indium
Make Technology Work

Demystifying Cloud Governance and Compliance: Best Practices for Managing Cloud Resources, Policies, and Access Controls

A Whitepaper

© Indium Software

The Need for Cloud Governance

Moving to the cloud has become a business imperative to remain competitive, improve customer satisfaction, lower costs, and increase revenues. But this migration is not just about shifting from the on-prem systems to a cloud infrastructure. It brings with it its own complexities and questions.

What is the objective of cloud migration? How to achieve it? How to ensure consistent performance of cloud services, maximize resource utilization and minimize security risks? All these questions increase the complexity of IT teams to manage the decentralized cloud infrastructure while ensuring scalability and flexibility.

Along with business compulsions, these are also issues associated with meeting regulatory requirements. Europe's General Data Protection Regulation (GDPR), for instance, is concerned with protecting personal data, requiring businesses to tighten their security controls to prevent breaches and leaks.

Cloud governance becomes essential in this context. Cloud governance is a framework of policies that guides the organization's cloud operations. It helps to enforce and monitor the cloud environments and ensure that they are aligned and work in a synchronized manner. It helps businesses strengthen their security posture and minimize risks.

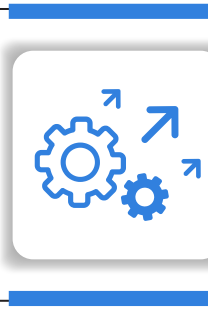
© Indium Software

Benefits of Cloud Governance

Beyond regulatory compliance, defining, implementing, and monitoring a cloud governance strategy can help businesses with the following:

Resource and Infrastructure Optimization: While the cloud reduces the overall cost of infrastructure because of the IaaS model, it can still experience some inefficiencies that need to be controlled and monitored. A good governance policy must define how the resources can be used effectively to keep costs low.

Improve Performance: Governance provides a bird's eye view of the entire cloud environment. This can help organizations optimize performance and increase operational efficiency by simplifying management and removing bottlenecks to productivity.



Reduce Security Risks: A good governance framework defines the access management strategy for the company and determines the processes to monitor security. This can help with faster identification of vulnerabilities and resolution to make the cloud infrastructure safe and compliant.

Ensure Business Continuity: The improved visibility of the cloud environment helps businesses better address challenges due to downtime or data breaches.

© Indium Software

Defining Cloud Governance for Improved Compliance

Often, businesses may use existing IT practices to build their cloud governance framework. But creating a new set of cloud-specific rules and policies can prove beneficial as it identifies the vulnerabilities and requirements specific to this environment. This would include areas such as:

Regulatory Requirements: There are several regulations and standards covering various aspects of data security and privacy. For example, in addition to GDPR, healthcare service providers in the US must also comply with HIPAA.

As credit card payments have become ubiquitous, specific elements of the Payment Card Industry-Data Security Standard (PCI-DSS) must be implemented.

Businesses will need legal and regulatory experts to guide them on these aspects to create a comprehensive governance framework. ISO 27001 or NIST SP 800-53 are used as the foundation for defining security controls.

Data Management: Data is gathered from multiple sources and can be structured or unstructured.They must be processed for deduplication, accuracy, and quality, and presented in a unified manner to empower the users to draw insights and make informed decisions.

This requires the right set of data management tools and technologies to meet business needs.

Data Security: Data is an asset that needs to be protected to help businesses retain their competitive edge. While the sources may be common, how it is processed and presented, what kind of reports and analytics are generated, and how these help the business can fall under the umbrella of trade secrets.

© Indium Software

Further, businesses also work with the personal data of employees and customers, accessible in confidence. Ensuring the data is not breached is the responsibility of the organization, and any theft is direct non-compliance and a reason to lose customer trust.

Risk Management: As technology advances and businesses opt for digital transformation, the risks to businesses do not end. Knowledge is power and helps businesses assess their risks to be prepared for them. This is also a regulatory requirement.

Businesses must identify risks, rank them based on impact, and put in mitigating measures to reduce the impact or eliminate the risk.

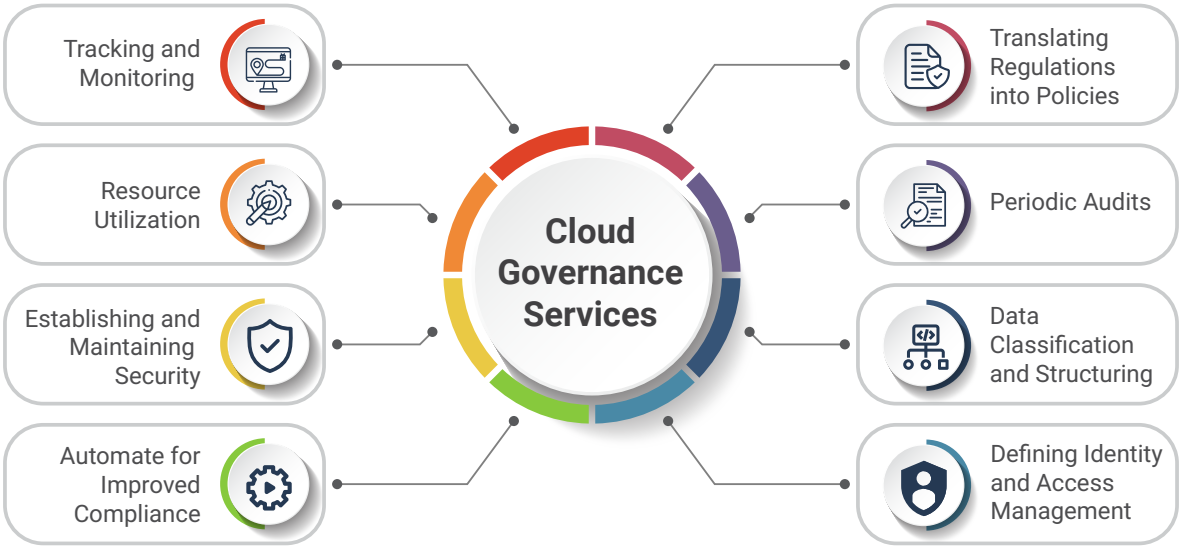
Cost Management: While the cloud environment is definitely more cost-effective than on-prem infrastructure, the costs can be brought down further with regular monitoring and tracking.

Governance policies must specify parameters and KPIs to monitor cloud performance and constantly identify ways to optimize resource utilization and lower operational costs.

Implementing Best Practices for Cloud Governance and Compliance

Indium Software is a cloud, data, and app modernization expert with several years of experience across domains. We facilitate businesses to leverage digital transformation technologies for innovation and growth. In addition to designing and implementing the cloud architecture and transforming business processes to meet the current-day needs for scalability and flexibility, we also help businesses with creating, implementing, and monitoring cloud governance and compliance.

Given below is a crystallization of our experiences in the form of best practices that can help businesses be compliant and protect their business interests better.



Best Practice #1 Translating Regulations into Policies: While a legal expert is required to interpret and create the formal policy document for an organization, giving form to the vision is essential. This includes creating the right contracts with third-party vendors, suppliers, customers, and so on.

Non-compliance can erode brand reputation and lead to penalties. Therefore, it is important for businesses to first understand the regulations and their applicability, and then create the policy.

The cloud migration must also happen after this stage to ensure the necessary controls are built in right from the start.

Best Practice #2 Periodic Audits: Regular audits must be conducted to evaluate the company's level of regulatory compliance, identify gaps, and correct them at the earliest. Audits can be done by internal resources or by external, third-party experts.

The reports must also be in a specified format and empower management with information to make quick, informed decisions.

Best Practice #3 Data Classification and Structuring: Assessing the existing data with the organization is the first step to setting guidelines for data management in the cloud.

© Indium Software

There must be clarity on where it is stored, who can access it, and the processes it has undergone. To improve data consistency and quality, organizations must define processes for classifying, cleaning, and organizing the data, and presenting a unified view of data.

Best Practice #4 Defining Identity and Access Management: Identity and access management is an important component of cloud management. Only authorized personnel must be provided access to sensitive data, that too with sufficient controls and precautions in place. This will prevent any unnecessary thefts or leaks.

Best Practice #5 Tracking and Monitoring Resource Utilization: Often unused applications may be running in the background, draining computing power and increasing costs.

There may be overprovisioned instances or storage that is not being used, raising the billing amount. For businesses in a multiple cloud environment, the complexity of tracking and monitoring these sources can be challenging.

Therefore, it is crucial to define and monitor parameters to make sure that the infrastructure has been designed properly and used only for the intended purpose. Tools such as CloudCheckr and CloudHealth, or a third-party review can evaluate and improve cost-effectiveness.

Best Practice #6 Establishing and Maintaining Security: While the cloud service providers have their security protocols, individual businesses using the infrastructure must define, establish, and maintain their own security.

It should be based on the organizational need and encompass protecting event logs, implementing security rules for accounts and regions, and reports and recommendations at the account level.

Beyond implementing, monitoring and auditing are also essential to identify new threats and upgrade security. Creating an automated, central monitoring solution can improve monitoring as it generates alerts in case a new threat is detected.

© Indium Software

Best Practice #7 Automate for Improved Compliance: The cloud infrastructure can be complex and require resources for monitoring and responding. Automation of cloud management improves resource utilization, lowers the total cost of ownership, and improves response to threats through the automatic generation of warnings. It can improve governance and efficiency by enforcing the adoption of tools, processes, and methodologies.

Cloud Governance Automation

One of the challenges cloud governance faces is the quick scaling up of needs which makes manual control limited and ineffective. Automation helps improve the efficiency of cloud governance.

Some of the key automation processes include:

- Infrastructure provisioning
- Cloud Security
- Compliance
- Network management
- Workload management
- Application development

Managing the different components individually can add to the complication, leading to higher costs, redundancies, and inconsistencies. Unifying the needs and automating on a single platform can simplify governance and make it more holistic. It can also free up IT teams to focus on monitoring and controlling cloud usage and strategy with greater effectiveness.

Automation of governance also empowers organizations with insights into cloud usage. This helps improve financial provisioning. It also helps improve visibility into the current usage of infrastructure and makes it more efficient.

Indium Software to Implement Cloud Governance and Compliance Best Practices

Indium Software has been recognized by ISG as one of the promising contenders for data engineering, which encompasses cloud engineering, application engineering, and data assurance, amongst others.

The Indium team has the experience and expertise to help our customers establish a cloud governance framework aligned with their organizational goals and objectives.

Our range of services includes providing guidance on policies, procedures, and best practices for cloud adoption, management, and usage.

Our cloud implementation strategy curates the best practices to ensure data protection, access control, and monitoring for keeping your data safe and secure.

Visit https://www.indiumsoftware.com/cloud-strategy-advisory-services/ to know more about our cloud engineering capabilities.

Indium provides end-to-end cloud solution architecture services that enable businesses to leverage the full potential of cloud technology.

We offer bespoke solutions that cater to the individual needs of the organization and ensure security and governance to ensure compliance.

Find out how Indium can help you design the right cloud solution: https://www.indiumsoftware.com/cloud-solution-architecture-services/

© Indium Software

FAQs

What kind of auditing is required to ensure compliance and governance?
Auditing must be of two kinds - internal and external. While internal auditing is by the staff and helps to catch irregularities quickly, external auditing by certified professionals can help uncover deeper issues.

What are some challenges of cloud governance?
Cloud systems not being integrated well, data duplication, lack of alignment of business goals and cloud systems, and security issues are the common challenges.

© Indium Software

USA
Cupertino | Princeton
Toll-free: +1-888-207-5969

INDIA
Chennai | Bengaluru | Mumbai | Hyderabad
Toll-free: 1800-123-1191

UK
London
Ph: +44 1420 300014

SINGAPORE
Singapore
Ph: +65 6812 7888

www.indiumsoftware.com

For Sales Inquiries
sales@indiumsoftware.com

For General Inquiries
info@indiumsoftware.com