

ORIGINAL RESEARCH

Open access

Managing Digital Ecosystem Dependence: A Governance Framework for Firms Using Cloud Platforms, AI Vendors, and Data Intermediaries

Nokuthula Dlamini^{1*}, Siphso Zulu¹

Abstract

Modern firms increasingly rely on external digital ecosystems to access infrastructure, artificial intelligence, data, and analytical capabilities that are difficult to build entirely in house. Cloud platforms, AI vendors, and data intermediaries now support core business operations rather than peripheral technical functions. This shift has expanded firm capabilities, but it has also created new forms of dependence. The central problem addressed in this article is that digital ecosystem dependence is often governed through fragmented IT, procurement, compliance, and legal processes. These arrangements can manage service delivery and contractual performance, but they are less suited to strategic vulnerabilities such as lock-in, opacity, bargaining asymmetry, data control loss, and exit difficulty. As a result, firms may become operationally efficient while becoming strategically constrained. The objective of this article is to develop a Digital Ecosystem Governance Framework for firms that depend on cloud platforms, AI vendors, and data intermediaries. The framework identifies the distinct dependence risks associated with each ecosystem partner type and integrates them into a unified governance logic. It treats dependence as a strategic management issue rather than a narrow technology sourcing problem. The proposed framework shows that effective governance of digital ecosystem dependence requires three interrelated capabilities: dependency risk assessment, protective governance mechanisms, and strategic governance oversight. Firms need contractual safeguards, technical portability, internal capability building, vendor diversification, data control mechanisms, and board-level visibility over dependence thresholds. The article contributes a governance-oriented perspective on how firms can use external digital ecosystems without becoming strategically captured by them.

Keywords Strategic risk, Digital ecosystem dependence, Cloud platforms, AI vendors, Data intermediaries, Governance framework

*Correspondence:

Nokuthula Dlamini
dlaminin@ukzn.ac.za

¹ Department of Digital Business Systems, Faculty of Commerce, University of KwaZulu-Natal, Durban, South Africa

Introduction

Firms increasingly compete through digital services that are embedded in external platforms, infrastructures, and data networks rather than fully owned internal systems. Platform ecosystem research shows that value creation often depends on complementarities among multiple actors, yet these complementarities also reshape firm boundaries and control over strategic resources [1]. Digital platforms allow

firms to scale innovation, access external capabilities, and connect with ecosystem partners, but they also expose firms to governance problems that are not captured by conventional internal hierarchy or market contracting models [2].

Digital ecosystem dependence becomes strategically significant when firms cannot easily substitute, exit, or internally reproduce the capabilities supplied by external

digital partners. Platform-based ecosystems can invert traditional firm control because external providers may own the interfaces, standards, data flows, and rules through which dependent firms operate [3]. The issue is therefore not only whether firms obtain reliable digital services, but whether they retain sufficient bargaining power, architectural flexibility, and strategic autonomy as their operations become ecosystem-embedded.

Existing IT governance and procurement practices often divide digital dependence into separate categories such as infrastructure contracting, vendor selection, data compliance, and software risk management. However, ecosystem theory suggests that interdependence, role allocation, and value capture are structurally linked across digital networks [4]. When governance remains fragmented, firms may negotiate cloud contracts, AI service agreements, and data partnerships separately while missing the cumulative strategic exposure created by their combined dependence.

This article addresses that gap by proposing a Digital Ecosystem Governance Framework for firms using cloud platforms, AI vendors, and data intermediaries. The framework draws on research showing that ecosystems broaden the locus of value creation beyond the firm while requiring new coordination and governance arrangements [5]. Its aim is to help managers identify dependence risks, compare risks across partner types, and design governance mechanisms that preserve strategic flexibility while still benefiting from external digital capabilities.

Digital Ecosystem Dependence

Digital ecosystem dependence refers to a strategic condition in which a firm's critical operations, innovation processes, analytics, customer interactions, or data assets rely on external digital actors whose resources cannot be easily replaced. Dynamic capability research suggests that firms benefit from digital platform ecosystems when they can integrate external resources with internal capabilities, but this integration also increases dependence on ecosystem architectures and partner decisions [6]. Dependence therefore emerges not simply from outsourcing, but from the embedding of firm routines, data, and decision processes within externally governed digital environments.

The strategic risk of dependence is intensified because digital platforms and infrastructures define interfaces, technical standards, access rules, and monetisation mechanisms. Research on digital platforms and infrastructures highlights that firms operate through layered architectures that are simultaneously enabling and constraining [7]. A dependent firm may gain speed and scale from external platforms while losing architectural discretion over migration, interoperability, data portability, and downstream innovation options.

Digital ecosystem dependence has multiple dimensions that should be distinguished analytically. The digital platform literature emphasises that platforms differ from traditional information systems because they support distributed innovation, network effects, and evolving ecosystem governance [8]. **Table 1** categorises the dimensions and risks of digital ecosystem dependence. This categorisation clarifies why dependence should be assessed across operational continuity, financial exposure, strategic autonomy, data control, regulatory risk, and reputational vulnerability rather than reduced to vendor performance alone.

Table 1. Digital Ecosystem Dependence: Dimensions, Sources, and Strategic Risks for Dependent Firms

Dependence dimension	Main source of dependence	Typical ecosystem partner	Strategic risk for dependent firms
Operational dependence	Critical business processes run through external digital infrastructure	Cloud platforms, software platforms, analytics platforms	Service disruption, reduced continuity, limited fallback capacity
Architectural dependence	Firm systems are built around proprietary interfaces, APIs, or technical standards	Cloud platforms, AI vendors	Lock-in, switching difficulty, integration rigidity

Analytical dependence	Decisions rely on externally supplied models, algorithms, or scoring systems	AI vendors, analytics providers	Algorithm opacity, model drift, biased outputs, reduced internal judgement
Data dependence	Data is sourced, enriched, stored, or interpreted by external intermediaries	Data brokers, data aggregators, data marketplaces	Data quality uncertainty, provenance risk, privacy exposure, loss of strategic data control
Financial dependence	Pricing, egress costs, subscription structures, and usage fees shape switching choices	Cloud platforms, AI vendors	Escalating costs, bargaining weakness, economic unattractiveness, exit costs
Strategic dependence	Competitive capabilities become tied to external ecosystem rules and partner priorities	Cloud platforms, AI vendors, data intermediaries	Loss of autonomy, reduced differentiation, vulnerability to partner strategy changes
Reputational dependence	External failures or misuse affect the focal firm's legitimacy	AI vendors, data intermediaries, cloud platforms	Customer distrust, regulator scrutiny, brand damage

Digital ecosystem dependence is especially important because digital transformation has changed the location of innovation and entrepreneurship from firm-owned assets toward externally connected platforms and services.

Research on digital innovation shows that digital technologies make resources more generative and recombining, but they also create new coordination challenges across organisational boundaries [9]. For managers, this means that dependence should be governed as a portfolio of strategic exposures rather than as isolated technology contracts.

Cloud Platform Dependence

Cloud platform dependence arises when firms rely on hyperscale providers for infrastructure, platform services, software environments, storage, security tools, and advanced analytics capabilities. Global platform research suggests that large digital platforms can become central coordination structures across markets and industries, which increases their influence over dependent firms' international and strategic choices [10]. In cloud contexts, this influence can appear through proprietary services, pricing models, certification requirements, data location rules, and ecosystem-specific development practices.

Cloud dependence is not inherently negative because cloud platforms provide scalability, resilience, security investment, and access to technical capabilities that many firms cannot efficiently develop alone. However, research on platform-dependent entrepreneurship shows that dependence creates power asymmetries when external platforms control access, visibility, technical rules, and the terms of value capture [11]. For firms using cloud services, similar asymmetries can emerge when migration costs are high, workloads are deeply integrated into proprietary services, and bargaining power is concentrated with a small number of hyperscalers.

Cloud platform dependence is also shaped by the boundaries of digital platforms and the interfaces through which firms connect to them. Platform boundary research shows that firm scope, platform sides, and digital interfaces interact in ways that affect governance and control [12]. **Table 2** identifies the specific governance challenges and risk factors of cloud platform dependence. The table highlights that cloud governance must address not only uptime and service-level performance, but also lock-in mechanisms, contractual leverage, data portability, security responsibility, and exit readiness.

Table 2. Cloud Platform Dependence: Governance Challenges, Lock-In Mechanisms, and Mitigation Strategies

Cloud dependence issue	Lock-in or risk mechanism	Governance challenge	Mitigation strategy
Proprietary cloud services	Applications depend on provider-specific databases, analytics tools, or serverless functions	Switching becomes technically complex and costly	Use modular design, containerisation, open standards, and portability reviews
Data egress and migration costs	Large data volumes become expensive to move out of the platform	Exit is economically unattractive even when technically feasible	Negotiate egress terms, classify portable data, and move exit costs in advance
Integrated security tooling	Security monitoring and identity management are tied to one provider's ecosystem	Firm may lose independent security visibility	Maintain independent security logs, third-party monitoring, and shared-responsibility audits
Service concentration	Core systems depend on one cloud provider or region	Outage or provider failure affects business continuity	Build resilient architecture, backup environment, and recovery playbooks
Contractual asymmetry	Standardised cloud terms limit negotiation leverage	Firm accepts terms that weaken audit, liability, or termination rights	Prioritise negotiable clauses for critical workloads and create escalation routes
Skills dependence	Internal teams specialise in one provider's	Capability becomes provider-specific rather than transferable	Invest in multi-cloud literacy, architecture documentation, and cross-provider training

	tools and certifications		
Strategic roadmap dependence	Firm innovation follows the provider's service roadmap	Digital strategy becomes indirectly shaped by cloud vendor priorities	Review cloud roadmap dependence during strategy cycles and maintain alternative technology options

Effective cloud governance therefore requires firms to move beyond narrow vendor administration and toward managed ecosystem participation. Research on managed ecosystems emphasises that value creation and capture require deliberate coordination among firms, communities, and ecosystem actors rather than passive reliance on external platforms [13]. For cloud-dependent firms, this means treating cloud architecture, contract design, capability development, and exit planning as integrated governance concerns rather than separate IT tasks.

AI Vendor Dependence

AI vendor dependence arises when firms rely on external providers for machine learning models, automated decision systems, generative AI services, model hosting, training pipelines, or vendor-specific APIs. Cloud provider management research shows that digital service dependence requires contingency-sensitive governance processes rather than uniform outsourcing routines [14]. This logic is even more important for AI vendors because dependence may involve not only technical service delivery, but also model behaviour, data access, intellectual property, and decision accountability.

AI vendor dependence differs from traditional software outsourcing because the purchased capability may be probabilistic, adaptive, and difficult to inspect directly. Research on artificial intelligence as a service shows that organisations increasingly acquire AI capabilities through external service models, creating dependence on vendor infrastructure, model updates, embedded analytics, and platform-specific development environments [15]. The dependent firm may gain rapid AI functionality but lose visibility into how models are trained, validated, updated, and aligned with organisational goals.

The governance challenge is intensified by algorithmic opacity and the managerial difficulty of evaluating AI systems without internal expertise. Research on managing artificial intelligence emphasises that AI changes organisational decision-making because it requires new forms of accountability, learning, and human oversight [16]. When vendors control model architecture, training data, performance monitoring, and update cycles, firms may struggle to detect drift, bias, declining accuracy, or misalignment between vendor optimisation and firm-specific risk tolerance.

AI vendor dependence should therefore be governed through a combination of contractual, technical, and organisational mechanisms. Legal and policy research on AI as a service highlights the importance of clarifying responsibilities, liabilities, and accountability when AI capabilities are supplied by external providers [17]. Firms should negotiate model audit rights, data ownership clauses, explanation requirements, update notification obligations, intellectual property protections, human review procedures, and internal AI literacy programs so that vendor dependence does not become organisational ignorance.

Data Intermediary Dependence

Data intermediary dependence emerges when firms rely on brokers, aggregators, marketplaces, data-sharing platforms, or analytics intermediaries to access, enrich, verify, or interpret data. Data governance research defines data governance as a system of decision rights and accountabilities for data-related processes, which makes it directly relevant when critical data assets are partially controlled outside the firm [18]. In this setting, dependence is not only about obtaining data, but about trusting external actors to shape the quality, legality, provenance, and strategic meaning of that data.

The dependence risk is particularly acute because data intermediaries can sit between firms and the data sources that inform customers, markets, supply chains, or risk assessments. Research on data intermediaries shows that these actors perform brokerage and facilitation roles in data ecosystems, but their position can also influence access, interpretation, and control [19]. When firms depend on intermediaries for data inputs, they may lose direct visibility into collection conditions, consent arrangements,

transformation methods, and potential biases embedded in supplied datasets.

Data broker research further indicates that intermediaries can operate in ways that are difficult for users, regulators, and dependent firms to observe fully. Studies of data brokers in surveillance capitalism show that data aggregation can generate opacity, privacy risks, and transnational governance challenges [20]. **Table 3** summarises the dependence risks and governance needs related to data intermediaries. The table clarifies why firms must govern provenance, quality, privacy compliance, contractual reuse rights, and strategic data control rather than simply buying data as a commodity.

Table 3. Data Intermediary Dependence: Risk Dimensions, Control Loss Mechanisms, and Governance Requirements

Risk dimension	Control loss mechanism	Consequence for dependent firms	Governance requirement
Data provenance risk	Firm cannot fully verify how data was collected, transformed, or licensed	Legal exposure, weak auditability, poor trust in downstream analytics	Provenance transparency and documentation
Data quality risk	Intermediary supplies incomplete, outdated, duplicated, or biased data	Poor decisions, model error, reputational harm	Quality assurance and validation
Privacy compliance risk	Consent, purpose limitation, or cross-border transfer conditions are unclear	Regulatory penalties and customer trust loss	Privacy warranties, compliance verification
Strategic data control risk	Firm becomes dependent on external data assets it cannot	Loss of differentiation and bargaining leverage	Internal data capability development

	reproduce internally		
Reuse and resale risk	Intermediary retains broad rights over data use or onward sharing	Competitive leakage and unclear ownership boundaries	Contractual restrictions on reuse and onward transfer
Analytical interpretation risk	Intermediary controls classifications, scores, enrichment logic, or segmentation	Hidden assumptions shape firm decisions	Methodological transparency
Ecosystem concentration risk	Few intermediaries control access to important data categories	Reduced bargaining power and higher switching costs	Supplier diversification and substitution planning

Data intermediary dependence also has a regulatory and market-order dimension because intermediaries increasingly mediate structured data sharing across sectors. Research on the Data Governance Act and data intermediation shows that new legal frameworks may both enable and constrain data intermediary roles in data markets [21]. For managers, this means that governance must combine contractual safeguards with regulatory monitoring and internal data strategy, especially where intermediaries influence data access and competitive positioning.

Proposed Digital Ecosystem Governance Framework

The proposed Digital Ecosystem Governance Framework is built around three pillars: dependency risk assessment, protective governance mechanisms, and strategic governance oversight. Research on formal and relational governance in AI outsourcing shows that firms need both contractual controls and trust-based coordination when external providers supply complex digital capabilities [22]. This article extends that logic across cloud platforms, AI vendors, and data intermediaries by treating dependence

as a cross-domain governance problem rather than a set of unrelated sourcing decisions.

The first pillar, dependency risk assessment, requires firms to map critical dependencies, classify partner-specific risks, measure substitutability, and monitor cumulative exposure across cloud, AI, and data relationships. Research on AI governance identifies best practices and barriers related to accountability, transparency, oversight, and organisational readiness [23]. Applied more broadly, these governance concerns imply that firms should maintain dependency registers, assess switching difficulty, monitor model and data risks, and connect vendor exposure to enterprise risk management.

The second pillar, protective governance mechanisms, focuses on contractual protections, technical portability, multi-vendor options, data control, audit rights, and internal capability building. Research on artificial intelligence capability shows that firms benefit when AI resources are combined with organisational capabilities rather than merely acquired as external tools [24]. Table 4 presents the proposed Digital Ecosystem Governance Framework. The framework shows how general governance principles can be translated into dependence-specific mechanisms for cloud platforms, AI vendors, and data intermediaries.

Table 4. Digital Ecosystem Governance Framework: Principles, Components, and Dependence-Specific Governance Mechanisms

Framework pillar	Governance principle	Cloud platform mechanisms	AI vendor mechanism
Dependency risk assessment	Make dependence visible before it becomes irreversible	Map critical workloads, proprietary services, regions, egress exposure, and recovery gaps	Map vendor models, APIs, training data access, update cycles, and decision use cases
Protective governance mechanisms	Reduce lock-in and preserve control	Use modular architecture, portability standards, multi-cloud options, and	Negotiate audit rights, explainability, model validation, data ownership,

		exit-tested contracts	and update controls
Strategic governance oversight	Treat dependence as an enterprise-level strategic risk	Set cloud concentration limits and review platform roadmap exposure	Define AI risk appetite and require human accountability for high-impact uses
Internal capability building	Avoid capability hollowing caused by excessive external reliance	Develop architecture literacy and cloud-independent operational knowledge	Build internal AI literacy, validation skills, and model risk management capacity
Exit and continuity readiness	Prepare for disruption, regulatory change, or partner failure	Maintain backup environments, migration documentation, and recovery playbooks	Maintain fallback decision processes and alternative model options
Relational governance	Coordinate with partners while preserving firm interests	Establish executive cloud governance reviews and escalation paths	Create model performance review routines and joint accountability forums
Governance learning	Use incidents and reviews to update dependence controls	Review outages, cost escalation, and migration constraints	Review model drift, bias incidents, and vendor update effects

The third pillar, strategic governance oversight, places digital ecosystem dependence within board-level and executive risk management rather than leaving it solely to technology teams. Recent research on data intermediaries and data intermediation services shows that intermediary roles are evolving and becoming more specialised, which increases the need for managerial understanding of ecosystem positions and control points [25]. The framework therefore requires senior managers to define acceptable

dependence thresholds, identify non-substitutable partners, and decide which digital capabilities must remain internally governable.

Figure 1 presents the proposed Digital Ecosystem Governance Framework for managing firm dependence on cloud platforms, AI vendors, and data intermediaries.

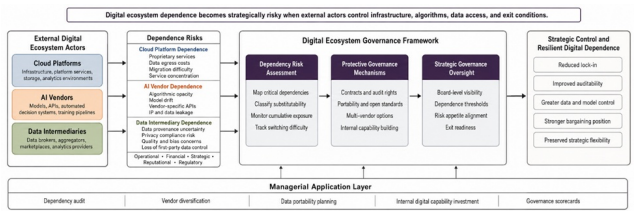


Figure 1. Digital Ecosystem Governance Framework for Managing Cloud Platform, AI Vendor, and Data Intermediary Dependence

Risk Mitigation and Managerial Application

Managers can apply the framework by beginning with a dependency audit that identifies which operations, data flows, models, interfaces, and customer-facing services depend on external digital actors. Open data intermediary research shows that intermediaries can contribute to data ecosystems, but their value depends on the roles they perform and the governance conditions surrounding those roles [26]. A dependency audit should therefore evaluate not only the presence of vendors, but also the degree to which each vendor controls continuity, data access, model interpretation, or strategic differentiation.

The second application step is vendor diversification, but diversification should be selective rather than symbolic. Cloud, AI, and data partners differ in substitutability, integration complexity, and risk profile, so managers should prioritise diversification where single-partner exposure threatens mission-critical continuity or strategic autonomy [27]. In practice, this means distinguishing between relationships that require full redundancy, relationships that require negotiated exit rights, and relationships where internal capability development is the more realistic mitigation strategy.

The third application step is in-house capability investment, because governance is weak when firms lack the knowledge to evaluate vendor claims. Research on cloud

vendor lock-in prediction and multi-cloud environments shows that lock-in can be assessed and mitigated through more systematic evaluation of technical dependence and placement choices [28, 29]. Similarly, firms should maintain internal expertise in cloud architecture, AI validation, data governance, privacy compliance, and contract interpretation so that external partners remain governed suppliers rather than invisible decision-makers.

The fourth application step is the creation of governance scorecards that translate dependence risk into recurring managerial review. Research on data market ordering argues that data intermediaries must be integrated into governance arrangements that shape data sharing and market accountability [30]. A practical scorecard should track concentration, portability, auditability, data provenance, privacy exposure, model transparency, exit feasibility, and internal capability depth, allowing executives to review digital dependence as part of strategic risk governance.

Limitations

The first limitation is that the framework is conceptual and has not yet been empirically tested across firms, industries, or regulatory environments. Ecosystem theory provides a strong foundation for understanding interdependence and role structure, but empirical research is needed to examine how firms actually measure and govern dependence in cloud, AI, and data intermediary relationships [4]. Future studies could test whether firms that apply dependency assessment, protective governance, and strategic oversight experience lower switching costs, fewer governance failures, or stronger digital resilience.

The second limitation is that the framework may simplify the heterogeneity of cloud platforms, AI vendors, and data intermediaries. Platform and infrastructure research shows that digital systems vary in architecture, governance, modularity, and ecosystem dynamics, which means that dependence mechanisms may differ substantially across provider types and technical layers [7]. For example, dependence on a cloud storage provider is not identical to dependence on a foundation model API, and dependence on a regulated data-sharing intermediary is not identical to dependence on an opaque commercial data broker.

The third limitation is that firm size, industry context, regulation, and internal digital maturity may moderate the

feasibility of the proposed governance mechanisms. Research on digital transformation indicates that firms differ in their ability to integrate digital resources, build capabilities, and respond to changing innovation conditions [9]. Small firms may lack bargaining power or technical expertise, while highly regulated firms may require stronger audit rights, data controls, and accountability structures than the general framework can specify in detail.

Conclusion

Digital ecosystem dependence is becoming a central strategic vulnerability for firms that rely on external cloud platforms, AI vendors, and data intermediaries. These relationships can generate scale, flexibility, analytical power, and innovation speed, but they can also produce lock-in, opacity, bargaining weakness, data control loss, and exit difficulty. The central argument of this article is that these risks cannot be governed adequately through fragmented IT, procurement, or legal routines alone.

The Digital Ecosystem Governance Framework developed in this article offers a structured way to identify, categorise, and mitigate dependence risks across three critical ecosystem partner types. It proposes that firms should combine dependency risk assessment, protective governance mechanisms, and strategic governance oversight. This integrated approach helps managers preserve the benefits of external digital ecosystems while reducing the likelihood that operational reliance becomes strategic capture.

Future research should empirically validate the framework, examine how dependence evolves over time, and assess which governance mechanisms are most effective in different industries and firm sizes. Managers should treat digital ecosystem dependence as a recurring strategic governance issue rather than a one-time sourcing decision. Firms that build internal capability, contractual protection, portability, and exit readiness will be better positioned to use external digital ecosystems without surrendering strategic control.

Acknowledgements

None

Conflict of interest

None

Financial support

None

Ethics statement

None

Received: 01 May 2025 Revised: 10 Jun 2025 Accepted: 20 Jul 2025

Published online: 18 September 2025

Rights and permissions

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Adner R. Ecosystem as structure: An actionable construct for strategy. *J Manag.* 2017;43(1):39-58.
- McIntyre DP, Srinivasan A. Networks, platforms, and strategy: Emerging views and next steps. *Strateg Manag J.* 2017;38(1):141-60.
- Parker G, Van Alstyne M, Jiang X. Platform ecosystems: how developers invert the firm¹. *MIS Q.* 2017;41(1):255-66.
- Jacobides MG, Cennamo C, Gawer A. Towards a theory of ecosystems. *Strateg Manag J.* 2018;39(8):2255-76.
- Kapoor R. Ecosystems: broadening the locus of value creation. *J Organ Des.* 2018;7(1):1-6.
- Helfat CE, Raubitschek RS. Dynamic and integrative capabilities for profiting from innovation in digital platform-based ecosystems. *Res policy.* 2018;47(8):1391-9.
- Constantinides P, Henfridsson O, Parker GG. Introduction—platforms and infrastructures in the digital age. *Inf Syst Res.* 2018;29(2):381-400.
- De Reuver M, Sørensen C, Basole RC. The digital platform: a research agenda. *J Inf Technol.* 2018;33(2):124-35.
- Nambisan S, Wright M, Feldman M. The digital transformation of innovation and entrepreneurship: Progress, challenges and key themes. *Res Policy.* 2019;48(8):103773.
- Nambisan S, Zahra SA, Luo Y. Global platforms and ecosystems. *J Int Bus Stud.* 2019;50(9):1464-86.
- Cutolo D, Kenney M. Platform-dependent entrepreneurs: Power asymmetries, risks, and strategies in the platform economy. *Acad Manag Perspect.* 2021;35(4):584-605.
- Gawer A. Digital platforms' boundaries: The interplay of firm scope, platform sides, and digital interfaces. *Long Range Plann.* 2021;54(5):102045.
- Altman EJ, Nagle F, Tushman ML. The translucent hand of managed ecosystems: Engaging communities for value creation and capture. *Acad Manag Annal.* 2022;16(1):70-101.
- Oesterle S, Jöhnk J, Keller R, Urbach N, Yu X. A contingency lens on cloud provider management processes. *Bus Res.* 2020;13(3):1451-89.
- Lins S, Pandl KD, Teigeler H, Thiebes S, Bayer C, Sunyaev A. Artificial intelligence as a service: classification and research directions. *Bus Inf Syst Eng.* 2021;63(4):441-56.
- Berente N, Gu B, Recker J, Santhanam R. Managing artificial intelligence. *MIS Q.* 2021;45(3):1433-50.
- Cobbe J, Singh J. Artificial intelligence as a service: Legal responsibilities, liabilities, and policy challenges. *Comput Law Secur Rev.* 2021;42:105573.
- Abraham R, Schneider J, Vom Brocke J. Data governance: A conceptual framework, structured review, and research agenda. *Int J Inf Manag.* 2019;49:424-38.
- Janssen H, Singh J. Data intermediary. *Int Policy Rev.* 2022;11(1).

Reviglio U. The untamed and discreet role of data brokers in surveillance capitalism: a transnational and interdisciplinary overview. *Int Policy Rev.* 2022;11(3):1-27.

Von Ditzfurth L, Lienemann G. The Data Governance Act:—Promoting or Restricting Data Intermediaries?. *Compet Regul Netw Ind.* 2022;23(4):270-95.

Beulen E, Plugge A, van Hillegersberg J. Formal and relational governance of artificial intelligence outsourcing. *Inf Syst E Bus Manag.* 2022;20(4):719-48.

Papagiannidis E, Enholm IM, Dremel C, Mikalef P, Krogstie J. Toward AI governance: Identifying best practices and potential barriers and outcomes. *Inf Syst Front.* 2023;25(1):123-41.

Mikalef P, Gupta M. Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance. *Inf Manag.* 2021;58(3):103434.

Schweihoff J, Lipovetskaja A, Jussen-Lengersdorf I, Möller F. Stuck in the middle with you: Conceptualizing data

intermediaries and data intermediation services. *Electron Mark.* 2024;34(1):48.

Shaharudin A, van Loenen B, Janssen M. Exploring the contributions of open data intermediaries for a sustainable open data ecosystem. *Data Policy.* 2024;6:e56.

Kumar D, Samalia HV, Verma P. Exploring suitability of cloud computing for small and medium-sized enterprises in India. *J Small Bus Enterp Dev.* 2017;24(4):814-32.

Hari Kumar P, Mala GA. H2RUN: An efficient vendor lock-in solution for multi-cloud environment using horse herd Runge Kutta based data placement optimization. *Trans Emerg Telecommun Technol.* 2022;33(9):e4541.

Alhosban A, Pesingu S, Kalyanam K. CVL: A cloud vendor lock-in prediction framework. *Mathematics.* 2024;12(3):387.

Richter H. Looking at the data governance act and beyond: How to better integrate data intermediaries in the market order for data sharing. *GRUR Int.* 2023;72(5):458-70.