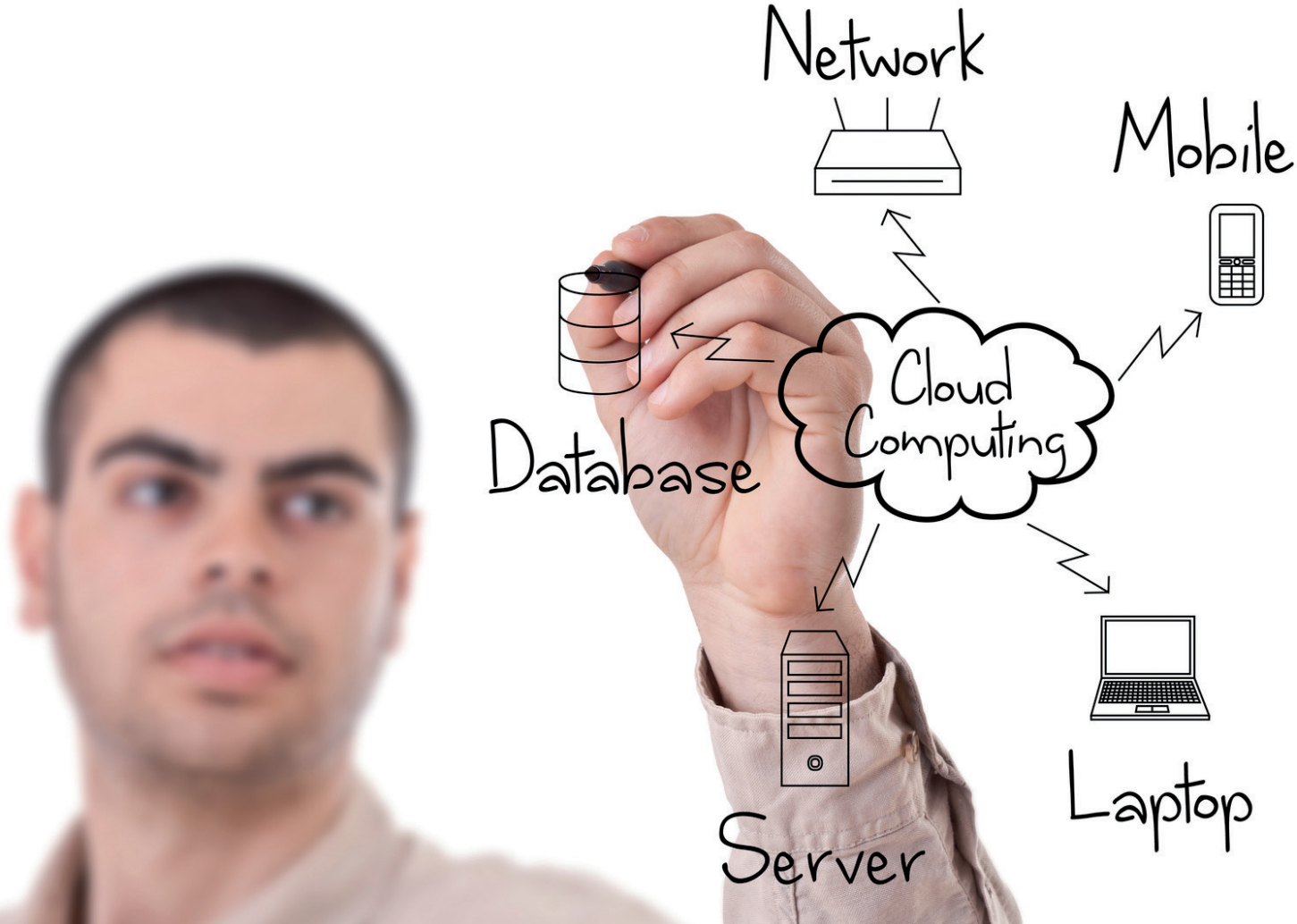
GMP Journal
The Journal for GMP and Regulatory Affairs

CLOUD COMPUTING FOR REGULATED GXP ENVIRONMENTS



ECA
European Compliance Academy

Consequences for European healthcare industries

European Computer Validation Conference

First experiences with Annex 11

4 - 5 June 2013, Barcelona, Spain

SPEAKERS

FROM AUTHORITIES:

KLAUS EICHMÜLLER
Regierung von Oberbayern
Munich

DR CHRISTA FÄRBER
Staatl. Gewerbeaufsichtsamt,
Hannover

KARL-HEINZ MENGES
Regierungspräsidium
Darmstadt

KNUD RYHL
Danish Medicines Agency

AUDNY STENBRÅTEN
Norwegian Medicines Agency

FROM INDUSTRY:

FRANK BEHNISCH
CSL Behring

EBERHARD KWIATKOWSKI
Bayer Pharma

BOB MCDOWALL
McDowall Consulting

YVES SAMSON
Kereon

DR WOLFGANG SCHUMACHER
F. Hoffmann-La Roche

DR JÖRG SCHWAMBERGER
Merck

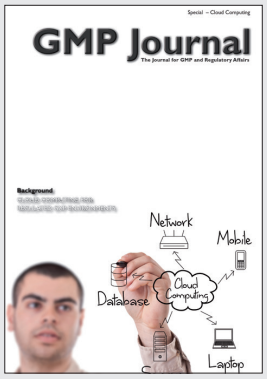
JENS SEEST
Leo Pharma

MICHAEL WEGMANN
F. Hoffmann-La Roche

HIGHLIGHTS:

- New requirements on computerised systems: what are the consequences for the European pharmaceutical industry?
- How to interpret these regulations and how to implement them pragmatically?
- What do inspectors expect from industry in the future?
- **3 pre-conference workshops**
  - Writing testable and verifiable User Requirement Specifications
  - Cloud Computing in a GxP Environment
  - Periodic Review / Periodic Evaluation of computerised Systems

This conference is recognised for the ECA GMP Certification Programme „Certified Computer Validation Manager". Please find details at www.gmp-certification.eu



Special; March 2013

Content

CLOUD COMPUTING FOR REGULATED "GXP" ENVIRONMENTS

During the last 5 years, various service providers developed multiple models for hosting services based on cloud computing. There is a big temptation for regulated organisations to consider such cloud services to reduce operational costs. However such decisions should be taken carefully since data are not only subject to GxP regulation but because they represent one of the most valuable parts of the company's capital.

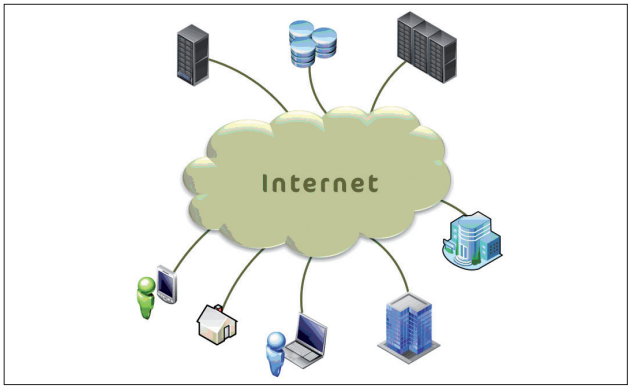
GMP Journal

Publisher:	CONCEPT HEIDELBERG GmbH Rischerstraße 8 69123 Heidelberg, Germany HRB Mannheim Nr. 705125
General Manager:	Oliver Schmidt
Chief Editors:	Oliver Schmidt, Wolfgang Heimes
Editorial Staff:	Dr Gerhard Becker, Dr Günter Brendelberger, Dr Robert Eicher, Dr Andreas Mangel, Sven Pommeranz, Oliver Schmidt, Axel H Schroeder.
Editors on this Issue:	Yves Samson
Graphic Concept & Realisation:	Wolfgang Heimes
Production:	abcdruck GmbH Waldhofer Straße 19 69123 Heidelberg
Contact:	info@concept-heidelberg.de

CLOUD COMPUTING FOR REGULATED "GXP" ENVIRONMENTS

Yves Samson, Kereon AG*

Since the beginning of the Internet, only network administrators and IT infrastructure architects took care of the effective topology and details of the network. End users needed only to know where and how to connect their terminal devices without any knowledge about the details behind the network outlet in the wall. That's how the term cloud developed which comes from the traditional graphical representation used for "Internet" as well as for "outside" IT Infrastructure.



From identified server to hyperlink

Starting by a "pure" network infrastructure (Internet), with the deployment of the World Wide Web, the Cloud began to propose more services and at the same time to become more abstract. While in the early time of Internet the connection to the ftp server of the Library of Congress was assumed to be connected to a hardware server located within the IT infrastructure of the Library, the use of web services became to be less location related and the end user started to ignore the real location of the servers behind the hypertext link.

Since the relationship to a clearly identified geographical location was lost, the Cloud was definitively born.

Various kinds of application could be deployed based on cloud computing, for example:

- Collaborative tools, including calendars, address books, mail services
- Dedicated applications such as ERP, relationship management system, procurement platform
- Information management systems, e.g. document management system.

Cloud definitions

Cloud computing is typically a generic and nebulous term describing a lot of various topologies and services where each of them has a specific meaning with specific benefits and concerns.

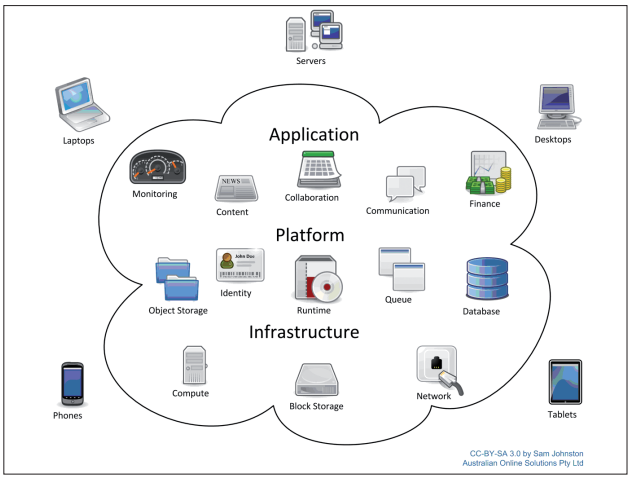
The cloud implies a kind of "black box" view. Indeed, the cloud is an abstraction of a collection of IT infrastructure components such as servers, storage systems, networks, etc. The cloud makes it possible for the user to ignore the detail of the IT infrastructure which supports their own application and data.

Only in September 2011, NIST[1] provided a formal and well accepted brief set of definitions about cloud computing covering:

- Service models
- Deployment models

Usually three models of services[1] are associated with cloud computing:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)



Each model represents a specific scope and implies a specific sharing of responsibility between service provider (SP) and regulated user (RU).

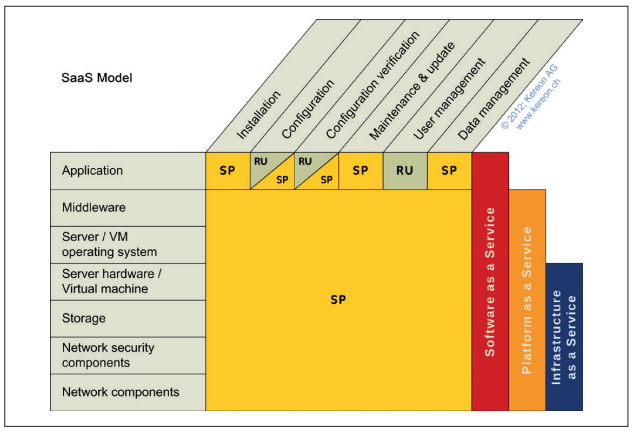
SaaS – Software as a Service

By the SaaS model, a configured application, including all necessary infrastructure and platform components as well as hosting facility, is delivered to the regulated user. The RU contribution is limited to the following activities:

- Final configuration and verification
- User management

The data reside in the cloud infrastructure under the SP's responsibility. The RU can only have an impact – if any – on backup scheduling. The RU will only request restore activities without any impact on their execution.

[1] Further service models can be found in the technical literature, although they mostly correspond to a combination of the three service models defined by NIST. This article focuses on the service models as defined by NIST, see [1].



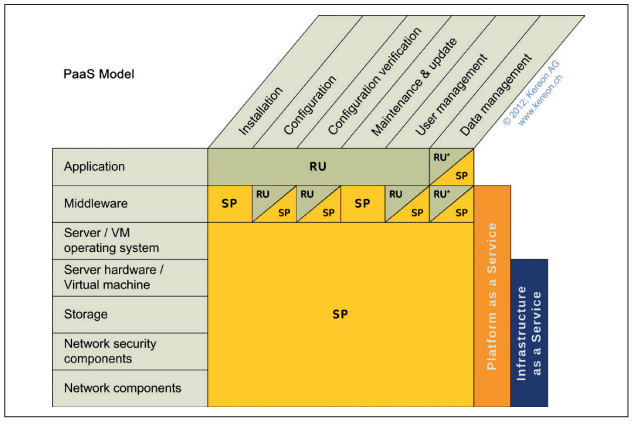
Application Operational and Performance Qualification (OQ, PQ) remain the RU's responsibilities. It is possible for the regulated user to buy the execution of qualification activities from the service provider. Nevertheless, from a regulatory point of view, the qualification activities remain in the scope of the RU's responsibility.

The SaaS model is similar to the ASP concept – Application Service Provider – as promoted in the late 1990ies. The regulated user does not own the application but he pays a right to use it.

PaaS – Platform as a Service

By the PaaS model, a middleware, including all necessary infrastructure components as well as hosting facility, is delivered to the regulated user. The RU has to perform the following activities:

- Middleware configuration and verification
- Application development respectively installation
- Application configuration and verification
- User management



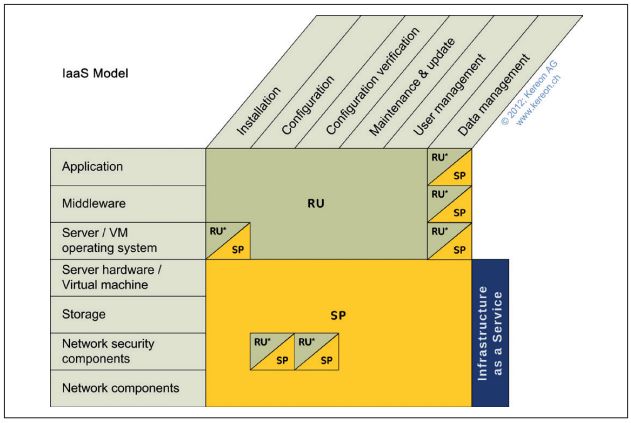
As by the SaaS model, the data reside in the cloud infrastructure under the SP's responsibility. The RU can only have an impact on backup scheduling. The RU will only request restore activities without having any impact on their execution.

Depending on the technology used and the agreed contract, the RU could be allowed to perform some data dumps to save data and configuration outside of the cloud.

IaaS – Infrastructure as a Service

By the IaaS model, computational and storage resources, including all necessary network components and hosting facilities, are delivered to the regulated user. Depending on the contract conditions, the RU has to perform the following activities:

- Installation, configuration and maintenance of the server operating system
- Installation, configuration and maintenance of the middleware
- Verification of the installed configuration
- Application development respectively installation
- Application configuration and verification
- User management



Like by the SaaS and PaaS models, the data reside in the cloud infrastructure under the SP's responsibility. The RU can only have an impact on backup scheduling. The RU will only request restore activities without having any impact on their execution.

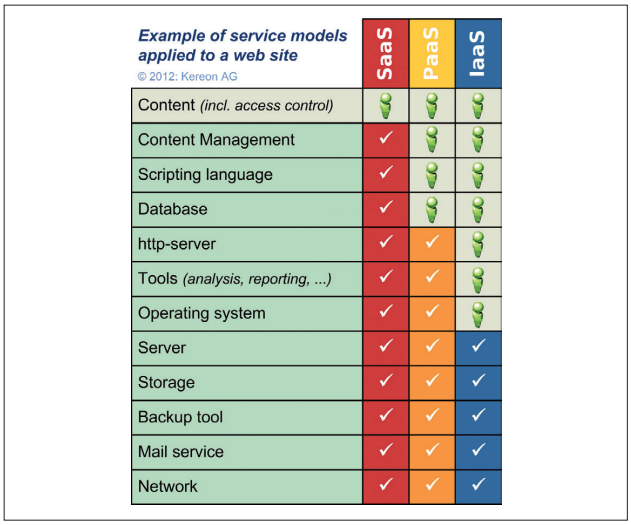
Depending on the technology used and the agreed contract, the RU could be allowed to perform some data dumps in order to save data and configuration outside of the cloud.

Based on the infrastructure used and on the contract conditions, it is possible for the RU to have some limited controls on network security components such as firewalls.

Practical example

Operating a web site requires the installation of an IT network, mail service, server hardware, operating system (Linux, Windows, …), http-server software (Apache, Tomcat, IIS, …), analysis and reporting tools, programming language (PHP, Perl, Ruby, …), content management software (Drupal, Joomla, Typo3, …), database (MySQL, Postgres, Oracle-DB, MS-SQL, …). Additionally data storage (SAN, NAS, …) and backup facilities must be installed in order to store and to secure the data.

The impact of the corresponding service models on the provided service package is shown in the following table. Depending on the service provider, in particular the scope of the platform can vary. Obviously, the content remains in the direct responsibility of the regulated user.



Cloud deployment models

Deploying applications over the cloud does not have to imply sharing infrastructure, platform or applications with external users. Indeed various deployment models are possible based on a cloud approach:

- Internal / external private cloud
  - The cloud infrastructure is designed and delivered for the exclusive use by the regulated user organisation. In such cases, the cloud could be operated by the internal IT organisation or by an IT outsourcer. The cloud infrastructure can be located "in-house" (internally) or externally.
- Community cloud
  - The cloud infrastructure is designed and delivered for the exclusive use by a specific community of user organisations. In such cases, the user organisations share common concerns, requirements as well as compliance needs.
- Public cloud
  - The cloud infrastructure is open for public use.
- Hybrid cloud
  - The cloud infrastructure is a combination of the above mentioned deployment models (private, community, public).

Benefits and concerns

The main benefits of cloud-based service delivery could be summarized as follows:

- Flexibility and service elasticity: capability to simply up- and down-size the delivered services without thresholds
- Rapid and on-demand service delivery: no delay due to procurement
- Better energy and resources management: "green IT"
- Availability and business continuity, if the cloud infrastructure is designed and managed adequately (see part II of this article in the next GMP Journal issue).

Even if cloud computing seems to be attractive, some significant concerns should be taken into account, especially for regulated organisations:

- Data privacy, data confidentiality
- Security
- Service availability
- Service provider dependency.

As soon as data are not stored within an internal private cloud[2], they are possibly accessible to third parties and at least partially out of direct control of the data owner (regulated user). The use of encryption may help to improve the data privacy and confidentiality. However, in such cases, one should not rely exclusively on built-in cloud encryption mechanisms, because such mechanisms could contain some back doors or other security weaknesses. Ideally encryption should be deployed and managed by the data owner themselves. Nevertheless even if the concept is simple, its implementation could imply the need to master various technological challenges and to suffer some negative impacts regarding performance and limitations during operation.

The marketing departments of cloud service providers like to advertise the availability of cloud solutions. Nonetheless, the last five years show a collection of significant interruption of service from some hours to several days. All cloud service providers have to report service breakdowns. In October 2011, the disruption of mail services during several days by a mobile phone company showed how companies are technology and service dependent. If a large part of the office work requires cloud access, companies will be simply unable to work in the case of service disruption. The "29th February 2012 bug" – 12 years after year 2000 – showed again the weaknesses[3] and the limited availability of some cloud solutions. The ability "to have access to the data anywhere" (marketing claim) can rapidly become "no access from anywhere" (sad reality).

By using cloud-based solutions, the RU has to manage a double dependency regarding its service provider:

- During operation, since the service must be available. The cloud service is the new and crucial "common mode failure" within the IT landscape.
- When changing the service provider, since the migration of data and application could represent a very expensive, time consuming, and challenging project. Every service level agreement (SLA) should define the conditions to cancel the service delivery as well as to move and to secure the data to another place. Surprisingly, this specific point is both rarely as well as inadequately addressed and the conditions for changing the service provider are unclear and they could jeopardize data integrity and availability.

Managing the complexity of cloud-based solutions

In the previous sections, the structure and the particularities of cloud-based solutions have been briefly presented. So far the questions related to the geographic location of cloud infrastructures have not been yet discussed.

The basic principle of cloud computing is to behave like a "black box". The services are available for the regulated user without needing to know where data and application

[2] Because of possible security weaknesses, data stored within the internal IT infrastructure may be subject to unauthorized access. Nevertheless it is simpler to limit and to control the access to data within an internal infrastructure than if the data are stored externally. This remark applied equally to data hosted by an outsourced datacentre operated by an external service provider.

[3] The same company did experience significant availability problems in September 2011 impacting all cloud-based services, because of load balancing malfunction inducing DNS-failures. Regarding the leap year issue, it is probably justified by a real sense for accuracy since the leap year is out of the scope of the solution's name "…365".

are effectively stored and operated. Because cloud service providers behave like insurance companies, very often they use and rely on external cloud service providers for increasing the service availability and for offsite backup.

This combination of services – service to the user and back-office services – makes the technical evaluation of offered solutions as well as the audit of cloud service providers more difficult. Petabytes of storage capacity, computational power, and network bandwidth are sold and bought as needed, like in a stock exchange. The location – yesterday audited by the regulated user – can be already obsolete tomorrow because data and (virtual) servers are hosted at another place, country, or continent. Several troubles in the past showed that suddenly the backup infrastructure hosted by an external provider is finally located at the other side of the street.

Since the regulated user remains responsible and accountable for its data and the compliance state of its applications, it is its responsibility to manage accurately its service providers. Supplier management starts with a supplier audit. It is obvious that cloud service providers cannot be audited like an API manufacturer. New approaches for auditing IT service providers are necessary, requiring:

- IT technology knowledge
- IT security knowledge
- Knowledge of current IT certifications (in-scope, out-of-scope, controls)
- Legal knowledge
- GxP and CSV knowledge.

Without "insider" know-how – i.e. IT infrastructure know-how – a meaningful audit of a cloud solution, including availability, security, maintainability, and business continuity aspects is effectively impossible. Regardless of the used technology and of the provider's competence, the devil remains in the details. It could be a good idea to have a sound knowledge on the current IT certifications and to understand the corresponding certification processes (self-assessment, third part audit, …) in order to avoid audit redundancies. Knowing and understanding the specific certification area would make possible to focus the audit on areas of interest which are not directly covered by the certification.

One of the particularities of cloud solutions is the complex network of responsibility, especially if the cloud service provider relies on external third-party cloud providers (offsite backup, redundancy). It seems pretty impossible to master such complex interdependencies without a knowledgeable lawyer. Likewise the definition of contracts and service level agreements (SLA) should be performed diligently, including on a legal level. If limitations and constraints are required by the regulated user, those have to be defined precisely without giving any space for interpretation. Such limitations could be related to the location of the datacentres. Constraints could be established in terms of control by the regulated user as well as information duty from the service provider to the regulated user. Everything is possible as long as it is clearly required and adequately stipulated.

Especially because cloud infrastructures are evolving rapidly, it is necessary to increase the frequency of follow-up and routine audits. It is a good idea to formalise such needs in the contract and SLA.

The growing complexity of the technology represents a real challenge for the auditors and multiple subject matter expertise is required to ensure the validity of IT service provider audits.

Regulatory and legal impacts

Even if the various players of the healthcare sector are used to dealing with regulatory requirements, the deployment of cloud-based solutions increases dramatically the complexity of the applicable legal and regulatory framework.

On the GxP side, Annex 11 to the European GMP Guide (see [2]) defines clearly the expected responsibilities and level of control for computerised systems involved by GMP activities. By extension, these requirements should be applied to systems involved in the other regulated GxP processes such as clinical, distribution, laboratory, and vigilance processes. Additionally, local GxP regulations (e.g. [3]) may require that the batch documentation has to be retained within locations[4] specified in the GMP license.

More complex is the legal situation. During the last 12 years, different states around the world developed a complex legal framework for fighting against:

- Terrorism
- Violation of intellectual property
- Counterfeiting
- Etc.

In many countries, the Internet is accused as the vector and dissemination carrier of illegal and/or dangerous information and content. The question is not to approve or to reject such a view but to understand its impact on the way how data privacy is currently considered.

European companies are used to observe data privacy laws and directives on national and on European level (see [4]). Even if such regulatory framework is not perfect, multiple legal protection mechanisms exist for ensuring a limited but a real respect for data privacy.

Since 2001, the USA is governed amongst others by the Patriot Act (see [5]). Initially elaborated for helping intelligence agencies to fight against terrorism, its enforcement throughout the last 10 years makes data privacy at the least challenging, but in fact impossible. One of the major concerns is related to the fact that stored records and data have to be handed over to US authorities on demand without a court order and without the data owner being told.

[4] The application of this principle to electronic batch records makes outsourcing and cloud-based strategies more difficult since some specific agreements must be defined between the regulated company and the service provider.

Many discussions outside of USA show that companies as well as lawyers and associations defending data privacy are deeply concerned with this rule. Not only European countries but also Canada shares this general concern.

USA-based cloud service providers tried to provide some guaranties regarding data privacy, for example by relying on subsidiaries based outside of USA and by avoiding providing services using datacentres located in the USA. Unfortunately, this approach has been rejected by US authorities, arguing that the Patriot Act applies as soon as an organisation has subsidiary located in the USA.

The consequence for organisations taking care of data privacy is to avoid the use of cloud services provided or supported (including in case of offsite backup and business continuity) by companies based in the USA.

It is interesting to notice, based on recent discussions with US cloud professionals, that many of the US companies providing cloud services are not aware about this privacy concern of non-US customers.

In several European countries, the number of projects for building "pure European" cloud should be considered as an answer to the Patriot Act, so improving the support of data privacy.

Last but not least, it should not be forgotten that some countries do not recognize intellectual property rules. Enforcement of data privacy and intellectual property based on non-disclosure agreements is not possible since the national law does not support it. Again, it is a good idea to avoid cloud services provided by companies based in such countries.

Innovative approach to IT Infrastructure compliance

Whatever are the concerns regarding the use of cloud-based solutions, cloud computing brings some innovations to consider in IT infrastructure management, compliance, and control.

One of the most interesting clauses by Annex 11[2] stipulates that internal IT departments should be considered analogous to third-party IT service providers.

This principle should help to bring more fairness by considering internal IT departments. Too often regulated companies tend to require a higher compliance level (increasing the related formalism and effort) by internal department than by external service providers. At the same time, these companies complain about high compliance costs.

Annex 11 should encourage regulated companies to define a commensurate IT compliance framework applicable equally to both internal IT departments as well as to third-party suppliers and service providers.

An observation of the behaviour of regulated companies shows that companies tend to privilege outsourced IT solutions in the case of business critical applications while they rely on their internal IT departments for operating less critical applications.

A consistent and logical decision process should prefer a solution provided by internal resources in case of critical applications. Otherwise, the leak of confidence into the own quality management system and teams could raise a lot of questions, in particular for regulators during inspection.

Within the last 20 years, IT organisations complain about the inadequacy of the "conventional" CSV approach for IT infrastructure. Indeed the rate of change by an IT infrastructure is much higher than by a production facility. However there is no reason for rejecting some levels of control for IT infrastructure supporting GxP-relevant activities.

Maybe the deployment of internal private clouds within the IT infrastructure of regulated companies could represent a way for improving the compliance efficiency and for limiting compliance and operation costs.

The abstraction level induced by a cloud-based approach could be helpful for defining an adequate and efficient change management strategy. Configuration and change management are based on the management of configuration items. The definition of meaningful configuration items with appropriate size, extend, and impact is the key for success and for efficiency.

Too often unluckily defined configuration items complicate the configuration and change management activities and cause high (and unnecessary) costs. The use of internal private cloud should help regulated organisations to formalise efficient IT infrastructure management strategies without jeopardizing the needed compliance level.

A meaningful application of risk-based approach to IT infrastructure compliance taking advantage of cloud computing technology could be one of the answers for limiting the operational costs. Outsourcing is surely not the sole solution for streamlining the costs.

Possible trends

An interesting experience shared by regulated companies that have used cloud-based solutions showed the following life cycle:

1. Application is operated by the internal IT department
2. Application is moved to an external cloud in order to limit the costs
3. Application is operated in an external cloud but …
   a. The level of control needs to be increased
   b. Application availability becomes a concern
   c. Data availability becomes a concern and cloud-offsite backup (and archiving) are needed

4. Cloud offsite backup is organized, using the company IT infrastructure (often for cost or practical reasons)
5. A cost review shows that, for a specific level of availability, operating the application internally would be less expensive than by using an external cloud.
6. Application operation is re-insourced.

As usual such life cycle is really dependent on the considered application and of the specific requirements. However, based on the mentioned clause of Annex 11 related to the consideration of internal IT departments, it is necessary to remember that both the compliance level as well as the application performance should not become lower for outsourcing reasons than by internal operation.

Ensuring data integrity, privacy, and confidentiality represent a cost. However missing these requirements could become very expensive, not specifically from a regulatory point of view, but in terms of business capability and of knowledge protection.

Legal requirements in some countries, the lack of protection of intellectual property in other countries, the non-respect of data privacy and intellectual property by some cloud service providers have to be taken into account by selecting the most appropriate scenario for operating a GxP-relevant application.

Auditing service providers is unavoidable but the scope of such audits requires well knowledgeable subject matter experts (IT, legal, GxP, CSV,…). The audit strategy must be modified to being more suitable to the cloud specifics.

Evaluation of cloud solutions

By evaluating a cloud solution, at least the following criteria must be considered:

1. Needs and constraints, including applicable regulatory and legal requirements
2. Service model: IaaS, PaaS, SaaS
3. Deployment model: private, public, community, hybrid
4. Geographical location: country hosting the cloud infrastructure, country where the provider is located
5. Contract conditions, including business continuity measures and contract exit conditions.

Multiple learned lessons are available on the Internet regarding failed deployments or malfunctions during operation of cloud-based implementation. It is highly recommended to take an attentive look at such information before planning and deploying cloud-based solutions.

Cloud computing is surely a useful tool for helping to master IT infrastructures. However, the way to operate and to use the cloud needs to be clearly and precisely defined, avoiding nebula. Additionally to the use of virtualisation, various open source software projects could help regulated organisations to plan, to implement , and to deploy internally cloud-based solutions in a secure and compliant manner.

*On the Author:

Yves Samson is founder and Director of the consulting firm Kereon AG located in Basle, Switzerland. He has been in computerized system validation since 1992. He is the editor of the French Version of GAMP®4 and GAMP®5 and he translated the PIC/S Guide PI 011 into French.

Literature

[1] National Institute of Standards and Technology, "NIST Special Publication 800-145 - The NIST Definition of Cloud Computing," NIST, Gaithersburg, 2011.

[2] European Medicines Agency, "EudraLex - Volume 4 Good manufacturing practice (GMP) Guidelines - Annex 11 "Computerised Systems"," EMA, London, 2011.

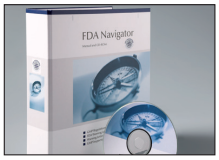
[3] "AMWHV - Verordnung über die Anwendung der Guten Herstellungspraxis bei der Herstellung von Arzneimitteln und Wirkstoffen und über die Anwendung der Guten fachlichen Praxis bei der Herstellung von Produkten menschlicher Herkunft," Bundesministerium der Justiz, 2006 - 2011.

[4] European Parliament and Council, "Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data," Official Journal of the European Commission, Brussels, 1995.

[5] 107th Congress, "H.R.3162 -- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act," Library of Congress, Washington DC, 2001.

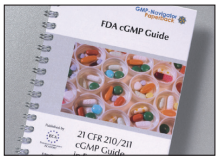
[6] Z. Whittaker, "Summary: ZDNet's USA PATRIOT Act series," ZDNet, 27 04 2011. [Online]. Available: http://www.zdnet.com/blog/igeneration/summary-zdnets-usa-patriot-act-series/9233.

GMP Handbooks • GMP Regulations



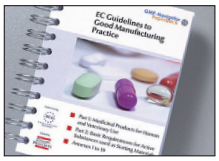
FDA Navigator with Warning Letters Report Handbook + CD ROM
Price Non ECA Members: € 399,-
Price ECA Members: € 260,-
(Annual Update € 199,-)

Copies ☐ Yes ☐ No



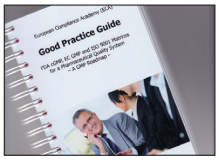
FDA cGMP Guide
• 21 CFR 210/211 cGMP Guide in English
• Paperback in the handy format 11.5 x 15 cm, 40 pages
Price Non ECA Members: € 18,-
Price ECA Members: € 12,-
When purchasing 10 to 50 copies € 15 per copy
When purchasing > **50 copies € 9.90 per copy**

Copies ☐



EC Guidelines to Good Manufacturing Practice
(Part 1 Medicinal Products and Part 2 Active Pharmaceutical Ingredients incl. Annexes 1-19)
NEW: Part 3 Site Master File, Quality Risk Management, Pharmaceutical Quality System, Internationally harmonised requirements for batch certification
NEW: Chapter 1 and 7, Annex 2
Incl. Draft Chapter 2 and 5
• Paperback in the handy format 11.5 x 15 cm
• GMP Guide in English
Price Non ECA Members: € 35,-
Price ECA Members: € 22,-
When purchasing 10 to 50 copies € 30,- per copy
When purchasing > **50 copies € 25,- per copy**

Copies ☐



ECA Good Practice Guide
"FDA cGMP, EC GMP and ISO 9001 Matrix for a pharmaceutical Quality System – A GMP Roadmap".
The revised ECA Good Practice Guide is a comprehensive juxtaposition containing the requirements laid down in FDA's cGMP Guide, the EU GMP Guide and ISO 9001. The Matrix has 21 pages as well as further 530 pages for the following three regulations.
• FDA cGMP Guide
• EU GMP Guide Part I, II, and III incl. all Annexes
• ISO 9001 Quality Management Systems
• ISO 9001/ICH10
Price Non ECA Members: € 149,-
Price ECA Members: € 99,-

Copies ☐

ICH Q7 GMP for Active Pharmaceutical Ingredients
with a Side-by-Side comparison and APIC's How-to-do Document (Version 6, October 2010)
• Paperback in the handy format 15 x 11,5 cm
• Complete text of ICH Q7 GMP for APIs and comparison of the interpretation by the Active Pharmaceutical Ingredients Committee (APIC)
Price Non ECA Members: € 49,-
Price ECA Members: € 32,-
When purchasing 10 to 50 copies € 44 per copy
When purchasing > **50 copies € 39 per copy**

Copies ☐

All prices plus postage, packing, and VAT (if applicable)

We hereby bindingly order the above items:

Title, First Name, Surname

Company | Department

Street | Postal Code / City

Phone/Fax | E-Mail

Please send order to: CONCEPT HEIDELBERG GmbH • Rischerstraße 8 • 69123 Heidelberg, Germany • Phone +49 6221 84 44-0 • Fax +49 6221 84 44-34

ISSN 1867-7975