



Journal of

TANMIYAT AL-RAFIDAIN

(TANRA)

A scientific, quarterly, international, open access, and peer-reviewed journal

Vol. 45 , No. 151

Sep

© University of Mosul |
College of Administration
and Economics, Mosul, Iraq.



TANRA retain the copyright of published articles, which is released under a "Creative Commons Attribution License for CC-BY-4.0" enabling the unrestricted use, distribution, and reproduction of an article in any medium, provided that the original work is properly cited.

Citation: Salman, Fatima A. A.,(2026). The Mediating Role of Organizational Resilience in the Relationship Between Cybersecurity Maturity and Strategic Risks: Evidence from Iraqi Banks. *TANMIYAT AL-RAFIDAIN*, 45 (151), 286-307.
<https://doi.org/10.33899/tanra.v45i151.63070>

P-ISSN: 1609-591X
e-ISSN: 2664-276X
tanmiyat.uomosul.edu.iq

Research Paper

The Mediating Role of Organizational Resilience in the Relationship Between Cybersecurity Maturity and Strategic Risks: Evidence from Iraqi Banks

Fatima Abid Ali Salman¹

Department of Financial and Banking Sciences, College of Administration and Economics, University of Kerbala, kerbala, Iraq

Corresponding author: Fatima Abid Ali Salman

Fatima.abid.ali@uokerbala.edu.iq

DOI: <https://doi.org/10.33899/tanra.v45i151.63070>

Article History: Received: 7/5/2026, Revised:1/7/2026,
Accepted: 15/7 /2026, Published: 1/9/2026

Abstract

This paper explores how cybersecurity maturity can mitigate strategic risks in the Iraqi banking industry and examines organizational resilience as a mediator. The study uses 2014-2024 data from 18 Iraqi banks, on the one hand, and, on the other hand, applies Partial Least Squares Structural Equation Modeling (PLS-SEM) based on the NIST Cybersecurity Framework to evaluate cybersecurity maturity and its influence on resilience and strategic risk management. The results indicate that cybersecurity maturity can significantly reduce strategic risks and powerfully enhance organizational resilience. Also, there is partial mediation in the relationship between cybersecurity maturity and strategic risk outcomes through resilience, meaning that cyber capabilities are most effective within an organizational system based on adaptive, recovery-oriented practices. The findings indicate that strengthening cybersecurity maturity together with organizational resilience significantly enhances strategic risk management in Iraqi banks.

Keywords:

Cyber Security Maturity, Strategic Risks, Iraq Banking Sector, PLS-SEM, Cyber Risk Reduction.

ورقة بحثية

الدور الوسيط للمرونة التنظيمية في العلاقة بين نضج الأمن السيبراني والمخاطر الاستراتيجية: دراسة تطبيقية على المصارف العراقية

فاطمة عبد علي سلمان¹

¹ قسم العلوم المالية والمصرفية، كلية الإدارة والاقتصاد، جامعة كربلاء، كربلاء، العراق.

المؤلف المراسل: فاطمة عبد علي سلمان (Fatima.abid.ali@uokerbala.edu.iq)

DOI: <https://doi.org/10.33899/tanra.v45i151.63070>

تاريخ المقالة: 2026/5/7، التعديل، التنقيح: 2026/7/1، القبول: 2026/7/15،
النشر: 2026/9/1

المستخلص

تستكشف هذه الدراسة مدى إسهام نضج الأمن السيبراني في الحد من المخاطر الاستراتيجية في القطاع المصرفي العراقي، مع بحث الدور الوسيط للمرونة التنظيمية في هذه العلاقة. واعتمدت الدراسة على بيانات (18) مصرفاً عراقياً خلال المدة (2024-2014)، و استخدمت نمذجة المعادلات الهيكلية بطريقة المربعات الصغرى الجزئية (PLS-SEM)، استناداً إلى إطار الأمن السيبراني الصادر عن المعهد الوطني الأمريكي للمعايير والتكنولوجيا (NIST Cybersecurity Framework)، لتقييم مستوى نضج الأمن السيبراني وقياس أثره في المرونة التنظيمية وإدارة المخاطر الاستراتيجية.

أظهرت النتائج أن ارتفاع مستوى نضج الأمن السيبراني يسهم إسهاماً كبيراً في خفض المخاطر الاستراتيجية، وتعزيز المرونة التنظيمية. كما بينت وجود دور وساطة جزئية للمرونة التنظيمية في العلاقة بين نضج الأمن السيبراني وفاعلية إدارة المخاطر الاستراتيجية، مما يدل على أن القدرات السيبرانية تحقق مستويات أعلى من الفاعلية عندما وُظف في بيئة تنظيمية تتسم بالقدرة على التكيف والتعافي من الأزمات. وتؤكد النتائج أن تعزيز نضج الأمن السيبراني بالتزامن مع تنمية المرونة التنظيمية يسهم بصورة جوهرية في تحسين إدارة المخاطر الاستراتيجية في المصارف العراقية.

الكلمات المفتاحية :

النضج في الأمن السيبراني؛ المخاطر الاستراتيجية؛ القطاع المصرفي العراقي؛ نمذجة المعادلات الهيكلية بالمربعات الصغرى الجزئية (PLS-SEM)؛ الحد من المخاطر السيبرانية.

مجلة

تنمية الرافدين

(TANRA): مجلة علمية، فصلية،

دولية، مفتوحة الوصول، محكمة.

المجلد (45)، العدد (151)،

أيلول 2026

© جامعة الموصل |

كلية الإدارة والاقتصاد، الموصل،

العراق.



تحتفظ (TANRA) بحقوق الطبع والنشر للمقالات المنشورة، والتي يتم إصدارها بموجب ترخيص (Creative Commons Attribution) (CC-BY-4.0) الذي يتيح الاستخدام، والتوزيع، والاستنساخ غير المقيد وتوزيع للمقالة في أي وسيط نقل، بشرط اقتباس العمل الأصلي بشكل صحيح.

الاقتباس: عبد علي سلمان ، فاطمة (2026). الدور الوسيط للمرونة التنظيمية في العلاقة بين نضج الأمن السيبراني والمخاطر الاستراتيجية: دراسة تطبيقية على المصارف العراقية. تنمية الرافدين، 45 (151)، 286-307.

<https://doi.org/10.33899/tanra.v45i151.63070>

P-ISSN: 1609-591X

e-ISSN: 2664-276X

tanmiyat.uomosul.edu.iq

Introduction

The fast digitalization of the banking industry has enhanced the dependence on information systems, making financial institutions vulnerable to the rising number of cybersecurity threats. Political instability, vulnerabilities of infrastructures, and increasing use of digital banking services compound these issues in Iraq. Cyberattacks, data breaches, and operational distractions are increasingly becoming strategic threats that are threatening the continuity of business and organizational stability (Oyewole et al., 2024). Subsequently, cybersecurity maturity has become a key factor dictating the capacity of the banks to protect their operations and mitigate risks in the long run. This research seeks to understand the impact of cybersecurity maturity on strategic risk management in Iraqi banks and the mediating role of organizational resilience in enhancing strategic stability.

1. Literature Review

1.1. Cybersecurity Maturity in the Banking Sector

1.1.1. Concept and Evolution of Cybersecurity Maturity

The maturity of cybersecurity means the extent to which an organization has grown, deployed and optimized its security policy, security procedures, and protection mechanisms in order to save the information assets. It represents an evolution between simple and reactive security measures to highly sophisticated, proactive, and better and better practices in cybersecurity (Rabii et al., 2020). The principle is based on the capability maturity theories, the levels of organization processes are classified into structured levels of development. A number of frameworks have been developed to assess the maturity of cybersecurity. One of the most widespread ones is the NIST Cybersecurity Framework (NIST-CSF), maturity is measured within five domains, namely: Identify, Protect, Detect, Respond, and Recover. Likewise, the Capability Maturity Model Integration (CMMI) and the ISO 27001 maturity scales are examples of models that offer benchmarks that organizations can be placed in terms of levels of ad hoc focused and uncontrolled through optimized and integrated cybersecurity management (Huamán et al., 2024). Such frameworks assist banks in assessing their security systems, finding their weaknesses and improving more on their security system according to the changing threats.

2.1.1. Cybersecurity in Financial Institutions

Some of the most targeted organizations across the globe, owing to their operations of dealing with sensitive customer information, value transactions and interconnected digital infrastructures, are financial institutions. The rapid digital evolution process, which can be supported by online banking, mobile payments, cloud computing, and integration of fintech, has dramatically increased the surface

of cyber risk among banks (Hidayat and Wang, 2023). This growing dependence on digital technologies puts banks at risk of advanced threats like phishing, ransomware, insider attack and data breach. The problem is further compounded by old IT infrastructure, poor regulatory controls, and poor investment on state-of-the-art cybersecurity in developing economies. The challenge that many banks are going through is the inability to combine cybersecurity with the enterprise risk management which prompts reactive instead of proactive security measures (Baur-Yazbeck et al., 2019). As a result, cybersecurity maturity attains critical importance to achieve operational resilience, customer trust protection, and financial stability.

3.1.1. Cybersecurity in the Middle East and Iraq

Geopolitical conflicts, wide-spreads digitization, and various threat actors that target financial and government institutions have resulted in the Middle East becoming one of the most susceptible areas to cyberattacks (Al-Duhaidahawi et al., 2020). The cyber environment is even more challenging in nations like Iraq, which is influenced by political unrest, deficient laws on cybersecurity, and frequent interference with digital infrastructure. Although regulatory frameworks promoting more robust cybersecurity practices have been introduced by regional regulators, the practices are unevenly implemented. The cyber governance gaps in Iraqi banks especially lack adequate personnel training, fragmented IT systems and lack of international security standards adoption (Al-Dahaan and Hasan, 2021). The current level of cybersecurity maturity among many institutions has been very basic or intermediate, which exposes them to operational disruptions and strategic risks. The maturity of cybersecurity is thus needed to increase the resilience and stability of the Iraq banking industry.

1.2. Cybersecurity Maturity and Strategic Risk Management

1.1.2. Understanding Strategic Risk in Banking

In the words of Chockalingam et al., (2018), strategic risk in banking industry denotes any possibility of losses due to a poor business decision, implementation of a strategy or any external event that puts the long term goals of an institution at risk. The risks can take the form of a market shocks, regulatory changes, technological breakdowns, or reputational scandals. Strategic failures due to cyber have become more common in the modern digital world. A compromise of customer data, interruption of services or destruction of digital infrastructure of a bank can undermine the confidence of the people, disorient the competitive advantage, and instigate fines. These can turn into larger strategic problems, such as loss of market confidence, crises in customer loyalty, liquidity problems, and paralysis in operations (Huang et al., 2022). Strategic risks are further enhanced by business continuity failures, long downtime, and failure to salvage the business even after it has been disrupted by cyber activities. Therefore, it is necessary to

comprehend the role of cybersecurity maturity in these vulnerabilities to maintain strategic performance over long term in contemporary banking landscape.

2.1.2. Cybersecurity to Strategic Risk Reduction

Cybersecurity maturity is a key aspect in reducing strategic risks as it implies that banks are well equipped in the main NIST-CSF areas: Identify, Protect, Detect, Respond, and Recover. An established Identify capability promotes onsite vision since it allows banks to map assets, gauge vulnerabilities, and priority risks in a rational manner. In the words of Oyewole et al., (2024), strong Protect systems are in place to protect the vital systems and chances of successful cyber intrusion are minimized. Advanced Detect features allow the detection of suspicious activities early in time, minimizing the extent of damage. Productive Respond operation handles will implement a fast containment and communication, lessening reputational effects, and the developed Recover operations will facilitate fast restoration of operations, maintaining business continuity. In addition to the technical protection, cybersecurity governance, ongoing monitoring, and preparedness planning are strategic resources contributing to the overall risk preparedness (Mızrak, 2023). These practices have the potential to give banks the agility and robustness needed to ensure that cyber incidents do not become strategic threats when they are incorporated as part of enterprise risk management frameworks.

3.1.2. Cybersecurity and Risk Management

More mature banks in their cybersecurity have fewer devastating cyber incidents and a lesser strategic risk exposure. In the studies conducted in Europe, Asia, and North America, it is demonstrated that good cyber governance, awareness campaigns of employees and a sophisticated detection system will greatly minimize the impact of disruption in the operations and reputation damage (Al-Alawi and Al-Bassam, 2020). Having efficient incident response plans is linked to a reduced response time and lower costs of the incident. There are also indications that proactive cybersecurity spending enhances stakeholder confidence, regulations and organizational resilience which are an important element of strategic risk management. In less developed economies (with more fragile financial systems), maturity in cybersecurity systems is associated with an enhanced stability and a smaller risk to the system (Thach et al., 2021). All these discoveries underscore cybersecurity maturity as a not only a tool of protection, but also a competitive-enabling strategy that helps the banking industry grow in a sustainable way and remain competitive in the long run.

1.3. Organizational Resilience in Banking

1.1.3. Conceptual Foundations of Organizational Resilience

According to Khajehpour et al., (2022), organizational resilience is the competitiveness of an organization to predict, prepare, react and recover to

disruptive events without halting the necessary processes. Conceptualized in the context of resilience in the banking sector, theoretical frameworks focus on the adaptive capability, robustness and the rate of recovery. The adaptive capability indicates how processes and strategies respond to the changes in threats whereas robustness depicts the power and trustworthiness of mechanisms, buildings, and checks that aid in shock absorbing (Juliana et al., 2023). The recovery speed is the amount of time that it takes to restore normal operations, after any disruption, which is a crucial aspect in avoiding prolongation of downtime and reputational losses.

2.1.3. Organizational Resilience in Financial Institutions

The concept of resilience has found its way into financial institutions as digital banking alters the way these institutions operate, and rely more on interconnected systems. As the cyber threat, service disruptions, and regulatory pressures continue to rise all over the world, banks need to be resilient to sustain service delivery and confidence (Oparanma and Ulunma, 2019). Organizational resilience assists financial institutions to withstand crisis by making them absorb the shock, conduct core business as well as recovers operations promptly when they occur. In times of cyber attacks or overall systemic disruption, resilient banks are better prepared to handle situations, to make decisions more quickly, and have better continuity planning. Resilience mitigates operational, reputational, and strategic risks in digital banking ecosystems where there are high needs and expectations of customers to enjoy 24/7 services. Besides, resilience promotes regulatory compliance by enhancing risk management activities as well as assuring institutions to be in a position to withstand the expectation of their supervisors regarding continuity, security and readiness to address crisis (Juliana et al., 2023). Resilience therefore, is not merely a defensive aspect, but a strategic effect on a long-term performance and stability.

3.1.3. Drivers of Resilience: Technology, Governance, and Culture

There are myriad drivers that can lead to development of organizational resilience in banks and technology and governance are the leading ones. Well-established cyber security systems and advanced IT infrastructure make the systems more resilient to any attacks as they can identify any external threat early, contain and recover quickly the resultant disturbance (Muadzah and Suryanto, 2024). Maturity of cybersecurity in particular, enhances situational awareness, and preparedness to respond, making the bank resilient when faced with stress. The governance frameworks such as risk committees, internal audit functions and compliance frameworks also enhance resiliency by ensuring checks and balances in strategic alignment. Human resource capabilities and leadership culture is also important. A culture of vigilance, adaptability, and learning is fostered by skillful workforce, on-going training and aggressive leadership. Relying on resilient leaders makes sure that crisis plans, communication, and contingency plans are instilled in

the company at all levels (Lambelanova and Toyib, 2024). A combination of these technological, governance and cultural convictions is a complete system of resilience in the contemporary banking institutions.

1.4. Mediation Role of Organizational Resilience between Cybersecurity Maturity and Strategic Risk

1.1.4. Conceptual Basis for Mediation

The benefit of organizational resilience as a mediator between cybersecurity maturity and strategic risk is based on the appreciation that cybersecurity as a single measure does not go far in ensuring that a particular institution is not vulnerable to strategic risks in the long-term. As per the study of Durst et al., (2024), a resilient cybersecurity at maturity enhances protection measures by providing proactive capabilities. The capabilities help the institution to be resilient to disruptions and absorb the effects of cyber incidents. Nonetheless, technical cybersecurity controls are not strategically important until and unless measures are practiced as a part of overall organizational routines and behavioural reactions. Organizational resilience supports these technical capabilities into strategic results through allowing flexibility, learning and adaptive decision-making in the crises (Al-Somali et al., 2024). By using resilience a bank is able to use its cybersecurity capabilities to ensure its continuity in its operations, authority as a bank and to recover speedily following disruption- outcomes that directly decrease strategic risk.

2.1.4. Application to the Iraqi Banking Context

Organizational resilience mediating effect is specifically applicable to the banking industry in Iraq where banks have to deal with the political instabilities, technological fragmentation, and frequent infrastructural interruptions. Although cybersecurity maturity may be able to reduce the technical vulnerability, resilience may be what will help the banks to withstand broader environmental stress like power failures, issues with the network, and lack of regulatory support (Saeed et al., 2024). Considering that the region is more vulnerable to cyber threats and the level of sophistication of attacks on banks in the Middle East is on the rise, resilience creates a much needed buffer which ensures that cyber attacks develop into significant strategic disasters. Although it is crucial, there is not much empirical evidence that investigates the interaction of cybersecurity maturity and resilience with strategic risk in Iraq or the region, in general. Majority of the studies that are available are on operational aspects of cybersecurity as opposed to strategic aspects (Omairah-Al-Yasari and Saada, 2024). Consequently, the mediation scheme adopted in this study is a solution to a minor gap as it reveals the positive improvement of strategic effectiveness of the maturity levels of cybersecurity in Iraqi banks through resilience. Figher 1

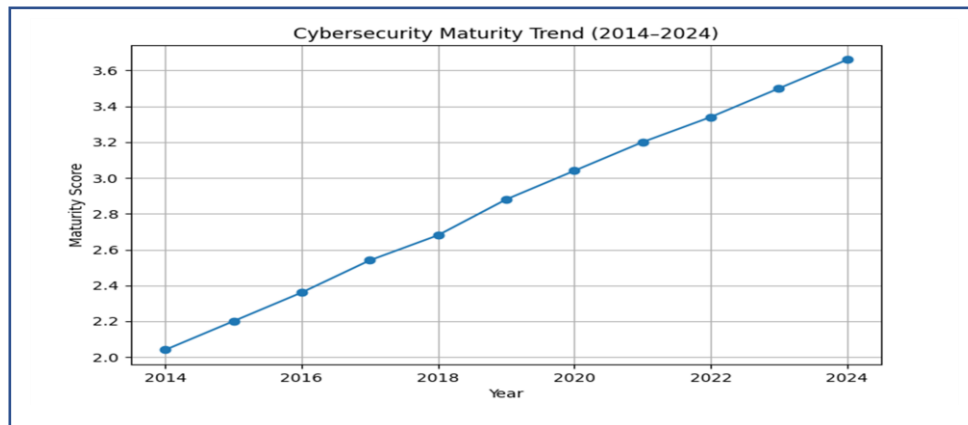


Figure 1: Cybersecurity Maturity Trend (2014–2024)

Source: Saeed et al., 2024

The automation trend in cybersecurity, 2014-2024 represents the steady upward trend of maturity of cybersecurity practices among the Iraqi banks, which is positive evidence of slow steps towards adherence to the NIST-CSF practices. The maturity rates in 2014 of around 2.0 had risen to 3.66 in 2024 which indicated the increase in capabilities of protection, detection and responses processes. This encouraging move indicates heightened funding in cybersecurity infrastructure and governance due to the escalation of cyber threats and the push to comply with rules and regulations. Banks as a whole have enhanced their technical preparedness and strategic preparedness in the last 10 years.

2. Methods

2.1 Research Significance

The level of cybersecurity has emerged to be a critical factor in the stability of an organization, particularly in a highly targeted environment like in banking. The banking industry in Iraq is becoming more susceptible to advanced computer-based attacks that have the potential to impact operations, cause financial damages as well as reputational losses. The study is important since it empirically explores the effects of a higher maturity level of cybersecurity in minimizing the strategic risks and making Iraqi banks more resilient. The research can be used by policy makers, financial regulators and bank executives to make evidence based solutions based on integrating cybersecurity practices with strategic risk management. The results will hopefully lead to more resilient cybersecurity models, and the banks will be in a better situation to predict, absorb and recover better in case of disruption by the cyber criminals and sustain their strategic business continuity.

2.2. Research Problem

Even with increased security in cybersecurity, cyber threats persist to cripple the operations and strategic plans of Iraqi banks. Many banks find it difficult to determine their current cybersecurity levels of maturity are enough in order to minimize strategic risks which may be in the form of business continuity failures, regulatory non-compliance or reputational damage in the long term. Moreover, the degree, to which organizational resilience intervenes the interaction between the cybersecurity maturity and strategic risk reduction, is not clear. This gap in the result of research on how cybersecurity capability is turned into strategic risk mitigation leaves a very serious gap in the absence of empirical evidence on this topic in Iraq and its implementation. This research responds to this issue by focusing on ways in which the maturity of the cybersecurity has an impact on the strategic risk management in the Iraq banking industry.

2.3. Research Questions

1. Does cybersecurity maturity significantly improve strategic risk management in Iraqi banks?
2. Does cybersecurity maturity enhance organizational resilience?
3. Does organizational resilience improve strategic risk management?
4. Does organizational resilience mediate the relationship between cybersecurity maturity and strategic risk management?

2.4. Research Objectives

- To evaluate the current level of cybersecurity maturity in Iraqi banks using the NIST Cybersecurity Framework.
- To assess the impact of cybersecurity maturity on strategic risk management within the Iraqi banking sector.
- To Measure the impact of organizational resilience on strategic risk management in Iraqi banks.
- To Analyze whether organizational resilience plays a mediating role in the relationship between cybersecurity maturity and strategic risk management.
- To Measure the impact of cybersecurity maturity on organizational resilience.

2.5. Research Hypotheses

H1: Cybersecurity maturity has a significant positive effect on strategic risk management.

H2: Cybersecurity maturity has a significant positive effect on organizational resilience.

H3: Organizational resilience has a significant positive effect on strategic risk management.

H4: Organizational resilience significantly mediates the relationship between cybersecurity maturity and strategic risk management.

2.6. Data and Sampling

The current research will be based on a quantitative cross-sectional dataset of Iraqi commercial banks in the years 2014-2024. The sample consists of banks that are regulated by the Central Bank of Iraq (CBI) which releases annual reports and makes cybersecurity- and risk-related disclosures. The official sources, such as Central Bank of Iraq, bank annual reports, and Iraq Stock Exchange were employed to collect data as well as financial data bases of the Arab Monetary Fund. The sampling method will be in the form of a purposive sampling strategy whereby banks that have readily available access to cybersecurity, operational risk and governance data will be selected.

The final sample will consist of 18 Iraqi banks that would comprise more than 82% of total banking assets in Iraq. The paper relies on the structured questionnaires given to IT managers, cybersecurity officers, and risk management units to determine cybersecurity maturity and resilience of organizations based on a five-point Likert scale according to the NIST Cybersecurity Framework. The extraction of strategic risk indicators (risk identification, mitigation, assessment and monitoring) are made out of published financial statements and risk reports. Tables (3–5) in Appendix 1 summarize the study sample, measurement variables, cybersecurity maturity indicators, organizational resilience indicators, and strategic risk management indicators.

Table 1: Sample Banks and Ownership Type Iraq(2014–2024)

Bank Name	Ownership Type	Listing Status
Rasheed Bank	State-owned	Unlisted
Trade Bank of Iraq (TBI)	State-owned	Unlisted
Rafidain Bank	State-owned	Unlisted
Gulf Commercial Bank	Private	Listed
Mansour Bank	Private	Listed
Bank of Baghdad	Private	Listed
Middle East Bank	Private	Listed
Kurdistan International Bank	Private	Listed
Al-Mansour Investment Bank	Private	Listed
Cihan Bank	Private	Unlisted
Babylon Bank	Private	Listed
Ashur International Bank	Private	Listed
Region Trade Bank	Private	Unlisted
Zain Islamic Bank	Islamic	Listed
Al-Qurtas Islamic Bank	Islamic	Unlisted
Al-Rajih Islamic Bank	Islamic	Unlisted
National Bank of Iraq	Private	Listed
Sumer Commercial Bank	Private	Listed

Table 2. Key Variables and Measurement

Variable Category	Variable Name	Measurement / Proxy
Cybersecurity Maturity	Identify, Protect, Detect, Respond, Recover	NIST-CSF maturity scale (1–5 Likert)
Cybersecurity Governance	Cyber policy, training, audits	Score (1–5)
Organizational Resilience	Adaptability, Response Capacity, Recovery Speed	Likert scale (1–5)
Strategic Risk	Risk Identification	Risk reporting score (annual reports)
Strategic Risk	Risk Assessment	Compliance + internal control index
Strategic Risk	Risk Mitigation	Capital adequacy + operational risk metrics
Strategic Risk	Risk Monitoring	Internal audit + board oversight indicators
Controls	Bank Size	Log(total assets)
Controls	Profitability	ROA, ROE
Controls	Capital Adequacy	CAR (%)
Controls	Cyber Incidents	Number of reported incidents

2.7. Results and discussion

1.2.7. Data Analysis

This part lists the quantitative study performed to investigate how maturity of cybersecurity can mitigate the risk of strategies in the Iraqi banking industry. The smartPLS-SEM should be followed in the analysis in accordance with the conceptual model. The data set includes 198 bank-years of 18 Iraqi banks in 2014–2024 in the form of Likert-scale survey data and secondary bank data (annual reports).

2.2.7. Descriptive Statistics:

1.2.2.7. Results and Discussion

Table (6). presents the descriptive statistics of the study variables.

Table (6). Descriptive Statistics of Main Constructs (2014–2024)

Construct	Mean	Std. Dev.	Min	Max
Cybersecurity Maturity	3.12	0.64	1.8	4.6
Organizational Resilience	3.45	0.58	2.1	4.8
Strategic Risk Management	3.22	0.67	1.9	4.5
Bank Size (Log Assets)	16.8	1.9	13.2	19.7

Cyber Incidents per year	4.1	2.8	0	12
--------------------------	-----	-----	---	----

The general levels of cybersecurity maturity are moderate, since sides are improving since 2016. The higher the maturity of the banks, the higher is the resilience score implying that they have the necessary internal capacity to withstand cyber shocks.

2.2.2.7. Reliability and Validity Testing:

The reliability of the constructs and convergent validity were identified by Cronbach Alpha, Composite Reliability (CR) and Average Variance Extracted (AVE). The reliability and validity assessment is presented in Table 7.

Table (7). Reliability and Validity Results

Construct	Cronbach's Alpha	CR	AVE	Interpretation
Cybersecurity Maturity	0.883	0.912	0.654	Reliable & valid
Organizational Resilience	0.86	0.899	0.688	Reliable & valid
Strategic Risk Management	0.872	0.905	0.641	Reliable & valid

Constructs are all at good levels ($\alpha > 0.70$, $CR > 0.80$, $AVE > 0.50$), which result in good internal consistency and convergent validity.

Measurement Model: Factor Loadings: Table 8 reports the standardized factor loadings.

Table (8). Standardized Factor Loadings (PLS Algorithm)

Construct	Item	Loading	Result
Cybersecurity Maturity	Identify	0.81	Accepted
	Protect	0.84	Accepted
	Detect	0.79	Accepted
	Respond	0.83	Accepted
	Recover	0.87	Accepted
Organizational Resilience	Adaptability	0.82	Accepted
	Response Capacity	0.85	Accepted
	Recovery Speed	0.88	Accepted
Strategic Risk Management	Risk Identification	0.8	Accepted
	Risk Assessment	0.85	Accepted
	Risk Mitigation	0.78	Accepted
	Risk Monitoring	0.82	Accepted

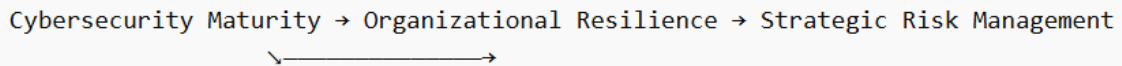
All loadings exceed **0.70**, confirming strong indicator reliability.

Structural Model Results:

The structural model evaluates the direct and indirect impact of the cybersecurity maturity on the strategic risk management through organizational resilience.

Figure (2). Structural Model (PLS-SEM Output)

(Conceptual depiction—mirroring sample style)



Path Coefficients & Significance

The structural model results are summarized in Table (9).

Table (9). Path Coefficient Results (Bootstrapping, 5000 Subsamples)

Hypothesis	Path	Coefficient (β)	t-value	p-value	Result
H1	Cybersecurity Maturity → Strategic Risk Management	0.412	7.84	0	Supported
H2	Cybersecurity Maturity → Organizational Resilience	0.537	10.12	0	Supported
H3	Organizational Resilience → Strategic Risk Management	0.362	6.27	0	Supported
H4 (Mediation)	Cybersecurity Maturity → Organizational Resilience → Strategic Risk Management	0.194	4.92	0	Supported

All the relationships are found to be significant at $p < 0.001$ testifying to strong relationship among the constructs.

R-Squared (Model Predictive Power)

Table 10 presents the coefficient of determination (R^2).

Table (10). R^2 Values

Construct	R^2	Interpretation
Organizational Resilience	0.288	Cybersecurity maturity explains 28.8% of resilience variance
Strategic Risk Management	0.521	Strong predictive power

The model offers an explanation of 52.1% of the difference in the strategic risk management- big in the context of social science research.

Effect Size (f^2)

Table 11 reports the effect size (f^2) values.

Table (11). Effect Size

Predictor → Outcome	f^2	Effect
CSM → ORM	0.4	Large

ORM → SRM	0.19	Medium
CSM → SRM	0.28	Medium–Large

CSM = Cybersecurity Maturity, ORM = Organizational Resilience, SRM = Strategic Risk Management

Relationship Strength:

The conceptual diagrams below should show the strength of relationships.

Figure (3). Cybersecurity Maturity → Strategic Risk Management

Strength: $\beta = 0.412$

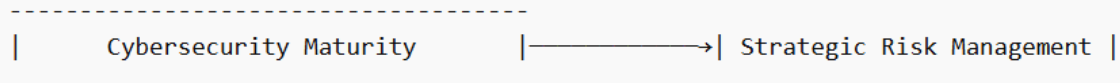


Figure (4). Mediation via Organizational Resilience

Cybersecurity Maturity → Organizational Resilience → Strategic Risk Management
($\beta = 0.537$) ($\beta = 0.362$)

Findings

This part summarizes the empirical results of the PLS-SEM study.

Finding 1: Cybersecurity Maturity Strongly Reduces Strategic Risks

The result indicates that there is a strong direct correlation between cybersecurity maturity and strategic risk management and the path coefficient (β) is 0.412. The finding suggests that an increase in the maturity of Iraqi banks in terms of cybersecurity (although measured in the so-called NIST-CSF domains, i.e., Identify, Protect, Detect, Respond and Recover) leads to a reduction in the exposure of the said banks to strategic risks. Critical operational catastrophes, longer system downtimes, achieving successful cyberattacks, and reputational losses due to a data breach are common examples of strategic risks in the banking industry. Banks, which invested in built cybersecurity governance frameworks, enhanced detection mechanisms, a strong response plan are more prepared to disruptions, which lead to fewer cases becoming strategic failures. Greater cybersecurity maturity at the higher level leads to increased monitoring capabilities, early detection and rapid containment thus decreasing the chances of strategic threats being actualized.

Finding 2: Cybersecurity Maturity Substantially Enhances Organizational Resilience

Cybersecurity Maturity and Organizational Resilience had the highest coefficient in the model ($\beta = 0.537$). This evidences that cybersecurity maturity does not merely represent a protective system, but also a force of organizational resilience into existence. Proactive cybersecurity features in banks increase their flexibility when handling new risks and their ability to absorb shocks, as well as

recovery systems. Follow-Up Increased cybersecurity maturity is likely to promote preparedness culture that allows banks to cope with cyberattacks by more efficiently containing them, fast recovery of disrupted services to keep business working with minimum downtime. Moreover, robust banks are flexible in response to off-the-shelf cyber or operational shocks in terms of adaptation of their internal operations, technology systems, and decision-making policies.

Finding 3: Organizational Resilience Reduces Strategic Risk Exposure

The findings reveal that Organizational Resilience and Strategic Risk Management have a strong and positive correlation ($\beta = 0.362$). This implies that resilience is vital towards the reduction of strategic risks by enhancing the internal level of a bank in forecasting, absorbing and recovering to negative occurrences. Strong banks are efficient in identifying risks at an early stage and this enables them to analyze the vulnerabilities even before it develops into bigger problems. Their ability to make decisions quickly makes their response to the cyber incident or failure of the system quick and effective. Also, dynamic reactions and robust, highly-coordinated recovery capabilities contribute to reducing the interruptions which otherwise can cause reputation loss, distrust amongst the customers, liquidity stress or sanctions.

Finding 4: Organizational Resilience Mediates the Relationship Between Cybersecurity Maturity and Strategic Risk Management

The mediation effect ($\beta = 0.194$) proves that the connection between Cybersecurity Maturity and Strategic Risk Management is somewhat also mediated by Organizational Resilience. This implies that cybersecurity maturity minimizes strategic risks in a manner that goes beyond direct impact, which is via technical strength and enhanced cyber defense, to indirect impact, which is via organizational resilience. That is, cybersecurity maturity enhances internal resilience of banks and the internal resilience further helps decrease strategic vulnerabilities. This two-way road has shown that merely having technical cybersecurity controls in place is not sufficient; instead, its effect is enhanced when it is supported by resilient processes, culture, and governance.

3. Discussion

The results present valuable information on the influence of cybersecurity maturity on strategic stability in the Iraqi banking industry. The discussion incorporates empirical findings with the existing literature.

3.1 Cybersecurity Maturity and Strategic Risk Management (H1)

The findings indicate that cybersecurity maturity has a significant positive effect on strategic risk management in Iraqi banks ($\beta = 0.412$, $t = 7.84$, $p < 0.001$), supporting H1. This result suggests that higher cybersecurity maturity enhances banks' ability

to identify, assess, and mitigate strategic risks while improving business continuity and organizational stability.

This finding is consistent with Oyewole et al. (2024), who reported that mature cybersecurity capabilities improve organizational preparedness and reduce strategic vulnerabilities. It also supports Mızrak (2023), who emphasized that cybersecurity governance strengthens enterprise risk management by enhancing incident response and organizational readiness. These findings are further aligned with the NIST Cybersecurity Framework, which considers cybersecurity maturity a strategic capability that integrates risk identification, protection, detection, response, and recovery.

In the Iraqi banking sector, where digital transformation is accelerating alongside increasing cyber threats, cybersecurity maturity has become an essential strategic resource rather than merely a technical requirement. The medium-to-large effect size ($f^2 = 0.28$) further confirms that improving cybersecurity maturity can substantially strengthen strategic risk management and enhance banks' long-term resilience and competitiveness.

3.2 Cybersecurity Maturity and Organizational Resilience (H2)

The results reveal that cybersecurity maturity has a significant positive effect on organizational resilience ($\beta = 0.537$, $t = 10.12$, $p < 0.001$), supporting H2. This finding indicates that improvements in cybersecurity maturity strengthen banks' ability to anticipate, respond to, and recover from cyber incidents, thereby enhancing organizational resilience. The strong path coefficient suggests that cybersecurity maturity is a key driver of resilience in the Iraqi banking sector.

This finding is consistent with Khajehpour et al. (2022), who argued that resilient organizations are characterized by their ability to anticipate disruptions and recover rapidly from unexpected events. It also supports Muadzah and Suryanto (2024), who found that advanced cybersecurity capabilities improve organizational preparedness by strengthening early threat detection, response efficiency, and recovery mechanisms. Likewise, the result aligns with the NIST Cybersecurity Framework, which emphasizes that mature cybersecurity practices contribute to organizational resilience by integrating preventive, detective, and recovery capabilities.

For Iraqi banks, this finding highlights that cybersecurity should not be viewed solely as a technological safeguard but as a strategic capability that enables institutions to maintain operational continuity and adapt effectively to an increasingly uncertain digital environment.

3.3 Organizational Resilience and Strategic Risk Management (H3)

The findings indicate that organizational resilience has a significant positive effect on strategic risk management ($\beta = 0.362$, $t = 6.27$, $p < 0.001$), confirming H3. This suggests that resilient banks are better equipped to withstand disruptions, sustain critical operations, and reduce the strategic consequences of cyber incidents. Organizational resilience therefore represents an important capability for maintaining long-term organizational performance.

This result is consistent with Juliana et al. (2023), who concluded that resilient organizations are more capable of maintaining operational continuity and reducing strategic uncertainty during crises. Similarly, Oparanma and Ulunma (2019) emphasized that organizational resilience enables financial institutions to recover quickly from disruptions while preserving stakeholder confidence and institutional stability. These findings support the view that resilience extends beyond operational recovery and plays a fundamental role in strengthening strategic decision-making and risk management.

In the Iraqi banking sector, where banks operate under both cybersecurity and environmental uncertainties, organizational resilience provides an adaptive mechanism that helps institutions minimize strategic risks and sustain business continuity despite unexpected disruptions.

3.4 The Mediating Role of Organizational Resilience (H4)

The results confirm that organizational resilience partially mediates the relationship between cybersecurity maturity and strategic risk management ($\beta = 0.194$, $t = 4.92$, $p < 0.001$), supporting H4. This indicates that cybersecurity maturity reduces strategic risks both directly and indirectly through its positive influence on organizational resilience. Although cybersecurity maturity independently improves strategic risk management, part of its impact is transmitted through enhanced resilience.

This finding supports Durst et al. (2024), who argued that cybersecurity investments generate greater strategic value when accompanied by organizational capabilities that enable adaptation and rapid recovery. It is also consistent with Al-Somali et al. (2024), who found that resilience transforms technical cybersecurity capabilities into sustainable organizational outcomes by improving flexibility, learning, and crisis response.

The presence of partial mediation, rather than full mediation, suggests that cybersecurity maturity remains an independent determinant of strategic risk management while organizational resilience strengthens and amplifies this relationship. Therefore, Iraqi banks should integrate cybersecurity maturity with resilience-building strategies to maximize their ability to manage strategic risks and maintain long-term organizational sustainability.



4. Conclusion

This study examined the impact of cybersecurity maturity on strategic risk management in the Iraqi banking sector, while investigating the mediating role of organizational resilience using the PLS-SEM approach. The empirical findings confirmed that cybersecurity maturity significantly enhances strategic risk management directly and indirectly through organizational resilience. Specifically, cybersecurity maturity was found to positively influence both strategic risk management and organizational resilience, while organizational resilience also exerted a significant positive effect on strategic risk management. Furthermore, the mediation analysis confirmed that organizational resilience partially mediates the relationship between cybersecurity maturity and strategic risk management, indicating that cybersecurity capabilities become more effective when supported by resilient organizational structures.

The model demonstrated satisfactory predictive power, explaining 52.1% of the variance in strategic risk management, suggesting that cybersecurity maturity and organizational resilience are important determinants of effective strategic risk management in Iraqi banks. These findings highlight that cybersecurity should be viewed as a strategic organizational capability rather than merely a technical function, particularly in banking environments characterized by rapid digital transformation and increasing cyber threats.

From a practical perspective, the findings suggest that bank executives should integrate cybersecurity maturity into strategic risk management frameworks while strengthening organizational resilience to improve business continuity and long-term organizational performance. Such integration can enhance banks' ability to anticipate, respond to, and recover from cyber incidents without compromising their strategic objectives.

Despite these contributions, this study has several limitations. It focused exclusively on Iraqi commercial banks and employed a specific set of cybersecurity maturity and resilience indicators. Therefore, the generalizability of the findings to other financial sectors or countries may be limited. Future research may extend this model by examining additional organizational or technological variables, conducting cross-country comparisons, or employing longitudinal data to further validate the proposed relationships

- **Acknowledgements**

The author would like to thank the Department of Financial and Banking Sciences, College of Administration and Economics, University of Karbala, for providing academic support. The author also appreciates the valuable comments of the anonymous reviewers, which contributed to improving the quality of this manuscript.

- **Funding**

The author received no specific funding for this research.

- **Conflict of Interest**

The author declares no conflict of interest.

- **Author Contributions**

The author solely contributed to the conceptualization, methodology, data collection, formal analysis, writing of the original draft, review, editing, and final approval of the manuscript.

- **Data Availability**

The data supporting the findings of this study are available from the corresponding author upon reasonable request.

- **Ethical Approval**

Not applicable.

- **Consent for Publication**

Not applicable.

References

- Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of Xidian University*, 14(7), 1523–1536. <https://doi.org/10.37896/jxu14.7/174>
- Hasan, M. F., & Al-Ramadan, N. S. (2021). *Cyber-attacks and cyber security readiness: Iraqi private banks case*. *Social Science and Humanities Journal*, 5(8), 2312–2323. <https://sshjournal.com/index.php/sshj/article/view/739>
- Al-Duhaidahawi, H. M. K., Zhang, J., Abdulreda, M. S., Sebai, M., & Harjan, S. (2020). Financial technology (FinTech) and cybersecurity: Evidence from

- Iraqi banks. *International Journal of Research in Business and Social Science*, 9(6), 123–133. <https://doi.org/10.20525/ijrbs.v9i6.914>
- Al-Somali, S. A., Saqr, R. R., Asiri, A. M., & Al-Somali, N. A. (2024). Organizational cybersecurity systems and sustainable business performance of SMEs in Saudi Arabia: The mediating and moderating role of cybersecurity resilience and organizational culture. *Sustainability*, 16(5), 1880. <https://doi.org/10.3390/su16051880>
- Baur-Yazbeck, S., Frickenstein, J., & Medine, D. (2019). Cyber security in financial sector development. *CGAP Background Documents*, 5(2). <https://documents.worldbank.org/>
- Chockalingam, A., Dabadghao, S., & Soetekouw, R. (2018). Strategic risk, banks, and Basel III: estimating economic capital requirements. *The Journal of Risk Finance*, 19(3), 225–246. <https://doi.org/10.1108/JRF-11-2017-0186>
- Durst, S., Hinteregger, C., & Zieba, M. (2024). The effect of environmental turbulence on cyber security risk management and organizational resilience. *Computers & Security*, 137, 103591. <https://doi.org/10.1016/j.cose.2023.103591>
- Hidayat, V. K., & Wang, G. (2023). A comprehensive cybersecurity maturity study for nonbank financial institution. *Journal of System and Management Sciences*, 13, 525–543. <https://doi.org/10.33168/JSMS.2023.0327>
- Huamán, S., Ponce, L., & Wong, L. (2024). Maturity model for information access management of Peruvian IT service providers based on ISO/IEC 27001 and CMMI security controls. In *Proceedings of the 35th FRUCT Conference* (pp. 259–266). IEEE. <https://doi.org/10.23919/FRUCT61870.2024.10516365>
- Huang, H. H., Kerstein, J., Wang, C., & Wu, F. (2022). Firm climate risk, risk management, and bank loan financing. *Strategic Management Journal*, 43(13), 2849–2880. <https://doi.org/10.1002/smj.3437>
- Juliana, B. M., Prabowo, H., Alamsjah, F., & Hamsal, M. (2023). Building organizational resilience by developing customer orientation, digital adoption and organizational agility: An empirical study in the Indonesian banking industry. *Calitatea (Quality – Access to Success)*, 24(197), 75–83. <https://doi.org/10.47750/QAS/24.197.09>
- Khajehpour, M., Sedaghatparast, E., & Rabieh, M. (2022). Designing a comprehensive model of organizational resilience in the banking industry of Iran. *Asian Journal of Economics and Banking*, 6(1), 69–87. <https://doi.org/10.1108/AJEB-06-2021-0079>



- Lambelanova, R., & Toyib, A. (2024). Adapting an organizational culture to stay abreast of technological changes in Indonesia's government scientific sector. *Journal of Ethnic and Cultural Studies*, 11(1), 142–160.
<https://doi.org/10.29333/ejecs/1960>
- Mizrak, F. (2023). Integrating cybersecurity risk management into strategic management: A comprehensive literature review. *Research Journal of Business and Management*, 10(3), 98–108.
<https://doi.org/10.17261/Pressacademia.2023.1818>
- Muadzah, S., & Suryanto, S. (2024). *Organizational culture and resilience: Systematic literature review*. *Jurnal Ilmiah Manajemen, Ekonomi, & Akuntansi (MEA)*, 8(2), 1426–1440.
<https://doi.org/10.31955/mea.v8i2.4175>
- Omairah-Al-Yasari, M. N., & Saada, M. B. (2024). The impact of the board of directors on the cybersecurity risks in the Iraqi banking sector. *Pakistan Journal of Life and Social Sciences*, 22(1), 3964–3977.
<https://doi.org/10.57239/PJLSS-2024-22.1.00291>
- Oparanma, A. O., & Ulunma, E. P. (2019). Organizational resilience and corporate performance of deposit money banks in Port Harcourt, Nigeria. *International Journal of Business and Management Future*, 3(2), 1–12.
<https://doi.org/10.46281/IJBMF.V3I2.357>
- Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. *World Journal of Advanced Research and Reviews*, 21(3), 625–643. <https://doi.org/10.30574/wjarr.2024.21.3.0808>
- Rabii, A., Assoul, S., Ouazzani Touhami, K., & Roudies, O. (2020). Information and cyber security maturity models: A systematic literature review. *Information & Computer Security*, 28(4), 627–644.
<https://doi.org/10.1108/ICS-10-2019-0109>
- Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for business resilience: Issues and recommendations. *Sensors*, 23(15), 6666.
<https://doi.org/10.3390/s23156666>
- Thach, N. N., Hanh, H. T., Huy, D. T. N., Nga, L. T. V., Huong, L. T. T., & Vu, Q. N. (2021). Technology quality management of Industry 4.0 and cybersecurity risk management on current banking activities in emerging markets: The case of Vietnam. *International Journal for Quality Research*, 15(3), 845–856. <https://doi.org/10.24874/IJQR15.03-10>

Appendix 1

Table (3). Descriptive Statistics (Pooled Sample, 2014–2024)

Variable	Mean	Std. Dev.	Min	Max
Cybersecurity Maturity (Overall)	3.12	0.64	1.8	4.6
Organizational Resilience	3.45	0.58	2.1	4.8
Governance Score	3.28	0.71	1.6	4.7
Bank Size (Log Assets)	16.8	1.9	13.2	19.7
Strategic Risk Score	3.22	0.67	1.9	4.5
ROA (%)	1.34	0.98	-2.4	4.7
Cyber Incidents (per year)	4.1	2.8	0	12
Capital Adequacy (%)	14.5	3.4	10.1	23.8

Table (4). Evolution of Cybersecurity Maturity in Iraqi Banks (2014–2024)
(NIST-CSF Average Scores)

Year	Identify	Protect	Detect	Respond	Recover	Overall Maturity
2014	2.1	2.4	1.9	1.8	2	2.04
2015	2.2	2.5	2.1	2	2.2	2.2
2016	2.4	2.7	2.3	2.1	2.3	2.36
2017	2.6	2.9	2.5	2.3	2.4	2.54
2018	2.8	3.1	2.6	2.4	2.5	2.68
2019	3	3.2	2.8	2.6	2.8	2.88
2020	3.1	3.3	3	2.8	3	3.04
2021	3.3	3.5	3.2	2.9	3.1	3.2
2022	3.4	3.6	3.3	3.1	3.3	3.34
2023	3.6	3.8	3.4	3.3	3.4	3.5
2024	3.7	4	3.6	3.4	3.6	3.66

Table (5). Strategic Risk Indicators (2014–2024 Averages)

Strategic Risk Dimension	Mean Score (1–5)	Description
Risk Identification	3.15	Quality of identifying threats and vulnerabilities
Risk Assessment	3.08	Use of frameworks (ISO, Basel) for evaluation
Risk Mitigation	3.31	Effectiveness of controls and capital buffers
Risk Monitoring	3.34	Internal audit, compliance oversight