International Journal of Business and Quality Research

https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

Banking Operational Resilience in the Digital Payment Ecosystem: A Qualitative Descriptive Study of Transaction Risk Management

Mochamad Choliq[1] *

[1]Institutional Business Group, PT. Bank Rakyat Indonesia (Persero) Tbk.

*Corresponding author: choliqadi@gmail.com

Abstract

Digital transformation has reshaped banking services by creating an increasingly integrated payment ecosystem involving banks, institutional customers, digital platforms, and third-party service providers. This study aims to analyze banking operational resilience in managing transaction risks within digital payment ecosystems, particularly transaction-status inconsistencies, timeouts, reconciliation, third-party risks, and institutional trust. A qualitative descriptive approach was employed to provide an in-depth understanding of operational processes and the experiences of parties involved in digital payment transactions. Data were collected through semi-structured interviews and documentation and analyzed thematically through coding, categorization, theme identification, and interpretation. The findings indicate that operational risk does not arise solely from total system failure but may emerge at points of interaction between interconnected systems when transaction status differs from actual financial finality. Reconciliation therefore serves as an early-warning mechanism for detecting exceptions before they develop into material financial exposures. Operational resilience is further strengthened through transaction monitoring, clear escalation procedures, effective third-party risk management, cross-party coordination, and transparent communication. The study concludes that mature digital banking transformation requires more than technological reliability; it requires an integrated capacity to detect disruptions, resolve anomalies, recover services, learn from incidents, and preserve institutional trust across the digital payment ecosystem effectively and sustainably.

Keywords: Digital Banking, Operational Resilience, Operational Risk, Digital Payment, Third-Party Risk, Institutional Trust.

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

INTRODUCTION

Digital transformation has transformed banking business processes from services that previously relied heavily on physical interaction to technology-based services that can be accessed quickly and almost without borders. Transactions that used to require several administrative stages can now be completed in seconds through various digital channels. These changes provide benefits for banks and customers because they increase the speed, convenience, and efficiency of services. However, the more digital a process is, the higher the organization's dependence on systems, data, connectivity, and the parties that support the implementation of these services. This condition is emphasized in the initial manuscript that digitalization basically does not eliminate operational risks, but changes the form and character of the risk. Research on banking digital transformation also shows that digitalization can increase exposure to operational risks through increased business volume, system failures, internal process problems, and internal and external disruptions (Uddin et al., 2023).

These risks become increasingly complex as digital payment services evolve into an ecosystem involving various organizations and technology systems. A series of transactions can involve users, banks, payment receiving institutions, platform providers, and digital payment channels. Each party may have adequate technology infrastructure and control mechanisms, but the success of the service is ultimately determined by the ability of the entire system to work consistently as a whole. Digitalization and increasing interconnection in the financial sector also increase dependence on third parties, so disruptions to one component can affect the provision of financial services more broadly. Therefore, operational risks in digital services need to be seen not only from the resilience of each system, but also from the relationships and dependencies that form between systems.

This phenomenon can be seen in the case of digital payments which is the empirical basis of this study. Payment of Education Development Contributions (SPP) at a higher education institution involves the institution as the recipient of the payment, the bank as the source of funds, the provider of the transaction management platform, and the payment channel used by the user. Under normal conditions, the user makes a payment, the account is debited, the transaction status is forwarded to the platform, then the institution receives information that the obligation has been paid. The problem arises when the transaction volume increases and there is a timeout in one part of the process series. This condition is important to study because research on third-party payment platforms shows that the development of digital payments carries its own characteristics of operational risks that require systematic management (Yao & Li, 2022).

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

In some transactions in this phenomenon, the debit process at the source of funds has not been completed, while the status on other systems has shown that the transaction was successful. Success information is then forwarded to the institution so that from the perspective of the transaction user the transaction has been completed and from the perspective of the institution the obligation has been paid. However, in terms of fund flow, the process is not completely final. This difference in status shows that digital operational risks are not always in the form of system down or overall technology failure. Risks can actually arise when several systems continue to work, but the information generated is no longer in sync.

These problems are increasingly important when transactions take place in large volumes and close to each other. Exceptions that only occur in one or two transactions may be resolved as routine operational problems, but the accumulation of problematic transactions can develop into material financial exposure. The impact is no longer limited to technology, but can touch the accuracy of reporting, financial responsibility, the quality of partner management, and institutional trust in the entire service ecosystem. This shows that the ability to manage digital risk is closely related to the concept of operational resilience. In an increasingly digitized and connected financial system, operational resilience is becoming increasingly important because payment service disruptions can affect customer activities and to a certain extent even trust in the financial system.

Operational resilience in this context is not enough to build by ensuring that the bank's internal systems can work normally. Banks also need to understand how their systems interact with other parties' systems, how transaction definitions are successfully determined, how timeouts are handled, and who is responsible when there is a discrepancy between the status of the system and the financial condition of the transaction. The initial literature shows that questions about the definition of successful transactions, the deadline for pending transactions, the delivery of information, and decision-making when the financial reality differs from the information received by the institution are important issues in the digital payments ecosystem. Reliance on third-party providers has even become a concern in the risk management of financial institutions because disruptions to critical services provided by third parties can affect the operational resilience of financial institutions.

In this context, reconciliation has a broader strategic function than just administrative activities after a transaction is completed. Reconciliation can serve as an early warning mechanism to find discrepancies between transaction data on one system and another. The sooner these discrepancies are discovered, the less likely exceptions are to develop into material financial exposures. The initial manuscript therefore emphasizes the

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

need for high-risk processes supported by faster reconciliation and exception monitoring that is able to detect abnormal patterns early on. In the framework of operational resilience, the ability to detect and respond to such disruptions is important because resilience is not only determined by the ability to prevent disruptions, but also by the organization's ability to maintain and restore critical services when disruptions occur.

Based on these conditions, research on banking operational resilience in the digital payments ecosystem is important to gain a deeper understanding of how transaction risks arise and are managed at the point of interaction between systems. The research is not only directed at the technological dimension, but also at the aspects of reconciliation, exception management, coordination between parties, third-party risk management, and communication in maintaining institutional trust. This perspective is important because in the initial manuscript it is explained that the ability to mediate, communicate, and maintain trust is as important as technical ability when dealing with transaction disruptions. The qualitative descriptive approach was chosen because it allows the research to obtain a close picture of the experiences and perspectives of the parties involved without having to be directed to build new theories. On that basis, this research is directed to analyze the operational resilience of banks in the digital payments ecosystem through transaction risk management, by placing operational experience as a basis for understanding the relationship between technology, processes, people, third parties, and institutional trust.

THEORETICAL REVIEW

Banking Digital Transformation

Digital transformation of banking is a process of comprehensive changes to business models, operational processes, interaction patterns with customers, and the provision of products and services by utilizing digital technology. This transformation is not limited to moving conventional services to electronic channels, but also includes the integration of technology into various parts of the banking value chain. The Basel Committee on Banking Supervision explained that the digitalization of the financial sector is developing through the use of various technologies, such as application programming interfaces (APIs), artificial intelligence and machine learning, distributed ledger technology, and cloud computing (BCBS, 2024). These developments have also encouraged the emergence of various technology-based service providers, including fintech companies, big tech, and third-party service providers who are increasingly involved in the provision of banking services.

For the banking industry, digital transformation provides opportunities to improve process efficiency, expand service access, accelerate transaction completion, and create a simpler and more integrated customer experience. The use of technology such as process

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

automation, big data, artificial intelligence, and cloud-based systems allows a number of activities that were previously carried out manually to be carried out more quickly, accurately, and consistently (Alam et al., 2025). The findings of Ayadi et al. (2025) also show that digitalization contributes to improving banking efficiency, although the magnitude of the benefits may vary based on the characteristics and business model of the bank. In the Indonesian context, Akbary et al. (2025) found that the relationship between digital transformation and banking efficiency is more complex and can differ based on the size of the bank, so digitalization does not automatically produce the same level of efficiency in each institution. From the customer's perspective, this transformation also needs to be followed by improving the quality of the user experience because customer experience is an important part of the acceptance of digital banking services (Wulandari et al., 2024).

This condition is in line with the phenomenon that shows that digital transactions allow users to make payments, sources of funds are processed, transaction status is forwarded through the platform, and institutions obtain electronic confirmations. BCBS (2024) emphasizes that digitalization does provide benefits for banks and customers, but these developments also bring new vulnerabilities and can magnify the risks that banks previously had.

Digital transformation thus has two sides that need to be managed in a balanced manner. On the one hand, the use of technology can increase operational efficiency and support risk management, but on the other hand, digitalization increases dependence on technology and expands the space for operational disruptions. Uddin et al. (2023), based on research on 264 banks in 43 countries, found that the digitalization of banking operations is one of the underlying factors that underlie increased exposure to operational risks along with increasing business volume. These risks include system failures, problems in internal processes, and disruptions originating from the internal and external environment. These findings show that improving technological capabilities should ideally be followed by increasing banks' capacity to identify, monitor, and control risks arising from digitalization.

In the context of this study, digital transformation is understood as a change that causes banking services to increasingly depend on the interconnectedness of various systems and parties in one ecosystem. This dependency makes the quality of services no longer only determined by the reliability of the bank's internal systems, but also by the ability of all connected systems to produce consistent processes and information. A transaction can involve institutions, banks, platform providers, and digital payment channels, so that disruptions at one point can affect the entire transaction process. Therefore, digital transformation in this study is the main context to understand why risk management

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

and operational resilience need to move from an approach oriented to an approach that looks at the interconnectedness of the entire ecosystem.

Banking Operational Risks

Operational risk is one of the main risks inherent in banking activities, including in the provision of technology-based services. Conceptually, operational risk is related to potential losses caused by the inadequacy or failure of internal processes, humans, systems, and external events. Yao and Li (2022) use this framework in analyzing operational risks on third-party payment platforms and show that risks can come from a variety of factors, ranging from human error and technological weaknesses to external attacks and non-compliance with regulations. Thus, operational risk should not be understood only as technological failures, but as risks formed through interactions between people, processes, technology, and the external environment.

The development of digital services has caused the character of operational risks to become increasingly dynamic as technology has become an integral part of almost all stages of transactions. Uddin et al. (2023) explained that technological innovations can increase operational risk exposure because technology allows for increased business volume, while system failures, internal process disruptions, and security threats remain inherent in technology-based activities. BCBS (2024) also shows that digitalization can expand the factors that test operational risks and bank resilience, especially due to the increasing interconnection and use of new technologies. Therefore, the greater the bank's reliance on digital processes, the more important the organization's ability to understand not only the possibility of technological failure, but also the business consequences of such failures.

Operational risks in the digital payments ecosystem can also appear in a form that is relatively invisible to users. A condition when the debit process at the source of funds has not been completed, but the transaction status on another system has shown that the payment was successful and the information is passed on to the institution. As a result, users and institutions view the transaction as complete, while the actual flow of funds is not final. This condition shows that operational risks are not always marked by a complete cessation of services, but can also arise as a missynchronization of status and information between systems that if not immediately known can develop into financial exposure.

Based on this perspective, operational risk management in digital payments needs to pay attention to the entire transaction cycle, from payment initiation to debit, confirmation, reconciliation, and settlement. Yao and Li (2022) show that the occurrence of operational risks on third-party payment platforms can result in significant losses, so the identification of risk causes and characteristics is an important part of its control. In this study, special

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

attention is paid to timeouts, suspended transactions, differences in status between systems, reconciliation delays, and differences between transaction success status and financial finality. Thus, operational risk is a concept used to understand what can experience failures in a digital transaction, how these failures develop, and the consequences they have on banks and service user institutions.

Operational Resilience

Operational resilience is an organization's ability to maintain the delivery of critical functions or services in the face of operational disruptions as well as effectively restore services after an outage occurs. This concept differs from a risk management approach that is solely prevention-oriented, as operational resilience also recognizes that not all disruptions can be eliminated. Digitalization makes the concept even more important because financial services depend on the technology and software infrastructure that supports the critical functions of financial institutions. The Financial Stability Board affirms the importance of continuity of services and critical functions supported by shared services such as information technology infrastructure and software services (FSB, 2023). Therefore, operational resilience places an organization's ability to deal with disruption as an integral part of risk management.

Operational resilience is also related to the organization's ability to anticipate how disruptions to one part of the system may affect the service as a whole. Digitalization increases interconnection between banks, technology providers, payment platforms, and other parties so that failure does not always stop at the organization where the disruption first occurs. BCBS (2024) reminds that digitalization can create new vulnerabilities and magnify existing risks, including strategic, reputational, and operational risks affected by increased interconnection. Operational resilience thus requires a broader perspective than simply maintaining the availability of the bank's internal systems. The organization's ability to coordinate with various parties in the ecosystem becomes just as important as the technical capabilities of the system.

In digital payment practices, one of the key elements that supports operational resilience is the organization's ability to detect transaction anomalies quickly and accurately. Reconciliation is no longer solely positioned as a back-office activity that is carried out after a transaction is completed, but has evolved into a control mechanism that allows discrepancies between transaction records, authorizations, and settlements to be identified as early as possible. Shanmugam (2025) explains that the implementation of real-time reconciliation allows payment verification to be carried out on an ongoing basis so that non-conformities, such as unrecorded transactions, duplicate transactions, and settlement

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

failures, can be identified immediately before they develop into greater operational risks. These findings are reinforced by Desai et al. (2024), who show that real-time transaction monitoring can be used to detect anomalous transactions that if not immediately detected can have serious implications for the payment system and its participants. Thus, the integration of transaction monitoring, anomaly detection, and reconciliation that is increasingly closer to real-time can be understood as an early warning mechanism that supports banks' ability to identify and control risks in a timely manner and strengthen operational resilience (BCBS, 2024).

In this study, operational resilience is placed as a central concept to analyze banks' ability to deal with transaction risks in the digital payments ecosystem. This resilience can be observed through the ability of banks and related parties to conduct transaction monitoring, detect exceptions, conduct reconciliation, implement escalation mechanisms, coordinate settlements, and conduct evaluations so that similar disruptions do not recur. FSB (2023) shows that digitalization has increased financial institutions' dependence on third-party services that support critical functions, so that the management of these dependencies becomes relevant for operational continuity. Thus, operational resilience in this study is not seen simply as the ability of technology to continue working, but as the capacity of organizations and ecosystems to continue to provide reliable services when facing conditions that do not run as planned.

Third-Party Risk Management

The development of the digital banking ecosystem has made banks increasingly dependent on third parties to support various technological functions and services. Platform providers, cloud service providers, fintech companies, software providers, and other technology partners can help banks gain specialized expertise, improve efficiency, expand service scale, and accelerate innovation. However, this dependence also causes some processes that affect service quality to not be completely under the direct control of banks. BIS (2026) explains that the use of third-party service providers can provide benefits in the form of expertise, efficiency, scalability, and increased operational resilience, but at the same time can reduce banks' direct control over operations and assets, including data. Therefore, relationships with third parties must be understood as part of the bank's risk ecosystem.

Third-party risk is becoming increasingly important because disruptions to service providers can affect functions that are critical to the continuity of bank operations. These risks can be in the form of disruptions to critical services, disruptions to service providers' supply chains (nth-party risk), or concentration risks when many critical activities depend on one or a small number of providers. BCBS in 2024 highlights that digitalization has

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

increased banks' reliance on third parties beyond traditional outsourcing patterns, while increasingly widespread supply chains and concentration risks require a stronger management framework. These developments show that it is not enough for banks to simply assess vendors before contracts are signed. Risk management must take place throughout the lifecycle of the relationship with service providers.

Third-party management in digital transactions needs to pay attention to how partners handle exceptions, execute escalation procedures, store and provide transaction data, and communicate information when anomalies occur. Clarity of financial and operational responsibilities is essential from the outset because a mature contract not only regulates how the parties work when the process is running normally, but also determines actions when something does not go as planned. This shows that the quality of third-party risk management has a direct relationship with the ecosystem's ability to resolve transaction disruptions.

The quality of third-party risk management is closely related to the ability of the banking ecosystem to respond to and resolve transaction disruptions, especially when critical services depend on external technology providers. This dependence causes disruptions that occur to third parties can affect the continuity of payment services and transaction settlement at financial institutions that use their services. Adeney et al. (2024) show that disruptions to material services provided by third parties can affect the ability of the financial system to provide vital services, including payment and settlement services. In line with that, Wittlin et al. (2026) emphasize the importance of third-party risk management and adequate responsibility sharing between financial institutions and technology providers in strengthening operational resilience.

Thus, third-party risk management in this study is not limited to vendor selection and evaluation, but includes relationship governance, division of responsibilities, SLAs, performance monitoring, exception handling, escalation mechanisms, service continuity, and readiness to face disruptions. BIS (2026) emphasizes the need for banks to have adequate risk management in relationships with third-party providers in order to be able to survive, adapt, and recover from operational disruptions. This means that handing over a function to a third party does not eliminate the bank's interest in ensuring that the risks from these functions are managed effectively. In the digital payments ecosystem, third-party risk management is ultimately one of the foundations to ensure that all parties can work as a consistent and resilient set of services.

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

Institutional Trust

Trust is one of the main foundations in the relationship between banks and customers and institutions that use services. In the digital environment, trust is not only formed through the security of funds, but also through the perception that the system is able to produce accurate transactions, be available when needed, and provide clear solutions when problems occur. Digitalization makes the user experience look simpler, but that simplicity actually depends on the orchestration of various systems and organizations behind the scenes (Desiraju et al., 2024). Users generally do not see APIs, switching, settlement, reconciliation, or SLAs between parties; users pay more attention to whether the promised service is actually running. Therefore, the ability to maintain service reliability is one of the cornerstones of building trust in digital banking.

Trust becomes even more important when there is a transaction disruption because it is at that time that the quality of the relationship between the bank and the institution is truly tested. Operational disruptions can produce impacts that go beyond the value of the transaction, especially if the institution has made a decision based on information that the payment has been successful. A single transaction anomaly that is not managed properly can give rise to financial risks, decreased trust, and disruption to institutional relationships that have been built in the long term. Reputational risks are also a concern in banking digitalization because BCBS (2024) assesses that new technologies and increased interconnections can magnify existing risks, including reputational risks. Thus, operational risk management has a relational dimension that cannot be separated from the technical dimension.

The maintenance of institutional trust is mainly determined by how the bank responds when an outage occurs. Institutions not only assess how long the system has been disrupted, but also pay attention to the openness of communication, speed of identification of root problems, clarity of responsibility, and the ability of all parties to find a proportionate solution. This is reflected in its implementation, which places the ability to mediate, communicate, and maintain trust as equally important as technical capacity in resolving transaction anomalies. Therefore, relationship management can be understood as one of the human dimensions of operational resilience because the organization's response to disruption also determines whether business relationships can be maintained after an incident occurs.

Ali (2024) shows that service recovery strategies in the form of explanations, apologies, and empathy have a positive effect on the quality of relationships between banks and customers after service failures. These findings are reinforced by Munawar and Hadianto (2024), who show that banking service recovery is related to customer satisfaction

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

and loyalty. From an operational resilience perspective, a customer-oriented approach also emphasizes the importance of transparency, clear communication, and the ability to maintain trust during operational disruptions. Thus, an organization's response to incidents not only serves to restore processes or services technically, but also becomes an important part of maintaining trust and the sustainability of business relationships after an outage occurs.

In this study, institutional trust is positioned as an important consequence of the quality of risk management and the resilience of banking operations. Banks that are able to detect problems early, provide information transparently, coordinate with partners, resolve transactions responsibly, and make repairs after incidents have a stronger basis for maintaining institutional trust. Conversely, lack of clarity of information, slow escalation, or inability to explain the financial status of a transaction can turn technical glitches into reputational and business relationship issues. This is in line with the argument that in the digital ecosystem it is not only the value of the transaction that is at stake, but the bank's reputation as a partner and the institution's belief that the bank is able to be present when conditions are not normal. Thus, institutional trust can be understood as the result of the interaction between technological reliability, process effectiveness, risk management quality, inter-stakeholder coordination, and the quality of human communication.

METHOD

This study uses a qualitative approach with a qualitative descriptive design to gain a deep understanding of the resilience of banking operations in managing transaction risk in the digital payments ecosystem. The qualitative descriptive design was chosen because the research is directed to comprehensively describe phenomena based on the experiences and perspectives of the parties involved, without testing the relationships between variables statistically or building new theories. Villamin et al. (2025) explained that qualitative descriptive design allows researchers to stay close to data (data-near) so that experiences, events, and phenomena can be understood directly based on the perspective of participants; this design also provides flexibility in the use of semi-structured interviews and thematic analysis. In this study, informants were selected purposively based on their knowledge and involvement in the digital payment process, such as institutional banking/relationship management practitioners, transaction operational units, information technology or digital banking, risk management, and other parties involved in the payment ecosystem. Data collection is carried out through semi-structured interviews and documentation, mainly to explore experiences regarding timeouts, missynchronization of transaction status, transaction finality, reconciliation, escalation mechanisms, third-party management, and

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

efforts to maintain institutional trust; The use of semi-structured interviews is relevant because it allows informants to explain their perspectives and experiences in a more in-depth and flexible manner.

The data obtained are then analyzed thematically through the process of organizing data, reading and understanding the transcript thoroughly, coding, grouping codes into categories, identifying themes, and interpreting inter-theme relationships according to the focus of the research. The analysis is directed to find patterns regarding sources of operational risk, transaction insynchronization, exception monitoring, reconciliation, coordination between parties, third-party risk management, operational resilience, and institutional trust. Thematic analysis is a widely used approach in qualitative research because it allows researchers to identify and interpret meaningful patterns contained in the data, although the analysis procedure needs to be systematically explained in order to maintain methodological transparency (DeJonckheere et al., 2024). The validity of research findings is maintained through source triangulation and triangulation techniques, by comparing information between informants and checking it against available documents and transaction process information; Strategies such as triangulation, audit trail, researcher reflexivity, and adequate evidence presentation can improve the credibility, dependability, confirmability, and transferability of qualitative descriptive research findings. With these procedures, the research is expected to be able to produce a complete and contextual picture of how banks and parties in the digital payments ecosystem identify, respond, and resolve transaction risks to build operational resilience.

RESULTS AND DISCUSSION

Ekosistem dan Alur Transaksi Pembayaran Digital

The results of the study of the digital payment process show that the implementation of banking transactions has developed into an ecosystem involving a number of parties with different functions and systems. In the case that was the focus of the study, the payment process for Education Development Contributions (SPP) involves university institutions as payment recipients, banks as fund source providers, platform providers as transaction system managers, and digital payment channels used by users. Under normal conditions, users make payments, source funds accounts are debited, transaction status is forwarded to the platform, and then institutions receive information that user obligations have been paid. This mechanism shows that the success of a transaction no longer depends on one system, but on the ability of several systems to work integrated. Thus, the more parties involved in the transaction chain, the more important is the alignment of processes and information among all parties.

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

This connectivity provides benefits in the form of speed and efficiency, but at the same time creates greater operational dependency. Each party may have adequate technology individually, but the success of services to users is determined by the ability of the entire system to work as a network. This condition is in line with the principle of operational resilience that places interconnection and dependency mapping as an important part of the management of digital financial services. The literature on operational resilience in payment systems also shows that the more digitalized, integrated, and interdependent the payment infrastructure, the higher the need for operational resilience (Khiaonarong et al., 2021). Therefore, banks need to have an end-to-end understanding of transaction flows and not just focus on the processes that take place in their internal systems.

From the perspective of this study, the transaction flow can be mapped into transaction initiation → processing of funds → debit sources → sending status → confirmation to institutions → reconciliation → settlement. Each point in the series can become a risk point when the information received by one system is different from the transaction conditions in other systems. End-to-end process mapping is important to identify the systems, people, processes, information, and third parties that support the provision of services. Current regulatory practices also emphasize the importance of mapping the resources and third-party dependencies required to provide essential payment services (Bank of England, 2023). Thus, transaction ecosystem mapping can be positioned as the first foundation in building the operational resilience of digital payments.

Transaction Status Misalignment as an Operational Risk

An important finding from the analyzed case is the emergence of risks due to the asynchronization of transaction status between systems. The problem occurs when the transaction volume increases and in some transactions the source of the debit process has not been completed, while other systems have received information that the transaction was successful. The status is then forwarded to the institution as a successful payment so that from the perspective of the transaction user the transaction has been completed and from the perspective of the institution the obligation has been paid. However, from the perspective of the flow of funds, the transaction is actually not completely final. This phenomenon shows that digital operational risks can occur even if there is no overall system failure.

These findings expand the way to understand operational risks in digital transactions. Risks do not only occur when a system goes down, a cyberattack, or a device failure, but can arise when multiple systems remain operational but produce inconsistent information. In such a situation, the problem lies at the inter-system meeting point, not just

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

in one specific application. Once the transaction flow is traced, the fundamental problem is not only the timeout, but how the status of the exception is communicated, how quickly the information is forwarded, and whether all parties have a common understanding of when the transaction is actually completed. This shows the importance of risk management that does not stop at the technical aspect, but also includes communication and governance procedures between parties.

The impact of this asynchronization becomes more serious when it occurs in large transaction volumes. A single transaction that experiences an exception may only cause administrative problems that are relatively easy to resolve, but hundreds or thousands of transactions under the same conditions can accumulate into material financial exposure. The research document shows that at this stage digital issues are no longer just a technological problem, but have turned into business problems related to financial responsibility, reporting accuracy, partner management, and institutional trust. Therefore, risk control needs to be designed not only to prevent systems from stopping working, but also to detect differences in transaction status between systems as early as possible.

Transaction Finality as a Benchmark for Digital Transaction Success

The results of the analysis further show that one of the fundamental problems in the digital payments ecosystem is the possibility of differences in the definition of transactions that are declared "successful". For one system, a transaction may be considered successful when an instruction has been received, while another system may consider the transaction successful after a certain process has been completed. From a bank's perspective, a transaction is not necessarily final if the source of funds has not been debited and the settlement process has not been fulfilled. This difference can create a situation where a digital transaction is declared successful, but financially the funds have not actually moved.

These findings show the need to distinguish between transaction status and financial finality. Transaction status is information generated by the system at a stage of the process, while financial finality is related to the actual settlement of payment obligations. When these two aspects do not run in sync, users can obtain information that does not reflect the actual condition of the transaction. The consequences are greater if the institution has made a decision based on the payment status, for example considering the user's obligations to have been paid off. Therefore, the definition of transaction success needs to be explicitly agreed upon by all parties in the ecosystem.

The results also show that digital payment designs should not only be speed-oriented, but need to pay equal attention to transaction certainty. The "successful" information provided to the user essentially creates business expectations and consequences. When

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

proof of success has been provided, the user assumes his or her obligations are completed and the institution can make a decision based on the information. Thus, one of the important dimensions of operational resilience is the ability to ensure that the transaction status displayed to the user has a clear link to the actual financial condition of the transaction.

Reconciliation as an Early Warning System

The results of the analysis show that reconciliation has a strategic position in digital payment risk management. In traditional practice, reconciliation is often seen as a back-office activity that is carried out after a transaction is completed to match transaction records from various sources. However, in a digital ecosystem with high transaction volumes, this function needs to evolve into an early detection mechanism for transaction anomalies. The research paper confirms that the sooner transaction differences are discovered, the less chance of exceptions developing into material exposures. Thus, reconciliation is part of a risk control system and not just an administrative procedure.

Conceptually, the process can be explained through a series of monitoring → detection → reconciliation → escalation → resolution. Monitoring functions to monitor transaction patterns, while detection identifies transactions that deviate from normal conditions. Reconciliation is then used to determine the location of data differences, followed by escalation to parties who have the authority to resolve the problem. After settlement is carried out, the results of the incident should be evaluated to improve control and prevent similar incidents. The operational resilience framework also places monitoring, reporting, incident management, and learning from previous incidents as important elements in maintaining critical services (Khiaonarong et al., 2021).

By implication, transaction processes that have high volume and risk levels require reconciliation that is closer to real-time or at least carried out in intervals that limit the accumulation of risk. Exception monitoring also needs to be designed to not just find individual differences, but to recognize abnormal patterns that occur repeatedly. This is in line with the idea that the goal of reconciliation is not simply to find differences, but to prevent anomalies from developing into financial losses. In this context, the speed of finding problems becomes just as important as the speed of processing transactions.

Managing Third-Party Risk in the Payment Ecosystem

The results of the study also show that digitalization has expanded the limits of banks' operational risks as the provision of services increasingly relies on third parties. Platform providers, payment channels, technology infrastructure providers, and other partners are part of the process that determines the success of transactions. The use of third parties does

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

allow banks to gain specialization, efficiency, scalability, and innovation. However, this dependence can also reduce the bank's direct control over certain processes and assets and introduce new risks or magnify existing ones. The Basel Committee places critical service risk, supply-chain risk, and concentration risk as an important part of the risk of relationships with third-party providers (BIS, 2026).

In the context of the case analyzed, it is not enough to manage third parties only through vendor selection and periodic evaluations. Banks need to know how partners handle exceptions, how escalation mechanisms are implemented, how transaction data is stored and traced, and how quickly information is provided when anomalies occur. The division of financial and operational responsibilities must also be clearly defined before services are executed. A mature contract not only explains how the parties work when everything is going normally, but also specifies actions when things don't go as planned.

These findings are consistent with recent developments in banking risk governance. The Basel Committee Principles of 2025 shift the traditional perspective of outsourcing towards broader third-party relationship management due to banks' increasing reliance on external service providers (BIS, 2025). In fact, recent studies show that digital trust is related to the assessment of various categories of third-party risk, with a strong influence on concentration risk and contingency planning, among others (Saveljeva & Volkova, 2026). Therefore, the operational resilience of banks is ultimately inseparable from the resilience of all partners who support its critical services.

Anomaly Management as Part of Relationship Management

The findings are quite typical of stating that handling transaction anomalies is not solely a technological and operational issue. In institutional banking relationships, how banks handle disruptions will affect the institution's perception of the quality of the relationships that have been built. Institutions not only pay attention to how quickly the system can be restored, but also how the bank responds, how open communication is carried out, and how quickly the root of the problem is discovered. Therefore, operational resilience has a technical dimension as well as a relational dimension.

When an anomaly occurs, the tendency to immediately find the culprit may not necessarily result in the best settlement for the business relationship. A more constructive approach is to build a shared understanding of the transaction flow, align data from all parties, determine where inconsistencies occur, and build solutions that remain accountable. In these conditions, communication and mediation skills are just as important as technical skills. For institutional bankers, success is not only measured by the resolution

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

of the disruption, but also the ability to prevent the problem from eroding the long-term relationship with the institution.

Thus, this research can expand the meaning of operational resilience by including relationship resilience as a practical dimension that emerges from the case. This means that a resilient organization is not only an organization that is able to return the system to normal conditions, but also is able to maintain the trust of stakeholders during and after a disruption. This is relevant in banking because institutional customers generally see banks and their partner ecosystems as a single service unit. Technical disruptions that are not managed through good communication can develop into reputational and business relationship risks.

Operational Resilience and Institutional Trust

Hasil analisis menunjukkan bahwa tujuan akhir pengelolaan risiko transaksi bukan semata-mata menghindari kerugian finansial, tetapi mempertahankan kepercayaan terhadap layanan perbankan. Pengguna tidak selalu mengetahui kompleksitas API, switching, settlement, rekonsiliasi, atau SLA yang bekerja di balik transaksi. Dari perspektif mereka, ukuran yang paling mudah diamati adalah apakah layanan yang dijanjikan benar-benar dapat bekerja sebagaimana mestinya. Kondisi ini menyebabkan gangguan operasional mempunyai potensi langsung untuk berkembang menjadi persoalan reputasi apabila tidak ditangani secara memadai.

Kepercayaan justru diuji ketika terjadi kondisi yang tidak normal. Bank yang mampu memberikan informasi secara cepat, transparan, dan konsisten serta menunjukkan kemampuan menyelesaikan persoalan dapat mempertahankan hubungan meskipun suatu insiden telah terjadi. Sebaliknya, ketidakjelasan status transaksi, keterlambatan informasi, dan ketidakpastian mengenai tanggung jawab dapat memperbesar dampak insiden. Studi terbaru di sektor perbankan juga menunjukkan relevansi hubungan antara digital trust, operational resilience, dan pengelolaan risiko pihak ketiga dalam tata kelola risiko perbankan digital (Saveljeva & Volkova, 2026). Dengan demikian, kepercayaan dapat dipahami bukan hanya sebagai hasil dari sistem yang tidak pernah mengalami gangguan, tetapi juga dari kemampuan bank mengelola gangguan secara bertanggung jawab ketika gangguan benar-benar terjadi.

Operational Resilience Model in the Digital Payments Ecosystem

Operational resilience is a process, not just a technological condition. Resilience starts with an understanding of end-to-end dependencies, followed by the ability to detect anomalies, ensure transaction finality, reconcile, coordinate with third parties, restore

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

services, and learn from each incident. The international framework also emphasizes banks' ability to survive, adapt, and recover from disruptions and manage third-party dependencies as part of operational resilience.

In terms of research novelty, the most potential point is not the claim that digital transactions contain risks—this has been discussed extensively—but in the integration of four layers of risk management, namely (1) insynchronization between systems, (2) reconciliation as an early warning, (3) risk coordination in a multi-stakeholder ecosystem, and (4) disruption management as a mechanism to maintain institutional trust. This novelty can only be confirmed after being systematically compared with previous research and confirmed through the results of interviews. With this construction, the experience of practitioners who are the main strength can be maintained, and raised into a scientific analysis of how technology, processes, people, governance, and trust work simultaneously in building the operational resilience of digital banking.

CONCLUSION

Based on the results of research and discussion, it can be concluded that digital transformation has formed an increasingly integrated banking payment ecosystem, but at the same time presents a more complex character of operational risks. These risks not only originate from technological failures in one system, but can also arise at points of interaction between systems when there are timeouts, differences in transaction status, or missynchronization between transaction success information and actual fund flow conditions. This condition becomes even more significant when transactions take place in high volumes because exceptions that are not immediately identified can accumulate into material financial exposure. Therefore, banking operational resilience needs to be built through a thorough understanding of the end-to-end transaction process, including establishing a consistent definition of when a transaction can be declared successful and final.

Transaction risk management in the digital payments ecosystem requires a control mechanism that is able to detect, respond, and resolve anomalies quickly and in a coordinated manner. Reconciliation has a strategic role as an early warning mechanism because it allows differences in transaction status and data to be known before they develop into larger problems, so they need to be supported by transaction monitoring, exception detection, escalation mechanisms, and clear settlement procedures. At the same time, dependence on platform providers and third parties requires banks to strengthen third-party risk management, especially in the aspects of responsibility sharing, exception handling, speed of information exchange, escalation mechanisms, and financial and

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Business and Quality Research
https://e-journal.citakonsultindo.or.id/index.php/IJBQR
E-ISSN: 2985-9468

operational responsibility arrangements. Thus, operational resilience is not only determined by technological sophistication and reliability, but is the result of integration between systems, processes, people, risk governance, and coordination of all parties in the payment ecosystem.

This research also shows that the success of digital transaction risk management is ultimately closely related to the bank's ability to maintain institutional trust. When a disruption occurs, service quality is not only assessed based on how quickly the system returns to operation, but also through open communication, speed of identification of root problems, the ability to coordinate and mediate, and the clarity of resolution provided to related parties. In this context, operational resilience can be understood as the ability of the banking ecosystem to detect disruptions, conduct reconciliation, coordinate resolutions, restore services, and take lessons from each incident without neglecting the quality of the relationship with the institution. This is in line with the main substance that emphasizes that in digital financial services, what is at stake when there is a disruption is not only the value of transactions, but also the bank's reputation, the quality of institutional relationships, and confidence in the bank's ability to deal with unplanned situations. Thus, a mature digital transformation is not only reflected in the speed and ease of transactions, but especially in the ability of banks to build a payment ecosystem that is reliable, adaptive, responsive, and trustworthy when facing operational disruptions.

Recommendations

Based on the results of the research, banks are advised to strengthen end-to-end operational resilience in every digital payment service, especially in transactions involving various systems and parties in one ecosystem. This can be done through increasing transaction monitoring, establishing uniform definitions of transaction status and finality, and developing an exception detection mechanism that is able to identify inconsistencies early. The reconciliation process also needs to be placed as part of the early warning mechanism, not just an administrative activity after the transaction is completed, so that the difference between transaction status and the flow of funds can be immediately known before it accumulates into material financial exposure. This is important because in large digital transactions, the speed of detecting anomalies is just as important as the speed of processing transactions.

Banks are also advised to strengthen third-party risk management through governance that not only focuses on the vendor selection and evaluation process, but covers the entire relationship cycle with technology partners and platform providers. Cooperation agreements and Service Level Agreements (SLAs) need to clearly regulate the mechanism

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

for handling exceptions, procedures and escalation deadlines, access to transaction data, reconciliation, continuity of service, and the sharing of operational and financial responsibilities in the event of a disruption. This is relevant to the finding that the use of third parties does not cause the risk to be completely transferred to partners, as customers and institutions ultimately view all parties involved as a single service. Therefore, vulnerability readiness testing, post-incident evaluation, and periodic communication between banks, platform providers, and user institutions need to be conducted to build a more adaptive and resilient payment ecosystem.

In addition to strengthening technology and risk governance, banks are advised to place communication and institutional trust maintenance as an integral part of operational resilience. When transaction anomalies occur, responses should be directed not only at finding technical causes or determining responsible parties, but also at fast and transparent information delivery, data alignment between parties, and proportionate and accountable settlements. Mediation, coordination, and relationship management capabilities are important because disruptions that are not handled properly have the potential to develop from operational issues to reputational risks and degrade the quality of institutional relationships. For further research, the study can be expanded to involve more banks, user institutions, platform providers, and payment system operators so that a comparative understanding of best practices in building operational resilience is obtained, as well as testing and refining the digital payment operational resilience model produced in this study.

REFERENCES

Adeney, R., Hitchins, A., Lane, C., Mehta, H., & Quashi, A. (2024). Operational Resilience in a Macroprudential Framework. Bank of England. https://www.bankofengland.co.uk/financial-stability-paper/2024/operational-resilience-in-a-macroprudential-framework

Akbary, N. M. M., Trinugroho, I., Risfandy, T., & Pamungkas, P. (2025). Digital Transformation and Efficiency: Evidence from Indonesian Banks. International Journal of Business and Society, 26(1), 135–150. https://doi.org/10.33736/ijbs.9555.2025

Alam, Y., Azizah, S. N., & Caroline. (2025). Digital Transformation in Banking Management: Optimizing Operational Efficiency and Enhancing Customer Experience. International Journal of Management Science and Information Technology (IJMSIT),

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

5(1), 46–55. https://doi.org/10.35870/ijmsit.v5i1.3646

Ali, A. A. (2024). Banking Service Recovery Strategies: Enhancing Relationship Quality And Behavioral Intentions. Review of Economic and Business Studies, 17(1), 227–239. https://doi.org/10.47743/rebs-2024-1-0010

Ayadi, R., Chiaramonte, L., Cucinelli, D., & Migliavacca, M. (2025). Digitalization and Banks' Efficiency: Evidence from a European Analysis. International Review of Financial Analysis, 97(January), 103837. https://doi.org/10.1016/j.irfa.2024.103837

Bank of England. (2023). Updated Outsourcing and Third-Party Risk Management: Recognised Payment System Operators and Specified Service Providers. Bankofengland.Co.Uk. https://www.bankofengland.co.uk/paper/2026/ss/updated-outsourcing-and-third-party-risk-management-ss-recognised-payment-system-operators?utm_source=chatgpt.com

BCBS. (2024). Digitalisation of Finance. Basel Committee on Banking Supervision. https://www.bis.org/publications/digitalisation-finance?utm_source=chatgpt.com

BIS. (2025). Principles for the Sound Management of Third-Party Risk. Bank for International Settlements. https://www.bis.org/publications/202512-guidelines-principles-sound-management-third-party-risk?utm_source=chatgpt.com

BIS. (2026). Sound Management of Third-Party Risk - Executive Summary. Bank for International Settlements. https://www.bis.org/publications/fsi-summary-sound-management-third-party-risk-executive-summary?utm_source=chatgpt.com

DeJonckheere, M., Vaughn, L. M., & Schondelmeyer, A. C. (2024). Qualitative Thematic Analysis in a Mixed Methods Study: Guidelines and Considerations for Integration. Journal of Mixed Methods Research, 18(3), 258–269. https://doi.org/10.1177/15586898241257546

Desai, A., Kosse, A., & Sharples, J. (2024). Finding a Needle in a Haystack: A Machine Learning Framework for Anomaly Detection in Payment Systems. https://www.bis.org/publications/working-paper-1188-finding-needle-haystack-machine-learning-framework-anomaly-detection-payment-systems?utm_source=chatgpt.com

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

Desiraju, K., Mishra, A. N., & Sengupta, P. (2024). Customer Perceptions on Open Banking Apps: Insights Using Structural Topic Modeling. Journal of Retailing and Consumer Services, 81(November), 104029. https://doi.org/10.1016/j.jretconser.2024.104029

FSB. (2023). Final Report on Enhancing Third-party Risk Management and Oversight – A Toolkit for Financial Institutions and Financial Authorities. Financial Stability Board. https://www.fsb.org/2023/12/final-report-on-enhancing-third-party-risk-management-and-oversight-a-toolkit-for-financial-institutions-and-financial-authorities/?utm_source=chatgpt.com

Khiaonarong, T., Leinonen, H., & Rizaldy, R. (2021). Operational Resilience in Digital Payments: Experiences and Issues. IMF ELIBRARY, 2021(288), 1–36. https://doi.org/10.5089/9781616355913.001

Munawar, M. M., & Hadianto, B. (2024). Banking Service Recovery and Consumer Loyalty: The Mediating Role of Satisfaction. International Journal of Applied Economics, Finance and Accounting, 20(1), 35–45. https://doi.org/10.33094/ijaefa.v20i1.1921

Saveljeva, J., & Volkova, T. (2026). Category-Specific Effects of Digital Trust on Third-Party Risks in the Banking Industry. The Journal of Risk Finance, 27(2), 329–345. https://doi.org/10.1108/JRF-08-2025-0383

Shanmugam, J. (2025). Real-Time Reconciliation Systems: Transforming Transaction Verification in Global Payment Networks. International Journal of Computational and Experimental Science and Engineering (IJCESEN), 11(3), 6607–6614. https://doi.org/10.22399/ijcesen.3890

Uddin, M. H., Mollah, S., Islam, N., & Ali, M. H. (2023). Does Digital Transformation Matter for Operational Risk Exposure? Technological Forecasting and Social Change, 193(122919 (December)), 1–22. https://doi.org/10.1016/j.techfore.2023.122919

Villamin, P., Lopez, V., Thapa, D. K., & Cleary, M. (2025). A Worked Example of Qualitative Descriptive Design: A Step-by-Step Guide for Novice and Early Career Researchers. Journal of Advanced Nursing, 81(8), 4351–5223. https://doi.org/10.1111/jan.16481

Wittlin, J., Ossowska, A., & Sawicka, K. (2026). Is DORA an Opportunity for More Balanced Distribution of Third-Party Risk Management Assurance Responsibilities Between

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.

Banks, Regulators and Technology Providers? Information & Communications Technology Law, 35(1), 109–116. https://doi.org/10.1080/13600834.2025.2514385

Wulandari, N., Jager, J. W. De, & Mahry, S. E. (2024). The Driving Factors of Digital Banking Intention and the Role of Customer Experience in Indonesia Banking Industry. Jurnal Administrasi Bisnis, 13(10–18). https://doi.org/10.14710/jab.v13i1.59623

Yao, Y., & Li, J. (2022). Operational Risk Assessment of Third-Party Payment Platforms: A Case Study of China. Financial Innovation, 8(19), 1–20. https://doi.org/10.1186/s40854-022-00332-x

Copyright to the author of some rights reserved This work is licensed under aCreative Commons Attribution-ShareAlike 4.0 International License.