

Business Continuity and Disaster Recovery Preparedness in African Financial Services: Lessons from the COVID-19 Pandemic

SAMUEL FADERO^{1*}, DEMILADE JOODA², SERIF OYINDAMOLA OYESIJ³, STANLEY NWAKAMMA⁴

¹*SanlamAllianz Life Insurance Ltd, Lagos Nigeria*

²*Fasyl Technology Ghana - Accra, Ghana*

³*Independent Researcher, Lagos Nigeria*

⁴*Independent Researcher, USA*

**Corresponding Author: Samuel Fadero*

Abstract- This review examines the preparedness of African financial institutions for business continuity and disaster recovery, with particular attention to the operational lessons exposed by the COVID-19 pandemic. It evaluates how banks, insurers, fintech firms, microfinance institutions, and payment providers responded to systemic disruption and how governance, technology, infrastructure, workforce capability, and regulatory oversight shaped resilience outcomes. The study adopts a structured narrative review approach, synthesising scholarly literature, regulatory perspectives, and pandemic-era evidence published up to 2020 to assess continuity concepts, risk assessment, business impact analysis, recovery prioritisation, digital service delivery, cybersecurity, third-party dependence, and institutional preparedness. The findings indicate that resilience across African financial services remains uneven, reflecting differences in technological maturity, capital strength, infrastructure reliability, governance quality, and access to digital channels. COVID-19 revealed critical vulnerabilities in branch-dependent operations, remote-working arrangements, customer access, power availability, cyber controls, vendor concentration, and recovery testing, while simultaneously accelerating digital banking, cloud adoption, mobile finance, and distributed operations. The review further establishes that effective preparedness requires the integration of business continuity management, disaster recovery, operational resilience, liquidity capacity, cybersecurity, and inclusive service design rather than fragmented compliance-oriented planning. It concludes that future resilience depends on tested, scenario-based frameworks capable of preserving critical services under prolonged and interconnected disruption. Accordingly, financial institutions and regulators should strengthen board-level oversight, recovery testing, digital and energy redundancy, third-party risk governance, workforce readiness, sector-wide stress testing, and cross-border coordination. Future

research should prioritise comparable African resilience metrics, cyber recovery, artificial intelligence, cloud concentration, climate-related disruption, and inclusive digital continuity to strengthen evidence-based supervisory and institutional resilience decisions continent-wide.

Keywords: business continuity management; disaster recovery; operational resilience; african financial services; COVID-19 pandemic; digital financial infrastructure

I. INTRODUCTION

1.1 Evolution of Business Continuity and Operational Resilience in African Financial Services

Business continuity in African financial services evolved from a narrow concern with data backup and post-incident restoration into a broader discipline concerned with sustaining critical services, managing operational risk and adapting institutions to systemic disruption. Globally, business continuity management (BCM) emerged from disaster recovery and crisis-management traditions, but progressively incorporated governance, risk assessment, business-impact analysis and organisational learning as firms became more dependent on interconnected technologies and external service providers (Herbane, 2010). For African banks, insurers and payment institutions, this evolution occurred within operating environments characterised by infrastructure constraints, expanding regulation and rapid technological change, making continuity increasingly inseparable from operational resilience.

This transformation also altered managerial responsibility, placing continuity within enterprise governance rather than leaving preparedness predominantly to information-technology departments or emergency-response teams across the institution itself.

The global financial crisis strengthened this shift by demonstrating that severe institutional disruption could arise not only from credit and market exposures but also from failures of processes, people, systems and controls. Evidence from South African banking scholarship showed that operational risk materially amplified the effects of the 2007–2008 crisis, reinforcing the need to integrate operational-risk governance with institutional preparedness (de Jongh et al., 2013). Consequently, continuity planning increasingly moved beyond maintaining alternative premises or restoring information technology toward preserving critical business functions under conditions of prolonged uncertainty.

This maturation was accompanied by more systematic integration of business continuity and disaster recovery. Rather than treating recovery as an isolated technical activity, resilience-oriented approaches linked strategic priorities, resource allocation, recovery objectives and operational responses across the disruption lifecycle (Sahebjamnia, Torabi & Mansouri, 2015). In African financial services, such integration became progressively important as digital channels expanded. Nigerian evidence on electronic banking, for example, demonstrates how service delivery increasingly depended on technology-mediated customer interfaces, thereby raising the operational significance of system availability, reliability and service quality (Ayo et al., 2016).

By the late 2010s, operational resilience was becoming a more explicit concern in banking risk management. South African research identified internal and external fraud, systems failures, execution problems and other operational events as material components of bank exposure, underscoring the need for preventive controls alongside recovery capability (Ferreira & Dickason-Koekemoer, 2019). At the organisational level, resilience also came to be understood as a dynamic capability comprising anticipation, coping and adaptation rather than merely

the capacity to return to a pre-crisis state (Duchek, 2020). This conceptual transition is especially pertinent to African financial institutions, whose continuity arrangements must accommodate technological, infrastructural and institutional volatility.

The movement from continuity to resilience also reflected a growing appreciation that effective preparedness depends on how organisations absorb disruption while preserving operational efficiency. Empirical evidence from a sub-Saharan African setting indicates that disruption absorption and recoverability represent distinct but complementary dimensions of operational resilience, each contributing differently under varying disruption intensities (Essuman, Boso & Annan, 2020). In parallel, BCM practice increasingly emphasised structured preparedness, critical-function protection and recovery effectiveness across banking, insurance and service organisations (Sawalha, 2020).

A further development concerned the human and organisational capabilities needed to sustain increasingly distributed operations. Although not specific to financial services, the supplied Nigerian study by Falemi, Akhigbe & Akin-Oluyomi (2020) is relevant only at this bounded level: it highlights capability development, digital collaboration and workforce adaptability across geographically dispersed operations. These ideas illuminate an important pre-pandemic trajectory in African finance, where resilience was progressively becoming a socio-technical capability linking people, processes, technology, governance and recovery arrangements. Thus, immediately before COVID-19, the sector had already moved substantially beyond conventional disaster recovery, although the pandemic would expose uneven maturity and reveal whether these evolving resilience practices could withstand simultaneous, prolonged and system-wide disruption.

1.2 COVID-19 as a Systemic Disruption to Financial-Service Operations

The COVID-19 pandemic transformed financial-service disruption from a largely institution-specific contingency into a simultaneous, economy-wide stress event. Unlike conventional operational incidents, the crisis combined public-health restrictions, abrupt

mobility constraints, deteriorating macroeconomic conditions and extreme uncertainty, thereby affecting both the demand for financial services and the capacity of institutions to deliver them. At the global level, the pandemic generated interconnected risks across banking, insurance, capital markets and payment systems, demonstrating how a health emergency could propagate rapidly through financial institutions and market expectations (Goodell, 2020).

African financial institutions confronted these pressures within heterogeneous technological and infrastructural environments. In Nigeria, containment measures and the contraction of economic activity weakened household and business income, disrupted commercial activity and intensified financial-system pressures, while policy responses sought to preserve liquidity and economic functioning (Ozili, 2020). These conditions complicated credit administration, customer servicing and the management of operational risk because banks simultaneously faced changing transaction patterns, borrower distress and restrictions on conventional face-to-face service delivery.

The pandemic also accelerated a fundamental reconfiguration of customer access. Evidence from Romanian retail banking showed that pandemic-related lifestyle changes positively influenced attitudes toward internet and mobile banking, indicating that digital channels became increasingly central when physical interaction was constrained (Baicu et al., 2020). A comparable African dynamic emerged in Morocco, where movement restrictions and social distancing highlighted the importance of digital transformation in participatory banking and increased interest in remote banking services, while also exposing cybersecurity and regulatory concerns associated with digital delivery (Amrani & Najab, 2020).

Operational disruption was therefore inseparable from broader financial instability. Extraordinary volatility across global financial markets revealed elevated systemic risk and rapid cross-country transmission of pandemic-related uncertainty, adding balance-sheet and investment pressures to the practical difficulties of maintaining day-to-day financial services (Zhang, Hu & Ji, 2020). For African institutions, this combination was particularly consequential: continuity plans

designed around localized technology failures, unavailable premises or short-duration emergencies were confronted by prolonged disruption affecting employees, customers, counterparties and critical service networks simultaneously. Branch access, cash handling, customer verification, credit processes, call-centre capacity and technology support consequently became interdependent continuity concerns. COVID-19 thus functioned as a systemic operational stress test, exposing the extent to which financial-service continuity depended on resilient digital infrastructure, adaptable work arrangements, responsive governance and the capacity to maintain trusted customer access under conditions of severe and persistent uncertainty. It also revealed that operational resilience had become inseparable from strategic financial stability.

1.3 Aim, Scope, and Review Approach

This review aims to critically examine the evolution, preparedness, and effectiveness of business continuity and disaster recovery practices within African financial services, with particular emphasis on the operational lessons revealed by the COVID-19 pandemic. It seeks to determine how financial institutions responded to prolonged disruption, maintained essential services, adapted governance and workforce arrangements, and strengthened technological resilience under conditions of systemic uncertainty.

The scope encompasses banks, insurance companies, fintech firms, microfinance institutions, payment service providers, and other regulated financial intermediaries operating across diverse African markets. Attention is given to business continuity management, disaster recovery planning, operational resilience, digital infrastructure, cybersecurity, remote operations, third-party dependencies, regulatory oversight, and institutional preparedness. The review also considers differences in technological maturity, infrastructure reliability, organisational capability, and regulatory environments that shape resilience outcomes across the continent.

Methodologically, the study adopts a structured narrative review approach, synthesising relevant scholarly literature, regulatory perspectives, industry evidence, and pandemic-era observations. The analysis is organised thematically to identify recurring

vulnerabilities, effective response mechanisms, and transferable lessons. Particular attention is devoted to the relationship between pre-pandemic preparedness and crisis performance, enabling the review to assess how COVID-19 exposed structural weaknesses while accelerating digital transformation and resilience-oriented reforms within African financial services. This framing supports balanced assessment across institutional and national contexts.

II. FOUNDATIONS OF BUSINESS CONTINUITY AND DISASTER RECOVERY IN FINANCIAL SERVICES

2.1 Business Continuity Management, Disaster Recovery, and Operational Resilience Concepts
Business continuity management (BCM), disaster recovery (DR), and operational resilience are closely related but conceptually distinct disciplines. BCM provides the overarching managerial architecture through which an institution identifies disruptive threats, determines critical activities, establishes response priorities, and maintains an acceptable level of service during interruption. In this sense, continuity is not merely an emergency plan but a cyclical governance process requiring preparation, implementation, testing, review, and improvement (Botha & von Solms, 2004). For African financial institutions, this distinction is important because service continuity depends simultaneously on technology, personnel, physical facilities, telecommunications, third parties, and confidence in transaction integrity.

DR constitutes a more technically concentrated component of this architecture. It concerns the restoration of information systems, data, infrastructure, applications, and supporting technology following disruptive events. ICT-intensive organisations therefore require recovery procedures that connect technical restoration with broader business priorities rather than treating system recovery as an isolated information-technology responsibility (Sambo & Bankole, 2016). Within Nigerian banking, the relationship is particularly evident because disaster recovery arrangements underpin the preservation of essential banking functions when operational interruptions threaten service delivery and institutional performance (Chukwuani, 2019).

BCM extends beyond recovery by determining what must be protected and in what order. Effective programmes identify critical functions, dependencies, minimum resource requirements, responsible personnel, and tolerable disruption thresholds, thereby translating organisational priorities into actionable continuity arrangements (Păunescu&Argatu, 2020). This approach is especially pertinent to financial services, where payments, liquidity management, customer authentication, settlement processes, digital channels, and regulatory reporting may have markedly different tolerances for downtime.

Operational resilience develops this logic further. Rather than concentrating solely on preventing disruption or restoring predetermined operating conditions, resilience concerns an organisation's capacity to detect threats, absorb shocks, adapt its response, and sustain essential functionality under changing circumstances. Organisational responses therefore depend on adaptive capacity and the ability to reconfigure resources as disruption unfolds (Burnard & Bhamra, 2011). This adaptive orientation broadens continuity planning from asset preservation toward maintaining viable service and value-delivery configurations when established processes become unavailable. Strategic BCM accordingly requires organisations to examine not only whether resources and processes can be recovered, but whether the underlying business model remains viable under adverse contingencies (Niemimaa et al., 2019).

The distinction between recovery and resilience is also temporal. Recovery seeks to restore operations after disruption, whereas resilience incorporates anticipatory preparedness, absorption, adaptation, and subsequent renewal. Evidence from disaster-affected enterprises demonstrates that reopening alone does not necessarily signify full recovery, since organisations may resume activity while remaining financially and operationally impaired (Asgary, Anjum & Azimi, 2012). Applied to African financial services, these concepts form a layered preparedness framework: BCM governs continuity requirements, DR restores enabling systems, and operational resilience strengthens the institution's capacity to continue delivering critical financial services despite severe, evolving, and interconnected disruptions. This layered

relationship is central to credible preparedness across increasingly digital institutions.

2.2 Risk Assessment, Business Impact Analysis, and Recovery Prioritisation

Risk assessment and business impact analysis (BIA) provide the analytical foundation for determining which financial services must be protected, how rapidly they should be restored, and what resources should receive precedence during disruption. Risk assessment identifies threats, vulnerabilities, likelihoods and potential consequences, while BIA examines the operational and financial effects arising when critical processes, technologies, facilities or external dependencies become unavailable. An effective BIA therefore converts broad risk information into service-criticality judgments, enabling institutions to distinguish between tolerable inconvenience and disruption capable of threatening regulatory obligations, liquidity, customer access or market confidence (Torabi, Rezaei Soufi & Sahebjamnia, 2014).

Within financial services, risk assessment must be sufficiently dynamic to capture interdependencies among digital platforms, payment networks, telecommunications, data centres, personnel and third-party providers. Enhanced continuity-oriented risk frameworks emphasise identifying disruptive scenarios, analysing their consequences, evaluating organisational exposure and selecting treatments consistent with continuity objectives rather than relying solely on conventional probability-impact matrices (Torabi, Giahi & Sahebjamnia, 2016). This is particularly significant for African institutions operating amid uneven infrastructure reliability and rapidly expanding digital financial ecosystems.

BIA translates these exposures into measurable recovery requirements. Critical processes are assessed according to the consequences of downtime and the rate at which those consequences escalate. Alternative BIA approaches demonstrate that prioritisation should incorporate both quantitative losses and qualitative effects, including reputational damage, legal exposure, customer harm and disruption to dependent activities (Sikdar, 2011). For banks, this means that core payments, settlement, customer authentication, treasury operations and transaction processing may

require substantially shorter recovery windows than administrative functions.

Recovery prioritisation must nevertheless reflect economic feasibility. Continuity strategies carry different implementation costs and recovery capabilities; consequently, decision makers must balance the desired continuity level against the cost of achieving specified recovery objectives (Rabbani et al., 2016). At the technology layer, recovery choices should similarly be matched to system criticality, data-loss tolerance and restoration requirements, as disaster-recovery research demonstrates substantial variation in solutions, architectures and evaluation approaches (Mendonça et al., 2019).

The African banking context further underscores the need to connect continuity assessment with enterprise risk governance. Nigerian evidence demonstrates that bank performance is sensitive to multiple risk categories, including liquidity, credit, leverage and capital-adequacy exposures, reinforcing the importance of systematic risk identification and prioritised controls when preserving institutional viability (Inegbedion, Vincent & Obadiaru, 2020). Evidence from Ghana likewise shows that operational risk has material implications for universal-bank performance, illustrating why operational exposures cannot be treated as secondary to traditional financial risks (Gadzo, Kportorgbi & Gatsi, 2019).

For African financial institutions, recovery prioritisation should therefore follow a defensible chain from threat identification to BIA, critical-service ranking and recovery-resource allocation. Such discipline enables scarce backup capacity, specialist personnel, alternative sites and technology resources to be directed first toward services whose interruption would produce the greatest systemic, financial, regulatory and customer consequences.

It also supports more credible escalation decisions by clarifying acceptable downtime, minimum operating capacity, dependency sequencing and the consequences of delayed restoration across interconnected customer-facing and back-office functions and dependencies.

2.3 Governance, Regulatory Oversight, and Institutional Preparedness

Governance, regulatory oversight, and institutional preparedness constitute the control architecture through which financial institutions convert continuity policies into credible operational capability. In African financial services, this architecture is especially important because disruptions may arise simultaneously from technological dependence, infrastructure constraints, market volatility, cyber risk, third-party failure, and public emergencies. Effective governance therefore requires boards and senior management to define risk appetite, assign continuity responsibilities, scrutinise preparedness, and ensure that recovery arrangements are embedded within enterprise-wide decision-making rather than delegated solely to technical functions. Evidence from Nigerian commercial banks indicates that governance characteristics materially influence institutional performance, reinforcing the importance of board structure, ownership incentives, and accountable oversight in confidence-sensitive banking environments (Okoye et al., 2020).

Regulatory oversight complements internal governance by setting minimum prudential expectations and creating incentives for institutions to maintain sound controls. Cross-country African evidence demonstrates that central-bank supervisory guidance on corporate governance is associated with stronger internal governance and greater bank stability, particularly where institutional conditions support enforcement and compliance (Mutarindwa, Schäfer & Stephan, 2020). Such oversight is relevant to business continuity because preparedness depends on more than documented plans: regulators must evaluate whether institutions possess credible escalation structures, tested recovery arrangements, adequate resources, and management accountability for critical services.

The effectiveness of regulatory requirements nevertheless depends on their institutional fit. Sub-Saharan African governance systems frequently operate within heterogeneous legal, cultural, and enforcement environments, making a rigid distinction between rules-based and principles-based regulation potentially inadequate. An integrated, co-regulatory approach involving government, corporations, and relevant stakeholders may therefore strengthen practical governance outcomes where formal

institutions alone are insufficient (Nakpodia et al., 2018). For financial institutions, this implies that preparedness standards should combine enforceable requirements with supervisory judgement proportionate to institutional complexity and systemic importance.

Internal risk governance is equally decisive. During the global financial crisis, banks whose chief risk officers had stronger organisational status and more direct access to boards performed comparatively better, suggesting that independence and authority within risk-management structures affect crisis responsiveness (Aebi, Sabato & Schmid, 2012). Similarly, stronger and more independent risk controls in U.S. bank holding companies were associated with lower tail risk and improved performance during stressful conditions (Ellul & Yerramilli, 2013). These findings are transferable to continuity preparedness because risk functions require sufficient authority to challenge business decisions, escalate vulnerabilities, and ensure that unresolved operational weaknesses receive executive attention.

Regulation must also recognise that governance structures shape how banks respond to prudential constraints. International evidence indicates that the effect of banking regulation on risk-taking varies with ownership structure and the relative power of shareholders, meaning that uniform regulatory requirements can produce different behavioural outcomes across institutions (Laeven & Levine, 2009). Preparedness should therefore be assessed through both formal compliance and observable organisational capability.

This distinction becomes critical when institutional weaknesses threaten survival. Evidence from U.S. bank failures shows that ownership and management structures can materially influence default risk, demonstrating that governance deficiencies may amplify vulnerability during severe stress (Berger, Imbierowicz & Rauch, 2016). In African financial services, credible preparedness consequently requires active board oversight, independent risk functions, enforceable supervisory standards, periodic testing, transparent reporting, and clear accountability for remediation. These elements provide the institutional discipline needed to transform business continuity and

disaster recovery from compliance exercises into operationally credible safeguards across diverse and increasingly interconnected financial ecosystems.

III. COVID-19 AND OPERATIONAL DISRUPTION IN AFRICAN FINANCIAL SERVICES

The COVID-19 pandemic exposed service continuity in financial institutions as a socio-technical challenge rather than a purely technological one. Restrictions on mobility, health risks and sudden workplace closures disrupted branch staffing, customer-facing activities and back-office coordination, while employees simultaneously confronted anxiety, altered job demands and unfamiliar work settings. Human-resource scholarship shows that crisis conditions required organisations to rethink employee support, adjustment and workforce management as work arrangements changed abruptly (Carnevale & Hatak, 2020). For financial institutions, the resulting challenge was to preserve critical functions without compromising staff safety, control discipline or service quality.

Remote working offered an important continuity mechanism, but its feasibility was uneven across occupations and national settings. Cross-country evidence indicates that the proportion of work capable of being performed from home is substantially lower in poorer economies, reflecting differences in occupational structures and enabling infrastructure (Dingel & Neiman, 2020). African banks therefore faced a practical division between functions that could migrate to virtual environments and branch-dependent activities requiring physical presence, including cash handling, document processing and certain customer-

verification procedures. This distinction made workforce segmentation, secure connectivity and rotation of essential personnel central to continuity planning.

At the same time, lockdowns accelerated dependence on digital channels. The pandemic-induced surge in digital technologies reshaped how organisations worked, communicated and delivered services, but also intensified dependence on reliable connectivity, digital literacy and secure information systems (De', Pandey & Pal, 2020). In Nigeria, these pressures interacted with pre-existing supply-side limitations in digital financial services. Evidence on Nigerian providers identifies technology, people and physical locations as important capabilities, while higher-order human and strategic capabilities were comparatively less developed (David-West, Iheanachor & Kelikume, 2018). Such structural constraints could weaken the capacity to scale remote and digital service delivery rapidly during systemic disruption.

Customer access posed a parallel challenge. The geographical concentration of financial institutions can shape the depth and distribution of financial inclusion, meaning that reduced physical accessibility can affect communities unevenly where viable alternatives are limited (Babajide et al., 2020). Digital substitution was therefore not automatically equivalent to inclusive continuity. Ghanaian evidence on mobile financial inclusion identifies network failures and service charges as significant user challenges, illustrating how customers may remain vulnerable even where mobile channels are technically available (Kodom et al., 2020).

Table 1. Illustrative Mapping of COVID-19 Service-Continuity Challenges in African Financial Services

Operational dimension	Pandemic-related challenge	Immediate service effect	Continuity requirement
Workforce	Illness, mobility restrictions and staff absence	Reduced operational capacity	Staff rotation, cross-training and remote access
Branch operations	Restricted physical access and distancing requirements	Lower branch throughput	Alternative service points and controlled branch access
Customer access	Limited mobility and digital exclusion	Difficulty obtaining routine financial services	Multichannel and low-bandwidth service options

Digital channels	Sharp increase in remote transactions	Capacity and reliability pressures	Scalable platforms and network redundancy
Customer support	Higher enquiries and changing procedures	Call-centre congestion and delayed resolution	Remote support and escalation protocols
Cash-dependent services	Continued need for physical transactions	Exposure to branch and ATM disruption	Cash-distribution and alternative-access planning

Source: Author's illustrative synthesis based on the reviewed literature.

Service continuity also depended on maintaining clear communication between headquarters, branches, call centres and customers. Where operating hours, access procedures or available channels changed rapidly, inconsistent information could magnify customer frustration and operational congestion. Institutions therefore needed coordinated communication protocols capable of directing customers toward functioning channels while preserving escalation pathways for complex or vulnerable cases.

More broadly, COVID-19 compelled organisations to reconsider operating models around digital interaction, reduced physical contact and changing customer behaviour. Business-model research during the pandemic indicates that firms had to reassess how value could be created and delivered under altered technological and market conditions (Seetharaman, 2020). For African financial institutions, service continuity therefore depended on coordinating branch rationalisation, workforce redeployment, digital-channel capacity and customer-support mechanisms rather than treating each problem independently. The operational challenge was especially acute for customers requiring cash, face-to-face assistance or low-bandwidth channels, and for institutions whose remote-working infrastructure had not been tested at scale. Effective continuity consequently required hybrid service arrangements capable of preserving access while protecting employees and sustaining critical transaction, lending, payment and customer-service functions throughout prolonged disruption.

3.2 Technology Dependence, Cybersecurity Exposure, and Third-Party Vulnerabilities

The COVID-19 pandemic intensified the technological dependence of financial services by moving employees, customers and transaction flows rapidly toward remote and digital channels. For African banks, this dependence created a dual

continuity problem: technology became the principal mechanism for sustaining service delivery while simultaneously expanding the attack surface. Research on Nigerian internet banking had already identified viruses, spam, hacking and deficiencies in advanced defensive technologies and legislative compliance as significant weaknesses, indicating that accelerated digital dependence entered the pandemic on an uneven security foundation (Wang, Nnaji & Jung, 2020).

The emergency shift to home working further altered institutional security boundaries. Employees increasingly accessed organisational systems through domestic networks, personal devices and rapidly deployed remote-access arrangements, while normal workplace controls became harder to enforce. The resulting environment heightened exposure to phishing, credential compromise and insecure configurations, demonstrating that continuity measures could generate new vulnerabilities when remote-working security was insufficiently prepared (Furnell & Shah, 2020). In financial institutions, these risks were amplified by the sensitivity of customer information, payment credentials and privileged access to transaction systems.

Technology dependence also extended beyond banks' organisational boundaries. Cloud computing offers scalability, flexibility and rapid access to computing resources, but banking adoption is strongly conditioned by trust, security and privacy concerns, making technological resilience dependent on how effectively externally hosted environments are governed (Asadi et al., 2017). This issue became especially salient during prolonged disruption because institutions needed infrastructure capable of supporting surges in online transactions and distributed work without weakening confidentiality, integrity or availability.

Third-party dependence introduces an additional layer of concentration and control risk. Information-technology outsourcing changes the client organisation's cyber-risk profile because part of the institution's exposure becomes linked to vulnerabilities and security practices within the service provider, challenging assumptions that responsibility can simply be transferred contractually (Benaroch, 2020). For e-banking specifically, outsourcing decisions involve interacting technological, organisational and environmental considerations, requiring banks to assess which channels and capabilities should remain internal and which may be entrusted to external providers (Hanafizadeh & Zare Ravasan, 2018).

The African digital-finance ecosystem also illustrates how cybersecurity exposure can propagate through interconnected providers, agents and customers. Ghanaian evidence on mobile-money services associates fraud vulnerability with weak internal controls, inadequate technological detection capability, insufficient training and stakeholder weaknesses, demonstrating that service resilience depends on controls extending across the wider delivery ecosystem rather than the regulated institution alone (Akomea-Frimpong et al., 2019).

Accordingly, pandemic-era continuity exposed a structural trade-off within African financial services: greater digital connectivity increased operational reach and substitutability for physical channels, yet also deepened reliance on networks, cloud environments, outsourced technology and ecosystem partners. Preparedness therefore required cybersecurity, third-party assurance, access control, incident response, vendor monitoring and recovery arrangements to be integrated into business continuity architecture rather than managed as separate technical disciplines. This integration became central to credible pandemic-era operational resilience.

IV. DIGITAL TRANSFORMATION AND DISASTER RECOVERY CAPABILITIES DURING THE PANDEMIC

4.1 Digital Banking, Cloud Infrastructure, Remote Operations, and Service Resilience

Digital banking became a central mechanism of service continuity as financial institutions progressively shifted transactions, customer interaction and back-office processes from branch-centred models towards networked platforms. Before COVID-19, this transformation was already reshaping banking through expanded connectivity, faster information processing and technology-enabled financial products, creating the foundations for institutions to serve customers without continuous physical contact (Gomber, Koch & Siering, 2017). During systemic disruption, these capabilities acquire a continuity function: mobile applications, internet banking, electronic payments and digital onboarding can substitute for inaccessible branches, reduce dependence on face-to-face interaction and preserve transaction flows when mobility is constrained.

The Nigerian context demonstrates why adoption quality matters as much as platform availability. Research on prospective online banking services in Nigeria found that customers differentiate among service attributes and that preferences influence willingness to adopt emerging banking technologies (Dauda & Lee, 2015). Service resilience therefore depends not simply on digitising existing processes but on ensuring that digital channels are usable, trusted and capable of supporting essential customer journeys under stressed conditions. Across Sub-Saharan Africa, digital finance also compensates for deficiencies in physical financial infrastructure; evidence from multiple countries shows that poorer infrastructure can increase reliance on mobile money where conventional financial access is limited (Mothobi & Grzybowski, 2017). This makes mobile connectivity itself part of the continuity architecture.

Cloud infrastructure strengthens this architecture by providing scalable computing capacity, resource pooling and flexible deployment, allowing organisations to adjust technological resources more rapidly than under exclusively fixed, on-premises

models (Marston et al., 2011). For financial institutions, such elasticity can support transaction surges, distributed applications, data availability and remote workforce access. Yet resilience requires deliberate architecture: cloud dependence without redundancy, governance and tested recovery arrangements may replace internal capacity constraints with external concentration and connectivity dependencies.

Remote operations formed the organisational counterpart to digital banking. COVID-19

demonstrated that collaboration platforms, shared digital workspaces and communication technologies could substitute for several affordances of co-located work, although enforced working from home also generated coordination and social challenges (Waizenegger et al., 2020). In financial services, secure remote access therefore needed to accommodate treasury, risk, compliance, customer-support and technology teams while preserving segregation of duties, authentication and supervisory visibility.

Table 2. Illustrative Service-Resilience Architecture for Digitally Enabled African Financial Institutions

Digital capability	Continuity contribution	Principal vulnerability	Resilience requirement
Mobile and internet banking	Maintains customer transactions during branch disruption	Network outages and platform overload	Scalable capacity and alternative channels
Cloud infrastructure	Provides flexible computing and distributed availability	Provider or connectivity concentration	Redundancy, portability and tested recovery
Digital payments	Reduces dependence on cash and physical interaction	Payment-network interruption	Multiple payment rails and failover capability
Remote-work platforms	Sustains critical back-office functions	Access-control and coordination weaknesses	Secure authentication and controlled privileges
Digital onboarding	Preserves customer acquisition and account access	Identity-verification failure	Resilient e-KYC and exception procedures
Interbank networks	Maintains institutional connectivity and settlement	Network dependency and cascading disruption	Network monitoring and alternative processing arrangements

Source: Author's illustrative synthesis based on the reviewed literature.

Digitalisation also changes the competitive and operational structure of banking. Technological disruption encourages customer-centric, platform-based models in which incumbents, FinTech firms and technology providers increasingly interact, potentially increasing efficiency while introducing new regulatory and dependency questions (Vives, 2019). The continuity implication is significant: critical services may depend on interconnected application interfaces, payment networks and external digital ecosystems rather than infrastructure controlled entirely by a single institution.

Longer-term evidence confirms that networked financial infrastructure can generate substantial

organisational value. Analysis of SWIFT adoption across thousands of banks found that digital network innovation was associated with performance effects developing over time, illustrating that resilient financial technology is not merely an emergency utility but a strategic institutional capability (Scott, Van Reenen & Zachariadis, 2017). For African financial institutions, pandemic preparedness consequently depends on integrating digital channels, elastic infrastructure, secure remote operations and interoperable payment networks into a coherent service-resilience architecture.

In African markets, these capacities must also accommodate uneven broadband quality, varying

levels of digital literacy and differences in institutional scale. Resilience therefore requires channel diversity, capacity monitoring and fallback arrangements capable of maintaining minimum service levels when a principal digital pathway becomes degraded or unavailable.

4.2 Data Protection, Backup, Redundancy, Failover, and Recovery Testing

Data protection and recoverability are fundamental to disaster preparedness in African financial services because digitally mediated banking depends on continuous access to accurate, confidential and transactionally consistent information. Protection must therefore encompass encryption, authentication, access control, integrity assurance and safeguards against unauthorised disclosure or destruction. Cloud environments intensify these requirements because outsourced storage and processing introduce additional privacy, trust and control challenges that must be addressed throughout the information lifecycle (Sun, 2020).

Within African digital environments, technical controls must also reflect local institutional capacity. Research from Ghana demonstrates that cloud-service security can be strengthened through structured authorisation, policy enforcement and technologies designed to preserve data integrity, illustrating the importance of embedding security controls directly within service architectures rather than treating protection as an external compliance activity (Okoampa-Larbi, Twum & Hayfron-Acquah, 2017).

For financial institutions, equivalent principles apply to customer records, payment information, transaction histories and authentication data replicated across primary and recovery environments.

Backup provides recoverability, whereas redundancy seeks to prevent interruption by maintaining alternative copies, components or sites capable of assuming workload. Multi-site disaster-recovery research demonstrates that geographically distributing redundant data can increase fault tolerance while requiring careful optimisation of storage capacity, recovery objectives and distribution costs (Sengupta & Annervaz, 2014). These considerations are particularly relevant to African banks whose critical platforms may encounter telecommunications failures, infrastructure outages or geographically concentrated disruption.

Failover extends redundancy into active service restoration. Disaster-tolerant data-centre architectures can combine active and standby resources across sites so that workloads migrate when infrastructure becomes unavailable, although resilience must be balanced against downtime and infrastructure costs (Nguyen, Kim & Park, 2016). Cloud-based disaster recovery similarly requires evaluation of availability, throughput and response performance rather than assuming that possession of secondary capacity automatically guarantees effective recovery (Andrade & Nogueira, 2019).

Illustrative Recovery-Resilience Priority Allocation

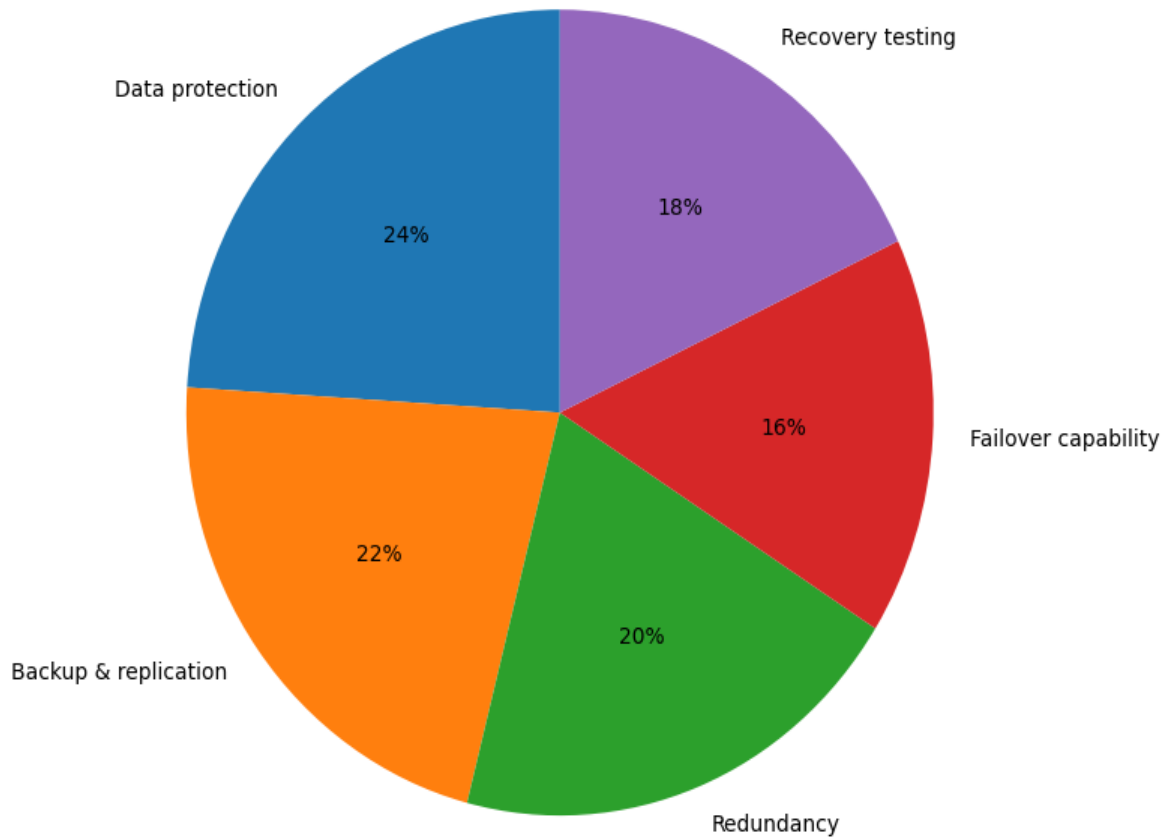


Figure 1. Illustrative Recovery-Resilience Priority Allocation

Note: The percentages are conceptual allocations developed solely to illustrate the relative interdependence of recovery capabilities; they are not empirical measurements.

Physical infrastructure remains integral to these digital arrangements. Optimised electrical-load distribution can strengthen continuity where alternative and hybrid power systems are required to maintain critical equipment during unreliable supply conditions (Sunday & Omoegun, 2019). Likewise, effective grounding contributes to equipment protection and operational reliability within electricity-dependent infrastructure supporting technology environments (Adeniji et al., 2020).

V. BUSINESS CONTINUITY PREPAREDNESS ACROSS AFRICAN FINANCIAL INSTITUTIONS

Business continuity preparedness across African financial institutions is uneven because banks,

insurers, microfinance institutions, fintech firms and payment providers operate with levels of capital strength, technological maturity, reach and regulatory capability. Preparedness therefore extends beyond possession of a formal continuity plan to encompass liquidity buffers, digital-channel capacity, workforce flexibility, alternative processing arrangements and tested recovery procedures. Evidence from African banks shows that compliance with Basel III capital and stable-funding thresholds can strengthen dimensions of bank stability, although effects vary across institutions and regulatory environments (Mutarindwa, Schäfer & Stephan, 2020).

Institutional preparedness is shaped by governance quality and the operating environment. African banking stability depends on interacting bank-level,

structural and institutional factors, including efficiency, asset quality, regulatory quality, government effectiveness and political stability. Continuity readiness therefore cannot be assessed solely through technical disaster-recovery capability; it must also consider whether governance systems can identify vulnerabilities, escalate emerging threats and sustain disciplined decision-making under stress (Ozili, 2018a). During disruption, institutions with weak governance or fragile balance sheets may face compounded operational and financial pressures.

Preparedness is further differentiated by the depth and inclusiveness of national financial systems. Across Africa, gaps in financial development and formal financial inclusion coexist with innovation, particularly mobile banking, which can overcome infrastructural and geographic barriers to service access (Allen et al., 2014). For continuity planning, institutions must preserve conventional banking functions while ensuring that digital alternatives remain accessible to customers distant from branches or dependent on low-cost mobile channels.

Financial robustness provides another layer of preparedness because institutions require sufficient absorptive capacity to continue operating while disruption suppresses revenues, weakens borrowers and increases operational expenditure. International banking evidence demonstrates that stronger capital positions improve the ability of banks, especially smaller institutions, to survive and maintain presence during severe financial stress (Berger & Bouwman, 2013). Although derived from the United States, this finding is conceptually relevant to African institutions because continuity arrangements are difficult to sustain when financial buffers are inadequate.

Physical infrastructure also constrains preparedness in African operating environments. Nigerian evidence on integrating solar power into small-scale industrial operations demonstrates the potential contribution of alternative energy systems where unreliable grid supply threatens operational continuity (Sunday & Omoegun, 2018). For financial institutions, the transferable implication is important: branches, data-processing facilities, ATMs, network equipment and recovery sites require dependable electricity if digital

and physical continuity arrangements are to remain functional during prolonged disruption.

Environmental control within critical facilities constitutes a preparedness concern. Research on energy efficiency and control strategies in air-conditioning systems highlights the importance of reliable thermal management and intelligent control for maintaining efficient operating environments (Sunday et al., 2019). Applied cautiously to financial services, this supports protection of technology rooms, communication equipment and recovery facilities against heat-related degradation. Across African financial institutions, credible preparedness therefore rests on an integrated capability combining financial strength, governance, digital reach, workforce readiness, infrastructure and tested continuity arrangements.

VI. LESSONS FROM THE COVID-19 PANDEMIC FOR STRENGTHENING FINANCIAL-SECTOR RESILIENCE

The COVID-19 pandemic demonstrated that financial-sector resilience depends on the capacity of institutions to absorb simultaneous operational, liquidity, credit and market shocks while continuing to support households and firms. A central lesson is that preparedness must be built before disruption occurs. Evidence from 24 African countries indicates that financial-sector technical efficiency, liquidity and market structure materially condition the capacity of financial systems to support economic activity during severe shocks, revealing uneven readiness across the continent (Winful, Sarpong Jr. & Dondjio, 2020). This implies that resilience strategies should integrate continuity planning with balance-sheet strength, liquidity management and institutional efficiency rather than treating disaster recovery as an isolated technical function.

The pandemic also reaffirmed the stabilising role of banks as providers of emergency liquidity. During the initial COVID-19 shock, firms drew heavily on pre-existing credit lines, requiring banks to accommodate an abrupt increase in corporate liquidity demand (Li, Strahan & Zhang, 2020). For African financial institutions, the lesson is that continuity arrangements must protect treasury operations, credit decision systems, payment infrastructure and liquidity-

monitoring capabilities because operational interruption can directly constrain the sector's capacity to transmit financial support to the wider economy.

Systemic-risk surveillance must likewise become more prominent. International evidence showed that systemic risk in major banking sectors increased sharply during the early phase of COVID-19, illustrating how a non-financial shock can propagate rapidly through interconnected financial institutions and markets (Rizwan, Ahmad & Ashraf, 2020). African regulators and institutions therefore require stress scenarios that combine epidemiological, macroeconomic, cyber, liquidity and operational disturbances rather than modelling disruptions independently.

A further lesson concerns digital resilience and inclusive access. Evidence from Sub-Saharan Africa demonstrates that digital finance can extend financial inclusion by overcoming geographic and conventional service-delivery barriers, although institutional and infrastructural conditions remain important (Achugamonu et al., 2020). Resilience planning should consequently preserve multiple digital channels, strengthen low-bandwidth access, and ensure that emergency migration from branches to electronic services does not deepen exclusion. More broadly, evidence from European banking indicates that broader financial inclusion can coexist with greater bank stability, reinforcing the strategic value of maintaining diversified and accessible customer relationships (Danisman & Tarazi, 2020).

COVID-19 also highlighted the importance of coordinated public-sector intervention. Nigeria's pandemic response showed how emergency fiscal measures, central-bank actions and support programmes were deployed amid constrained fiscal space, demonstrating that crisis management requires close interaction between financial institutions, monetary authorities and government (Ejiogu, Okechukwu & Ejiogu, 2020). The operational implication is that banks must maintain systems capable of rapidly implementing regulatory relief, restructuring credit, distributing intervention funds and adapting reporting requirements.

Taken together, these lessons reposition resilience as an enterprise-wide capability linking governance, liquidity, digital infrastructure, cybersecurity, workforce flexibility, customer accessibility and regulatory coordination. African financial institutions should therefore move from static continuity documentation toward tested, scenario-based resilience frameworks that preserve critical services, enable rapid adaptation and support economic intermediation throughout prolonged systemic disruption with measurable recovery objectives, clear accountability and regular cross-institutional testing exercises routinely.

VII. EMERGING PRIORITIES AND FUTURE RESEARCH DIRECTIONS

The post-pandemic resilience agenda for African financial services should move beyond restoring pre-crisis operating models toward designing institutions capable of anticipating, absorbing and adapting to compound disruptions. The first priority is the development of digitally resilient financial architectures that improve access without creating new sources of fragility. Digital finance can lower transaction costs and extend service availability, yet its benefits depend on infrastructure quality, consumer protection and the management of risks that may threaten financial stability (Ozili, 2018b). Future research should therefore examine how African banks, fintech firms and payment providers can measure the resilience contribution of digital channels under simultaneous cyber, power, telecommunications and liquidity shocks.

Artificial intelligence represents a second major research frontier. AI applications can strengthen risk detection, customer support, fraud monitoring and information processing, while potentially expanding digital financial inclusion (Mhlana, 2020). However, research in African financial services should move beyond adoption studies toward evaluating model robustness during crises, algorithmic bias, explainability, data scarcity and the governance of automated decisions. Comparative evidence is particularly needed on whether AI-enabled early-warning systems improve business-continuity decisions, incident escalation and recovery

prioritisation in institutions with different levels of technological maturity.

Cyber resilience must receive equivalent attention. Africa's expanding digital economy has increased exposure to cybercrime while institutional capabilities, legislation and enforcement remain uneven across jurisdictions (Kshetri, 2019). Future studies should investigate cyber-continuity integration rather than examining information security and disaster recovery separately. This includes ransomware-resistant backup, identity resilience, privileged-access recovery, cross-border incident coordination and sector-wide cyber exercises. Research should also assess whether regulatory fragmentation impedes collective response when disruptions affect payment networks, cloud providers or telecommunications infrastructure shared by multiple institutions.

The growing complexity of FinTech ecosystems creates an additional priority around third-party and concentration risk. Contemporary FinTech systems integrate cloud computing, big data, cybersecurity, service platforms and interconnected technical infrastructures, making resilience dependent on components that may sit outside the direct control of individual financial institutions (Gai, Qiu & Sun, 2018). African research should consequently map critical digital dependencies, identify single points of failure and develop metrics for evaluating cloud concentration, application-programming-interface dependencies and outsourced processing arrangements. Particular attention is required for smaller institutions whose limited bargaining power may constrain redundancy options.

Inclusive resilience should also become a central research concern. Evidence from Kenya demonstrates that mobile money can generate substantial long-term welfare gains and strengthen access to financial resources among previously underserved households (Suri & Jack, 2016). The future challenge is to determine whether digital continuity strategies remain effective during large-scale disruptions for rural populations, informal enterprises, women, low-income users and customers with limited connectivity. Research should evaluate low-bandwidth channels, agent-network resilience, offline transaction

capabilities and the consequences of prolonged telecommunications outages.

Regulatory innovation provides the final major frontier. FinTech growth requires regulatory approaches capable of supporting innovation while protecting stability and consumers, creating a stronger role for RegTech, data-driven supervision and regulatory experimentation (Arner et al., 2017). Future African research should assess interoperable supervisory technologies, cross-border resilience standards, real-time reporting and coordinated testing frameworks. More broadly, longitudinal and multi-country studies are needed to establish comparable resilience indicators, distinguish formal compliance from actual recovery capability, and evaluate how climate events, pandemics, cyber incidents and infrastructure failures interact. Such research would provide a stronger empirical basis for designing adaptive, inclusive and systemically resilient African financial institutions.

Priority should also be given to standardized stress-testing protocols that capture interdependencies between banks, mobile-money operators, utilities and technology vendors. Researchers should test resilience outcomes across institution size, ownership structure and regulatory maturity, while developing African datasets on outage duration, recovery performance, customer impact and third-party incidents to support supervisory benchmarking.

VIII. CONCLUSION

The study has demonstrated that business continuity and disaster recovery preparedness within African financial services must be understood as an integrated resilience capability rather than a narrow technical or compliance function. By examining the evolution of continuity practices, the conceptual relationship between business continuity management, disaster recovery and operational resilience, and the disruptive effects of COVID-19, the review achieved its objective of identifying the institutional, technological and infrastructural conditions that shape crisis readiness across the continent. The analysis showed that the pandemic exposed significant weaknesses in workforce mobility, branch-dependent service models, customer access, cybersecurity, third-party

reliance, power availability and recovery testing, while simultaneously accelerating digital banking, cloud adoption, remote operations and alternative service channels.

A central finding is that preparedness remains uneven across African financial institutions because resilience is influenced by governance quality, regulatory capacity, capital strength, technological maturity, infrastructure reliability and the inclusiveness of digital delivery systems. The review further established that effective recovery depends on rigorous risk assessment, business impact analysis, clear recovery prioritisation, tested failover arrangements and protection of both digital and physical infrastructure. COVID-19 also revealed that operational resilience is inseparable from financial stability, liquidity management, customer inclusion and coordinated public-sector response.

Accordingly, African financial institutions should institutionalise scenario-based continuity planning, strengthen board-level oversight, expand resilient digital and cloud architectures, diversify critical third-party dependencies, and conduct regular cross-functional recovery exercises. Regulators should promote harmonised resilience standards, sector-wide stress testing, cyber-incident coordination and proportionate supervisory requirements. Greater investment is also required in reliable energy, telecommunications redundancy, workforce capability and inclusive digital access. Future research should prioritise comparative, longitudinal evidence on recovery performance, cyber resilience, artificial intelligence, cloud concentration, climate-related disruptions and cross-border dependencies, thereby supporting a more adaptive, measurable and systemically robust financial sector across Africa. These measures are essential for safeguarding trust, continuity, and intermediation during future systemic shocks.

REFERENCES

- [1] Achugamonu, B.U., Omarkhanlen, A.E., Obindah, G., Arewa, A. and Okoye, L.U. (2020) 'Digital finance as a mechanism for extending the boundaries of financial inclusion in sub-Saharan Africa: A general methods of moments approach', *Cogent Arts & Humanities*, 7(1), 1788293. DOI: 10.1080/23311983.2020.1788293. (ResearchGate)
- [2] Aebi, V., Sabato, G. and Schmid, M. (2012) 'Risk management, corporate governance, and bank performance in the financial crisis', *Journal of Banking & Finance*, 36(12), pp. 3213–3226. DOI: 10.1016/j.jbankfin.2011.10.020.
- [3] Akomea-Frimpong, I., Andoh, C., Akomea-Frimpong, A. and Dwomoh-Okudzeto, Y. (2019) 'Control of fraud on mobile money services in Ghana: an exploratory study', *Journal of Money Laundering Control*, 22(2), pp. 300–317. DOI: 10.1108/JMLC-03-2018-0023.
- [4] Allen, F., Carletti, E., Cull, R., Qian, J.Q., Senbet, L. and Valenzuela, P. (2014) 'The African financial development and financial inclusion gaps', *Journal of African Economies*, 23(5), pp. 614–642. DOI: 10.1093/jae/eju015. (OUP Academic)
- [5] Amrani, O. and Najab, A. (2020) 'COVID-19 and Islamic banking services: Digitalisation as a post-crisis solution (case of Morocco)', *European Journal of Islamic Finance*, 16, pp. 1–10. DOI: 10.13135/2421-2172/4913. (Unito Journals)
- [6] Arner, D.W., Zetsche, D.A., Buckley, R.P. and Barberis, J.N. (2017) 'FinTech and RegTech: Enabling innovation while preserving financial stability', *Georgetown Journal of International Affairs*, 18(3), pp. 47–58. DOI: 10.1353/gia.2017.0036.
- [7] Asadi, S., Nilashi, M., Husin, A.R.C. and Yadegaridehkordi, E. (2017) 'Customers' perspectives on adoption of cloud computing in banking sector', *Information Technology and Management*, 18(4), pp. 305–330. DOI: 10.1007/s10799-016-0270-8.
- [8] Asgary, A., Anjum, M.I. and Azimi, N. (2012) 'Disaster recovery and business continuity after the 2010 flood in Pakistan: Case of small businesses', *International Journal of Disaster Risk Reduction*, 2, pp. 46–56. DOI: 10.1016/j.ijdrr.2012.08.001. (ScienceDirect)
- [9] Ayo, C.K., Oni, A.A., Adewoye, O.J. and Eweoya, I.O. (2016) 'E-banking users' behaviour: e-service quality, attitude, and customer satisfaction', *International Journal of*

- Bank Marketing, 34(3), pp. 347–367. DOI: 10.1108/IJBM-12-2014-0175. (ScienceDirect)
- [10] Babajide, A.A., Lawal, A.I., Amodu, L.O., Ewetan, O.O., Esowe, S.L. and Okafor, T.C. (2020) ‘Financial institutions concentration and financial inclusion penetration in Nigeria: a comparative analysis’, *Journal of Contemporary African Studies*, 38(4), pp. 610–626. DOI: 10.1080/02589001.2020.1822991. (ResearchGate)
- [11] Baicu, C.G., Gărdan, I.P., Gărdan, D.A. and Epuran, G. (2020) ‘The impact of COVID-19 on consumer behavior in retail banking: Evidence from Romania’, *Management & Marketing: Challenges for the Knowledge Society*, 15(S1), pp. 534–556. DOI: 10.2478/mmcks-2020-0031. (IDEAS/RePEc)
- [12] Benaroch, M. (2020) ‘Cybersecurity risk in IT outsourcing—Challenges and emerging realities’, in Hirschheim, R., Heinzl, A. and Dibbern, J. (eds.) *Information Systems Outsourcing: The Era of Digital Transformation*. 5th edn. Cham: Springer, pp. 313–334. DOI: 10.1007/978-3-030-45819-5_13.
- [13] Berger, A.N. and Bouwman, C.H.S. (2013) ‘How does capital affect bank performance during financial crises?’, *Journal of Financial Economics*, 109(1), pp. 146–176. DOI: 10.1016/j.jfineco.2013.02.008. (IDEAS/RePEc)
- [14] Berger, A.N., Imbierowicz, B. and Rauch, C. (2016) ‘The roles of corporate governance in bank failures during the recent financial crisis’, *Journal of Money, Credit and Banking*, 48(4), pp. 729–770. DOI: 10.1111/jmcb.12316.
- [15] Botha, J. and von Solms, R. (2004) ‘A cyclic approach to business continuity planning’, *Information Management & Computer Security*, 12(4), pp. 328–337. DOI: 10.1108/09685220410553541. (Emerald Publishing)
- [16] Burnard, K. and Bhamra, R. (2011) ‘Organisational resilience: Development of a conceptual framework for organisational responses’, *International Journal of Production Research*, 49(18), pp. 5581–5599. DOI: 10.1080/00207543.2011.563827. (Royal Holloway Research Portal)
- [17] Carnevale, J.B. and Hatak, I. (2020) ‘Employee adjustment and well-being in the era of COVID-19: Implications for human resource management’, *Journal of Business Research*, 116, pp. 183–187. DOI: 10.1016/j.jbusres.2020.05.037. (IDEAS/RePEc)
- [18] Chukwuani, V.N. (2019) ‘Credit risk management, disaster recovery and business continuity in the Nigerian banking industry: Implications on performance’, *Information and Knowledge Management*, 9(9), pp. 30–39. DOI: 10.7176/IKM/9-9-05. (IISTE)
- [19] Danisman, G.O. and Tarazi, A. (2020) ‘Financial inclusion and bank stability: Evidence from Europe’, *The European Journal of Finance*, 26(18), pp. 1842–1855. DOI: 10.1080/1351847X.2020.1782958. (IDEAS/RePEc)
- [20] Dauda, S.Y. and Lee, J. (2015) ‘Technology adoption: A conjoint analysis of consumers’ preference on future online banking services’, *Information Systems*, 53, pp. 1–15. DOI: 10.1016/j.is.2015.04.006.
- [21] David-West, O., Iheanachor, N. and Kelikume, I. (2018) ‘A resource-based view of digital financial services (DFS): An exploratory study of Nigerian providers’, *Journal of Business Research*, 88, pp. 513–526. DOI: 10.1016/j.jbusres.2018.01.034. (IDEAS/RePEc)
- [22] de Jongh, E., de Jongh, R., de Jongh, D. and van Vuuren, G. (2013) ‘A review of operational risk in banks and its role in the financial crisis’, *South African Journal of Economic and Management*
- [23] De, R., Pandey, N. and Pal, A. (2020) ‘Impact of digital surge during COVID-19 pandemic: A viewpoint on research and practice’, *International Journal of Information Management*, 55, 102171. DOI: 10.1016/j.ijinfomgt.2020.102171. (IDEAS/RePEc)
- [24] Dingel, J.I. and Neiman, B. (2020) ‘How many jobs can be done at home?’, *Journal of Public Economics*, 189, 104235. DOI: 10.1016/j.jpubeco.2020.104235. (IDEAS/RePEc)
- [25] Duchek, S. (2020) ‘Organizational resilience: a capability-based conceptualization’, *Business Research*, 13(1), pp. 215–246. DOI: 10.1007/s40685-019-0085-7. (Springer)
- [26] Ejiogu, A., Okechukwu, O. and Ejiogu, C. (2020) ‘Nigerian budgetary response to the COVID-19

- pandemic and its shrinking fiscal space: Financial sustainability, employment, social inequality and business implications', *Journal of Public Budgeting, Accounting & Financial Management*, 32(5), pp. 919–928. DOI: 10.1108/JPBAFM-07-2020-0101. (Emerald Publishing)
- [27] Ellul, A. and Yerramilli, V. (2013) 'Stronger risk controls, lower risk: Evidence from U.S. bank holding companies', *The Journal of Finance*, 68(5), pp. 1757–1803. DOI: 10.1111/jofi.12057.
- [28] Essuman, D., Boso, N. and Annan, J. (2020) 'Operational resilience, disruption, and efficiency: conceptual and empirical analyses', *International Journal of Production Economics*, 229, 107762. DOI: 10.1016/j.ijpe.2020.107762. (IDEAS/RePEc)
- [29] Falemi, A., Akhigbe, R. and Akin-Oluyomi, O.T. (2020) 'A conceptual supply chain talent development model for capability building across distributed operations', *International Journal of Multidisciplinary Research and Growth Evaluation*, 1(5), pp. 439–456. DOI: 10.54660/IJMRGE.2020.1.5.439-456. (All Multidisciplinary Journal)
- [30] Ferreira, S. and Dickason-Koekemoer, Z. (2019) 'A conceptual model of operational risk events in the banking sector', *Cogent Economics & Finance*, 7(1), 1706394. DOI: 10.1080/23322039.2019.1706394. (Taylor & Francis Online)
- [31] Furnell, S. and Shah, J.N. (2020) 'Home working and cyber security – an outbreak of unpreparedness?', *Computer Fraud & Security*, 2020(8), pp. 6–12. DOI: 10.1016/S1361-3723(20)30084-1.
- [32] Gadzo, S.G., Kporgbor, H.K. and Gatsi, J.G. (2019) 'Credit risk and operational risk on financial performance of universal banks in Ghana: A partial least squares structural equation model (PLS-SEM) approach', *Cogent Economics & Finance*, 7(1), 1589406. DOI: 10.1080/23322039.2019.1589406.
- [33] Gai, K., Qiu, M. and Sun, X. (2018) 'A survey on FinTech', *Journal of Network and Computer Applications*, 103, pp. 262–273. DOI: 10.1016/j.jnca.2017.10.011.
- [34] Gomber, P., Koch, J.-A. and Siering, M. (2017) 'Digital Finance and FinTech: Current research and future research directions', *Journal of Business Economics*, 87(5), pp. 537–580. DOI: 10.1007/s11573-017-0852-x.
- [35] Goodell, J.W. (2020) 'COVID-19 and finance: Agendas for future research', *Finance Research Letters*, 35, 101512. DOI: 10.1016/j.frl.2020.101512. (PubMed)
- [36] Hanafizadeh, P. and Zare Ravasan, A. (2018) 'A model for selecting IT outsourcing strategy: the case of e-banking channels', *Journal of Global Information Technology Management*, 21(2), pp. 111–138. DOI: 10.1080/1097198X.2018.1462070.
- [37] Herbane, B. (2010) 'The evolution of business continuity management: a historical review of practices and drivers', *Business History*, 52(6), pp. 978–1002. DOI: 10.1080/00076791.2010.511185. (Taylor & Francis Online)
- [38] Inegbedion, H., Vincent, B.D. and Obadiaru, E. (2020) 'Risk management and the financial performance of banks in Nigeria', *International Journal of Financial Research*, 11(5), pp. 115–128. DOI: 10.5430/ijfr.v11n5p115.
- [39] Kodom, M., Ackah, C., Steel, W.F. and Bokpin, G.A. (2020) 'Drivers of mobile financial inclusion in Ghana', *Enterprise Development and Microfinance*, 31(4), pp. 226–253. DOI: 10.3362/1755-1986.20-00008. (University of Ghana)
- [40] Kshetri, N. (2019) 'Cybercrime and cybersecurity in Africa', *Journal of Global Information Technology Management*, 22(2), pp. 77–81. DOI: 10.1080/1097198X.2019.1603527.
- [41] Laeven, L. and Levine, R. (2009) 'Bank governance, regulation and risk taking', *Journal of Financial Economics*, 93(2), pp. 259–275. DOI: 10.1016/j.jfineco.2008.09.003.
- [42] Li, L., Strahan, P.E. and Zhang, S. (2020) 'Banks as lenders of first resort: Evidence from the COVID-19 crisis', *The Review of Corporate Finance Studies*, 9(3), pp. 472–500. DOI: 10.1093/rcfs/cfaa009. (OUP Academic)
- [43] Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A. (2011) 'Cloud computing—The business perspective', *Decision Support Systems*, 51(1), pp. 176–189. DOI: 10.1016/j.dss.2010.12.006.

- [44] Mendonça, J., Andrade, E., Endo, P.T. and Lima, R. (2019) 'Disaster recovery solutions for IT systems: A systematic mapping study', *Journal of Systems and Software*, 149, pp. 511–530. DOI: 10.1016/j.jss.2018.12.023.
- [45] Mhlanga, D. (2020) 'Industry 4.0 in finance: The impact of artificial intelligence (AI) on digital financial inclusion', *International Journal of Financial Studies*, 8(3), 45. DOI: 10.3390/ijfs8030045.
- [46] Mthobi, O. and Grzybowski, L. (2017) 'Infrastructure deficiencies and adoption of mobile money in Sub-Saharan Africa', *Information Economics and Policy*, 40, pp. 71–79. DOI: 10.1016/j.infoecopol.2017.05.003.
- [47] Mutarindwa, S., Schäfer, D. and Stephan, A. (2020) 'Central banks' supervisory guidance on corporate governance and bank stability: Evidence from African countries', *Emerging Markets Review*, 43, 100694. DOI: 10.1016/j.ememar.2020.100694.
- [48] Mutarindwa, S., Schäfer, D. and Stephan, A. (2020) 'The impact of liquidity and capital requirements on lending and stability of African banks', *Journal of International Financial Markets, Institutions and Money*, 67, 101201. DOI: 10.1016/j.intfin.2020.101201. (IDEAS/RePEc)
- [49] Nakpodia, F., Adegbite, E., Amaeshi, K. and Owolabi, A. (2018) 'Neither principles nor rules: Making corporate governance work in Sub-Saharan Africa', *Journal of Business Ethics*, 151(2), pp. 391–408. DOI: 10.1007/s10551-016-3208-5.
- [50] Niemimaa, M., Järveläinen, J., Heikkilä, M. and Heikkilä, J. (2019) 'Business continuity of business models: Evaluating the resilience of business models for contingencies', *International Journal of Information Management*, 49, pp. 208–216. DOI: 10.1016/j.ijinfomgt.2019.04.010. (IDEAS/RePEc)
- [51] Okoye, L.U., Olokoyo, F., Okoh, J.I., Ezeji, F. and Uzohue, R. (2020) 'Effect of corporate governance on the financial performance of commercial banks in Nigeria', *Banks and Bank Systems*, 15(3), pp. 55–69. DOI: 10.21511/bbs.15(3).2020.06.
- [52] Ozili, P.K. (2018) 'Banking stability determinants in Africa', *International Journal of Managerial Finance*, 14(4), pp. 462–483. DOI: 10.1108/IJMF-01-2018-0007. (Emerald Publishing)
- [53] Ozili, P.K. (2018) 'Impact of digital finance on financial inclusion and stability', *Borsa Istanbul Review*, 18(4), pp. 329–340. DOI: 10.1016/j.bir.2017.12.003.
- [54] Ozili, P.K. (2020) 'COVID-19 pandemic and economic crisis: The Nigerian experience and structural causes', *SSRN Electronic Journal*. DOI: 10.2139/ssrn.3567419. (SSRN)
- [55] Păunescu, C. and Argatu, R. (2020) 'Critical functions in ensuring effective business continuity management: Evidence from Romanian companies', *Journal of Business Economics and Management*, 21(2), pp. 497–520. DOI: 10.3846/jbem.2020.12205. (VGTU Journals)
- [56] Rabbani, M., Rezaei Soufi, H. and Torabi, S.A. (2016) 'Developing a two-step fuzzy cost-benefit analysis for strategies to continuity management and disaster recovery', *Safety Science*, 85, pp. 9–22. DOI: 10.1016/j.ssci.2015.12.025.
- [57] Rizwan, M.S., Ahmad, G. and Ashraf, D. (2020) 'Systemic risk: The impact of COVID-19', *Finance Research Letters*, 36, 101682. DOI: 10.1016/j.frl.2020.101682. (IDEAS/RePEc)
- [58] Sahebjamnia, N., Torabi, S.A. and Mansouri, S.A. (2015) 'Integrated business continuity and disaster recovery planning: towards organizational resilience', *European Journal of Operational Research*, 242(1), pp. 261–273. DOI: 10.1016/j.ejor.2014.09.055. (Brunel University Research Archive)
- [59] Sambo, F. and Bankole, F.O. (2016) 'A normative process model for ICT business continuity plan for disaster management in small, medium and large enterprises', *International Journal of Electrical and Computer Engineering*, 6(5), pp. 2425–2431. DOI: 10.11591/ijece.v6i5.pp2425-2431. (IJECE)
- [60] Sawalha, I.H.S. (2020) 'Business continuity management: use and approach's effectiveness', *Continuity & Resilience Review*, 2(2), pp. 81–96. DOI: 10.1108/CRR-05-2020-0016. (DOI)
- [61] Scott, S.V., Van Reenen, J. and Zachariadis, M. (2017) 'The long-term effect of digital innovation on bank performance: An empirical

- study of SWIFT adoption in financial services', *Research Policy*, 46(5), pp. 984–1004. DOI: 10.1016/j.respol.2017.03.010.
- [62] Seetharaman, P. (2020) 'Business model shifts: Impact of Covid-19', *International Journal of Information Management*, 54, 102173. DOI: 10.1016/j.ijinfomgt.2020.102173. (ScienceDirect)
- [63] Sikdar, P. (2011) 'Alternate approaches to business impact analysis', *Information Security Journal: A Global Perspective*, 20(3), pp. 128–134. DOI: 10.1080/19393555.2010.551274.
- [64] Sunday, E.A. and Omoegun, G.O. (2018) 'Integrating solar power solutions in small-scale manufacturing industries in Nigeria', *International Journal of Scientific Research in Science, Engineering and Technology*, 4(8), pp. 832–853. (ResearchGate)
- [65] Sunday, E.A., Omoegun, G.O., Essien, M.A. and Oluokun, O.A. (2019) 'Thermodynamic efficiency and control strategies in residential air conditioning systems', *International Journal of Scientific Research in Civil Engineering*, 3(3), pp. 52–76. (IJRCE)
- [66] Suri, T. and Jack, W. (2016) 'The long-run poverty and gender impacts of mobile money', *Science*, 354(6317), pp. 1288–1292. DOI: 10.1126/science.aah5309.
- [67] Torabi, S.A., Giah, R. and Sahebjamnia, N. (2016) 'An enhanced risk assessment framework for business continuity management systems', *Safety Science*, 89, pp. 201–218. DOI: 10.1016/j.ssci.2016.06.015.
- [68] Torabi, S.A., Rezaei Soufi, H. and Sahebjamnia, N. (2014) 'A new framework for business impact analysis in business continuity management (with a case study)', *Safety Science*, 68, pp. 309–323. DOI: 10.1016/j.ssci.2014.04.017.
- [69] Vives, X. (2019) 'Digital disruption in banking', *Annual Review of Financial Economics*, 11, pp. 243–272. DOI: 10.1146/annurev-financial-100719-120854.
- [70] Waizenegger, L., McKenna, B., Cai, W. and Bendz, T. (2020) 'An affordance perspective of team collaboration and enforced working from home during COVID-19', *European Journal of Information Systems*, 29(4), pp. 429–442. DOI: 10.1080/0960085X.2020.1800417.
- [71] Wang, V., Nnaji, H. and Jung, J. (2020) 'Internet banking in Nigeria: cyber security breaches, practices and capability', *International Journal of Law, Crime and Justice*, 62, 100415. DOI: 10.1016/j.ijlcrj.2020.100415.
- [72] Winful, C.E., Sarpong Jnr., D. and Dondjio, I. (2020) 'Financial sector readiness to support economic activities under COVID-19: The case of the African continent', *Journal of Economics and International Finance*, 12(4), pp. 164–173. DOI: 10.5897/JEIF2020.1077. (ResearchGate)
- [73] Zhang, D., Hu, M. and Ji, Q. (2020) 'Financial markets under the global pandemic of COVID-19', *Finance Research Letters*, 36, 101528. DOI: 10.1016/j.frl.2020.101528. (IDEAS/RePEc)