Focus on Quality

Cloud Computing: How to Choose the Right Cloud Supplier

Advice for laboratories and organizations contemplating using cloud computing, including how to select a suitable cloud supplier for a regulated GxP laboratory — in other words, how to separate the clouds from the clods.

Yves Samson and R.D. McDowall

The introductory sentence from *A Tale of Two Cities,* written in the 19th century, summarizes, from a regulatory compliance perspective, the pros and cons of cloud computing in the 21st century (1):

> "It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness, it was the epoch of belief, it was the epoch of incredulity, it was the season of light, it was the season of darkness, it was the spring of hope, it was the winter of despair."

Cloud computing is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (2). The definition for the noun *clod* is as follows: a lump of earth or clay; a stupid person (often used as a general term of abuse) (3). There are many service providers and hosting companies available that have good quality facilities and provide high service availability, but few are suitable for a regulated GxP environment. Many service providers that are certified for various standards think they can provide a service for a regulated pharmaceutical company, but few can deliver.

Therefore, the purpose of this column is to provide advice to laboratories and organizations contemplating using the cloud and to provide advice on how to select a suitable cloud supplier for a regulated GxP laboratory — in other words, how to separate the clouds from the clods.

Background

In an earlier column installment (4), McDowall discussed the principles of cloud computing. Samson has published his views on cloud computing in two recent articles (5,6), in which he looked at cloud computing in regulated GxP environments, beginning with the basic elements of the types of service models that can be used: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). He then went on to discuss the management aspects of the cloud, regulatory and legal impacts, and approaches to IT infrastructure compliance.

In a recent article, Stokes discussed the following topics regarding cloud computing (7): differences of the cloud compared with traditional in-house IT services, the models of cloud computing, what cloud computing is not, developing a cloud strategy with monitoring, and management of the service providers. One aspect of cloud computing that is an essential part of this strategy is how to get your data back from the cloud if your organization changes its cloud supplier or brings the application back in house (7).

All three authors agree that there are three basic requirements for IT infrastructure operating in a regulated GxP environment that can be located within an organization, outsourced to a third party, or in the cloud (4–7):

- IT infrastructure — physical, virtual, and software elements — must be specified and qualified to show that it works as intended and must be kept under change control throughout the operational life. This is to comply with the specific requirements of the *European Union Good Manufacturing Practices (EU GMP)* Annex 11 that IT in-

frastructure be qualified (8) and the expectation of the pharmaceutical industry as explained in the *Good Automated Manufacturing Practice (GAMP) Good Practice Guide on IT Control and Compliance* (9), of which both the authors of this column were contributors.

- Written procedures must be in place and, when executed, records must show that the activities actually occurred. Records generated in this and the item above must comply with GxP regulations; for example, they must be documented contemporaneously with the activity and allow someone to identify the individual who performed the work and so on.
- Staff operating the infrastructure must be trained in the principles of GxP compliance, especially in change control. This is very important when the apparent business you are contracting with only has a few employees and subcontracts large parts of the work to third parties. This is an area that is fraught with problems for the unaware. In a previous column installment, McDowall looked at quality agreements for the laboratory (10) and the same principles apply to an agreement with a cloud supplier. This comes under the requirements of *EU GMP* Chapter 7 on outsourcing (11).

IT Infrastructure Elements

Before we go much further in this discussion, it is important to understand the scope of IT infrastructure. From the perspective of GAMP, IT infrastructure consists of category 1 infrastructure software (12,13) and category 1 hardware (12).

Category 1 software consists of two types:

- established or commercially available layered software (such as operating systems, databases, and programming languages)
- infrastructure software tools (such as network monitoring software, help desk, backup and recovery software and agents, security software, antivirus software, and configuration management utilities).

The software applications, tools, and utilities are installed on category 1 hardware, which is equated to equipment under the GxP regulations that has to be the appropriate design, adequate size, and suitably located for its intended purpose (14). When these qualified components are integrated together they form the IT infrastructure.

However, care has to be taken with some of the infrastructure tools, such as the help desk, because depending on how the application is used (for example, help desk tickets) it can develop into change control records. In this case, the application needs to be validated because it contains GxP records.

Regulatory Requirements for Cloud Computing

The importance of a secure, efficient, and effective IT infrastructure for pharmaceutical companies should not be underestimated. Pharmaceutical companies have a global supply chain and global research and development of which large elements are outsourced to third parties for which electronic data storage, processing, and communication is essential. Therefore, it is a primary business requirement that data stored in the network are secure because the network will contain:

- proprietary information supporting product licences and registration
- patient records from clinical studies
- batch records for product release
- stability data for products on the market.

Some of these data must be stored 5–50 or more years and be retrieved when required during an inspection or after a complaint. Pharmaceutical companies must comply with applicable GxP regulations and ensure that key data remain complete, accessible, and readable over decades without jeopardizing their integrity.

The problem is that third-party IT companies can work to ISO 27001, IT Infrastructure Library from British Standards (ITIL, www.bsi-global.com), Control Objectives for information and Related Technology (COBIT, www.iseca.org), or another IT quality framework, but do not consider or even understand that specific GxP requirements apply for pharmaceutical companies as discussed below.

IT Infrastructure Qualification

The basic element of a computerized system is the IT infrastructure that allows any application to run on it. Although it has been a regulatory expectation since the mid-1990s, qualification of IT infrastructure has been a regulatory requirement since only 2011 with the issue of the new version of *EU GMP* Annex 11 on computerized systems (8). In the "Principle of the Annex" it states simply: "The application should be validated; IT infrastructure should be qualified." Therefore, regardless of where the IT infrastructure is located — in-house, out-sourced to the ends of the globe, or in the cloud — the infrastructure must be qualified to run GxP applications. Furthermore, one of the prime requirements when selecting a cloud provider is to ensure that both the underlying physical infrastructure and the virtual environments created on it are qualified and kept under control.

What do we mean by *qualified* and *kept under control*?

Qualification is defined in the *EU GMP* glossary as the action of proving that any equipment works correctly and actually leads to the expected results (15). Implicit in this definition is that there must be a definition of what the equipment is supposed to do, so that when it is tested the results can be compared with the specification. When the results are compared with what is expected and they match, then the equipment is considered qualified. However, we also need to consider what the word *control* means.

Control means that there are procedures in place for carrying out work and as a result of executing these procedures records are created that can be reviewed, audited, or inspected at a later date. These procedures, including the qualification documents, must be preapproved before execution and reviewed after it. As noted above, staff members must also be trained in awareness of the applicable GxP regulations because they impact the work within the IT infrastructure. This

requirement includes subcontracted staff.

Service Providers: Requirements for Audits and Agreements

There are also further requirements that impact a cloud computing solution. *EU GMP* Annex 11, section 3.1 states (8):

> When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerized system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT departments should be considered analogous.

Put simply, there must be an agreement between the IT service provider, such as a hosting company, and the regulated user (that is, the pharmaceutical company, contract manufacturer, contract research laboratory, or clinical research organization). This agreement must cover the roles and responsibilities of the people involved and the services offered.

However before the pens hit the paper, there is a more important consideration that must be taken into account. Do we audit the cloud provider? Annex 11 provides some guidance in this respect.

- Clause 1 states that risk management should be applied throughout the lifecycle of the computerized system and take into account patient safety, data integrity, and product quality (8).
- More specifically, clause 3.2 states that the competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment (8).
- However, the audit reports must be shown to an inspector on request as noted in clause 3.4: "Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request" (8).

Therefore, from a regulatory perspective, have you done demonstrable due diligence? This expected due diligence should not be considered only from a regulatory point of view but also a business perspective, because in many cases the decision to move to a cloud-based solution will affect many types of data, such as GxP-relevant data and knowledge-related data as well. Table I shows further good manufacturing practices (GMP) related requirements ,such as 21 *CFR* 11 (16) for IT infrastructure, that need to be considered as part of an initial audit and included in the agreement between you and the hosting provider.

Although it may seem relatively easy to audit an active pharmaceutical ingredient (API) or a contract manufacturer, providing objective evidence with a reasonable degree of assurance that a cloud service provider is delivering a compliant, reliable, and secure service can often be a real challenge. This point will be developed further in this article.

Table I: Additional 21 *CFR* 11 and Annex 11 regulations applicable to IT infrastructure

Annex 11 Requirements for IT Infrastructure	21 *CFR* 11 Requirements for IT Infrastructure
• Staff and training records (Annex 11 item 2): qualifications and CVs / resumes • Training records including initial and on-going GxP awareness and competence • Security (Annex 11 items 7.1 and 12) • Backup and recovery (Annex 11 item 7.2) • Change control and configuration management (Annex 11 item 10) • Periodic evaluation (Annex 11 item 11) • User account management (Annex 11 item 12) • Incident management (Annex 11 item 13) documented and linked to CAPA	• GxP predicate rule requirements, for example: qualifications and CVs, resumes of staff • Training records including initial and regular ongoing GxP awareness and competence • 11.10(b) Generate accurate and complete copies of records • 11.10(c) Protection of records • 11.10(d) Limiting access to authorized individuals • 11.10 (e) Time stamped (audit trails)

Legal Requirements

In addition to GxP regulations on the IT infrastructure there may also be legal requirements to consider; these affect three main areas of a pharmaceutical company:

- data privacy
- intellectual property
- physical location of the server.

Data Privacy

When considering moving data to external cloud-based solutions a company should be aware that the data stored in the cloud are implicitly available to and readable by a third party, such as the United States' National Security Agency (NSA). Furthermore, if a pharmaceutical company wants to store patient-related data, there are mandatory confidentiality requirements that must be followed; therefore the decision to work with a cloud service provider must be taken carefully.

There is also the European Directive 95/46/EC (17) on the protection of personal data to consider. The United States developed the Safe Harbor agreement (18), which is intended to be compliant with the European directive. Unfortunately, the NSA has got around this agreement using PRISM (a clandestine mass electronic surveillance data mining program). Also, the United States Patriot Act (19) requires a service provider to hand over data to the United States government without requiring a court order or even informing the data owner.

Intellectual Property

Moving to a company's external cloud-based solution implies that data confidentiality will be more limited than for data stored internally, as long as the company maintains a reasonable level of information security.

During the last 25 years, several companies have had bad — sometimes fatal — experiences in cases of disregarded nondisclosure agreements. These troubles were possible because

Table II: GxP and legal considerations for cloud computing

Area	Key Questions
GxP requirements	• What GxP constraints apply to the data stored in an external cloud? • For good clinical practice (GCP) requirements, in particular, are these constraints compatible with the legal requirements applying to a company external cloud?
Legal requirements	• What laws apply to the data stored in a company's external cloud? • What are the applicable legal constraints in case of litigation?
Knowledge management	• How business critical are the data that may be stored on a company's external cloud? • Could the future business development of the company be significantly jeopardized if the stored data were accessed by an unauthorized person?

Table III: Key areas and criteria for auditing IT hosting providers (excluding the quality management system)

Area for Audit	Criteria
Data integrity maintained throughout record retention period	• Data confidentiality • Data security • Access control and user management • Data retention measures
Legal requirements placed on data stored in infrastructure	• Intellectual property claims • Patriot Act requirements and Safe Harbor agreements
Qualified infrastructure	• Correctly designed and specified infrastructure • Correctly installed infrastructure • Verified operation • Qualified infrastructure applications • Authored and approved specifications and designs • Installation plans and records • Component verified and tested to show correct operation versus the specification • Where appropriate, integration testing to the rest of the infrastructure • All infrastructure applications qualified — for example, network management software
Data management	• Backup and restore processes • Business continuity and disaster recovery • Archiving
Change management	• Does the change-control procedure involve the data owner for changes to infrastructure? • Does the change-control procedure involve the data owner for changes made to the system and application?
GxP knowledge	• Does the service provider know the regulations and the need for records of activities? • Regulations require an appropriate combination of education, training, and experience • Knowledge of GxP regulations to enable them to perform their job • There must be regular GxP update training (typically annually) • Formal training materials with assessment of competence
Quality assurance oversight of IT activities is essential	• Knowledge of individual • Quality assurance regulatory requirements • Sufficient technical knowledge of IT infrastructure • Individuals can be either: business QA with appropriate technical knowledge or regulatory compliance within IT

such agreements cannot supersede the local law. If intellectual property is weakly protected in a specific country, no nondisclosure agreement can improve the situation. This specific scenario applies in the case of cloud-based systems located in such countries too.

Physical Location of the Server

Although any system running in the cloud will be virtualized, the problem is in where the system is physically located. From a GxP perspective this information is very important because the data contained in a system could be subject to impounding or sequestration by a regulatory agency.

Additionally, in case of litigation, it can be necessary to identify clearly where — at which location — data are stored and to ensure that local authorities can have access to the data or that data sequestration can be directly performed.

Summary of GxP and Legal Requirements

Making a long story short, the applicable constraints and requirements should be considered on several levels, as shown in Table II. It should be clear that today no state, either in the Americas, Europe, or in other regions, can provide warranty that, from a legal point of view, data stored into a company external cloud will remain confidential without any unauthorized access by a third party.

Auditing a Cloud Provider

With the exception of the rare cases of cloud service providers dedicated to the pharmaceutical industry or to the related services, auditing a cloud service provider could represent a real challenge. Whereas the regulated user is focused on a middle-to-long term approach, relying on some certainty, a typical cloud service organization will act with agility, not specifically related to locations, often with rapidly changing personnel, and focused on a best effort approach. However, ensuring data integrity, accessibility, readability, and confidentiality requires some formal processes and controls that need to be verified during an audit.

Audit Objectives

When auditing a cloud service provider, it is important not to lose sight of

the main objective, which is to generate the confidence in the working capability and accuracy.

The review of the service provider's quality management system (QMS) and the necessary openness and transparency during this review help to build the confidence for the future customer-provider relationship.

However, because no organization is perfect, usually the audit will offer the following outcomes:

- Provide rational evidence for confidence.
- Address areas of concerns, with related corrective measures (action plan).

If the audited organization accepts the audit findings and agrees to modify their approach through implementing appropriate corrective and improvement measures, an audit can make sense for securing a future collaboration. Via this key topic, the clods can be segregated from the clouds.

What Are We Auditing Against?

Based on the above explanations, Table III provides an overview of the main audit areas to be considered.

Table IV: Regulatory requirements for staff training

Regulation	Regulatory Requirement
US GMP: 21 *CFR* 211.25(a)	• Training shall be in the particular operations that the employee performs and in current good manufacturing practice (cGMP) (including the current good manufacturing practice regulations in this chapter and written procedures required by these regulations) as they relate to the employee's functions. • Training in current good manufacturing practice shall be conducted by qualified individuals on a continuing basis and with sufficient frequency to assure that employees remain familiar with cGMP requirements applicable to them.
US GLP: 21 *CFR* 58.29	(a) Each individual engaged in the conduct of or responsible for the supervision of a nonclinical laboratory study shall have education, training, and experience, or a combination thereof, to enable that individual to perform the assigned functions. (b) Each testing facility shall maintain a current summary of training and experience and job description for each individual engaged in or supervising the conduct of a nonclinical laboratory study.
US GMP: 21 *CFR* 11.10(i)	• Determination that persons who develop, maintain, or use electronic record or electronic signature systems have the education, training, and experience to perform their assigned tasks.
EU GMP: Annex 11, Clause 2 Personnel	• There should be close co-operation between all relevant personnel such as process owner, system owner, qualified persons, and IT. • All personnel should have appropriate qualifications, level of access, and defined responsibilities to carry out their assigned duties.

Does ISO 27001 Certification Provide Compliance with GxP Regulations?

Quality standard and certifications should be leveraged within the specific context of GxP, because they represent — at least partially — a significant and reliable basement for the required good practices and regulated processes. The QMS of an IT hosting company can be certified to one or more quality standards such as

- ISO 27001 (20)
- Control objectives for IT (COBIT) (21)
- eSourcing capability model for service providers (eSCM-SP) (22)
- Payment card industry (PCI) or other financial industry regulations

Please note: Such quality standards and certifications cannot replace GxP regulations, which are mandatory requirements for a regulated user. This is not the place to agree or disagree with the GxP regulatory requirements; they have to be followed. The unique question is "How can a cloud solution be compliant with the GxP regulatory requirements?"

Pharmaceutical auditors assessing cloud service providers need to know and understand the main IT quality standards above to avoid useless redundancies during audits and assessments. Understanding the content and focus of such quality standards and certifications makes it possible to focus an audit on the areas of GxP requirements and procedures that are not really covered by the certification controls. For example, GxP training as well as GxP documentation skills as directed by the regulations will need to be addressed appropriately by any potential service provider. A simple summary of the required approach for a service provider can be summarized as:

- Say what you do: have a written procedure that staff are trained to follow
- Do what you say: follow the procedure — always or document the rational for departing from it
- Document it: have records to show that the procedure was followed

Particular attention should be given to the eSourcing capability model (eSCM) (22) because it covers both parties involved in an agreement:

- Service provider: eSCM-SP
- Client or customer: eSCM-CL

eSCM acknowledges that the conditions for a good, efficient, and compliant service delivery requires that both the service provider and client define and implement a consistent quality management approach. For this reason, auditing only the service provider based on eSCM-SP without auditing the regulated user (client) based on eSCM-CL is useless because such an approach would be inconsistent. That would be a novel approach for any GxP laboratory because usually the audits are one sided.

Ways of Auditing a Supplier

Given the fact that IT infrastructure is critical for any pharmaceutical company, it is surprising that many decisions are based on financial considerations. One reason for this is that IT generally reports through the finance group of an organiza-

Table V: Audit findings with the hosting company responses	
Audit Finding	**Company Response**
Installation qualification documents are not preapproved before execution.	Believes this is an inappropriate application of the GAMP standard, and also that the standard has been misinterpreted in this case.
IQ/OQ documents are not executed against equipment specifications to demonstrate fitness for intended use.	Product delivers qualified hardware and so this is beyond the scope of the product.
There is no specification and associated qualification testing, with associated quality assurance oversight, of the hypervisor layer	Acknowledged. A plan will be placed to qualify the hypervisor
GxP awareness training was only given to staff working greater than 80 h per year on the qualified infrastructure	Considers that only staff working for longer than 80 h on the infrastructure should be trained in GxP compliance.
Qualification documents are electronically signed in an EDMS. The electronic signatures are not compliant with the requirements of §11.50.	Utilizes EDMS as the predominant repository of documentation and the deployment of EDMS is considered fit for purpose across our client base. Utilization of a different document repository or amendment of its deployment is out of the scope of the product.
The EDMS was incompletely validated by the vendor of the software as only two test cases, both designed to pass, were found in the validation documents. There were no test cases for security, audit trail or other part 11 functions.	Considers this system adequately validated

tion. However, it is important that IT infrastructure, regardless of how it is delivered, provides a reliable and compliant service. From the perspective of a user much of this is hidden from view: Your workstation is plugged into a socket in the wall and as long as the required services are provided are you really worried about what happens at the end of the cable? You assume that IT is under control. Is this a valid assumption? Remember that the process owner (sometimes called the system owner) is the one responsible for the data generated that will be managed and supported by the IT infrastructure and systems. Hmmmm, what should we do?

So if you are outsourcing your IT services and infrastructure, sufficient due diligence needs to be performed to assure you that the service provider knows their job, follows written procedures, produces records, and has appropriately trained staff including all people who are subcontracted by the service provider. There are three basic options for auditing a supplier, including a cloud service provider:

- Questionnaire only
- Questionnaire plus follow up teleconference and review of documents
- Questionnaire plus on-site audit and verification of answers

We will consider the advantages and disadvantages of each approach.

Questionnaire

This is the option that is the quickest to perform, but leaves you with the least confidence in the supplier. You are reliant on the supplier being honest and truthful when it completes the questionnaire. Therefore, you must ensure that the questions asked are searching and, where appropriate, request supporting information such as a list of procedures or specifications and evidence of action for the qualification of a server.

When the completed questionnaire is received it needs to be reviewed and assessed and not thrown in a draw and forgotten. Are the answers acceptable or do you need to ask the company for clarification? In the end, you need to make a decision whether to use this supplier or not and the reasons for this should be documented in a summary report.

Questionnaire Plus Follow Up

The next option for supplier assessment is to send the questionnaire and review the completed document as outlined above. The next task is to organize a web session or teleconference to review the answers and ask follow-up questions in addition to reviewing documents. This addition to the questionnaire gives a laboratory an opportunity to go into more detail and verify the answers in the questionnaire. Topic areas can be discussed in detail and approaches to compliance confirmed. One specific issue is the ability to see and check documentation that has not been provided in the questionnaire around the infrastructure: some companies cite "intellectual property" reasons for refusing to disclose any design documentation. If this happens, you are presented with a very simple question: Have you identified a clod?

Questionnaire Plus On-Site Audit

The questionnaire is completed and reviewed as in the last two instances; in this option there is an on-site audit of the hosting facility or data center and the company offices. Note here that the audit may be in two parts because the hosting facility may not be in the same location as the offices. In fact, they could be in a different country. The dates of the visit need to be planned and the schedule agreed on, including time to move between buildings if needed. The offices will look at the quality management system including staff organization charts and training records, scope of accreditation — typically for ISO 27001 (20) — and procedures with records of activities occurring. Key areas to spend time reviewing during the audit are the organization chart and the staff training records.

- The organization chart should show where subcontracted staff are used. This is important for a number of reasons. Is there an agreement in place between the service provider and the subcontracted organization detailing roles and responsibilities?
- Training records, resumes or curricula vitae, and position descriptions

for service provider staff including subcontractors must be reviewed to determine if they have a combination of education, training, and experience. A problem with ISO standards is that they do not require current resumes or curricula vitae that are required for the pharmaceutical industry.

- A specific GMP requirement of US GMP and good laboratory practices (GLP) in §211.25(a) (14), GLP in §58.29 [Ref 23], Part 11 in §11.10(i) (16), and *EU GMP* Annex 11 clause 2 (8) as shown in Table IV. Therefore, you must determine if there is sufficient GxP awareness training for the staff of your potential service provider, including any subcontracted personnel. If GxP training was given, then who was the trainer and what were their qualifications, training, or experience to give it? Failure to understand and probe here can have serious compliance problems later.

Table VI: Topics to address in a service-level agreement

Service-Level Agreement Content	
Service Delivery*	**Controls and Accountability**
• List of relevant (applicable) regulations and rules (policies) • Specification and qualification of virtual infrastructure items • Change-control procedure including regulated user sign off for major changes • Handling usage queries and questions • Fault reporting and response, including feedback processes • Prioritization of faults • Escalation process • Providing work-arounds • Software patching • Installation of software upgrades • Resolution and closure • Maintenance of spares and consumables • Software and data backup and recovery • System management, administration, and housekeeping • Support of underlying hardware and infrastructure • Software tools to be used • Routine testing	• Controls — that is, procedures and records of activities • Availability of all documents for an audit or inspection • Quality of service, quality attributes (acceptance criteria) • Time to resolve issues before escalation • Corrective and preventive measures • Underpinning contracts • Roles and responsibilities: - IT supplier - Regulated user • Right of audit by regulated user • Right to audit by you • Commercial terms including end of contract terms and access to your data if company fails • Exit conditions from the contract including transfer of regulated user data and records

*According to appendix O2 (12).

How to Select an IT Service Provider

In this section we use our experience to help you navigate the cloudy waters of service providers and select an adequate one. Specifically, we provide examples of responses from questionnaires and examples of on-site audits. Many hosting providers have ISO 27001 accreditation, but how many have the requisite GxP knowledge and training to be a suitable hosting provider for regulated healthcare organizations? The process to separate the clouds from the clods is shown in Figure 1 and consists of three stages.

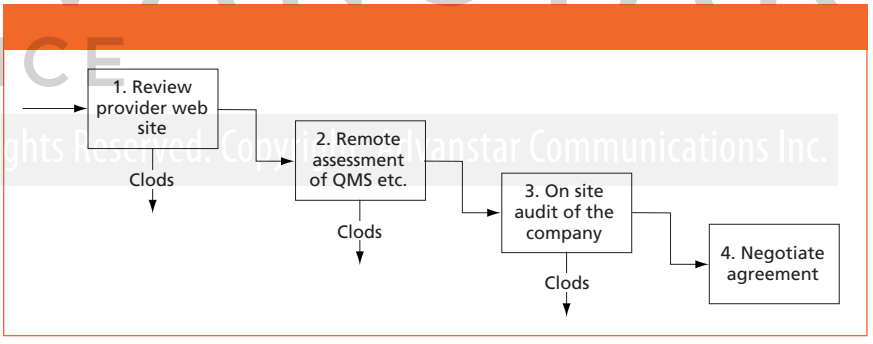

Figure 1: Process flow to help select an adequate cloud service provider.

Stage 1: Review Provider Web Sites

The first stage of the assessment process is a remote assessment of each potential hosting provider, which is achieved by looking on their web site. What you are looking for is information about their customers and knowledge of GxP regulations for the pharmaceutical system. Specifically,

- Does the company know about the GxP regulations?
- Is their infrastructure qualified and can they provide a GxP-compliant service?
- Do they have any regulated pharmaceutical customers?

If the answers are no, you have identified the clods and no further action is required. The potential clouds then move to stage 2 of the process.

Case Study Example

A web site search of about 20 web sites identified five potential hosting companies worthy of further consideration.

Stage 2: Remote Assessment of the Quality Management System

The remaining candidates are then sent a detailed questionnaire that asks questions about their accreditation schemes and their QMS such as quality manual, procedures, infrastructure qualification, and staff training and knowledge of GxP regulations. Some potential service providers may state that because they are certified against a specific standard such as ISO 27001 that this is acceptable to the pharmaceutical industry. However, ISO 27001 cannot ensure compliance with pharmaceutical industry regulations as there are gaps, as you have seen from the earlier sections in this column. Therefore, you need to ask specific questions to assess the hosting com-

Table VII: Types of agreements between a regulated user and a service provider	
Agreement Type	**Definition**
Definitions – service-level agreement (SLA) versus operation-level agreement (OLA)	• An SLA is an agreement or treaty between a service provider (IT) and the customer who is paying for the service. • An OLA is an agreement made between the service provider of an organization and another functional body of the same organization.
SLA	• An SLA is legally binding whereas an OLA is a best-effort agreement within an IT Infrastructure that defines the relationship among the internal support groups of an organization working to support the SLA.
OLA	• An OLA is an outcome of a particular SLA. After the SLA is agreed upon, the IT organization conducts sessions to find out what can fit an OLA to enable it to deliver the specified service.
Underlying contract (UC)	• Contract between the IT service provider and a third party to help the service provider deliver agreed services to a regulated customer.

pany's knowledge of pharmaceutical specific regulations:

- Question: Are specific controls in place for closed systems (that is, availability and protection of records, audit trails, sequencing, access, training, documentation, and change control)?
- Answer: 21 *CFR* Part 11 compliance is the responsibility of the customer on a solution-specific basis.

Clod alert! This is an interesting answer to a key question because it demonstrates no understanding of the Part 11 regulation or its interaction with the applicable predicate rule. Therefore, the company should be rejected without any further consideration.

- Question: How do you qualify a server? This question should also request evidence of the server specification and the execution of the installation.
- Answer: These documents are confidential and are not disclosed to customers.

This answer to this question means that you have identified another clod and that the company must be rejected. Any service provider is acting as your agent, but you are still responsible for their work. The qualification of a server is important and the documentation of the process needs to be available during the supplier qualification and for any inspection. We strongly recommend that the availability of any such material should be documented in any agreement between you and the company.

You also need to focus on asking questions around backup and recovery, change control, and configuration and incident management in the questionnaire to check that these functions are carried out in a compliant way.

Case Study Example

The five hosting companies were sent and returned questionnaires. Three companies were rejected because they responded with some of the examples cited above.

Stage 3: On-Site Audit of the Service Provider

In our view, this stage is essential if GxP-critical systems are being hosted externally to the laboratory or the parent organization and are also in compliance with Annex 11 clause 3.2 (8) because you may only be allowed to view some key documents at the supplier's site. This stage gives you much more detail and knowledge about a supplier than a questionnaire can ever provide. You should cover

- Details of the quality policy, quality manual, and procedures: Look at the services offered by the company within the QMS and how these are documented. For example, building and qualifying the physical infrastructure upon which the virtual systems will be installed; building and qualifying virtual infrastructure components and their integration; operating the infrastructure: both physical and virtual elements; change control processes for physical and virtual infrastructure including the records associated with a sample of change requests — some of these may require requalification of a component. Throughout this process you will be looking to see that records are created according to GxP principles.
- Data center facilities: Many hosting companies may not build their own ISO 27001-certified facility but may hire space in one. Therefore, you need to understand where your virtual server is located in case of seizure and so on.

Case Study Example:

The remaining two hosting companies were ranked with one as the preferred candidate for an on-site audit and the other held in reserve. Both companies claimed to have qualified IT infrastructure from the returned questionnaires plus any clarification questions. We will look at the audit findings from the preferred candidate together with the responses as shown in Table V. Although the company claimed compliance you will note that installation qualification and operational qualification documents are executed without approvals and that staff members that are untrained in GxP awareness are let loose to work on the infrastructure until they have clocked up 80 h. Not an appealing thought. Is this provider classified as cloud or clod?

As a result of this audit, the preferred supplier was rejected and the reserve supplier was audited. The audit was satisfactory and confirmed qualified infrastructure, GxP-compliant procedures and records, and adequately trained staff including GxP awareness training. They moved to the next stage in the process — the agreement.

What Do We Need in an Agreement?

In every business relationship, contracts are necessary, especially as we have noted under *EU GMP* Chapter

7 on outsourcing (11). A service-level agreement (SLA) is at first a contract between the user organization and a service provider, in this case a cloud or hosting company. *EU GMP* Annex 11, section 3.1 (8) has been extensively quoted earlier in this article, setting the conditions for a formal collaboration between a regulated organization and third parties.

To be efficient and useful, an SLA should address some or all of the topics shown in Table VI depending on the type of service required such as IaaS or PaaS. The different types of agreements and contracts are shown in Table VII.

Occasionally there may be the need for an underlying contract (UC), which is a contract between an IT service provider and a third party. The third party provides goods or services that support delivery of an IT service to a customer. The UC defines targets and responsibilities that are required to meet agreed service-level targets in an SLA (22). Such contracts should be clearly identified by elaborating a SLA or operation-level agreement (OLA) because they finally impact the real scope of responsibilities as well as the possible access to the data of the regulated user. It is also important that the GxP knowledge and procedures are sufficient within the third party of the UC.

Contract Management: How to Write a Contract?

Before any contract can be established, the service provider's QMS and the associated activities must have been audited and the audit results must be considered as acceptable. This allows the focus to shift from equipment qualification, which is covered by the QMS, to service delivery, which will be covered at first by the contract.

However, the definition of a service or operation contract requires expertise and a consistent approach. Failing to use the following recommendations can have fatal consequences for the service delivery and, in particular, for the service compliance. Successful contract management requires the following approach:

- Be careful.
- Be accurate.
- Be precise.
- Be as exhaustive as necessary.
- When reviewing agreements, be "critical;" keep your eyes open; avoid any assumptions and implicit (not formalized) requirements.

Contract management is a very specific activity with a major legal impact. For this reason, you should not hesitate to obtain the support of an IT lawyer. Large and global organizations try (and succeed) to establish service delivery based on ambiguous and contradictory terms of service. Long and small written contracts with multiple and complex clauses put the layman in an unbearable position.

Particular attention must be given to the exit conditions and break points in the contract. Such conditions are very critical in terms of business capability and business continuity. The most appropriate moment for negotiating safe and acceptable exit conditions is before signing the first contract and before storing the first data in the cloud. The honeymoon period before the contract is signed and any money has changed hands is the best time to negotiate these items.

Summary

Selecting a cloud service supplier that qualifies the IT infrastructure, knows the GxP regulations, and trains its staff in GxP awareness is critical for any pharmaceutical laboratory and its parent organization. Controlled and qualified IT infrastructure is the foundation of all quality work using computerized systems. Auditing the supplier and finding out how they understand and apply applicable regulations is critical before signing any contract. This allows expensive mistakes to be avoided and issues to be corrected before using a cloud service provider.

References

(1) C. Dickens, *A Tale of Two Cities* (Chapman & Hall, London, 1859).

(2) P. Mell and T. Grance, *The NIST Definition of Cloud Computing, NIST Special Publication 800-145* (National Institute of Standards and Technology, Gaithersburg, Maryland, 2011).

(3) *Shorter Oxford English Dictionary* (Oxford University Press, Oxford, 1988).

(4) R.D. McDowall, *Spectroscopy* **27**(4), 22–29 (2012).

(5) Y. Samson, *GMP Journal* Issue 9 October/November, 10–12 (2012).

(6) Y. Samson, *GMP Journal* Issue 10 April/May, 13–15 (2013).

(7) D. Stokes, *Pharm. Eng.* **33**(4), 1–11 (2013).

(8) European Commission Health and Consumers Directorate-General, *EudraLex: The Rules Governing Medicinal Products in the European Union. Volume 4, Good Manufacturing Practice Medicinal Products for Human and Veterinary Use. Annex 11: Computerised Systems* (Brussels, Belgium, 2010).

(9) ISPE, *Good Automated Manufacturing Guide (GAMP), Good Practice Guide: IT Control and Compliance* (International Society of Pharmaceutical Engineering, Tampa Florida, 2005).

(10) R.D. McDowall, *Spectroscopy* **28**(9), 28–35 (2013).

(11) European Commission Health and Consumers Directorate-General, *EudraLex: The Rules Governing Medicinal Products in the European Union. Chapter 7, Outsourced Activities*, (Brussels, Belgium, 2013).

(12) ISPE, *Good Automated Manufacturing Guide (GAMP), version 5* (International Society of Pharmaceutical Engineering, Tampa Florida, 2008).

(13) R.D. McDowall, *Spectroscopy* **24**(6), 22–31 (2009).

(14) Current Good Manufacturing Practice for Finished Pharmaceutical Products, in 21 *CFR* 211 (U.S. Government Printing Office, Washington, D.C., 2009).

(15) European Commission Health and Consumers Directorate-General, *EudraLex: The Rules Governing Medicinal Products in the European Union. Glossary* (Brussels, Belgium, 2010).

(16) Electronic Records; Electronic Signatures Final Rule, in 21 *CFR* 211 (U.S. Government Printing Office, Washington, D.C.,1997).

(17) European Directive 95/46/EU, "Protection of individuals with regard to the processing of personal data and

on the free movement of such data," European Commission (1995).
(18) Safe Harbor, US Department of Commerce, www.export.gov/safeharbor/.
(19) Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Public Law 107-56, 107th Cong. (26 October 2001).
(20) ISO/IEC 27001: 2013, Information technology— Security techniques — Information security management systems — Requirements (International Standards Organisation, Geneva, 2013).
(21) COBIT 5 (Control Objectives for Information and Related Technology) version 5 (Information Systems Audit and Control Association, 2012).
(22) eSourcing Capability Models (eSCM-SP for service providers and eSCM-CL for client organisations); see http://www.itsqc.org.
(23) Good Laboratory Practice for Non-clinical Studies in 21 *CFR* 58 (U.S. Government Printing Office, Washington, D.C., 1978).

R.D. McDowall is the Principal of McDowall Consulting and the director of R.D. McDowall Limited, and the editor of the "Questions of Quality" column for *LCGC Europe*, *Spectroscopy*'s sister magazine. Direct correspondence to: spectroscopyedit@advanstar.com

Yves Samson is the founder and director of the consulting firm Kereon AG located in Basel, Switzerland. He has more than 20 years of experience validating GxP computer systems and IT infrastructure qualification. He is editor of the French version of GAMP 4 and GAMP 5 and he translated the PIC/S Guide PI-011 into French.

For more information on this topic, please visit our homepage at: www.spectroscopyonline.com/mcdowall