

Secondary Publication



Fischer, Vanessa ; Beimborn, Daniel

The Platform Liaison Role: A Governance Mechanism for the AI Platform Era

Date of secondary publication: 10.09.2026

Version of Record (Published Version), Conferenceobject

Persistent identifier: urn:nbn:de:bvb:473-irb-117124x

Primary publication

Fischer, Vanessa; Beimborn, Daniel (2026): The Platform Liaison Role: Governance Mechanism for the AI Platform Era, in: Proceedings of the 32nd Americas Conference on Information Systems (AMCIS), Reno (Nevada), USA, Association for the Information Systems (AIS), S. 1–10.

Legal Notice

This work is protected by copyright and/or the indication of a licence. You are free to use this work in any way permitted by the copyright and/or the licence that applies to your usage. For other uses, you must obtain permission from the rights-holders.

This document is made available under a Creative Commons license.



The license information is available online:

<https://creativecommons.org/licenses/by/4.0/legalcode>

Association for Information Systems

AIS Electronic Library (AISeL)

AMCIS 2026 Proceedings

Americas Conference on Information Systems
(AMCIS)

August 2026

The Platform Liaison Role: A Governance Mechanism for the AI Platform Era

Vanessa Fischer

University of Bamberg, vanessa.fischer@uni-bamberg.de

Daniel Beimborn

University of Bamberg, daniel.beimborn@uni-bamberg.de

Follow this and additional works at: <https://aisel.aisnet.org/amcis2026>

Recommended Citation

Fischer, Vanessa and Beimborn, Daniel, "The Platform Liaison Role: A Governance Mechanism for the AI Platform Era" (2026). *AMCIS 2026 Proceedings*. 24.

https://aisel.aisnet.org/amcis2026/sig_osra/sig_osra/24

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2026 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

The Platform Liaison Role: A Governance Mechanism for the AI Platform Era

Full Paper

Vanessa Fischer

University Bamberg

vanessa.fischer@uni-bamberg.de

Prof. Dr. Daniel Beimborn

University Bamberg

daniel.beimborn@uni-bamberg.de

Abstract

Organizations' rapid adoption of third-party AI platforms has created governance challenges that existing frameworks do not yet adequately address. Unlike traditional IT vendors, AI platforms combine algorithmic opacity, rapid technological change, and concentrated market power, creating novel dependencies that violate a core assumption of established governance frameworks: that organizations control their technology infrastructure. To address this gap, this paper conceptualizes the Platform Liaison Role—a dedicated governance mechanism that bridges organizational AI strategy with third-party platform operations. Drawing on IT Governance Theory, Resource Dependence Theory, and Agency Theory, we specify three core mechanisms (communication routines, policy translation, and joint risk management), antecedents, boundary conditions, and mediation pathways for this role. Through theoretical derivation, we present five testable research propositions and implementation guidance. This paper extends governance frameworks to address external AI platform dependencies and provides practitioners with actionable guidance for establishing effective AI platform governance.

Keywords

Artificial Intelligence, AI Platform Governance, Platform Liaison Role, IT Governance Mechanisms, Boundary-Spanning

Introduction

Organizations worldwide are increasingly integrating third-party AI platforms—including Microsoft Azure, OpenAI, Google, Amazon, and Anthropic—into mission-critical operations (Dwivedi et al., 2023; McKinsey, 2025). Recent surveys indicate that 78% of organizations globally use AI in at least one business function (McKinsey, 2025). This adoption trajectory reflects recognition that AI capabilities increasingly determine competitive positioning across industries. Organizations are deploying AI platforms for customer service automation, content generation, decision support, predictive analytics, and operational optimization. It promises strategic value through enhanced decision-making, automated processes, and innovative services (Benbya et al., 2021). However, AI platforms also present unprecedented governance challenges that existing frameworks cannot adequately address.

AI platforms combine three distinguishing characteristics that create unique governance challenges: algorithmic opacity, which makes foundation models operate as "black boxes" resistant to inspection of weights, training data, or reasoning processes (Lebovitz et al., 2022; Shrestha et al., 2019); rapid technological change, which demands continuous governance recalibration as providers update models without advance notice or measurable impact disclosure (Mikalef et al., 2022); and concentrated market power, which creates asymmetric dependencies with high switching costs among a small number of providers controlling critical capabilities (Kretschmer et al., 2022). Traditional governance frameworks were designed for stable, transparent markets in which organizations controlled their technology infrastructure—conditions that are fundamentally absent in AI platform ecosystems (Trocin et al., 2023). IT governance (ITG) focuses on internal decision rights (Weill & Ross, 2004), while IT outsourcing governance frameworks address B2B relationships with clear specifications and measurable deliverables (Lacity et al., 2009). But, neither addresses the dynamic, opaque, asymmetric relationships that characterize AI platform dependencies (Gregory et al., 2021). When an AI platform provider updates a

model, the organization has no visibility into what has changed, limited ability to test implications, and few alternatives if changes prove problematic.

Emerging practice confirms this need. Job market postings for roles such as "AI Vendor Risk Manager" and "AI Platform Governance Lead" have grown substantially across large organizations, and 60% of organizations have established or plan to establish a dedicated AI governance function within 12 months, with AI governance rising to the second-most important strategic priority (IBM, 2025). The EU AI Act, which entered into force in August 2024, intensifies these pressures through mandatory risk assessments and accountability mechanisms for high-risk AI systems, with similar regulations emerging in the UK, Canada, and across the US (European Commission, 2024). However, comprehensive frameworks for these roles remain underdeveloped—reflecting the recency of AI platform dependencies as a distinct governance challenge—leaving organizations to improvise arrangements without role-specific theoretical guidance (Lebovitz et al., 2022; Shrestha et al., 2019). Two recent cases illustrate both the stakes and the improvisation. In *Moffatt v. Air Canada* (2024 BCCRT 149), a tribunal held the airline liable for misinformation provided by its chatbot, rejecting the argument that the chatbot was a separate legal agent—a pointed illustration of how accountability diffuses across the provider-user boundary in the absence of dedicated governance. Unilever's publicly described red-yellow-green vetting system for AI initiatives represents the opposite face of the same problem: a documented organizational attempt to systematize governance that nonetheless remains ad hoc and not anchored in a formalized role. Taken together, current practice confirms that organizations recognize the governance gap but have not yet converged on a dedicated, boundary-spanning role designed specifically for AI platform dependencies.

This paper conceptualizes the Platform Liaison Role—a dedicated boundary-spanning governance mechanism for managing external AI platform dependencies. Drawing on ITG, Resource Dependence Theory, and Agency Theory, we specify three core mechanisms, antecedents, boundary conditions, and five testable propositions. The framework extends ITG to external dependency contexts and provides researchers and practitioners with structured guidance for AI platform governance. The remainder presents theoretical foundations, the conceptualization, propositions, discussion, and a conclusion.

Theoretical Foundations

IT Governance

IT governance represents organizational design foundations by defining decision rights and accountability for IT resources (Weill & Ross, 2004). These governance objectives are achieved through three types of mechanisms: structures (organizational units and roles), processes (strategic decision-making and monitoring procedures), and relational mechanisms (collaboration and communication practices) (De Haes & Van Grembergen, 2009). However, these frameworks assume that organizations control their IT infrastructure—an assumption that is violated by external AI platform dependencies.

Platform governance research identifies governance mechanisms as critical for platform success (Huber et al., 2017; Schreieck et al., 2022) but largely adopts the provider's perspective—how platforms govern their ecosystems—leaving a gap for organizations dependent on AI platforms. Outsourcing and vendor governance literature addresses external IT providers through contractual mechanisms and performance monitoring (Lacity et al., 2009). However, AI platform relationships differ fundamentally from traditional IT outsourcing in three ways: continuous algorithmic updates alter system behavior without contract modifications (Veale & Zuiderveen Borgesius, 2021), concentrated market power limits negotiation of customized protections (Kretschmer et al., 2022), and extreme technical opacity creates information asymmetries that exceed traditional outsourcing (Burrell, 2016; Trocin et al., 2023).

The emerging AI governance literature focuses on algorithmic accountability, ethical guidelines, and regulatory compliance (Morley et al., 2020; Veale & Zuiderveen Borgesius, 2021). The EU AI Act established risk-based classification requiring different governance intensities for high-risk versus limited-risk applications (Hacker et al., 2023). However, this literature exhibits gaps, including a lack of practical implementation mechanisms translating high-level principles into day-to-day organizational practices (Morley et al., 2020), insufficient accountability structures spanning AI value chains from developers through deployers (Kaminski, 2019), and fragmented approaches failing to coordinate governance activities across organizational boundaries (Trocin et al., 2023).

Resource Dependence Theory

Resource Dependence Theory (RDT) explains how organizations manage critical external dependencies (Pfeffer & Salancik, 1978). RDT posits that organizational success depends on the ability to acquire and maintain external resources, and that this dependence creates power imbalances requiring active management strategies (Hillman et al., 2009). Hillman et al. (2009) synthesized RDT research and identified boundary-spanning as a key mechanism for managing external dependencies—dedicated organizational roles that link organizations with external resource providers through monitoring, communication, negotiation, and relationship management. AI platforms create textbook-like conditions for resource dependence: providers control critical capabilities that few organizations can replicate internally; markets are highly concentrated among a small number of major providers; switching costs are substantial due to technical integration, organizational learning, and contractual commitments (Kretschmer et al., 2022; Huber et al., 2017). RDT predicts that organizations facing such dependencies will establish boundary-spanning mechanisms. Foundational boundary-spanning research established that organizations create specialized roles for managing critical external relationships (Aldrich & Herker, 1977; Tushman & Scanlan, 1981). Boundary spanners perform two essential functions: information processing (gathering, filtering, and interpreting external information for internal use) and external representation (conveying organizational positions, needs, and capabilities to external parties).

Agency Theory

Agency Theory examines principal-agent relationships characterized by conflicting interests and information asymmetry (Jensen & Meckling, 1976; Eisenhardt, 1989). The theory identifies two fundamental problems. Adverse selection occurs when principals cannot observe agent characteristics and capabilities before contracting, creating the risk of selecting unsuitable partners. Moral hazard arises when principals cannot adequately monitor agent behavior after contracting, enabling agents to pursue self-interest at the principal's expense. Traditional agency mechanisms include contracts that specify expectations and consequences, monitoring systems that provide visibility into agent behavior, and incentive alignment that creates shared interests. AI platform relationships introduce agency problems where algorithmic opacity creates severe, persistent information asymmetries that standard mechanisms cannot easily address (Lebovitz et al., 2022). Unlike traditional relationships, where monitoring and disclosure can progressively reduce asymmetry, AI "black boxes" resist scrutiny even with organizational effort and provider cooperation (Shrestha et al., 2019). Organizations cannot inspect proprietary models, verify the provenance of training data, or audit algorithmic decision-making processes.

Our contribution integrates the three theoretical perspectives comprehensively. ITG provides the organizational context—the structures, processes, and relational mechanisms for managing technology resources across organizational boundaries. RDT provides the strategic imperative—explaining why organizations must actively manage dependencies on external AI platforms and the consequences of failing to do so. Agency Theory provides operational mechanisms—specifying how boundary-spanning roles address information asymmetry through monitoring, contracting, relationship management, and incentive alignment. Together, they form a complementary and jointly necessary theoretical foundation rather than three parallel or competing explanations.

Conceptual Framework

Definition of the Platform Liaison Role

While organizations have established roles that touch adjacent aspects of AI platform governance—Chief AI Officers (CAIO) or AI Governance Leads (IBM, 2025), vendor managers (Lacity et al., 2009), partner relationship managers, compliance officers, enterprise architects (Ross et al., 2006), and cross-functional AI committees (Shrestha et al., 2019)—none adequately governs third-party AI platform dependencies. Appendix A contrasts each adjacent role with the Platform Liaison Role in detail. Three mismatches explain why existing roles cannot simply be extended to cover these functions.

- *Scope mismatch.* Each adjacent role carries a primary mandate that excludes sustained, boundary-spanning engagement with external AI providers. CAIOs own enterprise AI strategy and

ethics (IBM, 2025); vendor managers own contracts and SLAs (Lacity et al., 2009); compliance officers monitor regulatory adherence; enterprise architects govern systems integration (Ross et al., 2006); and committees convene periodically rather than operate continuously (Shrestha et al., 2019). No one owns the ongoing translation of algorithmic, contractual, and regulatory change into organizational action.

- *Competency mismatch.* AI platform governance requires the simultaneous combination of AI-technical fluency to interpret model behavior and updates (Lebovitz et al., 2022; Shrestha et al., 2019), vendor-commercial acumen (Lacity et al., 2009), and AI-specific regulatory translation (Hacker et al., 2023; Veale & Zuiderveen Borgesius, 2021). This combination is rarely concentrated in any single adjacent role; extending existing positions' KPIs typically expands breadth at the expense of depth in at least one dimension.
- *Position mismatch.* Algorithmic opacity and often-unannounced model updates (Benbya et al., 2021; Mikalef et al., 2022) demand sustained, bidirectional presence at the organization-provider boundary (Aldrich & Herker, 1977; Tushman & Scanlan, 1981). Adjacent roles either sit internally (enterprise architects, compliance officers) or engage externally in bounded, episodic ways (vendor managers for contract events; committees for periodic reviews), providing neither the continuous information processing nor the external representation that boundary-spanning theory identifies as essential.

We define the platform liaison role as a dedicated organizational function managing the strategic relationship between the organization and its AI platform provider(s), serving as a boundary spanner who translates external technical standards and regulatory requirements into internal policies, facilitates bidirectional communication between organizational stakeholders and provider representatives, coordinates joint risk assessment and mitigation activities, represents organizational interests in provider interactions, and ensures ongoing alignment between platform capabilities and strategic organizational objectives. This definition extends foundational boundary-spanning research (Aldrich & Herker, 1977; Tushman & Scanlan, 1981) specifically to the AI platform governance context. The role may be performed by an individual, team, or distributed across positions, but functions must be clearly assigned and adequately resourced.

Core Governance Mechanisms

Our framework identifies three core mechanisms through which platform liaisons create value.

Mechanism 1: Policy Translation. Existing IT outsourcing and vendor governance frameworks address policy translation through contractual mechanisms and service level agreements designed for stable, specifiable deliverables (Lacity et al., 2009). AI platform governance introduces translation demands those frameworks cannot accommodate: algorithmic outputs are probabilistic and context-dependent rather than fully specifiable in advance (Lebovitz et al., 2022; Shrestha et al., 2019), regulatory requirements mandate translation of AI-specific compliance obligations including EU AI Act risk classifications (European Commission, 2024; Veale & Zuiderveen Borgesius, 2021), and the ethics-to-practice gap means high-level governance principles must be operationalized without established templates (Morley et al., 2020). Policy translation therefore involves systematically interpreting platform technical standards, provider policies, and regulatory guidance into actionable internal procedures and controls—bridging technical AI concepts with business process requirements, legal compliance needs, and risk management objectives.

Mechanism 2: Communication Routines. Vendor governance literature addresses communication through structured reporting routines designed for relationships where changes are contracted, documented, and foreseeable (Lacity et al., 2009). AI platform relationships fundamentally alter this dynamic: organizations have limited visibility into and control over AI platform updates, as providers may change model behavior, capabilities, or outputs without advance notice or measurable impact disclosure (Benbya et al., 2021; Dwivedi et al., 2023). Communication routines therefore establish structured, bidirectional channels—regular provider meetings, change notification protocols, escalation procedures, and feedback mechanisms—that continuously surface opaque behavioral changes through technically informed dialogue, enable organizational learning about platform capabilities and limitations, and convey organizational needs to providers (Aldrich & Herker, 1977; Lebovitz et al., 2022).

Mechanism 3: Joint Risk Management. Platform governance research examines risk management mainly from the provider perspective—how platforms govern ecosystems to manage participant risk and

maintain control (Huber et al., 2017; Schreieck et al., 2022). For user organizations, AI platform risk management is complicated by fragmented accountability: responsibility for incidents diffuses across training, deployment, and use contexts, and neither organizations nor providers can unilaterally assess risks arising from algorithmic opacity and emergent model behavior (Veale & Zuiderveen Borgesius, 2021; Shrestha et al., 2019). Joint risk management addresses this accountability gap by coordinating risk assessment, mitigation planning, and incident response across the provider-user boundary through shared liability frameworks and AI-specific procedures that neither party can develop independently.

Figure 1 summarizes the conceptual framework, linking antecedents to platform liaison role formalization, the three core mechanisms, and governance outcomes.

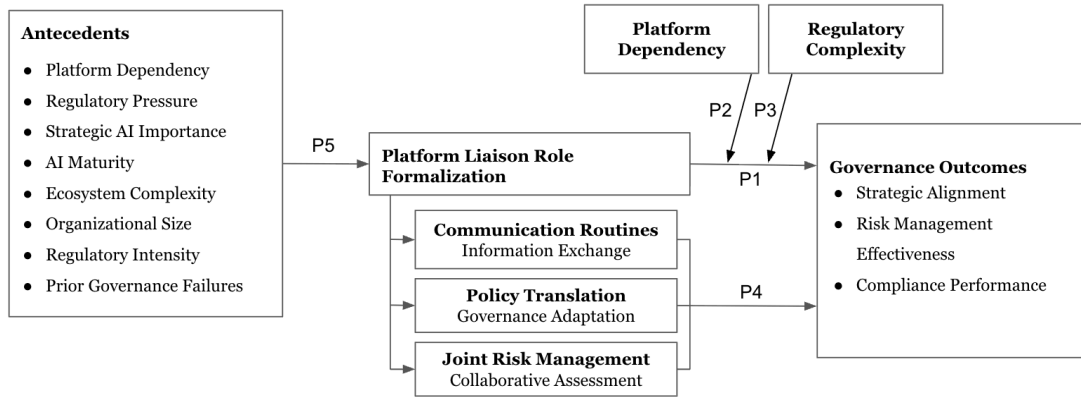


Figure 1. Conceptual Framework for Platform Liaison Role Formalization

These elements jointly characterize the platform liaison role and form the basis for the five testable propositions developed in the next section.

Research Propositions

Governance Outcome Propositions

The following propositions examine how the formalization of the platform liaison role affects governance outcomes across three theoretically distinct dimensions. Drawing on ITG research, we conceptualize AI platform governance outcomes as a multi-dimensional construct comprising: *strategic alignment*—the degree to which AI platform capabilities are aligned with organizational objectives; *risk management effectiveness*—the organization’s ability to identify, assess, and mitigate AI-related operational and compliance risks; and *compliance performance*—adherence to regulatory requirements and contractual obligations governing AI platform use (De Haes & Van Grembergen, 2009; Weill & Ross, 2004). Each proposition below addresses one dimension of this outcome space—P1 as a direct effect, P2 and P3 as conditional effects specifying when each dimension is most strongly realized—while Proposition 4 addresses the mediating mechanisms through which all three dimensions are collectively achieved.

ITG posits that alignment between IT capabilities and business objectives is achieved through governance mechanisms that create feedback loops between technology and business stakeholders (De Haes & Van Grembergen, 2009; Weill & Ross, 2004). The theory emphasizes that alignment is not a one-time achievement but requires continuous monitoring and adjustment as both technology capabilities and business needs evolve. In the context of AI platform dependencies, organizations lack direct control over platform capabilities, creating potential technology-strategy disconnects as platform providers make unilateral decisions about features, updates, and roadmaps without necessarily considering individual customer strategic priorities. Applying ITG, a formalized role represents a structural mechanism that enables continuous alignment monitoring by establishing dedicated responsibility for translating platform capabilities into business value and communicating business requirements to providers. The liaison’s boundary-spanning position creates the feedback loops that ITG identifies as essential for maintaining alignment in dynamic environments.

Proposition 1: Organizations with formalized platform liaison roles will exhibit higher AI-business strategic alignment than organizations without such roles.

Strategic alignment in this context is operationalized through the dimensions established in IS alignment research: shared understanding of AI platform capabilities and strategic intent between business and platform operations, communication quality in translating platform developments into strategic decisions, and joint planning that incorporates platform trajectory into organizational strategy (Bharadwaj et al., 2013; De Haes & Van Grembergen, 2009).

Beyond this direct effect on strategic alignment, the degree of platform dependency conditions how significantly these governance benefits materialize. RDT argues that organizations depend on external actors for critical resources, creating uncertainty and vulnerability (Pfeffer & Salancik, 1978; Hillman et al., 2009). The theory predicts that organizations respond to dependencies through boundary-spanning roles that manage external relationships, gather information, and reduce uncertainty. Critically, RDT posits that the value of boundary-spanning activities increases proportionally with dependency degree—when dependencies are weak, organizations have alternatives and lower stakes; when dependencies are strong, boundary-spanning becomes essential for organizational survival. In AI platform contexts, dependency degree varies based on the criticality of platform-enabled functions, availability of alternatives, and switching costs. Organizations with high platform dependency face greater risk exposure from platform failures, policy changes, or compliance issues, making effective external relationship management more consequential. Applying RDT, platform liaison activities (risk assessment, communication, policy translation) should yield greater risk management benefits when platform dependency is high, as the liaison's boundary-spanning function becomes more critical for reducing uncertainty and managing essential external relationships.

Proposition 2: The relationship between platform liaison formalization and risk management effectiveness will be positively moderated by platform dependency degree.

Agency Theory identifies information asymmetry as a fundamental problem in principal-agent relationships, in which agents possess superior information about their actions and capabilities, thereby creating moral hazard and adverse selection risks (Eisenhardt, 1989). The theory predicts that governance mechanisms reducing information asymmetry—such as monitoring, reporting, and specialized intermediaries—become more valuable as task complexity increases, because the costs and consequences of information gaps escalate with complexity. In AI platform relationships, organizations (principals) face information asymmetries regarding platform compliance with regulations, as providers (agents) possess superior technical knowledge of algorithmic operations, data-handling practices, and system architectures. This asymmetry intensifies in high regulatory-complexity environments where requirements span multiple jurisdictions, involve technical AI-specific provisions (e.g., EU AI Act risk classifications, algorithmic transparency requirements), and require continuous interpretation as regulations evolve (Veale & Zuiderveen Borgesius, 2021; Hacker et al., 2023). Applying Agency Theory, platform liaisons serve as specialized intermediaries who reduce information asymmetry by maintaining regulatory expertise, translating technical platform capabilities into compliance terms, and monitoring provider adherence to requirements. The value of this information-bridging function increases with regulatory complexity, as the costs of information asymmetry (non-compliance penalties, operational disruptions, reputational damage) escalate.

Proposition 3: Organizations operating in high regulatory-complexity environments will derive greater compliance performance from platform liaison roles than organizations in low-complexity environments.

Mediation by Core Mechanisms

ITG distinguishes between governance structures (organizational arrangements) and governance mechanisms (the specific practices through which governance is enacted) (De Haes & Van Grembergen, 2009; Weill & Ross, 2004). The theory posits that structures alone do not create governance value; rather, value emerges through the mechanisms that structures enable. Structures provide the organizational foundation—roles, responsibilities, reporting relationships—while mechanisms represent the actual governance activities—communication, decision-making, monitoring—that produce outcomes. In the platform liaison context, role formalization represents a structural intervention that creates organizational capacity for platform governance. However, formalization alone does not guarantee

governance effectiveness; effectiveness depends on whether liaisons enact specific governance mechanisms. Applying ITG, the three core mechanisms—communication routines (enabling information flow), policy translation (enabling compliance), and joint risk management (enabling proactive risk mitigation)—represent the pathways through which liaison role formalization creates governance value. Organizations that formalize liaison roles but fail to implement these mechanisms will not achieve expected governance outcomes, as the structure lacks the operational mechanisms through which governance is enacted.

Proposition 4: Platform liaison role formalization will improve governance outcomes across all three dimensions—strategic alignment, risk management effectiveness, and compliance performance—and this relationship will be mediated by communication routines, policy translation, and joint risk management.

Antecedents of Role Formalization

RDT predicts that organizations create boundary-spanning structures in proportion to their external dependencies (Pfeffer & Salancik, 1978; Hillman et al., 2009). When AI platform dependencies are high, organizations face greater exposure to unilateral provider decisions, capability lock-in, and governance failures, generating structural pressure to formalize dedicated liaison functions. Agency Theory further predicts that governance intermediaries become more valuable as information asymmetry and regulatory exposure increase (Eisenhardt, 1989; Hacker et al., 2023), because the costs of non-compliance and knowledge gaps escalate with regulatory intensity. ITG identifies strategic alignment as the central rationale for governance investment: as AI capabilities become integral to competitive positioning, organizations formalize the structures required to maintain continuous alignment between platform capabilities and business objectives (De Haes & Van Grembergen, 2009; Weill & Ross, 2004). Prior governance failures reinforce this process by making the costs of inadequate boundary management visible, motivating structural responses. Collectively, these mechanisms suggest that formalization likelihood increases systematically with platform dependency degree, regulatory pressure, strategic AI importance, and prior governance breakdowns. Strategic AI importance functions as an antecedent through ITG's principle that governance investment is calibrated to the strategic criticality of the IT resource: organizations devote more structural governance infrastructure to capabilities that are central to competitive positioning and operational continuity (Weill & Ross, 2004), making high strategic AI importance a consistent predictor of governance role formalization. Prior governance failures serve as an antecedent through the Agency Theory mechanism of revealed inadequacy: failures signal that existing oversight structures cannot manage AI platform information asymmetries and behavioral opacity, creating organizational pressure to establish dedicated monitoring and relationship management structures (Eisenhardt, 1989; Hacker et al., 2023).

Proposition 5: Platform dependency degree, regulatory pressure, strategic AI importance, and prior governance failures will each increase the likelihood of formalizing a platform liaison role.

Discussion

Theoretical Contribution

This paper makes three primary theoretical contributions through its conceptualization of the Platform Liaison Role. First, we extend ITG from internal technology management to external platform governance, specifying how governance mechanisms must adapt when decision rights, monitoring capabilities, and accountability structures span organizational boundaries (Weill & Ross, 2004). Second, we integrate three complementary theoretical perspectives — ITG for organizational design, RDT for strategic positioning, and Agency Theory for relationship dynamics — to show how governance structures enable strategies for managing dependencies through specific relationship mechanisms. Third, we develop a boundary-spanning conceptual framework (Figure 1) that applies and extends prior boundary-spanning principles to specify mechanisms, antecedents, and boundary conditions particular to AI platform contexts.

Practical Implications

Implementing the role raises questions about staffing, capabilities, and reporting. The liaison function may be held by an individual, a small team, or a cross-functional council, depending on organizational scale and platform portfolio breadth. The role typically reports to both the CIO (for technical fluency) and the Chief Risk Officer or CAIO (for risk and strategic oversight). The capability profile blends three rarely co-located elements: AI literacy sufficient to interpret model updates, commercial and vendor-relationship acumen, and legal/regulatory fluency. Core responsibilities track the three mechanisms specified above: policy translation, communication routines with provider representatives, and joint risk management. Implementation also carries real costs and challenges: executive sponsorship, protected budget, and the scarcity of candidates who combine the three capability elements are common constraints that can stall early attempts.

A predictable objection is that this is “IT governance by another name” absorbable by refining KPIs of existing roles. The three mismatches answer why it cannot: scope (no existing role owns sustained boundary-spanning engagement with external AI providers), competency (the required combination is rarely concentrated in a single role), and position (algorithmic opacity and continuous model updates demand bidirectional presence that committees and part-time add-ons cannot provide). The cost of formalization is small relative to the exposure it manages; its principal benefit is a single point of accountability that prevents responsibility from diffusing across adjacent functions.

Limitations and Future Research

This research has limitations common to conceptual papers that future work should address. First, the framework awaits empirical validation. The propositions require testing through multiple methods: qualitative case studies to assess construct validity and refine the liaison role definition, and quantitative surveys or archival studies to test the hypothesized relationships. The emerging evidence base for AI platform governance limits the availability of validated measurement instruments; however, to support future empirical testing, each construct admits an ‘operational’ definition with a candidate proxy. For example, *platform liaison role formalization* can be operationalized as the degree to which platform-liaison functions are assigned through a dedicated job description, reporting line, and decision authority over provider relationships. As a second limitation, the framework is also developed primarily with large, regulated, AI-dependent organizations in focus. Where platform dependency degree, regulatory pressure, and strategic AI importance are all high—typical of large firms in healthcare, finance, insurance, and public administration—formalizing a distinct role is likely to generate material governance benefits. Where these antecedents are weaker, the role’s functions may be absorbable by existing positions. Third, the framework assumes stable AI platform dependencies, though platform relationships are dynamic—providers may exit, merge, or significantly alter their offerings—and future research should examine how liaison roles adapt to such turbulence.

Despite these limitations, a credible empirical roadmap is feasible. Staggered implementation of the EU AI Act (European Commission, 2024) and analogous regimes (UK, Canada, US) creates exogenous variation in regulatory exposure across firms and sectors, enabling difference-in-differences designs that compare governance role formalization and governance outcomes before and after obligations take effect. Sector-specific mandates for high-risk AI systems (EU AI Act Annex III) supply candidate instruments for regulatory exposure, while provider-side policy shifts (e.g., changes to model deprecation notices or data processing terms) offer within-firm shocks useful for event studies. Peer adoption pressure within industry or geographic networks provides an additional instrument for role formalization.

Conclusion

Third-party AI platforms create novel resource dependencies characterized by algorithmic opacity, rapid evolution, concentrated market power, and regulatory complexity (Pfeffer & Salancik, 1978; Benbya et al., 2021). Existing governance frameworks—designed for internal resources and transparent vendor relationships—cannot adequately address these challenges. This paper theorizes the platform liaison role as a critical AI governance innovation grounded in ITG, RDT, and Agency Theory. Our conceptual framework identifies three core mechanisms—communication routines, policy translation, and joint risk management—translating the role into concrete, testable governance activities. While organizational titles

vary—CAIO, AI Governance Manager—for organizations with significant AI platform dependencies, particularly those in regulated industries, the platform liaison conceptualization provides essential guidance for governance structure and practice. Future research should empirically validate the framework, develop measurement instruments, and examine how roles evolve as AI technology and regulations mature.

References

- Aldrich, H., & Herker, D. (1977). Boundary spanning roles and organization structure. *Academy of Management Review*, 2(2), 217-230.
- Benbya, H., Pachidi, S., & Jarvenpaa, S. (2021). Artificial intelligence in organizations: Current state and future opportunities. *Journal of the Association for Information Systems*, 22(2), 281-303.
- Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly*, 37(2), 471-482.
- Burrell, J. (2016). How the machine ‘thinks’: Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1), 1-12.
- De Haes, S., & Van Grembergen, W. (2009). An exploratory study into IT governance implementations and its impact on business/IT alignment. *Information Systems Management*, 26(2), 123-137.
- Dwivedi, Y. K., et al. (2023). So what if ChatGPT wrote it? Multidisciplinary perspectives on opportunities, challenges, and implications of generative AI. *International Journal of Information Management*, 71, 102642.
- Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of Management Review*, 14(1), 57-74.
- European Commission. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union.
- Gregory, R. W., Henfridsson, O., Kaganer, E., & Kyriakou, H. (2021). The role of artificial intelligence and data network effects for creating user value. *Academy of Management Review*, 46(3), 534-551.
- Hacker, P., Engel, A., & Mauer, M. (2023). Regulating ChatGPT and other large generative AI models. *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency (FAcCT)*, 1112-1123.
- Hillman, A. J., Withers, M. C., & Collins, B. J. (2009). Resource dependence theory: A review. *Journal of Management*, 35(6), 1404-1427.
- Huber, T. L., Kude, T., & Dibbern, J. (2017). Governance practices in platform ecosystems: Navigating tensions between cocreated value and governance costs. *Information Systems Research*, 28(3), 563-584.
- IBM. (2025). The CEO's guide to generative AI: The rise of the Chief AI Officer. IBM Institute for Business Value.
- Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305-360.
- Kaminski, M. E. (2019). The right to explanation, explained. *Berkeley Technology Law Journal*, 34, 189-218.
- Kretschmer, T., Leiponen, A., Schilling, M., & Vasudeva, G. (2022). Platform ecosystems as meta-organizations: Implications for platform strategies. *Strategic Management Journal*, 43(3), 405-424.
- Lacity, M. C., Khan, S. A., & Willcocks, L. P. (2009). A review of the IT outsourcing literature: Insights for practice. *Journal of Strategic Information Systems*, 18(3), 130-146.
- Lebovitz, S., Lifshitz-Assaf, H., & Levina, N. (2022). To engage or not to engage with AI for critical judgments: How professionals deal with opacity when using AI for medical diagnosis. *Organization Science*, 33(1), 126-148.
- McKinsey. (2025). *The state of AI in 2025: Agents, innovation, and transformation*. McKinsey & Company.

- Mikalef, P., Conboy, K., Lundström, J. E., & Popović, A. (2022). Thinking responsibly about responsible AI and 'the dark side' of AI. *European Journal of Information Systems*, 31(3), 257-268.
- Moffatt v. Air Canada, 2024 BCCRT 149 (Civil Resolution Tribunal of British Columbia). <https://canlii.ca/t/k32j9>
- Morley, J., Floridi, L., Kinsey, L., & Elhalal, A. (2020). From what to how: An initial review of publicly available AI ethics tools, methods and research to translate principles into practices. *Science and Engineering Ethics*, 26(4), 2141-2168.
- Pfeffer, J., & Salancik, G. R. (1978). *The external control of organizations: A resource dependence perspective*. Harper & Row.
- Ross, J. W., Weill, P., & Robertson, D. C. (2006). *Enterprise architecture as strategy: Creating a foundation for business execution*. Harvard Business School Press.
- Schreieck, M., Wiesche, M., & Krcmar, H. (2022). Governing innovation platforms in multi-business organization. *European Journal of Information Systems*, 30(4), 401-423.
- Shrestha, Y. R., Ben-Menahem, S. M., & von Krogh, G. (2019). Organizational decision-making structures in the age of artificial intelligence. *California Management Review*, 61(4), 66-83.
- Trocin, C., Mikalef, P., Papamitsiou, Z., & Conboy, K. (2023). Responsible AI for digital health: A synthesis and a research agenda. *Information Systems Frontiers*, 25(6), 2139-2157.
- Tushman, M. L., & Scanlan, T. J. (1981). Boundary spanning individuals: Their role in information transfer and their antecedents. *Academy of Management Journal*, 24(2), 289-305.
- Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, 22(4), 97-112.
- Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business School Press.

Appendix A. Governance Roles Compared

Role	Primary Focus	Scope regarding External AI Platforms	Gap Addressed by Platform Liaison
CAIO / AI Governance Lead	Enterprise AI strategy, ethics, internal AI development	Strategic and advisory; limited operational engagement with provider roadmaps	Day-to-day translation of model updates into organizational action; sustained provider-facing presence
Vendor / Procurement Manager	Contracts, SLAs, procurement, commercial risk	Generalist vendor management; rarely equipped to assess algorithmic or model-level change	Technical interpretation of platform updates; algorithmic-opacity-aware escalation routines
Partner Relationship Manager	Business collaboration and value co-creation with strategic partners	Partnership-oriented; not focused on algorithmic opacity, continuous model updates, or AI-specific regulatory compliance	AI-specific technical fluency; joint risk management tied to model behavior, not partnership outcomes
Compliance Officer	Regulatory adherence, risk reporting, policy enforcement	Internally oriented; consumes policy rather than shaping joint procedures with provider	Joint risk management across provider-user boundary; co-development of AI-specific procedures
Enterprise Architect	Systems integration, technical design, architectural standards	Internal architecture; limited authority to represent organization to provider or translate provider-side change	External representation, negotiation, and strategic alignment with provider
Cross-Functional AI Committee	Periodic AI review, approval, and oversight drawn from multiple functions	Episodic convening; lacks operational continuity and dedicated ownership	Continuous, operational boundary-spanning; single point of accountability
Platform Liaison (proposed)	Boundary-spanning governance of external AI platform dependencies	Dedicated, continuous, bidirectional: policy translation, communication routines, joint risk management	Integrates the gaps above into a single formalized role

Note. Rows describe typical profiles; they vary in individual organizations. The Platform Liaison may be staffed by an individual, a small team, or a distributed function, but the functions in the final row should be formally assigned.