Kurdish Studies
Feb 2024
Volume: 12, No: 2, pp.2921-2936
ISSN: 2051-4883 (Print) | ISSN 2051-4891 (Online)
www.KurdishStudies.net

Received: December 2023 Accepted: January 2024
DOI: https://doi.org/10.58262/ks.v12i2.213

The Mediating Role of Cybersecurity on the Relationship between Internal Control and the Implementation of Cloud-Based Enterprise Resource Planning Systems in Jordanian Commercial Banks

Assistant Prof. Hebah Rabie[1]

Abstract

This study seeks to investigate the mediating role of cybersecurity on the relationship between internal control and the implementation of cloud-based enterprise resource planning systems among Jordanian commercial banks, with a focus on. Descriptive-analytical methodology was used to describe and analyze the research phenomenon in all Jordanian commercial banks, totaling 12 banks. The unit of analysis included all individuals involved in internal control matters, cloud-based enterprise resource planning systems, and cybersecurity from senior and middle management in the main departments of the lower-level commercial banks. These departments included the following: banking facilities, banking operations, branch operations, risk management, inspection and internal auditing, financial control, human resources, organizational and strategic planning, investment operations, information technology, as well as accounting, internal auditing, cybersecurity, and information protection departments. The Statistical Package for Social Sciences (SPSS V.20) was utilized for data processing and analysis. The study yielded several results, with the most significant being the statistically significant impact of internal control on the implementation of cloud-based enterprise resource planning systems in Jordanian commercial banks, with cybersecurity as a mediating variable. This indicates the crucial and positive role of internal control in enhancing the level of cybersecurity when implementing cloud-based resource planning systems in Jordanian commercial banks. The study's recommendations emphasize the necessity for Jordanian commercial banks to adopt best security practices to protect their cloud-based enterprise resource planning systems. Additionally, there is a need to train employees on secure and effective system usage. The study suggests that the management of Jordanian commercial banks should implement robust and clear cybersecurity policies and procedures, encompassing access rules, defining security responsibilities, incident reporting procedures, and ensuring understanding and compliance by all bank employees.

Keywords: *Internal Control Cloud-Based Enterprise Resource Planning Systems Cybersecurity Jordanian Commercial Banks*

Introduction

The financial sector, represented by banks, is among the most advanced sectors in implementing modern technology and cutting-edge techniques for internal control systems in its activities and operations. The optimal investment in these technologies aims to enhance operational efficiency, particularly through the application of cloud-based enterprise resource planning systems, as a means to achieve the sector's objectives. However, this utilization inevitably comes with some risks and threats that negatively impact workflow and the bank's

[1] Jerash University, Faculty of Business, Accounting Department, Jerash, Jordan, Email: drhebarabee@gmail.com

standing in the market.

Therefore, it is essential to adopt all measures and practices contributing to maintaining data security, combating fraud, complying with regulations, improving operational efficiency, minimizing risks and electronic security threats, and safeguarding the bank's reputation. This is achieved through the use of cybersecurity systems, which have proven successful in executing necessary procedures and instructions, requiring significant time and effort. These systems take appropriate measures for problem-solving, maintain resources and assets, provide services in appropriate and high-quality formats, assist in detecting vulnerabilities and threats, assess security weaknesses, ensure compliance with laws and legal requirements, and enhance customer trust.

The understanding the impact of internal control on the implementation of cloud-based enterprise resource planning systems, along with the mediating role of cybersecurity in Jordanian commercial banks were the main objective of this study.

Study Problem

Cloud computing has become a business necessity, as modern technological developments have imposed new patterns of financial activities on the business world. One of these patterns is cloud accounting, which many organizations, including banks, have adopted. Banks design financial and accounting systems using cloud technology to enhance the effectiveness of accounting procedures and reduce costs. However, this adoption has led to variations in regulatory activities due to differences in the regulatory environment, now characterized as a cloud environment. This shift introduces risks related to operations and information.
While cybersecurity is considered a crucial factor for instilling confidence in the use of cloud-based enterprise resource planning systems and enhancing control procedures, its effectiveness cannot be guaranteed across all banks. Therefore, the study problem revolves around the following questions:

1- "Is there an impact of internal control on the implementation of cloud-based enterprise resource planning systems in Jordanian commercial banks?"
2-"Does internal control have an impact on cybersecurity in Jordanian commercial banks?"
3- "Is there an impact of cybersecurity on the implementation of cloud-based enterprise resource planning systems in Jordanian commercial banks?"?
4- "Does the cybersecurity have a mediating role in the relationship between internal control and the implementation of cloud-based enterprise resource planning systems in Jordanian commercial banks?"

Research Hypotheses

According to the above mentioned questions, the current study develops the following research hypotheses:

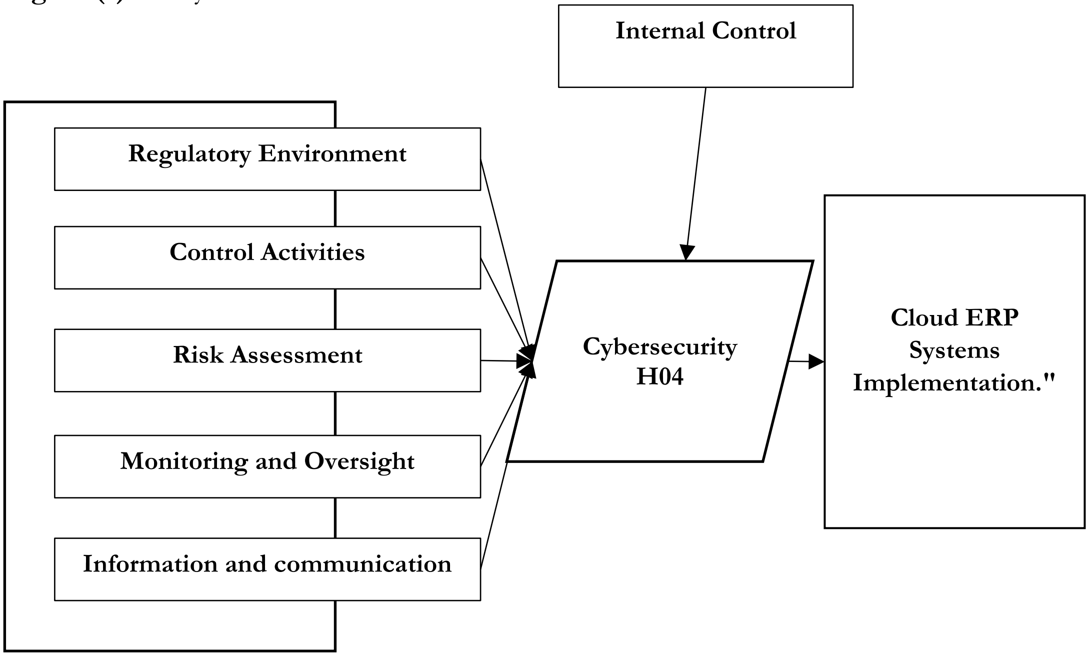
H01: *There is no statistically significant impact of internal control on the implementation of cloud-based enterprise resource planning systems in Jordanian commercial banks".*

H02: *There is no statistically significant impact of internal control on cybersecurity in Jordanian commercial banks".*

H03: *There is no statistically significant impact of cybersecurity on the implementation of cloud-based enterprise* *resource planning systems in Jordanian commercial banks".*

H04: *There is no statistically significant impact of internal control on the implementation of cloud-based enterprise resource planning systems in Jordanian commercial banks when cybersecurity is present as a mediating variable".*

Figure (1): Study Model.



Theoretical Side

Internal control has been defined by the International Institute of Certified Forensic Accountants as "an integrated system that includes organizational plans containing consistent methods and procedures adopted by the administrative unit to protect its assets, review the accuracy of its data, enhance the efficiency of its operations, and promote compliance with established administrative policies" (Ryabov, 2021).

Christopher et al. (2022) further define it as a set of processes and controls aimed at achieving the organization's overall goals by providing measurable and assessable internal systems and controls that protect the organization's assets and mitigate risks. It should ensure compliance with all activities and departments within the organization. According to Lennox et al. (2022), the internal control system is considered a safety valve to confirm the organization's business operations and enhance its readiness to protect against internal and external risks.

Therefore, internal control aims to ensure that banks achieve their strategic objectives by ensuring the effective and efficient implementation of operational and financial processes in ethical and economical ways (Al-Suwaidi, 2022). Additionally, it works towards enhancing productivity while preserving available resources from negative conditions, such as damage and loss, and non-utilization through appropriate evaluative methods. It also involves monitoring the implementation of management-set goals using control systems designed through responsible management, which, in this context, necessitates the application of cloud-based enterprise resource planning systems (Sharabsha & Bakhoush, 2019).

To ensure the continuity, development, and growth of banks, internal control systems are established. The application of banking operations requires organization, control over activities, monitoring employee behavior, and regulation to ensure the achievement of predefined objectives. This is accomplished through the presence of an internal control system characterized by suitable components capable of mitigating potential risks through the establishment of effective and applicable policies (Hanum & Ritonga, 2021).

One of the fundamental components and pillars that make an internal control system highly effective is a flexible, clear, and understandable organizational plan. The accounting system should also be sound, clear, and simple to achieve effective internal control at all stages of the processes through clarifying the accounting cycle and methods of documentation. Additionally, it is essential to separate tasks among employees to reduce the likelihood of intentional or unintentional deviations that may affect financial reports. It is crucial to select qualified and experienced employees, especially those responsible for the internal control system, to regulate performance and obligate all levels of staff from management to the lowest levels of the organizational structure to adhere to goals and plans, avoiding deviations at all levels. Therefore, mechanisms need to be established to deal with these deviations if found, through studying them and implementing corrective measures (Qourin et al., 2019).

From the researcher's perspective, banks need to provide protection against any cyber attacks they may face. Hence, they require what is known as cybersecurity. Goutam & Verma (2015) explained that cybersecurity involves functions concerned with managing technological risks related to the cyber environment through modern techniques.

According to Richardson et al. (2020), cybersecurity encompasses the measures and technical interventions taken to protect networks, information, data, and devices from unauthorized access to maintain the integrity and security of stored information. The importance of cybersecurity is highlighted in the methods and techniques used to protect networks, systems, and programs from electronic threats and attacks that may compromise, damage, or exploit information, as stated by Al-Omari (2020, p. 19).

In the view of Wolden et al. (2015), cybersecurity aims to provide the best basic requirements, including information confidentiality based on standards and practices, and the safety and integrity of information to reduce cyber risks on information and technological assets for all entities, whether internal or external threats. This ensures the availability of information when needed, and the goals of cybersecurity are achieved by fulfilling a set of fundamental axes to maintain information security. These axes include:

Technology: This involves the tools used to protect programs from electronic threats that may occur. It includes the utilization of security systems and software to strengthen and safeguard electronic systems from cyber threats.

Organizations and Individuals:

This encompasses organizations and individuals who utilize information and electronic systems. Ensuring information security requires collaboration and commitment from all members of the organization.

Activities and Operations:

This involves the methods used to employ individuals and the technology that limits or prevents electronic attacks. Here, the relationship between internal control systems and cybersecurity becomes apparent.

The internal control system and cybersecurity are considered essential factors in the current banking landscape. Businesses in general and banks in particular now heavily rely on electronic technologies and applications in conducting various activities and operations. This increased dependence has heightened their vulnerability to various breaches and violations.

The internal control system constitutes an essential part of the cybersecurity strategy, utilized to assess the availability of security and safety for a specific system. It contributes to identifying weaknesses in systems and applications through the assessment of security risks, discovering security vulnerabilities and weaknesses in system configurations, ensuring the proper closure of these vulnerabilities, and aiding in detecting cyber attacks to determine whether the system has been compromised or subjected to prior violations. Upon discovering such attacks, the internal control system is employed to analyze system logs and identify any unauthorized infiltration or exploitation (Bozkus & Caliyurt, 2018).

Moreover, the internal control system enhances awareness and security consciousness among bank employees. It highlights existing security vulnerabilities and outlines the necessary measures to avoid and mitigate their impacts. This increases their ability to monitor and detect cyber threats while working to prevent their occurrence (Stevens et al., 2020).

The internal control system represents a fundamental measure contributing to enhancing cybersecurity in banking operations. It aids in the detection and protection of sensitive data, financial information, and personal customer information within the bank by identifying security threats and cyber intrusions through system monitoring and data analysis. Additionally, it helps assess the implementation of security policies and procedures, ensuring their compliance with international and local standards and legislation.

Moreover, the internal control system ensures the bank's adherence to cybersecurity regulations by examining various records and reports, especially those related to the implementation of cloud-based enterprise resource planning systems. It identifies weaknesses in the system and recommends corrective actions to enhance cybersecurity in the bank. Furthermore, the internal control system, through its reports and statistics, reveals the level of cybersecurity in the bank, assisting in making appropriate and timely decisions to reinforce banking security (Huseynov et al., 2020; Shamsuddin et al., 2018).

In another perspective, cybersecurity plays a crucial role in ensuring the safety of Cloud ERP systems, protecting them from various cyber threats. This is achieved through the development of security procedures and policies (Jamm'e and Alash, 2021), the adoption of specialized protection systems, the implementation of advanced protection and encryption technologies, and regular updates (Ben Alqama and Saahi, 2019). Additionally, it involves strengthening collaborative relationships between technology service providers, government entities, security organizations, and financial institutions to mitigate cyber risks and secure financial data. Moreover, raising awareness among users about adopting appropriate security measures to safeguard their financial and personal information is emphasized, as well as providing competency and knowledge elements for bank employees in information technology to enhance and improve cybersecurity (Despotović et al., 2023).

Methodology:

A descriptive-analytical methodology was adopted in this study, which focuses on exploring detailed aspects of the phenomena under investigation, describing them, analyzing them, and extracting information. This approach contributes to a thorough understanding of the study's subject and enriches knowledge about it.

Population and Sample:

This study was conducted on Jordanian commercial banks, totaling 12 banks. All commercial banks were included in the research population, making the research sample consist of the entire population of 12 Jordanian commercial banks.

Unit of Observation and Analysis:

The unit of observation and analysis included all individuals involved in internal control matters, cloud enterprise resource planning systems, and cybersecurity from upper and middle management in the main departments of commercial banks. These departments include banking facilities, banking operations and branch operations, risk management, internal inspection and auditing, financial control, human resources, organization and strategic planning, investment operations, information technology, as well as accounting, internal auditing, cybersecurity, and information protection departments.

Data Collection:

A questionnaire was developed as a data collection technic from individuals within the research population. 240 questionnaires were distributed to the respondents, and 226 questionnaires were valid to statistical analysis, representing 94.2% of the total distributed questionnaires.

Distribution of Sample Individuals:

Table 1 describe the respondents of the questionnaire according to personal and functional characteristics.

Table (1): Description the Respondents of a Questionnaire According to Personal Data.

Variable	Category	Repeats	Percentage
Gender	Male	114	50.4
	Female	112	49.6
Age	Less than 30 years old	18	8.0
	From 30 – less than 40 years old	68	30.1
	From 40 – less than 50 years old	97	42.9
	50 years and over	43	19.0
Educational Qualification	Bachelor's	143	63.3
	Higher Diploma	10	4.4
	Master's	58	25.7
	Ph.D	15	6.6
Scientific Spinalization	Accounting	82	36.3
	Finance and banking	80	35.4
	Business management	5	2.2
	Economy	9	4.0
	Information Technology	22	9.7
	Other	28	12.4
Work Experience	Less than 5 years	17	7.5
	From 5 – less than 10 years	58	25.7
	From 10 – less than 15 years	87	38.5
	15 years and over	64	28.3
Total		226	100

From Table (1), a significant convergence is evident in the percentage of employees in Jordanian commercial banks from both genders (males and females), where the percentage of males was (50.4%), and the percentage of females was (49.6%). This indicates the commitment of Jordanian commercial banks to providing equal employment opportunities for both genders. The majority of employees fell within the age range of (40 – less than 50 years), accounting for (42.9%), suggesting the banks' interest in retaining their human resources. The high percentage aligns with the requirements for reaching leadership and managerial positions in terms of career progression, which necessitates lengthy periods. Moreover, the majority of employees held a Bachelor's degree, constituting (63.3%), indicating that Jordanian commercial bank employees possess the scientific and cognitive capabilities qualifying them for the required tasks. Regarding scientific specialization, it was found that the majority of employees in Jordanian commercial banks are specialized in the fields of accounting, finance, and banking. The percentage of specialization in accounting was (36.3%), and the percentage of specialization in finance and banking was (35.4%), aligning with the nature of the work in Jordanian commercial banks. Employees in these banks also demonstrated sufficient experience, contributing to the desirable performance of banking activities and operations. Approximately (38.5%) of employees have practical experience ranging from (10 – less than 15 years), and (28.3%) have experience ranging from (15 years and above).

Statistical Methods Used:

The text describes the statistical methods employed in the study, utilizing the Statistical Package for Social Sciences (SPSS V.20) for data processing and analysis. The following statistical methods were applied:

Descriptive Statistics: This includes means, standard deviations, frequencies, and percentages.

Cronbach's Alpha: used to test the stability of the research tool by measuring the internal consistency. It is a coefficient ranging from 0 to 1, with values below 0.70 indicating unreliability, and values equal to or exceeding 0.70 suggesting the stability of the research tool.

Variance Inflation Factor (VIF): Examining inflation and allowable variance.

Simple and Multiple Linear Regression Analysis: Used for data analysis along with Path Analysis, performed using the Amos program.

Data Analysis and Hypothesis Testing:

Stability of the Study Tool:

The study aims to measure the accuracy and reliability of the data collection tools. Cronbach's Alpha coefficient is used, with values below 0.70 indicating unreliability and the need for adjustments. Values equal to or exceeding 0.70 suggest stability, and increased values approaching 1.00 indicate higher stability.

Table (3): Displays the Stability Coefficient Results for the Dimensions of the Study Variables.

Variable	Dimensions	Paragraphs number	Alpha
Independent Variable	Regulatory Environment	5	0.690
	Control Activities	5	0.698
	Risk Assessment	5	0.714
	Information and communication	5	0.724
	Monitoring and Oversight	5	0.662
	Internal Control	25	0.913
Dependent Variable	Implementation of Cloud Enterprise Resource Planning Systems	5	0.720
Mediating variable	Cybersecurity	5	0.660

It is evident from Table (3) that all values of alpha have exceeded the minimum acceptable level threshold for statistical analysis purposes, which is (0.60), with alpha values ranging from (0.660-0.913).

Multicollinearity Test

Such test is used to to measure the strength of the correlation between independent variables in the research model. The presence of high correlation is considered one of the most important determinants negatively affecting the accuracy and reliability of data and its usability for analysis purposes. This test uses the Variance Inflation Factor (VIF) and Tolerance to assess multicollinearity, where the VIF values between (1.0-10.0) indicate no issue of high correlation, and Tolerance values between (0.1-1.0) indicate no issue. The following table presents the results of the VIF and Tolerance tests for the dimensions of the independent variable.

Table (4): Results of VIF and Tolerance Test.

Dimension	VIF	Tolerance
Regulatory Environment	1.722	0.581
Control Activities	1.870	0.535
Risk Assessment	1.758	0.569
Information and communication	2.002	0.500
Monitoring and Oversight	1.727	0.579

From Table (4), it is evident that all (VIF) values and Tolerance values were within the acceptable range for both tests. This indicates no high linear correlation among the independent variables' dimensions (Pevalin & Robson, 2009).

Descriptive Analysis of Study

Data Table (5) provides a summary of the mean scores and relative importance of research variables (Internal Control and its dimensions, Implementation of Cloud Enterprise Resource Planning Systems, and Cybersecurity). The table reveals a high level of interest among Jordanian commercial banks in internal control with an average score of (3.743). All dimensions showed high relative importance, with the highest mean score observed for the dimension of "Monitoring and Oversight" at a value of (3.805), while the lowest mean score was for the dimension of "Information and Communication" at a value of (3.690). The table also shows a high level of interest among Jordanian commercial banks in implementing Cloud Enterprise Resource Planning Systems with an average score of (3.699). Similarly, there is a high level of interest in Cybersecurity with an average score of (3.743).

Table (5): Mean Scores and Relative Importance of research Variables.

Variable	Mean	Rank	Relative importance
Regulatory Environment	3.779	2	High
Control Activities	3.699	4	High
Risk Assessment	3.770	3	High
Information and communication	3.690	5	High
Monitoring and Oversight	3.805	1	High
Internal Control	3.743	-	High
Implementation of Cloud Enterprise Resource Planning Systems	3.699	-	High
Cybersecurity	3.743	-	High

4-Hypothesis Testing

This study seeks to test four main hypotheses. The first research hypothesis aimed to test the direct relationship among the independent variable (Internal Control) and the dependent variable (Implementation of Cloud Enterprise Resource Planning Systems). While the second research hypothesis aimed to test the direct association among (Internal Control) the independent variable and the mediating variable (Cybersecurity). The third research hypothesis examines the relationship between (Cybersecurity) the mediating variable and (Implementation of Cloud Enterprise Resource Planning Systems) the dependent variable. The relationship between (Internal Control) the independent variable and (Implementation of Cloud Enterprise Resource Planning Systems) the dependent variable through the indirect causal relationship of the mediating variable (Cybersecurity) was examined through the fourth research hypothesis.

In order to test the first and second research hypotheses, Multiple Linear Regression analysis was conducted. While the third research hypothesis was analyzed using Simple Linear Regression analysis. The fourth hypothesis was tested through using Path Analysis with the assistance of the Amos program supported by SPSS software. The results are as follows:

The first research Hypothesis (H01) stated that "There is no statistically significant impact of Internal Control on the Implementation of Cloud Enterprise Resource Planning Systems in Jordanian commercial banks".

Table (6): The Result of Testing the First Research Hypothesis.

Dependent Variable	**Independent Variable**	**Unstandardized Coefficients**		**Standardized Coefficients**		
		Coefficient B	Standard Error	Coefficient β	Calculated T	Sig. T
Implementation of Cloud Enterprise Resource Planning Systems	Regulatory Environment	0.155	0.065	0.141	2.393	0.018
	Control Activities	0.218	0.063	0.205	3.428	0.001
	Risk Assessment	0.071	0.068	0.066	1.053	0.293
	Information and communication	0.293	0.063	0.292	4.639	0.000
	Monitoring and Oversight	0.278	0.062	0.254	4.510	0.000

Correlation Coefficient R	Coefficient of Determination R^2	Calculated F	Sig. F
0.812	0.659	84.987	0.000

Table (6) shows the findings of the multiple regression analysis for the impact of internal control on the implementation of cloud-based enterprise resource planning systems. The of correlation coefficient values was (0.812=R), indicates a significant relationship between internal control and the implementation of cloud-based ERP systems. The determination coefficient value (0.659=R2) suggests that internal control explains 65.9% of the variance in the implementation of cloud-based ERP systems. The F-value (84.987) at a significance level

(0.000) confirms the significance of the regression at a significance level (α≤0.05), indicating a statistically significant influence of internal control on the implementation of cloud-based ERP systems.

The regression coefficients reveal an impact of the control environment dimension on the implementation of cloud-based ERP systems, with a coefficient (B) of 0.155, standard error (0.065), Beta value (β=0.141), and T-value (2.393) with (0.0158) significance level. There is also an impact of the control activities dimension on the implementation, with a coefficient (B) of 0.218, standard error (0.063), Beta value (β=0.205), and T-value (3.428) at (0.001) significance level. Additionally, there is an impact of the information and communication dimension on the implementation, with a coefficient (B) of 0.293, standard error (0.063), Beta value (β=0.292), and T-value (4.639) at a significance level (Sig.=0.000). Moreover, there is an impact of the monitoring and oversight dimension, with a coefficient (B) of 0.278, standard error (0.062), Beta value (β=0.254), and T-value (4.510) with a significance level (Sig.=0.000). However, there is no significant influence of the risk assessment dimension on the implementation, with a coefficient (B) of 0.071, standard error (0.068), Beta value (β=0.066), and T-value (1.053) at a significance level (Sig.=0.293).

Based on the multiple regression analysis' results, the first hypothesis is rejected, and the and the result indicating a statistically significant impact of internal control on the implementation of cloud-based ERP systems in Jordanian commercial banks.

H02: *"There is no statistically significant impact of internal control on cybersecurity in Jordanian commercial banks".*

Table (7): Testing the Second Research Hypothesis.

Dependent Variable	**Independent Variable**	**Unstandardized Coefficients**		**Standardized Coefficients**		
		Coefficient B	Standard Error	Coefficient β	Calculated T	Sig. T
Cybersecurity	Regulatory Environment	0.202	0.063	0.196	3.190	0.002
	Control Activities	0.007	0.062	0.007	0.117	0.907
	Risk Assessment	0.260	0.066	0.259	3.938	0.000
	Information and communication	0.150	0.062	0.160	2.429	0.016
	Monitoring and Oversight	0.313	0.060	0.306	5.203	0.000
Correlation Coefficient R			Coefficient of Determination R^2	Calculated F	Sig. F	
0.791			0.626	73.777	0.000	

the results for the impact of internal control on cybersecurity was shown in Table (7). The value of correlation coefficient is 0.791 (R), indicating a significant relationship between internal control and cybersecurity. The determination coefficient value is 0.626 (R^2), suggesting that internal control explains 62.6% of the variance in cybersecurity. The F-value is 73.777 at (0.000) significance level, confirming the significance of the regression at a significance level (α≤0.05), indicating a statistically significant influence of internal control on cybersecurity.

The regression coefficients show an impact of the control environment dimension on cybersecurity, with a coefficient (B) of 0.202, standard error (0.063), Beta value (β=0.196), and T-value (3.190) at (0.002) significance level. There is also an impact of the risk assessment dimension on cybersecurity, with a coefficient (B) of 0.260, standard error (0.066), Beta value (β=0.259), and T-value (3.938) with a significance level (Sig.=0.000). Moreover, there is an influence of the information and communication dimension on cybersecurity, with a coefficient (B) of 0.150, standard error (0.062), Beta value (β=0.160), and T-value (2.429) at (0.016) significance level. In addition, there is an impact of the monitoring and oversight dimension, with a coefficient (B) of 0.313, standard error (0.060), Beta value (β=0.306), and T-value (5.203) at zero significance level. However, there is no significant influence of the control activities dimension on cybersecurity, with a coefficient (B) of 0.007, standard error (0.062), Beta value (β=0.007), and T-value (0.117) at a significance level (Sig.=0.907).

Based on the multiple regression analysis results, the second research hypothesis is rejected, and the result confirms that there is a statistically significant impact of internal control on cybersecurity in Jordanian commercial banks.

H03: "There is no statistically significant impact of cybersecurity on the implementation of cloud-based enterprise resource planning systems in Jordanian commercial banks".

Table (8): Testing the Third Research Hypothesis.

Dependent Variable	**Independent Variable**	**Unstandardized Coefficients**		**Standardized Coefficients**		
		Coefficient B	Standard Error	Coefficient β	Calculated T	Sig. T
implementation of cloud-based enterprise resource planning systems	cybersecurity	0.753	0.051	0.704	14.852	0.000
Correlation Coefficient R			Coefficient of Determination R^2	Calculated F	Sig. F	
0.704			0.496	220.588	0.000	

As shown in Table (8), the impact of cybersecurity on the implementation of cloud-based enterprise resource planning systems in Jordanian commercial banks. using simple regression analysis. The correlation coefficient value is 0.704 (R), indicating a significant association between cybersecurity and the implementation of cloud-based ERP systems. The determination coefficient value is 0.496 (R^2), suggesting that cybersecurity explains 49.6% of the variance in the implementation of cloud-based ERP systems. The F-value is 220.588 at (0.000) significance level, confirming the significance of the regression at a significance level ($\alpha \leq 0.05$), meaning a statistically significant influence of cybersecurity on the implementation of cloud-based ERP systems. The regression coefficients show an impact of the cybersecurity dimension on the implementation, with a coefficient (B) of 0.753, standard error (0.051), Beta value (β=0.704), and T-value (14.852) at zero significance level.

Based on the simple regression analysis findings, the third research hypothesis is rejected, and the results indicating a statistically significant impact of cybersecurity on the implementation of cloud-based enterprise resource planning systems in Jordanian commercial banks.

H04: "There is no statistically significant impact of internal control on the implementation of cloud-based enterprise resource planning systems in Jordanian commercial banks, with cybersecurity as a mediating variable".

Table (9): Testing the Fourth Research Hypothesis.

Model Fit								
Statement	Chi2	df	GFI	CFI	IFI	NFI	RAMSEA	Significance level
implementation of cloud-based enterprise resource planning	12.015	5	0.963	0.983	0.983	0.972	0.079	0.000

GFI	Goodness of Fit mus proximity
CFI	Comparative Fit Index
IFI	Incremental Fit Index
NFI	Normed Fit Index
RAMSEA	Root mean square error of approximation

Table (9) showed that the Chi^2 value is statistically significant, as the significance level (Sig=0.000) is less than 0.05. Additionally, the value of chi-square divided by the degrees of freedom equals (2.403), which is less than 5. The square root index for the approximation of the average of error squares (RAMSEA= 0.079) did not exceed the value (0.08). On the other hand, the goodness-of-fit index reached (GFI= 0.963), approaching one. The closer it gets to one, the better the fit quality. Similarly, the comparative fit index (CFI= 0.983) also approaches one. The incremental fit index (IFI= 0.983) and the normed fit index (NFI= 0.972) both approach one, indicating that all indicators suggest a good model fit.

Table (10): Direct, Indirect, and Total Effects for the Fourth Main Hypothesis.

Variable	**Direct effect**		**Indirect effect**		**Total effect**	
	Internal Control	Cybersecurity	Internal Control	Cybersecurity	Internal Control	Cybersecurity
implementation of cloud-based enterprise resource planning systems	1.077	-	-	-	1.077	-
Cybersecurity	1.165	0.023	0.025	-	1.165	1.190

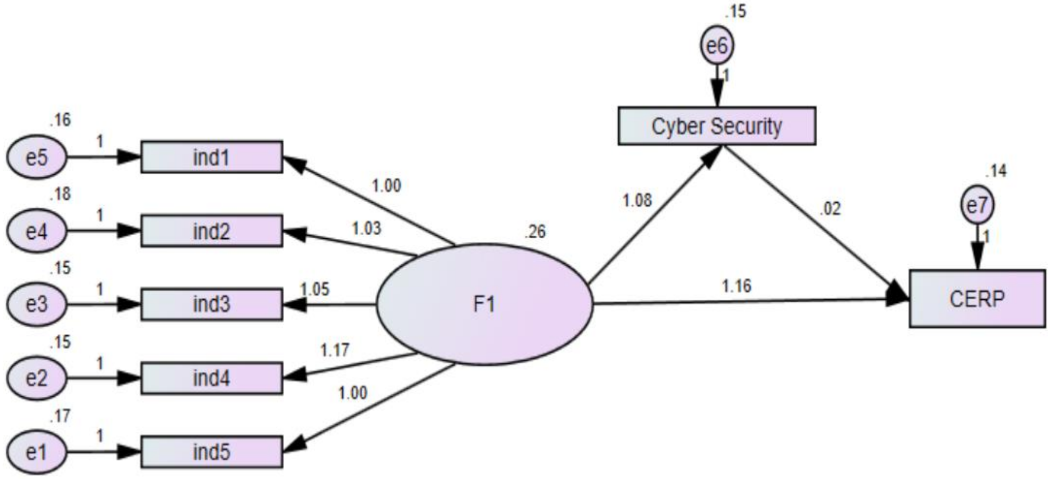
Table (10) reveals that "the significant direct effect of internal control on the implementation of cloud-based enterprise resource planning systems" was (1.077). Similarly, the significant direct effect of internal control on cybersecurity was (1.165). On the other hand, the "significant direct effect of cybersecurity on the implementation of cloud-based enterprise resource planning systems" was (0.023).

Furthermore, Table (10) demonstrates that the indirect effect of "internal control on the implementation of cloud-based enterprise resource planning systems through the mediating variable of cybersecurity" was (0.025). This is a statistically significant impact that confirms the meaningful mediating role of "cybersecurity in the relationship between internal control and the implementation of cloud-based enterprise resource planning systems". The total effect of internal control through the mediator on the cloud-based enterprise resource planning systems implementation was (1.190), signifying a statistically significant effect at a level less than 0.05.

Therefore, cybersecurity is considered a partial mediator. This confirms the positive role of cybersecurity as a mediating variable in the impact of internal control on the implementation of cloud-based enterprise resource planning systems when studying the collective dimensions of internal control. Hence, it can be concluded that there is an indirect effect of the combined dimensions of internal control on the implementation of cloud-based enterprise resource planning systems through cybersecurity as a mediating variable.

Based on the results of path analysis, the fourth hypothesis is not supported, which indicated that there is"a statistically significant effect of internal control on the implementation of cloud-based enterprise resource planning systems in Jordanian commercial banks, with cybersecurity as a mediating variable".

Figure (1): Hypothesis Four.



Results and Recommendations

Results

Based on the outputs of the data analysis and hypothesis testing, the following results have been obtained:

1-The results of the analysis showed a high level of interest among Jordanian commercial banks in internal control. This reflects the extent of interest and commitment of the management of these banks to enhance and improve their internal control mechanisms. It also indicates their efforts to mitigate potential risks by identifying and taking necessary measures to control them. Additionally, the results suggest a focus on enhancing transparency and accountability through defining responsibilities and ensuring the implementation of procedures and decisions according to established standards. The aim is to improve internal procedures and operations, providing opportunities for continuous improvement.

2-The analysis results demonstrated a high level of interest among Jordanian commercial banks in the implementation of cloud-based enterprise resource planning systems. This reflects the commitment of the management of these banks to adopt modern and advanced technology. They aim to improve efficiency, flexibility, and security in banking operations, and achieve comprehensive digital transformation within their environment.

3-The analysis results indicated a high level of interest among Jordanian commercial banks in cybersecurity. This reflects the significant attention given by the management of these banks to the growing digital threats. They adopt necessary measures and policies to protect systems, data, and sensitive information from electronic attacks and cyber threats. The results highlight their commitment to digital security and continuous efforts to improve it, providing secure and reliable banking services.

4- The results of testing the first main hypothesis demonstrated a statistically significant impact of internal control on the implementation of cloud-based enterprise resource planning systems in Jordanian commercial banks. This indicates the significant role and positive influence of internal control in the success and effectiveness of adopting and implementing cloud-based enterprise resource planning systems. Internal control helps identify and manage risks associated with the implementation of these systems, ensuring compliance with relevant security standards and regulations during the system's deployment. Additionally, internal control contributes to identifying and monitoring weaknesses in cloud-based enterprise resource planning systems, enhancing operational processes associated with the implementation of these systems.

5-The results of testing the second main hypothesis revealed a statistically significant impact of internal control on cybersecurity in Jordanian commercial banks. This underscores the significant role and positive influence of internal control in enhancing the level of cybersecurity within the bank. Internal control works to improve security measures within the bank, ensuring the presence of technological systems and policies to address cyber threats. It reinforces policies for defining and strictly enforcing permissions for employees and users, reducing the risks of unauthorized access and improper usage. Internal control also supports the implementation of monitoring and early detection systems for cybersecurity threats and electronic attacks, enabling timely responses. Moreover, it ensures the continuous enhancement of security policies, tools, and standards and monitors the compliance with security procedures.

6-The results of testing the third main hypothesis indicated a statistically significant impact of cybersecurity on the implementation of cloud-based enterprise resource planning systems in Jordanian commercial banks. This highlights the significant role and positive influence of cybersecurity in the successful implementation of cloud-based enterprise resource planning systems. Security measures contribute to providing data and information protection, enhancing trust and security for customers. Cybersecurity also plays a crucial role in minimizing the operational downtime of vital systems, achieving stability in operations, and reducing the likelihood of financial losses resulting from cyberattacks.

7-The results of testing the fourth main hypothesis showed a statistically significant impact of internal control on the implementation of cloud-based enterprise resource planning systems in

Jordanian commercial banks, with cybersecurity as a mediating variable. This indicates the crucial and positive role of internal control in enhancing cybersecurity when implementing cloud-based enterprise resource planning systems in Jordanian commercial banks.

Recommendations

Based on the above-mentioned results, the study recommends the following:

1- Commercial banks in Jordan should conduct continuous reviews and assessments of their internal control policies and procedures. They should update them periodically to align with legal and regulatory requirements and keep up with industry developments.

2-Provide ongoing training and development programs for internal control teams among commercial banks in Jordan to enhance their capabilities and knowledge of best practices and developments in the fields of internal control and accounting.

3-Jordanian commercial banks should identify their specific needs and objectives for cloud-based enterprise resource planning systems. They should carefully choose a system that aligns with their requirements and meets their goals.

4-Jordanian commercial banks should implement the best security practices to protect their cloud-based enterprise resource planning systems. This includes training employees on how to use the system securely and effectively.

5-The management of Jordanian commercial banks should adopt strong and clear cybersecurity policies and procedures. These should encompass access rules, delineation of security responsibilities, breach reporting procedures, and ensure understanding and compliance by all bank employees.

6-Jordanian commercial banks should develop incident response plans for cyber incidents and regularly test them to ensure the bank's readiness to handle any potential attacks.

7-Increase the commitment of Jordanian commercial banks to adhere to existing cybersecurity regulations and standards. This is crucial to maintain compliance and avoid legal violations.

References

- Al-Omari, Mohammed. (2020). Introduction to Cybersecurity. Dar Oran for Publishing and Distribution.
- Al-Suwaidi, Shibli Ismaeel. (2022). The role of internal control in combating corruption in procurement units in Palestinian public sector institutions. Arab Journal of Administration, 42(1), 73–94.
- Ben Alqama, Malika, & Saahi, Youssef. (2019). The role of financial technology in supporting financial and banking sectors. Al Ijtihad Journal of Legal and Economic Studies, 7(3), 85-107.
- Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, 33(4), 360-376.
- Christopher, D., Jennifer, O., & Chinedu, E. (2022). Administrative Internal Control System and Performance Effect: Focus on Telecommunication Industry in South-South and South-East Nigeria. **Linguistics and Culture Review,** 6: 169-193
- Despotović, A., Parmaković, A. & Miljković, M. (2023). Cybercrime and Cyber Security in Fintech. In *Digital Transformation of the Financial Industry: Approaches and Applications* (pp. 255-272). Cham: Springer International Publishing

- Goutam, R. K., & Verman, D. K. (2015). Top five cyber frauds. *International Journal of Computer Applications*, 119(7). 23-25.
- Gujarati, D.N. (2004). **Basic Econometrics**. (4thed.), UNA, New York: McGraw Hill
- Hanum, Z. & Ritonga, P. (2021). Pengaruh Sistem Pengendalian Internal terhadap Kinerja Kampus Islam Swasta di Kota Medan. **Seminar Nasional Teknologi Edukasi Dan Humaniora:** 811–815.
- Huseynov, T., Mammadova, U., Aliyev, E., Nagiyev, F., & Safiyeva, F. (2020). The impact of the transition to electronic audit on accounting behavior. *Economic and Social Development: Book of Proceedings*, *4*, 378-384.
- Intosai (2017). **Strategic Plan 2017-2022.** International Organisation of Supreme Audit Organisations. Available at: https://www.intosai.org/fileadmin/user_upload/EN_INTOSAI_Strategic_Plan_2017_22.pdf
- Jamm'e, Maryam, & Alash, Ahmed. (2021). The role of financial technology in promoting Islamic finance. Al Ibtida Journal, University of Blida, 11(1), 454-467.
- Lennox, C. S. & Wu, X. (2022). Mandatory Internal Control Audits, Audit Adjustments, and Financial Reporting Quality: Evidence from China. **The Accounting Review,** 97(1): 341-364.
- Qourin, Haj Qouidar, Abu Bakr Al-Siddiq, Qaidwan, and Ibn Yusuf, Ahmed. (2019). The role of internal control in mitigating banking risks: A case study of accredited banks in Algeria (with reference to international models). Academy for Social and Human Studies, 12(1), 35-45.
- Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for cyber security in schools: the human factor. *Educational Planning*, 27(2), 23-39.
- Ryabov, O. V. (2021). Organising Issues of Operative System of Internal Control in Banking Sector. Consulting company Ucom, USA.
- Sekaran, U. & Bougie, R. (2016). Research Methods for Business: A Skill Building Approach. John wiley and sons, USA.
- Shamsuddin, A., Adam, M. A., Adnan, S. A., & Yasin, Y. M. (2018). The effectiveness of internal audit function in managing cyber security in Malaysia's banking institutions. *International Journal of Industrial Management,* 8 (4).
- Sharabsha, Mona, & Bakhoush, Bushra. (2019). Internal Control on Banks (Published Master's Thesis). Mohammed Cherif Messaadia University, Souk Ahras, Algeria.
- Stevens, R., Dykstra, J., Everette, W. K., Chapman, J., Bladow, G., Farmer, A. & Mazurek, M. L. (2020, February). Compliance Cautions: Investigating Security Issues Associated with US Digital-Security Standards. *In NDSS*.
- Wolden, M., Valverde, R., & Talla, M. (2015). The effectiveness of COBIT 5 information security framework for reducing cyber-attacks on supply chain management system. *IFAC-Papers Online*, 48(3), 1846-7852.