

CLOUD GOVERNANCE VS CLOUD MANAGEMENT: WHAT'S THE DIFFERENCE?



It is undeniable that the cloud has changed business, and life, as we know it. From collaborating on a document with team members across the globe, to ensuring applications are always up-to-date, the cloud has allowed organizations to instantly share and deploy whenever needed.

This instant access doesn't come without its risks, however, and it's crucial that these be avoided at all costs. For both security and efficiency purposes, it is crucial that businesses have both cloud governance and cloud management—but what is the difference between the two? And how can organizations ensure they are correctly utilizing them?

(Understand [*IT governance & management basics*](#).)



What is cloud governance?

A first step in establishing a [successful multi-cloud strategy](#) is simply making clear the difference between governance and management. Organizations need to define how to control, operate, optimize, and secure their [cloud infrastructures](#) and the applications running in multiple clouds.

As with anything, and especially concerning the cloud, there must be protocols in place that minimize any risks. Cloud governance is a set of rules that ensures an organization's cloud capabilities to support and enable its business strategies.

Governance is essentially the activity of defining, continuously monitoring, and auditing the rules, guidelines, policies, and processes that allocate, coordinate, and control a given operation's resources and actions. Some governance rules could include:

- Roles and responsibilities definitions
- Compliance with industry regulations
- Disaster recovery policies
- Alert escalation procedures
- Enforcement of network policies

(Explore these [cloud governance best practices](#).)

Why is cloud governance important?

As an organization's cloud environments become more complex, this list of rules only continues to grow. For companies with hybrid clouds or highly sensitive data that is being sent across the cloud, governance only becomes more critical—especially if you're operating in the increasing number of countries that have stringent data privacy and data migration policies.

At the end of the day, however, cloud governance is not intended to execute the rules—it's simply a system that structures all of them.

What is cloud management?

All of these rules and regulations are a great idea in theory, but they are useless unless there is an efficient way to put them into practice.

Cloud management, then, is the process of maintaining administrative control and oversight of all aspects of cloud computing. This includes all cloud services and products, whether they are deployed in [private, public, or hybrid cloud environments](#).

This complementary activity of organizing, coordinating, and steering resources in full compliance with the defined governance ensures the strategic and operational objectives of the business are met while all assets operate under the established rules.

Cloud management is supplied through [cloud management tools](#), which provide businesses the ability to manage resources across the multi-cloud and multi-vendor landscape. Some common responsibilities that might be included in cloud management are:

- Organizing and steering corporate resources
- Ensuring compliance is being followed
- Maintaining data security

Why is cloud management important?

As organizations migrate more to the [infrastructure-as-a-service \(IaaS\) business model](#), they find that the increasingly larger amount of applications that are being deployed into the cloud requires more structure in order to monitor all of them.

With cloud management tools, IT departments can be confident that their cloud-based applications meet applicable compliance and are being watched for all security concerns. This visibility and control over the ecosystem of applications allow enterprises full transparency into their cloud infrastructure, optimizing applications, managing compliance, and reducing risks.

Benefits of proper cloud governance & management

- **Automation:** Working established processes and workflows can be automated, significantly raising efficiency.
- **Innovation:** The evolution of cloud offerings is driven by the provider, which in turn creates effective opportunities to evolve one's IT infrastructure at a low cost.
- **Optimization:** Having a huge integration capacity that can leverage the existing potential of alternative, more capable infrastructure that can be installed and integrated within a matter of minutes, hours, or a few days.
- **Change:** Proper processes in place over a highly dynamic and responsive IT landscape facilitate change management, quality assurance, and compliance.
- **CAPEX/OPEX:** Utilize the most appropriate IT assets for a fraction of the "traditional way" cost.
- **Profitability:** Organizations with above-average IT governance have been shown to have more than 20 percent higher profits than those with poor governance following the same strategy.

Real-world challenges addressed by cloud governance & management

Let's play governance and management out across key business functions.

Costs

A contract has been established with the [cloud services provider](#) (CSP) where costs per cloud resource are defined. These roles must be involved:

- The controller's office audits the observance of such an established cost table.
- The [Chief Information Officer](#) (CIO) establishes a continuous improvement workflow, leveraging existing frameworks and methodologies such as Kaizen, Six Sigma, and Lean to constantly analyze more cost/effective evolution paths to the existing cloud-based IT Infrastructure.

Budgets

Currently, almost every company area or department's budget has a direct or indirect share of IT costs represented. One of cloud-based services' main edges is precisely allowing dynamic allocation of assets, implying dynamic costs. Having the capacity to easily (only at a "mouse click" away) get additional resources leads to the natural "temptation" of triggering them.

- Team Leaders and Area Managers, with the steering support of the CIO, manage dedicated [existing IT resources to the best capacity](#) while promoting synergies that delay the need for IT infrastructure escalation.
- The CIO acts as an area manager towards the IT department within this topic.

(Understand the difference in [capital vs operating expenses](#).)

Operations

IT operations obey corporate guidelines, which must be adapted, configured, and monitored within a cloud IT landscape context. This ensures compliance with operational standards which fosters operational efficiency and security.

- The CIO audits and monitors the observance of existing ruling, including IT guidelines, internal adherence to the existing services contracts, and inherent SLAs with Cloud Service Providers.
- Area Managers confirm area users have proper awareness about Corporate Operations rulings through coaching sessions and training opportunities

Security

IT security has gained an all-new relevancy with cloud based services due to the higher exposure of hybrid IT landscapes.

- The [Chief Information Security Officer](#) (CISO) and CIO audit and monitor the observance of existing ruling, not only internally but also with regards to the Cloud Service Providers.
- Team Leaders and Area Managers lead by example, in this case, coaching and identifying training needs towards team members which ensures wide corporate IT security awareness.

Risks

[Risk management](#) is yet another component of corporate IT Operations that has gained an increased relevancy with the arrival of cloud based services. These range from proper IT Infrastructure [Load Balance](#) among providers, as well as geographies, to prevent service disruption to [shadow IT](#).

- The CIO defines and locally adapts, fine-tunes, audits, and monitors the observance of existing corporate policies towards risk mitigation.
- The Controller's Office audits and reports/blocks the attempted acquisition of unauthorized IT assets or resources by the areas that constitute potential shadow IT.
- Area Managers lead teams towards compliance by educating and reducing shadow IT and other practices that bear risks.

Getting started with cloud governance & management

There are three phases towards adopting and effectively running cloud governance and management:

1. **Design.** The hardest part—assessing where you are and what can be leveraged over a specified period within a cloud environment including expected savings (time and money) and gains in effectiveness. Add to it the defining and designing the inherent project, metrics, SLAs, goals, milestones, risk mitigation actions, etc.
2. **Implement.** Moving towards the cloud with proper governance and management
3. **Continuous Improvement.** Undergoing a continuous cycle of assessment towards getting things more efficient, and at the same time, more cost effective

(Learn about continual improvement.)

Forward-thinking with cloud governance and management

The cloud will continue to push forward strategies and business in innovative ways. It is up to organizations to ensure that their cloud ecosystems have the structures set in place, and the tools necessary to manage them, to ensure the infrastructure is steady for years to come.

Related reading

- [BMC Multi-Cloud Blog](#)
- [How To Accurately Estimate the Cost of Cloud Migrations](#)
- [What Are CMPs? Cloud Management Platforms Explained](#)
- [Change Management in the Cloud](#)
- [Common Roles in Cloud Computing](#)
- [The Cloud Today: Growth, Trends, Market Share & Outlook](#)