CLOUD COMPLIANCE: BEST PRACTICES FOR SUCCESS

After years of experimentation, business organizations are adopting cloud computing at scale. They have remained skeptical of their ability to manage regulatory compliance and security of sensitive information assets.

As they transition mission-critical IT workloads and apps to the cloud, their security posture is possibly a tradeoff between cost and performance of the cloud service. This is partly because government institutions mandate vastly different measures and policies on cloud computing. These mandates aren't optional—the related fines and lawsuits are not the only implications of failure to compliance.

Today's internet browsers are increasingly aware of their rights to data privacy and online security. Organizations that fail to protect user information stored in the cloud due to inadequate security measures as mandated by regulatory compliance therefore also compromise user trust and brand loyalty.

Since these regulations lay down the bare minimum requirements on security in the cloud, it's important to understand cloud compliance regulations and follow the industry proven best practices on cloud security and governance.

Cloud compliance stats

Compliance of cloud-based solutions is one of the leading challenges facing organizations that aim to migrate existing workloads to the cloud. According to recent research surveys:

- 94% of IT and security professionals believe that compliance is a top priority for their organization. At the same time, 45% are also not concerned about penalties for noncompliance.
- More than 50% of the organizations face the compliance and audit challenges associated with Infrastructure as a Service (IaaS) cloud solutions.
- 32% of the organizations found incorrect access authorizations and privileges assigned to users. 60% are considered as shadow administrators.
- Under two-thirds (63%) of users pause to consider the organization's data collection and storage practices before sharing sensitive information with them.
- Data classification due to cloud computing makes real and true encryption a challenge, according to 65% of organizations.

Cloud compliance regulations

Let's begin the discussion with a quick review of the common cloud compliance regulations applicable to organizations in different industry verticals:

- **HIPAA (Health Insurance Portability and Accountability Act)** mandates security of electronic healthcare information, confidentiality and privacy of health related information, and information access for insurance.
- **PCI DSS (Payment Card Industry Data Security Standard)** is a set of security standards that enable all organizations to accept, process, store and transmit credit card and financial information.
- **GLBA (Gramm-Leach-Bliley Act)** requires organizations to communicate how user information is shared and protected, provide right to opt-out and apply specific mandated protections.
- **PIPEDA (Personal Information Protection and Electronic Documents Act)** provides rules for organizations to handle user information in conducting commercial activities.
- **EU GDPR (General Data Protection Regulation)**, the most stringent privacy and security regulations, mandate an exhaustive set of requirements on organizations handling data of European Union (EU) residents. GDPR imposes harsh penalties for noncompliance.
- **SOX (Sarbanes–Oxley Act)** mandates requirements on financial disclosures, audits, and controls of information systems processing financial information.
- **U.S. State Breach Laws:** All 50 U.S. states require organizations to notify individuals in event of security breaches involving their personally identifiable information.
- **NIST (National Institute of Standards and Technology)** is the organization that provides guidelines on technology related matters such as standards, security, innovation, and economic competitiveness.
- **FedRAMP (Federal Risk and Authorization Management Program)** is a standardized program for security assessment and evaluation of cloud-based systems.

How to achieve cloud compliance

Cloud compliance regulations are constantly changing and updated to meet the growing demands of information security and user privacy. Adhering to the exhaustive set of cloud compliance regulations seems like a daunting task but we've put together a few important tips to successfully achieve compliance in the cloud:

Know your compliance regulations

Compliance is not easy but getting to know the applicable regulations is the first step toward achieving compliance. Understanding the regulations and optimizing the compliance infrastructure may require external assistance through consultants and experts, which is costly—but not as expensive as noncompliance.

Know your responsibilities

Cloud vendors typically only offer a model of shared responsibility as it pertains to security and compliance. It's important to fully understand your own responsibilities and adopt the measures

necessary to guarantee compliance from your end.

Manage information access & controls

Monitor how your data in the cloud is accessed and controlled. Look out for identity and access control lapses or anomalous behavior. Adopt the principle of least privilege access: users are allowed to access only the information and resources necessary, and no more.

Conduct audits routinely

Examine cloud compliance regularly. Identify the shortcomings of your IT environment as well as the organizational culture and workforce behavior, which may involve practices directly and indirectly violating compliance regulations.

Know how your data is stored

IT workloads are shared dynamically between hardware resources that make up a cloud environment. Especially for hybrid and multi-cloud environments, make sure that your IT asset distribution is optimized for minimal security risk.

Encrypt, encrypt, encrypt

Always encrypt sensitive business information, which means that the data remains secure even when it is compromised. Apply multiple layers of security where necessary and viable.

Related reading

- BMC Security & Compliance Blog
- BMC Multi-Cloud Blog
- What Is GRC? Governance, Risk, and Compliance Explained
- SecOps vs InfoSec: An IT Security Comparison
- Multi-Cloud vs Hybrid Cloud: What's The Difference?
- The State of SaaS Today: Growth Trends & Statistics