CLOUD GOVERNANCE BEST PRACTICES

Junking a legacy model to adopt the cloud? Certainly makes sense, considering the benefits of a cloud-native framework.

With unmatched operational excellence, though, comes a fresh set of challenges, such as:

- Security vulnerability
- Platform compatibility
- Complicated policy compliance
- Many more!

Let's take a look at how governance policies—tailored specifically to the cloud—are critical for enabling business and mitigating these new challenges.

What's cloud governance?

When working on the cloud at scale, organizations must consider strong cloud governance policies. Any good governance policy can help you to both:

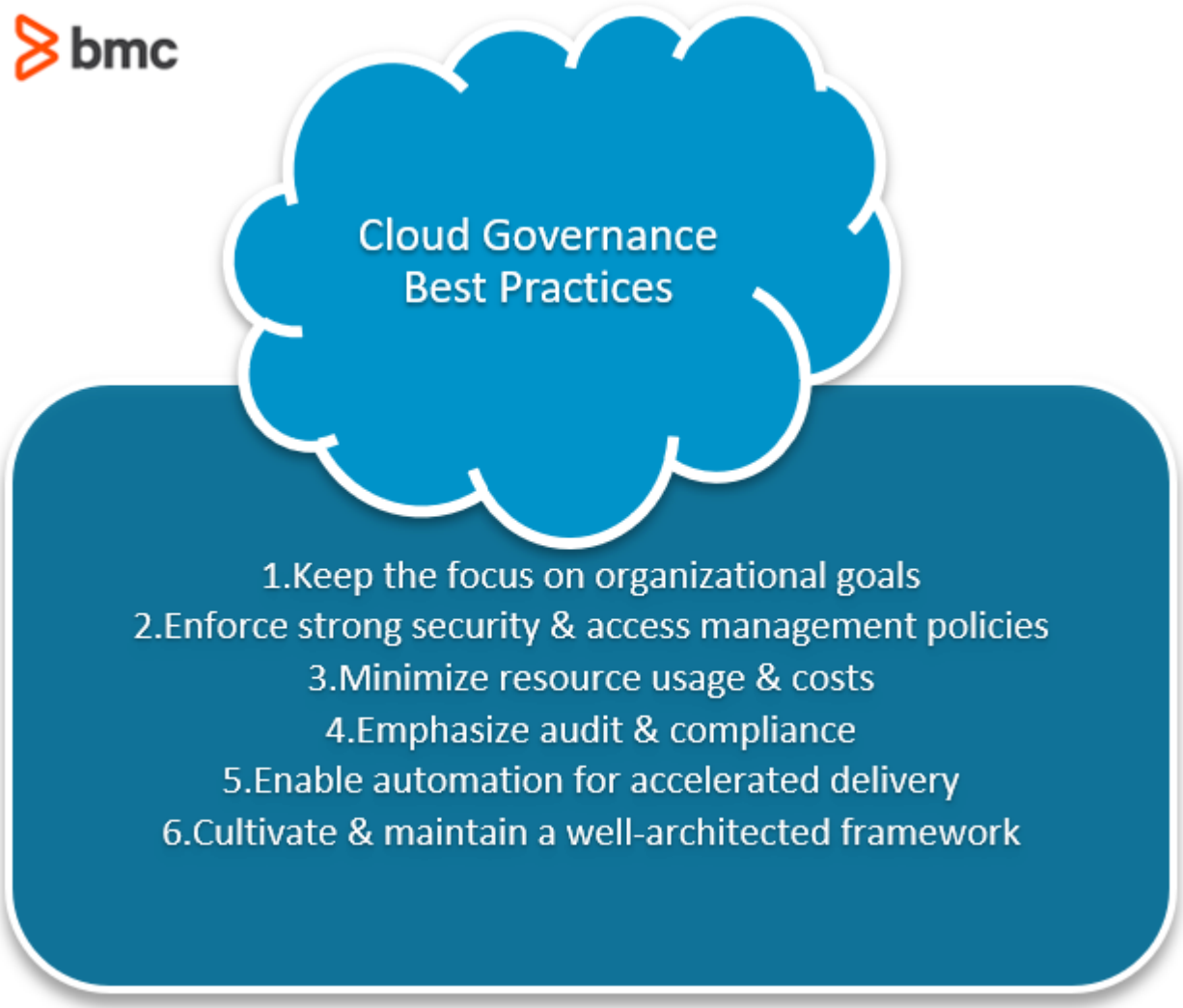
- Prevent known challenges
- Remain prepared for unknowns

Governance polices are essential enables for any business. They maintain your organization's standards for an efficient cloud framework. Broadly, governance practices can be categorized into:

- Operations
- Finance
- Risk & compliance

Unfortunately, it's not as simple as taking your existing governance policies and applying it to the cloud. You might need to adjust existing policies or create new ones altogether.

(Explore the critical IT policies every organization needs.)



Cloud governance best practices

No matter your size or industry, organizations should harness these six governance practices to make the most of their cloud framework.

Keep the focus on organizational goals

It doesn't matter whether you're adopting public, private, or hybrid cloud. Any cloud governance model must put the business first.

That is, your organization must align the cloud infrastructure and its usage with long-term financial and strategic busines goals. In real talk, this means designing every process and methodology within the cloud framework, and those supporting it, with the goal of reaching desired business outcomes.

(Read more about IT-business alignment and how to achieve it.)

Clearly define your cloud governance policy. Ensure that all terms, challenges, and benefits are well understood throughout the organization. (This is particularly important for organizations that are transitioning to a cloud environment, where unknowns and challenges are high).

As a best practice**,** the first step in any cloud migration is to draft and convey the business objectives across the organization. Failure to do so often results in disillusion, where the IT operations team operates and maintains an obscure cloud framework whose business objectives are either vague or completely unknown.

Enforce strong security & access management policies

Disregarding security is possibly the worst mistake you can make.

This is particularly alarming when you consider cloud environments that encompass a large number of connected devices and tool integrations—as most do. This increases the surface area that is susceptible to attack vectors.

Averting security incidents is an essential governance policy that helps organizations maintain an efficient and secured cloud ecosystem. While doing so, organizations may adopt a number of practices, such as:

- A DevSecOps model that blends security into all phases of development and operations.
- A security-as-code model that codifies security policies for automated delivery.
- A shift left testing approach that detects and prevents vulnerable defects during early stages of the software development lifecycle (SDLC).
- Identity and Access Management (IAM) tools for authentication and authorization control.

A diligent approach for hardened security is to consolidate governance policies around it. With centralized management of cloud security policies, organizations achieve an efficient model that can:

- Proactively mitigates risks
- Gain critical oversight of vulnerable flaws and failures

Minimize resource usage & costs

For every business, cost optimization is central to increasing its bottom line. With a strong governance mechanism, IT teams reduce costs in two key ways:

- Identifying and eliminating idle resources
- Optimizing the size of computing services

This also requires a policy framework that adopts practices such as:

- Discarding underutilized or unattached resources.
- Leveraging heatmap tools, such as AWS CloudWatch, to project resource demand.
- Designing applications that spin up resources only when required.
- Planning out the usage of spot/reserved instances for greater cost benefit.

To make this cost-efficient approach sustainable, consistently blend and evolve these resource utilization practices across other practices. This ensures that you're optimizing cost—with limited to

no impact on operational efficiency.

Emphasize audit & compliance

Customer data safety and protection is becoming mainstream, for both regulatory purposes and company standards.

Cloud governance should outline tools, processes, and personnel responsible for enforcing compliance within an existing workflow. Managed service providers (MSPs) are equally compliant with a proven demonstration of compliance, scope, and responsibilities of regulatory requirements.

Additional actions organizations can take to embed compliance:

- Make use of a policy-as-code model that automates policy execution within a delivery pipeline.
- Include procedures for conducting frequent audits to ensure you continue complying with standards and business objectives.

(Learn more about data ethics for companies.)

Enable automation for accelerated delivery

In any efficient cloud framework, automation is one element that acts both as an enabler and an outcomes. Effective automation governance should enforce the adoption of tools, processes, and methodologies that aid automation—without impacting efficiency.

Such practices may include:

- Adopting a DevOps model to automate delivery and integration.
- Leveraging tools for automated monitoring and alerts.
- Implementing persistent storage, databases, web servers, and virtual networks for faster application delivery.
- Enabling a container-based orchestration

A rule of thumb to automation: identify recurring processes that require manual effort. By modeling workflows to work autonomously, your organization can:

- Increase cost benefit
- Prevent human errors, which cause greater unknowns within an existing pipeline

Cultivate & maintain a well-architected framework

Your organization's processes and procedures certainly influence the efficiency of your cloud setup. They also equally impact the underlying architecture.

As an essential best practice, organizations should adopt and follow well-architected principles that ensure cloud-based applications are agile and resilient. The fundamental practices of any well-architected framework's fundamental practices are categorized as:

- **Operational excellence**. To make workloads run effectively with operational excellence, perform all operations as code, develop apps incrementally with small changes, and refine processes frequently.

- **Security.** Implement strong identity and access control in order to secure applications.
- **Reliability.** Reliable applications should recover automatically, have distributed workloads, and utilize only the resources required for production workloads.
- **Performance efficiency.** Use serverless platforms that bring operational efficiency. Deploy workloads across multiple regions to reduce latency.
- **Cost optimization.** Leverage cloud financial tools to help monitor resource usage and cloud expenditure. Additionally, your organization should focus on core development, delegating non-core services to third-party vendors.

Cloud governance for your organization

Your approach to cloud governance may vary by domain and organization. Still, these best practices are foundational for any successful cloud computing framework.

For organizations preparing for the cloud, perform a thorough assessment of business macros, available resources, and existing personnel skills—key factors that influence a seamless and successful migration.

Related reading

- BMC Multi-Cloud Blog
- IT Governance vs IT Management: Mastering the Differences
- Data Management vs Data Governance: Main differences
- SaaS vs PaaS vs IaaS: What's The Difference & How To Choose
- IT Security Policy: Key Components & Best Practices for Every Business
- 5 Great IT Governance Books