



MOONBAY
TECHNOLOGY



REGULATORY AFFAIRS, CLOUD COMPUTING, AND SECURITY

OVERVIEW

Cloud computing is growing in popularity. Gartner estimates that enterprises will spend \$112 billion cumulatively on software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) combined.¹ The life science industry is finding more uses for cloud computing and SaaS applications. This white paper describes the applicability of cloud computing in regard to SaaS and Regulatory Affairs.

Regulatory Affairs is the vital link between the regulatory agency and the life science company. Regulatory Affairs has the responsibility for assembling information from the company in a format that meets the Agency's requirements for electronic submissions. As the Regulatory Agencies are moving closer to becoming all-electronic, many companies are actively searching for solutions to meet their regulatory electronic submission requirements. SaaS is ideal for Regulatory Affairs because SaaS applications are run on the cloud computing model, meaning the applications are hosted and do not require installation of additional software and servers. End users in Regulatory Affairs can view the submission building process in real time and provide more control over the content that is submitted to the Agency. In addition, Regulatory Affairs can use this cloud-based solution and either build the submission in-house or outsource the submission, and still maintain control over the content and the submission. Cloud computing can reduce the risk of a hardware failure or loss of data during a critical submission.

Security is a concern for Regulatory Affairs utilizing cloud computing because of the company's "crown jewels" or intellectual property managed by the SaaS application and submitted to the Agency. If proactive steps are taken to protect the security, cloud computing can be a useful tool for Regulatory Affairs. In regard to compliance, Regulatory Affairs knows the drug sponsor is ultimately responsible for compliance, regardless of whether the information is managed behind the four walls of the company's facility or within the cloud. Achieving compliance when the company's information is in the cloud could pose challenges and risks to the security of the intellectual property. Data ownership is crucial for life science companies. Is it *clearly* stated in the service level agreement with your Regulatory SaaS provider that the data belongs to the customer? Disasters can take down a data center, resulting in power failures and service disruptions. Does your Regulatory SaaS vendor have procedures for backups and disaster recovery? Finally, cloud computing companies that cannot sustain themselves may go out of business. Business viability is essential when selecting a cloud computing vendor.

¹ Pettey, C., & Tudor, B. (June 22, 2010). "Gartner Says Worldwide Cloud Services Market to Surpass \$68 Billion in 2010." Press release. <http://www.gartner.com/it/page.jsp?id=1389313>



MOONBAY
TECHNOLOGY



SECURITY RISKS FOR CLOUD COMPUTING

Sensitive Information “In the Cloud”

For many life science companies, their “crown jewels” or intellectual property is the essence of their company. Companies in the start-up mode are not generating revenue and many of their key licensing deals are driven by their ownership of intellectual property. If key information is lost, stolen, or breached, it could be devastating to a company. Key information may include manufacturing materials and processes, clinical data, and other research data. Cloud computing could present risk to the security and protection of intellectual property for life science companies if proper steps are not taken to ensure the security of the SaaS application that is run in the cloud. Access to information in the cloud must be well-controlled. End-users that select weak passwords could place an entire company’s documents and information at risk. Finally, access to information could be affected when users get locked out of an account at a very inconvenient time, such as during a presentation or during a major regulatory submission.

Compliance

The customer is ultimately responsible when being investigated by a regulatory authority. The customer must ensure that their cloud computing vendor is qualified and certified. Is the hosting site SAS70 Type II compliant? SAS 70 is defined by Statement on Auditing Standards No. 70: Service Organizations. It is an auditing certification issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) and serves as a way to provide guidance to auditors when assessing internal controls of the service organization.

The cloud computing vendor should understand regulatory compliance and regulatory affairs and have a firm understanding of the current regulations for electronic records and electronic signatures (21 CFR Part 11). Without a basic understanding of compliance and regulations, the customer may be held responsible for the vendor’s inadequacies that are discovered during an inspection or audit.

Data Location and Data Ownership

Because electronic document and data location is outside the four walls of the company, it is important that the customer knows the location of the data center(s). Since cloud computing allows data to become virtualized or moved and stored anywhere in the cloud, customers should know the location of their data. Is the data center in the United States or in a foreign country? It is important for the company to know who “owns” the data. Find out if your data can be held “hostage” by the vendor if there is a dispute over the terms of the agreement. Finally, is the cloud computing environment shared? If so, what is being done to segregate the data?

Disaster Recovery

Cloud computing includes infrastructure that consists of services delivered through data centers, with storage virtualization technology reducing the need for backup tapes and reducing the risk that a natural disaster or a power outage will result in interrupted service. However, hardware can fail, causing interruption in the service provided by your cloud computing vendor. What steps are taken by your vendor for backup and recovery? Are the backup and recovery procedures well



MOONBAY
TECHNOLOGY



documented? Are they available for the customer to evaluate in order to accurately determine if backup and recovery efforts are sufficient in the event of a disruption in service?

Company Viability

In this changing economy, business viability should be carefully taken into consideration when selecting a cloud computing vendor. It is possible that your cloud computing vendor may become acquired by a larger company, as witnessed by several recent deals in the cloud computing space. It is also possible that your vendor could go out of business. Under these circumstances, how would you retrieve your data and documentation? In what form would your data be returned?

RISK MITIGATION FOR CLOUD COMPUTING

Public-vs.-Private Cloud

The intellectual property for life science companies must not be compromised. To protect this valuable asset, companies may opt for a private cloud instead of a public cloud. A “public cloud” exists when the servers, infrastructure, platform, and applications are hosted off-site by a third party, such as a large data center. A “private cloud” offers the same resources but is located within the four walls of the company. A private cloud will offer the same benefits of cloud computing, but with physical security provided by the company. In the event that a user is locked out whether utilizing a private or public cloud model, the company should know who controls access. Access should be controlled by an administrator within the company for a quick turn-around. The company administration must protect access by controlling and maintaining password complexity. Security for life science companies relying on cloud computing can only be as strong as the weakest password.

Compliance

A good place to start when evaluating the regulatory compliance of the cloud computing vendor is to ask for transparency. Ask for certifications and documentation. Ask to review an audit report. Ask the SaaS vendors what steps they have taken to develop their application in compliance with 21 CFR Part 11 Requirements. Ask for training records for the vendor’s system administrators. Ask your cloud computing vendor for validation documentation. If the cloud computing vendor understands regulatory compliance, then it should be willing to provide the necessary information for an auditor to make informed decisions regarding the cloud computing vendor’s compliance.



MOONBAY
TECHNOLOGY



Data Location and Data Ownership

Electronic document and data location in a public cloud poses a level of security risk. Ask the vendor for the exact location of the server. Knowing where the data will be located will help to understand the facility. Perform an audit prior to signing a contract. Ask for appropriate certifications and validation documentation.

Find out how the data is being segregated within the public cloud. Each client should have its own secure database if servers are multi-tenant. Multi-tenancy refers to software architecture where the software runs on a server, serving multiple clients or tenants.

Finally, in order to prevent your cloud vendor from withholding data and information, ask for a provision in the Service Level Agreement (SLA) stating that the data belongs to the customer at all times. This will prevent the customer from being denied accessibility to company-owned data and documentation when issues or conflicts occur between the vendor and the customer.

Disaster Recovery

It is important to ensure business continuity when a failure occurs. Companies should take steps to ensure uninterrupted service. Ask for procedures for disaster recovery. Also ask for their policies and procedures for backing up data. Understand the scheduled backups. Find out how long the cloud vendor will hold the backups. Ask for the power redundancy at the data center and find out the steps that are taken to restore service in the event of a server failure.

All the procedures for power redundancy, disaster recovery, and back up should be well documented and available for the customer to make a determination that business continuity will occur in the event of a service disruption.

Company viability

Taking into consideration business viability of a vendor, make sure that the terms of the SLA are understood. The customer should have clear ownership of the data under any circumstance. The customer should request that the code of the software application be placed in escrow. Having the code in escrow will ensure that the application will be available in the event of a vendor's bankruptcy or acquisition. If the cloud vendor is required to return the data, find out the form in which the data will be returned.

CONCLUSION

Regulatory Affairs can utilize cloud computing to manage documents and electronic submissions. Using cloud computing, Regulatory Affairs can put together information from the company in a format that meets the Agency's requirements for electronic submissions. As the Agency moves closer to all-electronic submissions, solutions can be found in SaaS applications to meet the regulatory e-submission requirements. SaaS applications do not require installation of additional software and/or servers in order to function. Furthermore, users in Regulatory Affairs can view the submission building process in real time and exert more control over the content that is submitted to the Agency. Regulatory Affairs can use the SaaS application as an in-house tool or can decide to outsource the submissions and still maintain control over the content and the submission. Cloud



MOONBAY
TECHNOLOGY



computing applications for Regulatory Affairs provide more control over both the content and submissions.

Security for cloud computing has been shown to be manageable if proactive steps are taken to protect the Intellectual Property of the company, thereby proving that cloud computing can be a useful tool for Regulatory Affairs to meet the company's regulatory milestones. The security risks for Regulatory Affairs using cloud computing applications can be controlled by protecting user access. Compliance can be achieved when the information is managed in the cloud, provided the cloud computing vendor provides transparency with regard to audits and documentation. Data ownership should be clearly stated in the service level agreement with your Regulatory SaaS provider. By requiring your software vendor to put into place procedures for back-up and disaster recovery, the company can ensure business continuity. Finally, ensuring company viability is important when selecting a Regulatory SaaS provider. The steps outlined in this white paper will give the company more confidence when using cloud computing as a tool to manage the needs and requirements of Regulatory Affairs.

ABOUT MOONBAY TECHNOLOGY

Moonbay Technology (MBT) delivers a straightforward, smart, and integrated document management and regulatory publishing system for life science companies. The interface is simple, and implementation and validation are faster than with traditional applications. As a web-based solution, Moonbay Technology reduces the total cost of system ownership. The workflows built into Moonbay Technology's applications follow the general practices of the life science environments. Pipeline RA™ has a company-wide central repository for all documentation and data and knows where and how to obtain and extract the information needed to build regulatory submissions. Pipeline RA™ is a single application covering general document management, regulatory e-publishing, compliance, and clinical management. Moonbay Technology integrates all work functions in the organization and provides a central repository for all data and documentation throughout the product lifecycle. With a single central repository, managing the document life cycle (including review cycles, version control, and audit trails) becomes effortless through automation. Document types based on the current CTD format are defined and included. Furthermore, building electronic submissions for regulatory authorities is a more streamlined and efficient process, resulting in faster milestone achievements. Moonbay Technology's applications are web-based, making an Internet browser the only system requirement. Each application can be personalized to include the client's logo on the user interface. The document types and countries with filed applications are also configurable. Applications are upgraded annually, and each version is fully validated before release. Moonbay Technology will maintain compliance documentation, such as procedures for Installation Qualification (IQ), Operation Qualification (OQ) and Performance Qualification (PQ), disaster recovery, change control, acceptance testing, and system monitoring. Built from the ground up, Moonbay Technology thoroughly understands the life science industry. The company has meticulously included workflows designed for companies with goods in product development and commercialization. Moonbay Technology also understands the financial positions of the many emerging life science companies. Subscription pricing allows early-stage companies to use these applications at any stage of product development.