Asian Economic and Financial Review
ISSN(e): 2222-6737
ISSN(p): 2305-2147
DOI: 10.55493/5002.v15i10.5653
Vol. 15, No. 10, 1592-1603.

URL: www.aessweb.com

Compliance with regulatory, legislative and contractual requirements for cyber security and its impact on the continuity of the Jordanian banking sector

Ola Khresat

Accounting Department, Zarqa University, Zarqa 13110, Jordan.
Email: okhresat@zu.edu.jo

Article History
Received: 16 October 2024
Revised: 13 August 2025
Accepted: 22 September 2025
Published: 31 October 2025

Keywords
Banking sector
Continuity
Contractual requirements
Legislative requirements
Regulatory requirements.

JEL Classification:
K100; K220; K240; G210.

ABSTRACT

This study aimed to research the compliance of the banking sector with the regulatory, legislative, and contractual requirements of cybersecurity and its impact on its continuity. The study focused on the Jordanian banking sector. A questionnaire was designed as a tool for the study and developed in a manner that covers all the variables of the study. It was distributed to the banking sector, with a total of 105 questionnaires distributed. Of these, 100 were recovered, representing a 95% response rate, which was used for hypothesis testing. Regarding the organizational, legislative, and contractual requirements of cybersecurity on the continuity of the Jordanian banking sector, the support of bank administration to the cybersecurity operations team and the provision of plans through which cybersecurity strategies are implemented are crucial to ensure the success of its tasks. The study recommends that banking sector departments conduct a comparison between their legislative requirements and international, global security standards when choosing passwords to protect their critical systems and data. Banks must also pay more attention to regulatory requirements, followed by contractual and legislative requirements.

Contribution/ Originality: This study is among the few that address the issue of cybersecurity across its various legal, regulatory, and legislative dimensions concerning the sustainability of the Jordanian banking sector. It demonstrates the impact of each requirement on sustainability, as adherence to these requirements helps reduce cyber-attacks and facilitates their rapid detection.

1. INTRODUCTION

The use of the term cybersecurity has increased greatly over the past few years, both at the local and international levels, and with the adoption of the e-government system implemented by many countries around the world, which provide their various services to their citizens via the Internet, which has become essential for everyone. A response in the community with a connection to the information space and a personal account. With it, users deal either with e-government or other entities, depending on the type of transaction (Maharjan & Chatterjee, 2019).

As the study by Ben Aliyah and Ayyash (2022) showed, there is an annual increase in financial losses resulting from the penetration of banks and financial institutions. Cybercrimes cost the global economy approximately 0.8% of GDP. This percentage encompasses data damage and destruction, stolen funds, loss of productivity, theft of personal and financial data, embezzlement, theft of intellectual property, fraud, costs associated with data and

systems recovery, damage to reputation, disruption of normal business operations after an attack, and forensic investigation expenses.

This, in turn, affects the accounting information contained in the financial reports, which impacts the continuity of the banking sector, which in turn constitutes the backbone of the economy. Therefore, maintaining the confidentiality, availability, and integrity of information is the Central Bank of Jordan's primary concern, as it provides security requirements necessary to protect its information assets in a manner consistent with laws and legislation in the Hashemite Kingdom of Jordan. To provide a secure work environment that helps achieve the national and strategic objectives of the bank, the Department of Information Security and Cybersecurity was established at the Central Bank of Jordan. This department seeks to create a resilient and reliable cyber environment and to strengthen the capabilities of information security and cybersecurity, including human resources, technology, and operations, to address information security threats. Cybersecurity and data protection at the Central Bank are managed throughout various stages of their lifecycle, starting from creation, passing through transmission, processing, storage, and ending with disposal. The aim is to eliminate threats and collaborate with relevant parties to build a participatory system that enhances preparedness to respond to cybersecurity incidents and manage the risks associated with information security and cybersecurity. The goal is to reach an acceptable level of security within the bank, in addition to contributing to the dissemination and reinforcement of awareness regarding information security and cybersecurity (Central Bank, 2023).

Many previous studies, both local and global, have focused on the relationship between cybersecurity tools and cost accounting systems, such as the study by Abdallah (2024). The study by Dasgupta, Yelikar, Naredla, Ibrahim, and Alazzam (2023) addressed the benefits of using AI-supported cybersecurity to enhance business efficiency. On the other hand, other studies have examined cybersecurity policies and their risks across various sectors, including the study by Al-Sarhan (2019) and the study by Daoud and Serag (2022), which showed that the implementation of cybersecurity policies affects the quality of accounting information in the banking sector. Meanwhile, other studies, such as the one by Al-Baghdadi (2021), highlighted the challenges facing society in achieving cybersecurity and the mechanisms to enhance it in electronic banks are significant. Reviewing the results of previous studies reveals a lack of research focused on compliance with cybersecurity requirements across various sectors, especially given the diversity and increase of threats, breaches, and cyberattacks. This situation necessitates stricter measures for these entities through legislation specifically targeting this type of crime. There is a general trend among both governmental and private sectors to comply with cybersecurity requirements, as such compliance reduces potential costs associated with cybercrimes faced by countries worldwide, particularly within banking and financial institutions. The impact of adherence to these requirements will influence the quality of accounting information, accounting systems, and both internal and external audits.

And thus, this study aimed to shed light on the impact of compliance with regulatory, legislative, and contractual cybersecurity requirements on the continuity of the Jordanian banking sector, especially after the issuance of the first edition of the Cybersecurity Framework for the financial and banking sector by the Central Bank of Jordan, which was prepared with the contribution and participation of banking institutions operating in the Kingdom.

2. THEORETICAL FRAMEWORK

The National Center for Cybersecurity (2023) indicated that, in light of the increase in electronic threats, it has become important to protect information and communications systems against electronic attacks, while at the same time working to maintain the secrecy, security, and safety of information, and providing access to infrastructure properties and national vital entities in a smooth and safe manner. Therefore, the decision came from the concerned authorities to establish the National Center for Cybersecurity (2019) in accordance with the Cybersecurity Law No. (16), defining its organizational and operational competencies in the field of cybersecurity, by working to

strengthen information technology systems and protect networks and operational technology systems and their hardware and software components, in addition to the services and other services they provide. It contains data, taking into account the increasing importance of cybersecurity in the life of societies.

Hartmann and Carmenate (2021) stated that with the increase in the size and complexity of cyber security risks that affect the bank's assets and lead to a breach in its systems and information, leading to financial losses as well as losses in information and daily bank transactions, L Therefore, confronting the risks of cyber security in financial institutions and banks as mentioned by Curti, Gerlach, Kazinnik, Lee, and Mihov (2019). It goes far beyond the individual level, but there is a need for secure protocols in the process of information security risks, insurance against mobile phone risks, and insurance against operational risks. Insurance against the risks of electronic attacks, communications, training, and the qualification of employees. In addition to using safe protocols.

(Shahimi & Mahzan, 2018) and Li, No, and Wang (2018) agreed on the types of cybersecurity risks, which are:

1. Risks related to confidentiality: Represented by another party's penetration of private data and information.
2. Risks related to integrity: Represented by the misuse of systems or followed by banks.
3. Risks related to performance: Represented by the disruption of operations and practices in banks.

The Carnegie Endowment Organization for International Peace documented that the most important cyber-attack was the Trojan horse: On April 11, 2022, impersonating bank employees to talk to customers to obtain confidential information such as payment data. Spyware was also used, resulting in theft. Victims' funds and information, as well as the theft of Ronin cryptocurrency: On and after March 23, 2022, the second-largest theft of cryptocurrencies occurred, leading to the loss of one million dollars in the Blockchain Ronin 615 project. The attackers exploited vulnerabilities to transfer users' digital assets from one encryption network to another. This resulted in the theft of funds and a cyber-attack on the Moscow Stock Exchange and Sberbank on 28/2/2022. The largest lender in Russia, the Moscow Stock Exchange, and Sberbank were exposed to cyber-attacks known as "refusal of service." The distributed denial-of-service (DDoS) attack led to the disruption of internet services, paralysis of operations, and the disruption of the stock exchange website. On March 27, 2019, a bank in Kuwait was robbed of $49 million due to a technical malfunction in the international transfer system, as announced by Kuwaiti Gulf Bank, which resulted in the transfer not being completed. The tool used for this attack was a DDoS attack, which overwhelmed the system and caused the failure of the transfer process.

Cormier, Magnan, and Morard (1995) and Kieso, Weygandt, and Warfield (2020) have mentioned that with the multiple risks that companies are exposed to in light of the occurrence of internal or external crises, or local or international problems that affect the facility's ability to continue, necessitate changing the strategies and policies that they follow according to the type of these risks. Therefore, in March 2020, the United States government issued the CARES ACT law. Some accounting considerations were put in place that should be taken into account when preparing reports and financial statements related to risks and economic downturns and their impact on the assumption of continuity. Deloitte, 2020. On the other hand, Essential Cybersecurity Controls-1:2018 emphasizes the resilience of cybersecurity as one of the basic controls. Its aim is to provide the requirements for cybersecurity resilience, managing the continuity of the entities' businesses, and reducing the effects of disruptions to critical electronic services and their information processing systems and devices as a result of disasters caused by cyber risks. The controls related to cybersecurity resilience include business continuity.

1. Defining, documenting, and approving cybersecurity requirements within the entity's business continuity management.
2. Applying cybersecurity requirements within the entity's business continuity management.
3. The business continuity management in the entity should cover, at a minimum, the following:

- Emphasizing the continuity of cyber security systems and procedures.
- Developing plans to confront cybersecurity incidents that may affect the continuity of the entity's business.
- Disaster Recovery Plan.

- Developing disaster recovery plans.

4. Cybersecurity requirements within the entity's business continuity management must be reviewed periodically.

Given the importance of the risks to which the banking sector is exposed locally and internationally in light of cybersecurity incidents, the study examined the impact of compliance with the regulatory, legislative, and contractual requirements of cybersecurity on the continuity of the Jordanian banking sector.

2.1. Previous Studies

Many studies have addressed cybersecurity and its risks across various sectors, including Khresat (2024); Zwilling et al. (2020) and Daoud and Serag (2022). The study by Khresat (2024) concluded that the culture of the institution acts as a mediator in assessing cyberspace risks and their management. It emphasizes the relationship between risks and responses. The study by Zwilling et al. (2020) found that internet users possess sufficient awareness of cyber threats but tend to implement only minimal protective measures. The research highlights the economic necessity for countries to invest in cybersecurity technology. Developed cities tend to have high GDP values, yet their populations often lack the tools and knowledge necessary to protect against cybersecurity risks. The study by Maharjan and Chatterjee (2019) revealed that banks safeguard their assets through robust information security infrastructure and techniques that prevent cyberattacks from occurring or escalating. Similarly, Li et al. (2018) agreed, stating that disclosures about cybersecurity risks help reduce them by encouraging companies to adopt cautious policies. Transparency about risks, regardless of their level or threat, is essential for data security. The study by Kilani (2020) found that all cybersecurity variables influence organizational internal processes, with data growth being the most impactful variable. The research by Matarneh, Al-Tarawneh, and Al-Adamat (2020) also indicated that cybersecurity governance plays a significant role in reducing risks associated with cloud accounting. The study by Ali (2019) emphasized the importance of increasing user awareness in banking services regarding cybercrime risks, noting that lack of awareness can heighten these risks. Additionally, Bamrara (2015) identified a positive relationship between databases and cyberattacks, highlighting the vital role of database maintenance agents in defending against such attacks. Conversely, the same study found a negative relationship between the role of database maintenance agents and the effectiveness of defending against cyberattacks. The study by More, Patel, and Singh (2015) concluded that cyberattacks are prevalent, with money theft being among the most frequent and effective types of attack.

Berberoglu and Uzuz (2018) concluded that cyber-attacks and their high volume do not affect the Turkish banking sector.

2.2. Commentary on Previous Studies

By reviewing numerous previous studies on cybersecurity and its risks in various sectors, such as the study by Khresat (2024); Zwilling et al. (2020) and Daoud and Serag (2022) previous studies have concluded that there is an impact of cybersecurity threats and they must be monitored through the development of responses to related risks using a relationship between risks and responses, according to the study by Zwilling et al. (2020) I have concluded that internet users are sufficiently aware of cyber threats, but they only implement the minimum level of protective measures.

Maharjan and Chatterjee (2019) emphasized that techniques should be employed to prevent cyber-attacks as soon as they occur. The study by Li et al. (2018) indicated that disclosures about cybersecurity risks have led to their reduction and that it is essential to disclose these risks regardless of their level or threat. From the above, it is evident that previous studies did not focus on compliance with cybersecurity requirements, despite a general trend across all sectors, whether governmental or private, to adhere to these requirements because they help reduce the potential costs associated with cybercrimes. However, prior research primarily concentrated on the impact of risks

without considering the fundamental pillar, which is compliance with cybersecurity requirements. The study by Kilani (2020) concluded that all cybersecurity variables influence organizational internal processes. Similarly, Matarneh et al. (2020) addressed the impact of cybersecurity governance in mitigating risks related to cloud accounting. The research by Ali (2019) highlighted the importance of increasing awareness and understanding among banking service users regarding cybercrime risks. Additionally, Bamrara (2015) demonstrated a positive relationship between databases and cyberattacks. Meanwhile, More et al. (2015) identified the existence of numerous cyberattacks, with money theft being the most frequent and impactful.

Berberoglu and Uzuz (2018) showed the impact of cyber-attacks and their effect on the Turkish banking sector.

Through previous studies that focused on the banking sector, the studies highlighted the impact of cyberattacks but did not focus on compliance with cybersecurity requirements. The researcher believes that by adhering to these requirements and complying with them, and by establishing deterrent laws and regulations, individuals, communities, and economies can be protected from the increasing forms of cybercrime that have surged in recent years.

2.3. Statistical Analysis and Hypothesis Testing

2.3.1. Hypotheses

H_{01}: There is no effect significant at the 5% level of compliance with the regulatory requirements of cybersecurity on the continuity of the Jordanian banking sector.

H_{02}: There is no effect significant at the 5% level of compliance with the legislative requirements of cybersecurity on continuity in the Jordanian banking sector.

H_{03}: There is no effect significant at the 5% level of compliance with contractual requirements for cybersecurity on the continuity of the Jordanian banking sector.

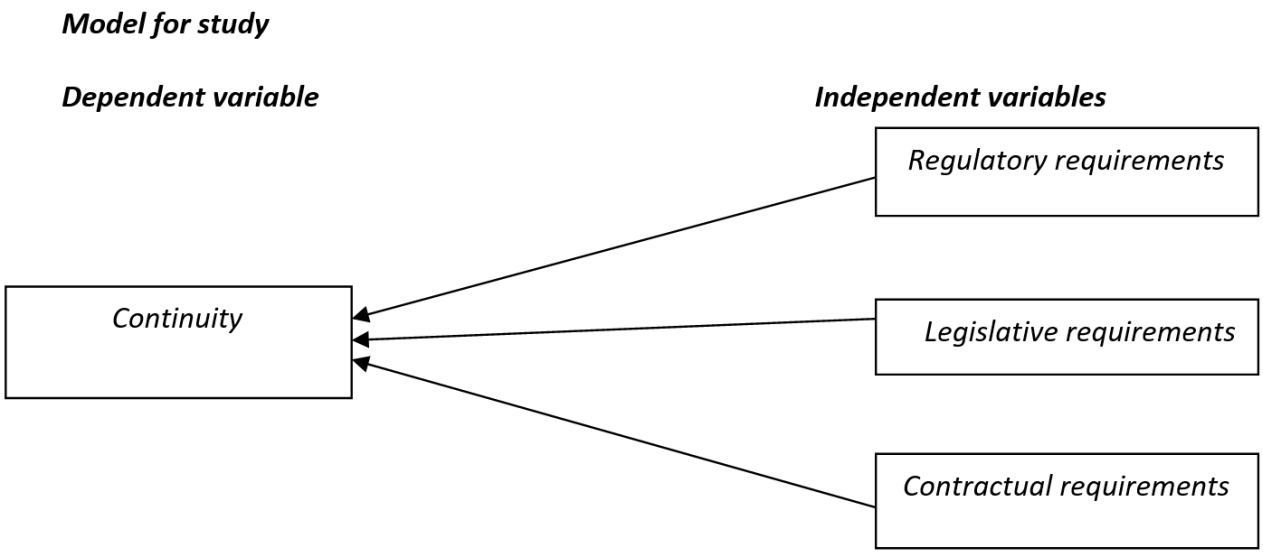

Figure 1. Model was prepared by the researcher.

Figure 1 shows the effect of the mediating variable, which is the three cybersecurity requirements, on the continuity of the Jordanian banking sector.

2.4. Model for Study

The study population included the Jordanian banking sector, which comprises all 23 banks operating in Jordan. A questionnaire was designed as a tool for the study and developed to cover all variables of interest. It was distributed to employees involved in risk management, financial control, inspection, regulation, strategic planning,

and technology within the banking sector in Jordan. The total number of questionnaires distributed was 105, with 100 recovered, resulting in a recovery rate of approximately 95%. The internal consistency of the questionnaire items was assessed using the Cronbach Alpha coefficient. This test measures the strength of the connection and cohesion between questionnaire items and provides an estimate of reliability. As shown in Table 1, the Cronbach Alpha coefficients for all questionnaire items exceeded 0.60%, which is considered the minimum acceptable level for reliability according to standard criteria.

Table 1. Table of internal consistency coefficients using Cronbach's alpha equation.

Variables	Number of paragraphs	Cronbach's alpha coefficient
Regulatory requirements	12	0.87
Legislative requirements	9	0.89
Contractual requirements	11	0.86
Continuity	13	0.87

Table 2. Matrix of correlation coefficients between study variables.

Variables	Regulatory requirements	Legislative requirements	Contractual requirements	Continuity
Regulatory requirements	1			
Legislative requirements	0.512	1		
Contractual requirements	0.401	586	*1*	
Continuity	0.681	*0.543*	0.677	*1*

Table 2 shows the matrix of correlation coefficients between the study variables. Through the table, it is clear that there is a linear correlation between the independent study variables and the dependent variable. As we can see from the table, the correlation is strong and positive between continuity and regulatory, legislative, and contractual requirements. This is because the absolute value of the correlation coefficients is greater than 50%. This indicates a general trend within the Jordanian banking sector to develop compliance processes with cybersecurity requirements to maintain the sector's continuity.

Table 3. Organizational requirements variable.

Ranking	Number	Paragraph	Mean	Standard deviations	Relative importance
1	7	Using security monitoring systems in the banking sector to monitor cyber activities and detect unusual patterns.	4.51	0.71	High
12	12	Securing contracts with suppliers of services and products in accordance with cybersecurity standards.	3.48	0.78	High
Regulatory requirements as a whole			4.09	0.77	High

Table 3 shows the standard deviation and arithmetic mean for the paragraphs of the regulatory requirements variable, where paragraph No. (7), which is "Using security monitoring systems in the banking sector to monitor cyber activities and detect unusual patterns," occupied the highest arithmetic mean, which is 4.51, with a standard deviation of 0.71. The reason is that the Jordanian banking sector defines cybersecurity policies that set the main principles and objectives of security in this sector.

Paragraph No. (12) "Securing contracts with service and product suppliers in accordance with cybersecurity standards" had the lowest mean of 3.48, with a standard deviation of 0.78.

This is because implementing these regulatory requirements contributes to the cybersecurity report within the organization and protects its data and systems from potential cyber threats. The mean for all regulatory requirements was 4.09, with a standard deviation of 0.77.

Table 4. Legislative requirements variable.

Ranking	Number	Paragraph	Mean	Standard deviations	Relative importance
9	1	The concepts of cybercrime and illegal activities on the Internet are defined.	3.49	0.60	High
1	7	There are additional laws at the regional or local level related to cybersecurity.	4.31	0.82	High
Legislative requirements as a whole			3.88	0.74	High

Table 4 shows the standard deviation and arithmetic mean for the paragraphs of the legislative requirements variable, where paragraph No. (7) was occupied, which states, "There are additional laws at the regional or local level related to cybersecurity." The highest arithmetic mean is 4.31, with a standard deviation of 0.82.

This paragraph appears at the top of my account because there are local legislative requirements developed by legislative bodies in Jordan, such as the Cybersecurity Law No. 6 of 2019, and there are international legislative requirements developed by global entities and organizations such as SWIFI, PCI, etc. As mentioned in paragraph (1): "The concepts of cybercrimes and illegal activities on the Internet are defined," the lowest arithmetic mean is 3.49, with a standard deviation of 0.60. The reason for this is that these requirements differ from one country to another and depend on the laws and regulations in place everywhere. The arithmetic mean for all legislative requirements is 3.88, with a standard deviation.

Table 5. Contractual requirements variable.

Ranking	Number	Paragraph	Mean	Standard deviations	Relative importance
11	3	Determine how to grant and withdraw permissions to access data and systems, and determine who can do this.	3.33	0.781	High
1	10	Dealing with disruptions and downtime: Determine how to address disruptions that may affect the cyber services provided.	4.12	0.699	High
Contractual requirements as a whole			3.79	0.683	High

Table 5 shows the standard deviation and arithmetic mean for the paragraphs of the contractual requirements variable, where paragraph No. (10), which is "Dealing with disturbances and cessation of service: determining how to deal with disturbances that may affect the provided cyber services," occupied the highest arithmetic mean, which is 4.12, with a standard deviation of 0.699. Because the banking sector is striving hard to protect individuals and economies from cybercrimes, as paragraph (3) stated, "Determining how to grant and withdraw permissions to access data and systems, and determining who can do this," the minimum arithmetic mean was 3.33, with a standard deviation of 0.781. This is due to the strict protection of the data and information shared between the parties. The arithmetic mean for all contractual requirements was 3.79, with a standard deviation of 0.683.

Table 6 shows the standard deviation and arithmetic mean for the paragraphs of the continuity variable, where paragraph No. (7) was occupied, which is: "It is important to maintain the continuity of business establishments for internal and external users of financial statements, in order to maintain the flow of profits from investments, and to preserve the contribution of business establishments to economic and social development and increasing the well-being of society," with an upper arithmetic mean of 4.40 and a standard deviation of 0.72.

Table 6. Continuity variable.

Ranking	Number	Paragraph	Mean	Standard deviations	Relative importance
1	7	It is important to maintain the continuity of business enterprises for internal and external users of financial statements, in order to maintain the flow of profits from investments, sustain the contribution of business enterprises to economic and social development, and increase the well-being of society.	4.40	0.72	High
13	9	The continuity assessment of the facility is carried out until the date of issuance of the financial statements, and management is required to evaluate the facility's ability to continue operating.	3.73	0.74	High
Overall continuity requirements			4.00	0.716	High

Because the quality of data and information increases trust in financial reports, which helps users of accounting information, both internal and external, in the decision-making process. As mentioned in Paragraph No. (9), "The continuity assessment of the facility is carried out until the date of issuing the financial statements, and management is required to evaluate the facility's ability to continue operating." The mean of the lowest arithmetic mean was 3.73, with a standard deviation of 0.74. The researcher believes that the issue of evaluation is a relative matter in the Jordanian banking sector. The arithmetic mean for all items was 4.00, with a standard deviation of 0.716.

2.5. Study Hypotheses and Their Testing

The study hypotheses were tested using the Smart PLS program, and the results of the hypothesis testing are as follows.

Table 7. Simple regression analysis of regulatory requirements on continuity.

Model summary						
Model	**R**	**R square**	**Adjusted R square**	**Std. error of the estimate**		
1	0.749[a]	0.561	0.5572	0.616041		
a. Predictors: (Constant), of regulatory requirements						
ANOVA						
Model		Sum of squares	df	Mean square	F	Sig.
1	Regression	65.7441	1	65.7431	173.238	0.000[b]
	Residual	51.61221	137	0.381		
	Total	117.3561	138			
a. Dependent variable: continuity						
b. Predictors: (Constant), regulatory requirements						
Coefficients						
Model	Unstandardized coefficients		Standardized coefficients		t	Sig.
	B		Std. Error	Beta		
1	(Constant)	0.398	0.204		1.952	0.003
	Regulatory requirements	0.856	0.065	0.748	13.162	0
a. Dependent variable: Continuity [1]						

Note: a. Predictors: (Constant), of regulatory requirements
ANOVA: a. Dependent Variable: continuity
b. Predictors: (Constant), regulatory requirements
Coefficients: a. Dependent Variable: continuity

Table 7 shows a positive correlation between compliance with regulatory requirements and continuity, where the value of the correlation coefficient was (R = 0.749), and the value of the coefficient of determination (R^2 = 0.560), indicating that compliance with regulatory requirements explains 56.6% of the variance in continuity. As shown in the table, the significance of the model is confirmed by the calculated F value of (173.238) at a significance

level (Sig F = 0.000), which is less than 0.05, indicating a statistically significant effect of compliance with regulatory requirements on continuity at the significance level (0.05 ≥ α). Accordingly, the null hypothesis (H_0) is rejected, and the alternative hypothesis (H_1) is accepted. The regression coefficients for compliance with regulatory requirements show that the B value at the regulatory requirements dimension is (0.856), and the calculated T value for this dimension is (13.162). At a significance level (Sig T = 0.000), which is less than 0.05, this indicates a significant impact of regulatory requirements on continuity in the Jordanian banking sector.

This is because the Central Bank of Jordan has set regulatory requirements for 2023, which include policies, procedures, and practices that must be implemented within the banking sector to ensure cybersecurity and maintain the continuity of the Jordanian banking sector.

Table 8. Simple regression analysis of legislative requirements on continuity.

Model summary						
Model		**R**	**R Square**	**Adjusted R square**	**Std. error of the estimate**	
1		0.402[a]	0.162	0.154	0.85108	
a. Predictors: (Constant), Legislative Requirements						
ANOVA [a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	18.8461	1	18.846	26.018	.000[b]
	Residual	98.5101	137	0.723		
	Total	117.3561	138			
a. Dependent Variable: Continuity						
b. Predictors: (Constant), Legislative Requirements						
Coefficients [a]						
Model		Unstandardized coefficients		Standardized coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.9021	0.2261		8.4192	0.000
	Legislative Requirements	0.3501	0.0692	0.401	5.1011	0.000
a. Dependent Variable: Continuity						

Note: Model Summary: a. Predictors: (Constant), Legislative Requirements
ANOVA: a. Dependent Variable: Continuity
b. Predictors: (Constant), Legislative Requirements
Coefficients: a. Dependent Variable: Continuity

Table 8 shows the existence of a positive correlation between compliance with legislative requirements and continuity, where the value of the correlation coefficient was (R=0.402), and the value of the coefficient of determination was (R^2=0.161). This indicates that the legislative requirements explain approximately 16.1% of the variance in continuity.

As can be seen from the table, the significance of the model, as the calculated F value was 26.018 and the level of significance (Sig F = 0.000) is less than 0.05, which indicates the presence of a statistically significant effect of compliance with legislative requirements on continuity at the significance level (0.05 ≥ α). Accordingly, the null hypothesis (H0) is rejected, and the alternative hypothesis (H1) is accepted. The values of the regression coefficients have appeared to comply with the legislative requirements, as it turns out that the value of B (legislative requirements) reached 0.350, and the calculated T value was 5.10162, with a level of significance (Sig T = 0.000), which is less than 0.05, indicating a significant impact of legislative requirements on continuity in the Jordanian banking sector.

This is due to the requirements developed by legislation in Jordan, namely the Cybersecurity Law of 2019, the Electronic Transactions Law of 2015, the Cybersecurity Risk Adaptation Instructions issued by the Central Bank of Jordan, and the Cybersecurity Framework for the Jordanian financial sector.

Table 9. Simple regression analysis of contractual requirements on continuity.

Model summary					
Model		**R**	**R square**	**Adjusted R square**	**Std. error of the estimate**
1		0.423[a]	0.179	0.173	0.84218
a. Predictors: (Constant), contractual requirements					

ANOVA[a]						
Model		Sum of squares	df	Mean square	F	Sig.
1	Regression	20.8941	1	20.895	29.459	0.000[b]
	Residual	96.4622	136	0.708		
	Total	117.3563	137			
a. Dependent variable: Continuity						
b. Predictors: (Constant), contractual requirements						

Coefficients[a]						
Model		Unstandardized coefficients		Standardized coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.923	0.21		9.157	0.000
	, contractual requirements	0.3471	0.064	0.422	5.428	0.000
a. Dependent variable: Continuity						

Note: Model Summary: a. Predictors: (Constant), contractual requirements
ANOVA:
a. Dependent Variable: continuity
b. Predictors: (Constant), contractual requirements
Coefficients
a. Dependent Variable: continuity

Table 9 shows the existence of a positive correlation between compliance with contractual requirements and continuity, where the value of the correlation coefficient reached (R.423a), and the value of the determination coefficient reached (R2.178). This indicates that the mother A percentage of (17.8%) was explained by legislative requirements) of the change in continuity.

As can be seen from the table, the significance of the model, as the calculated F value reached 29.459 and the level of significance (Sig F = 0.000) is less than 0.05, which indicates the presence of a statistically significant effect of compliance with security requirements. It is based on the continuity at the significance level ($0.05 \geq \alpha$). Accordingly, the null hypothesis (H0) is rejected, and the alternative hypothesis (H1) is accepted. The values of the regression coefficients for compliance with contractual requirements have appeared, as it turns out that the value of contractual requirements reached 0.347, and the value of the T statistic reached 5.428, with Sig T = 0.000, which is less than 0.05, indicating a significant impact of contractual requirements on continuity in the Jordanian banking sector.

This is because the contractual requirements pertain to the measures and conditions that must be included in service contracts and agreements to ensure cybersecurity, which in turn contributes to the protection of information and data when contracting with service providers.

3. RESULTS AND RECOMMENDATIONS

Based on the results of hypothesis testing, it was found that there is an impact of compliance with regulatory, legislative, and contractual requirements on continuity in the Jordanian banking sector at a significance level of 0.05. This indicates the correlation and positive impact of compliance with regulatory, legislative, and contractual requirements for cybersecurity on the continuity of the Jordanian banking sector, as the commitment and compliance of the Jordanian banking sector with regulatory, legislative, and contractual requirements achieve cybersecurity in this banking sector and its ability to deal with cyber-attacks and manage incidents. Responding to them through alternative emergency plans and continuous audit and control procedures increases the banks' ability to maintain the continuity of this sector. Compliance with regulatory, legislative, and contractual requirements also

impacts the continuity of the Jordanian banking sector due to bank management's support of the cybersecurity operations team and the provision of plans through which strategies are implemented. Cybersecurity, in order to ensure the success of their tasks. The results of this study were consistent with the study of both, (Daoud & Serag, 2022; Maharjan & Chatterjee, 2019; Zwilling et al., 2020).

Thus, the study recommends that the banking sector departments conduct a comparison between their legislative requirements, international security standards, and global practices when choosing a password to protect their systems and important data. Likewise, banks must give increased attention to regulatory requirements, followed by contractual and then legislative requirements.

The study also recommends that banks commit to disclosing their cybersecurity policies in their annual financial reports due to their impact on information security and the increase in customer trust. Additionally, it suggests incorporating cybersecurity requirements in line with the banking sector's strategy and objectives, as well as conducting continuous assessments of cybersecurity requirements within the banking sector.

Funding: This study received no specific financial support.
Institutional Review Board Statement: The study involved minimal risk and adhered to ethical guidelines for social science fieldwork. Formal approval from an Institutional Review Board was not required under the policies of Zarqa University, Jordan. Informed verbal consent was obtained from all participants, and all data were anonymized to ensure participant confidentiality.
Transparency: The author states that the manuscript is honest, truthful, and transparent, that no key aspects of the investigation have been omitted, and that any differences from the study as planned have been clarified. This study followed all writing ethics.
Data Availability Statement: Upon a reasonable request, the supporting data of this study can be provided by the corresponding author.
Competing Interests: The author declares that there are no conflicts of interests regarding the publication of this paper.

REFERENCES

Abdallah, M. A. (2024). Cybersecurity integration in cost accounting systems: A cross-national analysis. *Journal of Accounting and Information Security*, *15*(2), 113–129.

Al-Baghdadi, A. M. (2021). Cybersecurity challenges and enhancement mechanisms in electronic banking. *Journal of Cybersecurity and Financial Systems*, *12*(3), 45–62.

Al-Sarhan, H. (2019). The impact of implementing cybersecurity policy on the quality of accounting information in Jordanian commercial banks. Master's Thesis, Al-Bayt University. Mafraq, Jordan: Al-Bayt University.

Ali, S. (2019). Cybercrime risks and user awareness in banking services. *Journal of Financial Technology*, *8*(2), 101–114.

Bamrara, A. (2015). Database vulnerability and cybersecurity threats. *International Journal of Cyber Studies*, *3*(1), 55–70.

Ben Aliyah, N., & Ayyash, M. (2022). The economic impact of cybercrimes on the financial sector: A global perspective. *Journal of Financial Cybersecurity*, *10*(1), 22–37.

Berberoglu, G., & Uzuz, M. (2018). Impact of cyberattacks on the Turkish banking sector. *Journal of Information Security Research*, *12*(4), 44–59.

Central Bank. (2023). *Information security and cybersecurity readiness strategy*. Amman, Jordan: Central Bank Publications.

Cormier, D., Magnan, M., & Morard, B. (1995). The auditor's consideration of the going concern assumption: A diagnostic model. *Journal of Accounting, Auditing & Finance*, *10*(2), 201-222. https://doi.org/10.1177/0148558X9501000201

Curti, F., Gerlach, J., Kazinnik, S., Lee, M., & Mihov, A. (2019). *Cyber risk definition and classification for financial risk management*. Federal Reserve Bank of St Louis: Mimeo.

Daoud, M. M., & Serag, A. A. (2022). A proposed framework for studying the impact of cybersecurity on accounting information to increase trust in the financial reports in the context of Industry 4.0: An event, impact and response approach. *CAF – Journal of Commerce and Finance*, *42*(1), 20–61. https://doi.org/10.21608/caf.2022.251730

Dasgupta, S., Yelikar, B. V., Naredla, S., Ibrahim, R. K., & Alazzam, M. B. (2023). *AI-powered cybersecurity: Identifying threats in digital banking*. Paper presented at the 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). IEEE.

Hartmann, C. C., & Carmenate, J. (2021). Academic research on the role of corporate governance and IT expertise in addressing cybersecurity breaches: Implications for practice, policy, and research. *Current Issues in Auditing*, *15*(2), A9-A23. https://doi.org/10.2308/CIIA-2020-034

Khresat, O. (2024). The impact of the internal audit department in evaluating and managing cyber security risks and the mediating role of institutional culture in banks operating in Jordan. *Journal of Research Administration*, *6*(1), 15–35.

Kieso, D. E., Weygandt, J. J., & Warfield, T. D. (2020). *Intermediate accounting* (4th ed.). New York , U.S.A John Wiley and Sons Inc.

Kilani, M. (2020). Cybersecurity variables and their effects on internal organizational processes. *Journal of Cyber Management*, *5*(3), 73–88.

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*, 40-55. https://doi.org/10.1016/j.accinf.2018.06.003

Maharjan, R., & Chatterjee, J. M. (2019). Framework for minimizing cyber security issues in banking sector of Nepal. *LBEF Research Journal of Science, Technology and Management*, *1*(1), 82-98.

Matarneh, R., Al-Tarawneh, H., & Al-Adamat, A. (2020). Cybersecurity governance and cloud accounting risks. *International Review of Accounting and IT*, *7*(1), 35–50.

More, V., Patel, K., & Singh, R. (2015). Trends in cyberattacks: A financial perspective. *Cybersecurity and Risk Management Journal*, *2*(2), 19–34.

National Center for Cybersecurity. (2019). *Cybersecurity law No. (16): Organizational and operational mandates*. Amman, Jordan: National Center for Cybersecurity.

National Center for Cybersecurity. (2023). *National strategy for cybersecurity resilience*. Riyadh, Saudi Arabia: National Center for Cybersecurity Publications.

Shahimi, S., & Mahzan, N. (2018). Building a research model and hypotheses development and findings of exploratory interviews. *International Journal of Management Excellence*, *10*(2), 1257-1283.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82-97. https://doi.org/10.1080/08874417.2020.1712269