

Enterprises embarking on cloud modernization journeys increasingly adopt multi-cloud architectures, leveraging strengths across cloud providers. Among the most popular combinations is AWS and Microsoft Azure — a powerful duo offering broad global coverage, diverse service portfolios, and advanced tools for scalability. However, running workloads on both AWS and Azure simultaneously introduces complexity, especially around governance.

This article explores the governance framework necessary to effectively manage AWS + Azure multi-cloud setups. We'll cover the fundamental controls, policy guardrails, cost management strategies, and compliance imperatives enterprises must adopt for sustainable multi-cloud success.



Why Multi-Cloud? The Enterprise Perspective

Enterprises work with firms like **Future Processing**, **Accenture**, and **Deloitte** to design cloud modernization strategies that often incorporate multi-cloud:

- **Avoid vendor lock-in:** Using AWS and Azure together reduces dependency risks on one cloud provider.
- **Leverage best-of-breed services:** AWS excels in certain machine learning offerings, while Azure integrates seamlessly with Microsoft-centric enterprise tools.
- **Enhance resiliency:** Distributing workloads cross-cloud can reduce downtime risks from provider outages.
- **Meet regulatory or regional mandates:** Some industries impose cloud location restrictions or certifications better satisfied through multi-cloud.

However, this multi-cloud approach requires robust governance to maintain control, security, and cost efficiency.

AWS Azure Governance: Foundational Multi-Cloud Controls

Think about it: governance in a multi-cloud environment revolves around establishing consistent policies and guardrails that apply across aws and azure, while respecting their platform differences.

Identity and Access Management (IAM)

- **Unified Access Model:** Centralize access management by integrating AWS IAM and Azure Active Directory (AAD) with your enterprise identity provider (e.g., Azure AD, Okta).
- **Role-Based Access Control (RBAC):** Define roles consistently—developers, operators, auditors—to limit permissions per least privilege principle across both clouds.
- **Cross-Account and Cross-Subscription Policies:** Manage multi-account AWS setups and Azure subscriptions coherently to control user permissions at scale.

Policy Enforcement and Guardrails

- **AWS Service Control Policies (SCPs):** Use AWS Organizations SCPs to restrict services and actions across accounts.
- **Azure Policy:** Implement policy definitions and initiatives that enforce compliant cloud resource configurations in Azure.
- **Multi-Cloud Policy Layer:** Consider tools from cloud governance specialists to create a unified, cross-cloud policy framework so policies aren't duplicated or conflicting.

Resource Tagging and Inventory

- Adopt a consistent tagging strategy across both AWS and Azure to track ownership, environment, cost center, compliance status, and lifecycle stage.
- Use AWS Resource Groups and Azure Resource Graph to maintain an up-to-date inventory.

Security and Compliance Controls

- Centralize security monitoring with tools like AWS Security Hub and Azure Security Center, or use third-party SIEMs aggregating logs from both providers.
- Define security baselines incorporating network segmentation, encryption mandates, and vulnerability management aligned to industry standards.
- Ensure compliance with regulated industry mandates (e.g., HIPAA, PCI DSS, GDPR) by leveraging compliant controls native to AWS and Azure and validating them across clouds.

Enterprise Cloud Modernization and Regulated Industry Compliance

Partnering with consultancies such as **Deloitte** and **Accenture** helps enterprises navigate cloud modernization for regulated sectors—finance, healthcare, government—where governance isn't optional.

- **Built-in Compliance Frameworks:** AWS and Azure offer compliance blueprints and automated policy enforcement templates for regulated workloads.
- **Continuous Compliance Monitoring:** Leverage tools that automatically scan environments for drift from governance baselines.
- **Audit Trails and Reporting:** Maintain immutable logs across clouds for forensic and audit purposes, integrating with SIEM platforms.

Always require a written Statement of Work (SOW) from consulting partners, clearly specifying measurable compliance milestones—this eliminates vague promises around “cloud security” or “compliance achieved.”

Cloud Cost Controls and FinOps in Multi-Cloud

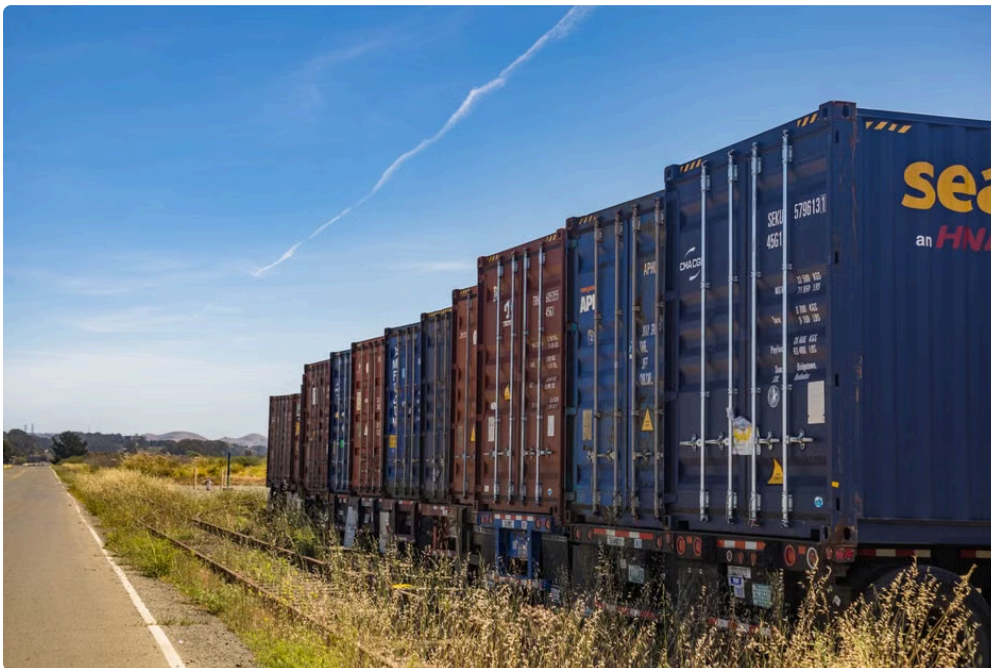
Running AWS and Azure side-by-side incurs overlapping costs. Without [devops consulting](#) governance, cloud bills escalate quickly.

- **Unified Cost Visibility:** Aggregate billing data from both AWS Cost Explorer and Azure Cost Management + Billing to create a single source of truth.
- **Cost Allocation by Tagging:** Enforce tagging policies that enable chargebacks and budgeting per business unit or project.
- **Automated Rightsizing:** Continuously monitor resource utilization to downscale underused instances.
- **Purchase Planning:** Use reserved instances or savings plans strategically in both clouds to optimize spend over time.
- **FinOps Practices:** Establish cross-functional teams with finance and engineering partners to govern cloud budgets through data-driven decision-making.

Remember, vendors tout “cost savings with cloud” often without baseline spend context. Demand transparency on timelines, tooling costs, and expected ROI for your multi-cloud FinOps initiatives.

Tools and Vendor Landscape: What Else to Consider?

While AWS and Azure provide many native governance capabilities, enterprise multi-cloud environments benefit from supplemental tools:



Domain Native Tools Third-Party Options Policy Enforcement AWS Organizations (SCPs), Azure Policy CloudHealth, Turbot, HashiCorp Sentinel Security Monitoring AWS Security Hub, Azure Security Center Palo Alto Prisma Cloud, Trend Micro Cloud One Cost Management AWS Cost Explorer, Azure Cost Management Cloudability, Apptio, CloudCheckr Compliance Automation AWS Config, Azure Policy Compliance Qualys, Dome9, Evident.io

Work with partners like **Future Processing** or Accenture who have validated expertise and partner badges for these vendors to help with tool selection and implementation.

Summary: Key Governance Takeaways for AWS + Azure Multi-Cloud

1. **Establish unified identity and access controls:** Integrate AWS IAM and Azure Active Directory for consistent RBAC.
2. **Define cross-cloud policies and guardrails:** Use native tools complemented by multi-cloud policy engines.
3. **Enforce tagging and resource inventory:** Key for visibility, compliance, and cost allocation.
4. **Embed security and compliance automation:** Critical in regulated industries to maintain continuous audit readiness.
5. **Implement FinOps governance:** Drive cost transparency and accountability across both clouds.
6. **Use vetted tools and partners:** Engage trusted consultancies and validated multi-cloud tools for sustainable governance.
7. **Document measurable outcomes:** Always insist on clear SOWs with deliverables aligned to enterprise goals.

Multi-cloud with AWS and Azure unlocks tremendous potential but demands a high discipline of governance. With clear policy frameworks, cost controls, and security practices in place—and leveraging expert partners—organizations can confidently embrace the best of both clouds for their modernization journey.