VIEW POINT

LIFE SCIENCES – ENSURING CLOUD COMPLIANCE

Infosys®
Navigate your next

What is Cloud Compliance?

Cloud usage poses threats to patient data, clinical trial data, and data related to pharmaceutical research and secret formulae since they are extremely confidential, sensitive, and valuable.

As such the integrity and security of data are of the highest priority to the regulatory bodies and pharmaceutical companies. They have set up regulations and guidance to control and inspect electronic data security and integrity.

This gives rise to the term – 'cloud compliance'. It is the process of complying with regulatory standards for cloud usage. This white paper will cover the key good practices (concepts excluding tools and technologies), that needs to be followed to ensure cloud compliance.

How to Achieve Cloud Compliance?

The first step towards achieving cloud compliance is to be aware of the standards and regulations that apply to your industry and organization as per geographies. Organizations need to analyze and work out regulations' applicability per their selected cloud model. Cloud security and compliance are a shared responsibility between cloud service providers (CSP) and organizations. Other than building a strong contract with CSP, ensuring compliance certifications (HIPAA, PCI-DSS, FedRAMP, GDPR, FIPS 140-2, NIST 800-171), understanding services, and reviewing SLAs, cloud compliance needs to be incorporated in all levels or phases by both CSP and customer. Cloud Security Alliance (CSA) organizations have also defined best practices and frameworks to ensure a secure cloud computing environment. The CSA Cloud Controls Matrix (CCM) is a cybersecurity control framework that covers key aspects of cloud computing. It is composed of 197 control objectives, structured in 17 domains. Compliance will come when the right actions will be imbibed in each activity associated with the cloud.

Let's understand some good practices to ensure cloud compliance-

Risk Assessment and Analysis

Analyzing and assessing risks related to each requirement helps mitigate future complications. Mitigation helps in reshaping processes and creating/updating manuals, controls, templates, and approaches to testing. Risk assessment is considered in all phases of the system life cycle to encounter underlying risk. Setting up a roles and responsibility matrix (R&R) during the initial phase of the project is also a good practice.

Security by Design (SbD) and Test Strategy

Embedding security into hardware and software (infrastructure, network, OS, code, and data layer) from the design phase is another approach toward cloud compliance. It is known as Security by Design (SbD). Setting up security requirements and architectural design decisions are often based on well-known security tactics and patterns. Qualifying infrastructure, OS hardening, base controls, and setting up a controlled environment form the basis of application validation.

Similarly, test strategy as per risk assessment must include cloud security-specific testing such as penetration testing that finds flaws in the security of a system by exploiting system vulnerabilities. It helps mitigate risks and protects vital business data.

An external vulnerability assessment and penetration test can identify the potential threat to systems from outside the defined network. Dynamic Application Security Testing (DAST) like black box testing, is used to test web applications through the front-end from outside of a web app, just like a hacker. Automated Application Security Testing should be conducted considering the application and interface security policy as well as application security baseline requirements.

DevOps Integration

Advancement to this is the DevOps integration that empowers infrastructure, application development, and maintenance with automated controls where security is embedded right from the infrastructure design to configuration to the release of the application. It supports the user with all compliance controls such as versioning, access control, security testing, and monitoring the health check of application/infrastructure, etc. Automation brings many flavors to cloud compliance by enabling automatic encryption, automatic security patching, reviews, etc.

IT credentials are generated, changed, stored, backed up, audited, and then revoked/deleted as per requirement. Cloud service customers need to describe and enforce their security policies, user roles, groups, and assets with due consideration of industry, regional, or corporate requirements.

Authorizations should be granted on the principle of least privilege to reduce security risks. The principle of least privilege (PoLP) is the concept of granting access only to the resources that are necessary to perform the assigned tasks. Controlled access to systems can be managed through the implementation of Single Sign-on (SSO), Multi-Factor Authentication (MFA), Privilege Access Management (PAM), Access Control List (ACL), and Separation of Duties (SOD). The physical areas where information security assets are kept should be protected from unauthorized access.

Data Asset Catalogue

It is used to identify and classify all data assets in terms of their criticality to the business and legal requirements considerations. It should specify ownership and responsibility for the data and describe the location(s) and acceptable use of the assets. Data asset catalogs should maintain a relationship (if any) between data assets. It should cover the flow of sensitive data and its permanent/temporary work storage. R&R of responsible parties should be mentioned in data asset catalogs.

DAM (Digital Asset Management) is another way to ensure that authorized people have access to the collection of digital assets to streamline the usage, tracking, and approval of assets. Agreements on data locations as well as data retention and deletion should be documented and followed.

Data Protection

The effective technique is the encryption of the data. Sensitive data should be encrypted, both at rest and when the data is in transit across a network, for example, between storage and processing, or between the provider's system and a customer system. Protective mechanisms such as HTTPS (Hypertext Transfer Protocol Secure), sFTP (Secure File Transfer Protocol) enables secure file transfers and secure communication over a computer network and the internet by using various encryption and authentication mechanism. OTR (Off the Record) tool encrypts emails prior to their transfer. Dropbox, a tool used for sharing encrypted files also ensures secure data transfer using a secure socket layer with transport layer security.

Classification of data, documentation of data flow, ownership, stewardship of data, ensuring data protection and privacy by design, and conducting data protection impact assessment are a few other data protection mechanisms that should be considered.

Networking

Network infrastructure are the devices such as routers and switches, services, and software that make up the network. Security of physical devices as well as cloud network should be fully visible. Network providers should be able to deal with denial of service (DDoS) attacks, detect intrusion and have prevention in place (e.g., firewalls). A network services agreement must be in place to identify security features and management requirements for the network. Networks must be monitored and tested regularly to check for vulnerabilities. Documentation of network architecture and security procedures should also be in place.

Tenant Isolation on Cloud

Tenant isolation mentions that every application needs to run in its own tenant and there should be different development, staging, and production environments for each application within its own tenant.

In the case of a multi-tenant cloud environment, proper separation of data belonging to a customer should be done. The key security principles of confidentiality, integrity, and availability should be applied to the handling of the data through the application of a set of policies and procedures which should reflect the classification of the data.

Maintenance and Operations

This plays a pivotal role in maintaining cloud compliance. It refers to operational processes such as internal/external audits, assessments, remediation activities, change management, incident management, periodic review of the system, access, audit trail logs, Service Level Agreements (SLAs) and methodologies, etc. Periodic security testing such as penetration testing and DAST along with an architecture assessment should also be part of maintenance.

Application, network, and infrastructure security metrics should be shared to understand the security health and eliminate further vulnerabilities. This phase also includes the execution of policies related to employees such as background screening, guidelines on assets, remote and home working, offboarding and onboarding, training, etc. Installation of a good anti-virus, malware protection software, and well-managed data backup and restoration process should be followed.

Continuous Monitoring and Reporting

Leveraging log tools, verification systems, and automation techniques helps monitor vulnerabilities. Monitoring tools need to be scalable to your growing cloud infrastructure and data volumes. It should lookout for constant or new and modified components. Monitoring alerts should be set up to monitor every layer of cloud infrastructure. It includes monitoring network traffic, running scans for detecting internal and external network vulnerabilities, and setting up a detection system for intruders. E.g., usage of SPLUNK SIEM tool, a monitoring and searching tool, that collects, analyzes, and correlates high volumes of network to generate alerts and reports

Data monitoring checks on data access, data change, data copy, data file name change, file classification changes, or data ownership change should be in place. Monitoring alerts should be set up as per definitions of threshold to inform data owner on data activity.

Continuous monitoring and analyzing incoming **emails** for malware and responding to abnormal activities in the mail using on-demand resources should be done to handle employee or user-level mistakes.

All activities (outsourced or insourced) must be monitored for information security controls (defined under ISO27001, NIST, Cybersecurity of FDA etc.). Suppliers are required to comply with the same security requirements as applicable to client organization.

Organizations must employ robust reporting capabilities such as periodic reports, releasing reports on trends, etc. to constantly measure security and compliance results.

Business Continuity and Disaster Recovery Setup

Business continuity consist of contingency plans and measures that should be periodically tested and updated to ensure operational continuity. DR methods (a subset of BCP), restore the use of critical systems and IT infrastructure, minimize business downtime, and focus on getting technical operations back to normal in the shortest time possible. BCP and DRP executions are requirements of 21 CFR Part 11, Annex11, etc. ISO 27001 provides a step-by-step process to ensure the continuity of business operations after a breach.

Awareness, Training, And Communication

The most important part is awareness and training on laws, compliance, and their adherence. According to statistics from a CompTIA study cited by shrm.org, "Human error accounts for 52 percent of the root causes of security breaches."

Employees should be aware of their responsibilities and roles and trained towards compliance requirements. They should execute their assigned task as per process and work instructions.

The most common precautionary steps include - educating staff about unsolicited emails, not sharing sensitive information with anyone, setting up permissions, tracking the versions, updating software, maintaining strong passwords, and identifying phishing scams. These controls should be verified periodically through audits, test mails, etc.

Building Compliance Into the DNA

Cloud compliance needs to be in the DNA of the organization. Continuous efforts and improvements are needed to build compliance. The points below help us to avoid any regulatory implications in future

- Building awareness
- Diligent adherence to the requirement of compliance
- Setting up a compliant computerized system

About the Author

Pooja Mishra

Pooja has experience in validation of application, Infrastructure Qualification and Cloud Validation, in scope of roles - validation manager, quality lead etc. She has experience in internal audits and periodic reviews as well.

References

- www.datamotion.com
- **SPECIAL REPORT 2019** - A Winning Strategy for Cybersecurity - ZD Net - Tech Republic
- **The Changing Faces of Cybersecurity Governance - WHAT TO DO BEFORE AND AFTER A CYBERSECURITY BREACH?**

Infosys®
Navigate your next

For more information, contact askus@infosys.com