

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



While clouds have proliferated in enterprise organizations – public, private, hybrid– it has become increasingly important to define strategy around cloud governance and management. 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.

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. In short, establishing and auditing the application of existing ruling.

Management is the complementary activity of organizing, coordinating and steering the corporate resources and actions in full compliance with defined governance while ensuring the achievement of strategic and operational objectives. In short, making sure objectives are met while assets operate under established rules.

Cloud Governance and Cloud Management must be cross functional responsibilities within a company and rarely if ever the dedicated responsibilities of a single employee or specific team.

Common Challenges Addressed by Cloud Governance & Management

Challenge	Topic	Cloud Governance	Cloud Management
Costs	A contract has been established with the Cloud Services Provider where costs per cloud resource are defined.	<p>Controller's Office - Audit the observance of such established cost table.</p> <p>CIO - Establish a continuous improvement workflow, leveraging existing frameworks and methodologies such as Kaizen, Six Sigma, Lean to constantly analyze more cost/effective evolution paths to the existing cloud based IT Infrastructure</p>	Area Managers - Performing the new cloud assets requisition within the defined "price table"
Budgets	<p>Currently, almost every company area or department's budget has a direct or indirect share of IT costs represented.</p> <p>One of cloud based services main edge is precisely allowing dynamic allocation of assets, implying dynamic costs.</p> <p>Having the capacity to easily (only at a "mouse click" away) getting additional resources leads to the natural "temptation" of triggering them.</p>	<p>Controller's Office - Monitoring IT budget share expenditure evolution versus available financial resources.</p>	<p>Team Leaders and Area Managers with the steering support of the CIO - Manage their dedicated existing IT resources to their best capacity while promoting synergies that delay the need for IT infrastructure escalation.</p> <p>The CIO acts as an area manager towards the IT department within this topic.</p>
Operations	IT operations obey by corporate guidelines, which must be adapted configured and monitored within a cloud IT landscape context, assuring compliance with operational standards which foster operational efficiency and <u>security</u> .	<p>CIO - Audit and monitor the observance of existing ruling, including besides IT guidelines internal adherence the existing services contracts and inherent SLAs with Cloud Service Providers.</p> <p>One major challenge is to accurately migrate frameworks such as <u>ITIL</u> and <u>COBIT</u> inherent processes (as well as other) over a mixed environment that combines traditional with Virtualized Hybrid Cloud based <u>IT Infrastructure</u>.</p>	Area Managers - Assure that their area's users have proper awareness (by means of coaching and sending them to training actions) about Corporate Operations ruling plus steering the team to behave per those.

Security	IT Security has gained an all new relevancy with cloud based services due to the higher exposure of hybrid IT landscapes	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 – Need to lead by example, in this case, coaching and identifying training needs towards their team members which ensure wide corporate IT security awareness.
Risks	Risk Management is also yet another component of corporate IT Operation that gained an added relevancy with the arrival of Cloud based services. These range from proper IT Infrastructure Load Balance both amongst providers as well as Geographies to prevent service disruption to Shadow IT.	CIO – It is the role of the CIO to define and or locally adapt/ fine tune, audit and monitor the observance of existing corporate policies towards risk mitigation. Controller's Office – auditing and reporting/ blocking the attempted acquisition of unauthorized IT assets or resources by the areas, that constitute potential Shadow IT.	Area Managers – Need to lead their teams towards compliance with IT ruling, refraining from undergoing or allowing the team to proceed with Shadow IT or other practices that bear risks by means of steering and promoting corporate awareness towards those potential risks.

Benefits of having proper Cloud Governance and Management in place

- **Automation** – working established processes and workflows can be automated, significantly raising efficiency.
- **Innovation** – the evolution of cloud offering 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/integrated within a matter of minutes, hours or a few days.
- **Change** – proper processes in place over a highly dynamic and responsive IT landscape facilitates 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.

Getting Started with Cloud Governance and Management

There are basically three phases towards adopting and effectively running Cloud Governance and Management:

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 - plus defining and designing the inherent project, metrics, SLAs, goals, milestones, risk mitigation actions, etc.

Implement

Moving towards the cloud with proper Governance and Management

**Continuous
Improvement**

Undergoing a continuous cycle of assessment towards getting things better yet more cost effective