STANDARD OPERATING PROCEDURE

Selection Process for Cloud Service Providers

Name and Role	Date
Authors: Dr Wolfgang Schumacher Michael Wegmann	01- 01-
Technical Advisory Committee Review: Bob McDowall Yves Samson Dr Andreas Mangel On behalf of the ECA IT Working Group (Cloud Computing Team)	01- 01- 01-
Approved by: Oliver Schmidt ECA	01-

Contents

Document Revision History

Version	Date	Reason for Change	Status
V 1.0		New Document	DRAFT

1.0 PURPOSE

This SOP provides guidance for the selection of cloud service providers. It defines the strategy for cloud service provider selection at <COMPANY> based on patient and product quality risk and criticality of data.

2.0 SCOPE

This SOP will provide guidance on how to select a cloud service provider used to process and store GxP data for <COMPANY> within the GxP areas of <COMPANY>.

3.0 CLOUD SERVICE PROVIDER SELECTION STRATEGY

3.1 INTRODUCTION

Cloud computing is defined by the National Institute of Standards and Technology (NIST) as "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." Further, cloud computing is identified through essential characteristics (e.g. broad network access, rapid elasticity, measured service, on-demand self-service, and resource pooling), service models (e.g. software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS)), and deployment models (e.g. public, private, hybrid, and community).

Drivers for moving to cloud computing include:

1. Increase in business agility and cost efficiency
2. Streamlined IT operations
3. Seamless integration and customization
4. Risk consideration
5. Cost / cost effectiveness

Selection considerations for a cloud service provider should be based on risk, security/privacy, technology, performance, reliability, operational transparency, and compliance to applicable regulatory requirements.

3.2 PROJECT INITIATION

Upon a business case being introduced to move an existing IT system or initiate a new IT system as a cloud computing solution a study would need to be conducted to determine the feasibility of such a project. Information Technology (IT) should lead this effort with the business process owner and Quality Assurance (QA) as participants (as needed).

For a new or existing system the application risk as determined through the Risk Assessment should be used to determine cloud-computing elements needed for the system.

Systems/applications should indicate in the Validation Plan how all criteria as noted in Section 3.2.1 are addressed, depending on its overall risk.

3.2.1 SCOPE & PERFORMANCE

3.2.1.1 Selection criteria to be considered (and as applicable defined in the URS, FS, and Design Specification for each specific system) for the capabilities of a cloud service provider are as follows:

3.2.1.1.1 Technology

- Load balancing
- Virtualization
- Multi-tenancy
- Public, private, or hybrid

3.2.1.1.2 Performance

- Input / output operations per second
- Throughput (either operations or volume per second)
- Utilization
- Latency
- Instance capacity (data storage)
- Connection bandwidth

3.2.1.1.3 Security & Privacy

Data Center Security	
	Hardware security
	Software security
	Web vulnerability scans and reports
	Penetration testing
Data Protection & Compliance	
	Data protection (encryption)
	Backup & Restore
	Data center location
	Data ownership declarations
Network Security	
	Connection security
Reliability	
	Disaster recovery
Trustworthiness	
	Auditing

3.2.1.1.4 Service Level Agreements

- Overall uptime of application/ service

Page-load times

Transaction processing times

Application Programming Interface response times

Reporting response times

Incident resolution times

Incident notification times

3.2.1.1.5 Operational Transparency

Monitoring and operational management

Performance management

Change management

Capacity and license planning, and usage management

Problem management

Service-level management

Service-level data integration

3.2.1.1.6 Incident and Service Management

Support

Contact and Consulting Services

3.2.1.1.7 Service Operations

System Management

Subcontractor Management

Controlling

Reporting and monitoring

De-cloud

3.2.1.1.8 Regulatory Requirements Compliance

21 CFR Part 11

EudraLex Volume 4 Annex 11

Audit and Health Regulatory Inspection support

3.2.1.1.9 Industry Standard Security Compliance

SAS70

ISO27001

Safe Harbor Agreements

3.2.1.1.10 Business Continuity

3.2.2 PROJECT SEQUENCE

3.2.2.1 Define the project

Verify that the IT system to be implemented (or migrated) as a cloud based solution is suitable for the cloud by conducting a feasibility study. Create a Validation Plan which includes the findings of the feasibility study as well as scope of the project, validation documentation for the project, and the validation approach to be used.

3.2.2.2 IT RFP (Request for Proposal)

The Process Owner should create a Request for Proposal (RFP) based on the selection criteria as noted in section 3.2.1.1. The RFP should be submitted to potential cloud service providers to obtain proposals for the project.

3.2.2.3 Bidding Process

Prospective cloud service vendors are to provide a proposal to <COMPANY> based on the RFP. <COMPANY> is to choose top candidates based on the responses from the proposals.

3.2.2.4 Pre-Audit/Assessment Top Candidates

A paper based or on-site pre-audit/assessment may be conducted from the selected top candidates to determine the adherence of the vendor to a formal quality management system and how the vendor deals with SDLC processes (e.g. validation).

Note: The Pre-Audit Questionnaire can be combined with the RFP.

3.2.2.5 Service Provider Selection

Based on the paper based pre-audit responses the Business Process Owner with input from IT and QA will make a recommendation to <COMPANY> management for cloud service provider selection (see section 3.2.2.11).

3.2.2.6 Audit Selected Cloud Service Provider

For projects with High risk a thorough on-site audit would be required and led by QA with IT and the Business Process Owner as participants (as needed).

For projects with Medium and lower risk the paper based pre-audit questionnaire would be sufficient.

3.2.2.7 Identify and Categorize Findings

Findings from the on-site audit for High risk and paper audit for Medium or lower risk cloud service providers are to be documented and categorized.

3.2.2.8 Resolve Critical Findings (if applicable)

Critical findings found during the on-site or paper audit would need to be addressed prior to the implementation of the system. A CAPA is to be opened detailing the critical findings, corrective actions and preventive actions as needed.

3.2.2.9 Implement Controls as needed

Based on the CAPA from the previous section controls are to be implemented to mitigate the risks found of the cloud service provider.

3.2.2.10 Final Disposition Rating

Based on the initial audit and if the findings are resolved or pending a final disposition rating would be assigned to the cloud service provider:

Compliant – no pending critical findings. All findings resolved.

Not Fully Compliant – less than six total critical findings. Two or less critical findings are pending with CAPA. A follow-up audit is to be conducted within six months to determine if all findings are resolved. If all findings are resolved service provider becomes a **Compliant** vendor.

Not Compliant – more than five total critical findings and more than two critical findings pending. An additional audit may be conducted upon request from the cloud service provider within six months of the original audit to verify that pending findings have been resolved.

Note: The cloud service provider would need to implement corrective measures following a Quality Agreement. If a Quality Agreement cannot be put in place with the Cloud Service Provider then management (documented) decision is required on starting/continuation of contract.

3.2.2.11 Final Decision for Use of a Cloud Service Provider

The final decision for use of a cloud service provider for a SaaS based system is to be made by the Business Management, together with the CIO.

3.2.2.12 Performing Ongoing Monitoring and Validation

Based on risk of the system and the vendor establish a frequency to monitor the operations of the cloud service provider.

For validation strategies follow Appendix A or B for recommended testing for respective cloud service models.

For high risk vendors (e.g. Not Fully Compliant disposition) parallel validation may be conducted to mitigate risk. Parallel validation would entail developing and executing User Acceptance Tests concurrently with the vendor to determine the maturity and capabilities of the cloud vendor and the validation status of the application, commensurate with its risk.

3.2.2.13 Periodic Review

The Periodic Review SOP is to be followed to periodically review the cloud based IT system to assure that the cloud based system is maintained in a validated state.

3.2.2.14 Retire Cloud Based IT System

The System Retirement SOP is to be followed upon the need to retire a cloud based system. The service provider is to assist in de-cloud process.

4.0 RESPONSIBILITIES

The role owners should be defined in the corresponding system validation documentation and the corresponding SLA.

Business Process Owner (Vendor Manager / Project Sponsor) is the System Owner and responsible for overall oversight and project coordination of cloud based system vendors.

In addition, they are responsible for managing the vendor and informing IT when vendors are developing / implementing computerized systems for use. The Business Process Owner is responsible for authoring the User Requirements Specification (URS) and ensuring that the system provided by the vendor meets those requirements as well as the business needs of <COMPANY>.

Information Technology (IT) is responsible for technology evaluation support, and may be the reviewer and approver of applicable documentation if there are technology integration with corporate IT systems and infrastructure.

Quality Assurance (QA) is responsible for independent oversight of validation activities and assuring validation meets current regulatory expectations for the cloud based system.

QA is also responsible for vendor audit (paper or on-site) of the cloud based system prior to their acceptance as a vendor for <COMPANY>, as well as during the life-cycle of these vendor systems.

	Business Process Owner	**QA**	**IT**	**Cloud Service Provider**
Vendor Audit	A (Lead Auditor)	I/C	C/R (Audit Team Member)	R (non-signatory collaborator)
User Requirements Specification	R/A	A	C/A	R (non-signatory collaborator)
User Acceptance Test Plan / Test	R/A	A	C	R (non-signatory collaborator)

Cases				
UAT Test Summary Report	R/A	A	C	I
Change Control	R/A	C/A	C	R (non-signatory collaborator)

Legend: R – Responsible (Author), A – Accountable (Approver), C – Consulted (Reviewer), I – Informed

Figure 2: Recommended Document Responsibilities Matrix

5.0 DEFINITIONS

Broad network access: capabilities are available over the network and accessed through standard mechanisms such as mobile phones, laptops, and Personal Digital Assistant (e.g. PDA, iPad).

Cloud Computing: 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 developed and implemented with minimal management effort or supplier (service provider) interaction.

Cloud Infrastructure as a Service (IaaS): the consumer is able to leverage cloud based fundamental computing resources, such as processing, storage, networks, where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications and possibly limited control of select networking components (e.g., host firewalls).

Cloud Platform as a Service (PaaS): the consumer is able to leverage IT infrastructure hosted in the cloud to run applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but still has control over the deployed applications and possibly application hosting environment configurations.

Cloud Software as a Service (SaaS): the consumer is able to use applications running on a cloud infrastructure accessed from various client devices. The consumer does not manage or control the underlying cloud infrastructure or even individual application capabilities with the possible exception of limited user-specific application configuration settings.

De-cloud: the process of leaving a cloud service provider to be able to return to host internally or to use another cloud service provider. One option is to recover the entire virtual infrastructure in its 'native' format, and transfer it 'as-is' internally or to another service provider with the same technology.

If not feasible, then export all of the data to an industry standard data format (e.g. XML, PDF) on durable media. This data would then be migrated into the new provider's environment or internal hosting environment.

Feasibility Study: an analysis of the viability of an idea. It describes a preliminary study undertaken to determine and document a project's viability. The results of this analysis are used in making the decision whether to proceed with the project or not. This analytical tool used during the project planning phase shows how a business would operate under a set of assumption, such as the technology used, the capital needs, and other financial aspects. The study is the first time in a project development process that show whether the project creates a technical and economically feasible concept.

Functional Specification (FS): A document which clearly and precisely defines how the computerized system will satisfy the user requirements and describe the functions in a testable and traceable format.

High Risk Vendor: Defined with a 'Not Fully Compliant disposition'. A high risk vendor would typically be used only if the vendor provides a unique technology which is business critical to the company. If the high risk vendor provides a technology which other cloud providers offer it is recommended to investigate other providers to determine if they would be more suitable (e.g. Compliant disposition).
Measured Service: cloud systems automatically control and optimize resource use by leveraging a metering capability appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

On-demand self-service: the regulated organization (often referred to as a consumer of cloud services) can easily provision computing capabilities, such as server time and network storage, as needed.

Quality Agreement (e.g., Quality Agreement SLA or Statement of Work): A formal agreement between <COMPANY> and the Cloud Service provider defining at a minimum:

- Quality System Requirements
- Audits and Regulatory Contacts
- Personnel and Training
- Change Management
- SDLC Methodology
- Non Conformance and CAPA
- Governance

This is to assure the availability, security, authenticity, and integrity of GxP data for <COMPANY>.

Rapid elasticity: capabilities can be rapidly and elastically provisioned to quickly scale out or in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Recovery Point Objective (RPO): maximum tolerable period in which data might be lost from an IT service due to a major incident

Recovery Time Objective (RTO): targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.

Resource pooling: the provider's computing resources are pooled to serve multiple users using a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned according to

consumer demand. Examples of resources include storage, processing, memory, network bandwidth, and virtual machines, and the user may not know where these are located.

User Requirements Specification (URS): A document which specifies the user requirements for a computerized system and defines its intended use.

6.0 REFERENCES

European Commission Guide Vol. IV, Annex 11: Computerised System, 30 June 2011

FDA 21 CFR Part 11, Electronic Records; Electronic Signatures

GAMP 5, A Risk-Based Approach to Compliant GxP Computerized Systems

The NIST Definition of Cloud Computing, Special Publication 800-145

NIST Cloud Computing Synopsis and Recommendations, Special Publication 800-146

Risk Management SOP

Periodic Review SOP

System Retirement SOP

7.0 APPENDIX

Appendix A - IaaS / PaaS Test Types and Phasing

Appendix B - SaaS Test Types and Phasing

Appendix A

IaaS / PaaS Test Types and Phasing

1. Configuration Verification - Conducted by <COMPANY> as a part of design review, design qualification, and/or infrastructure qualification. Standard designs/builds may be leveraged to minimize the scope of functional testing required.

2. Functional Verification - Conducted by <COMPANY> and to be performed after the infrastructure has been configured and installed. Extensive security verification will be conducted since the infrastructure is in a shared environment. Verification will include both positive and negative challenges. Verification will be conducted only on high risk infrastructure components. The vendor's core qualification is to be leveraged to avoid redundant verification.

3. Performance Verification - Conducted at <COMPANY> after the infrastructure has successfully passed functional verification. Stress/load testing would need to be conducted at usage times. Verification can serve as user acceptance verification.

4. Performance Monitoring - Conducted at the vendor's premises and to be performed after the infrastructure has been released for routine use. Verification would need to include monitoring at peak transaction times and periodic performance review. If the vendor has performed similar monitoring in the past, performance metrics may supplement the performance monitoring verification.

5. Disaster Recovery Testing - Testing is in two parts: the ability of the vendor to recover the infrastructure, and <COMPANY>'s ability to recover the application on the vendor's infrastructure. Leverage vendor's testing and ensure that Service Level Agreement (SLA) allocates responsibilities correctly.

6. Business Continuity Testing - Testing sponsor and supplier ability to resume business to normal under adverse conditions.

Appendix B - SaaS Test Types and Phasing

1. Configuration Verification - Conducted at both the vendor's and <COMPANY>'s premises to ensure that the configured system is capable of meeting <COMPANY>'s specific requirements. May be conducted as part of design review or design qualification or as part of a thorough system demonstration. Vendor's standard configuration documentation may be leveraged to minimize the scope of the configuration verification required.

2. Functional Testing - Conducted by <COMPANY> after the application has been configured and installed, or after the SaaS is provisioned to <COMPANY>. Extensive security testing would need to be conducted since the application is in a shared environment and considered to be an "Open" application. Verification will include both positive and negative challenges. Verification only on GxP significant and/or high risk configured application components. Vendor's core test activities and documentation is to be leveraged to avoid redundant test activities.

3. Performance Testing - Conducted at <COMPANY> after the application has successfully passed functional testing. Stress/load testing would need to be conducted at typical and peak load times. Performance testing can serve as user acceptance verification. It may be possible to leverage the vendor's own performance test

activities and documentation as far as the performance of the core application is concerned, leaving <COMPANY> to focus on network connectivity performance.

4. Performance Monitoring - Conducted at the vendor's premises and to be performed after the application has been released for routine use. Verification could include monitoring at peak transaction times and periodic performance review.

If the vendor has performed similar monitoring in the past, performance metrics may supplement the performance monitoring.

5. Disaster Recovery Testing - Testing the ability of the vendor to recover the infrastructure and the application and data integrity. Recovery testing must comply with <COMPANY> standard RTO and RPO objectives and also defined in user requirements and service contract. Leverage vendor's testing and ensure that SLA allocates responsibilities correctly.

6. Business Continuity Testing - Testing sponsor ability to resume business to normal under adverse conditions.