The Ultimate Guide to Cloud Compliance: GDPR, HIPAA, SOX, and More

The cloud offers unparalleled scalability and flexibility. However, it also introduces a new layer of complexity in terms of data security and compliance. To begin with, businesses must understand the shared responsibility model for cyber security. And no ultimate guide to cloud compliance would be complete without best practices for navigating multiple regulations.

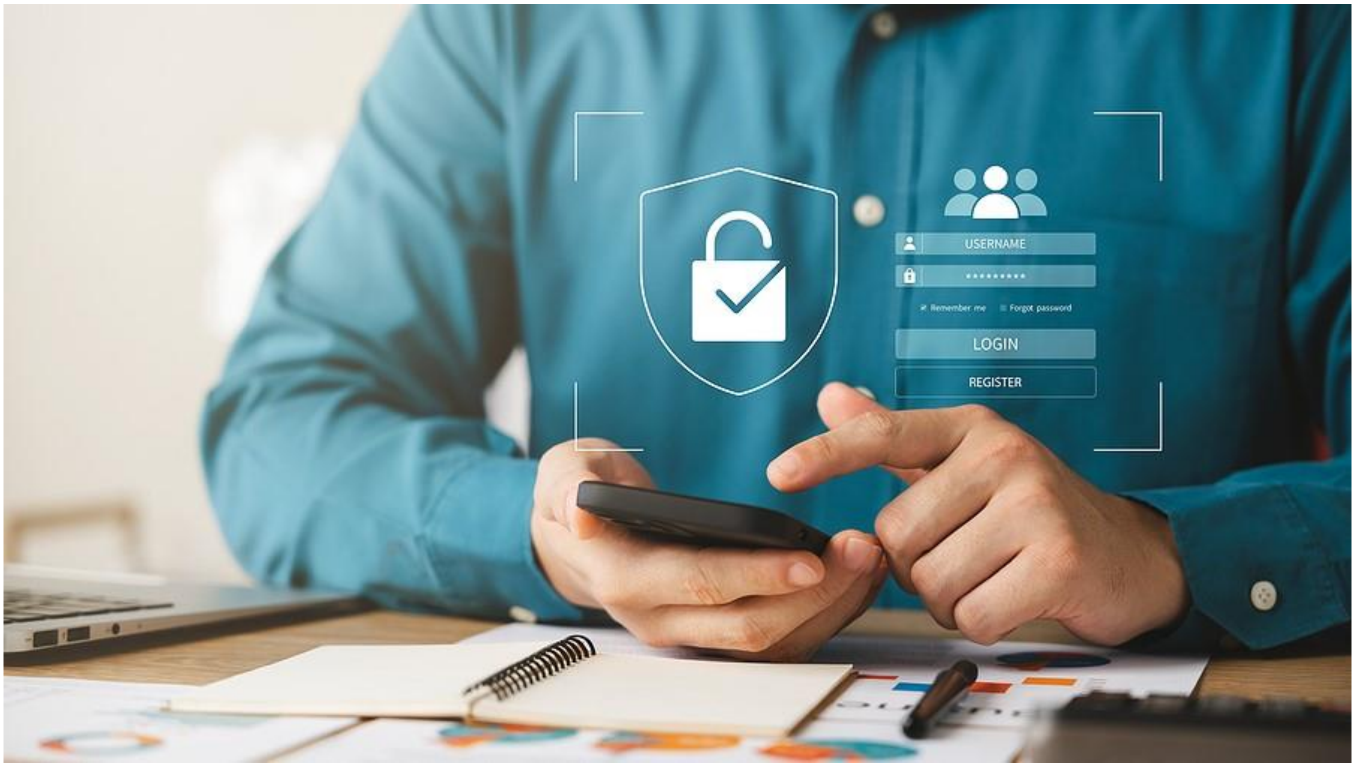
In the United States, the lack of any single, overarching cloud compliance law complicates the matter. Businesses must stay on top of a patchwork of federal and state laws, applicable international laws, and industry-specific regulations. This guide will help streamline the process.

Understanding the Shared Responsibility Model

Business leaders must remember that cloud compliance involves a shared responsibility between the cloud service provider and the customer. Under this shared responsibility model, cloud providers take responsibility for securing the underlying infrastructure, while the customer secures the data and workloads that live in the cloud.

For example, Microsoft secures its data centers and implements robust security around the hardware and networking equipment that supports Microsoft 365 services. It employs some encryption, provides continuous monitoring of the platform, and releases security patches for its applications.

Microsoft customers, on the other hand, must configure the Microsoft 365 security options properly and apply patches promptly. Additionally, they need to take steps to track and protect sensitive data. They must also secure user accounts and control data access. And they need to identify and protect endpoints that include every device that connects to the network.



Major Regulations to Consider

Organizations may need to comply with any number of privacy regulations, depending on their location and industry. But several key regulations apply widely and/or set the tone for other regulations. Understanding these landmark regulations will help organizations build an overall compliance strategy.

The **General Data Protection Regulation (GDPR)**, while a European law, still applies to many US businesses, and it serves as a model for many emerging regulations here in the States.

Key requirements of GDPR include the requirement to gain clear consent before processing personal data. Individuals also have the right to access their personal data or request a transfer of that data. And businesses must notify individuals promptly if a breach occurs.

The **Health Insurance Portability and Accountability Act (HIPAA)** sets the standard for protection of protected health information (PHI). It requires entities to implement stringent safeguards to protect PHI, including limiting PHI access to authorized personnel. It also requires organizations to encrypt PHI data, conduct regular risk assessments, and train employees.

The **Sarbanes-Oxley Act (SOX)** mandates strict controls relating to financial data and applies to all public companies in the US. It includes stringent requirements around retention and destruction of financial records. It also requires companies to strengthen IT controls around financial systems and data. And it mandates audit trails and regular risk monitoring.

Several states model their privacy laws on the **California Consumer Privacy Act (CCPA)**. It grants consumers the right to access and correct their data that businesses collect. It also guarantees individuals the right to opt out of the sale or sharing of their personal data, as well as to request deletion of their data. And businesses must take reasonable security measures.

Key Steps to Building a Compliant Cloud Environment

While each regulation has specific requirements, common themes run across regulations. Prioritizing those common elements will help businesses stay ahead of the compliance game.

- Data governance – Develop a comprehensive data governance framework that includes classifying and monitoring sensitive data, tightening access controls around that data, and implementing clear policies around data retention and data sharing.
- Vendor management – Review vendor contracts to ensure necessary language regarding data privacy and security. Additionally, carefully control vendor access and perform regular supply chain audits and monitoring.

- Incident response – Create, implement, and regularly update a plan for responding to data breaches, including mandated notifications.
- Continuous monitoring – Regularly monitor compliance status and make necessary adjustments. Automated compliance monitoring streamlines this process.

- Ensure consumer control over personal data – Display privacy policies clearly on public-facing apps and websites. Include easy-to-use forms for consumers to specify their preferences regarding sharing of personal information, targeted advertising, and cookies.

- Ensure reasonable security measures – In addition to measures already mentioned, implement encryption, strong authentication methods, role-based access controls, and comprehensive network security. Deliver regular employee training around security and compliance.

Additional Tips Round Out the Ultimate Guide to Cloud Compliance

Compliance concerns require substantial time, resources, and energy. However, by wisely leveraging compliance technology such as the compliance solutions from eGovernance.com, businesses can reduce much of the pain involved in regulatory compliance.

eGovernance Compliance allows you to tackle all data compliance monitoring mandates simultaneously, including HIPAA, GDPR, CCPA, SOX, PCI-DSS, and more. It gives wide visibility by connecting to all data storage locations through a single console. It also simplifies data classification, aids access control, and provides automated alerts to possible problems.

Take a proactive approach to regulatory compliance by contacting the compliance experts at eMazzanti Technologies.