IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY | an informa business
Unlimited Validation Knowledge Awaits...
Published on *IVT Network* (http://www.ivtnetwork.com)

Validation of Applications in a Cloud

Apr 1, 2015 11:00 pm EDT

Peer Reviewed: Computer Validation

INTRODUCTION

In recent years the industry has been moving into the implementation of systems that reside on a cloud. This has created the challenge in the industry about how to control, validate and ensure data integrity for these systems. Questions have been raised about not having control of the data in the cloud and whether these systems can be validated.

In theory the validation and implementation of cloud-based systems should be more simple and efficient than the traditional approach.

This article will discuss ideas about how to control, implement and validate cloud based systems

WHAT IS THE CLOUD?

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of three service models, and four deployment models.

The three service models include the following:

- Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure
- Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider
- Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software

The four deployment models include the following:

- *Private cloud.* The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise
- *Community cloud.* The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns
- *Public cloud.* The cloud infrastructure is made available to the general public or a large industry group and is owned by

an organization selling cloud services

- *Hybrid cloud*. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

CLOUD DATA & SECURITY DATA CHALLENGE

The biggest challenge related to cloud systems is data integrity and security management. Understanding these challenges is critical to a successful implementation that meets regulatory requirements. Trust and reliability in a cloud environment centers on four core concepts:

- Security – Issues around data integrity and resource access control, encryption and incident detection
- Control – The ability of the enterprise to directly manage how and where data and software is deployed, used and destroyed
- Service-Level Management – The definition, contracting and enforcement of service level agreements between a variety of parties
- Compliance – Conformance with required regulatory, legal and general industry requirements (such as Part 11, Annex 11, HIPAA and Sarbanes-Oxley)

The following security challenges are related to cloud systems:

- Audit/Reporting/Alerting
- Secure Mobile Devices
- Data Security at Rest
- Data Security in Transit
- Strong Authentication
- Personal-business-regulated Data Co-mingled
- Regulated company data – Non regulated company data Co-mingled
- Data segregation

Cloud security issues need to be well understood and mitigated with technical security controls and policies. The following security issues need to have appropriate controls:

- **Abuse and Nefarious Use**:
  Password and Key cracking, Launching dynamic attack points, Hosting malicious data, Botnet command and control, and Building rainbow tables.
- **Insecure Interfaces and APIs**:
  Used for provisioning, management, orchestration, and monitoring.
  Security/availability dependent on security of APIs.
  Weak APIs expose data to variety of security issues.
- **Malicious Insiders**:
  Combo of IT Services, cloud customers, competitors and lack of transparency of security process and procedure practices of Cloud provider.
- **Shared Technology Issues**:
  CPUs, disk partitions, other shared components not designed for strong compartmentalization
- **Data Loss or Leakage**:
  Risk can be amplified due to architectural/operational characteristics of cloud services,inconsistent crypto use, residual data issues, data center reliability, and disaster recovery
- **Account or Service Hijacking**:
  Credentials/passwords reuse, Eavesdrop on connection, Redirect users illegitimate site then launch attack based on your reputation

The risk associated with cloud based systems requires an assessment with a risk mitigation plan. The risk mitigation plan will define the approach for reducing and mitigating risk.

RISK MITIGATION CONSIDERATIONS

Cloud systems security risk requires a mitigation strategy. The following risk mitigation approach should be considered:

- Identification and Assessment of Cloud Components
- Implementation of Controls
- Security & Data Security

Identification and assessment of cloud components should include the following components:

- What components define the configured cloud?
- Where are they?
- How many applications running?
- How many users?
- All GMP or not?
- Hardware and Applications under Change Management?
- How changes are communicated and under control?
- How is data integrity and security provided in the cloud?

The controls needed for cloud-based systems are very similar for traditional implementations. Critical controls and procedures include change management, security, performance monitoring and reporting, and periodic review. The following additional controls need to be implemented to mitigate risk:

- Configuration Management
- Server Management
- Client Management
- Network Management
- Problem Management
- Help Desk
- Backup, Restore, and Archiving
- Disaster Recovery
- Supplier Management

CLOUD SECURITY & DATA INTEGRITY

The security and data integrity of cloud systems is the responsibility of the regulated company. It is critical to understand who has access to the data and whether they need access. Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. The location where the data reside needs to be understood by the customers. Data segregation is critical; data in the cloud typically reside in a shared environment alongside data from other customers. Encryption and segregating others customers from your data is critical for data integrity. Data recovery is another critical component to ensure data integrity using Backup and Restore procedures.

Change management is critical and needs to be clearly defined in service level agreements and vendor and customer procedures. The following aspects should be considered:

- Visibility to changes
- Adequate notification
- Ability to assess changes (depends on the service model)
- Approval of changes prior to release (depends on the service model)
- Testing
- Change impact assessments (technical, GxP, process)

These controls need to be clearly defined in the service level agreements and related procedures.

VALIDATION & QUALIFICATION

The validation of cloud-based systems should be more efficient and simple than traditional implementations of company hosted systems.

One of the critical areas is the supplier assessment. The goal of the assessment is to determine the supplier’s ability to meet clients’ expectations as related to controls needed to ensure security, data integrity, compliance with client procedures, and regulatory expectations. An off-site audit should be considered as the first step to assess cloud computing suppliers. The off-site supplier assessment should be based on a questionnaire that is intended to assess the vendor security, data integrity, and their system life-cycle processes. Off-site audits should be used to determine if the supplier merits further consideration. The responses from the questionnaire should be subject to a risk assessment to determine the need for an on-site audit.

An onsite vendor audit should be used when the intent is to leverage vendor life cycle activities to reduce the validation effort. The scope of the audit should be based on the type of service that will be provided to the customer and whether there is an intent to leverage their lifecycle activities such as testing that can be used instead of qualification.

Service level agreements are critical to define the expectations that the customer and to ensure alignment with regulatory requirement such as Part 11 and Annex11. The following areas should be included in the service level agreements:

- Availability and performance
- Change management
- Quality of service
- Security
- Business continuity / Backup and Recovery
- Personnel Qualification
- Testing
- Incident management
- Defining documentation and information ownership/responsibilities
- Performance monitoring expectations
- Incident reporting
- Alert & escalation procedures

The service level agreements need to have adequate details to communicate clearly to the vendor the customer expectations. Service level agreements need to include requirements that ensure alignment with Part 11 and Annex 11 requirements. This includes the following requirements:

- User access periodic reviews
- Audit trails periodic reviews
- Periodic restoration of backup data
- Archived data checked for accessibility, readability and integrity

The service level agreements need to be very specific about the vendor expectations related to providing the customer the access and information needed to perform the required periodic reviews. Service level agreements need also to define the processes and procedures required including details about the interaction between the customer and vendor.

The validation of cloud-based systems should be based on the risk level of the application. User requirements must be created and provide enough details to ensure that the system selected will meet customer expectations. Installation Qualification should be simple and based on the hardware and software requirements for the system. Vendor installation activities should be leveraged to minimize the level of effort. Operational Qualification activities should be based on the verification critical high risk system functions and should include the following:

- Security & Data Integrity
- Audit trails
- Electronic Signatures
- High & Medium Risk Requirements

Performance Qualification activities should verify workflow and business process requirements.

SUMMARY

Cloud-based applications offer a significant amount of efficiencies and enable fast implementation. Security challenges need to be clearly understood and mitigated. Service-level agreements are critical to communicate to the vendor the customer expectations and to ensure compliance with regulatory requirements such as Part 11 and Annex 11. Vendor life cycle activities such as testing should be leveraged by the customer to reduce the validation effort. In summary, cloud-based systems provide the industry a cost-efficient way for the implementation of GMP application. The validation of these systems should be simple but must ensure that all risk related to security and data integrity are tested and mitigated. Vendor testing document related to security controls such as penetration testing should be leveraged by the customer.

Source URL: http://www.ivtnetwork.com/article/validation-applications-cloud