Journal of Business Decision and Risk Sciences (JBDRS)

https://doi.org/

Journal Homepage: www.JBDRSJournal.com

ORIGINAL RESEARCH PAPER

Designing a Conceptual Framework for Enhancing Operational Resilience in the Banking Industry: A Study Based on International Documents

Seyyed Abdollah Razavi [a, *]; Samira Basirizadeh [b]

[a] *Department of Petroleum Economics and Energy Diplomacy, Tehran Faculty of Petroleum, Petroleum University of Technology (PUT), Abadan, Iran.*
[b] *Department of Economics and Islamic Banking, Faculty of Economics, Kharazmi University, Tehran, Iran.*

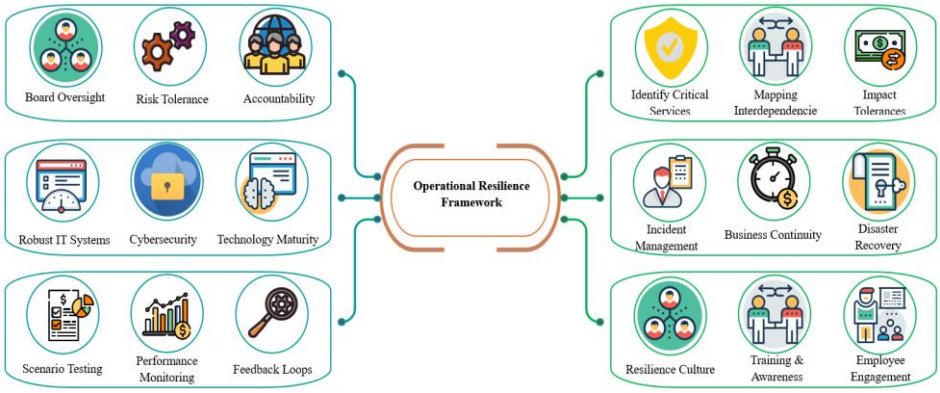
P A P E R I N F O

Paper history:
Received: 08/05/2026
Revised: 09/05/2026
Accepted in revised form: 09/20/2026
Published: 9/30/2026

***Keywords*:**
Operational Resilience;
Banking Industry;
Operational Risk;
Qualitative Meta-synthesis;
Bank Governance.

A B S T R A C T

The rapid expansion of digital banking, growing dependence on information technology, and increasing cyber and operational threats have made operational resilience a critical priority for financial institutions, particularly systemically important banks. Despite the development of international regulatory standards and supervisory frameworks, differences in regulatory approaches and fragmented requirements highlight the need for an integrated framework that captures the key dimensions of operational resilience. This study develops a conceptual framework for enhancing operational resilience in systemically important banks through a qualitative meta-synthesis of authoritative international documents. Six reference documents issued by major international regulatory and supervisory bodies were selected based on credibility, thematic relevance, comprehensiveness, applicability, and official status. The documents were systematically analyzed using open, axial, and selective coding. The analysis yielded 136 open codes and 12 axial categories, which were synthesized into six overarching themes: strategic resilience governance; critical service management; operational infrastructure resilience; preparedness, response, and recovery; monitoring, testing, and continuous learning; and human capital and resilience culture. Based on these themes, an integrated framework was developed to explain the relationships among the core dimensions of operational resilience. The findings indicate that operational resilience depends on the coordinated interaction of effective governance, protection of critical services, resilient digital and operational infrastructures, organizational preparedness, continuous learning, and a strong resilience culture. The proposed framework provides a conceptual foundation for policymaking, management system design, and implementation mechanisms in systemically important banks.



1. Introduction

Over the past two decades, the banking system has undergone fundamental transformations driven by digitalization. The expansion of non-branch-based services, increasing dependence on information technology, growing adoption of cloud computing, outsourcing of specialized services, and greater connectivity to digital ecosystems have improved the efficiency, speed, and quality of financial service delivery. At the same time, these developments have fundamentally altered the nature of operational risks [1]. In such an environment, a disruption in a technology system, an outsourced service provider, or even an internal process can, within a short period, affect millions of customers, financial markets, and the economic stability of nations.

* Corresponding Author: Seyyed Abdollah Razavi
E-mail address: srazavi@put.ac.ir
ISSN:
URL: https://www.jbdrsjournal.com/issue_53267_53271.html

Please cite this article as: S. A. Razavi, & S. Basirizadeh, *Journal of Business Decision and Risk Sciences (JBDRS)*, 2026, 2(3), 121-127. https://doi.org/

/© 2026 The Author(s). Published by Power of New Vision Movement Institute.

Consequently, operational resilience has, in recent years, evolved from a specialized topic in risk management to one of the strategic priorities of major banks and financial supervisory authorities worldwide [2].

Recent events have further underscored the significance of this issue. Widespread ransomware attacks, disruptions in payment systems, data center outages, cloud service failures, the outbreak of war, and the escalation of cyber threats have demonstrated that even banks with advanced infrastructures may remain vulnerable to operational disruptions. The experience of these events has shifted the perspective of regulatory authorities from "risk prevention" to "the ability to sustain service delivery during disruptions." As a result, the concept of operational resilience has gradually assumed a central position in supervisory policies and banking strategies.

In response to these developments, a collection of international standards and guidelines has been published in recent years by institutions such as the Basel Committee on Banking Supervision (BCBS), the Bank of England and UK financial regulatory authorities, the European Union, the Australian Prudential Regulation Authority (APRA), the Monetary Authority of Singapore (MAS), and the U.S. Federal Financial Institutions Examination Council (FFIEC). Although international operational resilience documents differ in scope and implementation requirements, they all emphasize the continuity of critical services, risk governance, and the enhancement of organizational resilience. However, previous studies have predominantly examined these documents independently and have rarely addressed the integration of their common components and their localization for the banking systems of developing countries, particularly Iran. Therefore, the present study, employing a qualitative meta-synthesis method, analyzes six international reference documents and, by extracting common themes, proposes a localized framework for enhancing the operational resilience of systemically important banks in Iran.

Operational resilience has, in recent years, become one of the key concepts in the literature on risk management and banking regulation. Unlike traditional approaches that focused on reducing the likelihood of operational risks, this concept emphasizes the organization's ability to anticipate, prepare for, respond to, sustain the delivery of critical services, and recover swiftly following a disruption [3]. From this perspective, disruption is inevitable, and the organization's success depends on maintaining critical functions under crisis conditions.

The Basel Committee defines operational resilience as the ability of a bank to prevent, adapt to, respond to, and recover from operational disruptions with the aim of sustaining critical services [3]. Furthermore, the Digital Operational Resilience Act has extended this concept to the capacity of financial institutions to withstand, respond to, recover from, and learn from information and communication technology-related incidents [4]. Therefore, operational resilience is not limited to crisis management or cybersecurity alone; rather, it encompasses all processes, technology, human resources, suppliers, and governance mechanisms [5].

From a theoretical standpoint, operational resilience is a type of dynamic capability that enables an organization to adapt to environmental changes and unforeseen disruptions while maintaining its core functions and pursuing continuous improvement [6]. Hence, operational resilience is an organizational capability that emerges from the interaction of governance, risk management, technology, culture, and learning [6,7].

Contemporary literature indicates that although financial supervisory authorities have adopted different approaches to developing operational resilience, they emphasize a set of common components. The first component is governance. Virtually all international frameworks place the ultimate responsibility for operational resilience on the board of directors and senior management, considering it part of the organization's governance system [3]. The second component is the identification of critical services. Under this approach, the focus has shifted from merely protecting systems and processes toward ensuring the continuity of services whose disruption could have serious consequences for customers, financial markets, or economic stability [8]. For this reason, the concept of impact tolerance has become one of the main pillars of the new frameworks.

Another dimension of operational resilience is digital operational resilience. The development of digital banking, cloud computing, artificial intelligence, and open banking has rendered information technology infrastructures an inseparable part of banking services. Accordingly, the Digital Operational Resilience Act and other international documents place particular emphasis on information technology risk management, cybersecurity, resilience testing, and third-party management [4].

In addition, recent research indicates that organizational culture, human capital, continuous learning, scenario-based testing, and continuous monitoring are also essential components of operational resilience. Organizations that document their crisis experiences, regularly conduct exercises, and incorporate test results into managerial decision-making typically experience a higher level of resilience [9-11].

Therefore, the theoretical literature demonstrates that operational resilience is a multidimensional concept, and its realization requires simultaneous coordination among managerial, technological, organizational, and supervisory dimensions. It is precisely this multidimensionality that justifies the use of integrative and exploratory methods to identify its components [12].

Chanon et al. [10], in a study entitled "A Practical Guide to Operational Resilience in the UK Financial Sector," published in the British Actuarial Journal, provided a practical guide for UK-based financial institutions subject to operational resilience requirements. By reviewing the latest equivalent guidelines in other countries and at the international level, they identified key issues affecting operational resilience, including risk culture, risk appetite, information technology, tolerance threshold setting, risk modelling, scenario planning, and customer-centric operational resilience. The findings indicated that implementing an operational resilience framework and a maturity assessment dashboard can help enhance the effectiveness of this system. They also emphasized the necessity of strengthening controls and operational risk management frameworks [13].

Tuominen [14], in a supervisory blog post of the European Central Bank entitled "Operational Resilience in the Digital Age," examined the implementation implications of the European Union's new Digital Operational Resilience Act (DORA). Referring to the doubling of cyberattacks in recent years and the growing dependence of banks on third-party information and communication technology (ICT) service providers, he outlined three main implications of DORA: (1) strengthening the incident reporting framework by covering a broader range of ICT-related indicators, (2) improving banks' preparedness against cyberattacks through threat-led penetration testing (TLPT), and (3) more rigorous oversight of third-party risks. He concluded that DORA has provided supervisors with new supervisory tools and that banks must swiftly address existing gaps in technology change risk management and third-party contracts.

Kamel et al. [15], in a study entitled "Enhancing Resilience, Adaptability, and Operational Risk Transformation through Competitive Intelligence," published in the Journal of Modern Business and Technology, examined the role of competitive intelligence as a strategic capability in reducing vulnerability and strengthening operational resilience in complex and turbulent environments. Employing a systematic literature review and template analysis approach, this study demonstrated that competitive intelligence can improve adaptive risk management processes by reducing information asymmetry and strengthening early warning systems. They recommended that competitive intelligence be formally integrated into enterprise risk governance frameworks and that synergy among intelligence, risk, and strategy units be developed.

Ningrum [16], in a study on "Digital Transformation and Operational Risk in Islamic Banking," analyzed the operational risk challenges arising from digital transformation in Islamic banking and examined mitigation strategies. The findings indicated that digital transformation, while increasing efficiency, amplifies operational risk complexity due to dependence on technology infrastructures, information systems integration, and inequality in human resource readiness. Effective risk mitigation strategies identified included strengthening internal controls, deploying technology-based risk management, reinforcing cybersecurity frameworks, implementing business continuity programmes, and establishing integrated IT governance.

Tuominen [17], in an interview with the European Central Bank entitled "Enhancing Banks' Capacity to Counter Digital Risks," examined the implementation experiences of DORA and the challenges facing banks. He emphasized that banks must shift their approach from reactive risk management to proactive resilience management and focus on regular testing of severe scenarios, transparency in the information technology supply chain, and strengthening an incident reporting culture.

The Basel Committee on Banking Supervision (BCBS), in its documents Principles for Operational Resilience and Principles for the Sound Management of Operational Risk, has established a fundamental framework for financial institutions. These principles emphasize the identification of critical services, setting impact tolerances for disruption, dependency mapping, testing of severe scenarios, and third-party risk management. According to analytical reports, more than 90 percent of banks have identified their critical business services, and approximately 65 percent have developed business continuity plans for these services [18].

The European Union, by adopting the Digital Operational Resilience Act (DORA), which has been enforceable since January 2025, has taken a significant step toward harmonizing digital resilience regulations at the Union level. This regulation includes requirements such as integrated incident reporting, threat-led penetration testing for systemic banks, and oversight of critical third-party ICT service providers. Supervisory data indicate that 38 percent of major incidents reported in 2025 were rooted in information technology changes, and costs associated with cloud services have increased from 4 percent in 2021 to 17 percent of banks' IT budgets in 2025 [19].

The Australian Prudential Regulation Authority (APRA) and the Monetary Authority of Singapore (MAS) have also, through the publication of the Operational Risk Management Standard and the Business Continuity Management Guidelines, respectively, contributed to establishing an operational resilience system in financial institutions under their supervision [18].

A review of existing studies indicates that, despite significant progress at the international level, important research gaps remain in this field:

First, the lack of framework integration: Although various regulatory bodies (Basel, the EU, Australia, Singapore, and the US) have each developed frameworks, an integrated conceptual framework that systematically elucidates the key components of operational resilience is rarely found in the research literature. Most existing

studies have either been limited to a specific geographical region (such as the UK or the EU) or have focused on technical and technological dimensions [12,13]. Second, the scarcity of qualitative meta-synthesis studies: Despite numerous studies in the field of operational risk and business continuity, no study employing a qualitative meta-synthesis method to extract overarching themes from international reference documents was identified. This gap becomes particularly significant when one considers that the aforementioned documents have approached the subject from different perspectives (regulatory, risk management, technological, and governance), and the need to synthesize these perspectives into a comprehensive conceptual framework is felt [14,15].

Third, the neglect of systematic interaction among components: Existing studies have often examined the components of operational resilience (governance, critical service management, infrastructure, readiness and recovery, monitoring and learning, and human capital) in isolation, with less attention paid to the systematic interaction among these dimensions. This is despite the fact that some authoritative sources explicitly refer to the role of organizational culture and human capital as fundamental prerequisites of resilience, which have received less attention in previous research [18,19].

Accordingly, the present study aims to fill these gaps and, using a qualitative meta-synthesis method, designs an integrated conceptual framework for enhancing operational resilience in the banking industry based on international reference documents.

2. Materials and Methods

The present study is applied in terms of objective and qualitative in terms of nature. Given that the aim of the research is to identify, integrate, and organize existing concepts in international documents and to propose a localized framework for enhancing the operational resilience of systemically important banks, qualitative meta-synthesis was selected as the primary research strategy. Qualitative meta-synthesis is a systematic method for integrating findings from qualitative studies and documents, enabling the extraction of shared concepts, themes, and patterns from various sources [20,21].

Unlike narrative reviews, which predominantly describe studies, meta-synthesis employs systematic analysis and multi-stage coding to generate new knowledge and produce conceptual frameworks [22]. Therefore, this method is considered the most appropriate approach for the present study, which seeks to design an integrative framework based on authoritative international documents.

2.1. Stages of Meta-Synthesis Implementation

In this study, the meta-synthesis process was conducted based on Sandelowski and Barroso's [20] seven-stage model. This model is one of the most well-known and widely used meta-synthesis frameworks in management and policy research, providing the possibility of transparent and reproducible data analysis. The stages of this research are presented in Table 1.

Table 1. Stages of Qualitative Meta-Synthesis Implementation in the Present Study

Stage	Description of Activity
1	Formulating the research question and determining the scope of the study
2	Searching for and identifying relevant international documents
3	Screening and selecting documents based on inclusion and exclusion criteria
4	Extracting data and key concepts
5	Open, axial, and selective coding
6	Extracting themes and designing the conceptual framework
7	Interpreting findings and presenting the proposed framework

2.2. Study Population and Document Selection

In this study, the selection of key operational resilience documents was conducted through a systematic approach. Following the initial identification of international standards and guidelines in the fields of operational resilience, risk management, business continuity, and digital resilience, documents were evaluated based on criteria such as the credibility of the issuing institution, direct relevance to banking, content comprehensiveness, and the official status of the version. During the screening stage, one-dimensional documents (such as those solely addressing cybersecurity or crisis management), drafts, and duplicate versions were excluded. Ultimately, six authoritative and comprehensive international documents from global financial regulatory institutions were selected as the primary sources for analysis (selection criteria are presented in Table 2).

Table 2. Document Selection Criteria

Criterion	Description
Source credibility	Published by official and international institutions in the field of banking and financial regulation
Thematic relevance	Direct focus on operational resilience or its key components
Comprehensiveness	Simultaneous coverage of managerial, operational, and technological dimensions
Applicability	Usability in systemically important banks
Official version	Publication of a final and enforceable version or an official guideline

In the final screening stage, six international documents possessing the highest degree of influence and content comprehensiveness in the field of operational resilience were selected for conducting the qualitative analysis stages and extracting the dimensions of the proposed framework. These documents form the basis of the coding process and thematic analysis in the present study. Details regarding the title, year of publication, and issuing institution of these documents are presented in Table 3:

Table 3. Selected Documents of the Study

No.	Document	Year	Issuing Institution
1	Principles for Operational Resilience	2021	Basel Committee on Banking Supervision (BCBS)
2	Operational Resilience Policy Statement	2021	Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) – United Kingdom
3	Digital Operational Resilience Act (DORA)	2022	European Union
4	Prudential Standard CPS 230	2023	Australian Prudential Regulation Authority (APRA)
5	Business Continuity Management Guidelines	2022	Monetary Authority of Singapore (MAS)
6	Business Continuity Management Booklet	2019	U.S. Federal Financial Institutions Examination Council (FFIEC)

2.3. Data Analysis Method

Following the selection of documents, the full text of each was systematically reviewed and analyzed. The unit of analysis in this study comprised propositions, requirements, principles, and key recommendations related to operational resilience. Data analysis was conducted based on Strauss and Corbin's [23] three-stage coding method. In the first stage, initial concepts were extracted from the text of the documents and recorded as open codes. Subsequently, similar codes were grouped into axial categories, and finally, through selective coding, overarching themes were identified and the conceptual framework of the study was designed. This process enabled the researcher to identify the relationships among various dimensions of operational resilience while maintaining conceptual coherence. The process of this analysis is illustrated in Figure 1.

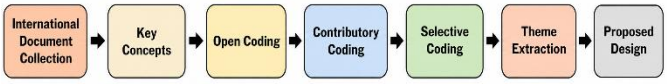


Figure 1. Data Analysis Process

2.4. Validity and Reliability of Findings

To enhance the validity of the research, strategies commonly employed in qualitative studies were utilized. Content validity was ensured through repeated review of the documents, continuous comparison of codes, and assessment of the consistency between extracted concepts and the original text. Furthermore, to increase reliability, the coding process was conducted in multiple stages, and the results of each stage were reconciled with the preceding stages. In addition, the initially extracted framework was shared with several experts in the field of banking risk management and operational resilience, and the necessary revisions were made based on their comments.

3. Result and Discussions

3.1. Data Preparation for Analysis

Following the selection of documents, the full text of each was independently studied. The unit of analysis in this study comprised policy propositions, supervisory requirements, executive principles, recommendations, and concepts related to operational resilience. To maintain analytical coherence, all key concepts of each document were first extracted and recorded as semantic units. Subsequently, similar concepts, regardless of differences in terminology or mode of expression, were placed alongside one another to prevent the creation of duplicate codes.

At this stage, the research focused on extracting concepts rather than interpreting them. Therefore, each concept was recorded with the least possible degree of researcher inference and with fidelity to the original text of the documents. This approach ensured that the open coding process was based on actual and traceable data, providing the necessary foundation for forming axial categories in subsequent stages.

3.2. Open Coding

In the first stage of data analysis, the full text of the six selected documents was studied line by line, and all concepts, requirements, principles, and recommendations related to operational resilience were extracted. At this stage, an effort was made to convert each independent proposition, without initial interpretation, into a short and meaningful concept. These concepts were recorded as open codes and formed the basis for analysis in subsequent stages. In the open coding process, the primary criterion was maintaining the closest possible proximity between the code and the original text of the documents. Hence, in cases where multiple documents used different vocabulary to express the same concept, a common title was selected for that concept following continuous data comparison. This process reduced duplicate codes and increased conceptual coherence.

In total, more than 400 semantic units were extracted from the six documents, which, after removing duplicates and merging similar concepts, were reduced to 136 unique open codes. These codes cover all dimensions related to governance, risk management, critical services, digital resilience, cybersecurity, third-party management, business continuity, organizational culture, resilience testing, organizational learning, and continuous improvement.

Table 4. Sample of the Open Coding Process

Document / Policy-Making Authority	Extracted Proposition	Open Code
Basel Committee	The board of directors bears ultimate responsibility for operational resilience.	Board responsibility in resilience
Basel Committee	The resilience strategy must be aligned with business objectives.	Resilience strategy alignment
UK Prudential Regulation Authority and Financial Conduct Authority	Critical services must be identified.	Identification of critical services
UK Prudential Regulation Authority and Financial Conduct Authority	An impact tolerance must be set for each service.	Setting impact tolerances
EU Digital Operational Resilience Act	The bank must have an ICT risk management framework.	ICT risk management
EU Digital Operational Resilience Act	Periodic digital resilience testing is essential.	Digital resilience testing
Australian Prudential Regulation Authority	Third-party risk must be assessed.	Third-party risk assessment
Australian Prudential Regulation Authority	The business continuity plan must be regularly reviewed.	Business continuity plan review
Monetary Authority of Singapore	Staff training is part of resilience.	Staff training and empowerment
U.S. Federal Financial Institutions Examination Council	Periodic exercises must be conducted.	Conducting resilience exercises
U.S. Federal Financial Institutions Examination Council	Programme performance must be monitored.	Resilience performance monitoring
U.S. Federal Financial Institutions Examination Council	Crisis lessons learned must be documented.	Learning from incidents

3.3. Analysis of Open Coding Results

An examination of the extracted codes indicates that, despite differences in the structure and scope of the documents, a significant proportion of concepts focus on a set of common themes. The highest frequency of codes pertains to resilience governance, critical service management, digital resilience, ICT risk management, business continuity, third-party management, and continuous monitoring. This indicates that financial supervisory authorities do not regard operational resilience merely as a technological or managerial issue; rather, they consider it the outcome of the simultaneous interaction of strategic, operational, technological, and human dimensions.

Furthermore, preliminary analysis revealed that certain concepts, although present in all documents, are expressed with different levels of emphasis. For example, the UK PRA and FCA documents place greater focus on critical services and impact tolerances, while the EU Digital Operational Resilience Act devotes the most attention to digital resilience and ICT risk management. In contrast, the Monetary Authority of Singapore and the U.S. Federal Financial Institutions Examination Council place greater emphasis on training, organizational preparedness, periodic testing, and learning from incidents. These differences served as the basis for forming the main categories of the research at the axial coding stage.

3.4. Axial Coding

Following the extraction of open codes, the axial coding stage was conducted with the aim of identifying relationships among concepts and organizing them into conceptual categories. At this stage, codes that shared commonality in meaning, purpose, and function were compared with one another using the constant comparison method and merged into broader categories. This process enabled the dispersed concepts extracted from the six international documents to be organized into a coherent and interpretable structure. The results of the analysis indicated that the 136 open codes could be classified into 12 axial categories. These categories represent the most significant common dimensions present in the international documents and provide the conceptual foundation necessary for extracting the final themes.

Table 5. Axial Categories Extracted from Document Analysis

Axial Category	Conceptual Description	Sample Open Codes
Resilience governance and leadership	Board accountability, senior management, policy-making, responsibility, and resource allocation	Board responsibility, resilience policy, governance structure
Critical service management	Identification of critical services, service dependencies, and their prioritization	Critical services, service dependencies, service mapping
Impact tolerances	Setting the acceptable level of disruption and service recovery objectives	Impact tolerances, recovery time, impact measurement
Operational risk management	Identification, assessment, and control of operational risks	Risk identification, risk assessment, internal controls
Digital resilience and information technology	ICT risk management, cybersecurity, and digital infrastructures	ICT risk, cyber resilience, data center
Third-party management	Assessment, monitoring, and control of risks arising from outsourcing	Third-party risk, outsourcing, supplier assessment
Business continuity and crisis management	Continuity of bank operations during disruptions and crisis management	Business continuity plan, crisis management, disaster recovery
Human capital and organizational culture	Developing a resilience culture, training, and staff accountability	Training, risk culture, staff awareness
Testing, exercising, and drills	Assessing organizational preparedness through regular testing	Scenario testing, exercises, simulation
Monitoring, reporting, and performance indicators	Continuous monitoring of resilience status and management reporting	Key performance indicators, management dashboard, continuous monitoring
Learning and continuous improvement	Documenting experiences and refining processes	Lessons learned, continuous improvement
Compliance and regulatory requirements	Adhering to legal requirements and accountability to supervisory authorities	Compliance, supervisory assessment, audit

An examination of the extracted categories indicates that operational resilience in international documents is described as an integrated management system. In this system, none of the dimensions operates independently; rather, each category constitutes a part of the chain of creating and sustaining organizational resilience. Among the extracted categories, resilience governance and leadership plays a foundational role, as all the documents under review have placed the ultimate responsibility for establishing and overseeing operational resilience on the board of directors and senior management. This finding indicates that operational resilience is, more than a technological project, a strategic issue at the level of corporate governance. The second important axis is critical service management. Unlike traditional risk management approaches that focused on protecting processes and systems, the new documents regard service protection as the central pillar of resilience. Under this approach, the bank must first identify its critical services, analyze their dependencies, and determine the acceptable tolerances for disruption for each service. Furthermore, the category of digital resilience and information technology reflects a paradigm shift in the banking system. The development of digital banking has rendered information technology risk one of the most significant sources of operational disruption. Accordingly, risk management, cybersecurity, data protection, and digital infrastructure resilience have assumed a special position in all modern frameworks. In contrast, the categories of testing, monitoring, and organizational learning demonstrate that operational resilience is not a static state but rather a dynamic and evolutionary process. Resilient banks continuously test their plans, monitor performance, and incorporate crisis lessons learned into the revision of policies and processes. Therefore, the axial analysis demonstrates that operational resilience is the outcome of the interaction among four main domains, including governance, critical services, operational infrastructures, and learning and continuous improvement mechanisms a matter that, at the next stage and during selective coding, will serve as the basis for extracting overarching themes. To better illustrate these relationships and present an integrated picture of the conceptual structure resulting from the analysis, the relational network among the axial categories is presented in Figure 2. This figure shows how the main categories are positioned around the central concept of "bank operational resilience" and provides the groundwork for extracting overarching themes at the selective coding stage. Figure 2 illustrates the conceptual network resulting from the axial coding stage. As can be observed, the axial categories extracted from international documents do not operate in isolation; rather, they interact with one another within an integrated system. At the center of this network lies the concept of "bank operational resilience," which is formed through the interaction among the dimensions of governance, critical service management, digital resilience, risk management, monitoring and continuous learning, regulatory compliance, and third-party management.



Figure 2. Conceptual Network of Axial Categories

The analysis of relationships among categories revealed that governance and organizational leadership plays a foundational role in shaping the other dimensions of operational resilience, while critical service management and digital resilience constitute the executive core of this system. Furthermore, continuous monitoring, scenario-based testing, and organizational learning serve as feedback mechanisms that drive the continuous improvement of the resilience system's performance. These findings indicate that operational resilience is the outcome of establishing a set of interconnected capabilities and cannot be achieved solely by strengthening one organizational dimension.

Accordingly, at the next stage, the axial categories were merged into overarching themes to extract the final research framework:

3.5. Selective Coding and Extraction of Overarching Themes

At the selective coding stage, the extracted axial categories were re-analyzed with the aim of identifying the conceptual core of the research. At this stage, the primary focus was on identifying relationships among categories and elucidating the macro-structure of operational resilience. To this end, each axial category was evaluated based on its role, function, and conceptual relationship with other categories, so that themes could be extracted which offer a more comprehensive picture of the concept of operational resilience.

The results of the analysis indicated that the twelve axial categories could be organized into six overarching themes. These themes constitute the conceptual core of the present study and elucidate the proposed framework for enhancing the operational resilience of systemically important banks.

Table 6. Overarching Themes Extracted from Thematic Analysis

No.	Overarching Theme	Conceptual Description	Constituent Axial Categories
1	Strategic resilience governance	Establishing governance structures, managerial accountability, and aligning resilience with the bank's macro-strategies	Governance and leadership, compliance and regulatory requirements
2	Critical service management	Identifying critical services, setting impact tolerances, and focusing on continuity of service delivery	Critical service management, impact tolerances
3	Operational infrastructure resilience	Protecting operational infrastructures, information technology, and the service supply chain	Operational risk management, digital resilience, third-party management
4	Readiness, response, and recovery	Developing the capability to respond, recover, and sustain bank operations under crisis conditions	Business continuity and crisis management
5	Monitoring, testing, and continuous learning	Continuously assessing preparedness, measuring performance, and cyclically refining processes	Testing and exercises, monitoring and reporting, learning and continuous improvement
6	Human capital and resilience culture	Developing organizational culture, enhancing awareness, and empowering staff to cope with disruptions	Human capital and organizational culture

The analysis of the extracted themes indicates that operational resilience is a multidimensional concept formed through the interaction of managerial, technological, organizational, and supervisory capabilities. Within this framework, strategic resilience governance is recognized as the foundation of the resilience system, as strategic direction-setting, policy-making, accountability, and resource allocation are carried out through this dimension. The second theme, critical service management, reflects the shift in regulatory authorities' approach from merely protecting assets toward protecting services. Under this approach, the bank first identifies its critical services and then determines the acceptable tolerances for disruption for each service, so that even under crisis conditions, the minimum level of service delivery is maintained.

The third theme, operational infrastructure resilience, reflects the growing dependence of banking services on information technology, cybersecurity, and the supplier network. The findings indicate that international documents regard operational risk management, digital resilience, and third-party management as inseparable components of a single system. Furthermore, the theme of readiness, response, and recovery emphasizes the importance of planning for crisis management and business continuity. This theme indicates that resilience is not limited to prevention alone; rather, the organization's ability to respond effectively and return swiftly to stable conditions is also among its main pillars. The fifth theme, monitoring, testing, and continuous learning, demonstrates the dynamic nature of operational resilience. Resilient banks continuously test their plans, monitor performance, and draw upon real-world experiences to refine processes. Finally, human capital and resilience culture is presented as the binding factor connecting all other dimensions. Without staff engagement, an appropriate organizational culture, and the development of specialized competencies, even the most advanced managerial and technological mechanisms will lack the necessary effectiveness.

3.6. Proposed Conceptual Model of the Research

The thematic analysis process demonstrated that the extracted overarching themes, although each elucidates a part of the concept of operational resilience, in practice operate as an integrated system interdependent upon one another. In other words, operational resilience is the outcome of simultaneously strengthening all identified dimensions, and weakness in any one of these dimensions can affect the effectiveness of the entire system.

Based on the research findings, the proposed operational resilience framework for systemically important banks comprises six main dimensions: strategic resilience governance, critical service management, operational infrastructure resilience, readiness and recovery, monitoring and continuous learning, and human capital and resilience culture. These dimensions, in continuous interaction with one another, enhance the organization's capacity to anticipate, withstand, respond to, sustain service delivery, and recover from operational disruptions.

Furthermore, the findings indicate that strategic governance plays the driving and guiding role for the entire system, while human capital and organizational culture provide the foundation for realizing the other dimensions. On the other hand, critical service management and operational infrastructure resilience constitute the executive core of the model, and their continuous improvement is ensured through ongoing monitoring, periodic testing, and the organizational learning cycle. The final conceptual model of the research is presented in Figure 3:



Figure 3. Research conceptual model: Overarching themes and structural relationships of bank operational resilience

The research findings demonstrated that the concept of operational resilience in international documents has moved away from a purely technological or crisis-management-based approach and has evolved into a comprehensive governance framework. In this framework, the primary objective is not the protection of systems but rather the preservation of continuity in the delivery of critical services under conditions of operational disruption. This conceptual transformation can be regarded as the most significant paradigm shift in banks' operational risk management over the past decade.

One of the most important findings of the research is the central role of strategic resilience governance across all documents examined. All six selected documents have placed the ultimate responsibility for designing, implementing, and overseeing the operational resilience system on the board of directors and senior management. This finding is consistent with the principles articulated in the Basel Committee document as well as the requirements of UK regulatory authorities, which regard operational resilience as part of the corporate governance system rather than merely a function of the IT department or risk management unit.

The second significant finding of the research is the shift in focus from processes to critical services. Unlike traditional risk management frameworks that predominantly focused on protecting assets, systems, or internal processes, the new documents emphasize identifying critical services, analyzing dependencies, and setting impact tolerances for each service. This attitudinal shift is particularly evident in the PRA/FCA documents and DORA, indicating that the criterion for a bank's success during a crisis is the continuity of service delivery to customers, not merely the recovery of technical infrastructures.

The analysis of documents also revealed that digital resilience has become one of the main pillars of operational resilience. The development of digital banking, the expansion of online services, and the increasing dependence on information technology have led to ICT risk management, cybersecurity, data management, and digital infrastructure resilience occupying a special position in all international frameworks. The adoption of DORA in the European Union further confirms this transformation and indicates that digital resilience is no longer a technical matter but is considered part of the strategic requirements of financial institutions.

On the other hand, the research findings indicate that third-party management and the service supply chain represent one of the most important emerging domains in operational resilience. Virtually all documents examined emphasize that banks must, in addition to managing internal risks, continuously assess and monitor their dependencies on technology service providers, outsourcing

companies, and other key partners. This finding is fully consistent with the requirements of Australia's CPS 230 Standard [21] and DORA regulations.

Furthermore, the present study demonstrated that operational resilience is not a static capability but rather a dynamic and learning process. Themes related to scenario-based testing, continuous monitoring, performance indicators, and learning from incidents indicate that resilient banks continuously test their plans, evaluate the results, and refine their processes and management mechanisms based on the experiences gained. This finding is consistent with the Dynamic Capabilities perspective and demonstrates that the organization's ability to learn and continuously adapt is one of the key factors in enhancing operational resilience.

Finally, the thematic analysis revealed that human capital and organizational culture play a fundamental role in the success of the operational resilience system. Although technology, infrastructure, and management processes are among the main pillars of resilience, without staff engagement, the development of a risk culture, continuous training, and organizational accountability, achieving sustainable resilience will not be possible. This issue has been particularly emphasized in the MAS [8] and FFIEC [9] guidelines.

In summary, the research findings indicate that international frameworks define operational resilience as an integrated management system formed through the interaction of governance, critical services, technology, human capital, risk management, continuous learning, and regulatory requirements. Accordingly, the framework proposed in this study can serve as a basis for designing a comprehensive operational resilience system in systemically important banks in Iran and can reduce the existing gap between international requirements and domestic implementation practices.

4. Conclusions

The present study, with the aim of designing a conceptual framework for enhancing the operational resilience of systemically important banks, employed a qualitative meta-synthesis method and thematic analysis, systematically analyzing six international reference documents including the Basel Committee (BCBS) Principles, the PRA/FCA framework, DORA regulations, the APRA CPS 230 Standard, MAS guidelines, and the FFIEC booklet. The research results demonstrated that, despite differences in the structure, scope, and implementation requirements of these documents, there is significant convergence regarding the fundamental components of operational resilience.

The data analysis led to the extraction of 136 open codes, 12 axial categories, and 6 overarching themes. These themes include strategic resilience governance, critical service management, operational infrastructure resilience, readiness and recovery, monitoring and continuous learning, and human capital and resilience culture, which, in interaction with one another, constitute the proposed conceptual framework of the research.

The research findings indicate that operational resilience in modern approaches does not merely mean crisis management or business continuity; rather, it is a strategic organizational capability that must be institutionalized at all levels of governance, processes, technology, human resources, and stakeholder relations. From this perspective, a bank's success during a crisis is evaluated not by the speed of recovering technology systems but by the ability to maintain critical services for customers and stakeholders.

Furthermore, the results demonstrated that international documents increasingly emphasize a service-oriented approach, digital resilience, third-party management, and the continuous learning cycle topics that have received less attention in many traditional risk management frameworks. This transformation reflects a paradigm shift in global banking regulation and a move from a reactive approach toward proactive management based on dynamic capabilities.

The findings of this study can serve as a basis for formulating policies and executive plans for establishing an operational resilience system in systemically important banks in Iran. Accordingly, it is recommended that senior bank managers regard operational resilience not as one of the functions of the risk management or IT unit but as one of the pillars of corporate governance and strategic management.

At the executive level, establishing a critical service identification system, setting impact tolerances, developing scenario-based testing, strengthening third-party risk management, and designing management dashboards for continuous monitoring of resilience status can constitute a significant step in increasing banks' preparedness against operational disruptions, cyberattacks, and widespread crises.

From a policy-making perspective, the results of this study can be utilized in formulating national guidelines by the Central Bank of the Islamic Republic of Iran, updating supervisory frameworks, and designing operational resilience requirements appropriate to the country's banking conditions. Furthermore, the proposed framework is capable of being adapted to the risk management system, corporate governance, and digital transformation requirements in the banking network.

Based on the research findings, a set of practical recommendations for enhancing the operational resilience of financial institutions is presented. These recommendations have been extracted from the comparative analysis of international frameworks and can be utilized in formulating policies, designing management systems, and developing regulatory requirements.

First, it is recommended that financial supervisory authorities develop a national framework for operational resilience that, while drawing on international experiences, is compatible with the structural characteristics of the country's financial system. This framework should clearly specify the responsibilities of the board of directors, critical service identification requirements, impact tolerances, third-party management, resilience testing, and reporting mechanisms.

Second, financial institutions need to systematically identify and prioritize their critical services. Resource allocation, business continuity planning, and crisis management should be based on the importance of these services so that, under disruption conditions, the highest level of service continuity is maintained.

Third, managing internal and external dependencies must become one of the main axes of the operational resilience system. Dependencies on technology service providers, data centers, information processing companies, and other essential suppliers must be continuously assessed, and alternative and recovery plans must be designed for each dependency.

Fourth, the regular implementation of scenario-based testing and crisis simulation should be considered part of the annual programme of financial institutions. These tests can assess the organization's preparedness against cyber disruptions, infrastructure outages, critical system failures, and other operational hazards, revealing existing weaknesses.

Fifth, it is recommended that operational resilience performance assessment systems be developed based on quantitative and qualitative indicators. The use of indicators such as service recovery time, the degree of impact tolerance achievement, the number of critical incidents, resilience test results, and the level of preparedness of organizational units can enable continuous performance assessment.

Finally, creating an organizational culture based on learning, experience sharing, and continuous improvement must be regarded as one of the fundamental requirements of operational resilience. Drawing on the experiences of past incidents, documenting lessons learned, and transferring knowledge among organizational units will significantly enhance the organization's capacity to face future crises.

Author Contributions

All authors contributed equally to the conception, preparation, and writing of this manuscript.

Conflict of Interest

The authors, while observing publication ethics in the referencing, declare the absence of interest of conflict.

Acknowledgement

All authors gratefully acknowledge support from Petroleum University of Technology (PUT).

AI Used Statment

The author retain full responsibility for the accuracy, originality, integrity, legality, and ethical compliance of all text, data, tables, figures, analyses, references, and conclusions, and have verified all AI-assisted outputs. Any fabrication, falsification, manipulation, plagiarism, copyright infringement, or other misuse of AI remains solely the responsibility of the authors and does not transfer or diminish their accountability for the published work.

References

[1] M. H. Uddin, S. Mollah, N. Islam, M. H. Ali, *Technological Forecasting and Social Change*, 2023, **197**, 122919120–131. https://doi.org/10.1016/j.techfore.2023.122919

[2] I. Gorobeț, Convergence of Banking Cybersecurity Strategies to the New Rules on Digital Operational Resilience. In: *Proceedings of the International Conference "Economic Security in the Context of Systemic Transformations"*. Chișinău: SEP ASEM, 2024, pp. 54-62. https://doi.org/10.53486/escst2023.06

[3] Basel Committee on Banking Supervision, *Principles for Operational Resilience*, Basel: Bank for International Settlements, 2021.

[4] European Parliament, Council of the European Union, *Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA)*, Official Journal of the European Union, 2022. http://data.europa.eu/eli/reg/2022/2554/oj

[5] M. Grimwade, *Journal of Risk Management in Financial Institutions*, 2023, **17(1)**, 71-88. https://doi.org/10.69554/FFSP1788

[6] S. Kohli, *Journal of International Crisis and Risk Communication Research*, 2025, **8(9)**, 163-171. https://doi.org/10.63278/jicrcr.vi.3254
[7] Prudential Regulation Authority, *Operational Resilience: Impact Tolerances for Important Business Services*, Supervisory Statement SS1/21, London: Bank of England, 2021.
[8] H. Mofid, M. R. Khosravi-Nikou, S. A. Razavi, M. Mohammadian, *Applied Thermal Engineering*, 2024, **245**, 122810. https://doi.org/10.1016/j.applthermaleng.2024.122810
[9] Monetary Authority of Singapore, *Guidelines on Business Continuity Management*, Singapore: Monetary Authority of Singapore, 2022.
[10] Federal Financial Institutions Examination Council, *Business Continuity Management Booklet*, FFIEC Information Technology Examination Handbook, 2019.
[11] S. A. Razavi, E. Ordoei, *Journal of Environmental Economics and Chemical Processes*, 2025, **2(4)**, 129-133. https://doi.org/10.22034/jeecp.2025.735022
[12] S. A. Razavi, A. Tarnian, *Journal of Environmental Economics and Chemical Processes*, 2026, **3(1)**, 29-33. https://doi.org/10.22034/jeecp.2024.735000
[13] R. D. Chanon, L. Habahbeh, P. J. M. Klumpes, S. Mann, *British Actuarial Journal*, 2025, 30, 125. https://doi.org/10.1017/S1357321725100202
[14] A. Tuominen, Operational Resilience in the Digital Age, *The Supervision Blog*, ECB Banking Supervision, 17 January 2025. https://www.bankingsupervision.europa.eu/press/blog/2025/html/ssm.blog20250117~32b79d4efa.en.html
[15] O. Kamel, M. M. Ibrahim, M. Moustafa, D. Edgar, *Journal of Modern Business and Technology*, 2025, **1(1)**, 1-15.
[16] A. R. Ningrum, *Maliki Interdisciplinary Journal*, 2026, **4(6)**, 160-169.
[17] A. Tuominen, Upgrading Banks' Capacity to Deal with Digital Risks, *Contribution for Eurofi Magazine*, ECB Banking Supervision, 24 March 2026. https://www.bankingsupervision.europa.eu/press/interviews/date/2026/html/ssm.in260324_5~3d0837ff0e.en.html.
[18] C. Thomas, Building Operational Resilience: A Framework, *360factors*, 26 June 2026. https://www.360factors.com/blog/operational-resilience/.
[19] A. Raufuss, D. Williams, T. Poppensieker, Operational Resilience Has Become Critical. How Are Banks Responding?, *McKinsey & Company*, 21 October 2025. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/operational-resilience-has-become-critical-how-are-banks-responding
[20] M. Sandelowski, J. Barroso, *Handbook for Synthesizing Qualitative Research*, New York: Springer Publishing Company, 2007.
[21] S. A. Razavi, A. K. Manshad, L. Kashani, Energy Strategy Reviews, 2026, 65, 102226. https://doi.org/10.1016/j.esr.2026.102226
[22] D. Walsh, S. Downe, *Journal of Advanced Nursing*, 2005, **50(2)**, 204-211. https://doi.org/10.1111/j.1365-2648.2005.03380.x
[23] A. Strauss, J. Corbin, Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. 2nd ed. Thousand Oaks, CA: Sage Publications, 1998.
[24] Australian Prudential Regulation Authority, *Prudential Standard CPS 230: Operational Risk Management*, Sydney: Australian Prudential Regulation Authority, 2023.