Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Secure Multi-Cloud Architectures for State Governments: A Governance-First Approach

Swapan Arora

Independent Researcher, USA

ARTICLE INFO

Received: 12 Feb 2026

Revised: 15 Feb 2026

ABSTRACT

State governments increasingly adopt multi-cloud strategies to enhance service delivery and reduce vendor dependencies, yet security governance remains fragmented across platforms. This article presents a governance-first architecture framework specifically designed for government multi-cloud environments that establishes centralized identity management, unified policy enforcement, and integrated compliance monitoring as foundational elements preceding workload deployment. The framework addresses critical security challenges, including fragmented identity and access management systems, inconsistent logging and monitoring capabilities, policy drift across platforms, and complex regulatory compliance requirements. Implementation follows a structured four-phase deployment strategy encompassing foundation establishment, identity integration, policy harmonization, and advanced governance capabilities. The governance-first architecture transforms traditional reactive security approaches into proactive governance-centered strategies that treat identity as the primary control plane for all multi-cloud operations. Technical implementation leverages cloud-native mechanisms while maintaining consistency through centralized governance policies that automatically translate into platform-specific configurations. Cost-benefit evaluation demonstrates substantial long-term operational benefits, including reduced security incidents, improved compliance audit efficiency, and decreased administrative overhead despite significant upfront investment requirements. The article concludes that governance-first architecture enables State governments to maintain security consistency while leveraging diverse cloud capabilities, ultimately supporting enhanced citizen services while meeting stringent regulatory requirements.

Keywords: Multi-Cloud Security, Governance Framework, Identity Federation, Policy Management, Government Cloud Computing

1. Introduction and Multi-Cloud Adoption Landscape

State government organizations throughout America face mounting pressure to modernize their technology infrastructure. Citizens expect digital services that match private sector experiences. Traditional systems find it difficult to satisfy these changing requirements. Solutions that conventional data centers cannot deliver are available via cloud computing. Government organizations see the need for scalable and flexible technology systems. Multi-cloud strategies have emerged as the preferred solution for complex government requirements. These strategies combine services from different cloud providers to optimize performance and reduce risks. Technology leaders in State governments prioritize cloud adoption as essential for operational improvement. The shift toward cloud computing represents more than a simple technology migration. It fundamentally changes how the government delivers services to citizens. Modern cloud platforms enable innovation while maintaining the security standards required for public sector operations [1].

Vendor diversification drives many government cloud adoption decisions. Single-vendor relationships present dependency issues that governmental agencies try to avoid. Vendor rivalry helps to keep prices and service standards reasonable. Government policies on procurement promote competitive settings for technological acquisitions. Different cloud providers excel in specific service areas rather

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

than offering uniform capabilities across all domains. Transportation departments benefit from providers with strong Internet of Things platforms. Public safety agencies require specialized security and compliance features. Administrative offices need robust productivity and collaboration tools. Data analytics capabilities support evidence-based policy development across various government functions. This specialization means that no single provider can optimally serve all government needs simultaneously [2].

Regulatory compliance adds complexity to government cloud selection processes. Federal programs establish baseline security requirements for government cloud services. State privacy laws impose additional restrictions on data handling and storage. Specialized government functions face sector-specific compliance requirements. Law enforcement agencies must meet criminal justice information standards. Healthcare-related government services require adherence to privacy regulations. Financial services within the government face banking and monetary oversight requirements. Each compliance framework influences which cloud providers and services government agencies can utilize. These regulatory constraints often necessitate different cloud platforms for different types of government data and applications. Compliance considerations frequently override cost or convenience factors in government cloud decisions [1].

Security challenges multiply when government organizations operate across multiple cloud platforms simultaneously. Each cloud provider implements unique security models and management interfaces. Identity management becomes fragmented when spread across different platforms. User accounts and permissions must be managed separately for each cloud environment. Monitoring and logging systems operate independently without coordination between platforms. Security policies may drift apart over time as different teams manage different cloud environments. These fragmentation issues create blind spots in government security operations. Threat detection becomes more difficult when security events are scattered across multiple systems. Incident response procedures must account for complex multi-platform scenarios. Government security teams struggle to maintain comprehensive visibility across their entire cloud footprint [2].

Traditional security frameworks focus on single-platform environments. These approaches prove inadequate for multi-cloud government operations. Existing frameworks do not address the unique challenges of public sector multi-cloud deployments. Government organizations face stricter regulatory requirements than private companies. Public sector risk tolerance differs significantly from commercial risk acceptance. Current security solutions often ignore these fundamental differences between government and private sector needs. Academic literature predominantly examines private sector multi-cloud implementations. Government-specific security challenges receive limited attention in existing publications. This gap leaves government organizations without adequate guidance for secure multi-cloud operations [2].

The governance-first architecture framework presented in this article addresses these critical gaps. It establishes governance mechanisms before deploying workloads across cloud platforms. Identity management becomes centralized across all cloud environments. Policy enforcement maintains consistency regardless of which cloud platform hosts specific services. Compliance monitoring integrates data from all platforms into unified reporting systems. This approach prevents the fragmentation issues that plague traditional multi-cloud implementations. Government organizations can maintain security oversight while benefiting from multi-cloud capabilities. The framework enables secure utilization of specialized services from different cloud providers. Centralized governance ensures that security standards remain consistent across all platforms [1].

Identity serves as the foundation for all security decisions in this governance model. Every access request undergoes evaluation through centralized identity systems. Resource provisioning follows consistent authorization processes across all cloud platforms. Security policies apply uniformly regardless of where government workloads operate. This consistency removes the security loopholes

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

often seen in multi-cloud situations. Government organizations can use the finest features of several cloud providers while keeping centralized control. Citizens receive better services through optimized cloud utilization. Security requirements remain satisfied through unified governance mechanisms that span all cloud platforms utilized by government organizations [2].

Driver Category	Government Requirements	Implementation Impact
Vendor Diversification	Avoid single-vendor dependencies and maintain competitive procurement environments	Reduces contract negotiation risks while requiring multi-platform expertise
Specialized Services	Access platform-specific capabilities for transportation, public safety, and analytics	Enables optimal service delivery but increases integration complexity
Regulatory Compliance	Meet federal mandates, State privacy laws, and sector-specific requirements	Ensures legal compliance while creating platform selection constraints

Table 1: Multi-Cloud Adoption Drivers in Government Environments. [2]

2. Security Challenges in Government Multi-Cloud Environments

Public sector organizations face serious security problems when using multiple cloud services. Government data requires stronger protection than typical business information. Cloud providers each have their own security methods and tools. Connecting different cloud systems creates new vulnerabilities. Hackers look for weak points between different platforms. Government IT departments struggle to protect all their cloud systems equally. Many security tools work well for single cloud setups but fail with multiple providers. The complexity grows rapidly as agencies add more cloud services. Traditional security methods cannot handle this increased complexity effectively [3].

Managing user accounts across different cloud platforms creates major headaches for government agencies. Workers need access to systems on various cloud providers during their daily tasks. Each cloud service requires its own login process and password requirements. Employees end up with numerous usernames and passwords to remember. IT staff must create accounts separately on every cloud platform. Password resets become time-consuming when spread across multiple systems. Removing access for departing employees requires actions on each platform. Tracking who has access to what gets almost impossible. When user data is distributed across everything, security audits get difficult. Many organizations forget to deactivate dormant accounts [3].

Security monitoring becomes fragmented when government agencies use multiple cloud providers. Each platform generates different types of security logs with unique formats. Security teams cannot easily combine information from different cloud systems. Analysts need training on separate tools for each cloud provider. Finding patterns across multiple platforms requires manual work and expertise. Automated threat detection systems cannot see the complete picture. Security incidents may be missed when they involve multiple cloud platforms. Response times slow down when teams must check several different systems. Investigation becomes difficult when evidence is spread across platforms. Many agencies end up with separate security teams for each cloud provider [4].

Security settings drift apart over time across different cloud platforms. Government agencies create detailed security policies for all their systems. However, each cloud provider has different ways to

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

implement these policies. IT teams must manually configure security settings on each platform. These manual processes lead to differences between supposedly identical systems. Updates get applied inconsistently across different cloud environments. Security assessments often reveal unexpected variations between platforms. Some systems end up with stronger protection than others. Attackers can exploit these differences to move between systems. Maintaining consistent security becomes a constant struggle for government IT departments [3].

Compliance becomes much harder when government operations span multiple cloud platforms. Federal regulations apply to all government cloud systems regardless of the provider. State laws add extra requirements for handling citizen information. Different government departments face specialized compliance rules. Each cloud provider offers different tools for meeting compliance requirements. Documentation formats vary between providers, making reporting difficult. Auditors struggle to evaluate compliance when systems are spread across platforms. Evidence collection requires accessing multiple separate systems. Certification processes may conflict between different platforms. Many agencies fail compliance checks due to gaps in their oversight [4].

Recent security breaches show the real dangers of fragmented cloud operations. State agencies have suffered attacks that went unnoticed for many months. These attacks often start with stolen passwords on one cloud platform. Hackers then move to other platforms through poorly configured connections. Separate monitoring systems fail to detect movement between platforms. Attack warning signs get lost in different logging systems. Investigations show that security varied significantly between platforms. Weaker security on some platforms made attacks easier. Recovery efforts struggle with coordination across multiple providers. Many agencies discover their incident response plans are inadequate for multi-platform attacks [3].

Most government agencies handle multi-cloud security through separate approaches for each provider. Different security products get installed for each cloud platform independently. Teams develop expertise in specific platforms rather than overall security. This creates communication problems between teams managing different platforms. Security rules get interpreted differently by teams with different backgrounds. Response procedures vary between platforms instead of being standardized. Information sharing suffers due to different tools and methods. The result is incomplete security coverage with dangerous gaps. Critical vulnerabilities emerge where different platforms connect [4].

Challenge Area	Primary Issues	Operational Impact
Identity Management	Fragmented authentication across platforms with separate credential requirements	Increases security risks and administrative overhead for user lifecycle management
Monitoring Fragmentation	Independent logging systems with different formats and correlation difficulties	Creates security blind spots and delays incident detection across platforms
Policy Drift	Gradual configuration divergence between platforms despite identical intentions	Enables attack vectors through inconsistent security implementations

Table 2: Critical Security Challenges in Government Multi-Cloud Deployments. [4]

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3. Governance-First Architecture Framework

The governance-first architecture framework represents a systematic reconceptualization of multi-cloud security that prioritizes the establishment of centralized governance capabilities as the essential foundation. This approach fundamentally reverses traditional implementation sequences by mandating comprehensive governance infrastructure deployment before workload implementation. Identity federation, policy management, and compliance monitoring must be fully operational before any application workloads are deployed across cloud platforms. The framework's theoretical foundation rests upon established principles from enterprise architecture governance frameworks that have proven effective in complex environments. Control objectives for information systems provide the foundational governance structure for multi-cloud implementations. Architecture framework governance models are specifically adapted for cloud environments to address unique challenges. Zero-trust security principles are integrated with policy-as-code methodologies to create unified governance models across platforms. Every access request, resource deployment, and configuration change becomes subject to centralized policy evaluation regardless of origin. This evaluation occurs regardless of the originating cloud platform or service type being accessed. The approach treats identity as the fundamental control plane for all multi-cloud operations across government systems requiring consistent security oversight [5].

The architectural model operates through a three-tier hierarchy designed to separate governance concerns from platform-specific implementation details effectively and efficiently. The Strategic Governance Tier establishes high-level policies, compliance requirements, and security objectives that remain constant regardless of underlying cloud platform changes or updates. This tier houses executive dashboards that provide leadership visibility into multi-cloud operations and strategic decision-making capabilities. Regulatory reporting capabilities are centralized within this tier to ensure consistent compliance documentation across all government systems. Strategic decision-making tools are provided for government leadership to maintain comprehensive oversight of multi-cloud operations and resource allocation. The Tactical Governance Tier translates strategic objectives into specific technical policies and operational procedures for implementation teams throughout the organization. This tier serves as the critical bridge between high-level governance requirements and platform-specific implementations that must be executed. Policy translation services convert abstract governance requirements into actionable technical specifications that can be implemented consistently. The Operational Governance Tier consists of platform-specific services and tools that implement governance decisions using native cloud capabilities optimized for performance. This tier maintains strict consistency with centralized policies while leveraging optimal platform-specific security features available from each provider [6].

Identity federation serves as the cornerstone of the governance framework by establishing a single authoritative source for all authentication and authorization decisions across platforms. The federated identity system implements a hub-and-spoke architecture where a central identity provider maintains authoritative identity information for all users. Government-certified solutions provide the foundation for enterprise-scale identity management across multiple cloud platforms simultaneously without compromising security. Cloud-native identity services can be leveraged when they meet stringent government security and compliance requirements established by regulatory frameworks. The central identity provider maintains comprehensive identity information for all users, including employees, contractors, and citizens accessing government services through various channels. Industry-standard protocols enable seamless integration across diverse technology environments that government organizations typically maintain in their infrastructure. Security assertion markup language provides web-based single sign-on capabilities for government applications requiring authenticated access. OpenID Connect enables modern application integration with standardized authentication flows that ensure consistent user experiences. Lightweight directory access protocol ensures compatibility with legacy government systems that cannot be immediately modernized or replaced [5].

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Centralized identity management provides several critical security advantages specifically designed for government organizational requirements and operational constraints. User lifecycle management becomes streamlined through single points of control for provisioning, modification, and deprovisioning access rights across all systems. Role-based access control can be implemented consistently using government-specific organizational structures and delegation patterns that reflect hierarchical authority structures. Emergency access procedures can be standardized and audited across all platforms during crises when rapid response is essential. Government organizations must maintain operational capabilities during emergency response scenarios requiring rapid access provisioning for temporary personnel and contractors. The unified policy engine represents the second foundational component implementing centralized definition, evaluation, and enforcement of security policies across all platforms. Open policy frameworks with specialized policy languages provide platform-agnostic policy definition capabilities for complex government requirements. Extensible Access Control Markup Language offers standardized policy expression for complex government requirements that span multiple regulatory frameworks. These standardized policy languages define platform-agnostic security rules that are subsequently translated into cloud-specific implementations automatically. Automated policy translation services ensure semantic consistency across different cloud platforms while leveraging optimal security capabilities available from each provider [6].

Policy definition follows a hierarchical model where high-level government security requirements are progressively refined into specific technical controls for implementation teams. Data governance policies define classification schemes, handling procedures, and retention requirements that automatically apply regardless of storage platform or location. Network security policies establish consistent firewall rules, network segmentation, and traffic monitoring across all cloud environments without exception. Compliance policies ensure regulatory requirements are consistently implemented and monitored across platforms with automated report generation capabilities. Cross-cloud compliance monitoring provides continuous visibility into security posture and regulatory compliance through unified data collection and analysis systems. Standardized collection agents are deployed across all cloud platforms to gather security-relevant telemetry, including access logs and configuration changes, systematically. Network traffic patterns and compliance-related events are continuously monitored across all government systems to detect anomalies and policy violations. Data normalization processes convert disparate log formats into common schemas for unified analysis and correlation across platforms. Unified rule sets identify security incidents, policy violations, and compliance deviations across all platforms simultaneously, enabling rapid response [7].

The monitoring framework supports both real-time alerting and historical analysis capabilities essential for government security operations and regulatory compliance requirements. Real-time monitoring enables immediate response to security incidents or policy violations through unified security operations center dashboards that provide comprehensive visibility. Historical analysis supports forensic investigations, compliance audits, and trend analysis for continuous improvement of security postures over time. Government organizations can identify emerging security risks and optimize their security postures through comprehensive data analysis and pattern recognition. Technical implementation of the governance framework leverages cloud-native services wherever possible to ensure optimal performance and scalability for government workloads. Identity federation utilizes each cloud platform's native identity services while maintaining consistency through centralized policy management and enforcement mechanisms. Resource roles are dynamically configured based on centralized identity decisions across all platforms, ensuring consistent access control implementation. Directory services are integrated through federation trusts that maintain security boundaries while enabling seamless user experiences. Identity and access management policies are synchronized with centralized authorization decisions automatically, reducing administrative overhead and potential errors [5].

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Policy enforcement utilizes cloud-native mechanisms, including resource tags for automated policy application across government workloads deployed on various platforms. Service control policies provide account-level restrictions that cannot be overridden by local administrators, ensuring consistent security enforcement. Admission controllers ensure that container-based workloads comply with governance policies before deployment, preventing non-compliant systems from operating. Maintaining consistency across the whole infrastructure, this approach guarantees governance rules are implemented using the most efficient tools on each platform. Integration patterns with the current government IT infrastructure note that State governments often run hybrid environments combining several technologies. On-premises systems, legacy apps, and cloud services have to operate perfectly together without endangering security or practical efficiency. Secure hybrid connection guarantees governance rules apply consistently across all components of infrastructure by means of specialized network links. Legacy system integration enables governance to be extended to already operating systems using standardized interfaces and communication protocols. Centralized governance can help current systems without needing major changes to operational procedures or total system replacements [6].

Architecture Tier	Core Components	Primary Functions
Strategic Governance	Executive dashboards, regulatory reporting, strategic decision tools	Establishes high-level policies and maintains leadership oversight of multi-cloud operations
Tactical Governance	Policy translation services, operational procedures, and integration management	Bridges strategic requirements with platform-specific technical implementations
Operational Governance	Platform-native services, automated enforcement, and real-time monitoring	Implements governance decisions using cloud-native mechanisms while maintaining consistency

Table 3: Governance-First Architecture Framework Components. [6]

4. Implementation Strategy and Operational Considerations

Planning carefully is needed to implement multi-cloud governance in government. Operating differently from businesses, government agencies. Bureaucratic systems can greatly extend project deadlines. Every change must satisfy strict regulatory standards. Service disruptions can impact millions of citizens directly. Government IT leaders prefer cautious approaches over risky innovations. A four-stage rollout works best for most agencies. Each stage builds on previous accomplishments without breaking existing systems. This method reduces anxiety among staff and leadership. Foundation work happens first before complex integrations begin [8].

Setting up core infrastructure comes first in any successful implementation. Identity management systems get installed before touching existing authentication. Security frameworks are developed in test environments away from production. Monitoring capabilities start tracking baseline performance immediately. Training begins early so staff understand upcoming changes. Government procurement adds months to typical installation schedules. Extra time actually helps because thorough testing becomes possible. Current operations continue unchanged while new systems prove themselves. Identity consolidation starts during the second stage of rollout. User accounts slowly move from individual platforms to centralized management. Old login systems stay operational as safety nets during migration. Groups of users transfer in waves rather than all at once. Technical teams watch carefully for any signs of trouble [9].

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Security policy enforcement begins in the third implementation phase. Rules start as monitoring tools that observe but do not block. This reveals conflicts before they cause service outages. Active enforcement grows stronger as confidence builds in system stability. Advanced features like automatic compliance checking arrive in the final phase. Each completed stage demonstrates value to skeptical stakeholders. Leadership sees measurable progress through regular status reports. Gradual implementation builds trust while reducing project risks. Workers adapt to new processes without feeling overwhelmed. Citizens never experience service interruptions during the entire transformation [8].

Managing organizational change proves just as important as technical implementation. Government employees often distrust new technology initiatives. Previous failed projects create lasting skepticism about innovation. Approval processes involve many people who must be convinced separately. Conservative cultures resist anything that seems risky or unproven. Success demands addressing different concerns at each organizational level. Senior executives want clear evidence of benefits and reasonable costs. Department managers focus on resource needs and staff training requirements. Technical workers worry about learning unfamiliar systems under tight deadlines. Tailored messaging helps each group understand their role in the transformation. Consistent communication maintains momentum during lengthy rollout periods [9].

Staff education goes far beyond typical computer training programs. Most government IT professionals know their current systems extremely well. However, multi-cloud governance introduces completely new concepts and approaches. Identity management across platforms requires specialized knowledge. Security policy creation uses languages many have never encountered. Monitoring multiple systems simultaneously demands different analytical skills. Compliance reporting combines technical expertise with regulatory understanding. Training must fit busy schedules and different learning preferences. Basic ideas are thoroughly discussed in conventional classroom sessions. Hands-on laboratories allow people to practice without endangering production processes. Experienced staff members guide new recruits through challenging transitions using mentor relationships. As technology advances, ongoing learning keeps abilities strong [8].

Budget analysis reveals high initial costs but strong long-term value. Software licenses and consulting fees create substantial startup expenses. New hardware and network upgrades add to early financial requirements. Training programs also require significant investment in human resources. Yet operational benefits begin appearing within the first year. Security problems become less frequent and less damaging. Compliance audits require much less manual preparation time. Daily administration tasks become more efficient through automation. Contract negotiations improve when agencies avoid vendor lock-in situations. Backup and recovery procedures work better with consistent governance. Most government organizations recover their investment within typical budget cycles [10].

Measuring success requires tracking progress across multiple dimensions simultaneously. Technical indicators show whether systems perform as designed. User adoption rates reveal how quickly people embrace new processes. Security metrics demonstrate improvements in threat detection and response. Operational measures track efficiency gains in routine administrative tasks. Staff productivity increases as unified interfaces replace multiple separate tools. Audit preparation becomes faster through automated documentation systems. Long-term strategic goals include better compliance scores and stronger security postures. Pilot projects teach valuable lessons that help larger deployments succeed [8].

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Implementation Phase	Key Activities	Success Indicators
Foundation Establishment	Deploy identity infrastructure, develop policies, establish monitoring	Identity system deployment completion and staff training metrics
Identity Integration	Consolidate user accounts, maintain legacy fallbacks, and migrate user groups	User adoption rates and authentication system integration percentages
Policy Harmonization	Enforce unified policies, monitor compliance, automate reporting	Policy compliance rates and security incident reduction measurements

Table 4: Implementation Phases and Success Metrics. [10]

Conclusion

The implementation of governance-first architecture for State government multi-cloud environments represents a fundamental advancement in addressing complex security and operational challenges inherent in public sector cloud adoption. The framework demonstrates that by establishing comprehensive governance mechanisms before workload deployment, government organizations achieve substantial improvements in security posture, regulatory compliance, and operational efficiency while maintaining the strategic benefits of multi-cloud implementations. Enhanced security consistency through centralized policy definition and enforcement across platforms, significantly improved compliance capabilities with automated monitoring and reporting, reduced operational complexity through unified management interfaces, and increased strategic flexibility through minimized vendor dependencies characterize the primary benefits of governance-first implementation. Organizations completing governance-first implementations typically report substantial reductions in security incidents, improvements in compliance audit efficiency, and reductions in administrative overhead within reasonable timeframes. Strategic implications for government leadership extend beyond immediate operational improvements to encompass fundamental changes in technology governance approaches and cloud strategy development. The framework enables aggressive cloud adoption strategies by providing confidence that security and compliance requirements maintain consistency regardless of platform choices, supporting innovation while managing risks effectively. However, several limitations constrain current implementations, including a focus on established cloud providers without addressing emerging services, limited analysis of smaller government entity requirements, and insufficient evaluation of international considerations for cross-border operations. Future opportunities include longitudinal outcome tracking across multiple organizations, comparative analysis across different governmental structures, emerging technology integration, including artificial intelligence and edge computing governance, and cross-jurisdictional studies examining implementation success factors across diverse regulatory environments. Government chief information officers should prioritize governance infrastructure investment as a prerequisite for expanded cloud adoption, establish cross-functional governance teams combining security and compliance expertise, develop collaborative relationships with other entities to share costs and experiences, and advocate for standardized governance frameworks to reduce complexity. Governance-first architecture provides a proven methodology for managing multi-cloud complexity while delivering measurable improvements in security, compliance, and operational effectiveness essential for government service delivery in interconnected environments.

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

References

[1] David Cumbow, "Breaking Down the NASCIO Top 10 for 2023," Cybersecurity and Infrastructure Security Agency Research, 2023. [Online]. Available: https://www.paloaltonetworks.com/blog/2023/01/nascio-top-10-for-2023/

[2] Hassen Ben Rebah, Hatem Ben Sta, "Cloud Computing: Potential Risks and Security Approaches," ResearchGate, 2018. [Online]. Available: https://www.researchgate.net/publication/320307817_Cloud_Computing_Potential_Risks_and_Security_Approaches

[3] Ashleigh Lee, "Addressing Multi-Cloud Security and Compliance for Federal Agencies: The Orca Approach," Federal Cloud Security Research Initiative, 2025. [Online]. Available: https://orca.security/resources/blog/multi-cloud-security-federal-agencies/

[4] Vincent C. Hu et al, "General Access Control Guidance for Cloud Systems," NIST Cybersecurity Framework, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-210.pdf

[5] The Redscan Team, "The Cloud Controls Matrix – what you need to know," Cybersecurity Standards Research Initiative, 2022. [Online]. Available: https://www.redscan.com/news/the-cloud-controls-matrix-what-you-need-to-know/

[6] Fang Liu et al., "Recommendations of the National Institute of Standards and Technology," NIST Technical Publications, 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf

[7] Payal Wadhwa, "Understanding FedRAMP Controls: An Up-to-date Guide (2025)," Government Cloud Security Framework, 2025. [Online]. Available: https://sprinto.com/blog/fedramp-controls/

[8] U.S. Government Accountability Office, "Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked," GAO Report GAO-19-58, 2019. [Online]. Available: https://www.gao.gov/products/gao-19-58

[9] Splunk, "A Brief Guide to Secure Multicloud for Public Sector Agencies." [Online]. Available: https://www.fbcinc.com/source/virtualhall_images/2024_Virtual_Events/USDA_Cyber/Splunk/a-brief-guide-to-securing-your-multi-cloud_(1).pdf

[10] Federal Chief Information Officers Council, "Federal Cloud Computing Strategy," Federal CIO Council Publications, 2021. [Online]. Available: https://cloud.cio.gov/strategy/