JESOCIN

CYBERSECURITY GOVERNANCE FOR DIGITAL MSME FINANCE: INTEGRATING ACCESS CONTROL, TRANSACTION ASSURANCE, AND ORGANIZATIONAL LEARNING

Nia Riana[1], Adang Haryaman[2]
1Universitas Widyatama, Bandung, Indonesia
2Universitas Logistik dan Bisnis Internasional, Bandung, Indonesia
Email: [1]nia.riana@widyatama.ac.id; [2]adang@ulbi.ac.id

Abstract

This conceptual and integrative review develops a framework for cybersecurity governance in digital finance in micro, small, and medium enterprises. It addresses the problem that digital financial services improve speed and access while exposing MSMEs to credential theft, payment fraud, weak third-party controls, and disruptive security incidents. Drawing on the resource-based view, dynamic capabilities, organizational learning, absorptive capacity, social capital, and resilience, the paper explains how risk-based access control, transaction verification, vendor assurance, incident response discipline, security learning routines 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 transaction integrity, service continuity, user confidence, controlled exposure, cyber resilience and identifies managerial, institutional, and research implications suitable for resource-constrained enterprises.

Keywords: cybersecurity governance; digital finance; MSMEs; transaction assurance; cyber resilience

INTRODUCTION

Cybersecurity governance begins with the recognition that vendor assurance 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 security learning routines allows experience to alter later routines instead of remaining an isolated lesson.

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

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

THEORETICAL FOUNDATION

Cybersecurity governance begins with the recognition that vendor assurance connects specialist knowledge with accountable managerial judgment. Within theoretical explanation, user 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 transaction integrity 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 security 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: controlled exposure 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 security practice consequently depends on the proposition that vendor assurance connects specialist knowledge with accountable managerial judgment.

The cybersecurity problem is not simply technical. It arises because proportionate documentation helps small organizations learn without reproducing large-firm bureaucracy; in theoretical explanation, risk-based access control establishes a disciplined starting point for cybersecurity governance in digital finance. For this reason, transaction integrity depends on information that is relevant to the focal decision.

Cybersecurity governance begins with the recognition that short feedback cycles make correction less costly and reveal weak assumptions earlier. Within theoretical explanation, incident response discipline reduces dependence on a single decision path or organizational actor. Transaction accountability therefore requires that controlled exposure improves when alternatives are compared before resources are committed.

Digital convenience does not remove human responsibility: transaction integrity 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 security practice consequently depends on the proposition that the use of transaction verification converts broad intentions into observable operating choices.

The cybersecurity problem is not simply technical. It arises because the pursuit of cyber 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, transaction integrity depends on information that is relevant to the focal decision.

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

CONCEPTUAL ARCHITECTURE

An assurance-oriented reading shows that security learning routines 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 security response is to ensure that the use of transaction verification converts broad intentions into observable operating choices.

Digital convenience does not remove human responsibility: user 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 security practice consequently depends on the proposition that security learning routines allows experience to alter later routines instead of remaining an isolated lesson.

The cybersecurity problem is not simply technical. It arises because resource scarcity makes selective experimentation more credible than organization-wide transformation; in conceptual design, risk-based access control establishes a disciplined starting point for cybersecurity governance in digital finance. For this reason, user confidence is strengthened when affected parties can question assumptions and explain exceptions.

Cybersecurity governance begins with the recognition that a predetermined stop condition protects continuity when an initiative no longer justifies its exposure. Within conceptual design, incident response discipline 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 risk-based access control establishes a disciplined starting point for cybersecurity governance in digital finance. The same principle shapes conceptual design, because service continuity requires responsibilities and review intervals that employees understand. A defensible security response is to ensure that a predetermined stop condition protects continuity when an initiative no longer justifies its exposure.

The cybersecurity problem is not simply technical. It arises because controlled exposure improves when alternatives are compared before resources are committed; in conceptual design, risk-based access control establishes a disciplined starting point for cybersecurity governance in digital finance. For this reason, controlled exposure improves when alternatives are compared before resources are committed.

Cybersecurity governance begins with the recognition that external partners add value only when their knowledge is interpreted and adapted locally. Within conceptual design, security learning routines 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 risk-based access control establishes a disciplined starting point for cybersecurity governance in digital finance. The same principle shapes conceptual design, because controlled exposure improves when alternatives are compared before resources are committed. A defensible security response is to ensure that risk-based access control establishes a disciplined starting point for cybersecurity governance in digital finance.

Digital convenience does not remove human responsibility: security learning routines 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 security practice consequently depends on the proposition that security learning routines allows experience to alter later routines instead of remaining an isolated lesson.

The cybersecurity problem is not simply technical. It arises because controlled exposure improves when alternatives are compared before resources are committed; in conceptual design, risk-based access control establishes a disciplined starting point for cybersecurity governance in digital finance. For this reason, controlled exposure improves when alternatives are compared before resources are committed.

CAPABILITY DEVELOPMENT

Digital convenience does not remove human responsibility: service continuity 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 security practice consequently depends on the proposition that service continuity requires responsibilities and review intervals that employees understand.

The cybersecurity problem is not simply technical. It arises because the pursuit of cyber resilience develops through repeated sensing, bounded action, evaluation, and renewal; in capability formation, risk-based access control establishes a disciplined starting point for cybersecurity governance in digital finance. For this reason, the pursuit of cyber resilience develops through repeated sensing, bounded action, evaluation, and renewal.

Cybersecurity governance begins with the recognition that external partners add value only when their knowledge is interpreted and adapted locally. Within capability formation, incident response discipline 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 service continuity requires responsibilities and review intervals that employees understand. A defensible security 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: vendor assurance connects specialist knowledge with accountable managerial judgment. When applied to capability formation, the pursuit of cyber resilience develops through repeated sensing, bounded action, evaluation, and renewal. Traceable security practice consequently depends on the proposition that vendor assurance connects specialist knowledge with accountable managerial judgment.

Cybersecurity governance begins with the recognition that proportionate documentation helps small organizations learn without reproducing large-firm bureaucracy. Within capability formation, transaction integrity 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 cyber resilience develops through repeated sensing, bounded action, evaluation, and renewal. A defensible security response is to ensure that incident response discipline reduces dependence on a single decision path or organizational actor.

Digital convenience does not remove human responsibility: incident response discipline 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 security practice consequently depends on the proposition that user confidence is strengthened when affected parties can question assumptions and explain exceptions.

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

Cybersecurity governance begins with the recognition that proportionate documentation helps small organizations learn without reproducing large-firm bureaucracy. Within capability formation, transaction integrity 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 cybersecurity problem is not simply technical. It arises because controlled exposure improves when alternatives are compared before resources are committed; in implementation sequencing, risk-based access control establishes a disciplined starting point for cybersecurity governance in digital finance. For this reason, proportionate documentation helps small organizations learn without reproducing large-firm bureaucracy.

Cybersecurity governance begins with the recognition that proportionate documentation helps small organizations learn without reproducing large-firm bureaucracy. Within implementation sequencing, incident response discipline 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 service continuity requires responsibilities and review intervals that employees understand. A defensible security response is to ensure that the use of transaction verification converts broad intentions into observable operating choices.

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

security practice consequently depends on the proposition that security learning routines allows experience to alter later routines instead of remaining an isolated lesson.

The cybersecurity problem is not simply technical. It arises because security learning routines 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, user 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 security response is to ensure that service continuity requires responsibilities and review intervals that employees understand.

Digital convenience does not remove human responsibility: vendor assurance 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 security practice consequently depends on the proposition that resource scarcity makes selective experimentation more credible than organization-wide transformation.

The cybersecurity problem is not simply technical. It arises because service continuity requires responsibilities and review intervals that employees understand; in implementation sequencing, vendor assurance connects specialist knowledge with accountable managerial judgment. For this reason, short feedback cycles make correction less costly and reveal weak assumptions earlier.

Cybersecurity governance begins with the recognition that resource scarcity makes selective experimentation more credible than organization-wide transformation. Within implementation sequencing, service continuity requires responsibilities and review intervals that employees understand. Transaction accountability therefore requires that vendor assurance 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 security response is to ensure that service continuity requires responsibilities and review intervals that employees understand.

GOVERNANCE AND RISK

Cybersecurity governance begins with the recognition that resource scarcity makes selective experimentation more credible than organization-wide transformation. Within governance safeguards, incident response discipline reduces dependence on a single decision path or organizational actor. Transaction accountability therefore requires that risk-based access control establishes a disciplined starting point for cybersecurity governance in digital finance.

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 service continuity requires responsibilities and review intervals that employees understand. A defensible security response is to ensure that incident response discipline reduces dependence on a single decision path or organizational actor.

Digital convenience does not remove human responsibility: risk-based access control establishes a disciplined starting point for cybersecurity governance in digital finance. When applied to governance safeguards, the pursuit of cyber resilience develops through repeated sensing, bounded action, evaluation, and renewal. Traceable security practice consequently depends on the proposition that service continuity requires responsibilities and review intervals that employees understand.

The cybersecurity problem is not simply technical. It arises because incident response discipline 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 cyber resilience develops through repeated sensing, bounded action, evaluation, and renewal.

Cybersecurity governance begins with the recognition that service continuity 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 transaction verification 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 security practice consequently depends on the proposition that a predetermined stop condition protects continuity when an initiative no longer justifies its exposure.

The cybersecurity problem is not simply technical. It arises because transaction integrity depends on information that is relevant to the focal decision; in governance safeguards, incident response discipline reduces dependence on a single decision path or organizational actor. For this reason, the use of transaction verification converts broad intentions into observable operating choices.

Cybersecurity governance begins with the recognition that the pursuit of cyber resilience develops through repeated sensing, bounded action, evaluation, and renewal. Within governance safeguards, user confidence is strengthened when affected parties can question assumptions and explain exceptions. Transaction accountability therefore requires that transaction integrity 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 security response is to ensure that the pursuit of cyber resilience develops through repeated sensing, bounded action, evaluation, and renewal.

Digital convenience does not remove human responsibility: the use of transaction verification 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 security 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 service continuity requires responsibilities and review intervals that employees understand. A defensible security response is to ensure that transaction integrity 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 cyber resilience develops through repeated sensing, bounded action, evaluation, and renewal. Traceable security practice consequently depends on the proposition that controlled exposure improves when alternatives are compared before resources are committed.

The cybersecurity problem is not simply technical. It arises because vendor assurance 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.

Cybersecurity governance begins with the recognition that transaction integrity 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 controlled exposure improves when alternatives are compared before resources are committed. The same principle shapes performance interpretation, because vendor assurance connects specialist knowledge with accountable managerial judgment. A defensible security response is to ensure that the use of transaction verification converts broad intentions into observable operating choices.

The cybersecurity problem is not simply technical. It arises because security learning routines allows experience to alter later routines instead of remaining an isolated lesson; in performance interpretation, security learning routines allows experience to alter later routines instead of remaining an isolated lesson. For this reason, security learning routines allows experience to alter later routines instead of remaining an isolated lesson.

Cybersecurity governance begins with the recognition that controlled exposure improves when alternatives are compared before resources are committed. Within performance interpretation, controlled exposure improves when alternatives are compared before resources are committed. Transaction accountability therefore requires that controlled exposure 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 security 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: risk-based access control establishes a disciplined starting point for cybersecurity governance in digital finance. When applied to performance interpretation, risk-based access control establishes a disciplined starting point for cybersecurity governance in digital finance. Traceable security practice consequently depends on the proposition that risk-based access control establishes a disciplined starting point for cybersecurity governance in digital finance.

The cybersecurity problem is not simply technical. It arises because security learning routines allows experience to alter later routines instead of remaining an isolated lesson; in performance interpretation, security learning routines allows experience to alter later routines instead of remaining an isolated lesson. For this reason, security learning routines 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 cyber resilience develops through repeated sensing, bounded action, evaluation, and renewal. Traceable security practice consequently depends on the proposition that resource scarcity makes selective experimentation more credible than organization-wide transformation.

The cybersecurity problem is not simply technical. It arises because the use of transaction verification 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.

Cybersecurity governance begins with the recognition that security learning routines 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 risk-based access control establishes a disciplined starting point for cybersecurity governance in digital finance.

An assurance-oriented reading shows that user confidence is strengthened when affected parties can question assumptions and explain exceptions. The same principle shapes managerial and institutional implications, because vendor assurance connects specialist knowledge with accountable managerial judgment. A defensible security response is to ensure that incident response discipline 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, transaction integrity depends on information that is relevant to the focal decision. Traceable security practice consequently depends on the proposition that service continuity requires responsibilities and review intervals that employees understand.

Cybersecurity governance begins with the recognition that user confidence is strengthened when affected parties can question assumptions and explain exceptions. Within managerial and institutional implications, the pursuit of cyber 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 security 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 transaction verification converts broad intentions into observable operating choices. Traceable security practice consequently depends on the proposition that incident response discipline reduces dependence on a single decision path or organizational actor.

RESEARCH AGENDA AND CONCLUSION

The cybersecurity problem is not simply technical. It arises because risk-based access control establishes a disciplined starting point for cybersecurity governance in digital finance; 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.

Cybersecurity governance begins with the recognition that incident response discipline 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 vendor assurance connects specialist knowledge with accountable managerial judgment.

An assurance-oriented reading shows that service continuity requires responsibilities and review intervals that employees understand. The same principle shapes future research and conclusion, because vendor assurance connects specialist knowledge with accountable managerial judgment. A defensible security response is to ensure that transaction integrity depends on information that is relevant to the focal decision.

Digital convenience does not remove human responsibility: the pursuit of cyber resilience develops through repeated sensing, bounded action, evaluation, and renewal. When applied to future research and conclusion, transaction integrity depends on information that is relevant to the focal decision. Traceable security practice consequently depends on the proposition that controlled exposure improves when alternatives are compared before resources are committed.

The cybersecurity 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, controlled

exposure 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 security response is to ensure that vendor assurance 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, vendor assurance connects specialist knowledge with accountable managerial judgment. Traceable security practice consequently depends on the proposition that service continuity requires responsibilities and review intervals that employees understand.

The cybersecurity problem is not simply technical. It arises because vendor assurance connects specialist knowledge with accountable managerial judgment; in future research and conclusion, service continuity 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.