---|---|---|---|---|
| | manner | | | | |
| 40 | Cybersecurity governance helps secure the opportunity for creativity and initiative for the auditor when performing the audit task | 3.623 | .6876 | Medium | 8 |
| **The dependent variable: the risks of electronic auditing** | | **3.728** | | | **High** |

It appears that the answers of the study sample members for the statements related to the dependent variable: the risks of electronic auditing and the meansrelated to them, came at a high level, as the arithmetic mean reached (3.728). And it ranged between (3,951) and (3,333). The statement "Cyber security governance contributes to protecting assets and ensuring the integrity of financial data" came in first place with an arithmetic mean (3.951) and a standard deviation of (.4932). The statement which states that "cybersecurity governance helps achieve quality in the audit process" ranked last, with an arithmetic mean of (3,333) and a standard deviation of (.6644). As for the standard deviations, it is noted that they are low, and they indicate that the answers of the study sample are close and similar to a large extent.

**Second: testing hypotheses:**

The main hypothesis states that: There is no statistically significant effect of cybersecurity governance standards in reducing the risks of electronic auditing in Jordanian commercial banks from the point of view of the certified public accountant. To test the hypothesis, multiple linear regression analysis (Multiple Regression) was used to find out this effect, as the results contained in Table (5) show the following:

Table (5): Multiple Regression Analysis of the Impact of Cybersecurity Governance Standards on Reducing the Risks of Electronic Auditing

| (R)= 998 , (R2)= 996, (Adj R2)= 424 | | | | | |
|---|---|---|---|---|---|
| تحليل التباين (ANOVA) | | | | | |
| **Sig** | **F value** | **Means sum** | **D.F** | **Squares sum** | **Model** |
| 0.000* | 8.439 | 73.639 | 3 | 220.919 | Regression |
| | | .840 | 73 | 61.354 | Remain value |
| | | - | 76 | 282.273 | Total |
| **(Coefficients) analysis** | | | | | |
| **Sig** | **T value** | **(Beta)** | **Standard error** | **Cybersecurity governance variables included in the regression model** | |
| .000 | 5.25 | - | .055 | **(**0.397**) Fixed limit** | |
| .000 | 7.783 | .381 | .267 | Cybersecurity governance strategy | |
| .000 | 6.219 | .359 | .238 | Cybersecurity related to human | |

 ISSN:2336-2693 | E-ISSN:2336-4890

| | | | | |
|---|---|---|---|---|
| | | | | resources |
| .000 | 6.774 | .397 | .223 | Cybersecurity risk management |

* Statistically significant at (0.05 ≥α) of significance level.

It is evident from Table (5) that the three criteria that were adopted as independent variables for cybersecurity governance and that were adopted as independent variables combined, i.e. the value of the coefficient of determination (R2) explain the differences between (99.7%) of the respondents of the study sample in the audit Electronic where the value of the modified coefficient of determination (Adj. R2). (.424) And based on the value of (F) for the model, which amounted to (8.439), and its level of significant significance (P), which amounted to (0.000), it turns out that the effect of these three criteria on the risks of electronic audit is statistically significant. It was found through the values of the standard transactions (Beta) shown in Table No (7) that the cybersecurity risk management variable was the most influential in electronic auditing, as the value of the standard parameter () was (.397), which is a statistically significant value. (t) Significance (Sig) (.000) which is less than the level of significance (0.05), followed by the standard for cybersecurity governance strategy, where the value of the standard parameter () reached (.381), which is a statistically significant function, where the value of (t Significance (Sig) (.000) which is less than the level of significance (0.05). Finally, the cybersecurity standard related to human resources came and was the least influential in electronic auditing, where the value of the standard parameter () was (.359), which is a statistically significant , Where the significant value (t) was (Sig) (.000) which is less than the level of significance (0.05). Accordingly, the main null hypothesis of the study is rejected, and the alternative hypothesis is accepted, which states: "There is a statistically significant effect of cybersecurity governance standards in reducing the risks of electronic auditing in Jordanian commercial banks from the point of view of the certified public accountant." As for testing the hypotheses stemming from this hypothesis, the results showed the following:

The first rejects, and accepts the alternative hypothesis, which states that “there is a statistically significant impact of the cybersecurity governance strategy in reducing the risks of electronic auditing in Jordanian commercial banks from the point of view of the certified public accountant” where the significant (t) value (Sig) was less than the significance level (0.05).

It rejects the second hypothesis, which states that “there is a statistically significant effect of cybersecurity related to human resources in reducing the risks of electronic auditing in Jordanian commercial banks from the point of view of the certified public accountant, as the value of (t) moral (Sig) is less than the level of significance. (0.05).

Rejects the third hypothesis, which states that “there is a statistically significant effect of cybersecurity risk management in reducing the risks of electronic auditing in Jordanian commercial banks from the point of view of the certified public accountant”, as the value (t) is less than the level of significance. (0.05).

**Results:**

The results of the hypothesis test indicated that there is a statistically significant effect of the cybersecurity governance standards in reducing the risks of electronic auditing in Jordanian commercial banks from the viewpoint of the certified public accountant. It was found that cybersecurity governance standards contribute to protecting assets, ensuring the integrity of

ISSN:2336-2693 | E-ISSN:2336-4890

financial data, and helping to analyze assets, fixed assets and account balances. It also contributes to reducing the cost of preserving work papers and detecting fraud and fraud, and provides adequate opportunity to implement all audit procedures quickly and accurately. The results of the sub-hypothesis test also revealed the following:

First: The existence of a statistically significant impact of the cybersecurity governance strategy in reducing the risks of electronic auditing in Jordanian commercial banks from the point of view of the certified public accountant. And the arithmetic means of the statements related to this criterion came at a high level. It was found that the bank is developing a cybersecurity governance strategy in line with its objectives and requirements, and is also keen to increase cybersecurity capabilities, attract inventions and innovations, and deliver their benefits. It was found that the bank has an information technology plan through which the cybersecurity governance strategy is developed, approved, applied and updated.

Second: The existence of a statistically significant impact of cybersecurity related to human resources in reducing the risks of electronic auditing in Jordanian commercial banks from the point of view of the certified public accountant. The arithmetic means of the statements related to this standard came at a high level, and it was found that the bank's management is keen on recruiting employees and ensuring that the important aspects of cybersecurity work are presented, and that recruitment and training plans are audited to ensure that they reflect the specific needs of the bank. Core, through which cybersecurity policies and procedures are communicated to workers,

Third: The existence of a statistically significant effect of managing cybersecurity risks in reducing the risks of electronic auditing in Jordanian commercial banks from the point of view of the certified public accountant, and that the arithmetic means of the statements related to this standard came at a high level. It was found that the bank’s management is exercising its supervisory and supervisory role when identifying and measuring cybersecurity risks and developing alternative strategies to confront them, and that the bank uses external consultants with specialization in the field of cybersecurity risk management. It was also found that the extent of compliance with strategies and policies for managing cyber security risks in the bank is being followed up from before the steering committee; documents are audited to ensure that cybersecurity risks are part of the IT governance framework.

**Recommendations:**

The researcher recommends the necessity of adhering to the instructions for adapting to traffic risks issued by the Central Bank of Jordan, due to their impact on reducing the risks of electronic auditing in Jordanian commercial banks, by following the following mechanisms:

1- The necessity of auditing a cybersecurity governance strategy or management interview to determine resource requirements and the method by which they are identified and approved.

2- The management reviews the minutes of the periodic organizational steering committee meetings for the cybersecurity governance strategy and takes into account the development of the performance indicators of this strategy.

3- Working on developing the means, methods and processes related to the cybersecurity governance strategy and related systems to be able and effective in implementing information technology systems.

4- That the strategic cybersecurity plan related to human resources is audited to ensure

ISSN:2336-2693 | E-ISSN:2336-4890

that it includes the requirements of people for current and future needs and to determine the competence and training of current and new employees.

5- The bank management meets with human resources managers to evaluate the mechanism of action for important positions in cases of emergency or long absence.

6- The necessity of auditing the cybersecurity risk management plan or any other documents to ensure that the responsibilities for risk management have been clearly defined and the resources identified effectively during the completion of the IT goals.

7- Working on interviewing persons responsible for cybersecurity risks to determine whether their cost has been appropriately estimated and providing adequate resources.

8- Emphasize the importance of auditing training or publishing mechanisms such as e-mail, notes, and notes to ensure that issues related to non-compliance with cybersecurity governance are mentioned.

**References:**

Abu Shanab, Imad, Harb, Yusra, and Abu Al-Basal and Wijdan, (2019), Electronic Services, Al-Mutanabi Publishing House, Irbid, Jordan.

Al Hroub, Muzaffar Nile, (2015), The Impact of Governance on the Quality of the Independent Chartered Accountant Report: (Field Study in Jordanian Commercial Banks), Master Thesis, Isra University, Amman, Jordan.

Al-Khalidi, Nahedh, (2015), The effect of using electronic data processing methods on increasing the effectiveness of auditing offices operating in the Gaza Strip, The Scientific Journal, Islamic University, 23 (1): 282-304.

Al-Khasawneh, Reem Okab, (2013), The Role of Electronic Auditing in Achieving Competitive Advantages in Auditing Offices in the Hashemite Kingdom of Jordan, a scientific study presented to the Second International Scientific Conference of the College of Business and Finance, entitled: The Role of Excellence and Leadership in the Excellence of Business Organizations, held during the period 21-22 / 5/2013 AD at the International Islamic Sciences University, Amman - Jordan.

The Cyber Risks Adaptation Instructions Guide issued by the Central Bank of Jordan in 2018 to audit cyber risks in information technology.

Zahlan, Antoine, (2019), The Arabs and the Challenges of Science and Information Technology, Center for Arab Unity Studies, Beirut, Lebanon.

Al-Omair, Omair Abdullah, (2018), The Role of Electronic Auditing in Improving Internal Auditing in Kuwaiti Public Shareholding Companies, Master Thesis, Al-Bayt University, Mafraq, Jordan.

Al-Maghrabi, Mona Mohamed, (2018), The Impactful Role of Information Security Governance in Reducing the Risks of Accounting Information Systems: A Field Study, Benha University Journal, Volume 3, Issue 5, pp. 54-67.

Al-Muhtadi, Sawsan Zuhair (2020). Electronic Governance Technology, Osama House for Publishing and Distribution, Amman, Jordan.

Nassour, Reem (2015), The Impact of Information Technology Governance on the Quality of Financial Reports: Field Study, PhD Thesis, Accounting Department, Tishreen University, Syria.