JESOCIN

DIGITAL PAYMENT FRAUD RECOVERY IN SMALL ENTERPRISES: A GOVERNANCE MODEL FOR DETECTION, CUSTOMER RESPONSE, AND CONTROL RENEWAL

Ricky Agusiady[1], Adang Haryaman[2]
[1]Universitas Sangga Buana YPKP, Bandung, Indonesia
[2]Universitas Logistik dan Bisnis Internasional, Bandung, Indonesia
Email: [1]ricky.agusiady@usbypkp.ac.id; [2]adang@ulbi.ac.id

Abstract

This conceptual and integrative review develops a framework for digital payment fraud recovery in micro, small, and medium enterprises. It addresses the problem that small enterprises increasingly depend on digital payments but may lack coordinated routines for detecting anomalies, protecting customers, preserving evidence, and restoring trustworthy operations after fraud. Drawing on the resource-based view, dynamic capabilities, organizational learning, absorptive capacity, social capital, and resilience, the paper explains how transaction anomaly detection, rapid account containment, customer-centered response, evidence preservation, post-incident control renewal can be organized as mutually reinforcing routines. The proposed pathway moves from problem diagnosis and capability mapping to bounded experimentation, evidence review, resource reconfiguration, and learning retention. No primary survey, interview, experimental, administrative, or statistical data are claimed. The framework links these mechanisms to loss containment, customer protection, transaction confidence, operational recovery, fraud resilience and identifies managerial, institutional, and research implications suitable for resource-constrained enterprises.

Keywords: digital payments; fraud recovery; customer protection; internal control; small enterprises

INTRODUCTION

Fraud-recovery governance begins with the recognition that customer-centered response connects specialist knowledge with accountable managerial judgment. Within problem definition, ethical responsibility remains with identifiable people even when technology or partners support the work. Transaction accountability therefore requires that post-incident control renewal allows experience to alter later routines instead of remaining an isolated lesson.

An assurance-oriented reading shows that loss containment depends on information that is relevant to the focal decision. The same principle shapes problem definition, because customer-centered response connects specialist knowledge with accountable managerial judgment. A defensible recovery response is to ensure that transaction confidence is strengthened when affected parties can question assumptions and explain exceptions.

Digital convenience does not remove human responsibility: operational recovery improves when alternatives are compared before resources are committed. When applied to problem definition, loss containment depends on information that is relevant to the focal decision. Traceable fraud-response practice consequently depends on the proposition that resource scarcity makes selective experimentation more credible than organization-wide transformation.

THEORETICAL FOUNDATION

Fraud-recovery governance begins with the recognition that customer-centered response connects specialist knowledge with accountable managerial judgment. Within theoretical explanation, transaction confidence is strengthened when affected parties can question assumptions and explain exceptions. Transaction accountability therefore requires that external partners add value only when their knowledge is interpreted and adapted locally.

An assurance-oriented reading shows that loss containment depends on information that is relevant to the focal decision. The same principle shapes theoretical explanation, because resource scarcity makes selective experimentation more credible than organization-wide transformation. A defensible recovery response is to ensure that ethical responsibility remains with identifiable people even when technology or partners support the work.

Digital convenience does not remove human responsibility: operational recovery improves when alternatives are compared before resources are committed. When applied to theoretical explanation, a predetermined stop condition protects continuity when an initiative no longer justifies its exposure. Traceable fraud-response practice consequently depends on the proposition that customer-centered response connects specialist knowledge with accountable managerial judgment.

The payment-fraud problem is not simply technical. It arises because proportionate documentation helps small organizations learn without reproducing large-firm bureaucracy; in theoretical explanation, transaction anomaly detection establishes a disciplined starting point for digital payment fraud recovery. For this reason, loss containment depends on information that is relevant to the focal decision.

Fraud-recovery governance begins with the recognition that short feedback cycles make correction less costly and reveal weak assumptions earlier. Within theoretical explanation, evidence preservation reduces dependence on a single decision path or organizational actor. Transaction accountability therefore requires that operational recovery improves when alternatives are compared before resources are committed.

Digital convenience does not remove human responsibility: loss containment depends on information that is relevant to the focal decision. When applied to theoretical explanation, proportionate documentation helps small organizations learn without reproducing large-firm bureaucracy. Traceable fraud-response practice consequently depends on the proposition that the use of rapid account containment converts broad intentions into observable operating choices.

The payment-fraud problem is not simply technical. It arises because the pursuit of fraud resilience develops through repeated sensing, bounded action, evaluation, and renewal; in theoretical explanation, ethical responsibility remains with identifiable people even when technology or partners support the work. For this reason, loss containment depends on information that is relevant to the focal decision.

Fraud-recovery governance begins with the recognition that a predetermined stop condition protects continuity when an initiative no longer justifies its exposure. Within theoretical explanation, evidence preservation reduces dependence on a single decision path or organizational actor. Transaction accountability therefore requires that the pursuit of fraud resilience develops through repeated sensing, bounded action, evaluation, and renewal.

CONCEPTUAL ARCHITECTURE

An assurance-oriented reading shows that post-incident control renewal allows experience to alter later routines instead of remaining an isolated lesson. The same principle shapes conceptual design, because resource scarcity makes selective experimentation more credible than organization-wide transformation. A defensible recovery response is to ensure that the use of rapid account containment converts broad intentions into observable operating choices.

Digital convenience does not remove human responsibility: transaction confidence is strengthened when affected parties can question assumptions and explain exceptions. When applied to conceptual design, a predetermined stop condition protects continuity when an initiative no longer justifies its exposure. Traceable fraud-response practice consequently depends on the proposition that post-incident control renewal allows experience to alter later routines instead of remaining an isolated lesson.

The payment-fraud problem is not simply technical. It arises because resource scarcity makes selective experimentation more credible than organization-wide transformation; in conceptual design, transaction anomaly detection establishes a disciplined starting point for digital payment fraud recovery. For this reason, transaction confidence is strengthened when affected parties can question assumptions and explain exceptions.

Fraud-recovery governance begins with the recognition that a predetermined stop condition protects continuity when an initiative no longer justifies its exposure. Within conceptual design, evidence preservation reduces dependence on a single decision path or organizational actor. Transaction accountability therefore requires that resource scarcity makes selective experimentation more credible than organization-wide transformation.

An assurance-oriented reading shows that transaction anomaly detection establishes a disciplined starting point for digital payment fraud recovery. The same principle shapes conceptual design, because customer protection requires responsibilities and review intervals that employees understand. A defensible recovery response is to ensure that a predetermined stop condition protects continuity when an initiative no longer justifies its exposure.

The payment-fraud problem is not simply technical. It arises because operational recovery improves when alternatives are compared before resources are committed; in conceptual design, transaction anomaly detection establishes a disciplined starting point for digital payment fraud recovery. For this reason, operational recovery improves when alternatives are compared before resources are committed.

Fraud-recovery governance begins with the recognition that external partners add value only when their knowledge is interpreted and adapted locally. Within conceptual design, post-incident control renewal allows experience to alter later routines instead of remaining an isolated lesson. Transaction accountability therefore requires that external partners add value only when their knowledge is interpreted and adapted locally.

An assurance-oriented reading shows that transaction anomaly detection establishes a disciplined starting point for digital payment fraud recovery. The same principle shapes conceptual design, because operational recovery improves when alternatives are compared before resources are committed. A defensible recovery response is to ensure that transaction anomaly detection establishes a disciplined starting point for digital payment fraud recovery.

Digital convenience does not remove human responsibility: post-incident control renewal allows experience to alter later routines instead of remaining an isolated lesson. When applied to conceptual design, external partners add value only when their knowledge is interpreted and adapted locally. Traceable fraud-response practice consequently depends on the proposition that post-incident control renewal allows experience to alter later routines instead of remaining an isolated lesson.

The payment-fraud problem is not simply technical. It arises because operational recovery improves when alternatives are compared before resources are committed; in conceptual design, transaction anomaly detection establishes a disciplined starting point for digital payment fraud recovery. For this reason, operational recovery improves when alternatives are compared before resources are committed.

CAPABILITY DEVELOPMENT

Digital convenience does not remove human responsibility: customer protection requires responsibilities and review intervals that employees understand. When applied to capability formation, a predetermined stop condition protects continuity when an initiative no longer justifies its exposure. Traceable fraud-response practice consequently depends on the proposition that customer protection requires responsibilities and review intervals that employees understand.

The payment-fraud problem is not simply technical. It arises because the pursuit of fraud resilience develops through repeated sensing, bounded action, evaluation, and renewal; in capability formation, transaction anomaly detection establishes a disciplined starting point for digital payment fraud recovery. For this reason, the pursuit of fraud resilience develops through repeated sensing, bounded action, evaluation, and renewal.

Fraud-recovery governance begins with the recognition that external partners add value only when their knowledge is interpreted and adapted locally. Within capability formation, evidence preservation reduces dependence on a single decision path or organizational actor. Transaction accountability therefore requires that external partners add value only when their knowledge is interpreted and adapted locally.

An assurance-oriented reading shows that ethical responsibility remains with identifiable people even when technology or partners support the work. The same principle shapes capability formation, because customer protection requires responsibilities and review intervals that employees understand. A defensible recovery response is to ensure that ethical responsibility remains with identifiable people even when technology or partners support the work.

Digital convenience does not remove human responsibility: customer-centered response connects specialist knowledge with accountable managerial judgment. When applied to capability formation, the pursuit of fraud resilience develops through repeated sensing, bounded action, evaluation, and renewal. Traceable fraud-response practice consequently depends on the proposition that customer-centered response connects specialist knowledge with accountable managerial judgment.

Fraud-recovery governance begins with the recognition that proportionate documentation helps small organizations learn without reproducing large-firm bureaucracy. Within capability formation, loss containment depends on information that is relevant to the focal decision. Transaction accountability therefore requires that ethical responsibility remains with identifiable people even when technology or partners support the work.

An assurance-oriented reading shows that ethical responsibility remains with identifiable people even when technology or partners support the work. The same principle shapes capability formation, because the pursuit of fraud resilience develops through repeated sensing, bounded action, evaluation, and renewal. A defensible recovery response is to ensure that evidence preservation reduces dependence on a single decision path or organizational actor.

Digital convenience does not remove human responsibility: evidence preservation reduces dependence on a single decision path or organizational actor. When applied to capability formation, a predetermined stop condition protects continuity when an initiative no longer justifies its exposure. Traceable fraud-response practice consequently depends on the proposition that transaction confidence is strengthened when affected parties can question assumptions and explain exceptions.

The payment-fraud problem is not simply technical. It arises because transaction confidence is strengthened when affected parties can question assumptions and explain exceptions; in capability formation, the use of rapid account containment converts broad intentions into observable operating choices. For this reason, proportionate documentation helps small organizations learn without reproducing large-firm bureaucracy.

Fraud-recovery governance begins with the recognition that proportionate documentation helps small organizations learn without reproducing large-firm bureaucracy. Within capability formation, loss containment depends on information that is relevant to the focal decision. Transaction accountability therefore requires that ethical responsibility remains with identifiable people even when technology or partners support the work.

IMPLEMENTATION PATHWAY

The payment-fraud problem is not simply technical. It arises because operational recovery improves when alternatives are compared before resources are committed; in implementation sequencing, transaction anomaly detection establishes a disciplined starting point for digital payment fraud recovery. For this reason, proportionate documentation helps small organizations learn without reproducing large-firm bureaucracy.

Fraud-recovery governance begins with the recognition that proportionate documentation helps small organizations learn without reproducing large-firm bureaucracy. Within implementation sequencing, evidence preservation reduces dependence on a single decision path or organizational actor. Transaction accountability therefore requires that short feedback cycles make correction less costly and reveal weak assumptions earlier.

An assurance-oriented reading shows that short feedback cycles make correction less costly and reveal weak assumptions earlier. The same principle shapes implementation sequencing, because customer protection requires responsibilities and review intervals that employees understand. A defensible recovery response is to ensure that the use of rapid account containment converts broad intentions into observable operating choices.

Digital convenience does not remove human responsibility: the use of rapid account containment converts broad intentions into observable operating choices. When applied to implementation sequencing, the pursuit of fraud resilience develops through repeated sensing, bounded action, evaluation, and renewal.

Traceable fraud-response practice consequently depends on the proposition that post-incident control renewal allows experience to alter later routines instead of remaining an isolated lesson.

The payment-fraud problem is not simply technical. It arises because post-incident control renewal allows experience to alter later routines instead of remaining an isolated lesson; in implementation sequencing, external partners add value only when their knowledge is interpreted and adapted locally. For this reason, transaction confidence is strengthened when affected parties can question assumptions and explain exceptions.

An assurance-oriented reading shows that short feedback cycles make correction less costly and reveal weak assumptions earlier. The same principle shapes implementation sequencing, because resource scarcity makes selective experimentation more credible than organization-wide transformation. A defensible recovery response is to ensure that customer protection requires responsibilities and review intervals that employees understand.

Digital convenience does not remove human responsibility: customer-centered response connects specialist knowledge with accountable managerial judgment. When applied to implementation sequencing, short feedback cycles make correction less costly and reveal weak assumptions earlier. Traceable fraud-response practice consequently depends on the proposition that resource scarcity makes selective experimentation more credible than organization-wide transformation.

The payment-fraud problem is not simply technical. It arises because customer protection requires responsibilities and review intervals that employees understand; in implementation sequencing, customer-centered response connects specialist knowledge with accountable managerial judgment. For this reason, short feedback cycles make correction less costly and reveal weak assumptions earlier.

Fraud-recovery governance begins with the recognition that resource scarcity makes selective experimentation more credible than organization-wide transformation. Within implementation sequencing, customer protection requires responsibilities and review intervals that employees understand. Transaction accountability therefore requires that customer-centered response connects specialist knowledge with accountable managerial judgment.

An assurance-oriented reading shows that short feedback cycles make correction less costly and reveal weak assumptions earlier. The same principle shapes implementation sequencing, because resource scarcity makes selective experimentation more credible than organization-wide transformation. A defensible recovery response is to ensure that customer protection requires responsibilities and review intervals that employees understand.

GOVERNANCE AND RISK

Fraud-recovery governance begins with the recognition that resource scarcity makes selective experimentation more credible than organization-wide transformation. Within governance safeguards, evidence preservation reduces dependence on a single decision path or organizational actor. Transaction accountability therefore requires that transaction anomaly detection establishes a disciplined starting point for digital payment fraud recovery.

An assurance-oriented reading shows that a predetermined stop condition protects continuity when an initiative no longer justifies its exposure. The same principle shapes governance safeguards, because customer protection requires responsibilities and review intervals that employees understand. A defensible recovery response is to ensure that evidence preservation reduces dependence on a single decision path or organizational actor.

Digital convenience does not remove human responsibility: transaction anomaly detection establishes a disciplined starting point for digital payment fraud recovery. When applied to governance safeguards, the pursuit of fraud resilience develops through repeated sensing, bounded action, evaluation, and renewal. Traceable fraud-response practice consequently depends on the proposition that customer protection requires responsibilities and review intervals that employees understand.

The payment-fraud problem is not simply technical. It arises because evidence preservation reduces dependence on a single decision path or organizational actor; in governance safeguards, external partners add value only when their knowledge is interpreted and adapted locally. For this reason, the pursuit of fraud resilience develops through repeated sensing, bounded action, evaluation, and renewal.

Fraud-recovery governance begins with the recognition that customer protection requires responsibilities and review intervals that employees understand. Within governance safeguards, ethical responsibility remains with identifiable people even when technology or partners support the work. Transaction accountability therefore requires that external partners add value only when their knowledge is interpreted and adapted locally.

Digital convenience does not remove human responsibility: the use of rapid account containment converts broad intentions into observable operating choices. When applied to governance safeguards, ethical responsibility remains with identifiable people even when technology or partners support the work. Traceable fraud-response practice consequently depends on the proposition that a predetermined stop condition protects continuity when an initiative no longer justifies its exposure.

The payment-fraud problem is not simply technical. It arises because loss containment depends on information that is relevant to the focal decision; in governance safeguards, evidence preservation reduces dependence on a single decision path or organizational actor. For this reason, the use of rapid account containment converts broad intentions into observable operating choices.

Fraud-recovery governance begins with the recognition that the pursuit of fraud resilience develops through repeated sensing, bounded action, evaluation, and renewal. Within governance safeguards, transaction confidence is strengthened when affected parties can question assumptions and explain exceptions. Transaction accountability therefore requires that loss containment depends on information that is relevant to the focal decision.

An assurance-oriented reading shows that a predetermined stop condition protects continuity when an initiative no longer justifies its exposure. The same principle shapes governance safeguards, because proportionate documentation helps small organizations learn without reproducing large-firm bureaucracy. A defensible recovery response is to ensure that the pursuit of fraud resilience develops through repeated sensing, bounded action, evaluation, and renewal.

Digital convenience does not remove human responsibility: the use of rapid account containment converts broad intentions into observable operating choices. When applied to governance safeguards, ethical responsibility remains with identifiable people even when technology or partners support the work. Traceable fraud-response practice consequently depends on the proposition that a predetermined stop condition protects continuity when an initiative no longer justifies its exposure.

PERFORMANCE AND LEARNING

An assurance-oriented reading shows that external partners add value only when their knowledge is interpreted and adapted locally. The same principle shapes performance interpretation, because customer protection requires responsibilities and review intervals that employees understand. A defensible recovery response is to ensure that loss containment depends on information that is relevant to the focal decision.

Digital convenience does not remove human responsibility: ethical responsibility remains with identifiable people even when technology or partners support the work. When applied to performance interpretation, the pursuit of fraud resilience develops through repeated sensing, bounded action, evaluation, and renewal. Traceable fraud-response practice consequently depends on the proposition that operational recovery improves when alternatives are compared before resources are committed.

The payment-fraud problem is not simply technical. It arises because customer-centered response connects specialist knowledge with accountable managerial judgment; in performance interpretation, external partners add value only when their knowledge is interpreted and adapted locally. For this reason, proportionate documentation helps small organizations learn without reproducing large-firm bureaucracy.

Fraud-recovery governance begins with the recognition that loss containment depends on information that is relevant to the focal decision. Within performance interpretation, ethical responsibility remains with identifiable people even when technology or partners support the work. Transaction accountability therefore requires that short feedback cycles make correction less costly and reveal weak assumptions earlier.

An assurance-oriented reading shows that operational recovery improves when alternatives are compared before resources are committed. The same principle shapes performance interpretation, because customer-centered response connects specialist knowledge with accountable managerial judgment. A defensible recovery response is to ensure that the use of rapid account containment converts broad intentions into observable operating choices.

The payment-fraud problem is not simply technical. It arises because post-incident control renewal allows experience to alter later routines instead of remaining an isolated lesson; in performance interpretation, post-incident control renewal allows experience to alter later routines instead of remaining an isolated lesson. For this reason, post-incident control renewal allows experience to alter later routines instead of remaining an isolated lesson.

Fraud-recovery governance begins with the recognition that operational recovery improves when alternatives are compared before resources are committed. Within performance interpretation, operational recovery improves when alternatives are compared before resources are committed. Transaction accountability therefore requires that operational recovery improves when alternatives are compared before resources are committed.

An assurance-oriented reading shows that external partners add value only when their knowledge is interpreted and adapted locally. The same principle shapes performance interpretation, because external partners add value only when their knowledge is interpreted and adapted locally. A defensible recovery response is to ensure that external partners add value only when their knowledge is interpreted and adapted locally.

Digital convenience does not remove human responsibility: transaction anomaly detection establishes a disciplined starting point for digital payment fraud recovery. When applied to performance interpretation, transaction anomaly detection establishes a disciplined starting point for digital payment fraud recovery. Traceable fraud-response practice consequently depends on the proposition that transaction anomaly detection establishes a disciplined starting point for digital payment fraud recovery.

The payment-fraud problem is not simply technical. It arises because post-incident control renewal allows experience to alter later routines instead of remaining an isolated lesson; in performance interpretation, post-incident control renewal allows experience to alter later routines instead of remaining an isolated lesson. For this reason, post-incident control renewal allows experience to alter later routines instead of remaining an isolated lesson.

MANAGERIAL AND POLICY IMPLICATIONS

Digital convenience does not remove human responsibility: short feedback cycles make correction less costly and reveal weak assumptions earlier. When applied to managerial and institutional implications, the pursuit of fraud resilience develops through repeated sensing, bounded action, evaluation, and renewal. Traceable fraud-response practice consequently depends on the proposition that resource scarcity makes selective experimentation more credible than organization-wide transformation.

The payment-fraud problem is not simply technical. It arises because the use of rapid account containment converts broad intentions into observable operating choices; in managerial and institutional implications, external partners add value only when their knowledge is interpreted and adapted locally. For this reason, a predetermined stop condition protects continuity when an initiative no longer justifies its exposure.

Fraud-recovery governance begins with the recognition that post-incident control renewal allows experience to alter later routines instead of remaining an isolated lesson. Within managerial and institutional

implications, ethical responsibility remains with identifiable people even when technology or partners support the work. Transaction accountability therefore requires that transaction anomaly detection establishes a disciplined starting point for digital payment fraud recovery.

An assurance-oriented reading shows that transaction confidence is strengthened when affected parties can question assumptions and explain exceptions. The same principle shapes managerial and institutional implications, because customer-centered response connects specialist knowledge with accountable managerial judgment. A defensible recovery response is to ensure that evidence preservation reduces dependence on a single decision path or organizational actor.

Digital convenience does not remove human responsibility: resource scarcity makes selective experimentation more credible than organization-wide transformation. When applied to managerial and institutional implications, loss containment depends on information that is relevant to the focal decision. Traceable fraud-response practice consequently depends on the proposition that customer protection requires responsibilities and review intervals that employees understand.

Fraud-recovery governance begins with the recognition that transaction confidence is strengthened when affected parties can question assumptions and explain exceptions. Within managerial and institutional implications, the pursuit of fraud resilience develops through repeated sensing, bounded action, evaluation, and renewal. Transaction accountability therefore requires that proportionate documentation helps small organizations learn without reproducing large-firm bureaucracy.

An assurance-oriented reading shows that proportionate documentation helps small organizations learn without reproducing large-firm bureaucracy. The same principle shapes managerial and institutional implications, because a predetermined stop condition protects continuity when an initiative no longer justifies its exposure. A defensible recovery response is to ensure that ethical responsibility remains with identifiable people even when technology or partners support the work.

Digital convenience does not remove human responsibility: ethical responsibility remains with identifiable people even when technology or partners support the work. When applied to managerial and institutional implications, the use of rapid account containment converts broad intentions into observable operating choices. Traceable fraud-response practice consequently depends on the proposition that evidence preservation reduces dependence on a single decision path or organizational actor.

RESEARCH AGENDA AND CONCLUSION

The payment-fraud problem is not simply technical. It arises because transaction anomaly detection establishes a disciplined starting point for digital payment fraud recovery; in future research and conclusion, external partners add value only when their knowledge is interpreted and adapted locally. For this reason, ethical responsibility remains with identifiable people even when technology or partners support the work.

Fraud-recovery governance begins with the recognition that evidence preservation reduces dependence on a single decision path or organizational actor. Within future research and conclusion, ethical responsibility remains with identifiable people even when technology or partners support the work. Transaction accountability therefore requires that customer-centered response connects specialist knowledge with accountable managerial judgment.

An assurance-oriented reading shows that customer protection requires responsibilities and review intervals that employees understand. The same principle shapes future research and conclusion, because customer-centered response connects specialist knowledge with accountable managerial judgment. A defensible recovery response is to ensure that loss containment depends on information that is relevant to the focal decision.

Digital convenience does not remove human responsibility: the pursuit of fraud resilience develops through repeated sensing, bounded action, evaluation, and renewal. When applied to future research and conclusion, loss containment depends on information that is relevant to the focal decision. Traceable fraud-

response practice consequently depends on the proposition that operational recovery improves when alternatives are compared before resources are committed.

The payment-fraud problem is not simply technical. It arises because external partners add value only when their knowledge is interpreted and adapted locally; in future research and conclusion, operational recovery improves when alternatives are compared before resources are committed. For this reason, proportionate documentation helps small organizations learn without reproducing large-firm bureaucracy.

An assurance-oriented reading shows that resource scarcity makes selective experimentation more credible than organization-wide transformation. The same principle shapes future research and conclusion, because short feedback cycles make correction less costly and reveal weak assumptions earlier. A defensible recovery response is to ensure that customer-centered response connects specialist knowledge with accountable managerial judgment.

Digital convenience does not remove human responsibility: short feedback cycles make correction less costly and reveal weak assumptions earlier. When applied to future research and conclusion, customer-centered response connects specialist knowledge with accountable managerial judgment. Traceable fraud-response practice consequently depends on the proposition that customer protection requires responsibilities and review intervals that employees understand.

The payment-fraud problem is not simply technical. It arises because customer-centered response connects specialist knowledge with accountable managerial judgment; in future research and conclusion, customer protection requires responsibilities and review intervals that employees understand. For this reason, resource scarcity makes selective experimentation more credible than organization-wide transformation.

REFERENCES

Adler, P. S., & Kwon, S.-W. (2002). Social capital: Prospects for a new concept. Academy of Management Review, 27(1), 17-40.

Barney, J. (1991). Firm resources and sustained competitive advantage. Journal of Management, 17(1), 99-120.

Chesbrough, H. W. (2003). Open Innovation: The New Imperative for Creating and Profiting from Technology. Harvard Business School Press.

Cohen, W. M., & Levinthal, D. A. (1990). Absorptive capacity: A new perspective on learning and innovation. Administrative Science Quarterly, 35(1), 128-152.

Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. Business Research, 13, 215-246.

Dwivedi, Y. K., et al. (2021). Artificial intelligence: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management, 57, 101994.

Eisenhardt, K. M., & Martin, J. A. (2000). Dynamic capabilities: What are they? Strategic Management Journal, 21(10-11), 1105-1121.

Geissdoerfer, M., Savaget, P., Bocken, N. M. P., & Hultink, E. J. (2017). The circular economy: A new sustainability paradigm? Journal of Cleaner Production, 143, 757-768.

March, J. G. (1991). Exploration and exploitation in organizational learning. Organization Science, 2(1), 71-87.

Nahapiet, J., & Ghoshal, S. (1998). Social capital, intellectual capital, and the organizational advantage. Academy of Management Review, 23(2), 242-266.

Nambisan, S. (2017). Digital entrepreneurship: Toward a digital technology perspective of entrepreneurship. Entrepreneurship Theory and Practice, 41(6), 1029-1055.

OECD. (2021). The Digital Transformation of SMEs. OECD Publishing.

Sarker, S., Chatterjee, S., Xiao, X., & Elbanna, A. (2019). The sociotechnical axis of cohesion for the IS discipline. MIS Quarterly, 43(3), 695-719.

Spigel, B. (2017). The relational organization of entrepreneurial ecosystems. Entrepreneurship Theory and Practice, 41(1), 49-72.

Stam, E. (2015). Entrepreneurial ecosystems and regional policy: A sympathetic critique. European Planning Studies, 23(9), 1759-1769.

Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of sustainable enterprise performance. Strategic Management Journal, 28(13), 1319-1350.

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. Strategic Management Journal, 18(7), 509-533.

Verhoef, P. C., et al. (2021). Digital transformation: A multidisciplinary reflection and research agenda. Journal of Business Research, 122, 889-901.

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. Journal of Strategic Information Systems, 28(2), 118-144.

West, J., & Bogers, M. (2014). Leveraging external sources of innovation: A review of research on open innovation. Journal of Product Innovation Management, 31(4), 814-831.