International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 3
Article Received: *25 July 2026* ***Revised:*** *12 August 2026* ***Accepted:*** *12 September 2026*

Building Operational Resilience in Egyptian Banks through Information Security Governance: The Role of Cyber Resilience Culture and Top Management Support

Abdullah Mohamed Zaky Elsaied
Cloud and Disaster Recovery Expert, Dammam, Saudi Arabia
Abdullah_zaky@live.com

Yousof Mohamed Salaheldin Mohamed
Cyber security technical lead, Dammam, Saudi Arabia
Salah.yousof@gmail.com

Amr Mohamed Abdelfatah Elsayed
Cybersecurity GRC Expert, Ryiadh, Saudi Arabia
eng.amrelsayed@outlook.com

Tarek Hisham El Rayes
Chief Information Security Officer, First Abu Dhabi Bank Misr (FABMISR), Cairo, Egypt
trayes2@gmail.com

Hossam Mohamed Sherif
Strategy, Governance, Risk, Compliance & Business Continuity Consultant, Dammam, Saudi Arabia
hosamdba@hotmail.com

Abstract—The accelerating digitalization of banking services has increased both operational efficiency and exposure to sophisticated cyber threats. Although financial institutions continue to invest in cybersecurity technologies, the literature remains comparatively fragmented across technical security, risk management, business continuity, governance, and operational resilience. This conceptual paper develops the Banking Information Security Governance and Operational Resilience (BISGOR) Framework to explain how Information Security Governance (ISG) can strengthen Operational Resilience (OR) in Egyptian banks. The framework positions Cyber Resilience Culture (CRC) as a mediating mechanism and Top Management Support (TMS) as a moderating condition. Grounded in the Resource-Based View (RBV) and Dynamic Capability Theory (DCT), the study integrates peer-reviewed research on information security governance, cyber resilience, operational resilience, security culture, and executive support. It argues that ISG establishes strategic alignment, accountability, risk ownership, oversight, and cross-functional coordination; CRC translates these formal mechanisms into shared preparedness, reporting, collaboration, learning, and adaptive behavior; and TMS strengthens this translation through visible commitment, resources, authority, and strategic direction. Five hypotheses are developed and a 30-item proposed operationalization is provided for subsequent empirical validation. The paper contributes to Information Security Management research by shifting the unit of analysis from isolated technical protection to governance-driven continuity of critical banking services and by addressing a geographically underrepresented African banking context.

Keywords- Information Security Governance; Operational Resilience; Cyber Resilience Culture; Top Management Support; Cybersecurity; Banking Sector; Egyptian Banks; Information Security Management.

II. INTRODUCTION

A. Background of the Study

The banking sector has undergone extensive digital transformation through mobile banking, cloud services, artificial intelligence, application programming interfaces, digital payments, and increasingly interconnected third-party ecosystems. These developments improve accessibility and efficiency but also expand the attack surface and create new operational dependencies. Financial institutions are particularly attractive cyber targets because of the value of financial assets, sensitive information, transaction infrastructures, and their systemic importance (Aslan et al., 2023; Gulyás & Kiss, 2023; Jang-Jaccard & Nepal, 2014).

Traditional cybersecurity programs have understandably emphasized preventive and detective controls. However, a bank may successfully contain a cyber incident while still failing to maintain a critical service. This distinction has moved attention from protection alone toward cyber resilience and operational resilience: the ability to withstand disruption, continue

important services, recover within acceptable conditions, and adapt after an incident (Dupont, 2019; Leo, 2020).

Financial-sector resilience is inherently cross-functional. Cybersecurity may prioritize containment, BCM may prioritize service restoration, ERM may assess risk exposure, IT may focus on technology recovery, Operations may prioritize customer continuity, and senior management must resolve trade-offs among these objectives. Resilience therefore depends not only on the maturity of each function but also on the governance mechanisms that coordinate them.

Miya and Joseph (2025), in a bibliometric analysis of 228 Scopus-indexed publications covering two decades of financial-sector cyber resilience, identify persistent fragmentation between resilience and risk management, insufficient emphasis on recovery and operational continuity, limited systems thinking, and inadequate attention to shared resilience culture. These gaps provide the principal point of departure for the present paper.

Information Security Governance (ISG) provides a plausible management mechanism for addressing this fragmentation. ISG moves information security from a narrow technical responsibility toward board-level alignment, accountability, risk ownership, oversight, policy, performance monitoring, and coordinated decision-making (Schinagl & Shahim, 2020; Soomro et al., 2016). Recent empirical work also confirms that business alignment, top-management support, awareness, and security controls materially influence Information Security Management performance (Almuqrin, 2024).

Accordingly, this paper develops BISGOR, a conceptual framework explaining how ISG may enhance OR through CRC and under stronger TMS, with the Egyptian banking sector as the intended contextual domain.

B. Research Problem

Cybersecurity effectiveness and operational resilience are related but not equivalent. Consider a ransomware attack on a bank's electronic transfer platform. The security team may isolate the affected servers and prevent lateral movement, thereby achieving a technical containment objective. Nevertheless, if customers cannot transfer funds for several hours, the institution still experiences an operational-resilience failure.

The management problem is therefore not simply whether cybersecurity, risk, BCM, IT, and Operations perform their individual duties. It is whether governance aligns their objectives, establishes decision rights, clarifies risk ownership, and enables coordinated action around critical services. Existing literature does not yet provide sufficient integrated explanation of how formal ISG becomes organizational resilience, particularly within Egyptian banks.

The central research problem is therefore: there is insufficient integrated understanding of how Information Security Governance contributes to Operational Resilience in Egyptian banks and how Cyber Resilience Culture and Top Management Support shape this relationship.

C. Research Gap

Theoretical gap: ISG, cybersecurity, cyber resilience, and OR are frequently developed in separate research streams, leaving the governance-to-resilience mechanism under-theorized (Dupont, 2019; Sepúlveda Estay et al., 2020).

Mechanism gap: formal governance does not automatically become resilient behavior. Security-culture research identifies management support, policy, awareness, and training as important cultural foundations, yet relatively few frameworks explain culture as a mediator between governance and resilience outcomes (Uchendu et al., 2021).

Leadership gap: TMS is commonly modeled as a general success factor. Less attention has been given to its role as a boundary condition that strengthens the extent to which governance becomes shared resilience culture.

Contextual gap: financial-sector cyber-resilience research remains geographically uneven, and Miya and Joseph (2025) explicitly identify underrepresentation of African contexts. Egyptian banking therefore offers a relevant context for theory development and later validation.

Methodological gap: much of the resilience literature is conceptual, bibliometric, review-based, or case-oriented. A coherent, falsifiable model linking governance, culture, leadership, and critical-service resilience remains needed.

D. Research Contributions

First, the paper integrates ISG and OR within one banking-oriented framework.

Second, it introduces CRC as the mediating mechanism through which formal governance can become shared preparedness, collaboration, learning, and adaptive behavior.

Third, it positions TMS as a moderator rather than merely an independent antecedent.

Fourth, it integrates RBV and DCT to explain both the strategic value and adaptive development of resilience capabilities.

Fifth, it tailors the framework to Egyptian banks, responding to an underrepresented African context.

Sixth, it provides a complete proposed operationalization that makes the conceptual framework empirically testable without claiming results that have not been collected.

E. Research Objectives and Questions

Objective	Corresponding Research Question
Examine the conceptual effect of ISG on OR.	RQ1: To what extent can ISG enhance OR in Egyptian banks?
Explain how ISG influences CRC.	RQ2: How can ISG influence CRC?
Explain how CRC contributes to OR.	RQ3: How can CRC strengthen OR?
Develop the mediating role of CRC.	RQ4: Does CRC theoretically mediate the ISG-OR relationship?
Develop the moderating role of TMS.	RQ5: Under what conditions can TMS strengthen the ISG-CRC relationship?

III. RELATED WORK AND THEORETICAL BACKGROUND

A. Information Security Governance

ISG refers to the structures, responsibilities, policies, decision rights, oversight mechanisms, and accountability arrangements through which information security is aligned with organizational objectives. Schinagl and Shahim (2020) describe the evolution of ISG from a technical basement issue to a boardroom concern. Soomro et al. (2016) likewise argue that information security management requires a holistic

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 3
Article Received: *25 July 2026* ***Revised:*** *12 August 2026* ***Accepted:*** *12 September 2026*

approach incorporating policy, awareness, business-IT alignment, infrastructure management, and human factors. In BISGOR, ISG is therefore treated as a strategic organizational capability rather than a collection of technical controls.

B. Operational Resilience

OR represents the capacity to continue important services during disruption, recover within acceptable conditions, and adapt following adverse events. In banking, OR is particularly important because technology failure or cyberattack can affect customers, payments, third parties, regulatory obligations, and financial stability. Leo (2020) identifies complexity, interconnectedness, third-party dependence, and digitalization as major drivers of operational-resilience concern in banking.

C. Cyber Resilience

Cyber resilience complements prevention-oriented cybersecurity by emphasizing anticipation, withstanding, response, recovery, and adaptation. Dupont (2019) argues that financial institutions require resilience because cyber incidents cannot be completely prevented. Miya and Joseph (2025) similarly show that financial-sector resilience requires integration of technology, risk management, continuity, governance, organizational preparedness, and culture.

D. Cyber Resilience Culture

CRC refers to shared organizational values and behaviors that support cyber preparedness, early reporting, cross-functional collaboration, learning, recovery, and continuous improvement. Uchendu et al. (2021) identify management support, policy, awareness, and training among recurring components of cybersecurity culture. Da Veiga and Martins (2015) demonstrate that information-security culture can be operationalized as an organizational construct. BISGOR extends this logic toward resilience-oriented culture rather than general awareness alone.

E. Top Management Support

TMS represents executive commitment expressed through strategic direction, visible sponsorship, resource allocation, communication, governance oversight, and organizational authority. Almuqrin (2024) identifies TMS as a significant factor in Information Security Management performance, while Uchendu et al. (2021) link management support with security culture. BISGOR therefore treats TMS as a condition that strengthens the conversion of formal governance into shared resilience behavior.

F. Summary of Previous Studies

Study	Context / Method	Main Contribution	Gap Relevant to BISGOR
Dupont (2019)	Financial institutions; conceptual	Positions resilience as complement to prevention.	No integrated ISG-CRC-TMS-OR model.
Leo (2020)	Banks; annual-report analysis	Highlights operational resilience, dependencies, measurement.	Disclosure focus; governance mechanism not tested.
Soomro et al. (2016)	Literature review	Calls for holistic information-security management.	No banking OR outcome.
Schinagl & Shahim (2020)	ISG literature review	Moves security from technical to board-level governance.	No integrated resilience culture pathway.
Uchendu et al. (2021)	Systematic culture review	Identifies management, policy, awareness, training.	Limited real-world framework evaluation; no OR mediation.
Almuqrin (2024)	Empirical SEM	Shows TMS, alignment, awareness, controls affect ISM performance.	Outcome is ISM performance, not OR.
Miya & Joseph (2025)	228 Scopus documents; bibliometric	Identifies technical bias, fragmentation, recovery and culture gaps.	Does not test integrated governance-culture-leadership-resilience model.
BISGOR	Conceptual theory integration	Links ISG, CRC, TMS, and OR in Egyptian banking.	Provides integrated and testable model.

IV. THEORETICAL FOUNDATION

A. Resource-Based View

The Resource-Based View (RBV) argues that valuable organizational resources and capabilities can contribute to sustained advantage (Barney, 1991). BISGOR conceptualizes ISG as such a capability: governance structures, accountability, security knowledge, decision rights, and risk ownership allow a bank to coordinate resources and protect critical services. The RBV therefore explains why mature governance can contribute to OR.

B. Dynamic Capability Theory

Dynamic Capability Theory (DCT) emphasizes the capacity to integrate, build, and reconfigure organizational capabilities under changing conditions (Teece et al., 1997). Cyber threats, technologies, regulations, and dependencies evolve continuously. CRC reflects this adaptive dimension because it embeds learning, preparedness, collaboration, and continuous improvement in organizational routines.

C. Integrated Theoretical Logic

RBV explains the strategic value of ISG; DCT explains how governance is translated and reconfigured into adaptive resilience. CRC acts as the behavioral translation mechanism, TMS acts as the leadership enabling condition, and OR represents the critical-service capability/outcome. This integrated logic provides the theoretical foundation for the five BISGOR hypotheses.

V. PROPOSED BISGOR FRAMEWORK AND HYPOTHESES

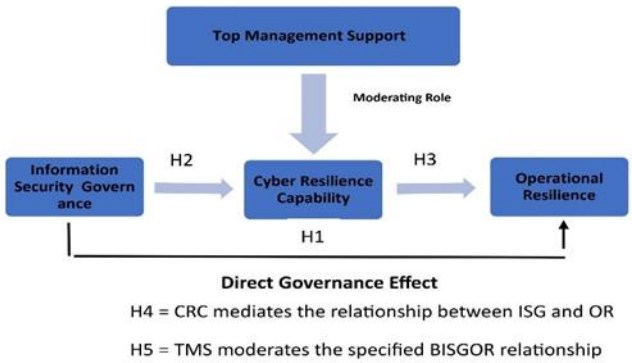

Figure 1. Proposed Banking Information Security Governance and Operational Resilience (BISGOR) Framework.

Figure 1 conceptualizes ISG as the principal antecedent of OR. ISG is expected to influence OR directly and indirectly through CRC. TMS is positioned as a moderator of the ISG-CRC relationship. The framework therefore integrates formal governance, organizational culture, leadership support, and critical-service resilience.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 3
Article Received: *25 July 2026* ***Revised:*** *12 August 2026* ***Accepted:*** *12 September 2026*

A. H1: ISG → OR

Effective governance aligns security decisions with business priorities, clarifies accountability and risk ownership, and coordinates security with continuity and operational requirements. H1: Information Security Governance has a positive effect on Operational Resilience in Egyptian banks.

B. H2: ISG → CRC

Governance shapes roles, communication, policy, awareness, and accountability. These mechanisms can influence how employees understand and enact resilience. H2: Information Security Governance has a positive effect on Cyber Resilience Culture.

C. H3: CRC → OR

Preparedness, shared responsibility, reporting, collaboration, and organizational learning should improve the ability to withstand and recover from cyber disruption. H3: Cyber Resilience Culture has a positive effect on Operational Resilience.

D. H4: Mediating Role of CRC

Formal governance may not produce resilience unless it becomes embedded in organizational behavior. H4: Cyber Resilience Culture mediates the relationship between Information Security Governance and Operational Resilience.

E. H5: Moderating Role of TMS

Executive commitment, resources, authority, and strategic communication can strengthen the implementation of governance and its cultural effects. H5: Top Management Support positively moderates the relationship between Information Security Governance and Cyber Resilience Culture.

VI. RESEARCH METHODOLOGY

A. Research Design

This study adopts an integrative conceptual research design aimed at theory integration and framework development. It does not report fabricated empirical results. Instead, it synthesizes established theoretical and empirical findings from Information Security Management, cyber resilience, operational resilience, organizational culture, leadership, and banking research to derive a coherent set of relationships culminating in BISGOR.

B. Literature Identification and Source Selection

The conceptual development was guided by peer-reviewed studies directly addressing ISG, cyber resilience, OR, information-security/cybersecurity culture, TMS, and banking resilience. Priority was given to peer-reviewed journal articles, systematic or integrative reviews, banking/financial-sector studies, management-oriented information-security research, recent gap-identification studies, and foundational theoretical sources. Miya and Joseph (2025) serves as the principal gap-identification study because it systematically maps two decades of financial-sector cyber-resilience research.

C. Inclusion and Exclusion Logic

Literature was considered conceptually relevant when it addressed governance or management of information security; organizational cyber resilience; continuity or recovery of critical services; security/resilience culture; senior-management support; integration of cybersecurity, risk management, and BCM; or banking operational resilience. Highly technical studies focused exclusively on algorithms, encryption, malware classification, or network configurations were not used as primary construct-development sources unless they provided direct organizational or financial-sector resilience insight.

D. Conceptual Synthesis Procedure

Stage	Purpose	Output
1. Domain fragmentation	Identify research streams treated separately.	Cybersecurity, ISG, ERM, BCM, cyber resilience, OR.
2. Organizational mechanisms	Identify mechanisms linking governance to resilience.	CRC and TMS.
3. Theoretical mapping	Map constructs to management theory.	RBV + DCT.
4. Relationship development	Translate synthesis into falsifiable paths.	H1-H5 and BISGOR.

E. Construct Operationalization

The present paper is conceptual, but each construct is operationalized to demonstrate empirical testability. The proposed wording is adapted to the banking context and should be expert-reviewed and pilot-tested before a future empirical study; the paper does not claim that all wording below is copied verbatim from prior validated scales.

Construct	Code	Proposed Measurement Item	Supporting Basis
ISG	ISG1	Information security objectives are clearly aligned with the bank's overall business objectives.	Schinagl & Shahim (2020); Almuqrin (2024)
ISG	ISG2	Roles and responsibilities for information security are clearly defined across the bank.	Schinagl & Shahim (2020); Soomro et al. (2016)
ISG	ISG3	Senior management regularly oversees information security risks and performance.	Almuqrin (2024)
ISG	ISG4	Information security risks are incorporated into enterprise risk-management processes.	Miya & Joseph (2025); Soomro et al. (2016)
ISG	ISG5	Formal governance mechanisms support compliance with information-security requirements.	Schinagl & Shahim (2020)
ISG	ISG6	Information-security decisions consider their impact on critical banking services.	Dupont (2019); Leo (2020)
ISG	ISG7	Information-security performance is regularly monitored and reported to appropriate management levels.	Almuqrin (2024)
ISG	ISG8	Cybersecurity, risk management, BCM, and banking operations are coordinated through defined governance mechanisms.	Miya & Joseph (2025)
CRC	CRC1	Employees understand that cyber resilience is a shared responsibility across the bank.	Uchendu et al. (2021); Miya & Joseph (2025)
CRC	CRC2	Employees are encouraged to report cybersecurity incidents and weaknesses promptly.	Da Veiga & Martins (2015)
CRC	CRC3	Different departments collaborate effectively when responding to cyber incidents.	Uchendu et al. (2021); Miya & Joseph (2025)
CRC	CRC4	Employees receive adequate awareness and training regarding their roles during cyber incidents.	Uchendu et al. (2021)
CRC	CRC5	The bank regularly learns from cyber incidents and incorporates lessons into future practices.	Miya & Joseph (2025)
CRC	CRC6	Employees can raise security concerns without inappropriate negative consequences.	Da Veiga & Martins (2015)
CRC	CRC7	Preparedness for cyber disruption is embedded in routine organizational activities.	Miya & Joseph (2025)
CRC	CRC8	Continuous improvement of cyber resilience is considered an organizational priority.	Uchendu et al. (2021)
TMS	TMS1	Top management demonstrates visible commitment to information security and cyber resilience.	Almuqrin (2024); Uchendu et al. (2021)
TMS	TMS2	Top management provides adequate resources for security and resilience initiatives.	Almuqrin (2024)
TMS	TMS3	Senior managers actively communicate the importance of cybersecurity and operational resilience.	Uchendu et al. (2021)
TMS	TMS4	Top management supports collaboration among cybersecurity, risk, BCM, IT, and business operations.	Miya & Joseph (2025)
TMS	TMS5	Senior management becomes directly involved when major cyber incidents threaten critical services.	Dupont (2019)
TMS	TMS6	Top management aligns information-security initiatives with strategic business priorities.	Almuqrin (2024); Schinagl & Shahim (2020)

Construct	Code	Proposed Measurement Item	Supporting Basis
OR	OR1	The bank can continue delivering critical services during significant cyber disruptions.	Dupont (2019); Leo (2020)
OR	OR2	Critical banking services can be restored within acceptable timeframes following cyber incidents.	Dupont (2019); Miya & Joseph (2025)
OR	OR3	The bank can withstand the operational impact of significant cyber incidents.	Dupont (2019)
OR	OR4	The bank has effective arrangements for responding to unexpected cyber disruptions.	Miya & Joseph (2025)
OR	OR5	The bank can adapt processes and controls following new cyber threats or major incidents.	Dupont (2019); Miya & Joseph (2025)
OR	OR6	Alternative arrangements are available to maintain critical services when primary systems are disrupted.	Leo (2020); Miya & Joseph (2025)
OR	OR7	Cyber incidents are managed in a way that minimizes disruption to customers and critical services.	Dupont (2019); Leo (2020)
OR	OR8	Lessons learned from disruptions are used to strengthen future operational resilience.	Miya & Joseph (2025)

F. Proposed Empirical Validation

A subsequent empirical study can use a quantitative cross-sectional survey of professionals in Information Security, Cybersecurity, ERM, Operational Risk, BCM, IT, Banking Operations, Compliance, Internal Audit, Digital Transformation, and relevant management roles across Egyptian banks. A five-point Likert scale can be used for the proposed reflective indicators. PLS-SEM is appropriate for simultaneously evaluating direct, mediating, and moderating relationships. Measurement assessment should include indicator reliability, internal consistency, convergent validity, discriminant validity, and collinearity; structural assessment should include path coefficients, R^2, effect sizes, predictive relevance, mediation, moderation, and bootstrapped confidence intervals.

G. Methodological Rigor and Ethics

Methodological rigor is supported by grounding BISGOR in foundational management theory and contemporary Information Security Management literature, explicitly defining construct boundaries, deriving relationships from identified gaps, and keeping a clear distinction between existing evidence, conceptual inference, and future empirical validation. The present conceptual paper uses published literature and does not involve human participants, customer data, confidential bank information, security configurations, or incident logs.

VII. CONCEPTUAL DISCUSSION

A. Governance as the Starting Point of Resilience

BISGOR proposes that resilience begins with coordinated governance rather than isolated controls. ISG establishes the architecture through which security, risk, continuity, recovery priorities, and critical-service objectives can be aligned.

B. Culture as the Translation Mechanism

Formal policies become operational only when they influence routine behavior. CRC explains how governance becomes shared preparedness, early reporting, cross-functional collaboration, learning, and continuous improvement.

C. Leadership as a Boundary Condition

The same governance design can produce different outcomes under different leadership conditions. Strong TMS supplies resources, strategic visibility, authority, and conflict resolution, thereby strengthening the ISG-CRC relationship.

D. From Cybersecurity Success to Service Resilience

BISGOR deliberately distinguishes technical containment from resilience of critical banking services. The ultimate management outcome is not merely whether an attack is blocked, but whether important services remain within tolerable disruption and recover effectively.

VIII. THEORETICAL AND PRACTICAL IMPLICATIONS

A. Theoretical Contributions

- Integrates ISG and OR in a single banking-oriented model.
- Explains the governance-to-resilience relationship through CRC.
- Extends TMS research by conceptualizing it as a moderator.
- Combines RBV and DCT to explain strategic value and adaptation.
- Responds directly to fragmentation, recovery, culture, and regional gaps identified in recent financial-sector cyber-resilience research.

B. Practical Implications

For banks, BISGOR provides a management blueprint for connecting Information Security, Cybersecurity, ERM, BCM, IT, Operations, and Executive Management around critical services. For executives, it highlights visible sponsorship, resources, accountability, and cross-functional authority. For CISOs, it broadens performance from technical metrics toward continuity and recoverability. For risk and BCM functions, it creates an explicit mechanism for integrating cyber risk with service resilience. For regulators, it offers a structured way to assess whether governance, culture, and leadership conditions support resilience beyond technical compliance.

IX. LIMITATIONS AND FUTURE RESEARCH

The paper is conceptual and therefore does not claim empirical confirmation of the proposed relationships.

The framework is tailored to Egyptian banking; generalization to other countries and sectors requires validation.

CRC is intentionally narrower than general information-security culture and should be tested for discriminant validity.

Future research should examine bank size, ownership, digital maturity, outsourcing intensity, and regulatory profile as controls or moderators.

Future empirical work may validate BISGOR using PLS-SEM, longitudinal designs, cross-country comparisons, objective resilience indicators, case studies, or mixed methods.

Extensions may incorporate cybersecurity maturity, organizational agility, digital trust, third-party risk governance, or ERM maturity.

X. CONCLUSION

Cyber threats have transformed information security from a predominantly technical concern into a strategic management challenge for financial institutions. Preventing incidents remains essential, but a bank's ability to maintain and restore critical services when prevention fails has become equally important. This paper develops BISGOR to explain how ISG may enhance OR through CRC and under stronger TMS.

Grounded in RBV and DCT, BISGOR conceptualizes ISG as a strategic organizational capability, CRC as the behavioral mechanism through which governance becomes resilience, TMS as the leadership condition that strengthens this transformation, and OR as the continuity and adaptive capability of critical banking services. The framework therefore moves beyond isolated cybersecurity controls toward governance-driven resilience.

The principal contribution is an integrated, falsifiable model that responds to recent calls for stronger integration of cybersecurity, risk management, recovery, organizational preparedness, and shared resilience culture in the financial sector. The Egyptian banking context provides a relevant setting for subsequent validation and contributes to a geographically underrepresented stream of cyber-resilience research.

XI. REFERENCES

1- Almuqrin, A. (2024). How about enhancing organizational security: Critical success factors in information security management performance. Journal of Global Information Management, 32(1), 1-18. https://doi.org/10.4018/JGIM.358745
2- Aslan, A., Ozkan-Okay, M., Yilmaz, A., & Aksu, M. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333. https://doi.org/10.3390/electronics12061333
3- Barney, J. (1991). Firm resources and sustained competitive advantage. Journal of Management, 17(1), 99-120. https://doi.org/10.1177/014920639101700108
4- Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. Computer Law & Security Review, 31(2), 243-256. https://doi.org/10.1016/j.clsr.2015.01.005
5- Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. Journal of Cybersecurity, 5(1), tyz013. https://doi.org/10.1093/cybsec/tyz013
6- Gulyás, O., & Kiss, G. (2023). Impact of cyber-attacks on the financial institutions. Procedia Computer Science, 219, 84-90. https://doi.org/10.1016/j.procs.2023.01.267
7- Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973-993. https://doi.org/10.1016/j.jcss.2014.02.005
8- Laxman, N., Krohmer, D., Damm, M., Schwarz, R., & Antonino, P. O. (2023). Understanding resilience: Looking at frameworks & standards—A systematic study from cyber perspective. In 2023 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 295-300). IEEE.
9- Leo, M. (2020). Operational resilience disclosures by banks: Analysis of annual reports. Risks, 8(4), 128. https://doi.org/10.3390/risks8040128
10- Miya, N. F., & Joseph, N. (2025). Banking on resilience: 20 years of cybersecurity evolution. South African Journal of Information Management, 27(1), a2019. https://doi.org/10.4102/sajim.v27i1.2019
11- Schinagl, S., & Shahim, A. (2020). What do we know about information security governance? From the basement to the boardroom: Towards digital security governance. Information & Computer Security, 28(2), 261-292. https://doi.org/10.1108/ICS-02-2019-0033
12- Sepúlveda Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. Computers & Security, 97, 101996. https://doi.org/10.1016/j.cose.2020.101996
13- Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009
14- Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. Strategic Management Journal, 18(7), 509-533. https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z
15- Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109, 102387. https://doi.org/10.1016/j.cose.2021.102387