Cybersecurity and Audit Resilience in Digital Finance: Global Insights and the Pakistani Context

Muhammad Asif[1], Huma Shah[2] and Hafiz Abdul Hai Asim[3]

https://doi.org/10.62345/jads.2025.14.3.47

Abstract

The rapid digitalization of finance has intensified cyber threats, making cybersecurity indispensable to audit resilience. This paper aims to synthesize global insights on cybersecurity and audit resilience in digital finance, analyse specific challenges in Pakistan, and identify actionable strategies for fostering a robust digital financial ecosystem. A comprehensive literature review was conducted across multiple databases (Semantic Scholar, Google Scholar, Dimension, Lens, PubMed). An initial 995 papers were identified, 655 screened, 486 deemed eligible, and 35 most relevant papers were included for in-depth analysis. Eight unique search groups covered foundational concepts, global and local contexts, regulatory frameworks, and critiques of these areas. Global literature affirms cybersecurity frameworks (NIST CSF, ISO/IEC 27001) and AI-driven analytics as crucial for enhancing audit resilience. Human factors (digital literacy, training) remain critical vulnerabilities. However, in Pakistan, challenges include partial implementation of regulatory guidelines, pervasive digital literacy gaps, weak governance, and significant third-party dependencies. These factors collectively impede effective cyber-audit resilience, creating a gap between global best practices and local realities. This review uniquely bridges global perspectives on cyber-audit resilience with the specific institutional and socio-economic context of Pakistan. It contributes theoretically by using Institutional and Organizational Resilience Theories to explain implementation disparities. This systematic review offers policy-relevant solutions to Pakistani policymakers, regulators, auditors, and financial institutions for enhancing audit integrity and fostering a secure digital financial landscape.

Keywords: Cybersecurity, Audit Resilience, Digital Finance, FinTech, Regulatory Frameworks.

Introduction

The digitalization of the financial services industry has ushered in a new era of efficiency, access, and innovation, fundamentally transforming how financial services are produced and accessed globally. The sector's increasing use of advanced technological applications (cloud computing, AI, blockchain, and mobile platforms) has significantly heightened the sophisticated profile of cyber threats to which financial institutions are being exposed (Saeed et al., 2023; Cheng et al., 2024; Wang et al., 2024; Adejumo & Ogburie, 2025; Reddem, 2024; Oyeniyi et al., 2024). Here, every aspect of cybersecurity has a core and foundational role in every aspect of audit resilience, not

[1]*Assistant Professor, Federal Urdu University of Arts, Science, and Technology, Islamabad.*
Corresponding Author Email: dr.asifmails@gmail.com
[2]*PhD Scholar, Department of Education, GC University Faisalabad. Email: humaalizaidi53@gmail.com*
[3]*MPhil Management Science and Principal, GHS Laleka, School Education Department, Bahawalnagar, Pakistan. Email: asimawans786@gmail.com*

Compliance with ethical standards: There are no conflicts of interest (financial or non-financial). This study did not receive any funding.

only to prove and protect digital assets, but to protect and preserve the entire financial system's integrity, reliability, and trust (Saeed et al., 2023; Cheng et al., 2024; Wang et al., 2024; Adejumo & Ogburie, 2025; Reddem, 2024; Oyeniyi et al., 2024).

In the modern digital finance ecosystem, this denotes the enhanced capacity of financial institutions and their control systems to actively anticipate, effectively endure, and swiftly recover from a disruptive incident, especially those of cyber origin. The systemic pressure and the reciprocal nature of digital finance increases (amplifies) the effects of any given breach, which can cause a systemic breakdown within the ecosystem, undermine consumer confidence, destabilize markets, and impose a severe regulatory sanction and an irreparable reputational damage on the institutions (Cheng et al., 2024; Adejumo & Ogburie, 2025; Reddem, 2024). Therefore, cybersecurity is not a peripheral concern. It is an inherent part of the audit process, through which auditors can analyze the emerging risks accurately, confirm the adherence to the evolving standards, and guarantee continuity of essential financial processes in the face of persistent threats (Saeed et al., 2023; Cheng et al., 2024; Wang et al., 2024; Adejumo & Ogburie, 2025; Reddem, 2024; Oyeniyi et al., 2024). In particular, the ability to preserve and uphold audit integrity while assuring confidence, even in the midst of cyber turbulence, is exceptionally fundamental to sustaining stakeholder confidence and regulatory equilibrium.

In the digital finance space, it is noteworthy and concerning that high and low sophistication cyber threats are on the rise, including highly advanced ransomware assaults, targeted phishing attacks, intricate deep fake impersonation schemes, and more (Adejumo & Ogburie, 2025; Katuri, 2025; Cheng et al., 2024; Saeed et al., 2023; Ali et al., 2024; Oyeniyi et al., 2024; Dawodu et al., 2023). The multifaceted deployment of cloud services, the rapid development of AI-powered finance, and the increasing availability of mobile money apps all serve to amplify the threats. The level of investment and the critical nature of the data at stake require not only strong cybersecurity and thorough audit processes, but also effective compliance policies and processes, especially considering the enhanced regulatory environment (Olutimehin, 2025; Reddem, 2024; Grigoryan & Mirzoyan, 2023; Yedluri, 2025; Hussain et al., 2023; Kolo et al., 2024; Oluoha et al., 2024).

This reality applies to many emerging economies, where the need to strengthen audit cybersecurity has become an urgent necessity. Pakistan, in particular, comes to the forefront as the digital finance ecosystem is currently undergoing robust, rapid, and accelerated growth. The nation's deepening financial inclusion and innovation can be attributed to the rapid growth of FinTech startups, widespread mobile banking, and increasing use of outsourced IT services (Rehman, 2021; Ali et al., 2025; Jabeen et al., 2025; Nadeem et al., 2023). Digitalaysia has transformed the positive aspect, and the digital weaknesses of the Pakistan environment sensitive (characteristic) to those obsolete. These are the gaps in deteriorated (unacceptable) infrastructure, pockets of neophobic digital illiteracy, and emerging techno-regulatory frameworks that are unable to keep pace with technological obsolescence (Rehman, 2021; Ali et al., 2025; Jabeen et al., 2025; Nadeem et al., 2023).

Despite the efforts of the primary regulatory units, including the State Bank of Pakistan (SBP) and the Securities and Exchange Commission of Pakistan (SECP), to strengthen cybersecurity standards and promote optimal practices, the situation remains inconsistent in the financial sector. A significant number of institutions are still unable to ensure the effective implementation of robust cybersecurity measures in their audit procedures, being often deterred by operational constraints in the form of restricted financial resources, the pronounced shortage of human resources well-versed in cyber-auditing, and decentralized control (Rehman, 2021; Ali et al., 2025; Jabeen et al., 2025; Nadeem et al., 2023). The audit profession is itself facing a steep adaptation

process as the conventional audit practices are not proving sufficiently effective to meet the complexity of digital risk and the new needs of cyber resilience (Rehman, 2021; Ali et al., 2025; Jabeen et al., 2025; Nadeem et al., 2023; Saeed et al., 2023; Obiki-Osafiele et al., 2024; Hussain et al., 2023; Ali et al., 2024; Oluokun et al., 2024; Oyeniyi et al., 2024; Dawodu et al., 2023; Kafi & Akter, 2023; Oladele et al., 2023; Javaheri et al., 2023; Wang et al., 2024). The recent high-profile cyberattacks on Pakistani banks, e-commerce platforms, and payment systems have *pointed to* the lack of effectiveness in both technological defenses and governance frameworks. The overall capacity of the financial sector to withstand and recover from a sophisticated cyberattack remains a significant concern (Rehman, 2021; Ali et al., 2025; Jabeen et al., 2025; Nadeem et al., 2023).

It is within this context of *intricate and shifting situations* that the present review paper pursues a tripartite purpose. First, it aims to critically establish the case for cybersecurity as an indivisible component of audit resilience in the age of digital finance, reflecting the global consensus on the dynamic threat landscape and its implications for financial assurance. Second, it examines the challenges, vulnerabilities, and opportunities confronting Pakistan's financial sector as it undergoes accelerated digitalization, situating these within both local realities and international benchmarks. Third, the review synthesizes global and national literature to identify practical, evidence-based strategies for building a robust, secure, and dependable digital financial ecosystem in Pakistan. Accomplishing these goals will enhance the author's contributions to the management accounting, auditing, and digital finance domains by advancing the literature on the interplay between cybersecurity and auditing in the context of the 'auditing reshaped' proposal. For developing nations, the insights contained in the studies will help policymakers, regulators, auditors, and financial entities strengthen the digital financial system, while also outlining an important future research agenda at the intersection of technology, auditing, and Accountability (Saeed et al., 2023; Cheng et al., 2024; Wang et al., 2024; Rehman, 2021; Adejumo & Ogburie, 2025; Ali et al., 2025; Jabeen et al., 2025; Nadeem et al., 2023; Reddem, 2024; Oyeniyi et al., 2024).

Methodology

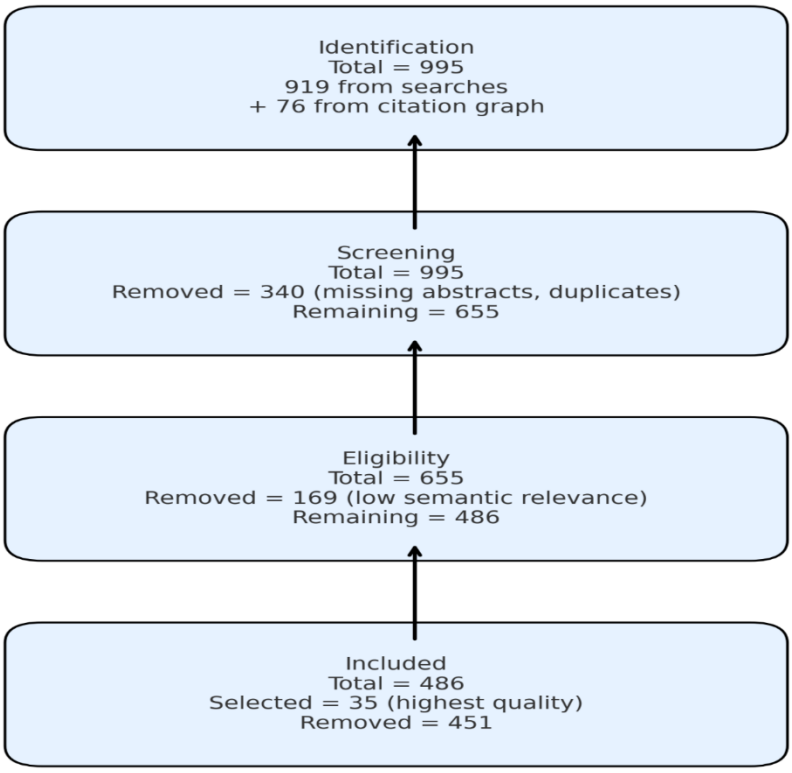
The initial search strategy was designed to cover foundational concepts, global and local literature, regulatory frameworks, and critical analyses. These groups combined keywords such as "cybersecurity," "digital finance," "fintech," "audit resilience," "financial technology," "cyber threats," "regulatory frameworks," "AI-driven fraud detection," and "Pakistan financial sector" with Boolean operators (AND, OR) to refine the search. Examples of search strings included: ("cybersecurity" AND "digital finance" AND "audit resilience"), ("fintech Pakistan" AND "cybersecurity challenges"), ("AI" AND "fraud detection" AND "audit resilience"), and ("regulatory compliance" AND "cyber risk" AND "financial services"). The search was deliberately restricted to the period between 2020 and 2025, ensuring that the review captured the most up-to-date debates, regulatory frameworks, and challenges in cybersecurity and audit resilience. The implementation of all strategy components was instrumental in producing a comprehensive analysis that incorporated insights from both the technology and governance domains.

The first phase of the identification process resulted in the Collection of 995 papers, of which 655 were subjected to a first-level screening exercise guided by titles and abstracts to determine their relevance to cybersecurity, digital finance, and audit resilience. Papers falling outside the scope were excluded, including those addressing purely technical aspects of cybersecurity without financial relevance, as well as finance-related studies that lacked a digital or auditing dimension.

Only English-language articles were considered, with preference given to those published in reputable journals, defined as peer-reviewed and indexed in Google Scholar, Semantic Scholar, or comparable academic databases. Eligibility at this stage required a clear focus on cybersecurity, digital finance, or audit resilience in either conceptual or applied terms. The most relevant papers were those that provided rigorous methodological frameworks, robust empirical findings, or distinctive insights into the Pakistani financial sector.

Following this process, 486 articles were deemed qualified for full-text review. Each article was examined in detail to evaluate its contributions to the research questions, methodological soundness, and applicability to both global and Pakistani contexts. Articles that failed to engage substantively with cybersecurity or audit resilience in digital finance, or that lacked critical insights, were excluded at this stage. From this pool, 35 articles were selected as the most relevant and significant. These were distinguished by their empirical strength, theoretical depth, and contribution to either global perspectives or the specific dynamics of Pakistan's financial sector. This rigorous multi-phase selection process is represented graphically in the flow diagram (Figure 1), which outlines the number of identified, screened, eligible, and finally included studies. The systematic methodology employed here ensures both transparency and replicability of the review process.

Figure 1: Flow diagram of the search and selection process for included papers



Results

The selected literature provides the complex view of cybersecurity and audit resilience in the fast-developing digital financial space. The 35 articles under consideration represent a wide spectrum of methodological approaches that may be systematic reviews, empirical studies, conceptual

analyses, case studies, and technical frameworks. A larger proportion of these publications is devoted to the complex overlap of cybersecurity and audit resilience in the global context and the complex processes of the emerging markets. A distinct body of literature focuses on the particular issues and opportunities of the financial sector in Pakistan (Olutimehin, 2025; Saeed et al., 2023; Obiki-Osafiele et al., 2024; Hussain et al., 2023; Ali et al., 2024; Oluokun et al., 2024; Oyeniyi et al., 2024; Dawodu et al., 2023; Kafi & Akter, 2023; Oladele et al., 2023; Javaheri et al., 2023; Wang et al., 2024; Slapničar et al., 2020; Ezinwa et al., 2024).

Attributes of the Literature

The 35 chosen articles present a cross-sectional view of cybersecurity and audit resilience in digital finance that covers the different methodological approaches including systematic reviews, empirical analysis, case study, and conceptual investigations. The literature is predominantly on the convergence of these issues in the global and emerging market setting and there is a sub-literature on the financial sector of Pakistan. The central thematic threads of the body of work include the organizational strategies, technological innovations (including AI-based solutions), the key role of the human factors, and how a secure digital financial environment is influenced by regulatory and governance frameworks. To illustrate this diversity, a comparison of five illustrative studies is provided in Table 1. Further analysis of the literature's structure, including frequently contributing authors and journals, is depicted in Table 2, highlighting established research communities in this evolving domain.

Table 1: Comparison of key studies on cybersecurity and audit resilience in digital finance

Paper	Methodology	Focus Area	Key Results	Regulatory Context
(Olutimehin, 2025)	Logistic regression, sector analysis	Banking & DeFi	Compliance reduces attacks; DeFi needs tailored frameworks	NIST CSF, ISO/IEC 27001, PCI DSS
(Saeed et al., 2023)	Systematic literature review	Digital transformation & resilience	DT increases efficiency but raises cyber risks; staged readiness needed	PRISMA, global standards
(Oluokun et al., 2024)	Exploratory study	Fintech, AI & GRC	AI + GRC enhances resilience, compliance, and risk management	Regulatory compliance focus
(Dawodu et al., 2023)	Strategic review	Accounting & cybersecurity	Alignment critical for data confidentiality and financial security	GDPR, PCI DSS, global standards
(Wang et al., 2024)	Qualitative interviews	Banking sector (Pakistan)	Integration, compliance, and training are key for resilience	SBP, SECP, local governance

Table 2: Authors & journals that appeared most frequently in the included papers.

Type	Name	Papers
Author	Adetunji Paul Adejumo	(Adejumo & Ogburie, 2025; Adejumo & Ogburie, 2025)
Author	Saqib Saeed	(Saeed et al., 2023; Saeed et al., 2023)
Author	Chinonso Peter Ogburie	(Adejumo & Ogburie, 2025; Adejumo & Ogburie, 2025)
Journal	World Journal of Advanced Research and Reviews	(Adejumo & Ogburie, 2025; Adejumo & Ogburie, 2025; Mukala, 2025; Oladele et al., 2023)
Journal	International Journal of Social Science Exceptional Research	(Hussain et al., 2023; Oluoha et al., 2024)
Journal	Sensors (Basel, Switzerland)	(Saeed et al., 2023; Saeed et al., 2023)

Main Findings: Cybersecurity as Audit Resilience Backbone

The collected literature consistently affirms cybersecurity as the indispensable foundation for audit resilience within digital finance. This foundational role manifests primarily through three interconnected areas, each presenting both robust capabilities and inherent challenges for the auditing profession.

Firstly, the implementation of robust cybersecurity frameworks and standards is widely recognized as critical for mitigating cyber risks and bolstering audit capabilities. Global standards such as NIST CSF, ISO/IEC 27001, PCI DSS, and GDPR provide structured, multi-layered approaches for identifying, protecting, detecting, responding to, and recovering from cyber incidents (Olutimehin, 2025; Reddem, 2024; Grigoryan & Mirzoyan, 2023; Saeed et al., 2023). Compliance with these frameworks, especially when reinforced by routine and independent audits, significantly contributes to improving the defensive posture of an institution and the auditor's capacity to report on the integrity of data and system controls. To the auditors, these frameworks provide a systematic outline for evaluating the level of security maturity and the organization's capacity to provide reliable financial data. Nevertheless, it is often noted that contextual adaptations would be required when dealing with new and rapidly evolving architectures such as Decentralized Finance (DeFi) because of the architectural complexities involved and unique governance frameworks that would challenge the transferability of such traditional controls (Olutimehin, 2025; Yedluri, 2025; Slapničar et al., 2020).

Secondly, AI-powered threat detection and sophisticated analytics are a transformative element, as they will help institutions to move beyond the purely reactive approaches to incidents to proactive and predictive monitoring. To detect abnormal tendencies (patterns) that could be indicative of fraud or cyberattacks, AI-based systems in real-time analyze large volumes of data based on transactions, network traffic, and user behavior (Adejumo & Ogburie, 2025; Mukala, 2025; Yedluri, 2025). Such a capability substantially improves detection rates and incident response times, which directly lead to greater effectiveness of auditing by facilitating continuous monitoring, risk management, and verification of compliance. Although the audit profession is advancing, it remains challenging to prove the integrity and impartiality of AI algorithms, which necessitate the development of new skills in data science and interpretable AI to ensure transparency and confidence in automated controls (Oluokun et al., 2024; Thapaliya, 2024). Lastly, the literature unanimously emphasizes the importance of human factors. Human error and the overall shortage in digital literacy and exposure to social engineering (e.g., phishing) or insider threats are increasingly becoming prominent vulnerabilities despite the increasing technological

sophistication (Katuri, 2025; Saeed et al., 2023; Lois et al., 2020; Wang et al., 2024). The detailed training programs for employees, the process of continuous awareness, and the cultivation of a highly cybersecure organizational culture are deemed vital countermeasures. The premise that the best technology is not a silver bullet to resilience, unless a vigilant and informed workforce is present, remains a persistent challenge to both management and auditors (Obiki-Osafiele et al., 2024; Hussain et al., 2023; Ezinwa et al., 2024).

Regulatory and Governance Developments

The increasing cyber threat environment has dramatically altered the regulatory and governance structures across all regions worldwide, with a direct impact on audit resilience in digital finance. Accountability and disclosure of cyber risks, increased audit responsibility, and operational resilience: International organizations and domestic regulators are becoming stricter in their requirements, asking financial institutions to disclose more about cyber risks, conduct their audits more responsibly, and enhance their operational resilience. The most notable ones are the Digital Operational Resilience Act (DORA) of the European Union, which requires all digital operational resilience testing and incident reporting, and the new cybersecurity disclosure requirements of the U.S. Securities and Exchange Commission, which imposes a responsibility on all major companies to disclose material cyber incidents promptly (Olutimehin, 2025; Reddem, 2024; Cohn et al., 2020). Additionally, operational resilience is becoming an integral part of the Basel III/IV-based frameworks, rendering it a systemic issue (Grigoryan & Mirzoyan, 2023; Yedluri, 2025). These laws will compel institutions to take active measures to address cyber risks, publicly report incidents, and integrate resilience into their core operations.

This change in regulation marks a milestone in the conceptualization of audit resilience. As a process, the practice must be perceived as dynamic and adaptive, rather than merely a compliance-focused exercise. This requires sustained observation of cyber threats, the promotion of joint regulatory conditions, and the systematic integration of cyber-risks in every aspect of audit activity (Olutimehin, 2025; Reddem, 2024; Grigoryan & Mirzoyan, 2023). There are growing expectations that auditors will take a more proactive role in resilience efforts, addressing the constantly evolving risks, and providing advice to their clients on resilience strategies in addition to their responsibilities of verifying past transactions (Hussain et al., 2023; Kolo et al., 2025; Slapničar et al., 2020; Wang et al., 2024). This adaptive model focuses on learning through experience, the pursuit of continuous improvement, and the capacity of audit functions to restructure swiftly in response to emerging threats, thereby ensuring ongoing assurance in the face of technological volatility.

The Pakistani Context: Gaps and Opportunities

Although global practices offer a sound model for making cyber-audits more robust, their implementation in the new market, Pakistan, is influenced by the systems' specific weaknesses of implementation, as well as the gigantic possibilities of personalization. Pakistan is experiencing a period of rapid growth in digital finance. It is characterized by the high level of FinTech startup proliferation, the expansion of mobile banking services across the board, and an increased reliance on third-party IT service providers (Rehman, 2021; Ali et al., 2025; Jabeen et al., 2025; Nadeem et al., 2023). This degree of digitalization has not only had a tangible positive impact on financial inclusion and innovation at the national level but has also highlighted systemic vulnerabilities in a local context.

These kinds of weaknesses are intricate in nature and are owed to several significant reasons. To start with, the legacy infrastructure that is yet to be retired in most established financial institutions is inherently susceptible, as the systems are more challenging to secure, repair, and integrate with the latest cybersecurity safeguards. Second, the lack of digital literacy among large groups of the population exposes users to low-end social engineering tricks, which effectively turn them into convenient vectors in cyberattacks (Rehman, 2021; Ali et al., 2025; Jabeen et al., 2025; Nadeem et al., 2023). This poses a greater danger, as the employees themselves or the customers may not be aware that they are committing breaches. Third, due to a dynamic regulatory framework, it will be susceptible to failure to keep up with the swift technological shifts, which may generate periods when new products in digital finance fall into a regulatory grey space, thus increasing systemic risk. Such breaches of technological protection and governance systems are particularly evident in the example of the major cyberattacks on Pakistani banks, e-commerce platforms, and payment systems in recent years, which have posed the questions of the overall financial sector robustness to such advanced cyber-attacks (Rehman, 2021; Ali et al., 2025; Jabeen et al., 2025; Nadeem et al., 2023).

Although the most significant regulatory authorities, such as the State Bank of Pakistan (SBP) and the Securities and Exchange Commission of Pakistan (SECP), are trying their best to improve their cybersecurity policies and best practices, the actual implementation of these in the financial sector remains unbalanced. The challenge of effectively incorporating adequate cybersecurity controls in their audit procedures is still a problem facing many institutions, which is often constrained by realistic factors like limited financial resources, an acute lack of qualified staff dedicated to cyber-audits, and divided oversight functions (Saeed et al., 2023; Obiki-Osafiele et al., 2024; Hussain et al., 2023; Wang et al., 2024). This often results in a compliance-focused mindset, rather than a proactive resilience strategy.

Moreover, the high rate of FinTech startups and the growing reliance on third-party IT vendors bring about distinct vulnerabilities. The FinTechs also encourage innovation, but due to their rapid pace of growth, they might overlook the importance of robust cybersecurity practices, having more limited security teams and less developed systems as compared to banking entities. The reliance on third-party services dramatically increases the attack surface, as a breach of one vendor can affect multiple financial institutions simultaneously (Saeed et al., 2023; Obiki-Osafiele et al., 2024; Ali et al., 2024; Oluokun et al., 2024). Local research strongly emphasizes the creation of purpose-designed regulatory frameworks that directly pertain to FinTechs, capacity-building measures to solve (address) the skills gap, and the concept of regulatory experimentation (e.g., sandboxes) to test innovative resilience solutions in a controlled setting. It is also emphasized that cybersecurity and related contractual requirements must be managed at high levels regarding all the vendors in the entire supply chain in the digital finance sector (Oyeniyi et al., 2024; Dawodu et al., 2023; Kafi & Akter, 2023; Oladele et al., 2023; Javaheri et al., 2023). Therefore, proactive and adaptive measures play a significant role in cultivating a secure and robust virtual finance ecosystem in Pakistan.

Discussion

The literature indicates that audit resiliency in digital finance is founded on a cybersecurity-based pillar, which is crucial for maintaining trust, stability, and operational continuity in the digital age of rapid change. The information in Section 3 obtained reveals a specific trend: the robust framework, the tools driven by AI, and the strict adherence to the regulations are all the building blocks of the appropriate defense mechanisms against the constantly increasing variety of cyber-

threats (Olutimehin, 2025; Adejumo & Ogburie, 2025; Reddem, 2024; Grigoryan & Mirzoyan, 2023; Yedluri, 2025; Hussain et al., 2023) This kind of transformation presupposes that audit functions are not realised reactively but become an inseparable part of proactive risk management and incident response. (Olutimehin, 2025; Reddem, 2024; Grigoryan & Mirzoyan, 2023; Yedluri, 2025; Hussain et al., 2023; Kolo et al., 2025; Oluoha et al., 2024; Oyeniyi et al., 2024; Dawodu et al., 2023; Kafi & Akter, 2023; Oladele et al., 2023; Ali et al., 2025; Javaheri et al., 2023; Saeed et al., 2023; Cohn et al., 2020; Wang et al., 2024; Slapničar et al., 2020; Ezinwa et al., 2024).

The research highlights significant (substantial) gaps, especially in emerging markets like Pakistan. Here, the partial implementation of existing guidelines, persistent digital literacy deficits, and inherent weaknesses in governance structures collectively impede substantial progress in building robust cyber-audit resilience (Saeed et al., 2023; Obiki-Osafiele et al., 2024; Hussain et al., 2023; Ali et al., 2024; Oluokun et al., 2024; Oyeniyi et al., 2024; Dawodu et al., 2023; Kafi & Akter, 2023; Oladele et al., 2023; Javaheri et al., 2023; Wang et al., 2024). While a wealth of global best practices and frameworks are readily available, their effective adaptation to localized contexts remains a formidable challenge. This necessitates targeted empirical studies, thoughtful regulatory experimentation, and comprehensive capacity-building initiatives tailored to the specific socio-economic and institutional realities of these regions.

The quality of evidence supporting the effectiveness of established cybersecurity frameworks (e.g., NIST CSF, ISO/IEC 27001) and AI-driven solutions is generally strong. Numerous empirical and sectoral studies across various regions consistently demonstrate that adherence to these frameworks significantly reduces the likelihood of cyberattacks and enhances the capacity for recovery. For instance, the claims detailed in Table 3, such as "Compliance with cybersecurity frameworks reduces cyberattack likelihood and enhances audit resilience" and "AI-driven threat detection and analytics significantly improve real-time monitoring and incident response," are supported by substantial evidence (scores of 9/10 and 8/10, respectively) from multiple, peer-reviewed sources (Olutimehin, 2025; Reddem, 2024; Grigoryan & Mirzoyan, 2023; Yedluri, 2025; Hussain et al., 2023; Kolo et al., 2025; Oluoha et al., 2024; Oyeniyi et al., 2024; Dawodu et al., 2023; Kafi & Akter, 2023; Oladele et al., 2023; Ali et al., 2025; Javaheri et al., 2023; Saeed et al., 2023; Slapničar et al., 2020; Ezinwa et al., 2024; Adejumo & Ogburie, 2025; Mukala, 2025; Obiki-Osafiele et al., 2024; Adewumi et al., 2024; Jony et al., 2024; Owolabi et al., 2024; Patricia et al., 2024; Kokogho et al., 2025; Odeyemi et al., 2024; Thapaliya, 2024). This robustness is often derived from quantitative analyses of incident data, case studies demonstrating successful implementations, and comparative studies across different financial institutions.

Conversely, the evidence base is notably weaker for claims about the seamless or automatic implementation of global best practices in developing contexts, as well as the inherent sufficiency of current regulatory approaches in rapidly evolving markets. For example, the assertion that “local constraints limit seamless implementation of global best practices in developing countries” receives a weak evidence strength score (3/10) in Table 3, because while local studies consistently highlight persistent gaps in digital literacy, governance, and resource allocation, comprehensive empirical research demonstrating the causal link between these constraints and the failure of global practices is less abundant. Similarly, the claim that "Current frameworks are insufficient for decentralized finance (DeFi) and require adaptation" (5/10) is supported by conceptual arguments about DeFi's unique risks, but perhaps less by widespread empirical evidence of traditional frameworks' outright failure in these nascent sectors (Olutimehin, 2025; Ali et al., 2024; Oyeniyi et al., 2024; Javaheri et al., 2023). This highlights a crucial area for future research, particularly in

accounting and auditing, where empirical investigation into the effectiveness of implementation and contextual adaptation is critically needed.

The critical importance of human factors, including employee training, digital literacy, and a robust organizational culture, is supported by moderate evidence (7/10). Findings consistently demonstrate that social engineering and insider threats remain significant attack vectors, and that adequate training can mitigate these risks (Asif, 2022; Katuri, 2025; Saeed et al., 2023; Obiki-Osafiele et al., 2024; Hussain et al., 2023; Ali et al., 2024; Oluokun et al., 2024; Oyeniyi et al., 2024; Dawodu et al., 2023; Kafi & Akter, 2023; Oladele et al., 2023; Javaheri et al., 2023; Lois et al., 2020; Wang et al., 2024; Slapničar et al., 2020; Ezinwa et al., 2024). However, measuring the direct impact of these interventions on overall audit resilience across diverse organizations presents methodological challenges, resulting in slightly lower evidence strength compared to purely technical controls.

Table 3: Key claims and support evidence identified in these papers

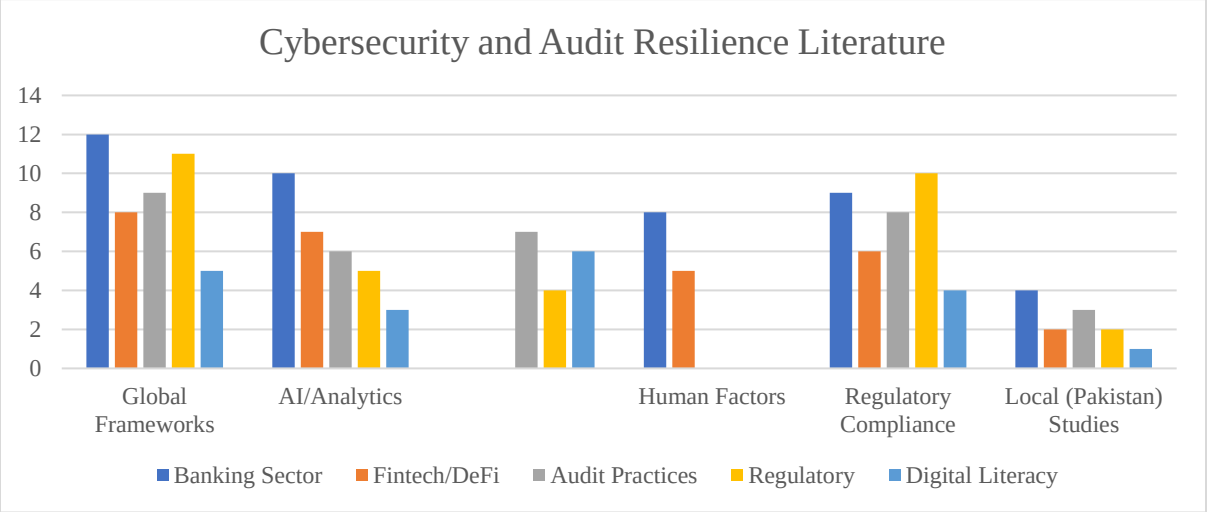
Claim	Evidence Strength	Reasoning	Papers
Compliance with cybersecurity frameworks reduces cyberattack likelihood and enhances audit resilience	Evidence strength: Strong (9/10)	Supported by empirical and sectoral studies across multiple regions and regulatory contexts	(Olutimehin, 2025; Reddem, 2024; Grigoryan & Mirzoyan, 2023; Yedluri, 2025; Hussain et al., 2023; Kolo et al., 2025; Oluoha et al., 2024; Oyeniyi et al., 2024; Dawodu et al., 2023; Kafi & Akter, 2023; Oladele et al., 2023; Ali et al., 2025; Javaheri et al., 2023; Saeed et al., 2023; Slapničar et al., 2020; Ezinwa et al., 2024)
AI-driven threat detection and analytics significantly improve real-time monitoring and incident response	Evidence strength: Strong (8/10)	Multiple studies show improved detection rates and reduced response times in financial institutions	(Adejumo & Ogburie, 2025; Adejumo & Ogburie, 2025; Mukala, 2025; Yedluri, 2025; Obiki-Osafiele et al., 2024; Hussain et al., 2023; Ali et al., 2024; Oluokun et al., 2024; Oyeniyi et al., 2024; Dawodu et al., 2023; Kafi & Akter, 2023; Adewumi et al., 2024; Jony et al., 2024; Oladele et al., 2023; Owolabi et al., 2024; Patricia et al., 2024; Javaheri et al., 2023; Kokogho et al., 2025; Odeyemi et al., 2024; Thapaliya, 2024)
Human factors (training, digital literacy) are critical to effective cybersecurity and audit resilience	Evidence strength: Moderate (7/10)	Consistent findings on the impact of social engineering and insider threats; training mitigates risk	(Katuri, 2025; Saeed et al., 2023; Obiki-Osafiele et al., 2024; Hussain et al., 2023; Ali et al., 2024; Oluokun et al., 2024; Oyeniyi et al., 2024; Dawodu et al., 2023; Kafi & Akter, 2023; Oladele et al., 2023; Javaheri et al., 2023; Saeed et al., 2023; Lois et al., 2020; Wang et al., 2024; Slapničar et al., 2020; Ezinwa et al., 2024)
Regulatory compliance and audit accountability are improving but face challenges in emerging markets	Evidence strength: Moderate (6/10)	Evidence of partial implementation and regulatory gaps, especially in Pakistan	(Saeed et al., 2023; Obiki-Osafiele et al., 2024; Hussain et al., 2023; Ali et al., 2024; Oluokun et al., 2024; Oyeniyi et al., 2024; Dawodu et al., 2023; Kafi & Akter, 2023; Oladele et al., 2023; Javaheri et al., 2023; Wang et al., 2024)
Current frameworks are insufficient for decentralized	Evidence strength:	DeFi faces unique risks (smart contract	(Olutimehin, 2025; Ali et al., 2024; Oyeniyi et al., 2024; Javaheri et al., 2023)

finance (DeFi) and require adaptation	Moderate (5/10)	exploits, oracle manipulation) not addressed by traditional models	
Seamless implementation of global best practices in developing countries is limited by local constraints	Evidence strength: Weak (3/10)	Local studies highlight persistent gaps in digital literacy, governance, and resource allocation	(Saeed et al., 2023; Obiki-Osafiele et al., 2024; Hussain et al., 2023; Ali et al., 2024; Oluokun et al., 2024; Oyeniyi et al., 2024; Dawodu et al., 2023; Kafi & Akter, 2023; Oladele et al., 2023; Javaheri et al., 2023; Wang et al., 2024)

Research Gaps

Despite a wealth of global research, significant gaps remain in empirical studies on the implementation and effectiveness of cyber-audit resilience frameworks within the Pakistani context. As illustrated in the Research Gaps Matrix (Figure 2), there is a notable disparity in research coverage. The heatmap clearly indicates that while foundational concepts have received considerable attention, localized empirical research on digital literacy, governance, and the adaptation of global AI/analytics solutions to resource-constrained environments shows significant deficiencies.

Figure 2: Bar graph illustrating the distribution of research coverage by topic and study attribute, highlighting identified gaps in local (Pakistani) studies



Open Research Questions

Addressing these gaps necessitates a focused agenda for future investigation. The following open research questions, also summarized in Figure 2, provide clear directions for advancing understanding and practice, with a particular emphasis on the Pakistani context and generalizable insights for similar emerging markets:

Table 4: Open research questions for advancing cyber-audit resilience in digital finance, with a focus on the Pakistani context

Question	Why
How effective are SBP and SECP cybersecurity guidelines in improving audit resilience in Pakistani digital finance?	Empirical evaluation is needed to assess real-world impact and identify barriers to effective implementation.
What are the most significant digital literacy and governance gaps affecting cyber-audit resilience in Pakistani fintech and banking?	Understanding these gaps will inform targeted interventions and capacity-building efforts for local stakeholders.
How can global best practices in AI-driven audit resilience be adapted to resource-constrained, emerging market contexts?	Adaptation is crucial for ensuring that advanced solutions are feasible and effective in local environments.

In summary, while global advances in cybersecurity and audit resilience offer a strong foundation, localized research and adaptive frameworks are essential for safeguarding digital finance in Pakistan and similar emerging markets.

Conclusion

Cybersecurity is central to audit resilience in digital finance, underpinning trust, stability, and operational continuity in an era of rapid digital transformation. While global frameworks and AI-driven solutions offer robust defenses, their effectiveness depends on consistent regulatory enforcement, human factors, and judicious local adaptation, especially in emerging markets like Pakistan, where systemic vulnerabilities persist. A collaborative, adaptive, and context-sensitive approach, integrating global best practices with local strategies, is thus essential for building truly resilient digital financial ecosystems.

References

- Adejumo, A., & Ogburie, C. (2025a). Strengthening finance with cybersecurity: Ensuring safer digital transactions. *World Journal of Advanced Research and Reviews*, *25*(3), 1527–1541. https://doi.org/10.30574/wjarr.2025.25.3.0908
- Adejumo, A., & Ogburie, C. (2025b). The role of cybersecurity in safeguarding finance in a digital era. *World Journal of Advanced Research and Reviews*, *25*(3), 1542-1556. https://doi.org/10.30574/wjarr.2025.25.3.0909
- Adewumi, A., Ewim, S., Sam-Bulya, N., & Ajani, O. (2024). Leveraging business analytics to build cyber resilience in fintech: Integrating AI and governance, risk and compliance (GRC) models. *International Journal of Multidisciplinary Research Updates*, *8*(2), 23–32. https://doi.org/10.53430/ijmru.2024.8.2.0050
- Ali, A., Shah, M., Foster, M., & Alraja, M. (2025). Cybercrime resilience in the era of advanced technologies: Evidence from the financial sector of a developing country. *Computers*, *14*(2), 38. https://doi.org/10.3390/computers14020038
- Ali, G., Mijwil, M., Buruga, B., & Abotaleb, M. (2024). A comprehensive review on cybersecurity issues and their mitigation measures in FinTech. *Iraqi Journal For Computer Science and Mathematics*, *5*(3), 45-91. https://doi.org/10.52866/ijcsm.2024.05.03.004
- Ali, S., Razzaque, A., Yousaf, M., & Shan, R. (2025). An automated compliance framework for critical infrastructure security through artificial intelligence. *IEEE Access*, *13*, 4436–4459. https://doi.org/10.1109/ACCESS.2024.3524496
- Asif, M. (2022). Integration of Information Technology in Financial Services and its Adoption by the Financial Sector in Pakistan. *Inverge Journal of Social Sciences*, *1*(2), 23–35. https://doi.org/10.63544/ijss.v1i2.31

- Cheng, S., Li, J., Luo, L., & Zhu, Y. (2024). Cybersecurity governance and digital finance: Evidence from sovereign states. *Finance Research Letters,* Article 105533, 17 pages. https://doi.org/10.1016/j.frl.2024.105533
- Cohn, A., Helleputte, C., Cicco, D., Hirsbrunner, S., Russotto, J., Šemeta, A., Tsakanakis, S., & Weinstein, J. (2020). *Cybersecurity resilience: The EU cryptic way of promoting a digital single market for finance*. European Capital Markets Institute.
- Dawodu, S., Abrahams, T., Ewuga, S., Kaggwa, S., Uwaoma, P., & Hassan, A. (2023). Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security. *World Journal of Advanced Research and Reviews, 20*(3), 1743–1756. https://doi.org/10.30574/wjarr.2023.20.3.2691
- Ezinwa, E., Okoye, C., Nwankwo, E., Mhlongo, N., Odeyemi, O., & Ugochukwu, C. (2024). Securing financial data storage: A review of cybersecurity challenges and solutions. *International Journal of Science and Research Archive, 11*(1), 1968–1983. https://doi.org/10.30574/ijsra.2024.11.1.0267
- Grigoryan, L., & Mirzoyan, L. (2023). Cybersecurity risks and its regulations: The philosophy of cybersecurity audit. *WISDOM, 25*(1), 67–77. https://doi.org/10.24234/wisdom.v25i1.970
- Hussain, N., Babalola, F., Kokogho, E., & Odio, P. (2023). A cybersecurity framework for FinTech platforms: Tackling data breaches and building resilient systems for customer trust. *International Journal of Social Science Exceptional Research, 2*(1), 116–128. https://doi.org/10.54660/ijsser.2023.2.1.116-128
- Jabeen, M., Jabeen, B., Ali, K., & Kausar, S. (2025). Unlocking the impact of digital finance on the digital landscape of businesses in Pakistan. *Journal of Social & Organizational Matters, 4*(1), 370–390. https://doi.org/10.56976/jsom.v4i1.191
- Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2023). Cybersecurity threats in FinTech: A systematic review. *Expert Systems with Applications, 233*, Article 122697. https://doi.org/10.1016/j.eswa.2023.122697
- Jony, M., Arafat, M., Islam, R., Rafi, S., Jalil, M., & Hossen, F. (2024). AI-powered cybersecurity in financial institutions: Enhancing resilience against emerging digital threats. *Advanced International Journal of Multidisciplinary Research, 2*(6), 1-18. https://doi.org/10.62127/aijmr.2024.v02i06.1113
- Kafi, M., & Akter, N. (2023). Securing financial information in the digital realm: Case studies in cybersecurity for accounting data protection. *American Journal of Trade and Policy, 10*(1), 15-26. https://doi.org/10.18034/ajtp.v10i1.659
- Katuri, S. (2025). Cybersecurity threats in digital banking: A comprehensive analysis. *International Journal on Science and Technology, 16*(1), 1-16. https://doi.org/10.71097/ijsat.v16.i1.2655
- Kokogho, E., Okon, R., Omowole, B., Ewim, C., & Onwuzulike, O. (2025). Enhancing cybersecurity risk management in fintech through advanced analytics and machine learning. *International Journal of Frontiers in Science and Technology Research, 8*(1), 1-23. https://doi.org/10.53294/ijfstr.2025.8.1.0023
- Kolo, F., Joseph, S., Ogunmolu, A., Ejiofor, V., & Oyekunle, S. (2025). Mitigating cybersecurity risks in financial institutions through strategic third-party risk governance frameworks. *Journal of Engineering Research and Reports, 27*(5), 173-193. https://doi.org/10.9734/jerr/2025/v27i51501
- Lois, P., Drogalas, G., Karagiorgos, A., & Tsikalakis, K. (2020). Internal audits in the digital era: Opportunities, risks, and challenges. *Euromed Journal of Business, 15*(2), 205–217. https://doi.org/10.1108/EMJB-07-2019-0097
- Mukala, S. (2025). Cybersecurity in financial services: A technical deep dive into protection, compliance, and threat mitigation. *World Journal of Advanced Research and Reviews, 26*(1). https://doi.org/10.30574/wjarr.2025.26.1.1129
- Nadeem, M., Hashmi, S., & Khan, M. (2023). Exploring the interplay of cybersecurity and cybercrime in Pakistan's digital landscape. *Contemporary Issues in Social Sciences and Management Practices, 2*(4), 207-222. https://doi.org/10.61503/cissmp.v2i4.94
- Obiki-Osafiele, A., Agu, E., & Chiekezie, N. (2024). Protecting digital assets in Fintech: Essential cybersecurity measures and best practices. *Computer Science & IT Research Journal, 5*(8), 1884–1896. https://doi.org/10.51594/csitrj.v5i8.1449
- Odeyemi, O., Okoye, C., Ofodile, O., Adeoye, O., Addy, W., & Ajayi-Nifise, A. (2024). Integrating AI with blockchain for enhanced financial services security. *Finance & Accounting Research Journal, 6*(3), 271-287. https://doi.org/10.51594/farj.v6i3.855

- Oladele, T., Jooda, T., Aghaunor, C., Kassie, J., & Oyirinnaya, P. (2023). Strengthening cyber resilience in financial institutions: A strategic approach to threat mitigation and risk management. *World Journal of Advanced Research and Reviews, 20*(3). https://doi.org/10.30574/wjarr.2023.20.3.2424
- Oluoha, O., Odeshina, A., Reis, O., Okpeke, F., Attipoe, V., & Orieno, O. (2024). A digital resilience model for enhancing operational stability in financial and compliance-driven sectors. *International Journal of Social Science Exceptional Research, 3*(1), 365–386. https://doi.org/10.54660/ijsser.2024.3.1.365-386
- Oluokun, A., Bolatito, A., & Ameyaw, M. (2024). Building cyber resilience in fintech through AI and GRC integration: An exploratory study. *GSC Advanced Research and Reviews, 20*(1), 228-237. https://doi.org/10.30574/gscarr.2024.20.1.0245
- Olutimehin, A. (2025). Assessing the effectiveness of cybersecurity frameworks in mitigating cyberattacks in the banking sector and its applicability to decentralized finance (DeFi). *Asian Journal of Research in Computer Science, 18*(3), 130-151. https://doi.org/10.9734/ajrcos/2025/v18i3583
- Owolabi, I., Mbabie, C., & Obiri, J. (2024). AI-driven cybersecurity in FinTech & cloud: Combating evolving threats with intelligent defense mechanisms. *International Journal of Multidisciplinary Research in Science, Engineering and Technology, 7*, 12. https://doi.org/10.15680/IJMSRET.2024.0712004
- Oyeniyi, L., Ugochukwu, C., & Mhlongo, N. (2024). Developing cybersecurity frameworks for financial institutions: A comprehensive review and best practices. *Computer Science & IT Research Journal, 5*(4), 903-925. https://doi.org/10.51594/csitrj.v5i4.1049
- Patricia, O. O., Adesoga, T., Ojo, A., Olagunju, O., Ajayi, O., & Adebayo, Y. (2024). Cybersecurity strategies in fintech: Safeguarding financial data and assets. *GSC Advanced Research and Reviews, 20*(1), 50-56. https://doi.org/10.30574/gscarr.2024.20.1.0241
- Reddem, P. (2024). Cybersecurity in banking and finance: Navigating the digital threat landscape. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10*(5), 852-861. https://doi.org/10.32628/CSEIT241051073
- Rehman, T. (2021a). Cybersecurity for E-banking and E-commerce in Pakistan. In A. Ismail (Ed.), *Handbook of research on advancing cybersecurity for digital transformation* (pp. 163–184). IGI Global. https://doi.org/10.4018/978-1-7998-6975-7.ch009
- Rehman, T. (2021b). Digital transformation of E-commerce services and cybersecurity for modernizing the banking sector of Pakistan. In A. Ismail (Ed.), *Handbook of research on advancing cybersecurity for digital transformation* (pp. 354–375). IGI Global. https://doi.org/10.4018/978-1-7998-6975-7.ch018
- Saeed, S., Altamimi, S., Alkayyal, N., Alshehri, E., & Alabbad, D. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors, 23*(15), 6666. https://doi.org/10.3390/s23156666
- Saeed, S., Suayyid, S., Al-Ghamdi, M., Al-Muhaisen, H., & Almuhaideb, A. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors, 23*(16), 7273. https://doi.org/10.3390/s23167273
- Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2020, June). Effectiveness of cybersecurity audit [Paper presentation]. 6th Corporate Governance Finance and Accounting Conference, Ljubljana, Slovenia. https://doi.org/10.2139/ssrn.3741877
- Thapaliya, S. (2024). Examining the influence of AI-driven cybersecurity in financial sector management. *The Batuk, 10*(2), 129-144. https://doi.org/10.3126/batuk.v10i2.68147
- Wang, S., Asif, M., Shahzad, M., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & Security, 147*, Article 104051. https://doi.org/10.1016/j.cose.2024.104051
- Yedluri, U. (2025). Enhancing cyber resilience in financial institutions: A data protection framework. *World Journal of Advanced Engineering Technology and Sciences, 15*(1), 486-496. https://doi.org/10.30574/wjaets.2025.15.1.0229