Modern Applied Science; Vol. 14, No. 3; 2020
ISSN 1913-1844 E-ISSN 1913-1852
Published by Canadian Center of Science and Education

The Impact of Cyber Governance in Reducing the Risk of Cloud Accounting in Jordanian Commercial Banks - from the Perspective of Jordanian Auditing Firms

Prof Dr. Osama Abdul Moniem Ali[1], Dr. Ala Jaber Matarneh[2], Dr. Ahmed Almalkawi[3] & Dr. Hamzeh Mohamed Alhawamdeh[4]

[1]Full Professor, Accounting Department, Jerash University, Jordan

[2]Associate Professor, Accounting Department, The World Islamic Sciences and Education University, Jordan

[3] Associate Professor, Business and Administrative sciences Department, Jerash University, Jordan

[4] Assistant Professor, Business and Administrative sciences Department, Jerash University, Jordan

Correspondence: Prof Dr. Osama Abdul Moniem Ali, Full Professor, Accounting Department, Jerash University, Jordan

Received: January 17, 2020 Accepted: February 23, 2020 Online Published: February 26, 2020

doi:10.5539/mas.v14n3p75 URL: https://doi.org/10.5539/mas.v14n3p75

Abstract

The objective of this study is identifying the impact of cyber governance on reducing the risk of cloud accounting in the Jordanian commercial banks. To achieve the objectives of this study, the descriptive and analytical approach was used; the study community is composed of external legal accountants who practices auditing in Jordan, (477) of them are practicing external auditing at the end of (2018) according to the statistics of the Jordanian association of certified public accountants (JACPA). Due to the difficulty and cost of the comprehensive survey, a simple random sample was taken. The sample included (213) auditors. The questionnaire was distributed to the sample of the study by the researchers personally and through e-mails, (182) questionnaires were recovered, after excluding (7) for the incompetence, of which (175) were valid for the statistical analysis. Thus, the percentage of retrieved and analyzed questionnaires was (82.2%), which is statistically acceptable. and In order to analyze the study data and test hypotheses, the statistical package for social sciences (SPSS) was used in the various statistical analyses, which are the descriptive statistics and coefficient of internal consistency (Cronbach's alpha). also, The multiple correlation test was used, using the Pearson correlation coefficient, Multiple linear regression and stepwise regression analysis. The study came to find several results , the most important was The presence of a statistically significant impact of cyber security governance (cybersecurity security governance requirements, cybersecurity program, cyber security policy, cyber information management, evaluating and managing cyber risks) in reducing cloud accounting risks in Jordanian commercial banks, The most important recommendations are the need for Jordanian commercial banks to adopt the cyber governance as a basic reference to their banking policy to address the risks associated with the use of cloud accounting, As well as the need to establish a special department for human resources management within the bank which would have a pioneering intellectual orientation to cope with modern trends in cyber governance.

Keywords: cyber governance, cloud accounting, auditing, Jordanian commercial banks, central bank

1. The Problem of Study

Many banks face problems due to the severe weakness in the systems of cyber governance and the basic elements of cloud and administrative accounting, which is reflected in the inflationary employment and the absence of duplicative structures, powers overlapping, and the lack of clarity of plans and objectives and weak accountability, The difficulties experienced by the banks came as a result of the formal role of the boards of directors and the consequent weakness of the control procedures. Which requires the building of effective cyber governance systems and cloud accounting systems which are capable of reducing fraud, manipulation and could face the risks of cloud accounting, thus ensuring that the objectives of the credibility of the financial statements, the efficiency and effectiveness of operations and adherence to policies, laws and regulations have been achieved? The problem of the study lays in the following main questions:

The first main question: What is the level of implementation of cybersecurity governance in Jordanian commercial banks?

The second main question: What is the level of reducing cloud accounting risks in Jordanian commercial banks?

The third main question : Is there an impact of cyber security governance (cyber security governance requirements, cyber security program, cyber security policy, cybersecurity information management, evaluating and managing cyber risks) in reducing cloud accounting risks in Jordanian commercial banks? The following sub-questions are branched from it as follows:

- The first sub-question: is there an impact of the requirements of cyber security governance on the risks of cloud accounting.
- The Second sub- question: Is there an impact of the cyber security program on the risks of cloud accounting.
- The Third sub- question: Is there an impact of cyber security policy on the risks of cloud accounting.
- The Fourth sub- question: Is there an impact of cyber security information management on the risks of cloud accounting.
- The Fifth sub- question: Is there an impact of evaluating and managing cyber risks on the risks of cloud accounting.

2. The Importance of the Study

The importance of the study stems from the importance of cyber governance and accounting systems that are applied in commercial banks for their vital role in the nature of the banks' work by achieving the main objectives of the credibility of the financial statements and achieving the efficiency of operations and their compliance with policies, laws and regulations. As well as addressing the risks to the work and the risks of cloud accounting that prevent the achievement of these objectives and thus improve their control capabilities.

3. Objectives of the Study

The study aims to achieve the following:

1. Clarifying the impact of the implementation of cyber governance on reducing the risk of cloud accounting in Jordanian commercial banks.

2. To shed light on the basic concepts of cyber governance and the concepts of cloud computing and its intellectual property when applied in Jordanian commercial banks.

3. Studying the impact of cyber security governance (cyber security governance requirements, cyber security program, cyber security policy, cybersecurity information management, Evaluating and managing cyber risks in reducing cloud accounting risks in Jordanian commercial banks.

4. Hypotheses of the Study

Based on the questions of the problem of the study, the study depends on the assumptions that:

The main hypothesis: There is no statistically significant impact at the significance level ($\alpha \leq 0.05$) of cyber security governance (cyber security governance requirements, cybersecurity program, cybersecurity policy, cybersecurity information management, Evaluating and managing cyber risks) in reducing cloud accounting risks in commercial banks Jordanian.

The following sub-assumptions are subdivided from the main hypothesis:

- H01-1: There is no statistically significant impact at the significance level ($\alpha \leq 0.05$) of the requirements of cyber security governance on the risks of cloud accounting.
- H01-2: There is no statistically significant impact at the significance level ($\alpha \leq 0.05$) of the cyber security program on the risks of cloud accounting.
- H01-3: There is no statistically significant impact at the significance level ($\alpha \leq 0.05$) of cyber security policy on the risks of cloud accounting.
- H01-4: There is no statistically significant impact at the significance level ($\alpha \leq 0.05$) of the cybersecurity information management on the risks of cloud accounting.
- H01-5: There is no statistically significant impact at the significance level ($\alpha \leq 0.05$) of Evaluating and managing cyber risks on the risks of cloud accounting.

5. Sample of the Study

The study community is composed of external legal accountants who practices auditing in Jordan of which (384) are practicing external auditing at the end of (2017), according to the statistics of the Jordanian association of certified public accountants (JACPA). Due to the difficulty and the cost of the comprehensive survey, a simple random sample was taken. Which was determined by (Krejcie & Morgan) .The sample included (192) auditors. The questionnaire was distributed to the sample of the study by the researchers personally and through e-mails, the number of questionnaires recovered was (184), of which (175) were valid for the statistical analysis, after excluding (9) for the incompetence. Thus, the percentage of retrieved and analyzed questionnaires was (91.1%), which is statistically acceptable.

6. Methodology of the Study

The analytical descriptive approach was adopted. The researchers obtained the necessary data for this study from the following sources:

1- Primary resources: The preliminary data needed for this study was obtained through a questionnaire prepared and distributed to a group of auditors who formed the study sample, and then the data was collected and analyzed using the SPSS software to test the validity of the hypotheses.

2- Secondary resources: The secondary data related to this study was obtained by reference to books, university transcripts, scientific researches, reports and articles in newspapers and magazines in order to build the theoretical framework of the study and achieve its objectives.

7. Theoretical Aspect

7.1 Introduction

The emergence of accounting programs has led to a significant improvement in accounting practices. Given the enormous amount of information and time needed to process this information, accounting software has become a very useful tool for accountants to do their work faster and more efficiently. Although accounting programs have existed for decades, they have continued to develop their capabilities over the years, and this development continues (Dimitriua, O. & Mateia, and M. 2015). For that the 20th century saw great progress in the transfer of information, technology accelerated, and social networks emerged. And The Internet has become faster, more reliable, less expensive and has expanded in almost every area. But more importantly, they challenged the foundations of traditional business models. In addition, smartphones have encouraged the spread of cloud services. Information that is relevant and constantly updated is considered crucial in the process of making any economic decision, especially in a competitive environment such as we are witnessing nowadays. Companies can grow or disappear at the same speed, depending on their ability to evolve and adapt to the best existing technology frameworks, since traditional frameworks are no longer sufficient(Pacurari, D. &Nechita, E. 2013).Cloud accounting software has become increasingly popular over time, leading accounting firms as well as accounting organizations, including the American Institute of Certified Public Accountants (AICPA), to increase the level of interest in cloud technology by providing a broad range of cloud-based services and guidance. Which benefits accounting profession and that's through a systematic approach to risk assessment, including the development of effective cloud application policies and the Risk Response Plan, which enable companies to test the effectiveness of this new technology and increase operational efficiency with respect to their accounting business (Dimitriua, O. & Mateia, M. 2015).

7.2 The Concept of Cloud Computing and Its Own Technologies

Cloud accounting can be defined simply as storing, processing and using data available on multi-site computers by accessing it over the Internet. This means that users of these data can benefit from the high capacity of computer systems, which does not require large capital investments to meet their needs, and that they can access their data from anywhere as long as they are connected to the Internet.

The availability of financial information from anywhere in the world and at any time has become an urgent necessity. The availability of data of costs, revenues, sales, corporate finance over the Internet provides limited access through independent access to space and time (Wyslocka, E & Jelonek, D. 2015). The key condition for exploiting the benefits of cloud computing is to fill gaps in judgments And related laws, and in addition to improving conditions for users, solving information security problems, encouraging the public sector to benefit from the services of these systems and to support further research and development in the field of cloud computing. The rapid growth of cloud computing takes into account the need to work on the implementation of a legal framework for data protection and the development of standard standards governing the processing Process and which considered necessary to increase the integrity of the provision of this service.

Cloud computing enables companies to quickly deliver new products to the market, through more effective collaboration with international partners, as well as advanced, low-cost computing resources. The operations performed through the cloud service allow close cooperation between various service providers and increase the possibility of cooperation and access to information between different companies, which promote the internationalization of operations and economic activities, But on the other hand, the barriers of cloud computing are represented as users' fear that the data stored and transmitted over the Internet will be used or detected in unexpected ways. In addition, companies need to be confident and reassuring to service providers about the security of their information. This aspect is one of the most important considerations by business owners who want to take advantage of new solutions. Data transfer through the internal network (LAN) Gave business owner's confidence by restricting any person who is not authorized to obtain data.

7.3 *The Impact of Effective Accounting Techniques on Cloud Computing* Include (Marand et al, 2013: pp. 2836-2846)

1. Database (for data analysis).
2. Expert systems (Assist in analysis of deviations and risk analysis).
3. Neural Network (Prediction Tools).
4. Data storage (to provide user-specific information).
5. Decision support programs (help with data analysis and decision support).
6. High connection (to improve access to information).
7. Digital confirmations and signatures (ongoing audit).
8. Artificial intelligence (the possibility of change in reports according to circumstances).
9. Synchronization in both search and data analysis (data analysis and decision support).

7.4 Orientations of the Jordanian Central Bank to Find a Governance Cybernetics in the Face of the Risks of Cloud Computing

The Central Bank of Jordan has issued special instructions to banks to try to face the threat of using information technology represented by the risks of cloud computing, which led to finding a solution by the Central Bank through the use of what is known as cyber governance, and was according to the following conditions and instructions: (Central Bank of Jordan, 2018)

First: Conditions of cyber security governance.

Banks must adhere to the following:

1- The Board of Directors shall include in its membership and those authorized by its committees senior executive management people with the appropriate skills and knowledge to understand and manage the cyber risks.

2- The Council or whoever delegates its committees shall assume the following responsibilities and tasks according to their positions :

   1. Adoption of the Cyber Security Policy.
   2. Adopting the Cyber Security Program.
   3. Check compliance with the Cyber Security Policy and Program.

3- The senior executive management shall assume the following responsibilities and tasks according to its position :

   1. Ensure the application and updating of cyber security policy.
   2. Ensure that the cyber security program is implemented in a manner that is integrated with the overall framework of IT risk management and continues to be updated and developed.
   3. Ensure a comprehensive Cyber Risk Register and ensure that it is continuously updated and that it is compatible with the company's Risk Profile IT file.
   4. Monitor the level of cyber risks continuously.
   5. Adopt the lists of authorizations relating to security management and cyber security in terms of identifying the entity, multiple sides, people, or responsible parties, and those responsible in a final

manner (Accountable) the consulted, and those that are informed, for all the risk management and processes Control and overall control processes.

Second: Cyber Security Policy and Program:

Banks should implement and continue to update the Cyber Security Program to ensure that the confidentiality, reliability and availability of information in the ICT environment is met, with the minimum program including:

1- Identifying internal and external threats of cyber risks.
2- Identifying and classifying the risks and sensitivity of information in an ICT environment.
3- Identifying those with access to and can use the information and the ICT environment.
4- Implement the cyber security policy and procedures and the operation and the ICT environment necessary to ensure the protection of information assets and sensitive information in the company from illegal penetration.
5- Detect successful and unsuccessful illegal infiltration attempts as soon as possible.
6- Take the necessary corrective actions to control and minimize the negative effects of cyber risks.
7- Procedures for restarting the Company's operations after their interruption, including those related to the services as well as legal and regulatory requirements within the acceptable time and period specified in the Business Continuity Plan.

Third: Cyber security policy: (Central Bank of Jordan, 2018)

The policy of the following topics should include the minimum of :

1- Identifying roles and responsibilities, including decision-making within the Bank in relation to the management of cyber risks, including emergencies and crises.
2- Data Governance and Classification.
3- Security and information management and the ICT environment in the company.
4- Customer data privacy.
5- Cyber risk management.
6- Controls protection to reduce and control cyber risks.
7- Business continuity and disaster recovery plans.
8- Cooperate with the parties concerned to respond effectively to and recover from cyber attacks.
9- Monitoring and developing systems, networks and applications.
10- Physical and environmental security controls.
11- Managing process assigned to the third party.
12- To sensitize and train employees within the company regarding cyber security to ensure that all employees in the bank apply to all items of cyber security policy.
13- Determine the mechanism of disclosure to the parties concerned on the items of the cyber security policy each according to his role.
14- Identification of the owner, scope of application, periodicity of review and updating, powers of access, distribution, objectives, responsibilities, working procedures, penalties in case of non-compliance and compliance inspection mechanisms.

Fourth: Responsibilities of the Cyber security Information Manager

The bank should manage the security of information related to cyber security through an information security manager so that it does not administratively follow the IT department and is independent in a manner that ensures non-conflicts of interest and has the practical experience and professional knowledge necessary to be responsible for the following tasks as a minimum:

1- Supervise directly the development and implementation of the cyber security program and policy and ensure that they are continuously reviewed and updated.
2- Assess the adequacy and efficiency of the cyber security program and policy.

3- Review the effectiveness of the security controls adopted in the company's cyber security policy on an ongoing basis.
4- Identify and assess cyber risks.
5- To submit at least semi-annual reports or whenever necessary to the Board and the Executive in relation to cyber security in the Company, provided that the report shall include the following minimum matters:
   - Deviations related to the application of cyber security policy and procedures.
   - Results of the risk assessment.
   - Results of an assessment of the adequacy and efficiency of the cyber security program and policy.
   - Recommendations, procedures and requirements to be implemented.
   - Summary reviews the most important events of threats and breaches of cyber security experienced by the company during the reporting period.

Fifth: Cyber Risk Management:

Banks should determine the following to be able to assess the cyber risks that they may face:

1- Critical functions and operations in the Bank.
2- The information origins in the Company and the understanding of its operations, procedures, systems and related resources and information systems and the access to it, including internal and external systems associated with it.
3- The Bank should classify its functions, critical operations and information assets in terms of their importance and sensitivity, and continuously review and update the classifications.

Sixth: Cyber Risk Assessment : (Central Bank of Jordan, 2018)

Banks should analyze cyber risk factors continuously in terms of identifying the following:

1- Internal threats.
2- External threats.
3- Weaknesses in the management of ICT environment resources.
4- Weaknesses in the ability of the ICT environment to enable the operations of the company.
5- Weaknesses in the management of the risks on the ICT environment.

So the researchers agree with (Grembergen. 2002) that the risks at the company or bank level cannot be eliminated permanently, but the management of the company and the bank has the responsibility to reduce these risks to the acceptable minimum. The risk management process is an ongoing process that begins by assessing the level of exposure of the company and the Bank to risks and identifying the main risks. . Therefore, when the risks are identified, they should be minimized using the usual tools and controls for proper cyber governance applications. For that, the researchers believe that cyber governance practices in risk management and proper application can effectively contribute to eliminating or reducing the risks of cloud computing by following these steps:

1- Analysis and evaluation of IT risk and cloud computing risk.
2- Monitor the efficiency of internal controls.
3- Apply controls to reduce IT risk and cloud computing risk.
4- Establish the necessary procedures to ensure transparency about the risks of interest to the company or the bank.
5- Keep in mind that a proactive risk management approach is a competitive advantage.
6- Insisting that risk management is an integral part of the operations of the company or the bank.
7- Ensuring that IT services are sound, blocking information about people without authority, and those transactions are correct and can be trusted.

8. Practical Side

8.1 Methodology of the Study

The study relied on the descriptive analytical approach to describe the phenomenon under study, where a questionnaire was designed to measure the variables of the study, find the relationship between them and analyze them, with the aim of building interpretations of data and information, and answering questions that were asked in the study problem.

8.2 Sample of the Study

The study community is composed of external legal accountants who practices auditing in Jordan of which (477) are practicing external auditing at the end of (2018), according to the statistics of the Jordanian association of certified public accountants (JACPA). Due to the difficulty and the cost of the comprehensive survey, a simple random sample was taken. Which was determined by (Krejcie & Morgan) .The sample included (213) auditors. The questionnaire was distributed to the sample of the study by the researchers personally and through e-mails, the number of questionnaires recovered was (182), of which (175) were valid for the statistical analysis, after excluding (7) for the incompetence. Thus, the percentage of retrieved and analyzed questionnaires was (82.2%), which is statistically acceptable.

8.3 Sources of Data Collection

The researchers relied on two types of sources to obtain the data necessary for this study. These sources were as follows:

1- Secondary resources: Secondary data related to this study were obtained by referring to books, university theses, scientific research, reports and articles in newspapers and magazines in order to build the theoretical framework for the study and achieve its goals.

2- Primary resources: These sources are represented in the questionnaire, which was designed to achieve the purpose of the study, in a manner consistent with the study problem and its questions, and the nature of the data and information to be obtained, after reviewing the literature related to the topics of the study, and benefiting from the opinions and experiences of the specialists. The questionnaire was distributed to a group of auditors who formed the study sample, and then collected and analyzed data using the SPSS software, to test the validity of the hypotheses.

To find out the extent to which the sample members agree to the questionnaire paragraphs, a five-Likert scale was used to measure the responses of the study sample individuals, as the following weights were given: (Strongly agree = 5, Agree = 4, Neutral = 3, Disagree = 2, Strongly disagree = 1). The relative importance of the topics of the questionnaire and its paragraphs were also judged as follows:

Table 1. Determining the relative importance of the responses of the sample

	Individuals		
Average	*Less than 2.33*	*From 2.33 to less than 3.66*	*From3.66 To less than 5.00*
relative importance	low	Moderate	High

Statistical methods used

The SPSS program was used to analyze study data and test its hypotheses, as the following statistical tools were used:

1- Descriptive statistics measures, through iterations, percentages, arithmetic mean and standard deviations, to describe the characteristics of the study sample and the degree of their approval of the study tool paragraphs and their variables.

2- Internal consistency coefficient (Cronbach's Alpha), to test the stability of the study tool.

3- Pearson correlation coefficient, to test the presence of the phenomenon of Multicollinearity.

4- Analysis of Multiple and Stepwise Linear Regression, to test the study hypotheses.

Study tool stability test

The stability of the tool used to measure the variables included in the study was tested using the Cronbach Alpha Coefficient test, where the scale result is statistically acceptable if the value of the Cronbach alpha is greater than (0.60) (Sekaran, 2006, 311), and the closer the value is to (100%) This indicates higher stability degrees for the study tool, and given the data in the following table, the coherence coefficient of Cronbach Alpha was measured

for the study variables and their dimensions and for the study tool as a whole to find out the consistency of the answers, as follows:

Table 2. The coherence coefficient values for the study tool paragraphs

No	*Topics*	*Number of sections*	*Coefficient of Cronbach's Alpha*
1	Cyber security governance requirements	7	0.809
2	Cyber Security Program	8	0.828
3	Cyber Security Policy	8	0.851
4	Cyber Security Information Management	8	0.847
5	Evaluating and managing cyber risks	6	0.872
	Cyber Security Governance	37	0.946
6	Identity and Access Management	6	0.832
7	Data protection	6	0.848
8	IT Risk: Virtual Operating Risk.	5	0.907
9	IT support	3	0.804
10	Organization	3	0.760
	Cloud Accounting Risks	23	0.928
	All paragraphs	60	0.963

We notice from Table (2) that the value of the internal consistency factor of Cronbach alpha for all paragraphs of the study tool was (0.963), and their number are (60) paragraphs, as the Cronbach factor of alpha reached (0.946) for the paragraphs measuring the cyber security governance, while the Cronbach alpha factor reached (0.928) for paragraphs measuring cloud accounting risks, and therefore all values are greater than (0.60). This is an indication of the consistency between the paragraphs of the study tool, the reliability of the study tool and the reliability of it for conducting statistical analysis.

Table 3. Description of the demographic and personal characteristics of the study sample

Variable	*Category*	*repeats (n=175)*	*percentage*
Qualification	Bachelor (BSc)	129	73.3
	Masters (MSc)	25	14.3
	PhD	13	7.4
	other	8	5.0
Scientific specialization	Accounting	134	76.6
	Finance and Banks	19	10.9
	IT	10	5.7
	Economics	5	2.8
	Management	7	4.0
Number of professional certificates (in addition to JCPA)	One certificate	29	16.6
	Two certificate	8	4.6
	More than Two	2	1.1
	None	136	77.7
Practical experience	Less than 5 years	15	8.6
	From 5 years to less than 10 years	24	13.7
	From 10 years to less than 15 years	67	38.3
	From 15 years to less than 20 years	53	30.3
	20 years and more	16	9.1

Table (3) indicates that the vast majority of individuals in the sample have a first university degree (Bachelor's), where their percentage reached (73.3%), and the percentage of those with a master's degree reached (14.3%), this indicates that the external auditors have The scientific knowledge that enables them to practice the auditing profession with sufficient knowledge. It was also found that the majority of respondents possess sufficient knowledge of accounting and auditing matters related to cyber governance, as the percentage of scientific specialization (accounting) reached (76.6%) of the respondents. This is confirmed by the percentage of the scientific experience category (from 10 years to less than 15 years), which reached (38.3%), as this ratio confirms that the auditors have adequate practical experience in the field of cloud computing risks. The previous table also indicates that (77.7%) of the study sample members do not have other professional certificates except for the JCPS certificate, which is a prerequisite for practicing the auditing profession in Jordan, and this may be due to the increased volume of professional burdens placed on the external auditor, which hinders his ability to obtain other professional certificates

Describing the answers of the respondents

Arithmetic averages, standard deviations, and relative importance ranks were used to describe the responses of the sample members on the questionnaire paragraphs and their topics. The results were as follows:

First: Cyber Security Governance

Cyber security governance included the following dimensions: cybersecurity governance requirements, cyber security program, cybersecurity policy, Cyber Security Information Management, and Evaluating and managing cyber risks.

Table 4. The arithmetical averages , standard deviations and relative importance of the cyber security governance

No	*Domains*	*Arithmetical mean*	*Standard deviations*	*rank*	*degree*
1	Cyber security governance requirements	4.032	0.665	5	High
2	Cyber Security Program	4.239	0.477	2	High
3	Cyber Security Policy	4.215	0.479	3	High
4	Cyber Security Information Management	4.401	0.463	1	High
5	Evaluating and managing cyber risks	4.1194	0.575	4	High
cyber security governance measure		4.216	0.445		High

Table (4) indicates that the trend of the sample members was towards the high relative importance of cybersecurity governance, where the arithmetic average reached (4.216), with a standard deviation of (0.445), the dimension (Cyber Information Security Administration) came first, with an arithmetic average of (4.401), a standard deviation of (0.463), and with a high relative importance, while (Cyber Security Governance Requirements) dimension came last , with an arithmetic average of (4.032), a standard deviation of (0.658), and with a high relative importance as well . it is showed that all dimensions of cyber security governance are of high relative importance.

Second: Cloud accounting risks

Cloud accounting risks included the following dimensions: identity and access management, data protection, IT risks: virtual operating risks, IT support, and organization.

Table 5. The arithmetical averages , standard deviations and relative importance of the Cloud accounting risks

No	*Domains*	*Arithmetical mean*	*Standard deviations*	*rank*	*degree*
1	Identity and Access Management	4.055	0.631	4	High
2	Data protection	4.484	0.501	1	High
3	IT Risk: Virtual Operating Risk.	4.361	0.627	2	High
4	IT support	3.910	0.707	5	High
5	Organization	4.097	0.661	3	High
	Cloud accounting risks	4.182	0.507		High

Table (5) indicates that the trend of the sample members was towards the high relative importance of the risks of cloud accounting, where the arithmetic average was (4.182), and a standard deviation of (0.507), (data protection) dimension came in the first place, with an average of (4,484) , a standard deviation of (0.501), and with a high relative importance, while (IT support) came last, with an arithmetic average of (3.910), a standard deviation of (0.707), and with a high relative importance as well. It is showed that all dimensions of Cloud Accounting risks have emerged with a high relative importance.

Test of Study hypotheses

The study relied in the hypothesis test on the multiple regression analysis and the stepwise regression analysis in order to answer the study questions. before proceeding with the analysis, it was confirmed that the data is free from the phenomenon of multiple correlation, as this phenomenon indicates that there is a near-perfect linear correlation between two or more variables, which amplifies the value of the R2 coefficient and makes it greater than its actual value, and for this the linear correlation coefficient was calculated for each variable tested, and the results were as follows:

Table 6. Correlation matrix for independent variables

variable	*Cyber security governance requirements*	*Cyber Security Program*	*Cyber Security Policy*	*Cyber Security Information Management*	*Evaluating and managing cyber risks*
Cyber security governance requirements	1.000				
Cyber Security Program	0.469**	1.000			
Cyber Security Policy	0.591**	0.785**	1.000		
Cyber Security Information Management	0.443**	0.548**	0.734**	1.000	
Evaluating and managing cyber risks	0.503**	0.548**	0.701**	0.764**	1

** Significant at the significance level of 0.01

Table (6) shows that the highest correlation coefficient value appeared between the two independent variables (cyber security program) and (cyber security policy), which reached (0.785), while the correlation coefficient value between other independent variables was less than that, and this indicates that there is no presence of the phenomenon of multiple linear correlation between the variables of the independent study, where the values of the linear correlation coefficient that exceed (0.80) may be considered an indication of the presence of multiple linear correlation (Guajarati, 2004, 359), and therefore it can be assured that the study sample is free from the problem of multiple high linear correlation.

Results of the main study hypothesis test H0: There is no statistically significant impact at the significance level ($\alpha \leq 0.05$) of cybersecurity governance (cyber security governance requirements, cybersecurity program, cybersecurity policy, cybersecurity information management, evaluating and managing cyber risks) in reducing cloud accounting risks in Jordanian commercial banks.

Table 7. Sample Summary and ANOVA Variation Analysis

Dependant variable	*Summary*				*ANOVA*	
	Correlation coefficient	*The coefficient of determination R^2*	*Adjusted R^2*	*Sample model error*	*Calculated F*	*Sig (F)*
cloud accounting risks	0.843	0.710	0.702	0.277	82.795	0.000

Table (7) shows the significance of the model, where the value of (F = 82.795) and the level of significance (SigF = 0,000) is less than (0.05), and this confirms the significance of the model, as the value of the correlation coefficient (R = 0.843) indicated the relationship between the independent variables and the dependent variable And, the value of the determination coefficient (R^2 = 0.710) indicated that what percentage of (71.0%) of the variance in (cloud accounting risks) can be explained by the variance in the independent variables, with any other factors remaining constant.

We therefore reject the main null hypothesis, and accept the alternative, which states:

“There is a statistically significant imapct at the significance level (α≤0.05) of cyber security governance (cyber security governance requirements, cybersecurity program, cybersecurity policy, cyber information security management, evaluating and managing cyber risks) in reducing cloud accounting risks in Jordanian commercial banks ".

The following is a summary of the results of testing the hypotheses branching from the main hypothesis, based on the regression coefficients table.

Table 8. Regression coefficients for the main hypothesis

Regression coefficients				
Independent Variable	*(B) coefficients*	*Standard error*	*Calculated T*	*Sig (T)*
Cyber security governance requirements	0.145	0.042	3.345	0.001
Cyber Security Program	0.098	0.046	2.108	0.037
Cyber Security Policy	0.417	0.090	4.611	0.000
Cyber Security Information Management	0.165	0.078	2.102	0.037
Evaluating and managing cyber risks	0.496	0.0.61	8.184	0.000
Regression constant	0.617	0.211	2.922	0.004

First hypothesis test results:

The value of the regression coefficient (0.145) indicated the impact of cybersecurity governance requirements in reducing cloud accounting risks, which was significant, as the value of t (3.435) was at a level of significance (Sig. = 0.001).

Therefore, we reject the first null hypothesis, which states:

"There is a statistically significant imapct of requirements at the significance level (α≤0.05) of cybersecurity governance in reducing cloud accounting risks in Jordanian commercial banks"

Second hypothesis test results:

The value of the regression coefficient (0.098) indicated the impact of the cybersecurity program in reducing cloud accounting risks, which was significant, as the value of t (2.108) was at the level of significance (Sig. = 0.037).

Therefore, we reject the second null hypothesis, which states:

"There is a statistically significant impact at the level of significance (α≤0.05) of the cybersecurity program in reducing cloud accounting risks in Jordanian commercial banks"

Third hypothesis test results:

The value of the regression coefficient (0.417) indicated the impact of cybersecurity policy in reducing the risks of cloud accounting, which was significant, as the value of t (4.611) was the level of significance (Sig. = 0.000).

Therefore, we reject the third null hypothesis, and accept the alternative that states:

"There is a statistically significant impact at the level of significance (α≤0.05) of cybersecurity policy in reducing cloud accounting risks in Jordanian commercial banks"

Fourth hypothesis test results:

The value of the regression coefficient (0.165) indicated the impact of cyber security security in reducing cloud accounting risks, which was significant, as the value of t (2.102) was at a level of significance (Sig. = 0.037).

Accordingly, we reject the fourth null hypothesis, and accept the alternative that states:

"There is a statistically significant impact at the significance level (α≤0.05) of the Cyber Security Information Management in reducing cloud accounting risks in Jordanian commercial banks"

Fifth hypothesis test results:

The value of the regression coefficient (0.496) indicated the impact of evaluating and managing cyber risks in reducing cloud accounting risks, which was significant, as the value of t (8.184) was at the level of significance (Sig. = 0.000).

Accordingly, we reject the fifth null hypothesis, which states:

"There is a statistically significant impact at the level of significance (α≤0.05) for Evaluating and managing cyber risks in reducing cloud accounting risks in Jordanian commercial banks"

To determine which dimensions of cybersecurity governance have the most impact in reducing cloud accounting risks, a progressive multiple regression analysis was used, and the results were as shown in Table 9.

Table 9. Results of the stepwise regression analysis for the main hypothesis H0

model	*cybersecurity governance*	*B*	*Calculated T*	*Sig* Significance level*	*The coefficient of determination R2*	*F Calculated*	*Sig* Significance level*
First	Evaluating and managing cyber risks	0.702	17.296	0.000	0.634	299.137	0.000
Second	Evaluating and managing cyber risks	0.534	9.882	0.000	0.671	175.551	0.000
	Cyber Security Policy	0.277	4.436	0.000			
Third	Evaluating and managing cyber risks	0.563	10.663	0.000	0.694	129.078	0.000
	Cyber Security Policy	0.367	5.597	0.000			
	Cyber security governance requirements	0.153	3.543	0.001			
Fourth	Evaluating and managing cyber risks	0.562	10.742	0.000	0.703	100.371	0.000
	Cyber Security Policy	0.489	5.789	0.000			
	Cyber security governance requirements	0.152	3.561	0.000			
	Cyber Security Program	0.105	2.249	0.026			
Fifth	Evaluating and managing cyber risks	0.496	8.184	0.000	0.710	82.795	0.000
	Cyber Security Policy	0.417	4.611	0.000			
	Cyber security governance requirements	0.145	3.435	0.001			
	Cyber Security Program	0.098	2.108	0.037			
	Cyber Security Information Management	0.165	2.102	0.037			

*** The effect is statistically significant at (α≤0.05)**

The results of the stepwise regression analysis show the order of entry of the variables in the regression model that represents the impact of cyber security governance in reducing cloud accounting risks, as it was found that (evaluation and management of cyber risks) came first, and explained (63.4%) of the variance in the dependent variable And when adding (cybersecurity policy) in the second model, the interpretation rate increased to reach (67.1%), and adding (cyber security governance requirements) in the third model increased the interpretation rate to reach (69.4%). As for adding (cybersecurity program) in the fourth model, it led to an increase in the interpretation rate to reach (70.3%), while the interpretation rate reached (71.0%) when adding (Cyber Security Information Management) in the fifth model. We note that the effect of all independent variables was significant at a significance level less than (0.05).

9. Results

After performing the statistical analysis and answering the study questions, the results can be summarized as follows:

- The increasing level of application of the cybersecurity governance in Jordanian commercial banks, where the arithmetic average reached (4.216), and all dimensions have emerged with a high relative importance.
- The increasing level of risk reduction of cloud accounting in Jordanian commercial banks, where the arithmetic average reached (4.182), and all dimensions have emerged with a high relative importance.
- The presence of a statistically significant effect of cyber security governance (cyber security governance requirements, cybersecurity program, cyber security policy, cyber information security management, evaluation and management of cyber risks) in reducing cloud accounting risks in Jordanian commercial banks. Where the moral effect appeared in all dimensions of cyber security governance, when testing the hypotheses branching from the main hypothesis.
- One of the most important dimensions of cyber security governance is the evaluation and management of cyber risks in reducing the risks of cloud accounting in Jordanian commercial banks.

10. Recommendations

1. Aiming of Jordanian commercial banks to adopt cyber governance as a key reference to their banking policy to address the risks associated with the use of cloud computing.
2. Establishing a special department of human resources management within the bank which has a pioneering intellectual orientation to keep pace with the modern trends of cyber governance.
3. Activate the role of security controls of all types (preventive, exploratory and corrective) and increase the level of application against the environmental risks surrounding the bank which is likely to occur as a result of the application of cloud accounting.
4. Increase the degree of assurance of the provision of security controls for the appropriate cloud accounting, which ensures the safety of information security for banks.
5. Security risks in cloud accounting should be identified by commercial banks in order to obtain a clear picture of sound internal controls and relevant responses that the company should take to ensure that the company's business continues smoothly without fear of data disruption.
6. The management of commercial banks should assess the risks of cloud services provided to them on whether the cloud provider is capable of dealing with the data of banks and the applications used by them or both, and the identification of the risk of data breaches and the risk of any damage to the applications which will slow or stop the processes in banks.

References

Central Bank of Jordan (2018). *Cloud Computing Guideline.* Amman, Jordan. http://www.cbj.gov.jo/EchoBusv3.0/SystemAssets/Ticker%20News/%D8%A7%D9%84%D8%AF%D9%84%D9%8A%D9%84%20%D8%A7%D9%84%D8%A7%D8%B1%D8%B4%D8%A7%D8%AF%D9%8A%20%D9%84%D9%84%D8%AD%D9%88%D8%B3%D8%A8%D8%A9%20%D8%A7%D9%84%D8%B3%D8%AD%D8%A7%D8%A8%D9%8A%D8%A9%20%D9%86%D9%87%D8%A7%D8%A6%D9%8A%20_%D9%85%D8%B9%D8%AA%D9%85%D8%AF.pdf

Central Bank of Jordan (2018). *Cyber Security Governance Instructions.* Amman, Jordan. http://www.cbj.gov.jo/EchoBusv3.0/SystemAssets/New%20HTML/%D8%AA%D8%B9%D9%84%D9%8A%D9%85%D8%A7%D8%AA%20%D8%A7%D9%84%D8%AA%D9%83%D9%8A%D9%81%20%D9

%85%D8%B9%20%D8%A7%D9%84%D9%85%D8%AE%D8%A7%D8%B7%D8%B1%20%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9.pdf

Dimitriua, O. & Mateia, M. (2015). *Cloud accounting: a new business model in a challenging context, Emerging Markets Queries in Finance and Business.* Romania. https://www.researchgate.net/publication/289993037_Cloud_Accounting_A_New_Business_Model_in_a_Challenging_Context https://doi.org/10.1016/S2212-5671(15)01447-1

Grembergen, W. V. (2002). *Introduction to the Minitrack: IT Governance and its Mechan-isms.* Paper presented at the 35th Hawaii International Conference on System Sciences (HICSS), Hawaii. https://scholarspace.manoa.hawaii.edu/bitstream/10125/41788/paper0639.pdf

Marand, A. A., Marand, E. A. & Dashtebayaz, M. L. (2013). Investigating the effects of cloud computing on accounting and its comparison with traditional models. *Advances in Environmental Biology, 7*(10 S1), 2836-2847.https://doi.org/10.29358/sceco.v0i18.227

Păcurari, D. & Nechita, E. (2013). Some considerations on cloud accounting. Studies and Scientific Researches. *Economics Edition,* (18), 193-198.

Wyslocka, E. & Jelonek, D. (2015). Accounting in the cloud computing. *TOJSAT, 5*(4), 1-11.