UnifyBCS
Bridging the digital divide

SECURITY GUIDE

How Cloud Deployment Affects Compliance

Organizations that need to ensure ongoing compliance have to address several key requirements before they can migrate sensitive data to the cloud. This security guide explores the compliance challenges facing organizations that take on cloud deployment initiatives, the key requirements for keeping cloud-based data and resources protected and compliant, and the approach Gemalto provides to effectively address these objectives.

Compliance in the Cloud: The Fears and Challenges

Many enterprises want to take advantage of the performance, cost savings, and scalability that cloud-based Infrastructures offer. However, compliance requirements don't vanish when an enterprise deploys a cloud-enabled solution, whether it's a software-as-a-service (SaaS) application, platform-as-a-service (PaaS) or a full Infrastructure-as-a-service (IaaS) deployment. As regulated organizations look to lever age the cloud more fully, they must contend with several issues:

> **Clarification of security responsibilities.** When organizations migrate regulated data to cloud-enabled and particularly public cloud environments, they have to rely on their cloud vendors for at least some of their compliance measures. The respective roles and responsibilities of client and vendor will vary significantly depending on the cloud model deployed. For example, in an IaaS environment, a customer will retain such responsibilities as data protection and patching, while a vendor may be responsible for physical security, network segmentation, and isolating tenants in multi-tenant environments. Regardless of the cloud model adopted, organizations will need to ensure the lines of responsibility are drawn clearly, and that the vendor's security measures are demonstrable and auditable.

> **Addressing the implications of regional mandates.** There are many regulations that are not only specific to a given region but that stipulate where sensitive information assets can and can't reside. For example, before a federal U.S. government agency migrates sensitive assets to the cloud, management will need to ensure the cloud provider won't store or manage information assets in facilities outside of the U.S. Likewise, in some European countries, a healthcare provider wouldn't be able to use a cloud provider's services to store patient data unless the provider's facilities were located solely within the specific country's borders.

UnifyBCS Data Protection solutions can help organizations:

> Protect more data in more locations.

> Lever age central control and visibility.

> Ensure compliance—no matter what changes.

> **Safeguarding data privacy and trust.** When regulated data is under the control of a cloud provider, organizations must have a clear understanding of how that data may be retained. For example, some cloud providers have a policy specifying that, in the event of a contract termination, they will retain customer data until all debts are paid, which would be a non-starter for many regulated organizations. In other cases, if a cloud provider is subpoenaed, they may agree to hand over records for one or more clients to legal authorities. Finally, issues surrounding the cloud provider's proper destruction of instances and virtual machine images canalso present concerns.

In order to meet their regulatory mandates in virtualized cloud environments, organizations must go beyond basic user access controls and proactively apply robust security policies.

Sustaining Compliance in the Cloud: The Requirements

In order to meet their regulatory mandates in virtualized cloud environments, organizations must go beyond basic user access control s and proactively apply robust security policies. To achieve these objectives, organizations need to address the following requirements:

> **Control privileged user access.** To comply with many security mandates, organizations have to guard against insider threats and mitigate the risks posed by malicious administrators. Organizations need to ensure that, even in multi-tenant public cloud environments, security teams have the visibility and control they need to safeguard sensitive assets. To do so, organizations must logically separate virtual instances that hold sensitive data. As a result, security teams gain the controls they need to ensure a cloud provider's administrators can't abuse their super-user privileges and that users with access to one instance can't gain access to another group's instances. In addition, organizations need to enforce separation of duties—for example, requiring multiple administrators to conduct critical administrative tasks, such as policy changes and key export.

> **Guard against unauthorized virtual machine copying.** In cloud-enabled environments, virtual machine images or instances are constantly migrated across virtual machines. Given the fluidity of these environments, organizations need to ensure that virtual instance images, and the sensitive data they possess, are not inadvertently left on systems, and potentially stored in insecure systems. Organizations must also retain complete control over how data is isolated, protected, and shared in multi-tenant cloud environments. By encrypting virtualized instances, organizations can significantly reduce the number of ways users can get sensitive data off physical images, and so guard against a host of vulnerabilities. In addition, organizations have to more granularly apply security policies to specific subsets of data; for example, at the column level in a database. This represents a way to have data secured as it progresses through workflows, both in on-premises and cloud-based applications.

> **Ensure visibility and auditability.** Enterprises and cloud providers need to ensure they have visibility over the enforcement of security policies, and that access, modification, and administration of sensitive assets can be concretely and definitively reported on and verified by external auditors. For example, the Payment Card Industry Data Security Standard (PCI DSS) offers a host of requirements related to reporting, auditing, and logging the activities surrounding regulated data. As organizations migrate to the cloud, these obligations can quickly grow very challenging to contend with. To ensure compliance, organizations must be able to centrally, comprehensively, and efficiently track activities relating to regulated data—even for data in cloud environments. For example, this requires authentication management platforms that enable organizations to centrally manage authentication devices and policies across both on-premises and cloud-based applications and services. In addition, organizations must have a centralized, efficient way to manage encryption and keys across the enterprise, which streamlines the process of tracking access to sensitive data and procedures.

A Comprehensive Approach to Compliance

UnifyBCS recommends organizations take a comprehensive approach to compliance that includes:

> **A unified data protection foundation** that addresses compliance needs across a wide set of systems, formats, and locations.

> **Centralized control and visibility** that establishes a central point of control and management, enabling organizations to "prove" control of data and policies.

> **The ability to evolve with changing mandates and infrastructures** so that organizations can adapt easily and quickly to new regulations and new technologies—including virtualization and cloud offerings.

All three of these principles are critical to the success of cloud-enabled deployments. Built with these Compliance Infrastructure principles in mind, UnifyBCS Data Protection solutions can help organizations:

> **Protect more data in more locations.** The UnifyBCS Data Protection solutions offer protection of data across more systems and cloud services than any other vendor. Plus, our solutions are proven every day in the most demanding, processing-intensive environments—scaling to support millions of records and trillions of transactions.

> **Leverage central control and visibility.** UnifyBCS Data Protection solutions enable policies and control s to be centrally implemented, managed, and audited, which helps boost security and administrative efficiency. With UnifyBCS, security teams can centrally set, enforce, and update security policies across all users, deployments, and use cases.

> **Ensure compliance—no matter what changes.** UnifyBCS Data Protection solutions feature a modular deployment model that equips customers with optimal efficiency and flexibility in implementing and adapting security mechanisms. Consequently, organizations can sustain compliance—while they adapt to changing mandates, business requirements, and evolving cloud initiatives.

Conclusion

The cloud enables significant advantages to organizations—including cost savings, improved agility, and improved services. With UnifyBCS, organizations can maximize the benefits of the cloud while they ensure compliance with relevant regulatory mandates. Regardless of where the data resides or is moving within the network, UnifyBCS helps to enable compliance in the cloud and across the organization as a whole by applying strong multi-factor authentication to cloud-based applications, securing sensitive data with encryption and enabling organizations to centrally own, manage and secure their encryption keys.

About UnifyBCS's SafeNet Identity and Data Protection Solutions

UnifyBCS's portfolio of Identity and Data Protection solutions offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy Industry-leading protection of data, digital identities, payments and transactions–from the edge to the core. UnifyBCS's SafeNet Identity and Data Protection solutions enable enterprises across many vertical s, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and Identity management solutions to protect what matters, where it matters. Through these solutions, UnifyBCS helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, an digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Contact Us: For all office locations and contact information, please visit www.unifybcs.com

UNIFYBCS.COM