

Wawan Ichwanudin¹, Nida Garnida Fitrianti²

¹Universitas Sultan Ageng Tirtayasa, Banten, Indonesia

²Yayasan Kreatif Indonesia Emas, Bandung, Indonesia

Correspondence: ichwan0308@untirta.ac.id; NidaFitrianti@gmail.com

Abstract

Background: Digital Trust Architecture in Cooperative Commerce Platforms addresses an increasingly practical concern in digital platforms used by cooperatives and local enterprises. Organizations may introduce visible programs, digital tools, or partnership arrangements, yet outcomes remain uneven when responsibilities and feedback routines are weak. This article treats digital trust architecture as an organizational capability that must be translated into repeatable decisions rather than as a one-time initiative.

Aims: The article develops a conceptual framework linking digital trust architecture with adoption, trust, and transaction completion. It also identifies governance conditions and implementation risks that can strengthen or weaken those relationships.

Review Approach: An integrative conceptual review is used to connect established perspectives from digital transformation, technology acceptance, information governance, and platform ecosystems. The manuscript does not claim original survey, interview, experimental, or transaction data.

Results and Conclusion: The synthesis identifies four operating mechanisms—usable interface design, reliable identity and transaction records, transparent data practices, and assisted digital access—and proposes a staged pathway for diagnosis, pilot implementation, review, and scale. The central conclusion is that performance improves when information, decision rights, and learning routines are aligned with the needs of the people who use and deliver the service.

Contribution: The contribution is a practical, testable structure for assessing digital trust architecture in resource-constrained settings without assuming that technology, communication, or formal policy automatically creates capability.

Keywords: Digital Trust Architecture; Digital; Adoption; Digital Transformation; Community Development

1. INTRODUCTION

In community-oriented organizations, digital trust architecture is rarely a stand-alone technique. It is embedded in everyday decisions about information, relationships, resources, and accountability. The practical challenge is therefore not simply whether an organization adopts a new practice, but whether that practice becomes reliable enough to shape recurring behavior in digital platforms used by cooperatives and local enterprises.

The literature relevant to this problem suggests that capabilities are produced through combinations of resources, routines, and relationships rather than through isolated assets. In this article, digital trust architecture is examined through digital transformation, technology acceptance, information governance, and platform ecosystems. These perspectives are useful because they connect internal execution with external expectations and allow the analysis to consider both organizational performance and stakeholder consequences.

A further issue concerns distribution. Improvements in adoption or trust can appear positive at the organizational level while additional workload, access barriers, or uncertainty are transferred to weaker stakeholders. For that reason, the analysis does not treat performance as a single aggregate score. It asks whether gains remain credible after considering inclusion, accountability, and the practical capacity of people expected to implement the new routine.

The article addresses two questions. First, through which mechanisms can digital trust architecture influence performance in digital platforms used by cooperatives and local enterprises? Second, under what governance and resource conditions might those benefits weaken or reverse? The contribution is a framework that can guide pilot design and later empirical testing without presenting conceptual reasoning as evidence of causal impact.

2. CONCEPTUAL FOUNDATION

2.1 Defining the focal capability

This article defines digital trust architecture as a repeatable organizational capability for coordinating decisions in digital platforms used by cooperatives and local enterprises. The definition deliberately separates capability from mere presence. A policy, application, training program, or communication channel may exist without changing behavior. Capability is present when people understand the routine, information is available when needed, exceptions can be handled, and the organization can improve the process after evidence shows a recurring problem.

2.2 Theoretical lenses

Four lenses are particularly relevant: digital transformation, technology acceptance, information governance, and platform ecosystems. Together they explain why the same formal initiative can produce different outcomes. Resource and capability perspectives focus attention on what the organization can reliably do; relationship and stakeholder perspectives clarify how legitimacy and trust are formed; learning perspectives explain why repeated feedback matters; and governance perspectives show how decision rights shape implementation.

The framework therefore treats the focal capability as a bridge between managerial intent and stakeholder experience. In practical terms, managers should be able to point to observable routines such as usable interface design, reliable identity and transaction records, transparent data practices, and assisted digital access. If these routines are absent, claims about capability should be treated cautiously, even when adoption indicators appear strong.

Capability element	Diagnostic question	Expected effect	Illustrative evidence
Usable Interface Design	How consistently is usable interface design performed?	Adoption	Evidence from records, observation, and stakeholder feedback
Reliable Identity And Transaction Records	How consistently is reliable identity and transaction records performed?	Trust	Evidence from records, observation, and stakeholder feedback
Transparent Data Practices	How consistently is transparent data practices performed?	Transaction Completion	Evidence from records, observation, and stakeholder feedback
Assisted Digital Access	How consistently is assisted digital access performed?	Digital Capability	Evidence from records, observation, and stakeholder feedback

The table is diagnostic rather than prescriptive. Future empirical studies should adapt indicators to organizational size, regulation, digital maturity, and the practical meaning of 'community' in the study setting. The aim is to make the construct measurable without forcing a single operating model on diverse organizations.

2.3 Capability maturity and boundary conditions

Capability maturity can be viewed as a progression from ad hoc activity to stable routines and, eventually, adaptive routines. At an early stage, digital trust architecture may depend on a few experienced individuals. A more mature stage is reached when responsibilities are documented, information is shared, and common exceptions can be resolved without escalation. The strongest stage is not perfect standardization; it is the ability to adjust a stable process when evidence shows that stakeholder needs or operating conditions have changed.

This maturity perspective also clarifies boundary conditions. privacy concerns, digital exclusion, fragmented records, and automation without accountability can reduce the value of a formally sound process. These risks should therefore be examined alongside capability indicators rather than treated as separate compliance concerns. A mature organization makes such tensions visible and uses them to refine the operating model.

3. REVIEW APPROACH

The manuscript uses an integrative conceptual review. The purpose is theory development and practical synthesis, not estimation of an average causal effect. Sources are selected because they clarify constructs, mechanisms, and boundary conditions relevant to digital trust architecture. The review combines foundational work with later studies on organizational capability, stakeholder relationships, digitalization, service design, and community-oriented management.

3.1 Analytical procedure

The analysis proceeds in four steps. First, the focal capability is separated from adoption or activity indicators. Second, recurring mechanisms are identified at the levels of people, process, information, and relationships. Third, each mechanism is linked to operational and stakeholder outcomes. Fourth, boundary conditions are specified where an apparently positive intervention could create exclusion, dependency, hidden workload, or weak accountability.

Step	Purpose	Output
1. Construct separation	Distinguish capability from formal adoption	Working definition and observable routines
2. Mechanism mapping	Identify how the capability can produce outcomes	Mechanism-to-outcome map
3. Stakeholder check	Examine who gains, who bears cost, and who has voice	Distribution and inclusion lens
4. Boundary analysis	Identify failure conditions and governance needs	Propositions and implementation safeguards

3.2 Unit of analysis and boundaries

The focal unit is an organization or coordinated local network operating in digital platforms used by cooperatives and local enterprises. The analysis is most applicable where multiple actors must coordinate service, information, or resources. Relevant actors include members, platform administrators, frontline staff, and payment and technology partners. The framework does not assume that all actors have equal power or capability; that asymmetry is treated as an empirical condition that can influence results.

3.3 Responsible interpretation

Because the paper is conceptual, propositions are presented as expectations for future testing rather than confirmed findings. Any empirical extension should report the actual data source, sampling process, instrument, analysis, and ethics procedures where applicable. Authors and editors should also verify affiliations, correspondence details, references, and contribution statements before publication.

3.4 Evidence strategy for future empirical work

Future research should combine process evidence with outcome evidence. Process evidence can show whether usable interface design, reliable identity and transaction records, transparent data practices, and assisted digital access are actually performed, while outcome evidence can test changes in adoption, trust, transaction completion, and digital capability. Using both types of evidence reduces the risk of attributing outcomes to an initiative that was only partially implemented.

Researchers should also document the comparison period and concurrent changes. If pricing, staffing, promotion, regulation, or technology changes at the same time as the focal intervention, simple before-and-after differences should not be interpreted as proof of causality. Where feasible, phased rollouts, matched units, repeated measures, or mixed-method designs can strengthen inference while preserving contextual detail.

4. AN INTEGRATED CAPABILITY FRAMEWORK

The proposed framework links enabling conditions, four operating mechanisms, and two sets of outcomes. Enabling conditions include role clarity, usable information, appropriate skills, and governance rules. The operating mechanisms are usable interface design, reliable identity and transaction records, transparent data practices, and assisted digital access. Outcomes are assessed both inside the organization and among affected stakeholders, preventing narrow performance measures from hiding transferred costs.

4.1 Usable Interface Design

Usable Interface Design matters because it determines whether digital trust architecture can be executed under ordinary operating conditions. A useful test is whether staff and partners can explain the sequence, locate the required information, identify who owns an exception, and learn from a repeated failure. When these conditions are present, the mechanism can support adoption without relying on heroic individual effort.

4.2 Reliable Identity And Transaction Records

Reliable Identity And Transaction Records matters because it determines whether digital trust architecture can be executed under ordinary operating conditions. A useful test is whether staff and partners can explain the sequence, locate the required information, identify who owns an exception, and learn from a repeated failure. When these conditions are present, the mechanism can support trust without relying on heroic individual effort.

4.3 Transparent Data Practices

Transparent Data Practices matters because it determines whether digital trust architecture can be executed under ordinary operating conditions. A useful test is whether staff and partners can explain the sequence, locate the required information, identify who owns an exception, and learn from a repeated failure. When these conditions are present, the mechanism can support transaction completion without relying on heroic individual effort.

4.4 Assisted Digital Access

Assisted Digital Access matters because it determines whether digital trust architecture can be executed under ordinary operating conditions. A useful test is whether staff and partners can explain the sequence, locate the required information, identify who owns an exception, and learn from a repeated failure. When these conditions are present, the mechanism can support digital capability without relying on heroic individual effort.

Operating mechanism	Primary outcome	Boundary risk
Usable Interface Design	Adoption	Privacy Concerns
Reliable Identity And Transaction Records	Trust	Digital Exclusion
Transparent Data Practices	Transaction Completion	Fragmented Records
Assisted Digital Access	Digital Capability	Automation Without Accountability

4.5 Interaction among mechanisms

The four mechanisms are mutually dependent. Usable Interface Design can create a clear starting point, but it will not sustain performance if reliable identity and transaction records is weak or if information is lost when responsibility moves between actors. Likewise, assisted digital access has little value when lessons are collected but never translated into changes in rules, staffing, or resource allocation.

This interaction suggests that managers should diagnose the weakest connection rather than improve every component simultaneously. In digital platforms used by cooperatives and local enterprises, a targeted correction to one bottleneck can be more effective than a broad technology investment. The framework therefore supports staged capability building: stabilize the basic routine, make evidence visible, close recurrent exceptions, and only then expand the operating scope.

5. STAKEHOLDER, GOVERNANCE, AND INCLUSION CONDITIONS

5.1 Stakeholder roles

Implementation requires explicit roles for members, platform administrators, frontline staff, and payment and technology partners. The strongest arrangements make responsibilities visible at the point where work occurs. For example, the actor who receives a complaint, verifies a record, approves an exception, or communicates a change should know what evidence is required and when responsibility transfers to another role. Ambiguity at handoffs often creates more friction than the absence of technology.

5.2 Governance as an operating condition

Governance should be proportionate to risk. In the context of digital trust architecture, this means clear decision rights, transparent criteria, reviewable records, and an escalation route for unusual cases. Governance is not synonymous with additional bureaucracy. A small organization may need only a short rule set and a disciplined review rhythm, provided those rules are consistently used and exceptions are visible.

5.3 Inclusion and distribution

A community orientation adds a distributional question: who can participate and who bears the cost of coordination? A process may improve average efficiency while making access harder for people with limited digital skills, time, transport, or bargaining power. Managers should therefore examine assisted pathways, workload distribution, and whether smaller partners can meet requirements without disproportionate cost.

Risk	Early signal	Response principle	Primary actor
Privacy Concerns	Monitor whether privacy concerns appears during routine delivery	Assign an owner, document the exception, and review recurring patterns	Members
Digital Exclusion	Monitor whether digital exclusion appears during routine delivery	Assign an owner, document the exception, and review recurring patterns	Platform Administrators
Fragmented Records	Monitor whether fragmented records appears during routine delivery	Assign an owner, document the exception, and review recurring patterns	Frontline Staff
Automation Without Accountability	Monitor whether automation without accountability appears during routine delivery	Assign an owner, document the exception, and review recurring patterns	Payment And Technology Partners

These controls protect the community objective of the model. They also improve managerial learning because problems become observable and comparable over time rather than remaining informal stories. For digital trust architecture, this is particularly important when the organization relies on multiple channels, partners, or volunteer and part-time roles.

5.4 Safeguards and grievance mechanisms

A workable grievance mechanism need not be complex. Participants should know where to raise a concern, what information is required, who reviews it, and how long a response should take. The organization should distinguish between isolated dissatisfaction and patterns that reveal a process defect. Aggregated patterns should be reviewed at management level because they often expose unclear rules, workload imbalances, or unintended exclusion.

Safeguards are especially important where privacy concerns or fragmented records could create unequal consequences. Transparent escalation criteria and an exit option can reduce dependency without undermining operational discipline. The objective is not to eliminate disagreement but to ensure that affected actors have a credible route to explanation, correction, and learning.

6. PERFORMANCE AND LEARNING ARCHITECTURE

Performance should be measured as a linked scorecard rather than a collection of activity counts. For digital trust architecture, the relevant outcome portfolio includes adoption, trust, transaction completion, digital capability, and platform retention. Activity measures can still be useful—for example, number of participants, messages, training sessions, or transactions—but they should be connected to evidence that the underlying capability is becoming more reliable.

6.1 Operational measures

Operational measures should capture completion, accuracy, cycle time, exception frequency, and closure. Denominators must be explicit so that improvements are not created by selective reporting. Where data are limited, small organizations can use weekly samples and exception logs rather than building an expensive dashboard. Consistency and follow-up are more important than metric volume.

6.2 Stakeholder and relationship measures

Relationship measures should test whether stakeholders experience the intended benefit. Depending on the setting, this may include trust, repeat participation, perceived fairness, access, satisfaction, or willingness to recommend. Qualitative evidence remains useful because transaction records rarely explain hidden work, exclusion, or why people disengage.

6.3 Learning measures

Learning measures ask whether recurring evidence changes routines. Useful indicators include the time between identifying a repeated problem and implementing a verified correction, the proportion of corrective actions closed, the degree to which new staff can execute the process independently, and whether partners receive feedback they can use.

Layer	Illustrative metric	Decision supported
Reliability	Share of cases completed as promised	Is the routine stable enough to scale?
Relationship	Adoption	Do stakeholders experience the intended benefit?
Efficiency	Cycle time and avoidable rework	Where is coordination cost accumulating?
Learning	Days from recurring issue to verified process change	Does evidence improve the operating model?
Inclusion	Completion and access by participant group	Who is being left behind?

6.4 Interpreting the scorecard

The scorecard should be read as a set of connected signals. A rise in adoption is encouraging, but it may not represent sustainable progress if cycle time deteriorates, staff rework increases, or access becomes more difficult for some stakeholder groups. Managers should therefore look for movement across several layers rather than celebrating one favorable indicator in isolation.

Baseline discipline is equally important. Measures should be defined before the pilot wherever possible, including the denominator, data source, owner, and review frequency. When data quality is weak, the organization should acknowledge the limitation and use a smaller set of reliable measures rather than creating false precision from inconsistent records.

7. PROPOSITIONS FOR EMPIRICAL TESTING

P1. Stronger usable interface design will be positively associated with adoption, provided responsibilities and information are clear.

P2. Stronger reliable identity and transaction records will improve trust when records are timely and comparable across actors.

P3. Transparent Data Practices will strengthen transaction completion when affected stakeholders have a workable role in implementation.

P4. Assisted Digital Access will improve digital capability when recurring exceptions are reviewed and converted into process changes.

P5. Transparent governance will strengthen the relationship between digital trust architecture and adoption by reducing ambiguity and perceived unfairness.

P6. Inclusion safeguards will moderate the effect of digital trust architecture on stakeholder outcomes by reducing barriers for participants with lower resources or digital readiness.

Proposition	Primary predictor	Expected outcome	Boundary condition
P1	Usable Interface Design	Adoption	Privacy Concerns
P2	Reliable Identity And Transaction Records	Trust	Digital Exclusion
P3	Transparent Data Practices	Transaction Completion	Fragmented Records
P4	Assisted Digital Access	Digital Capability	Automation Without Accountability
P5	Transparent governance	Platform Retention	Privacy Concerns
P6	Inclusion safeguards	Adoption	Digital Exclusion

A multilevel design is appropriate because operating reliability, staff capability, and stakeholder outcomes can change at different speeds. Researchers should specify the level of each variable and avoid combining individual perceptions, organizational records, and network outcomes into a single index without a clear theoretical justification.

7.1 Research design implications

The propositions can be tested sequentially. Early studies may focus on whether the mechanisms are distinguishable and measurable in digital platforms used by cooperatives and local enterprises. Later work can examine mediation and moderation, for example whether transparent governance strengthens the effect of usable interface design on adoption, or whether inclusion safeguards reduce adverse effects for less-resourced participants.

Longitudinal designs are particularly useful because capability development is cumulative. A cross-sectional survey may capture perceptions of the current system but cannot show whether repeated learning has improved the routine. Panel data, repeated process audits, or case-based time series can reveal whether corrections persist after initial management attention declines.

Measurement should also separate implementation fidelity from outcome strength. An intervention that is faithfully implemented but produces weak outcomes raises a theoretical question about the mechanism. An intervention that is only partially implemented raises a different managerial question. Treating those situations as equivalent would make both research findings and practical recommendations less precise.

8. A STAGED IMPLEMENTATION PATHWAY

Organizations should begin with a specific friction point rather than a broad transformation slogan. For digital trust architecture, a pilot is most useful when the problem is visible, responsibilities can be named, and baseline evidence is available. A staged approach protects scarce resources and creates deliberate decision points before scale.

Stage	Core work	Evidence before progression
1. Diagnose	Map the current process, stakeholders, failures, and baseline measures	Named problem owner and agreed scope
2. Standardize	Clarify definitions, responsibilities, records, and service rules	Staff can explain and execute the routine
3. Pilot	Test the change with limited users, geography, or service scope	Reliable completion and visible unit economics
4. Learn	Review operational, stakeholder, workload, and inclusion evidence	Documented corrective actions and unresolved risks
5. Scale	Expand only elements that remain reliable and beneficial	Capacity, governance, and support controls ready

8.1 Choosing the pilot

A useful pilot for digital trust architecture should be small enough to observe closely but important enough that participants care about the result. Scope can be limited by product, member segment, service type, location, or time period. The pilot should also state what will not be attempted, which reduces pressure to solve every adjacent problem at once.

8.2 Review rhythm

A simple governance rhythm is usually sufficient: a short weekly operational review, a monthly scorecard that includes stakeholder and workload measures, and a periodic decision on whether to scale, redesign, pause, or discontinue. The key discipline is closure. An issue that appears repeatedly without a named owner is evidence that the learning system is incomplete.

8.3 Capability transfer

External advisers, technology providers, or partner institutions can accelerate implementation, but the operating organization should gradually acquire the ability to execute and improve the routine independently. Capability transfer is visible when local staff can explain the logic, diagnose common exceptions, and make justified adjustments without permanent dependence on an outside operator.

8.4 Scale, redesign, or pause

Scale should be treated as a decision, not as the default reward for completing a pilot. Expansion is justified when service reliability, stakeholder outcomes, resource requirements, and governance controls remain acceptable together. If privacy concerns or digital exclusion intensifies as volume grows, redesign may be more responsible than immediate expansion.

A pause can also be productive. It creates time to repair data definitions, staffing assumptions, partner agreements, or inclusion barriers before they become embedded in a larger system. Discontinuation is appropriate when the model cannot meet its stated objective at an acceptable level of cost and risk. Learning from a discontinued pilot should be documented so that the organization does not repeat the same failure under a new label.

9. DISCUSSION

The framework shifts attention from adoption to operating capability. This distinction matters because a visible initiative may exist without producing a stable routine. The proposed relationships therefore emphasize mechanisms and boundary conditions rather than assuming that the presence of a program is equivalent to its effectiveness.

9.1 Theoretical implications

The first implication is that digital trust architecture should be treated as a capability with observable mechanisms rather than a label attached to a project. This makes it possible to distinguish weak adoption from strong execution. The second implication is that stakeholder and governance conditions moderate performance: privacy concerns or digital exclusion can interrupt an otherwise plausible pathway from practice to outcome.

The framework also connects organizational and community levels. Improvements in adoption are valuable, but they should be interpreted alongside access, workload, voice, and capability distribution. This is especially important in community settings where the same people can be members, customers, workers, suppliers, or volunteers at different points in the process.

9.2 Managerial implications

Managers should begin by identifying the most important recurring decision linked to digital trust architecture, then ask what information, authority, and capability are required to make that decision well. Investment should follow the bottleneck. If records are unreliable, another digital channel may multiply errors. If responsibility is unclear, additional reporting can document problems without resolving them.

A balanced scorecard should therefore combine reliability, relationship, efficiency, learning, and inclusion. Managers should also make boundary risks visible, particularly privacy concerns, digital exclusion, fragmented records, and automation without accountability. These risks are not arguments against implementation; they are design conditions that help prevent a well-intended initiative from producing hidden costs.

9.3 Limitations and research agenda

This article is conceptual and does not estimate causal effects. The review is purposeful rather than exhaustive, and the proposed indicators require validation in specific sectors and regions. Future studies can use longitudinal case designs, surveys, comparative field studies, process observation, or mixed methods. Where feasible, researchers should document concurrent changes in price, staffing, technology, regulation, or market conditions so that outcomes are not attributed to the focal capability without adequate evidence.

9.4 Practical research agenda

A practical next step is to develop short, context-sensitive measurement instruments for digital trust architecture. These instruments should combine observable process indicators with stakeholder perceptions rather than relying on perception scales alone. Comparative studies could then examine whether the same mechanisms operate differently across cooperatives, social enterprises, public programs, and community-based organizations.

Future work should also examine distributional effects over time. Average improvements may conceal who gained access, who lost bargaining power, whose workload increased, or which participants exited. Reporting these patterns would strengthen the relevance of community-oriented management research and help practitioners distinguish genuine capability building from short-lived performance improvements.

10. CONCLUSION

Digital Trust Architecture in Cooperative Commerce Platforms is best understood as an operating capability rather than a discrete intervention. The framework developed in this article proposes that digital trust architecture creates stronger outcomes when organizations coordinate usable interface design, reliable identity and transaction records, transparent data practices, and assisted digital access, while maintaining transparent governance and workable access for affected stakeholders. The resulting performance should be evaluated through both organizational and community-level evidence.

For practitioners, the practical starting point is one recurring decision, one clearly defined stakeholder problem, and a small set of measures that can be reviewed consistently. For researchers, the six propositions provide a basis for empirical testing across different organizational forms. The central discipline is to connect claims of improvement with observable routines, boundary conditions, and evidence of learning over time.

The broader implication is that community-oriented management should be judged by the durability and distribution of capability, not only by visible activity. When digital trust architecture is supported by clear roles, useful evidence, fair governance, and a credible learning loop, organizations are better positioned to improve performance without weakening the relationships on which local value creation depends.

This conclusion remains conditional until tested empirically. The framework is intended to guide better questions, clearer measurement, and more disciplined pilots. It should be refined when evidence from specific sectors contradicts or qualifies the proposed relationships.

REFERENCES

- Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *Journal of Strategic Information Systems*, 28(2), 118–144.
- Verhoef, P. C., et al. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, 122, 889–901.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340.
- Rogers, E. M. (2003). *Diffusion of Innovations* (5th ed.). Free Press.
- OECD. (2021). *The Digital Transformation of SMEs*. OECD Publishing.
- Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99–120.
- Freeman, R. E. (1984). *Strategic Management: A Stakeholder Approach*. Pitman.
- Teece, D. J. (2007). Explicating dynamic capabilities. *Strategic Management Journal*, 28(13), 1319–1350.
- Prahalad, C. K., & Ramaswamy, V. (2004). Co-creation experiences: The next practice in value creation. *Journal of Interactive Marketing*, 18(3), 5–14.
- Ostrom, E. (2010). Beyond markets and states: Polycentric governance of complex economic systems. *American Economic Review*, 100(3), 641–672.
- Putnam, R. D. (1993). *Making Democracy Work*. Princeton University Press.
- Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a theory of stakeholder identification and salience. *Academy of Management Review*, 22(4), 853–886.
- Eisenhardt, K. M., & Martin, J. A. (2000). Dynamic capabilities: What are they? *Strategic Management Journal*, 21(10/11), 1105–1121.
- Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory*, 18(4), 543–571.
- Kotter, J. P. (1995). Leading change: Why transformation efforts fail. *Harvard Business Review*, 73(2), 59–67.
- Granovetter, M. (1985). Economic action and social structure: The problem of embeddedness. *American Journal of Sociology*, 91(3), 481–510.
- Bryson, J. M. (2004). What to do when stakeholders matter. *Public Management Review*, 6(1), 21–53.
- Scott, W. R. (2014). *Institutions and Organizations: Ideas, Interests, and Identities* (4th ed.). Sage.