Ensuring Compliance for Cloud at Life Sciences Organizations

Abstract

Cloud computing is becoming a reality across the life sciences industry driven by the need to manage cost pressures, optimize operational efficiencies, and build robust IT capabilities. However, being a highly regulated industry, players face significant compliance challenges while leveraging the cloud. In addition to managing security risks in a shared computing environment, organizations also need to ensure that regulatory commitments are met effectively.

Redefining IT Delivery and Management with Cloud

Life sciences organizations have been maximizing cloud adoption for non-regulated and non-mission critical applications, but have been conservative in shifting regulated services. Applications on the cloud pose multiple challenges in terms of security and data privacy, which makes it all the more difficult to maintain regulatory compliance . Ensuring accountability and managing risks are the key challenges that organizations face in embracing cloud as the IT environment is managed by the service provider.

Challenges Faced by Life Sciences Organizations

Besides managing inherent risks of security, reliability, data privacy, and change management associated with cloud adoption, life sciences companies also need to ensure compliance with regulations set by the Food and Drug Administration (FDA) and European Medicines Agency (EMEA) and other regulators worldwide. Compliance with US FDA Code of Federal Regulation Title 21, CFR Part 11 Electronic Records and Electronic Signatures, and the

European Union GMP Annex 11 Computerized Systems compounds the challenge. These include:

- Establishing documented evidence that infrastructure process equipment, ancillary systems, and subsystems are compliant with approved design specifications, and are capable of consistently operating within established limits and tolerance levels
- Ensuring complete documentation to substantiate that computerized systems consistently perform according to predetermined specifications and quality
- Retaining necessary records for the required duration
- Securing data to ensure only authorized access and maintaining integrity of records
- Maintaining audit trails for all actions including creation, modification, and deletion of records to ensure compliance with 21 CFR Part 11/Annex 11 requirements

Cloud service providers have been addressing some concerns through compliance with SSAE16, PCI DSS, HIPAA, US-EU Safe Harbor Framework, ISO 27001 Certification, and SOX standards.

Managing Regulatory Compliance in a Shared IT Environment

Ensuring effective IT compliance management requires multiple levels of controls to ensure data reliability, reduce risk, and optimize governance:

- **Application Control**

Comprises activities such as system validation to ensure integrity and confidentiality of a business application and its data in order to be compliant with ER/ES requirements

- **Application Environment Configuration**

Includes configuring applications per the organization's business processes, and combining activities such as changing configuration parameters and interface for COTS applications

- **Infrastructure and Platform Control**

Encompasses activities such as qualification of infrastructure software, change and security controls, and patch management to ensure that the operating system and other platform software comply with regulations

	Application Control	Application Configuration	Platform Control	Infrastructure Control
Iaas	RO	RO	RO	CSP
Paas	RO	RO	CSP	CSP
Saas	CSP	CSP	CSP	CSP

The extent of control of Regulated Organizations (RO) vis-à-vis Cloud Service Providers (CSP), based on the type of cloud services model

Evaluating Risks and Facilitating a Mitigation Strategy

On a private cloud, RO is fully responsible for governance as well as audit and review activities. However, in a public, community, or hybrid cloud, IT compliance responsibilities are distributed between CSP and RO, and vary based on the type of service.

Organizations should assess risks based on the deployment model to help identify the best suited cloud model that meets both security and regulatory requirements. Here’s a more detailed look at each of the deployment models:

Activity	Public/Community/Hybrid Cloud (Responsibility)		
	Iaas	Paas	Saas
Infrastructure qualification	CSP	CSP	CSP
Platform (Infrastructure software) qualification	RO	CSP	CSP
System validation	RO	RO	CSP
Compliance with record retention requirements	RO	RO	CSP
Maintenance of audit trail and electronic signature	RO	RO	CSP
Compliance with data security and integrity requirements	RO	RO	CSP

The responsibilities of the regulated organization (RO) and the cloud service provider (CSP) across compliance activities in various cloud deployment models

- **Infrastructure as a Service**

The CSP controls infrastructure in an IaaS setting, while the RO is responsible for managing the platform and application.

On a private cloud, infrastructure qualification requirements can be enforced by the RO. However, the company needs to evaluate the risks due to non-adherence to processes by the cloud service provider. It is therefore recommended LS organizations closely monitor CSPs and perform audits on a regular basis.

For an off-premise private cloud, organizations may face challenges of data integrity and availability. Therefore, controls such as standard operating procedures (SOPs) and service level agreements (SLAs) need to be defined and established.

On a public cloud, the infrastructure must be qualified and maintained in a qualified state for hosting any application supporting GxP (Good 'x' Practices, e.g., Good Manufacturing Practice) related activities. To mitigate the risk of non-compliance, the RO should:

- Audit the processes related to cloud deployment and identify gaps.
- Review key qualification deliverables such as qualification plan, and installation and operational qualification services.

- Perform additional qualification activities to close identified gaps.
- Establish robust quality or SLAs for process compliance.
- Platform as a Service

The CSP controls the infrastructure and the platform, while application management is performed by RO.

The risk exposure is similar to that of the IaaS model, therefore the same controls should be applied to minimize risk. In addition, companies need to:

- Audit the vendor to verify data security process and access controls
- Verify the provider's security testing and vulnerability assessment processes
- Perform additional penetration testing and vulnerability assessment
- Verify the process for data segregation between multiple customers
- Evaluate security of the change control process for infrastructure software management
- Define stringent SLAs for security requirements
- Software as a Service

All aspects of the infrastructure and platform should be evaluated. Organizations should determine a detailed risk identification and mitigation plan. Under this model, RO needs to deploy mitigation plans such as:

- Perform additional activities like operation or performance qualification as required to close the gaps in a software validation process.
- Conduct additional testing to verify if configurations are appropriate, and aligned with organization's business processes.
- Test inbound and outbound data flow to make sure any improper integration does not lead to inaccurate data flows. Any integration with SaaS should be treated as GAMP category 5, custom-built software and extensively validated.
- Define SOPs and SLAs to ensure timely communication and establish pre-defined timelines for software changes. This

should include a provision for RO to perform impact analysis of the software change and make an informed change approval decision. This can help mitigate risks due to deployment of frequent patches and identify where an organization is not in sync with change control.

- Audit the security framework and conduct additional security testing to avoid data security and confidentiality issues in a multi-tenancy environment.
- Deploy SOPs and SLAs and perform regular audits to monitor compliance with procedures and minimize risks arising from non-adherence to procedural controls.
- Perform an assessment and close gaps in audits trails and electronic signature functional requirements to eliminate non-compliance with Part 11/annex 11 requirements.
- Define and ensure process and operational compliance for compliance with other part 11/annex 11 controls (accurate and complete copies of records, protection of records, limiting system access, operational system checks, authority checks, device checks, policies for accountability, integrity for electronic signatures, password controls, and training)

Organizations also need to assess risks based on the deployment model to help identify the appropriate cloud model that meets security and regulatory requirements.

Conclusion

Cloud technologies are gaining ground in the life sciences and pharmaceutical industry. Several companies are experiencing their benefits, and others aim to determine ways of ensuring compliance while transitioning to the cloud. The absence of a standard risk assessment framework, and disparate deployment models and vendor competencies make cloud adoption complex.

However, there is positive traction for cloud adoption, and CSPs are working to meet industry expectations by ensuring compliance with security and privacy standards. Developing a well-formulated strategy and working closely with CSPs can help life sciences companies accelerate deployment, and maximize returns on their cloud investments, while mitigating risks.

About The Authors

Kavitha Ayalasomayajula

Kavitha Ayalasomayajula is a Domain Consultant with the Pharma IT Solutions and Innovation Group of the Life Sciences unit at TCS. She has been associated with TCS for over 15 years and is a domain expert in IT regulatory compliance for the pharmaceutical industry, including computer system validation, and electronic records and electronic signatures regulations.

Contact Visit TCS' Life Sciences Business unit page for more information

Email: lshcip.pmo@tcs.com

Subscribe to TCS White Papers

TCS.com RSS: http://www.tcs.com/rss_feeds/Pages/feed.aspx?f=w
Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

TCS Design Services I M I 12 I 16