Volume 1, Issue 1, Mei 2026
E-ISSN : xxx-xxxx

JOURNAL OF ADVANCED RESEARCH AND STUDIES IN COMPUTING AND INFORMATION SCIENCES

ellpub

Cloud Sovereignty, Data Governance, and Institutional Trust: Comparative Information Systems Transformation in the European Union and Australia, 2020–2026

Matthew Collins[1]

Matthew Collins

School of Computing and Information Systems
University of Melbourne
Email: matthew.collins@unimelb.edu.au

***Corresponding Author:** matthew.collins@unimelb.edu.au

Citation: Aziz (2026). Cloud Sovereignty, Data Governance, and Institutional Trust: Comparative Information Systems Transformation in the European Union and Australia, 2020–2026
Matthew Collins1 (Book Antiqua 14pt Bold). *Journal of Social Sciences and Humanities Perspectives*, *10*(4), xx–xx. https://doi.org/0000-0000

Published: 11/05/2026

ABSTRACT

This article examines cloud sovereignty and data governance as central challenges of contemporary information systems transformation through a comparative analysis of the European Union and Australia between 2020 and 2026. The study argues that cloud computing has evolved from an enterprise infrastructure model into a strategic governance architecture shaping digital sovereignty, cybersecurity, public-sector modernization, regulatory compliance, and economic resilience. The European Union and Australia were selected because both are advanced digital economies with extensive cloud adoption, yet they differ in regulatory philosophy, institutional architecture, market dependency, and sovereignty strategy. The European Union emphasizes regulatory sovereignty, data protection, interoperability, and trusted cloud ecosystems through GDPR, the Data Governance Act, the Data Act, and cloud certification initiatives. Australia emphasizes pragmatic cloud adoption, cybersecurity uplift, sovereign capability, and risk-based public-sector cloud governance. The findings indicate that cloud governance effectiveness depends on interoperability, procurement discipline, cybersecurity assurance, data classification, institutional coordination, and public trust. This article contributes to computing and information sciences by conceptualizing cloud sovereignty as a socio-technical governance framework linking infrastructure architecture, institutional accountability, digital innovation, and national resilience.

Keywords: cloud sovereignty; data governance; cloud computing; cybersecurity; information systems; European Union; Australia; digital sovereignty; public-sector transformation; institutional trust

INTRODUCTION

Cloud computing has become one of the foundational infrastructures of contemporary digital transformation. Between 2020 and 2026, public agencies, universities, hospitals, banks, logistics firms, and technology companies increasingly migrated workloads to cloud platforms to improve scalability, resilience, analytics, artificial intelligence capability, and cost efficiency. Yet the same transition has generated new governance challenges concerning data sovereignty, vendor dependency, cybersecurity, cross-border data transfers, public procurement, regulatory compliance, and institutional trust. Cloud computing is therefore no longer merely an information technology service model; it has become a strategic infrastructure of computational governance.

This study argues that cloud sovereignty should be understood as a socio-technical governance problem. The question is not whether data should remain physically located within national territory, but how institutions govern control, access, auditability, portability, jurisdictional exposure, cybersecurity assurance, and public accountability across distributed cloud environments. Cloud sovereignty thus connects computing architecture, legal authority, institutional implementation, economic innovation, and social trust.

The European Union and Australia provide analytically significant comparative cases. The European Union has developed one of the most elaborate digital sovereignty agendas in the world, linking cloud governance to data protection, competition policy, cybersecurity certification, interoperability, data spaces, and industrial strategy. Australia has pursued a more pragmatic and risk-based approach, emphasizing secure public-sector cloud adoption, cybersecurity resilience, critical infrastructure protection, and sovereign capability. Both systems depend heavily on global cloud service providers, but they differ in their governance response to dependency.

The global context underscores the significance of the topic. OECD and World Bank reports identify cloud computing as a major enabler of digital productivity, public-sector modernization, AI deployment, and data-driven innovation (OECD, 2024; World Bank, 2024). At the same time, cybersecurity reports show that cloud misconfiguration, identity compromise, ransomware, and supply-chain attacks have become central vectors of organizational risk (ENISA, 2023; World Economic Forum, 2024). Public institutions now face a complex governance dilemma: cloud platforms are necessary for digital modernization, but reliance on concentrated global providers may weaken sovereignty, resilience, and accountability.

Existing literature provides important foundations. Armbrust et al. (2010) conceptualized cloud computing as a scalable utility model transforming computing economics. Buyya et al. (2019) highlighted cloud systems as distributed computing infrastructures enabling elastic resource provisioning. Kitchin (2021) examined how data infrastructures reshape governance and social power. DeNardis (2020) argued that

control over digital infrastructure increasingly structures geopolitical and economic authority. Floridi (2023) emphasized that digital sovereignty concerns governance over informational environments rather than isolation from global networks. Other scholars analyze cloud governance through cybersecurity, privacy, public procurement, and platform dependency (Bradford, 2020; Lynskey, 2023; Shackelford, 2021).

However, current scholarship remains limited in several ways. While previous studies emphasize cloud adoption and technical architecture, they often under-theorize institutional accountability. Other studies examine digital sovereignty normatively but do not sufficiently analyze cloud architecture, interoperability, identity management, encryption, data classification, and procurement governance. Existing literature also remains limited in comparing how advanced democracies manage cloud dependency under different regulatory and institutional conditions.

This article identifies five research gaps. First, a theoretical gap persists in conceptualizing cloud sovereignty as computational governance rather than territorial data localization. Second, an empirical gap concerns how cloud governance affects public-sector implementation and institutional trust. Third, a comparative gap exists regarding regulatory-sovereignty and pragmatic-risk cloud governance models. Fourth, a technological governance gap concerns how architecture choices such as multi-cloud, sovereign cloud, encryption, portability, and identity federation shape accountability. Fifth, a computational-policy gap concerns how cloud dependency affects innovation capacity, resilience, and economic development.

The novelty of this article lies in developing cloud sovereignty as a socio-technical governance framework. The article contributes to computing and information sciences by integrating cloud architecture, information systems governance, cybersecurity, public administration, and digital policy. The study argues that sovereignty in cloud environments is not achieved through isolation but through accountable control over infrastructure dependencies, data flows, access rights, and institutional responsibilities.

The analytical framework links cloud architecture to governance control, institutional accountability, digital trust, innovation capacity, and socio-economic resilience. The causal logic is as follows: cloud architecture shapes data location, access, and dependency; governance controls determine accountability and compliance; accountability influences institutional trust; trust affects adoption and innovation; innovation and resilience shape socio-economic transformation. The research objective is to examine how the European Union and Australia governed cloud sovereignty and data governance between 2020 and 2026 and to evaluate the implications for computing, institutional implementation, and digital transformation.

METHODOLOGY

This study employs a comparative information systems governance methodology integrating cloud architecture analysis, computational governance theory, institutional process tracing, and digital policy evaluation. The European Union and Australia were selected because they are advanced digital economies with high cloud adoption, strong cybersecurity agendas, and significant public-sector digital transformation programs, yet they differ in regulatory philosophy and institutional architecture. The European Union represents a regulatory-sovereignty model grounded in

data protection, interoperability, cybersecurity certification, digital market regulation, and strategic autonomy. Australia represents a pragmatic-risk governance model emphasizing secure cloud adoption, critical infrastructure resilience, sovereign capability, and operational cybersecurity. The unit of analysis is the cloud governance ecosystem, including legal frameworks, cloud procurement systems, cybersecurity requirements, data classification schemes, interoperability standards, public-sector adoption, vendor dependency, and institutional trust mechanisms.

The empirical basis consists of European Union digital governance instruments, Australian government cloud and cybersecurity strategies, OECD and World Bank digital economy reports, ENISA cybersecurity reports, cloud security frameworks, public procurement guidance, institutional technology reports, and peer-reviewed computing and information systems literature from 2020–2026. The analysis combines comparative architecture assessment, document-based process tracing, and socio-technical interpretation to identify causal mechanisms linking cloud design to governance outcomes. Triangulation is achieved by comparing policy frameworks, technical standards, institutional reports, and scholarly evidence. Ethical considerations include privacy, surveillance, vendor lock-in, jurisdictional exposure, public-sector dependency, and cybersecurity risk. The principal limitation is that detailed cloud contracts, incident data, and sovereign cloud performance metrics are often confidential. Nevertheless, the comparative framework provides a robust basis for evaluating cloud sovereignty as an information systems governance problem.

Findings and Discussion

1. Cloud Sovereignty as Control Rather Than Localization

The first finding is that cloud sovereignty is more accurately understood as accountable control than simple data localization. The European Union has increasingly framed cloud governance through digital sovereignty, data protection, interoperability, and trusted data spaces. GDPR provides strong legal foundations for personal data processing and cross-border transfer control, while the Data Governance Act and Data Act seek to improve data sharing, portability, and fair access. European cloud certification initiatives further aim to increase trust in cloud services through security assurance and compliance standards.

Australia's approach is less explicitly sovereignty-centered but strongly focused on risk management and secure adoption. Public-sector cloud governance emphasizes data classification, security assessment, procurement controls, and cyber resilience. Rather than seeking full infrastructural independence, Australia has prioritized trusted cloud use and sovereign capability in sensitive domains.

The comparison reveals that sovereignty does not require complete domestic ownership of cloud infrastructure. Instead, it requires enforceable control over access, jurisdiction, security, portability, and accountability. A cloud system may be locally hosted but poorly governed; conversely, a cross-border cloud system may be accountable if contractual, technical, and legal safeguards are robust.

This finding challenges simplistic localization narratives. Cloud sovereignty is multidimensional. It includes legal sovereignty, operational sovereignty, technological sovereignty, and institutional sovereignty. Effective governance therefore requires a layered approach integrating law, architecture, procurement, cybersecurity, and oversight.

2. Interoperability, Portability, and Vendor Dependency

The second finding is that interoperability and portability are central to cloud governance because they determine whether institutions can avoid lock-in and preserve strategic flexibility. The European Union has increasingly emphasized data portability, interoperability standards, and contestable digital markets. These priorities reflect concerns that concentrated hyperscale cloud markets may produce dependency and weaken public-sector bargaining power.

Australia similarly faces vendor dependency risks because public institutions rely heavily on global cloud providers. However, Australia's approach is more procurement-oriented and operational, focusing on contract management, security accreditation, and risk assessment rather than broad market restructuring.

The comparison demonstrates that vendor dependency is not only an economic issue; it is an information systems governance issue. Cloud platforms shape system architecture, data formats, identity management, application development, analytics capability, and cybersecurity operations. Once institutions build deeply around proprietary services, migration becomes costly and technically complex.

This finding extends platform governance scholarship by showing that cloud dependency creates infrastructural power. Cloud providers do not simply host systems; they shape computational possibilities. Therefore, public institutions require portability strategies, multi-cloud governance, open standards, exit planning, and procurement expertise.

3. Cybersecurity Assurance and Institutional Resilience

The third finding is that cybersecurity assurance is the operational foundation of cloud trust. Cloud adoption can improve security through professionalized infrastructure, continuous monitoring, redundancy, and advanced identity systems. Yet it also introduces risks related to misconfiguration, identity compromise, shared responsibility ambiguity, and supply-chain exposure.

The European Union addresses these risks through cybersecurity regulation, ENISA guidance, certification schemes, and data protection enforcement. The emphasis is on harmonized assurance and regulatory trust. Australia addresses cloud security through national cybersecurity strategy, critical infrastructure regulation, and public-sector security frameworks. The emphasis is operational readiness and resilience.

The comparative evidence indicates that cloud resilience depends on shared responsibility clarity. Organizations often misunderstand which security obligations belong to cloud providers and which remain with customers. This creates governance gaps. Effective cloud governance requires identity and access management, encryption, logging, configuration management, incident response, and continuous compliance monitoring.

This finding contributes to information security literature by showing that cloud security is a governance relationship rather than a product feature. Institutional resilience requires technical controls and organizational capability.

4. Public-Sector Transformation and Digital Trust

The fourth finding is that cloud governance shapes public-sector transformation and institutional trust. Cloud computing enables scalable digital services, AI analytics, data integration, and remote administration. However, public trust depends on whether citizens believe that public data are securely, lawfully, and accountably governed.

The European Union's rights-based governance model strengthens trust by embedding cloud use within data protection and digital rights frameworks. However, regulatory complexity may slow implementation and increase compliance burdens. Australia's pragmatic approach may accelerate adoption and operational modernization but requires strong transparency to maintain legitimacy.

The comparison indicates that digital trust is produced through alignment between technical capability and institutional accountability. Public agencies cannot rely solely on cloud provider assurances. They must demonstrate oversight capacity, security competence, data minimization, and accountability.

The socio-economic implications are significant. Trusted cloud systems enable digital public services, research infrastructures, AI innovation, and small-business digital transformation. Weak cloud governance may produce breaches, lock-in, public distrust, and strategic vulnerability.

Table 1. Analytical Matrix of Comparative Computing Governance and Information Systems Development

Variable	Case 1: European Union	Case 2: Australia	Empirical Evidence	Analytical Interpretation
Governance Model	Regulatory sovereignty and digital autonomy	Pragmatic risk-based cloud governance	GDPR, Data Act, cloud certification; Australian cloud and cyber strategies	Different governance philosophies shape cloud control
Sovereignty Logic	Legal, data, and market sovereignty	Security, resilience, and sovereign capability	EU digital sovereignty agenda; Australian cyber resilience policy	Sovereignty is multidimensional
Cloud Architecture Priority	Interoperability, portability, trusted data spaces	Secure adoption, classification, operational assurance	EU data spaces; public-sector cloud guidance	Architecture determines governance flexibility
Vendor Dependency	Addressed through regulation and market contestability	Addressed through procurement and risk management	Digital markets and procurement reports	Dependency is institutional and technical
Cybersecurity Model	Harmonized certification and regulatory assurance	Operational cybersecurity and critical infrastructure resilience	ENISA reports; Australian cybersecurity strategy	Security assurance creates institutional trust
Data Governance	Strong rights-based personal data governance	Risk-based data classification and control	GDPR and data governance instruments	Data rules shape cloud legitimacy
Institutional	Multi-level	National	EU digital	Coordination

Coordination	EU governance across member states	public-sector coordination	policy structures; Australian government cloud governance	affects implementation consistency
Innovation Outcome	Trusted data economy and AI-ready infrastructure	Accelerated cloud adoption and digital service delivery	OECD and World Bank digital economy reports	Governance influences innovation pathways
Public Trust Mechanism	Rights, compliance, and certification	Security, reliability, and service continuity	Regulatory and institutional trust frameworks	Trust emerges from accountability plus performance
Socio-Economic Implication	Strategic autonomy and data-driven innovation	Resilient digital government and cloud-enabled economy	Digital transformation reports	Cloud governance shapes national resilience

The table demonstrates that cloud governance cannot be reduced to data location or provider choice. The European Union and Australia illustrate different pathways toward trusted cloud transformation. The EU emphasizes regulatory sovereignty, legal safeguards, and market structuring. Australia emphasizes cyber resilience, procurement discipline, and pragmatic institutional implementation. The deeper analytical insight is that cloud sovereignty emerges from the interaction of architecture, law, procurement, cybersecurity, and institutional trust.

Conceptual Model

Cloud Sovereignty Governance Model

Cloud Architecture → Control Mechanisms → Institutional Accountability → Digital Trust → Innovation Capacity → Socio-Economic Resilience

This model proposes that cloud architecture determines where data are stored, how systems interact, which actors control access, and how dependency is structured. Control mechanisms such as encryption, identity management, data classification, portability, and contractual safeguards create institutional accountability. Accountability produces digital trust among public agencies, firms, and citizens. Trust enables adoption and innovation. Innovation capacity supports productivity, public-sector modernization, AI deployment, and socio-economic resilience.

The model contributes to computing and information sciences by showing that cloud sovereignty is not merely a legal or geopolitical concept. It is an information systems governance model in which technical architecture and institutional design jointly determine public value.

CONCLUSION

This article examined cloud sovereignty and data governance in the European Union and Australia between 2020 and 2026. The study directly answers the research objective by demonstrating that cloud sovereignty is best understood as accountable control over cloud dependencies rather than territorial localization alone.

The findings show that the European Union and Australia represent distinct but complementary governance models. The European Union emphasizes regulatory sovereignty, data protection, interoperability, and trusted cloud ecosystems. Australia emphasizes secure adoption, cyber resilience, pragmatic risk management, and sovereign capability. Both models reveal that cloud transformation requires more than migration to scalable infrastructure. It requires governance over vendor dependency, cybersecurity, portability, data access, and institutional responsibility.

The theoretical contribution is the cloud sovereignty governance model, which links architecture, control mechanisms, accountability, digital trust, innovation capacity, and socio-economic resilience. The empirical contribution lies in comparing two advanced digital governance systems through information systems variables rather than generic cloud adoption narratives.

The technological governance implications are substantial. Public institutions should adopt cloud strategies that include portability planning, multi-cloud governance, identity control, encryption, auditability, data classification, procurement transparency, and incident response readiness. Information systems policy should treat cloud infrastructure as public governance infrastructure.

The study is limited by restricted access to proprietary cloud contract data and confidential incident metrics. Future research should compare sovereign cloud initiatives in Germany, France, Singapore, Japan, and Canada, and should empirically evaluate the performance of multi-cloud and hybrid-cloud governance models.

Ultimately, cloud computing will remain central to digital transformation. Its public value will depend not on scalability alone but on whether institutions can govern cloud infrastructures with accountability, resilience, and trust.

REFERENCES

Armbrust, M., Fox, A., Griffith, R., et al. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50–58.

Bradford, A. (2020). The Brussels effect: How the European Union rules the world. Oxford University Press.

Buyya, R., Srirama, S. N., Casale, G., et al. (2019). A manifesto for future generation cloud computing. ACM Computing Surveys, 51(5), 1–38.

DeNardis, L. (2020). The internet in everything: Freedom and security in a world with no off switch. Yale

University Press.

ENISA. (2023). Cloud cybersecurity and certification frameworks. European Union Agency for Cybersecurity.

Floridi, L. (2023). The ethics of artificial intelligence: Principles, challenges, and opportunities. Oxford University Press.

Kitchin, R. (2021). Data lives: How data are made and shape our world. Bristol University Press.

Lynskey, O. (2023). Grappling with data power. Theoretical Inquiries in Law, 24(1), 189–220.

OECD. (2024). Digital economy outlook 2024. OECD Publishing.

Shackelford, S. J. (2021). Cybersecurity law, policy, and governance. Cambridge University Press.

World Bank. (2024). Digital progress and trends report. World Bank.

World Economic Forum. (2024). Global cybersecurity outlook 2024. World Economic Forum.

