SAIC®

SECURE MULTI-CLOUD IMPLEMENTATION: **PROVEN STRATEGIES FOR MISSION IMPACT**

Now more than ever, federal agencies are navigating immense pressures to be efficient in their mission delivery. At the same time, they must meet evolving security requirements and modernization needs. In this equation, cloud technology is a prerequisite and foundation for agility, scalability and resilience across government missions.

Each cloud service provider (CSP) operates differently, using its own methods, tools and services. What works in one often does not work in another. This makes it difficult for agencies to manage risk and respond to events consistently, since every CSP monitors and reports issues in its own way. Agencies need the ability to bring all this data together into a single view to gain clear oversight and effective governance.

Managing multiple providers also requires broad expertise. IT teams may find they need more staff with different skills to cover the unique demands of each CSP.

A secure multi-cloud approach helps address these challenges. It creates a unified way to manage different providers and a proven path to ensuring that cloud adoption delivers sustainable value. When approached with rigor, it strengthens the security posture, optimizes costs and enhances operational resilience. It also unlocks ongoing access to best services from each provider and, most importantly, empowers agencies to achieve their mission outcomes even in an era of constrained resources.

THIS INSIGHTS GUIDE SHARES SIX PRINCIPLES FOR SUCCESS IN SECURE MULTI-CLOUD SOLUTIONS. IT ALSO REVIEWS:

- How secure multi-cloud delivers mission impact
- Three stages of maturity in the multi-cloud journey
- What to consider when evaluating procurement models
- Real-world successes

Six Principles for Success with Secure Multi-Cloud

Based on SAIC's experience in implementing and operating secure multi-cloud solutions, we have identified six principles for success:

1. **Start with outcomes, not mandates.** Focus on mission impact and operational benefits rather than compliance-driven adoption. Prioritize mission and operational continuity, stronger security, faster modernization and long-term cost and efficiency optimization.

2. **Invest in organizational change.** The most critical factor in multi-cloud success is organizational change, not technology. Cloud adoption fundamentally alters how agencies operate, requiring a cloud-first mindset across all processes and practices. This transformation must include establishing cross-functional governance boards that align acquisition, security and operations teams, along with clear ownership of requirements across the organization. Successful agencies treat frameworks like NIST standards as flexible guidelines rather than rigid requirements, adapting and combining them to create governance structures that map directly to mission objectives.

3. **Partner with proven providers.** Multi-cloud success requires experience, relationships and proven methodologies that only come from successful large-scale implementations. Agencies need comprehensive training in cloud economics, security frameworks and operational practices, plus scenario-based preparedness for incident response and disaster recovery.

   Partnering with providers that have proven multi-cloud experience at scale is essential. These partners bring established relationships with cloud providers and third-party vendors, plus the organizational structures (like Cloud Centers of Excellence) that maintain consistency and best practices across cloud initiatives.

4. **Think holistically.** Multi-cloud is not multiple single clouds. Rather, it's a unified approach to cloud computing that requires integrated management and governance. Success requires treating multiple clouds as one environment, with visibility across all platforms.

   Key capabilities include automated compliance monitoring, configuration drift detection, consolidated financial management and FinOps practices that provide clear visibility into multi-cloud spending and optimization opportunities.

5. **Plan for the long term.** Multi-cloud benefits are realized over time through operational maturity and optimization, not immediate deployment. Agencies should approach adoption as an ongoing journey, building toward resilience and efficiency.

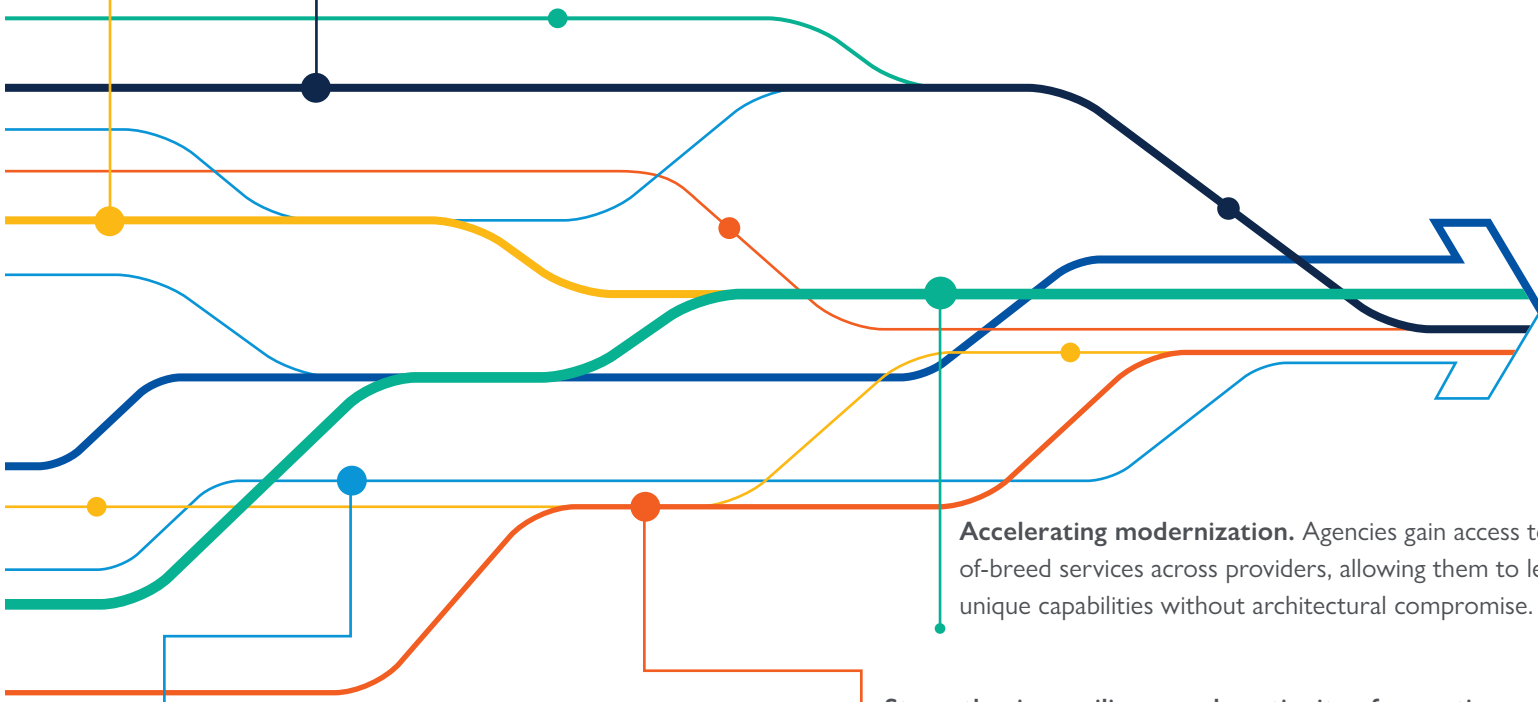
6. **Rationalize the IT portfolio.** Over time, many IT environments accumulate technical debt from past changes, add-ons and customizations. A secure multi-cloud approach works best when that debt is reduced. By auditing the IT portfolio, agencies can remove duplication, simplify complexity and shed legacy baggage. Application and service rationalization, guided by an experienced partner, accelerates modernization and improves availability, performance and governance.

Moving from Mandates to Mission Impact

Whether driven by mandate or best practices, leading agencies recognize that secure multi-cloud provides strategic benefits and outcomes that directly advance core missions. Advantages include:

Avoiding vendor lock-in and futureproofing against change. Secure multi-cloud solutions guard against technological obsolescence and give agencies negotiating leverage with cloud service providers. More importantly, this approach ensures mission continuity regardless of shifts in vendor relationships.

Enhancing security and visibility. When properly implemented, multi-cloud supports consistent Zero Trust enforcement across all environments with unified telemetry and threat detection. This strengthens the overall security posture compared to fragmented single-cloud deployments.



Accelerating modernization. Agencies gain access to best-of-breed services across providers, allowing them to leverage unique capabilities without architectural compromise.

Optimizing costs and efficiency. Beyond initial procurement savings, mature multi-cloud implementations enable FinOps practices and right-place/right-price workload placement, driving long-term operational efficiency.

Strengthening resilience and continuity of operations. Cross-cloud failover capabilities and diversified infrastructure dependencies enhance mission resilience and meet business continuity requirements.

Mapping Multi-Cloud Journeys

Understanding where an agency sits on the cloud maturity spectrum is crucial for determining the right approach and setting realistic expectations. Each stage presents distinct challenges and opportunities.

EARLY STAGE: BUILDING THE FOUNDATION	INTERMEDIATE STAGE: SCALING AND OPTIMIZING	MATURE STAGE: MAXIMIZING STRATEGIC VALUE
CHARACTERISTICS	**CHARACTERISTICS**	**CHARACTERISTICS**
• Limited or no cloud adoption beyond basic experimentation • Traditional organizational structures and change-management processes • Lack of cloud-native governance frameworks • Lack of expertise in basic cloud principles	• Some applications and workloads successfully migrated to cloud • Basic automation and DevSecOps practices emerging • Champions within the organization who understand cloud benefits • Ready to tackle more complex applications and requirements	• Excellent visibility across security, operational and cost perspectives • Capable of informed workload placement decisions across clouds • Unified management and optimization tools • Cloud-native organizational culture and processes
KEY CHALLENGES	**KEY CHALLENGES**	**STRATEGIC ADVANTAGES**
• Lack of organizational structure to handle cloud operations effectively • Cultural resistance to new approaches to application development, change management and IT operations • Limited technical expertise and cloud-native thinking • Absence of governance frameworks for cloud security, cost management and operational oversight	• Complex migration workloads that move beyond initial "low-hanging fruit" to business-critical applications • The need for consistent DevSecOps practices across all deployments • Transitioning from manual processes to automated cost management • Overcoming resistance from program offices that view multi-cloud as "adding complexity"	• Exceptional security posture with proactive and reactive capabilities • Lowest time-to-discovery for security incidents and operational issues • Comprehensive operational dashboards with historical performance analytics • Strategic cloud provider relationships for optimal pricing and capabilities • Dynamic workload optimization based on mission priorities and threat conditions
WHERE TO FOCUS	**WHERE TO FOCUS**	**WHERE TO FOCUS**
• Comprehensive training beyond technical skills • Leadership buy-in and organizational change management • Framework establishment (governance, security, operational) • Partnership with experienced providers for guidance and handholding	• Advanced DevSecOps implementation and security automation • Unified logging, monitoring and threat detection across providers • Cross-cloud key management and data protection standardization • Software supply chain security (SBOMs, provenance, SLSA frameworks)	• Cloud-to-edge integration for distributed mission requirements • AI/ML-driven orchestration for enhanced mission agility • Cross-cloud failover and disaster recovery capabilities • Innovation partnerships with cloud providers for emerging technologies

At any stage of the multi-cloud journey, agencies will face foundational decisions about how to evaluate and procure cloud services. The choice comes down to direct procurement, a managed services partner or a hybrid mix.

Procurement Options: Direct, Managed and Hybrid

When buying cloud services, agencies can work directly with providers, use a managed services partner to handle much of the work or choose a hybrid approach that mixes both. Each option has trade-offs depending on how much control the agency wants to keep and how much support it needs, as shown below:

CAPABILITY	DIRECT PROCUREMENT	MANAGED SERVICES	HYBRID
Security operations with consistent compliance mapping and service level agreement (SLA) accountability	X	✓	**Shared** – agency keeps some control, partner covers the rest
Integration with existing enterprise services, such as Identity, Credential and Access Management (ICAM) and network architecture	X	✓	**Shared** – partner helps, but agency manages some pieces
Single contract coverage for any service any bureau needs with guaranteed delivery	X	✓	**Partial** – some services bundled, others bought directly
Risk mitigation with skill shortages and specialized role requirements covered by experienced partners	X	✓	**Shared** – agency staff handle some, partner provides extra expertise

Cost and Efficiency Considerations

- **Direct Procurement:** Agencies keep full control, but costs can be higher and managing multiple providers is complex.
- **Managed:** A partner reduces the complexity, negotiates better pricing and gives predictable costs.
- **Hybrid:** Agencies directly manage some services while leaning on a partner for tough or resource-heavy areas. This balances control with support.

How SAIC Can Help

SAIC has helped design, deploy and operate some of the most secure and effective multi-cloud environments across both federal, civilian and defense missions. These multi-cloud successes demonstrate the importance of discipline, partnership and a clear focus on mission outcomes. By working alongside agencies, SAIC applies proven experience to help strengthen security, improve resilience, unlock innovation and experience the full value of cloud—achieving results that matter, together.

SAIC's Track Record: Real-World Successes

SAIC has a proven track record across multiple successful cloud programs:

GOVERNMENT'S FINANCE AGENCY: A MULTI-CLOUD SUCCESS STORY

- A shared services model transforming the agency's entire IT infrastructure
- Integrated ORCA Cloud Security Platform to centralize data for faster remediation
- Enterprise-wide adoption improving security posture across the agency's bureaus
- Built-in fraud, waste and abuse controls and FinOps governance protecting taxpayer dollars
- Communities of practice advancing cloud skills across the agency

AIR FORCE CLOUD ONE: CLOUD INNOVATION AT SCALE

- Multi-bilion-dollar program supporting 150+ applications and systems in production
- Significant cost savings by moving to serverless frameworks
- Doubled cloud adoption in one year
- 40% average ATO inheritance accelerating deployment timelines
- Certified at high-security impact levels 2, 4, 5 and 6 across leading commercial cloud providers

VIRGINIA VITA: STATE-LEVEL EXCELLENCE

- Cloud provisioning reduced from months to minutes through automation
- Centralized service management across 68 state agencies
- Supporting 70,000+ end users and 500 IT services from nine major service suppliers
- Recognized with NASCIO's State IT Recognition Award for Enterprise IT Management Initiatives

INDUSTRY RECOGNITION

- Named a Leader in the IDC MarketScape: U.S Federal Government Cloud Professional Services 2024 Vendor Assessment

Secure Multi-Cloud as a Strategic Enabler

Secure multi-cloud implementation is both a major opportunity and a complex challenge for federal agencies. Achieving success demands organizational transformation, strategic thinking and partnership with providers who have proven their capabilities at mission scale.

The agencies that will thrive are those that view multi-cloud not as a compliance requirement but as a strategic enabler for mission success. With the right approach, secure multi-cloud becomes a foundation for accomplishing more with fewer resources while maintaining the highest standards of security and operational excellence.

By following proven methodologies and learning from successful implementations, agencies will find that secure multi-cloud delivers on its promise of stronger security, cost optimization and mission agility.

Achieving success demands organizational transformation, strategic thinking and partnership with providers who have proven their capabilities at mission scale.

SAIC®

To learn more, visit: saic.com/secure-multi-cloud

saic.com