QUALITYKIOSK TECHNOLOGIES | BOOTLABS

A GUIDE TO ACHIEVING GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE IN THE CLOUD

WHITE PAPER

Cloud challenges

Security and Robustness

Organizations often have siloed teams with individual cloud initiatives during the cloud adoption journey. But this approach is a recipe for disaster. Cloud security is a 'shared responsibility', and it requires necessary service controls to be enforced.

Speed and Control

It is difficult for organizations to find the right balance between speed and control. This is one of the major challenges of an integrated Governance, Risk, and Compliance (GRC) framework.

Prioritization

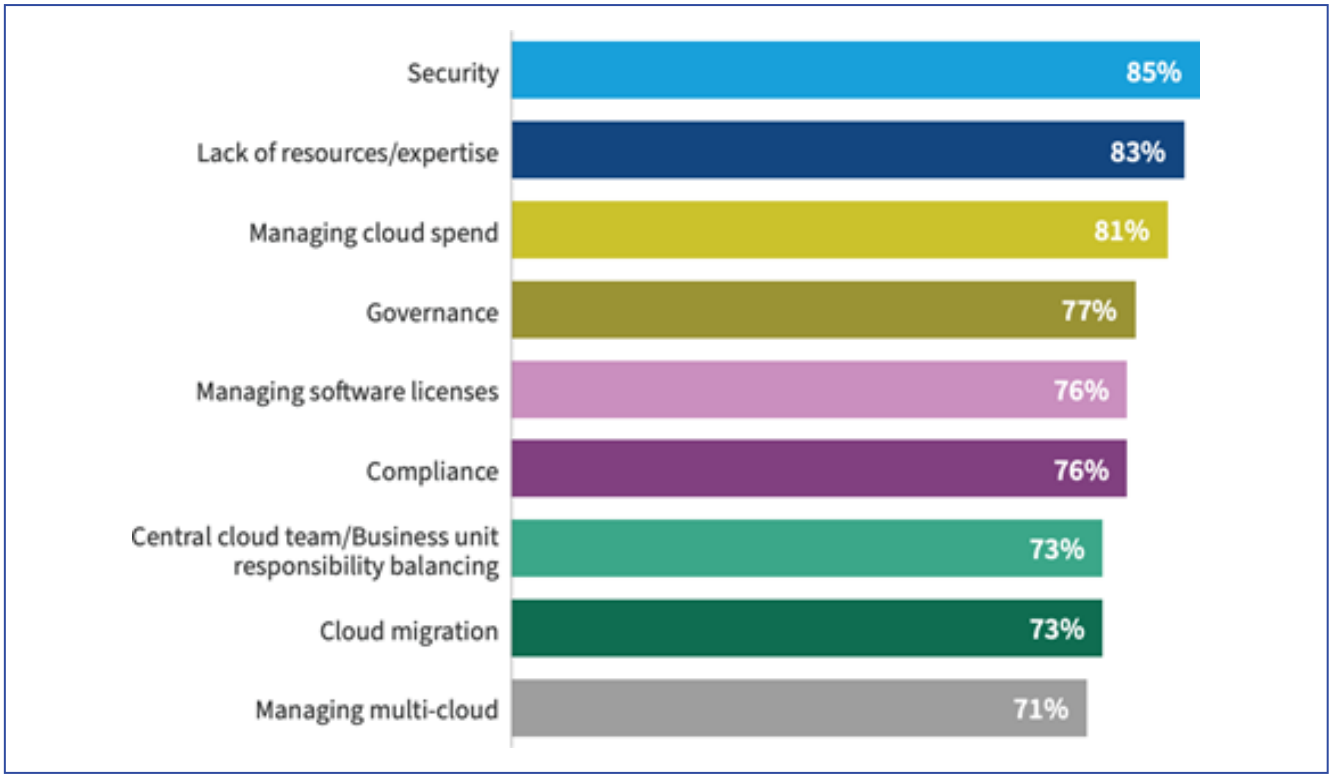
The right priorities need to be set to achieve the right results. This is crucial, especially with the abundance of data that is made available due to the variety of tools that are used today.

Standardization

Lack of standardization causes chaos within an organization, which will cause severe problems during Cloud adoption. This leads to a lack of visibility of security threats, and they may not be reported.

Timelines

An organization's risk management requires up-to-date information about security posture. Manual assessments only provide limited information with that risks applicable only at the time of the assessment. But timely information is needed for effective risk management.



An integrated GRC solution can address the challenges mentioned above.

Governance, risk management, and compliance in the cloud

This whitepaper is designed to guide IT leaders on how to approach the GRC requirements an organization needs to adhere to while embarking on their Cloud journey. A GRC framework usually sets the foundation for meeting security and compliance needs. Cyber security in the cloud is as important as on-premises security. Every organization must understand the cloud transformation dynamics and deploy a robust governance strategy at every stage of their cloud journey to benefit from the cloud solutions.

A good cyber governance, risk, and compliance (GRC) program demands an organization try to embrace complexity, uncertainty, and the dynamics involved in Cloud adoption. It is fundamental to securing the important cog in the wheel -- mission-critical applications -- as it provides a broad approach to managing cyber risks and enables them to meet their security and compliance objectives proactively. As businesses look toward increasing cloud adoption, they should also consider extending the GRC program to address cloud services and gain greater visibility into vulnerabilities.

"IT leaders who view the Cloud, bundled with GRC framework, as an enabler will excel in their digital transformation journey."

Businesses evolve every day and so do regulatory policies. Therefore, it is difficult to achieve the desired level of digitalization. The risks involved too are interdependent as the controls are also shared between the organization and the Cloud. The complexity increases further when adopting a multi-cloud strategy. However, with a continuous GRC framework, you can address these complexities, reap the Cloud benefits, and continue to grow more than ever, especially when you need to address a regulatory policy immediately.

In a nutshell, a GRC strategy should cover the following:

- Inventory and catalog of Cloud assets and services
- Implementation of security controls on Cloud resources
- Continuous monitoring of security and compliance requirements
- Automation of security and compliance changes
- Continued improvement of processes in use

Migrating to the Cloud is a journey, and the Cloud platforms' rapid evolution enables multi-functional teams to focus on core problems. Cloud Governance inclusion for an enterprise should always be an iterative and evolving process. This will benefit the cloud ecosystem that you are building. As digitalization is becoming more prominent, organizations should consider a GRC framework, such as from BootLabs, inducted into their strategy to drive an efficient cloud governance, risk management, and compliance program.

The GRC framework

GRC is one of the significant cloud challenges for any organization. A quick summary of GRC and its capabilities is shown below.

GOVERNANCE

Cloud Governance is a set of rules and policies adopted by organizations that run their workloads in the Cloud.

RISK MANAGEMENT

Risk management is the set of processes through which an organization can identify, analyze, and respond appropriately to risks.

COMPLIANCE

Compliance means conforming to the requirements stated by the regulatory bodies.

The GRC initiatives

GRC is one of the significant cloud challenges for any organization. A quick summary of GRC and its capabilities is shown below.

TAGGING

Assigning metadata to a cloud resource, which helps during RBAC, cost reporting, and automation. It is fundamental to providing enterprise-level visibility and control.

FORENSICS

Log analysis to capture potential compromised resources and to know how it's compromised. RCA outcomes from forensic investigations to promote and motivate preventive measures.

GOVERNANCE

The Cloud environment's ability to adhere to regulatory policies applicable to the organization. On maturity, this initiative is bundled with other capabilities to adhere to governance requirements.

SERVICE ONBAORDING

Ability to review and approve services based on internal, compliance, and regulatory requirements. It includes documentation, risk assessment, and implementation patterns.

LOG STORAGE

Enabling log collection and storage centrally to evaluate, monitor, assess, and audit access, and actions performed.

ITSM

Capturing planned modifications to configurable items in a Cloud environment within the defined scope. An approved change indicates changes with minimal risk to existing infrastructure.

AUDIT AND ASSESSMENT

Validating assertions that changes (what, when, and how) pertaining to the Cloud environment are performed in accordance with the regulatory policies.

DATA DE-IDENTIFICATION

Anonymize data subsets and information processed to reduce their sensitivity and prevent the underlying data format. The ability of data tokenization to minimize access to underlying data is critical.

Importance of cloud governance, risk management and compliance

An organization uses the Cloud to run their mission-critical workloads; GRC frameworks have the following benefits.

Standardization

A proper GRC framework reduces the management of irregularly designed structures in which accounts/ projects/ cost centers are used while adopting the Cloud. Every Cloud provider recommends best practices for the same. These workloads, when segregated for use, would provide standardization that improves cost control, sustainability, and security.

Reduce Operations Overhead

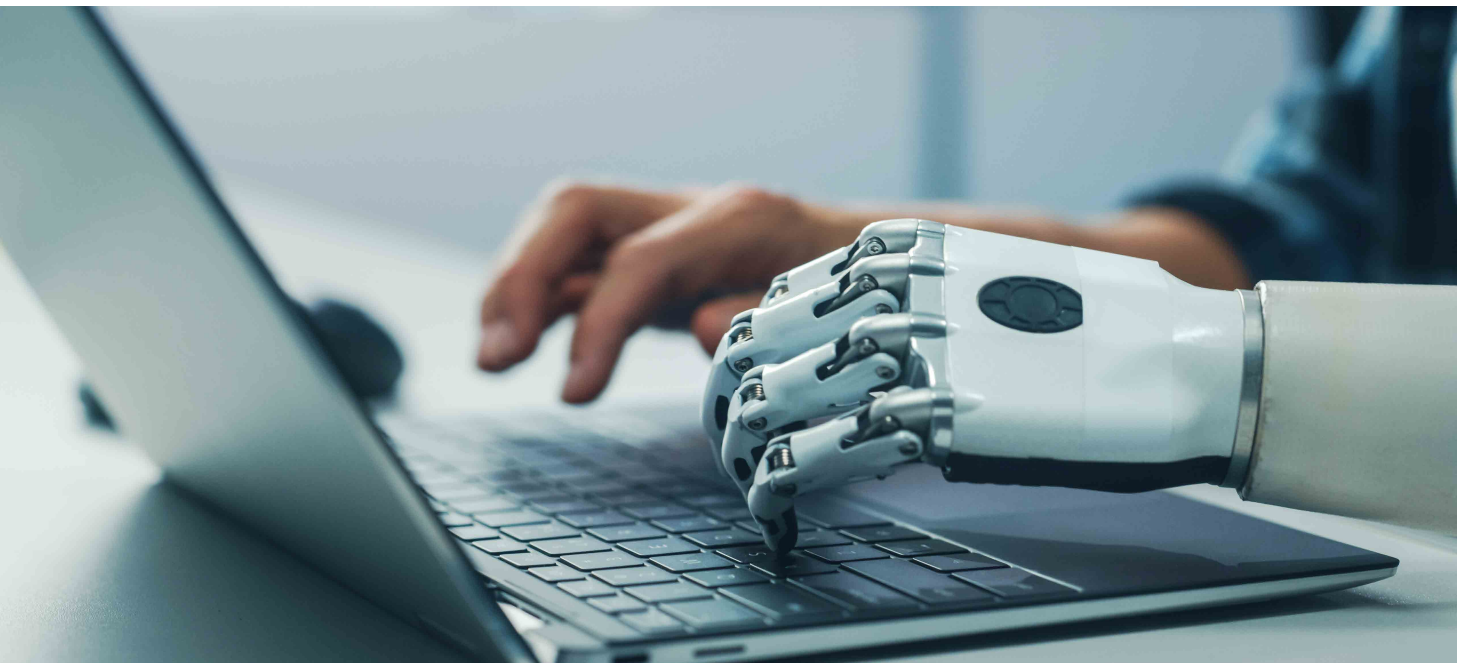
Organizations tend to use spreadsheets or perform manual processes to track the Cloud workloads' visibility. It's evident that this is error-prone, inefficient method is not sufficient for extensive cloud adoption. The GRC solution enables them to define centralized policies and apply them to all the cloud workloads. This centralization makes it easier to manage the cloud and reduce operational overhead.

Better Focus on Cloud Security

Without GRC, organizations do not have proper visibility of data, systems, or the deployed workloads. This situation increases cloud spend and poses a challenge for the security teams. GRC frameworks help mitigate this risk of security breaches and spikes in the Cloud costs. It also protects the confidentiality, integrity, and availability of information. The visibility of sensitive information and the assurance of appropriate security guidelines would enhance the overall security management.

Optimize Cloud Spend

A long-lasting FinOps story is essential for any organization to have accountability for the monthly Cloud spend. The GRC initiative helps you sail through your FinOps journey smoothly as it evolves every day.



Our managed services for GRC initiatives

Managed Services

Leverage Cloud-native services and build custom platforms, including platforms for application deployment, infra provisioning, compliance, and governance needs at scale, to accelerate your cloud journey.

Sailor

Sailor is a multi-cloud, no-code/ low-code platform that simplifies Cloud governance, optimizes cost, and increases efficiency.

Custom Accelerators

- Fast track cloud migration journey via custom platforms
- Build landing zone with standalone Terraform script, Automation
- Achieve Day 2 compliance and security
- Automate application onboarding platform
- Customize FinOps dashboards

Cloud Consulting (Cloud Lens & Transformation Blueprint)

Ambitions, Roadmap, Journey Management, Discovery & Assessment, Transformation Recommendations, Business Case & TCO Analysis

DevSecOps

- Zero Trust Model
- Perimeter Security
- Application Security
- Identity & Secrets Management
- Security Analytics
- Automated Pipelines for Infra and applications

360° Cloud Operations

- Poly Cloud Secure Landing Zone
- PaaS
- Reliability Engineering
- Cloud operations enhancements
- SRE
- Observability

Achieving GRC in the cloud using BootLabs GRC Framework

The below methodology was used for Microsoft Azure use case for one of our clients. We have similar use case applied on other clouds as well.

Governance

Implementing Governance across your Cloud environment

- Accounts & Subscriptions
- Policies & Management
- Inventory Management
- Cost Management
- Azure Management Groups
- Azure Policies & Azure Blueprints
- Azure Resource Graph
- Microsoft Cost Management

Risk Management

Implementing risk management for your Cloud environment

- Threat & Vulnerabilities
- Security well
- architected frameworks dentification & protection of mission-critical information assets
- Monitoring frameworks for all users & system actions
- Advanced ATP
- Well architected frameworks for Banking & FinTech on Azure Cloud
- Org assessment on important assets coupled with Cloud security controls
- Azure Activity Logs & Monitoring

Compliance

Implementing compliance management for your Cloud environm

- Continuous Compliance
- Laws & Regulations
- Policies, Processes, and Controls
- Reports & Certifications
- Azure Security Control
- Shared Responsibility
- Organisation Operational Framework
- Shared Responsibility

BootLabs GRC Methodology leverages tools and frameworks created by BootLabs, coupled with Cloud services and in certain cases third parties, that help address all the pillars of GRC.

Customers can leverage BootLabs sailor platform to provide end to end automation or leverage BootLabs managed services to create a custom GRC framework specific to the Organization requirement.

BootLabs implementation methodology

BootLabs GRC framework

DISCOVERY & ASSESSMENT

Discover the current state of Cloud adoption and its assets.

Assess cloud security risks, identify gaps, and create a roadmap for a secure cloud environment as an integrated part of your cloud journey.

PLAN

Device a strategy that complies with existing or new or a mix of cloud environments with minimal disruption to end user.

IMPLEMENT & AUTOMATE

Create an automated solution for GRC to reduce cost, time, and effort.

Reduce the risk and simplify the Cloud GRC.

EVALUATION

Evaluate that the controls in the Cloud environment are effective and that all the guidelines and practices are implemented.

CONTINUOUS MONITORING

Improve the framework continuously by tracking and monitoring risks and compliance issues.

About QualityKiosk Technologies

QualityKiosk Technologies is one of the world's largest independent Quality Assurance (QA) and digital transformation enablers, helping companies build and manage applications for optimal performance and user experience. Founded in 2000, the company specializes in providing QA automation, performance assurance, Robotic Process Automation (RPA), synthetic monitoring, site reliability engineering (SRE), digital testing as a service (DTaaS), customer experience, Cloud, and data analytics solutions and services.

With a strong presence across 25+ countries and an expanding workforce of more than 3000 employees, we enable some of the leading banking, e-commerce, automotive, telecom, insurance, OTT, entertainment, pharmaceuticals, and financial services brands to achieve their business goals. We have been featured in renowned global advisory firms, including Forrester, Gartner, and The Everest Group for our innovative, IP-led quality assurance QA solutions and services and the positive impact we have created for clients in the fast-changing digital landscape. To learn more, visit https://www.qualitykiosk.com.

+1 347 304 9098

letsconnect@qualitykiosk.com

www.qualitykiosk.com

QUALITYKIOSK TECHNOLOGIES