Kurdish Studies
Jan 2024
Volume: 12, No: 1, pp. 3556-3568
ISSN: 2051-4883 (Print) | ISSN 2051-4891 (Online)
www.KurdishStudies.net

Received: October 2023 Accepted: December 2023
DOI: https://doi.org/10.58262/ks.v12i1.252

The Impact of Cyber Governance on Financial Technology Implementation: The Mediating Role of Internal Control Effectiveness

Associate Prof Hani Al-Rawashdeh[1], Associate Prof. Ala, Rabie[2], Prof. Osamah Abdul-Munim Ali[3], Assistant Prof. Hebah Rabie[4], Assistant Prof. Deaa Al-Deen Al-Sraheen[5]

Abstract

The current study seeks to identify the impact of cyber governance on the implementation of financial technology, in addition to the mediating role of internal control effectiveness in Jordanian commercial banks using a descriptive-analytical approach to achieve the research objectives. A comprehensive survey method was employed encompassed all the Jordanian commercial banks listed on the Amman Stock Exchange (ASE), resulting in a sample size of 12 Jordanian banks. The designed questionnaire was distributed to employees at various management levels in the all Jordanian commercial banks and analyzed using each of (SPSS) and the AMOS softwires. The study yielded several results, with the most significant being that there is a significant impact of cyber governance on the implementation of financial technology through the mediating role of internal control effectiveness. This finding indicates the positive influence of cyber governance on financial technology implementation, achieved through its direct impact on internal control effectiveness, which in turn affects the implementation of financial technology in Jordanian commercial banks. Key recommendations emphasize the necessity for Jordanian commercial banks to allocate necessary resources for the development and enhancement of cyber governance. This includes providing appropriate technology, training employees in information security and cyber threat recognition, and investing in advanced security and protection systems. Additionally, it is recommended for Jordanian commercial banks to pay greater attention to enhancing their internal control effectiveness. This can be achieved by defining and clarifying roles and responsibilities for employees within the bank, developing internal control policies and procedures to optimize financial technology usage, ensure operational safety and efficiency, protect financial information, and mitigate potential risks.

Keywords: *Cyber Governance, Financial Technology, Internal Control Effectiveness, Jordanian Commercial Banks.*

Introduction

Due to a series of financial scandals involving numerous large companies in recent years, many countries and organizations have increasingly focused on the concept of cyber governance. This attention stems from the various benefits highlighted by different studies regarding the role of governance in improving and developing financial outcomes for banks and companies.

Furthermore, the rapid advancement of technological evolution and the emergence of the

[1] Jerash university, Faculty of Business, Accounting department, Jerash. Jordan Email: hrawashdeh73@yahoo.com
[2] Jerash university, Faculty of Business, Accounting department, Jerash. Jordan Email: rabeiala008@gmail.com
[3] Jerash university, Faculty of Business, Accounting department, Jerash. Jordan *Corresponding Author Email: al_osama@yahoo.com
[4] Jerash university, Faculty of Business, Accounting department, Jerash. Jordan Email: drhebarabee@gmail.com
[5] Al al-Bayt University, School of Business, Accounting department, Mafraq. Jordan Email: Dr-Deaa@aabu.edu.jo

modern digital and financial technology revolution have introduced various contemporary concepts to the banking sector. This sector, with its financial and accounting aspects, is greatly impacted. The banking sector is well-suited to benefit from financial technology due to several reasons: it generates a substantial amount of data, faces challenges in securing and maintaining data, and struggles with managing associated costs. Furthermore, the banking sector is governed by numerous evolving rules and regulations, being a pioneering sector in systems computerization. Such systems play a pivotal role in the success, discipline, and accurate decision-making and investments of institutions.

Consequently, commercial banks are compelled to enter the realm of digitization by engaging with financial technology within its broad concept. This engagement has led to the enforcement of laws and regulations by competent authorities such as the Central Bank of Jordan that govern the sector's operations and the implementation of digital technology. These guidelines create a new form of advanced cyber governance in the banking sector, aligned with the modern digital environment. This is aimed at ensuring internal control efficiency capable of comprehending the risks of operation within a high-tech environment, distinct from traditional banking sector control methods.

As such, internal control is considered one of the tools of cyber governance, playing a crucial role in safeguarding banks. It assists in managing and protecting against internal risks related to management and employees, as well as external risks within the business environment. This, in turn, ensures the protection of stakeholders' interests, including major shareholders, investors, government and institutional bodies, as well as employees within these banks. Therefore, the current research seeks to explore the impact of cyber governance on financial technology implementation, considering the mediating role of internal control effectiveness in Jordanian commercial banks.

Research Problem

The problem of the current study can be summarized through that this study's attempt to address the following questions:

Key Question 1: Does cyber governance, represented by its dimensions (cybersecurity governance requirements, cybersecurity policy, cybersecurity program, cyber risk assessment and management, and cybersecurity information management), have an impact on the implementation of financial technology in Jordanian commercial banks?

Subsidiary questions generated from the key question 1 are:

1. ” Do the cybersecurity governance requirements have an impact on the implementation of financial technology in Jordanian commercial banks”?
2. “Does the cybersecurity policy have an impact on the implementation of financial technology in Jordanian commercial banks”?
3. 3. “Does the cybersecurity program have an impact on the implementation of financial technology in Jordanian commercial banks”?
4. “Does the cyber risk assessment and management have an impact on the implementation of financial technology in Jordanian commercial banks”?
5. “Does the cybersecurity information management have an impact on the implementation of financial technology in Jordanian commercial banks”?

Key Question 2: Does cyber governance have an impact on the effectiveness of internal control in Jordanian commercial banks?

Key Question 3: Does internal control effectiveness have an impact on the implementation

of financial technology in Jordanian commercial banks?

Key Question 4: Does cyber governance have an impact on the implementation of financial technology, with the presence of internal control effectiveness as a mediating role, in Jordanian commercial banks?

Research Objectives

Through the research problem that mentioned, the most important objectives that seeks to be achieved by the current study can be summarized as follows:

1. To examine the impact of cybersecurity governance requirements on the implementation of financial technology in Jordanian commercial banks.
2. To examine the impact of cyber governance on the internal control effectiveness in Jordanian commercial banks.
3. To identify the impact of internal control effectiveness on the implementation of financial technology in Jordanian commercial banks.
4. To Examine the impact of cyber governance on the implementation of financial technology, with the presence of internal control effectiveness as a mediating variable, in Jordanian commercial banks.

Study Hypotheses

The current study aims to test the following hypotheses at a significance level ($\alpha \leq 0.05$):

Key Hypothesis (H01): *There is no statistically significant impact of cyber governance, represented by its dimensions (cybersecurity governance requirements, cybersecurity policy, cybersecurity program, cyber risk assessment and management, and cybersecurity information management) on financial technology implementation in Jordanian commercial banks.*

From the key hypothesis 1, the following sub-hypotheses are branched out:

H01-1: *There is no statistically significant impact of cybersecurity governance requirements on financial technology implementation in Jordanian commercial banks.*

H01-2: *There is no statistically significant impact of cybersecurity policy on financial technology implementation in Jordanian commercial banks.*

H01-3: *There is no statistically significant impact of cybersecurity program on financial technology implementation in Jordanian commercial banks.*

H01-4: *There is no statistically significant impact of cybersecurity risk assessment and management on financial technology implementation in Jordanian commercial banks.*

H01-5: *There is no statistically significant impact of cybersecurity information management on financial technology implementation in Jordanian commercial banks.*

Key Hypothesis 2 (H02): *There is no statistically significant impact of cyber governanceon the internal control effectiveness in Jordanian commercial banks.*

Main Hypothesis 3 (H03): *There is no statistically significant impact of internal control effectiveness on financial technology implementation in Jordanian commercial banks.*

Main Hypothesis 4 (H04): *There is no statistically significant impact of cyber governance on the financial*

technology implementation, with the presence of internal control effectiveness as a mediating variable, in Jordanian commercial banks.

The Theoretical Background

Cybersecurity Governance: An Intellectual Introduction

When delving into the topic of cybersecurity governance in the context of advanced financial technology applications and their impact on the effectiveness of internal control systems in banks, it is essential to understand the nature of cybersecurity governance. Cybersecurity governance serves as protection for networks, operational technology systems and information technology systems in banks, including their components of software, hardware, data, and services against any unauthorized access, disruption, alteration, entry, use, or exploitation (National Cybersecurity Authority, 2018). The Central Bank of Jordan sees cybersecurity governance as crucial for availability and protecting of bank-related-information, maintaining the confidentiality, and its integrity within cyberspace from any cyber threat. This is achieved through a set of means, policies, guidelines, and best practices (Central Bank of Jordan, 2022). Researchers agree with Al-Saeed (2019) and Ali et al. (2020) that in the context of cybersecurity, governance refers to the administrative principles, rules, and methods followed by an entity to regulate decision-making authorities, define responsibilities, and enforce accountability in executing tasks and duties related to protecting the entity from electronic attacks or misuse of information assets while ensuring the continuity of operational processes in case of incidents or disasters. Consequently, cybersecurity governance aims to direct, monitor, guide, enhance, and facilitate the coordination of efforts among relevant entities, aligning with the interests and aspirations of the entity's stakeholders, without violating agreements and laws to which the entity is a party.

The Intellectual Reality of Financial Technology

There are intellectual opinions among researchers that stem from various conceptual backgrounds when attempting to understand the intellectual concept of financial technology. Leong and Sung (2018) view it as innovative design that enhance financial service operations by suggesting technological tools to address different business cases, that may generate new business models. On the other hand, Abdulrahim and Ben Qadour (2018) describe it as "products and services that rely on technology to improve the quality of traditional financial services." Abu Karsh defines it (2019) as a technological invention employed in financial services, contributing to the development of new technology that competes with traditional financial markets. Boumod et al. (2020) characterize it as technologies used to improve or provide financial services and ways people interact with money through electronic inventions, financial transfers, payments, accounting records, and electronic wallets.

Therefore, researchers consider financial technology as innovative technological methods and techniques in the financial field. The purpose is for banks to utilize advanced digital technology means to provide financial services characterized by high quality.

Researchers believe that within the realm of cybersecurity governance, banks should formulate strategies, prioritize, and make decisions regarding the implementation of advanced financial

technology applications. This includes determining where, when, and how these technologies will be applied. For example, many banks prioritize technological applications that assist them in internal control, risk management, and compliance, often referred to as Regulatory Technology (Reg Tech). Additionally, banks may gradually adopt modern technologies, starting with support functions, front-end facilities, followed by middle and back-office facilities (Tierno, 2021). This approach aims to balance reaping benefits and accumulating expertise on one hand, and controlling risks on the other, based on precise calculations considering the opportunities, savings, risks, and expenses these technologies may bring. With the advancement of digital technology, banks have become capable of offering sophisticated financial services that meet the needs of their clients at lower costs. Financial technology utilizes innovative information systems, automated operational technology, and modern digital technology to provide more cost-efficient financial services. These services span from asset management to lending, portfolio investment consulting, big data analytics to alternative payment systems. This transformation in banking and financial intermediation is made possible through the adoption of financial technology (Al-Anzi, 2020).

Internal Control Systems in Banks under the Presence of Cybersecurity Governance and Advanced Financial Technology

The presence of pioneering cybersecurity governance and advanced financial technology applications in Jordanian banks has contributed to the establishment of effective control systems. The importance of having an advanced and efficient internal control system in the context of financial technology is increasing for several reasons. One such reason is that the processing and storage of data for accounting operations are done in a non-readable format, making it challenging for individuals to monitor and ensure the accuracy and objectivity of this data, unlike traditional systems (Feyen et al., 2021).

Moreover, a digitally supported control system is capable of processing large datasets, whether accounting or administrative, surpassing manual processing and reducing the likelihood of errors (Douglass et al., 2022). Traditional internal control systems may provide more flexibility, leading unscrupulous employees to embezzle significant amounts from the organizations they work for (COBIT, 2019). Therefore, banks need effective means to manage and assess risks to protect customer data. All banks are required to conduct continuous or at least annual assessments of technology risks, especially when introducing new systems (Qurain et al., 2019).

Researchers emphasize the necessity for banks and their regulatory entities to adopt a comprehensive system for cybersecurity governance and advanced financial technology as an integral part of cybersecurity governance. This aims to create alignment between the bank's objectives and its internal control system on one hand, and between financial technology and the mitigation of risks, as well as the enhancement of regulatory and organizational compliance, on the other hand.

Methodology

Research Population and Sample

The population of the current research consists of all Jordanian commercial

banks listed on the ASE, there were (12) commercial banks worked in Jordan as of the end of 2022. Thus, through employing the comprehensive survey methodology, the final sample included all (12) Jordanian commercial banks listed on the ASE.

Unit of Study Analysis

This unit of analysis in the current study was composed of a sample of employees at various management levels of top, middle, and lower management levels within the head office of each bank. This included general managers and their deputies, head of departments, such as the dept. of customer services, financial facilities, internal control, head of the lending, debt and credit, open market, operations department, investments and foreign operations, banking system supervision, internal audit and regulation and computer and Information dept.

Due to the unavailability of an exact count of employees in above mentioned positions, 20 questionnaires were distributed in each bank to reach the employees in the above-mentioned positions as possible. The total of distributed questionnaires was (240) questionnaires, (202) were retrieved as valid questionnaires for statistical analysis with a retrieval rate of (84.2%) of the total distributed questionnaires.

Analysis

Before starting the process of analysis and test the research hypotheses, it is necessary to ensure that there are no violations of the basic assumptions of linear regression. This is to ensure that the research data is ready for the analysis process.

To test the stability (internal consistency) of the study instrument (the questionnaire), the Cronbach's Alpha Coefficient was used to measure the attitudes of the individuals towards the research variables. Sekaran and Bougie (2016) pointed out that the research instrument is deemed reliable and consistent when the value of this test was (0.70) or above. Table (1) shows that the Cronbach's Alpha coefficient was calculated for the dimensions related to each variable of the research model.

(Table 1): Cronbach's Alpha Coefficient Values (Internal Consistency Measure).

No.	Variable	No. of items	Alpha's value
1	Cyber security governance requirements	5	0.798
2	Cyber Security Program	5	0.836
3	Cyber security policy	5	0.874
4	Cyber information security management	5	0.859
5	Cyber risk assessment and management	5	0.851
6	Cyber governance	25	0.954
7	Financial technology implementation	5	0.814
8	Internal Control Effectiveness	5	0.857
	Study instrument	35	0.966

Cronbach's Alpha coefficient for the questionnaire items ranged from (0.798) to (0.954), and the value for all items was (0.966). Consequently, all values of this test were greater than (0.70), indicating consistency among the questionnaire items, the reliability of the research instrument, and its suitability for statistical analysis.

The linear assumption is one of the most important key assumptions that should be verified in addition to the make sure that the data is free from collinearity issues. before starting the data analysis process.

(Table 2): Study Model Variables Correlation Matrix.

	CGR	**CSP**	**CSP**	**CISM**	**CRAM**	**CG**	**CTI**	**ICE**
CGR	1.000							
CSP	0.666**	1.000						
CSPR	0.714**	0.749**	1.000					
CISM	0.637**	0.756**	0.691**	1.000				
CRAM	0.662**	0.719**	0.666**	0.788**	1.000			
CG	0.831**	0.888**	0.873**	0.896**	0.884**	1.000		
CTI	0.675**	0.743**	0.727**	0.772**	0.772**	0.845**	1.000	
ICE	0.647**	0.624**	0.667**	0.695**	0.761**	0.777**	0.732**	1.000

Where: CGR=Cyber security governance requirements, CSP= Cyber Security Policy, CSPR= Cyber Security Program, CISM=Cyber information security management, CRAM= cyber risk assessment and management, CG= Cyber governance, FTI= Financial technology implementation, ICE=Internal Control Effectiveness
(**) denotes significance at the 0.01 level.

Table (2) shows that the high correlation coefficient level was between the "Cyber Information Security Management" and "Cyber Risk Assessment and Management," which reached (0.788). The coefficient value that is less than (0.90), indicating no violation of collinearity issue between research variables. While the coefficient value that above (0.90) indicating of multicollinearity issue (Sekaran & Bougie, 2016).

On the other hand, significant linear relationships were observed between the research variables in the research model. Correlation coefficients between "Cyber Governance," "Financial Technology Implementation," and "Internal Control Effectiveness" were significant. This supports the research hypotheses of the current study.

Descriptive Analysis

Descriptive statistics are one of the most important analytical tools in research methodology and as an essential part of the analysis process, as it helps to understand phenomena under investigation and their details in an accurate and detailed manner., as they describe and summarize the research data in quantitative ways as shown in table 3 through focusing on the means and standard deviations, in addition to the relative importance rankings were relied upon to describe the respondents' answers to the items and dimensions of the questionnaire.

(Table 3): Description of Study Model Variables and Their Sub-Dimensions.

No.	**Variable**	**Mean**	**Std. Dev.**	**Rank**	**Relative importance**
1	CGR	4.222	0.555	1	High
2	CSPR	4.163	0.601	3	High
3	CSP	4.184	0.645	2	High
4	CISM	4.100	0.682	4	High
5	CRAM	4.088	0.640	5	High
6	CG	4.152	0.547	-	High
7	FTI	4.044	0.647	-	High

8	ICE	4.141	0.697	-	High

Where: CGR=Cyber security governance requirements, CSP= Cyber Security Policy, CSPR= Cyber Security Program, CISM=Cyber information security management, CRAM= cyber risk assessment and management, CG= Cyber governance, FTI= Financial technology implementation, ICE=Internal Control Effectiveness

Table (3) shows that the sample respondents' attitudes were towards high level of relative importance of "Cyber security governance requirements", with a mean of (4.222) and a standard deviation of (0.555). While the dimension "Cyber Risk Assessment and Management" appeared last in the fifth rank with a mean of (4.088) and a standard deviation of (0.640). The table also shows that the sample respondents' attitudes were towards high relative importance of financial technology implementation, with a mean of (4.044) and a standard deviation of (0.647). Similarly, the "Internal Control Effectiveness" appeared with an average of (4.141) and a SD of (0.697), indicating high level of relative importance.

Factor Analysis Test

This type of analysis is a form of factor analysis and is referred to Confirmatory Factor Analysis (CFA) which is which is one of the important part of SEM "Structural Equation Modeling". The purpose of conducting this kind of test to examine the consistency of the dimensions of the research model with its theoretical structure. Table 4, presents several indicators of quality and goodness of fit:

(Table 4): Confirmatory Factor Analysis.

Index	CMIN/DF	CFI	GFI	NFI	RMSEA
Refence Value	<5	>0.90	>0.90	>0.90	<0.10
Calculated Value	3.956	0.968	0.929	0.958	0.078

The results shown in Table (4) indicate that the value of squared chi value divided by its DFto estimate one sense of variable importance. Value is (CMIN/DF = 3.956), which is less than 5. Additionally, the value of (RMSEA) is Approximately (0.078), a value close to (0). In addition, the goodness-of-fit index (GFI) is (0.929), approaching 1, which indicates a good fit. Similarly, the Comparative Fit Index (CFI) is (0.968), also approaching 1, and the Normed Fit Index (NFI) is (0.958), also approaching 1. This suggests that all indicators refer to good model fit.

Hypotheses Testing

This study was based on four basic hypotheses as previously mentioned.In order to test the research hypotheses, Path Analysis has been used, each of H01, H02 and H03 were tested using the results of direct regression "Regression Estimates". Meanwhile, the H04 was examined through the outcomes of both indirect and direct effects as well as the total effect. Table (5) displays the results of testing the first three research hypotheses (H01, H02 and H03).

Table (5) The Outcomes of the Direct Regression Analysis.

Hypothesis	Regression Path	Estimate Regression Coefficient	S.E Standard Error	C.R Critical Ratio	P Significance level
H01	Cyber Security→ Financial technology implementation	0.958	0.090	10.681	0.000
H02	Cyber Security→ Internal control effectiveness	1.005	0.067	14.923	0.000

H03	Internal control effectiveness → Financial technology implementation	0.054	0.021	2.571	0.009

As for the H01 hypothesis, the regression coefficient of "Cybersecurity Governance" on "Financial Technology implementation" was (Estimate=0.958). The CR value was (10.681), with a P value (0.000). Such results indicating a significant positive impact of Cybersecurity Governance on Financial Technology implementation, which is support our first research hypothesis H01. Therefore, the first research hypothesis (H01) is accepted.

Table 5 shows that there is a positive and significant impact between the "Cybersecurity Governance" and "Internal Control Effectiveness" based on the values of regression coefficient of the variable (Estimate=1.005), The CR value (14.923), with a P value of (0.000). Thus, the second research hypothesis H02 is also supported and accepted.

As for the impact of Internal Control Effectiveness on Financial Technology implementation in Jordanian commercial banks. The results mentioned in Table 5 show that there is a significant and positive impact of Internal Control Effectiveness on Financial Technology implementation based on the values of Estimate (0.054). the value of CR was (2.571), with a significance level (P=0.009). This result supports our third research hypothesis. Thus, the H03 is accepted and supported.

Table 6 shows the results of testing the the mediating role of "Internal Control Effectiveness in the relationship between Cybersecurity Governance and Financial Technology implementation", results are as follows:

Table (6) Presents the Indirect, Direct, and Total Effect Coefficients.

	Direct effect		**Indirect effect**		**Total effect**	
	Cyber Security	Internal Control Effectiveness	Cyber Security	Internal Control Effectiveness	Cyber Security	Internal Control Effectiveness
Internal Control Effectiveness	1.005	-	-	-	1.005	-
Financial technology implementation	0.958	0.054	0.055	-	1.013	0.054

As shown in Table (6), there is a a significant direct effect of "Cybersecurity Governance on Internal Control Effectiveness with a value of (1.005), whereas the significant direct effect of "Cybersecurity Governance on Financial Technology implementation" which was (0.958). On the other hand, the results also show that there is a significant direct effect of "Internal Control Effectiveness on Financial Technology implementation" at the value of (0.054).

Furthermore, Table (6) indicates that the value of indirect effect of "Cybersecurity Governance on Financial Technology implementation, with the mediating variable of Internal Control Effectiveness" was (0.055). This considered as a significant effect that confirms there is a mediating role of "Internal Control Effectiveness in the relationship between Cybersecurity Governance and Financial Technology implementation". While the total effect value of "Cybersecurity Governance with the mediating variable of Internal Control Effectiveness" was (1.013), a significant effect at a significance level below 0.05. Therefore, the role of Internal Control Effectiveness is deemed partial mediation.

These results support the positive mediating role of "Internal Control Effectiveness" in the impact of "Cybersecurity Governance on Financial Technology implementation". Hence, it can be concluded that there is an indirect effect of "Cybersecurity Governance on Financial Technology implementation with the presence of Internal Control Effectiveness as a mediating variable". Consequently, H04 which stated that there is a statistically significant impact of Cybersecurity Governance on Financial Technology implementation through the mediating role of Internal Control Effectiveness was accepted and supported.

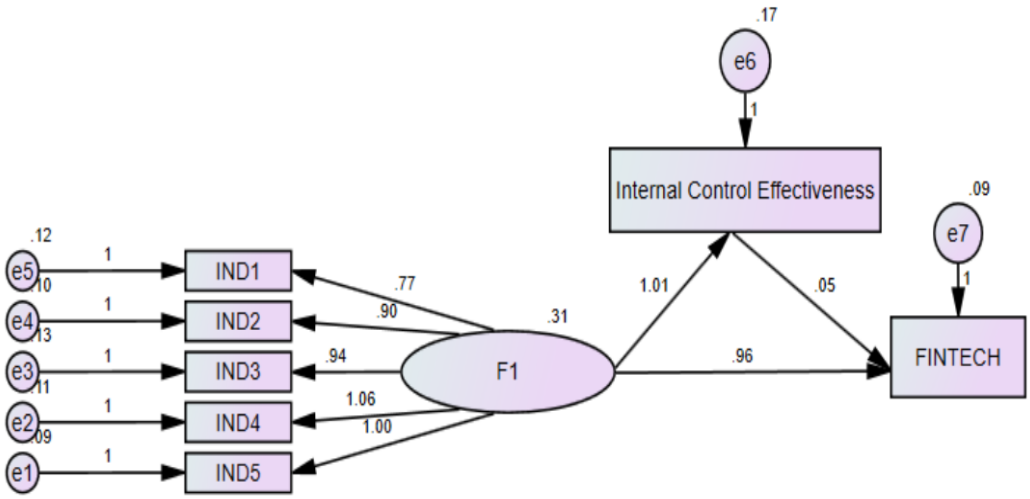

Figure (1): Testing the Fourth Research Hypothesis (H04).

Discussion and Recommendations

According to the previously mentioned results, there is a high relative importance of "Cybersecurity Governance" in Jordanian commercial banks. All dimensions have shown a high level of significance. This signifies that the management of commercial banks in Jordan is aware of the importance of cybersecurity and information technology in securing and protecting their electronic systems and data from cyber threats. This results also includes enhancing the security of electronic banking operations, safeguarding customers' sensitive financial and personal data, and ensuring confidentiality. These measures contribute to building trust among customers and investors and protecting the bank's reputation.

The high relative importance of "Financial Technology implementation" in Jordanian commercial banks. This indicates that the management of these banks acknowledges the significance of digital transformation and the use of technology to enhance their banking operations and services. This strategic shift aims at achieving operational efficiency, cost reduction, and delivering more efficient and flexible services to customers, better meeting their needs.

In addition, the high relative importance of "Internal Control Effectiveness" in Jordanian commercial banks. This highlights the recognition of the importance of an effective internal control system by the management of Jordanian banks. Such a system contributes to improving performance, achieving objectives, enhancing the safety of banking operations, and mitigating potential risks. This, in turn, increases the confidence of customers, shareholders, and other

stakeholders in the bank, while also reinforcing its reputation and competitive capabilities in the banking market.

There is a statistically significant impact of "Cybersecurity Governance on Financial Technology implementation" in Jordanian commercial banks. This signifies that the presence of an effective cybersecurity governance system contributes to enhancing security and confidence in the utilization of financial technology, improving its implementation, and ensuring the safety of customers' and users' financial data and information. This is achieved through the protection provided by cybersecurity measures against cyber threats, breaches, and the reduction of potential risks associated with financial technology.

The results also concluded that there is a statistically significant impact of "Cybersecurity Governance on the Internal Control effectiveness" in Jordanian commercial banks. such result indicates a positive influence of an effective cybersecurity governance system on the efficiency of internal control within Jordanian commercial banks. The presence of a high-quality and effective cybersecurity governance system contributes to enhancing and improving the internal control process and ensuring the safety of operations and protection against potential financial risks. Maintaining the security of the cybersecurity system and guarding against cyber threats and breaches ensures a secure and trustworthy environment for financial operations and information.

There is a statistically significant impact of "Internal Control Effectiveness on the Financial Technology implementation" in Jordanian commercial banks. This points to the positive effect of enhancing internal control effectiveness on the implementation and utilization of financial technology. Improving the quality and effectiveness of internal control mechanisms contributes to enhancing and improving the application of financial technology by ensuring the safety and security of financial operations and information, and by adhering to financial standards and regulations.

The statistically significant impact of "Cybersecurity Governance on the Financial Technology implementation "through the mediating role of Internal Control Effectiveness in Jordanian commercial banks" is shown in the hypotheses testing results. This suggests the positive impact of "Cybersecurity Governance on financial technology implementation", achieved through its direct influence on Internal Control Effectiveness. In turn, Internal Control Effectiveness impacts the implementation of Financial Technology. The presence of a legal, institutional, and technical framework that ensures effective and secure management of cybersecurity challenges protects sensitive information, ensures operational continuity, and minimizes potential cyber risks. This contributes to maintaining operational integrity, internal control within the bank, and activating the role of internal control in risk monitoring, assessment, and compliance with financial laws, regulations, and standards. Consequently, this enhances trust, security, and the implementation of financial technology.

Recommendations

- Based on the results of the study and the discussion that mentioned previously, this study concludes with a set of recommendations that would spot the light on some aspects that can be presented to the top management of commercial banks operating in Jordan, in addition to decision-makers and regulators in this sector. Jordanian commercial banks should allocate the necessary resources for the development and enhancement of cybersecurity governance. This

includes providing appropriate technology, training employees on information security and cyber threat recognition, and investing in advanced security and protection systems.

- Continuous improvements in internal operations and the implementation of effective internal control procedures should be undertaken by Jordanian commercial banks. This ensures the proper implementation of security policies and practices, effective cyber threat monitoring, and efficient response mechanisms.
- Regular updates and upgrades of systems and software should be conducted by Jordanian commercial banks to address security vulnerabilities and enhance cybersecurity.
- Regular reports and reviews should be conducted by Jordanian commercial banks to assess the effectiveness of cybersecurity governance measures and financial technology strategies. Necessary actions should be taken to improve performance and security.
- A greater emphasis on enhancing internal control effectiveness is recommended for Jordanian commercial banks. This can be achieved through defining roles and responsibilities of employees within the bank, developing policies and procedures for internal control, and ensuring proper use of financial technology to ensure operational safety, efficiency, protection of financial information, and risk reduction.
- Regular assessment of the performance of the internal control system and the risks faced by Jordanian commercial banks is advised. Measuring achieved results, identifying weaknesses, prioritizing areas for improvement, and implementing necessary actions are crucial.
- Effective communication channels should be established within different departments of Jordanian commercial banks to improve information flow and knowledge exchange in the field of internal control.
- Jordanian commercial banks should adopt a clear strategy for financial technology usage, encompassing goals and plans for technology development and effective utilization. A specialized technical team should be provided to support and maintain financial technology, ensuring swift response to any technical issues or glitches.
- Continuous development and improvement of technological infrastructure and financial applications, including networks, devices, software, mobile applications, and electronic platforms, are recommended. Regular updates should be applied to stay current with modern technological advancements.
- Strong cybersecurity governance frameworks should be established by Jordanian commercial banks to ensure enhanced security and efficiency in banking operations and the protection of financial information. This contributes to the successful implementation of financial technology.

References

Abdulrahim, Waheeba, and Ben Qadour, Ashwaq (2018). Trends in Financial Technology in Light of Successful Companies' Experiences. Al Ijtihad Journal of Economic and Legal Studies, 7(3), 11-35.

Abu Karsh, Shareef (2019). The FinTech Era. Journal of Financial and Banking Studies, 1(27), 8-12.

Al-Anzi, Salem (2020). The Role of Digital Transformation in Activating Mechanisms for Regulating Financial Technology Risks and its Impact on Electronic Banking Services in the Face of the COVID-19 Crisis: A Field Study on Kuwaiti Banks. The Scientific Journal for Financial and Administrative Studies and Research, 6(1), 127-150.

Al-Saeed, Fadi, (2019), Messages on Cybersecurity Governance, retrieved 25 /9/ 2023 from

:https://www.linkedin.com.

Ali Osamah, Matarneh Ala, Almalkawi, Ahmed & Mohamed, Hamzeh (2020). The Impact of Cyber Governance in Reducing the Risk of Cloud Accounting in Jordanian Commercial Banks-from the Perspective of Jordanian Auditing Firms Modern Applied Science; Published by Canadian Center of Science and Education.Vol. 14، No. 3.

Boumod, Iman, Shawi, Shafiha, and Matraf, Awatef (2020). Financial Technology Innovations and Their Role in Enhancing the Performance of Arab Islamic Banks. Economic Insights Journal, 10(1), 334-348.

Central bank of Jordan (2022).Banking sector manual . retrieved 04/10/2023 :https://www.cbj.gov.jo/Pages/viewpage.aspx?pageID=141

COBIT 2019, (2018). A business framework for the governance and management of enterprise IT. Rolling Meadows, IL.: ISACA.

Douglass, A., Martínez, G. M. F. & Holmes, A. F. (2022). Bringing COSO to Life: Engaging Students with Real World Examples of Internal Controls Using Digital Storytelling. Journal of Accounting Education, 58.

Feyen, E., Frost, J., Gambacorta, L., Natarajan, H. & Saal, M. (2021). Fintech and the Digital Transformation of Financial Services: Implications for Market Structure and Public Policy. BIS Papers,(117): 1-64

Gujarati, D.N. (2004). Basic Econometrics. (4th ed.), UNA, New York: McGraw Hill

Leong, K., & Sung, A. (2018). Fin tech financial Technology: what is it and how to use technologies to create business value in fin tech way? .*International Journal of Innovation, Management and Technology*, 9(2), 74-78.

Qurain, Haj Ghouidar, Abu Bakr Al-Siddiq, Qaidwan, and Ibn Youssef, Ahmed. (2019). The Role of Internal Control in Mitigating Banking Risks: A Case Study of Accredited Banks in Algeria (with Reference to International Models), The Academy for Social and Humanities Studies, 12(1): 35-45.

National Cybersecurity Authority (2018) retrieved (23/ 9 / 2023) from : https://nca.gov.sa/

Sekaran, U. & Bougie, R. (2016). Research Methods for Business: A Skill Building Approach. John wiley and sons, USA.

Tierno, P. (2021). Bank Use of Cloud Technology. Retrieved (30/8/2023) , Congressional Research Service Available at: https://crsreports.congress.gov/product/pdf/IF/IF11985