



**Ready, Set,
Governance:
Effective Cloud
Governance
Strategies for Your
Business**

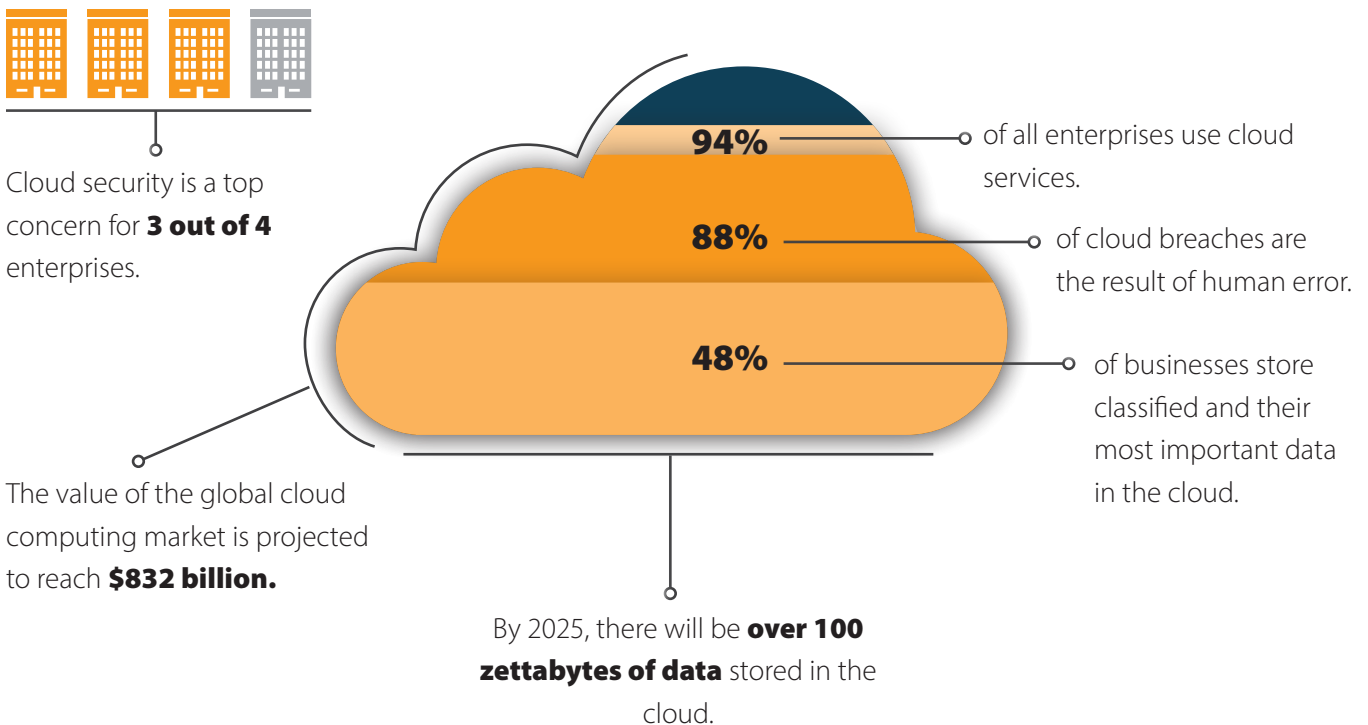
INTRODUCTION



The journey toward cloud adoption is well underway for many organizations, due to its high performance, enhanced security, and lowered IT costs. However, more often than not, organizational leaders treat cloud adoption as a one-and-done operation without implementing clear guidelines to maximize its benefits. Developing comprehensive rules for how to work with(in) the cloud obligates departments to hold themselves accountable to allotted budgets, maintain cloud security best practices, and switch the organization from a reactive to a proactive approach to cloud management, use, and security.

Cloud governance is an organization-wide strategy, not a technology. Establishing effective cloud governance requires people, leadership, and a vision just as much as it requires well-defined policies and procedures.

Cloud Statistics

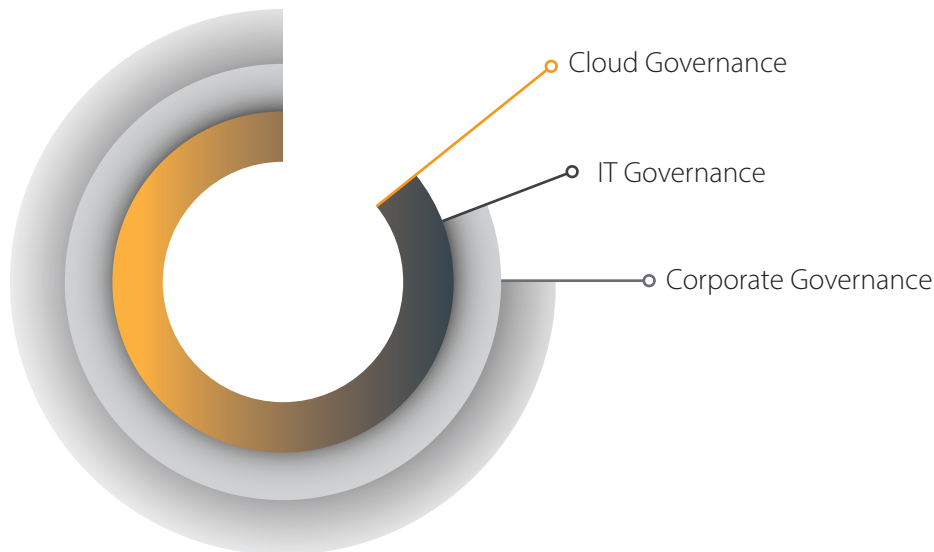


Cloudwards, 2022¹

WHAT IS CLOUD GOVERNANCE?



Cloud governance is the process of defining, implementing, and monitoring a framework of policies that guides an organization's cloud operations. This process regulates how users work in cloud environments to facilitate consistent performance of cloud services and systems.² Cloud governance is a component of IT governance, which is a component of the overall corporate governance strategy.



Cloud governance is not the same as cloud management, but they work together to accomplish a common goal, to effectively operate, control, optimize, and secure cloud infrastructure. Think of cloud governance as the track, the cloud as the train, and cloud management as the conductor. The track is laid, and the conductor is there to ensure a safe journey without the train derailing.

The cloud is vulnerable to various risks in the technological environment that need to be controlled. The governance policy facilitates risk management, achieves business objectives without compromising shareholders' needs, and enables optimal utilization of the cloud infrastructure.³

KEY BENEFITS OF CLOUD GOVERNANCE



Developing and implementing a perfect cloud solution is not something that can be achieved overnight, but the final product is worth it. The most notable immediate and long-term benefits of establishing cloud governance include:

- ◆ **Controlled access**— By designating who owns each area of asset and software management, your cloud governance plan will limit who can access and make changes to the cloud. Controlling access to critical assets is vital and will ensure greater visibility and enhance the reliability of your cloud processes.
- ◆ **Reduced security risks**— Once your organization commits to moving data to the cloud, it is imperative that security measures are developed to protect that data. Your cloud governance plan will help identify vulnerabilities in your system, enact plans to mitigate risk, and establish metrics to gauge the impact of security measures.

- ◆ **Enhanced compliance readiness**— Aligning your cloud governance program with your compliance requirements allows you to build compliance review and standards into your processes and architecture. Then, when it comes time to document your compliance, you will have a thorough archive of your system’s history, current status, and plans to enhance compliance.
- ◆ **Lowered costs**— Cloud governance shifts workflows from analog to automated. Instead of relying on time-consuming manual processes, cloud governance helps automate the management of everything from budgets to policies. This can also trigger automated responses to cloud activity, which reduces the manpower needed to enforce your cloud governance, resulting in reduced costs.⁴

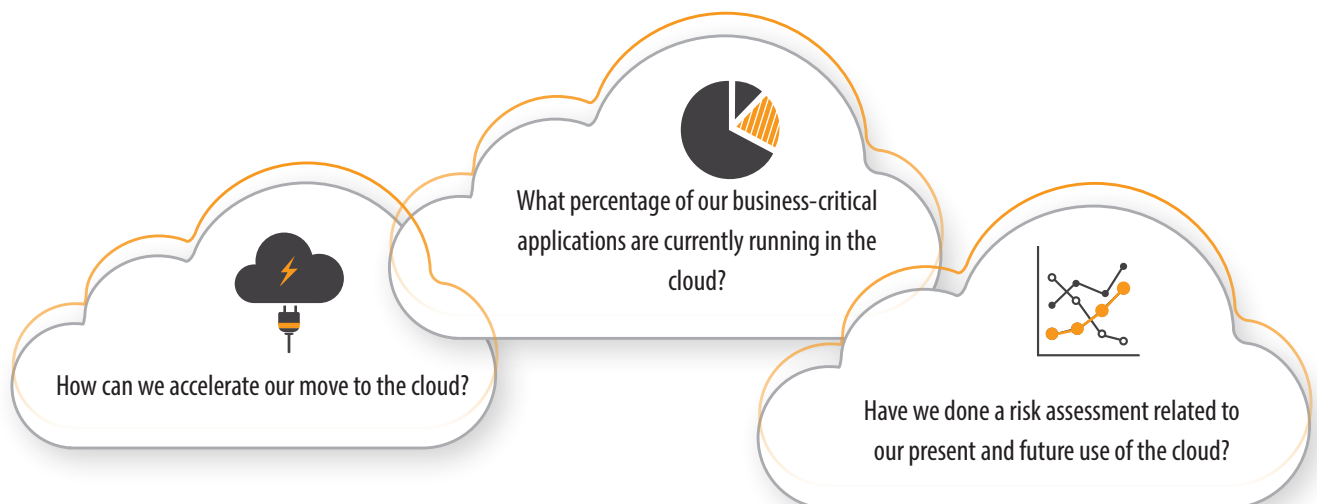
Cloud governance tools and processes not only simplify the overall cloud journey for organizations, but also help identify and mitigate security and compliance risks— all this while unlocking tangible business value from cloud-based innovation.⁵

ESTABLISHING GOVERNANCE

Getting Started

Before committing rules to paper, consider how cloud governance will impact or alter the current corporate policy. Any variation to business protocol or technology platforms can introduce risk to the organization and hamper governance adoption efforts. In short, it is important to evaluate the current policies before adding more to the pile. It is also necessary to assemble an inventory of assets already deployed in the cloud, understand their interrelations, and identify security risks.

Unsurprisingly, establishing clear direction requires extensive input from business leadership. Management teams, board members, and other key decision makers need to understand their cloud infrastructure and see that their cloud computing initiatives are not only an IT concern but an enterprise-wide strategy. The following questions are important to ask when developing a cloud governance strategy:





ISACA, 2021⁶

Cloud Governance Model Principles and Core Components

A good starting point in developing your cloud governance model is to make sure it addresses the following five principles:

- ◆ **Compliance with policies and standards**— Cloud usage standards must be consistent with regulations and compliance standards followed by your organization and others in your industry.
- ◆ **Alignment with business objectives**— The cloud strategy must be an integral part of the overall business and IT strategies. All cloud systems and policies should demonstrably support business goals.
- ◆ **Collaboration**— Owners, users of cloud infrastructure, and other stakeholders in relevant organizational units must agree on how to make appropriate and mutually beneficial use of cloud resources.
- ◆ **Change management**— Changes to the cloud environment must be implemented in a consistent and standardized manner, subject to the appropriate controls.
- ◆ **Dynamic response**— Cloud governance should rely on monitoring and automation to dynamically respond to events in the cloud environment.⁷

As with most IT strategies, cloud governance should be customized to the individual organization to function most effectively. That said, all cloud governance models should be comprised of three core components, people, processes, and technology, and should cover the entire cloud life cycle, including identifying, configuring, migrating, managing, and decommissioning cloud assets. Lastly, a comprehensive model will address six domains that span the cloud life cycle:



Security and Compliance Management

Security and compliance management refers to assessing risks, privacy, identity and access management, data encryption, application security, and contingency planning. From a governance perspective, the objectives of information security practices are shaped by a combination of business objectives and regulations.

Financial Management

Financial management policies provide a framework to make business decisions about cloud resources. Adjust cloud usage to manage spending within budgeted parameters, and establish policies for cost control, reporting, and alerts. Most cloud vendors provide cost reporting tools. If those do not meet your needs, look to third-party services to fill that gap.



Operations Management

The focus of operations management is to control how cloud resources deliver services. A clear, well-defined operations management practice is one of the best ways to prevent shadow IT operations from creeping into your cloud environment. Good cost monitoring and performance monitoring can also help identify when cloud resources are deployed outside of normal operating procedures.



Data Management

Your governance strategy and practices should include clear guidance to manage the full life cycle of data in your organization. Governance policies help data owners, product managers, and application developers understand how to protect data based on its classification. Take advantage of cloud providers' data management tools to automatically migrate data to different storage systems or delete data that is no longer useful.



Performance Management

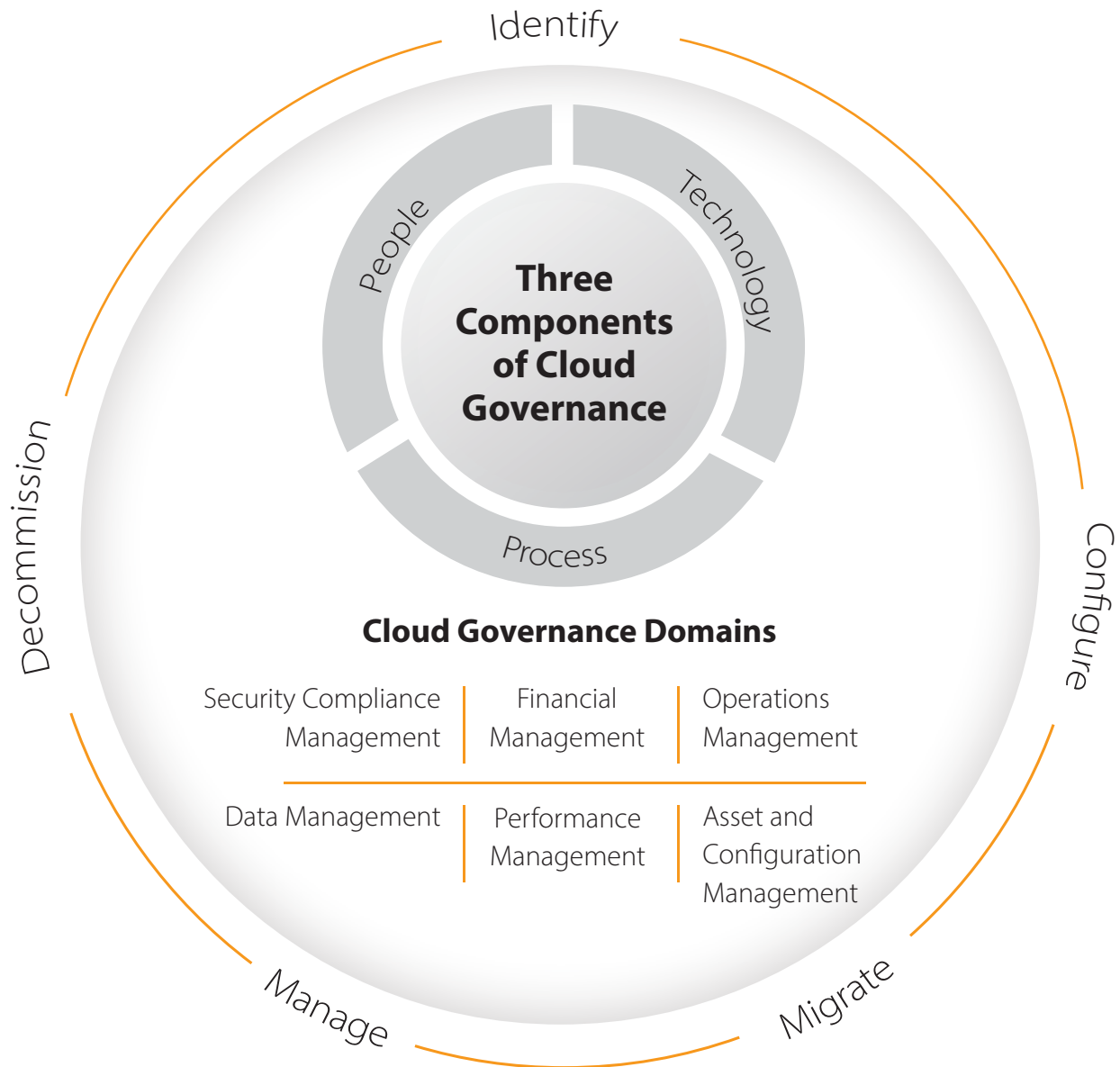
Performance management in cloud computing focuses on monitoring applications and infrastructure resources to ensure the organization delivers expected levels of IT services and efficient usage of cloud infrastructure.

Asset and Configuration Management

A big challenge for organizations is to maintain a dynamic array of cloud infrastructure resources within the bounds of what they expect to deploy. Teams should rely on controlled processes to deploy large clusters or use high-cost cloud services. Configuration management helps organizations control the use and storage of credentials and encryption keys.⁸



Cloud Life Cycle



Industry-Approved Framework

An example of an industry-approved framework organizations can use to build their cloud governance strategy is the Control Objectives for Information and Related Technologies (COBIT) framework. While not cloud-specific, COBIT is a flexible framework that provides room for innovation and customization. The COBIT framework:

- ◆ Is platform-agnostic.
- ◆ Addresses nearly all technical considerations for cloud computing.
- ◆ Provides clearly defined risk assessment measures, and a maturity scale.

The purpose of using an established control framework to develop a cloud governance strategy is that the knowledge gained from the framework's IT processes will help uncover governance priorities and requirements, inform future business cases for governance improvements, gain stakeholder support, and monitor projected cloud benefits.

CLOUD GOVERNANCE MATURITY



A cloud maturity model represents a gradual progression of an organization's use of the cloud. Remember, cloud maturity models have different criteria based on your company's industry and size. Below is an example of a cloud maturity model:

0

Stage 0: Nonexistent (Legacy)

Stage zero means that the company is exclusively relying on on-premise infrastructure. No department is using cloud-based resources, or their use is extremely minor.

1

Stage 1: Initial (Ad Hoc)

Stage one means that the company has just started using cloud services. Typically, companies begin using the cloud in individual departments or projects. Companies at this stage have no centralized strategy or governance for cloud use. While the cloud is a useful asset, there is no alignment with business objectives or any conscious effort to maximize the positive impact of the cloud.

2

Stage 2: Managed (Yet Still Opportunistic)

Businesses at stage two have started to officially organize their use of the cloud. In addition to Software as a Service (SaaS) and Infrastructure as a Service (IaaS), these companies are also using Platform as a Service (PaaS) to run and manage applications without the complexity of dealing with the underlying infrastructure.

3


Stage 3: Optimized (Defined and Systematic)

Companies at stage three have fully embraced cloud computing and are actively driving business transformation. As with the previous stage, companies rely on a mix of IaaS, PaaS, and SaaS, but also use advanced cloud features, such as auto-scaling, advanced monitoring, and in-depth analytics.

4

Stage 4: Innovative (Fully Managed)

At stage four, organizations' use of the cloud becomes a continuous cycle of optimizing cloud infrastructure. All cloud processes are highly documented, and teams make all changes based on strictly defined protocols. These companies also have in-depth governance rules and are using the cloud to stay ahead of the competition.



Cloud governance consists of leadership, organizational structure, direction, and processes that ensure IT sustains and extends the enterprise's mission, strategies, and objectives in a planned manner.¹⁰

CONCLUSION



The Bigger Picture

While some might consider governance a roadblock to “getting things done,” having the right controls and processes in place is necessary for effective optimization and management of the cloud. That’s why decision makers must take into account their organization’s unique policies, cloud assets, and overall business objectives to determine how cloud governance will support and complement the components of corporate and IT governance already in place. Ignoring the bigger picture, implementing cloud governance as an afterthought, neglecting to inform the cloud service provider of governance requirements, or not involving the IT department in the creation process will only cause more headaches in the future.

ABOUT SECURANCE



Securance has more than two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.



SOURCES



1. <https://www.cloudwards.net/cloud-computing-statistics/>
2. <https://www.redhat.com/en/topics/automation/what-is-cloud-governance>
3. <https://www.jigsawacademy.com/blogs/cloud-computing/cloud-governance>
4. <https://www.lucidchart.com/blog/cloud-governance-framework>
5. <https://pulse.microsoft.com/en/transform-en/na/fa1-why-cloud-governance-is-key-to-the-success-of-your-cloud-journey/>
6. <https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-16/key-questions-to-address-for-effective-cloud-governance>
7. <https://www.imperva.com/learn/data-security/cloud-governance/>
8. <https://www.techtarget.com/searchcloudcomputing/tip/How-to-design-and-implement-a-cloud-governance-framework>
9. <https://phoenixnap.com/blog/cloud-maturity-model>
10. <https://dzone.com/articles/cloud-governance-a-holistic-view>

Ready, Set, Governance: Effective Cloud Governance Strategies for Your Business
© 2023 Securance LLC. All Rights Reserved.



13916 Monroes Business Park, Suite 102, Tampa, FL 33635 • 877.578.0215

www.securanceconsulting.com

