Enterprise Architecture Governance for Hybrid Cloud Security in Multinational Enterprises: A Systematic Literature Review

Xi Nan
University of Melbourne
1592260984@qq.com

Yueyang Mao
University of Melbourne
maoyueyangm-yy@outlook.com

Yumeng Liao
University of Melbourne
liaoyumenglynn@outlook.com

Shuang Liang
University of Melbourne
verita0927@gmail.com

Rod Dilnutt
University of Melbourne
rpd@unimelb.edu.au

Abstract

This report examines how enterprise architecture governance frameworks can manage security responsibility boundaries between cloud providers and multinational enterprises during hybrid cloud migration. Based on a systematic literature review of peer-reviewed and foundational sources, it synthesises research on hybrid cloud governance complexity, the limitations of shared security responsibility, enterprise architecture governance mechanisms, and cross-border accountability challenges. The review finds that hybrid cloud migration creates a structural governance gap because operational control is partly transferred to providers while accountability often remains with the enterprise. The shared responsibility model is necessary but insufficient: it identifies broad obligations but does not consistently ensure their visibility, verification, or enforcement. Enterprise architecture governance can address this gap through decision rights, accountability structures, standards alignment, and continuous compliance review. However, multinational contexts can constrain these mechanisms through regulatory fragmentation, data sovereignty, provider dependence, and internal coordination demands. The review contributes an integrated framework that maps each unresolved property of shared responsibility, including visibility, verifiability, and enforceability, to a specific EA governance mechanism, thereby extending EA governance theory into the domain of security responsibility management. The report concludes that enterprises should establish governance before or alongside migration, explicitly map security decision rights, and align governance with recognised cloud security standards.

Keywords: *enterprise architecture governance; hybrid cloud migration; security responsibility boundaries; multinational enterprises; shared responsibility model*

Introduction

The rapid proliferation of hybrid cloud adoption among multinational enterprises has fundamentally transformed how organisations design, operate, and govern their IT infrastructures. As enterprises migrate critical workloads across combinations of private data centres and public cloud platforms, they encounter not only technical complexity but a deeper and more consequential challenge: the governance of security responsibility. When infrastructure spans organisational and jurisdictional boundaries, the question of who is accountable for securing which assets and under what authority becomes difficult to answer clearly. This ambiguity is not merely an operational inconvenience; it represents a structural governance problem with significant implications for enterprise risk, regulatory compliance, and organisational resilience.

Enterprise architecture (EA) governance offers a conceptual and practical lens through which this problem can be examined. EA governance encompasses the frameworks, principles, and mechanisms through which organisations establish authority, coordinate decision-making, and maintain accountability across complex, distributed IT environments. In the context of hybrid cloud migration, EA governance is particularly relevant because it addresses the overarching question of how enterprises can retain strategic control over security responsibilities even when operational control is partially delegated to external cloud providers. Despite this relevance, existing literature suggests that current governance models, most notably the shared responsibility model promoted by major cloud providers, are insufficient for managing the nuanced and dynamic security boundaries that characterise hybrid cloud environments, particularly for multinational enterprises operating across multiple regulatory regimes.

This report investigates the following research question: How can enterprise architecture governance frameworks manage security responsibility boundaries between cloud providers and multinational enterprises during hybrid cloud migration? This review is in scope of multinational enterprises undertaking hybrid cloud migration, with attention to EA governance issues concerning security responsibility boundaries between cloud providers and enterprise stakeholders. The review deliberately excludes detailed cloud infrastructure design, technical security implementation, jurisdiction-specific legal analysis, and any form of primary data collection, such as interviews or surveys.

To address this research question, the report is structured as follows. The Method section outlines the literature search and selection process. The Literature Review is organised around four themes: the governance complexity introduced by hybrid cloud migration; the limitations of the shared responsibility model in ensuring clear accountability; EA governance mechanisms for clarifying and coordinating security responsibility boundaries; and the additional challenges that multinational contexts, including cross-border data flows and regulatory fragmentation, pose for the application of EA governance. The Discussion section synthesises these themes into a direct response to the research question and identifies implications for practice and future research, followed by a conclusion that summarises key findings and offers recommendations.

Method

This study adopts a systematic literature review approach, following Webster and Watson (2002), to investigate how enterprise architecture governance frameworks can address security responsibility boundaries in hybrid cloud environments for multinational enterprises. This review synthesises existing academic and professional literature rather than collecting primary data.

Literature was sourced through the University of Melbourne Library, including Web of Science. Google Scholar and SciSpace were initially used but later excluded because many results could not be verified as peer-reviewed. Key search strings included “hybrid cloud” AND “security governance”, “shared responsibility model” AND “accountability”, “enterprise architecture” AND “cloud security”, and “data sovereignty” AND “multinational enterprise”, etc.

Inclusion criteria required peer-reviewed journal articles and conference papers from established venues. Books and seminal works were included where they provided foundational theoretical grounding. The publication’s main range was 2015 to 2026, covering approximately the past decade. This starting point was chosen because hybrid cloud adoption became widespread in enterprise contexts from 2015, and the GDPR was adopted in 2016, which created the cross-border governance pressures that this review addresses. Earlier works published after 2000 were included, where they established foundational concepts cited extensively in recent literature. Exclusion criteria eliminated non-English publications, purely technical papers without governance implications, and unverified sources.

Key themes related were identified through the reading of titles, keywords, abstracts, and full texts. Results were progressively narrowed through relevance screening. Therefore, four themes emerged from this process and form the structure of the literature review: hybrid cloud governance complexity, limited shared responsibility models, EA governance mechanisms, and cross-border compliance challenges. Figure 1 summarises these four themes and the logical progression among them, which structures the review that follows.

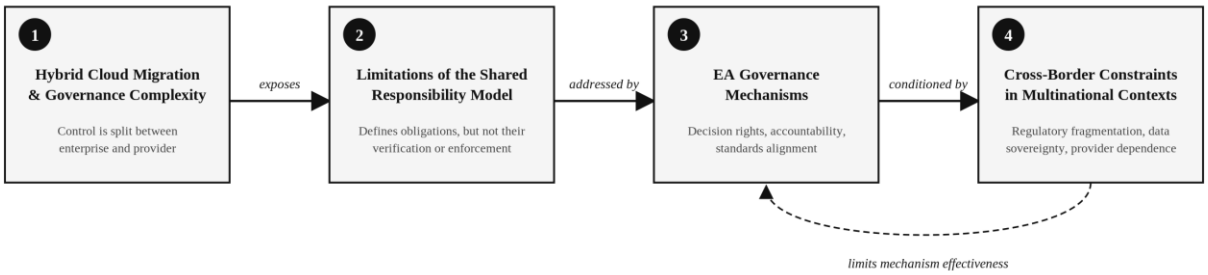

Figure 1. Thematic structure of the literature review

Literature Review

Hybrid Cloud Migration and Increasing Governance Complexity

The large-scale adoption of hybrid cloud infrastructure among multinational enterprises has emerged as a defining trend in contemporary IT strategy (He & Wang, 2015, p. 11). Ali et al. (2025) observe that organisations increasingly deploy hybrid and multi-cloud architectures to balance operational flexibility, cost efficiency, and regulatory compliance, resulting in environments where sensitive workloads are distributed across private data centres and multiple public cloud platforms simultaneously. The technical complexity of cloud migration is well-documented: integrating legacy systems with heterogeneous cloud services introduces interoperability gaps and data locality concerns that complicate governance (Gholami et al., 2016). Security concerns occupy a central position in these migration decisions. Kajiyama et al. (2017) find that risk perception, particularly around data loss, unauthorised access, and loss of direct control, remains one of the primary factors shaping whether and how enterprises commit to cloud adoption, reflecting the inherent tension between the strategic benefits of migration and the governance risks it creates.

The governance complexity arising from hybrid cloud environments manifests in several concrete and interconnected ways. Brandis et al. (2019) argue that traditional single-domain governance models, designed for environments under unified organisational control, are fundamentally ill-suited to cloud scenarios where compliance becomes a shared responsibility distributed across providers, brokers, customers, and auditors rather than residing within a single organisational boundary. This structural mismatch is compounded by three overlapping challenges: the multiplication of accountable parties across the cloud supply chain, where no single entity retains comprehensive oversight (Brandis et al., 2019); the blurring of control boundaries between enterprise-managed and provider-managed infrastructure, as organisations frequently lack visibility into where data is stored, replicated, or processed across cloud layers (Ali et al., 2025; Gholami et al., 2016); and the fragmentation of data across jurisdictions governed by differing legal and regulatory regimes, where achieving compliance becomes increasingly complex when multiple providers operate across distinct legal environments (Ali et al., 2025). Collectively, these pressures erode the clarity of security ownership that effective governance depends upon, creating ambiguity about which actor bears responsibility for detecting, responding to, and remediating security incidents at any given layer of the stack. This structural complexity exposes the fundamental limitations of existing security governance models, which are most acutely visible in the implementation of the shared responsibility model, as examined in the following section.

Limitations of Shared Security Responsibility in Ensuring Accountability

The shared responsibility model is the dominant framework for allocating security obligations between cloud providers and customers. Cloud Security Alliance (2017) defines this framework across governance areas, including compliance, data security, identity management, and incident response, establishing that providers secure underlying infrastructure while customers manage data protection, access configuration, and compliance obligations. However, while the model identifies broad responsibility categories, it does not explain how those responsibilities should be verified or enforced when organisations operate in hybrid cloud environments.

Cloud computing is built on outsourcing, and this creates a fundamental security problem. Hashizume et al. (2013) argue that when organisations hand over essential infrastructure to third-party providers, they may lose direct control over security, privacy, and compliance. The result is a gap between who is accountable and who actually controls the systems: customers are still responsible for meeting regulatory obligations, but the technical controls they need are in the hands of providers. Ouedraogo et al. (2015) add that closing this gap requires security transparency and mutual auditability between both parties. Therefore, without sufficient visibility into practices of the provider side, the customers may be formally responsible but unable to verify whether provider obligations have been met, reducing the shared responsibility to a statement of duty rather than an enforceable mechanism.

The accountability gap also exists on the customer side. Chauhan and Shiaeles (2023) demonstrate that organisations consistently struggle to operationalise their assigned responsibilities, with implementation gaps around misconfiguration, access control, and monitoring arising from role ambiguity and insufficient technical capacity rather than the absence of frameworks. Jaatun et al. (2020) argue that genuine accountability requires more than obligation allocation, which requires evidence, reporting tools, and verifiable mechanisms that allow responsible actors to demonstrate compliance. Simhadri (2025) further argues that multi-cloud environments suggest the fundamental limits

of delegated responsibility and that deeper collaboration, continuous monitoring, and shared ownership between providers and customers are needed. Collectively, the literature suggests that the shared responsibility model is necessary but insufficient. It defines who is responsible without ensuring that responsibility is visible, implemented, or enforceable. EA governance mechanisms can fill this gap by turning broad responsibility categories into clear decision rights, control ownership, and architecture standards that can be enforced.

EA Governance Mechanisms for Clarifying and Managing Security Responsibility Boundaries

EA governance frameworks provide the structural foundation through which organisations establish authority, coordinate decision-making, and maintain accountability across complex IT environments. Tamm et al. (2022) demonstrate that EA generates organisational benefits through three key mechanisms: improving IS decision-making, IS project delivery, and IS platform quality, with each mechanism depending on the quality of EA service provision. Janssen (2019), drawing on a study of more than fifteen cases, shows that architectural governance is a condition for the ability to create business value from the EA function, as governance ensures that EA models, principles, and standards are used and translated into firm value rather than remaining unused artefacts. At the level of constituent elements, EA governance frameworks typically encompass architecture principles, governance structures, technical standards, and accountability mechanisms that together establish internal authority and coordinate cross-functional action (Abunadi, 2019; Hillmann et al., 2024). Collectively, these elements are capable of assigning authority, enforcing standards, and verifying compliance, making them inherently suited to delineating security responsibility boundaries in complex IT environments.

The application of these elements to security responsibility boundaries can be shown by the convergent evidence across governance, security, and EA research. An integrated conceptual model by Mayer et al. (2019) demonstrates that EA management and information system security risk management can be systematically combined, providing a theoretical basis for EA governance frameworks to translate abstract security requirements into structured organisational responsibility allocations. This integration is operationalised through project governance, which Kurnia et al. (2021) identify as a core EA activity area. Drawing on their empirical framework, EA activity functions through three complementary mechanisms: architecture principles that constrain the behavioural boundaries of each responsible party, establishing decision rights; technical standards that regulate implementation choices, achieving standards alignment; and compliance reviews that verify whether assigned responsibilities have been executed, enforcing accountability structures. These mechanisms collectively address the definition, assignment, and verification of security responsibilities that the shared responsibility model leaves unresolved. The applicability of this approach extends to externally imposed compliance pressures, with research suggesting that EAM shows potential for translating regulatory obligations such as GDPR requirements into internally actionable responsibility rules mapped to specific organisational roles and controls, though empirical validation of this capacity remains limited (Georgiadis & Poels, 2021).

Recognition of these governance mechanisms extends beyond conceptual EA literature into emerging cloud governance practice. Industry guidance on enterprise cloud governance emphasises that roles and responsibilities between cloud service providers and client organisations must be explicitly defined, while governance authority and accountability remain with the enterprise rather than being delegated to providers (Mazula & Lamprecht, 2023). It reflects a central governance tension in hybrid cloud environments, which is that although operational control over infrastructure may be partially externalised to cloud providers, responsibility for security oversight, compliance, and risk management is still organisationally internal. Therefore, in addition to the contractual responsibility allocation, effective cloud governance also relies on the governance mechanisms that can maintain organisational oversight, enforce accountability, and coordinate security responsibilities across complex cloud environments.

Applying EA governance mechanisms to hybrid cloud environments requires addressing structural challenges of conventional IT governance frameworks. Defining IT governance as the specification of decision rights and accountability frameworks to encourage desirable behaviour in IT use, Weill and Ross (2004) reframe cloud security responsibility as a problem of systematically allocating authority across organisational and provider boundaries. Cloud adoption intensifies this challenge: migrating to cloud services restructures organisational risk by partially transferring operational control to providers, making a redesign of IT governance structures necessary to reestablish control boundaries under conditions of shared authority (Prasad & Green, 2015). Compounding this, the available cloud

governance and security frameworks, including ITIL, COBIT, and ISO/IEC 27001, were developed for different purposes and individually leave significant gaps in cloud governance coverage (Bounagui et al., 2019); comparative analysis confirms that these standards differ substantially in their control coverage and audit mechanisms, meaning reliance on any single framework risks leaving responsibility boundary gaps unaddressed (Hegde et al., 2024). These findings show that EA governance should play a coordinating role to align responsibility definitions across frameworks.

Sustaining this coordination over time requires moving beyond static responsibility assignments. Continuous monitoring and certification mechanisms for cloud services address this by converting point-in-time responsibility allocations into dynamic compliance verification sustained across the cloud service lifecycle (Lins et al., 2019). This shift reflects a broader requirement of digital governance: that control, coordination, and accountability mechanisms must operate dynamically across distributed infrastructure environments rather than being fixed at a single point of assessment (Hanisch et al., 2023). Therefore, in addition to the impact of the technical design of governance frameworks, the effectiveness of these mechanisms is also under the condition of organisational and regulatory contexts.

Cross-Border Accountability and Security Challenges for Applying EA Governance in Multinational Enterprises

These organisational and regulatory contexts prove particularly consequential for multinational enterprises operating across jurisdictions. The EA governance mechanisms examined in the preceding section centred on decision rights allocation, risk governance redesign, standards alignment, and accountability structures. While these mechanisms establish a coherent framework for managing security responsibility boundaries, their application across jurisdictions introduces conditions that the preceding analysis does not fully address.

Regulatory fragmentation across jurisdictions presents a structural challenge to EA governance's ability to define security responsibility boundaries. At the regulatory level, states have adopted divergent data privacy regimes with extraterritorial reach, generating overlapping and conflicting obligations that complicate the application of a unified governance framework (Voss, 2020). This fragmentation extends into cloud governance: conflicting data rights and cloud architectures require simultaneous coordination across legal, compliance, audit, and technology functions, a demand that can exceed the capacity of conventional governance structures (Gozman & Willcocks, 2019). At the organisational level, evidence from a bank's cloud register shows that such misalignment concentrates around poorly designed legal risk controls, including international data transfer practices (Anderson-Princen, 2022). These studies collectively suggest that regulatory fragmentation can translate into weakened internal control performance, undermining the governance conditions on which boundary definition and enforcement depend. None of them, however, indicates how EA governance can maintain effective boundary control under such fragmented conditions.

Beyond regulatory fragmentation, data sovereignty and structural dependence on cloud infrastructures introduce additional constraints on boundary governance. Woods (2018) frames data sovereignty as a jurisdictional problem, showing that overlapping legal claims over cloud-held data are often resolved through case-specific sovereign-deference reasoning, making uniform outcomes across jurisdictions difficult to achieve. Tang (2022) broadens this issue by showing that data localisation and surveillance access obligations place the transnational structure of cloud computing in tension with territorial state authority, constraining enterprise data control across their cloud environments. Blancato and Carr (2026) extend this to the geopolitical level, showing that reliance on dominant hyperscale cloud providers generates trust deficits around access to and control over cloud infrastructures. Collectively, these studies suggest that security responsibility boundaries are not merely technical or contractual divisions; they are shaped by contested legal authority, infrastructure control, and trust in cross-border cloud environments.

These external constraints generate internal governance design problems: enterprises must determine who owns which security decisions, how compliance obligations are allocated across providers, and where residual risks are assigned. Addressing these problems requires EA governance mechanisms centred on accountability, oversight, and decision rights. While Spagnoletti et al. (2025) show that distributing data control across regulated ecosystems generates functional and distributional tensions requiring ongoing contractual and procedural coordination, particularly where subcontractors operate under differing legal obligations, Anderson-Princen (2022) demonstrates that managing these risks depends on internal control design quality rather than provider arrangements alone, with misalignment

concentrated where controls fail to capture residual legal and operational risks. Collectively, these studies indicate that external constraints can condition how hybrid cloud governance mechanisms are applied in multinational enterprises. However, the literature tends to examine regulatory fragmentation, data sovereignty, and infrastructure-related dependence separately, rather than explaining how these constraints can be integrated into a coherent EA governance approach. This leaves limited guidance on how EA governance frameworks should structure decision rights, accountability mechanisms, standards alignment, and compliance review under overlapping regulatory, sovereignty, and operational conditions during hybrid cloud migration.

Discussion

Hybrid cloud migration creates a structural gap in enterprise security governance where operational control is partially transferred to external providers. The shared responsibility model can address this by defining responsibility categories across provider and customer domains, but it does not ensure that these responsibilities are visible, verifiable, or enforceable in practice. EA governance frameworks provide the infrastructure needed to close this gap through mechanisms centred on decision rights allocation across organisational and provider boundaries, accountability structures that make assigned responsibilities enforceable, and technical standards alignment across the hybrid cloud stack. However, the effectiveness of the mechanisms is constrained in multinational contexts: regulatory fragmentation, contested data sovereignty, and internal control design demands will limit their consistent application across jurisdictions. Each unresolved property maps onto a specific mechanism: decision rights allocation makes responsibility ownership visible; standards alignment renders compliance verifiable against a common baseline of controls; and accountability structures make assigned obligations enforceable. Figure 2 presents this synthesis as an integrated framework.

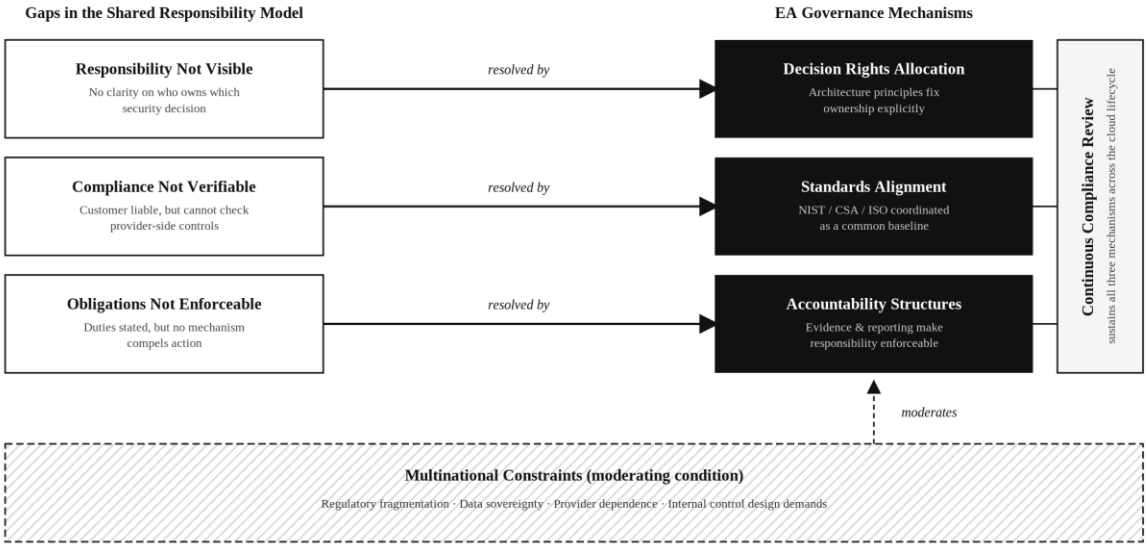

Figure 2. EA governance mechanism framework

This review extends EA governance theory beyond its established domains of IT planning and business-IT alignment into the domain of security responsibility management, demonstrating that EA governance frameworks possess structural properties suited to responsibility boundary definition, assignment, and verification. It further repositions the shared responsibility model as a necessary but insufficient governance instrument, indicating that EA theory needs to engage more directly with cloud-specific governance challenges rather than treating existing frameworks as adequate responses to the governance problems that hybrid cloud migration creates.

For multinational enterprises undertaking hybrid cloud migration, this review offers three practical recommendations. EA governance structures should be established before or alongside technical migration, as retrospective governance design is less effective at capturing responsibility boundaries at the point where they are created. Decision rights over

cloud security should be explicitly mapped in EA governance artefacts, and compliance review mechanisms should be designed to operate continuously across the cloud service lifecycle. EA governance frameworks should also be deliberately aligned with established cloud security standards, including those developed by NIST, CSA, and ISO, to prevent the governance gaps that arise when organisations rely on a single framework with incomplete control coverage.

This review has three limitations. Since this review synthesises existing literature, its findings speak to patterns across the scholarship and may not translate directly to any particular organisational context. The literature directly addressing EA governance in hybrid cloud security responsibility contexts is also sparse, and several conclusions required inference across adjacent bodies of literature spanning EA governance, cloud security, and IT governance, which introduces interpretive limitations. Finally, this review focuses on governance mechanisms at the enterprise level; policy-level implications, including how regulatory frameworks might reflect EA governance requirements, fall outside the scope of this review.

Three directions for future research follow from these gaps. Empirical studies are needed to examine EA governance mechanisms in real multinational hybrid cloud migration contexts, where the interaction between governance design and regulatory environment can be directly observed. Future research can also investigate how EA governance can be adapted for highly regulated industries with the most acute data sovereignty and cross-border compliance pressures. Finally, given that EA governance frameworks are designed primarily around static instruments, including architecture principles, documentation, and periodic compliance reviews, future research should examine how these frameworks can be integrated with dynamic cloud-native tools such as automated compliance checking and continuous monitoring platforms, enabling governance mechanisms to operate in real time rather than at fixed assessment points.

Conclusion

This report suggests that EA governance frameworks provide the structural mechanisms needed to define, assign, and enforce security responsibility boundaries in hybrid cloud migration. These mechanisms can translate broad responsibility statements into enforceable governance arrangements through decision rights allocation, accountability structures, standards alignment, and continuous compliance review across the cloud service lifecycle. The shared responsibility model is necessary because it identifies provider and customer obligations, but insufficient because it does not ensure these obligations are visible, verifiable, or consistently enforced. EA governance is positioned to address this gap.

The key takeaway is that security responsibility boundaries are not purely technical or contractual. In multinational enterprises, they are shaped by hybrid cloud complexity, provider dependency, regulatory fragmentation, data sovereignty, and internal coordination demands. Therefore, EA governance should be designed as an active coordination mechanism rather than a static documentation exercise.

For practice, multinational enterprises should establish EA governance before or alongside cloud migration, explicitly map cloud security decision rights in architecture artefacts, maintain continuous compliance review, and align EA governance with recognised cloud security standards such as NIST, CSA, and ISO. However, this review is limited by the scarcity of studies directly linking EA governance to security responsibility boundaries in multinational hybrid cloud migration, its reliance on secondary literature, and the absence of primary organisational evidence to validate its findings. Further empirical research is therefore needed.

References

Abunadi, I. (2019). Enterprise architecture best practices in large corporations. *Information*, *10*(10), 293. https://doi.org/10.3390/INFO10100293

Ali, S., Talpur, D. B., Abro, A., Alshudukhi, K. S., Alwakid, G. N., Humayun, M., Bashir, F., Wadho, S. A., & Shah, A. (2025). Security and privacy in multi-cloud and hybrid cloud environments: Challenges, strategies, and future directions. *Computers & Security*, *157*, Article 104599. https://doi.org/10.1016/j.cose.2025.104599

Anderson-Princen, J. M. (2022). Cloud outsourcing in the financial sector: An assessment of internal governance strategies on a cloud transaction between a bank and a leading cloud service provider. *European Business Organization Law Review*, *23*(4), 905–936. https://doi.org/10.1007/s40804-022-00252-4

Blancato, F. G., & Carr, M. (2026). The trust deficit. EU bargaining for access and control over cloud infrastructures. *Journal of European Public Policy*, *33*(3), 936–967. https://doi.org/10.1080/13501763.2024.2441418

Bounagui, Y., Mezrioui, A., & Hafiddi, H. (2019). Toward a unified framework for cloud computing governance: An approach for evaluating and integrating IT management and governance models. *Computer Standards & Interfaces*, 62, 98–118. https://doi.org/10.1016/j.csi.2018.09.001

Brandis, K., Dzombeta, S., Colomo-Palacios, R., & Stantchev, V. (2019). Governance, risk, and compliance in cloud scenarios. *Applied Sciences*, *9*(2), Article 320. https://doi.org/10.3390/app9020320

Cloud Security Alliance. (2017). Security guidance for critical areas of focus in cloud computing v4.0. CSA. https://cloudsecurityalliance.org/research/guidance/

Georgiadis, G., & Poels, G. (2021). Enterprise architecture management as a solution for addressing general data protection regulation requirements in a big data context: a systematic mapping study. *Information Systems and E-Business Management*, 19(1), 313–362. https://doi.org/10.1007/s10257-020-00500-5

Gholami, M. F., Daneshgar, F., Low, G., & Beydoun, G. (2016). Cloud migration process—A survey, evaluation framework, and open challenges. *Journal of Systems and Software*, *120*, 31–69. https://doi.org/10.1016/j.jss.2016.06.068

Gozman, D., & Willcocks, L. (2019). The emerging Cloud Dilemma: Balancing innovation with cross-border privacy and outsourcing regulations. *Journal of Business Research*, *97*, 235– 256. https://doi.org/10.1016/j.jbusres.2018.06.006

Hanisch, M., Goldsby, C. M., Fabian, N. E., & Oehmichen, J. (2023). Digital governance: A conceptual framework and research agenda. *Journal of Business Research, 162*, Article 113777. https://doi.org/10.1016/j.jbusres.2023.113777

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(1), Article 5. https://doi.org/10.1186/1869-0238-4-5

He, W., & Wang, F.-K. (2015). A hybrid cloud model for cloud adoption by multinational enterprises. *Journal of Global Information Management*, *23*(1), 1–23. https://doi.org/10.4018/jgim.2015010101

Hegde, T., Gangl, J., Babenko, S., & Coffman, J. (2024). Cloud security frameworks. In *Proceedings of the IEEE/ACM 16th International Conference on Utility and Cloud Computing (UCC '23)* (Article 58, pp. 1–6). ACM. https://doi.org/10.1145/3603166.3632553

Hillmann, P., Kesseler, M., Schnell, D., Mihelcic, G., & Karcher, A. (2024). Enterprise architecture governance of excellence. In *Proceedings of the 26th International Conference on Enterprise Information Systems (ICEIS 2024)* (Vol. 2, pp. 603–613). SCITEPRESS. https://doi.org/10.5220/0012399000003690

Jaatun, M. G., Pearson, S., Gittler, F., Leenes, R., & Niezen, M. (2020). Enhancing accountability in the cloud. *International Journal of Information Management*, 53, Article 101498. https://doi.org/10.1016/j.ijinfomgt.2016.03.004

Janssen, M. (2019). Governance as a condition for creating business value from enterprise architecture. In *Proceedings of the 21st International Conference on Enterprise Information Systems* (pp. 229–235). Springer. https://doi.org/10.1007/978-3-030-24854-3_16

Kajiyama, T., Jennex, M., & Addo, T. (2017). To cloud or not to cloud: How risks and threats are affecting cloud adoption decisions. *Information & Computer Security*, *25*(5), 634–659. https://doi.org/10.1108/ICS-07-2016-0051

Kurnia, S., Kotusev, S., Shanks, G., Dilnutt, R., Taylor, P., & Milton, S. K. (2021). Enterprise architecture practice under a magnifying glass: Linking artifacts, activities, benefits, and blockers. *Communications of the Association for Information Systems, 49*, 668–698. https://doi.org/10.17705/1CAIS.04936

Lins, S., Schneider, S., Szefer, J., Ibraheem, S., & Sunyaev, A. (2019). Designing monitoring systems for continuous certification of cloud services: Deriving meta-requirements and design guidelines. *Communications of the Association for Information Systems*, *44*(1). https://doi.org/10.17705/1CAIS.04425

Mayer, N., Aubert, J., Grandry, E., Feltus, C., Goettelmann, E., & Wieringa, R. (2019). An integrated conceptual model for information system security risk management supported by enterprise architecture management. *Software & Systems Modeling*, 18(3), 2285–2312. https://doi.org/10.1007/s10270-018-0661-x

Mazula, D., & Lamprecht, C. (2023). Redefining enterprise cloud technology governance. *ISACA Journal, 2023*(3). https://www.isaca.org/resources/isaca-journal/issues/2023/volume-3/redefining-enterprise-cloud-technology-governance

Milan Chauhan, & Stavros Shiaeles. (2023). An analysis of cloud security frameworks, problems and proposed solutions. *Network*, 3(3), 422–450. https://doi.org/10.3390/network3030018

Ouedraogo, M., Mignon, S., Cholez, H. et al. Security transparency: the next frontier for security research in the cloud. *J Cloud Comp 4*, 12 (2015). https://doi.org/10.1186/s13677-015-0037-5

Prasad, A., & Green, P. (2015). Governing cloud computing services: Reconsideration of IT governance structures. *International Journal of Accounting Information Systems, 19*, 45– 58. https://doi.org/10.1016/j.accinf.2015.11.004

Simhadri, S. (2025). From shared responsibility to shared fate: redefining cloud security paradigms in multi-cloud environments. *Computer Fraud & Security*. https://doi.org/10.52710/cfs.850

Spagnoletti, P., Kazemargi, N., Constantinides, P., & Prencipe, A. (2025). Data control coordination in the formation of ecosystems in highly regulated sectors. *Journal of the Association for Information Systems*, *26*(4), 977–1008. https://doi.org/10.17705/1jais.00920

Tamm, T., Seddon, P. B., & Shanks, G. (2022). How enterprise architecture leads to organisational benefits. *International Journal of Information Management, 67*, Article 102554. https://doi.org/10.1016/j.ijinfomgt.2022.102554

Tang, M. (2022). The challenge of the cloud: Between transnational capitalism and data sovereignty. *Information Communication & Society*, *25*(16), 2397–2411. https://doi.org/10.1080/1369118X.2022.2128598

Voss, W. G. (2020). Cross-border data flows, the GDPR, and data governance. *Washington International Law Journal*, *29*(3), 485–531.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, *26*(2), xiii–xxiii. https://doi.org/10.2307/4132319

Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business School Press.

Woods, A. K. (2018). Litigating data sovereignty. *Yale Law Journal*, *128*(2), 328–406.