jamk.fi

ADOPTING CLOUD COMPUTING AND HOSTED SERVICES IN PHARMACEUTICAL INDUSTRY

Ville Harjulampi

Master's Thesis
December 2013

Degree Programme in Information Technology
Technology and transportation

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

DESCRIPTION

Author(s)	Type of publication	Date
Harjulampi, Ville	Master's Thesis	09.12.2013
	Pages 62	Language English
		Permission for web publication (X)

Title

Adopting cloud computing and hosted services in pharmaceuticals industry.

Degree Programme

Master´s Degree Programme in Information Technology.

Tutor(s)

Huotari, Jouni

Turunen, Ilkka

Assigned by

FinVector Vision Therapies Oy

Abstract

Cloud computing has become popular among consumers and within bigger corporations as well. Information technology services that used to be internal only can be now taken into cloud using various combinations of cloud technology.

In this thesis cloud computing was examined from pharmaceutical company point of view. There are several regulations, directives, guidelines, recommendations and legislation that need to be taken into consideration before making any cloud computing decisions.

The outcome of the research was better understanding of the technology behind cloud computing and how it can be approached. Regulatory factors were also reviewed. Additionally a risk based approach model was generated as a roadmap into cloud computing.

During the research work it became clear that the subject is still being highly debated among industry mainly because of overlapping, partly outdated and fragmented regulatory requirements. However, pharmaceutical industry can implement and benefit from cloud computing.

Keywords

Cloud computing, pharmaceuticals, validation, qualification

Miscellaneous

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

KUVAILULEHTI

Tekijä(t) Harjulampi, Ville	Julkaisun laji Opinnäytetyö	Päivämäärä 09.12.2013
	Sivumäärä 62	Julkaisun kieli Englanti
		Verkkojulkaisulupa myönnetty (X)

Työn nimi
Adopting cloud computing and hosted services in pharmaceuticals industry.

Koulutusohjelma
Master´s Degree Programme in Information Technology.

Työn ohjaaja(t)
Huotari, Jouni
Turunen, Ilkka

Toimeksiantaja(t)
FinVector Vision Therapies Oy

Tiivistelmä

Pilvipalveluista on viime aikoina tullut suosittuja niin yksityishenkilöiden kuin suurempienkin yritysten keskuudessa. Aiemmin ainoastaan yritysten sisäisiä tietotekniikkapalveluita voidaan nykyään siirtää pilvipalveluihin hyödyntäen monenlaisia yhdistelmiä erilaisista pilvipalvelumalleista.

Tässä opinnäytetyössä pilvipalveluita lähestytään lääketeollisuuden näkökulmasta. On olemassa useita asetuksia, direktiivejä, ohjeistuksia, suosituksia sekä lainsäädäntöä joka pitää ottaa huomioon ennen pilvipalveluiden käyttöönottoa.

Opinnäytetyön lopputuloksena oli erilaisten pilvipalveluiden teknologioiden tarkastelua ja riskipohjaisen lähestymismallin luominen jota voidaan käyttää vaihtoehtona lääketeollisuuden pilvipalveluissa. Erilaisia viranomaisvaatimuksia ja suosituksia myös tarkasteltiin työn aikana.

Tutkimustyön aikana kävi ilmeiseksi, että aihe on vielä kiistainalainen teollisuuden parissa johtuen päällekkäisistä, osittain vanhentuneista ja hajanaisista viranomaisvaatimuksista. Pilvipalveluiden käyttöönotto on kuitenkin mahdollista.

Avainsanat (asiasanat)
Pilvipalvelut, lääketeollisuus, validointi, kvalifiointi

Muut tiedot

Contents

FIGURES

TABLES

TERMINOLOGY

Term	Definition
94/46/EC	Data protection directive released by European Union.
AWS	Amazon web services, cloud computing service.
CIO	Chief information officer.
Cloud computing	Use of computing resources as a service across the network.
Computer System	A group of hardware components and associated software designed and assembled to perform a specific function or group of functions.
CSA	Cloud security alliance.
EMEA	European medicines agency.
ENISA	European union agency for network and information security.
ERP	Enterprise resource planning system.
EU	European union.
EudraLex Volume 4 Annex 11	European Commission has published a set of guidance for manufacturing and distributing medicinal products for pharmaceutical industry in the European Union. Annex 11 applies to computerized systems.
FDA	US food and drug administration.
FMEA	Failure mode effect analysis, systematic analysis tool for failure analysis.
GAMP	Good automated manufacturing practice, published by ISPE.
GMP	Good manufacturing practice.
GMP significant application	Software application which have direct access to GMP data.
GMPIA	GMP impact assessment.
GxP	General term where x represents for example manufacturing (“GMP”) or laboratory (“GLP”).

Term	Definition
HIPAA	The health insurance portability and accountability act (US).
IaaS	Infrastructure as a Service, cloud deployment mode.
IEEE	Institute of electrical and electronics engineers.
ISACA	Global association to promote knowledge and practices. In the past known as the Information systems audit and control association.
ISPE	International society for pharmaceutical engineering.
ITU	International telecommunication union.
NIST	National institute of standards and testing.
PaaS	Platform as a service, cloud deployment mode.
QRM	Quality risk management.
Qualification	Process of assurance which ensures that predefined acceptance criteria can be achieved.
RPN	Risk priority number.
SaaS	Software as a service, cloud deployment mode.
SAS 70	Auditing standard.
SSAE-16	Auditing standard.
SD	System description. A written description of a system, including diagrams as appropriate.
URS	User Requirements Specification. A URS defines, clearly and precisely what the user wants the system do.
US-EU Safe Harbor	Framework for US based companies' compliance for 95/46/EC directive.
Validation	To establish documented evidence that the system does what it was intended to do.
VA (Vendor Assessment)	Documented evidence that verify that the vendor have a high level of confidence and meet with technical, commercial, and regulatory requirements.

1 INTRODUCTION

Cloud computing and hosted IT services are nowadays becoming more and more popular (Bittman 2012). Cloud computing solutions have evolved over the time offering better set of tools for all-sized companies and organizations. These tools usually contain for example communications management, data storage and hosted applications.

Cloud computing has become an essential way of work not just for large companies and IT professionals but for regular home computer users. It is seldom recognized that popular email services, social networking sites and web stores for tabloid and smartphone applications all have in common wide utilization of cloud computing services for their infrastructure. Because of this lack of understanding cloud computing privacy issues have not been paid attention as much as for example for online banking. Small and bigger companies have also been neglecting the cloud computing risks and privacy issues brought by more attractive and possibly better service levels than traditional IT solutions.

However, recently these issues have been brought to public attention even by mainstream newspapers publishing news on risks of cloud computing (Lassila 2012).

Authorities such as European Union (EU), Institute of Electrical and Electronics Engineers (IEEE), International Telecommunication Union (ITU) and others have taken actions by providing guidelines and standards for cloud computing implementation. Various sectors of business need to follow different authorities whilst certain top level legislation and directives should be followed by all.

This thesis work consists of technology review, regulation and standard review, pharmaceutical sector specific technology introduction, information on cloud computing security, interview of an expert and from approach model that can be used as a template for case studies.

2 BACKGROUND TO THE RESEARCH

The purpose of this thesis is to evaluate implementation of cloud computing and hosted IT services from pharmaceutical industry point of view. Pharmaceutical industry needs to follow regulatory guidelines and recommendations from several authorities such as European Union, European Medicines Agency and U.S. Food and Drug Administration depending on which market area they are focusing.

Various regulatory authors, organizations and commercial service providers may offer their solutions but how to evaluate and identify the ones that applies for certain sector?

The objectives of the thesis are

- Gain enough knowledge of cloud computing and hosted IT services to support pharmaceutical companies in selection of the relevant service(s)
- Understand implementation requirements
- Understand regulatory factors
- Improve technical knowledge and develop fuller understanding on this area of technology.

Project deliverables will be recommendations as to whether the technology can be applied and if so the benefits to the business, likely costs and regulatory consequences.

Main emphasis of the research consists of literature reviews, expert interviews and potentially case studies making the research method triangulation instead of using just one method. It is likely that theoretical framework will be created, analyzed whether framework has theoretical relevance to research problem and formed into theoretical body of knowledge.

3 CLOUD COMPUTING

3.1 History of the term

Even though cloud computing has a connection back to early days of computing and using shared mainframe computing resources the term cloud computing was first time used in the year 1997:

> *The first time the term was used in its current context was in a 1997 lecture by Ramnath Chellappa where he defined it as a new "computing paradigm where the boundaries of computing will be determined by economic rationale rather than technical limits alone."* (Sourya 2011.)

In the 2000s cloud computing has become widely accepted and used term.

3.2 Definitions

By Wikipedia (Cloud computing 2012) cloud computing has the following definition: "Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet)."

National Institute of Standards and Testing (NIST) definition of cloud computing (Mell 2011, 2-3) consists of three sections: Cloud computing has five essential characters, three service models and four deployment models.

3.3 Key characteristics of cloud computing by NIST definition

3.3.1 On-demand self-service

This characteristics means that the customer is in control of provisioning process and doesn't need interaction with service provider in order to obtain computing resources. For example customer logs in to a self-service portal, selects wanted resources, pays and gets resources automatically.

3.3.2 Broad network access

This characteristic describes that access to cloud computing resources should be available using standard protocols (such as HTTP protocol) and devices using thin or thick platforms. It also promotes the idea of computer programs interacting with cloud environment using standard protocols – not just people and devices (Carstensen, Golden & Morgenthal 2012, 17-18).

3.3.3 Resource pooling

Resource pooling characteristics describes the transition from dedicated resources into resource pooling. Computing resources can be assigned dynamically as required within organization(s) in efficient manner. End user isn't necessarily aware of the exact location of computing resource. In real life scenarios pooling idea has been utilized for hundreds of years; for instance tap water uses common pool of water without each individual having their own wells. It becomes responsibility of waterworks to provide enough resources to the common pool – in similar way end user of computer resource pool cannot be responsible for the usage peaks.

3.3.4 Rapid elasticity

User of cloud computing resources needs to be able to obtain computing resources quickly at the same time without the feel of running out of resources.

3.3.5 Measured service

This characteristic describes that reporting, monitoring and controlling of resource usage should be available both for provider and end user in order to provide transparency.

3.4 Service models

There are three service models, IaaS, PaaS and SaaS. All three can be provided either via on-premise or off-premise solution.

3.4.1 Infrastructure as a Service (IaaS)

IaaS was previously known as hardware as a service or HaaS. In this model cloud operator provides computers, physical or virtual machines, network and the storage space. It is the responsibility of end user to install operating system, middleware and application software on those machines and take care of application patching. Amazon Web Services (AWS) is an example of IaaS implementation. Pay-per-use model is usually used in this implementation.

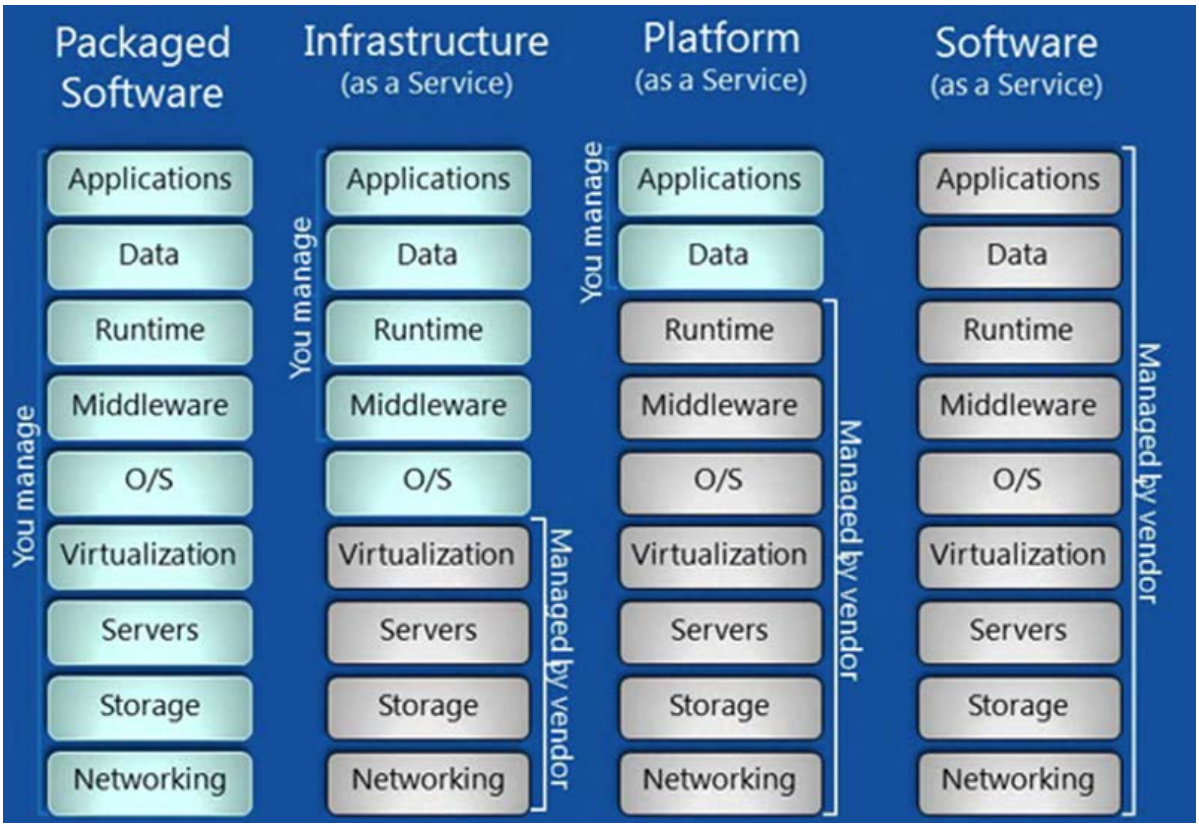

Figure 1 – Three main layers of cloud computing (Ludwig 2011)

3.4.2 Platform as a Service (PaaS)

In PaaS the cloud service operator provides same as in IaaS but in addition also manages the operating systems, middleware and system runtime. Microsoft Azure is one example of PaaS solutions.

3.4.3 Software as a Service (SaaS)

SaaS service model requires the least of administration from the end user. Usually the end user just needs to connect to an application running on the service provider's platform. Connections to could services can be established by internet browser or by a specific client application. An example of SaaS in business environment is Cisco's Webex web meeting software. An enterprise resource planning (ERP) software could also be served as a service.

3.5 Deployment models

3.5.1 Public cloud

In public cloud applications, storage and other resources are available to end users through internet – direct connection is not in general an option (Wikipedia, 2012). According to Turunen (2011, 13) public cloud is the most offered solution at the moment. Public cloud is an off-premises solution.

3.5.2 Private cloud

Private cloud is operated within organization's own borders – cloud computing services are available only to selected number of people. Private clouds can be managed either by organizations' own IT department or by external service provider. Bittman (2012) suggests that "2012 will be the year that private cloud moves from market hype to many pilot and mainstream deployments". Private cloud can be either an on-premises and/or off-premises solution. One example of such platform is Amazon Virtual Private Cloud.

3.5.3 Hybrid cloud

Hybrid cloud is a combination of at least two clouds which can be private or public clouds. The idea is to provide for example independency from internet-connection problems by running certain services in a private cloud. Hybrid cloud can be either an on-premises and/or off-premises solution.

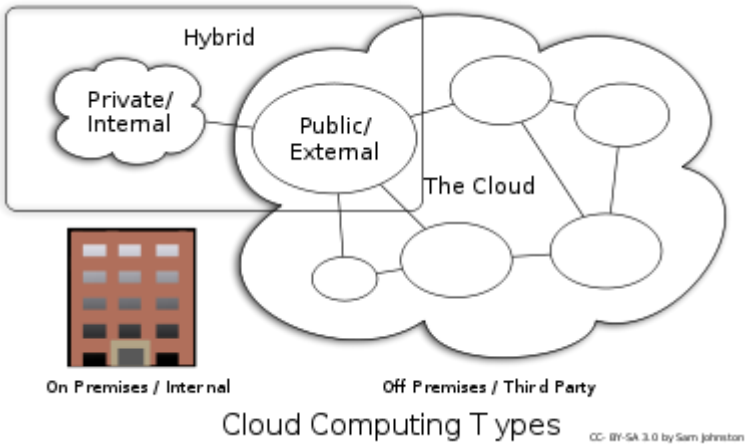

Figure 2 – Cloud computing types (Cloud computing 2012).

3.5.4 Community cloud

Community cloud offers shared resources only for limited number of organizations or individuals. Those communities usually have similar requirements and they might work in same projects or research. Community cloud can be either an on-premises and/or off-premises solution. As an example joint venture of pharmaceutical companies could create community cloud which complies with specific regulations.

3.6 Cloud service provider pioneers

One of the very first commercial service providers if not the first was Salesforce.com which in the year 1999 provided concept for providing applications for enterprise use via a website. Others to follow were Amazon Web Services (AWS) in the year 2002 and Google docs in 2006. In 2006 Amazon's EC2-network was introduced to public as a service where people can run their own applications running on Amazon's hardware (Sourya 2011).

These three companies were in top 10 cloud computing providers in 2012 (Top 10 cloud computing providers of 2012 2011).

3.7 Summary

In this chapter the technology behind cloud computing was reviewed. Different service and deployment models may be cumbersome to understand without proper introduction especially when these models can be mixed in various combinations. Then again – cloud computing uses ancient old concepts like resource pooling which was used by Roman Empire in aqueducts to distribute water to the end users.

From validation and regulatory point of view it is important to recognize technology behind the commercial products.

4 REGULATIONS AND STANDARDS FOR IT

4.1 EudraLex Volume 4 Annex 11

European Commission has published a set of guidance for manufacturing and distributing medicinal products for pharmaceutical industry in the European Union. The title is “EudraLex - Volume 4 of "The rules governing medicinal products in the European Union"”. The basic structure has three parts titled "Basic Requirements for Medicinal Products", "Basic Requirements for Active Substances used as Starting Materials" and "GMP related documents". Parts divide into chapters and document templates.

There are nineteen more specific annexes for Volume 4. Annex 11 (EC 2011) describes how computerized systems which are used in conjunction with good manufacturing practices (GMP) regulated activities should be treated. This applies to all pharmaceuticals companies under GMP regulations. Four main principles of the Annex 11 state

> *The application should be validated; IT infrastructure should be qualified. Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of the process*. *(EC 2011)*

In more details Annex 11 lists requirements under seventeen main clauses for computerized systems.

4.2 EU Data Protection Directive

4.2.1 94/46/EC Data Protection Directive

European Union directive 95/46/EC (also known as Data Protection Directive) adopted in the year 1995 regulates how personal data can be processed within the European Union. Personal data can include credit card numbers, addresses, personal records etc. The term processing is defined by Article 2 b

> *'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction (EC 1995)*

A point worth noticing from cloud computing point of view is that the directive doesn't separate manual or automatic data processing; it applies to both data handling methods.

4.2.2 General Data Protection Regulation

A new legal framework proposal to replace 95/46/EC has been introduced in January 2012 with a target adoption date in 2014 and being effective in 2016 after two year transfer period.

This new General Data Protection Regulation (EC 2012) will be aimed against the privacy challenges from rapid technology evolvement including social media and cloud computing. The regulation "extends the scope of the EU data protection law to all foreign companies processing data of the EU residents" (New draft European data protection regime 2012).

In the draft proposal there will be new privacy rights for EU citizens.

> *The "right of portability" will allow a transfer of all data from one provider to another upon request, for example transfer of a social media profile or email, whereas the "right to be forgotten" will allow people to wipe the history clean (New draft European data protection regime 2012).*

4.2.3 US-EU Safe Harbor

Safe Harbor framework has been created by US department of commerce in order to streamline US based companies' privacy and personal data handling compliance with the 95/46/EC directive. If a US based company fulfills the requirements set by the Safe Harbor framework it has sufficient level of

processing EU citizen personal data and can operate in areas applicable for 95/46/EC.

For example corporations doing business within the EU cannot send personal data outside the EU unless there is at least equal level of privacy data protection. Safe Harbor compliance has been determined to comply with requirements by EC Commission with decision 2000/520/EY (EC 2000)

US based organizations have a checklist for joining the Safe Harbor provided by US department of commerce

It is critically important that an organization read the U.S.-EU Safe Harbor Privacy Principles, 15 FAQs, and enforcement documents before submitting a self-certification form (U.S.-EU Safe Harbor homepage 2013).

List of Safe Harbor compliant companies is publicly available on Export.gov website. At the time of the writing (September 2013) there are 4130 US based companies.

Recently there has been criticism against the safety of Safe Harbor compliance due to raised concerns of internet surveillance by the US National Security Agency. The German Conference of Data Protection Commissioners has urged to “suspend agreements that allow European companies to transfer personal data of European citizens to the U.S.” because of “mass surveillance of communications by the U.S. National Security Agency” (Essers 2013)

4.3 Good Automated Manufacturing Practice (GAMP)

GAMP is a set of guidelines published by International Society for Pharmaceutical Engineering (ISPE). GAMP is an evaluation guide to ensure that pharmaceutical company has sufficient quality for drug manufacturing by covering all areas of production. This covers materials, facilities, equipment, training aspects and even hygiene of the staff. At the time of the writing (September 2013) latest version of the GAMP guide is version 5, published in 2008.

From IT point of view GAMP5 guide sets for example a framework for software validation by categorizing software into five classes. GAMP class 1 is classified being low risk category whilst category 4 and 5 are higher risk categories requiring code validation and life-cycle requirements (Martin & Perez 2008). GAMP defines operating system and utilities such as middleware part of the IT infrastructure.

Category	GAMP 4	GAMP 5
1	Operating system	**Infrastructure software** (OS, middleware, DB managers, etc.)
2	Firmware	No longer used – Firmware is no longer functionally distinguishable
3	Standard software	**Non-configured software** – Includes default configurable SW
4	Configurable software packages	**Configured software** – configured to satisfy business process
5	Custom software	Custom Software

Figure 3 – GAMP4 and GAMP5 software categories (Martin & Perez 2008).

Off-the shelf type of software such as office software products fall into category 3.

GAMP5 guide provide tools for assessing risks by using factors such as severity, probability, detectability and risk class to form
a) Risk class = severity * probability
b) Risk priority = risk class * detectability

These can be used in assistance for mitigating IT risks.

4.4 ISO/IEC

4.4.1 ISO/IEC 27001:2005 Information security management systems

This standard was approved in the year 2002 by BSI and later adopted by ISO/IEC in the year 2005. It is currently being revised and the new version is estimated to be available in the year 2013.

The scope of the standard is to provide set of specifications of which organizations may use in seeking certification for their information security management systems. It has 8 sections that define ISMS requirements, management responsibilities, internal ISMS audits, management review of the ISMS and continuously improvement of ISMS.

Approximately 1000 organizations are certified every year by accredited certification auditors making total amount of certified organizations to 7940 (August 2012). Notably more than half of organizations are Japanese whilst no ISO/IEC 27001:2005 certified Finnish organizations are present (International Register of ISMS Certificates 2012)

There are cloud computing service providers which have obtained ISO/IEC 27001:2005 certification for their ISMS. Amazon Web Services LLC (platforms Amazon EC2, Amazon S3 and Amazon VPC) and Microsoft Global Foundation Services Windows Azure platform have received the certificate among others.

4.4.2 ISO/IEC 27002:2005 Code of practice for information security management

This standard was approved in the year 2005. It was previously known as ISO/IEC 17799:2005 but was renamed to ISO/IEC 27002:2005 in the year 2007 in order to import it to the 27000 standard series. Wording of remained identical.
ISO/IEC Secretariat JTC1/SC27 is currently revising the standard and it has been estimated that new version will become published in the year 2013

ISO/IEC 27002 has 15 sections which have total of 39 control objectives for information security management. As an example the standard defines

business continuity as a section which includes two control objectives for resilience and disaster recovery.

Figure 4 – ISO27002 (ISO27001 Security 2013)

4.4.3 ISO/IEC 27017 Security in cloud computing (DRAFT)

This standard is currently in 20.20 preparatory stage at the time of writing (September 2013). It is based on upcoming revision of ISO/IEC 27002 and the working title is “Guidelines on Information security controls for the use of cloud computing services based on ISO/IEC 27002”.

The standard is expected to provide more cloud computing specific security control recommendations than ISO/IEC 27002.

4.4.4 ISO/IEC 27018 (DRAFT)

This standard is currently (September 2013) in 30.20 committee stage. ISO/IEC Secretariat JTC1/SC27 is currently creating the standard with working title “Code of practice for data protection controls for public cloud computing services”.

Mitchell lists the following content of the upcoming standard:

> *•Objective is to collect and organize security categories and their controls from current data protection regulations.*
> *•Help public cloud service providers to comply with their obligations and make this transparent to their customers.*
> *•Customers can select cloud-based data processing services that allow them to meet their obligations.*

4.4.5 ISO/IEC 27036-x Information security for supplier relationships (DRAFT)

This standard is going to be divided into several standards from 27036-1 through 27036-5. Standard will define how to evaluate and mitigate security risks when using IT services or information supplied by 3rd parties.
27036-1 Overview and concepts (1st draft available)
27036-2 Common requirements (1st draft available)
27036-3 Guidelines for ICT supply chain security (1st draft available)
27036-4 Outsourcing (pre-draft)
27036-5 Guidelines for security of cloud services (pre-draft)

4.4.6 ISO/IEC 14971:2012 Application of risk management to medical devices

This standard provides risk management tools for helping manufacturers to introduce medical devices on the market. Standard is not just for medical devices but it can be utilized by pharmaceutical companies also from risk management process point of view.

Standard introduces four steps for risk management process: risk analysis, risk evaluation, risk control and production and post-production information.

4.5 Quality risk management (ICH Q9)

European Medicines Agency (EMA) has released a guideline document for quality risk management called ICH Q9. The guideline provides qrm tools such as processes and examples for various aspects of pharmaceutical quality. The guideline presents a model of initiating a qrm management process via risk assessment, risk control, risk communication and risk review.

The question of a quality risk may become significant for pharmaceutical products and therefore it is important to mitigate those risks on computerized systems.

4.6 Summary

A pharmaceutical company must follow several regulations starting from national legislation. Also several guidelines, tools and standards have been released which can be helpful in running good business practices. It is important to recognize the various aspects of regulations especially if company operates in several countries.

European Union has paid attention to privacy and companies seeking for cloud based option should double-check to these privacy requirements. Recent skepticism on effectiveness of the safe harbor agreements caused by the espionage claims may lead into major revision of the agreement.

5 CLOUD COMPUTING IN PHARMACEUTICAL INDUSTRY

The question of using cloud based applications in pharmaceutical industry is complicated and requires multiple levels of analysis. Various applications, data, GMP significance, cloud deployment models and difference between pharmaceutical companies does not justify simple “yes” or “no” conclusions for cloud computing suitability. The following gathers some of the factors affecting to the decision making.

5.1 Applications types

The most important question related to outsourcing applications to cloud is the potential impact to the GMP significant applications (Stokes 2012, 66).

Standard office products, communication tools, financial systems are typically classified to non-GMP applications unless a connection to GMP data exists. GMP significant applications may include customer relationship management (CRM), enterprise resource planning (ERP), statistical analysis software, laboratory inventory management software (LIMS) and various other types of software which have direct access to GMP data.

Pharmaceutical organization considering usage of cloud based applications in any form should perform an application classification in order to identify regulatory requirements. It is recommended of performing initial implementations with low-risk systems to minimize failure impacts

> *Any new technology or new approach to IT solutions presents risks. Even if the technical risks have been evaluated and addressed, there is a risk that the procedural controls (e.g., security controls, staff training, and validation) will be lacking or just challenged by the authorities because they are different from traditional approaches (Gorban 2012)*

5.2 Data types

Pharmaceutical industry can generate various types of data such as clinical trial data, IP information, work instructions, batch manufacturing records, certificates, finance data, personal information etc. which all may have different frameworks and regulations for data handling. Extensive reviews of regulation requirements should be done if electronic records of GMP relevant data will be stored in a cloud based solution. GMP relevant data may also include spreadsheets and databases.

Data classification is a vital process before any data should be stored in any cloud based system. An example of steps for the data classification has been defined:

1. *Identify the data that will be processed or stored in the cloud.*
2. *Classify the information in regards to sensitivity towards loss of the CIA criteria. This would include identifying regulatory requirements for the data.*
3. *Define the rules by which particular information classes of instances must be stored, transmitted, archived, transported and destroyed. Many handling requirements result from contractual or regulatory requirements.*
   (Cox 3-4)

5.3 Layers or responsibility

When evaluating cloud implementation options from regulatory point of view it is important to underline the different layers of responsibility of each deployment model. IaaS gives much more flexibility for the end user whereas SaaS usually requires the least of administration for the system. Carstensen et al. (2012) illustrates in figure 5 a so called trust boundary which defines responsibilities of service user and service provider. Trust boundary separates the responsibility of application, OS/middleware and infrastructure layers in IaaS, PaaS and SaaS deployment models. For example in SaaS application, OS/middleware and infrastructure is responsibility of the service provider but in IaaS infrastructure only is service provider’s responsibility.

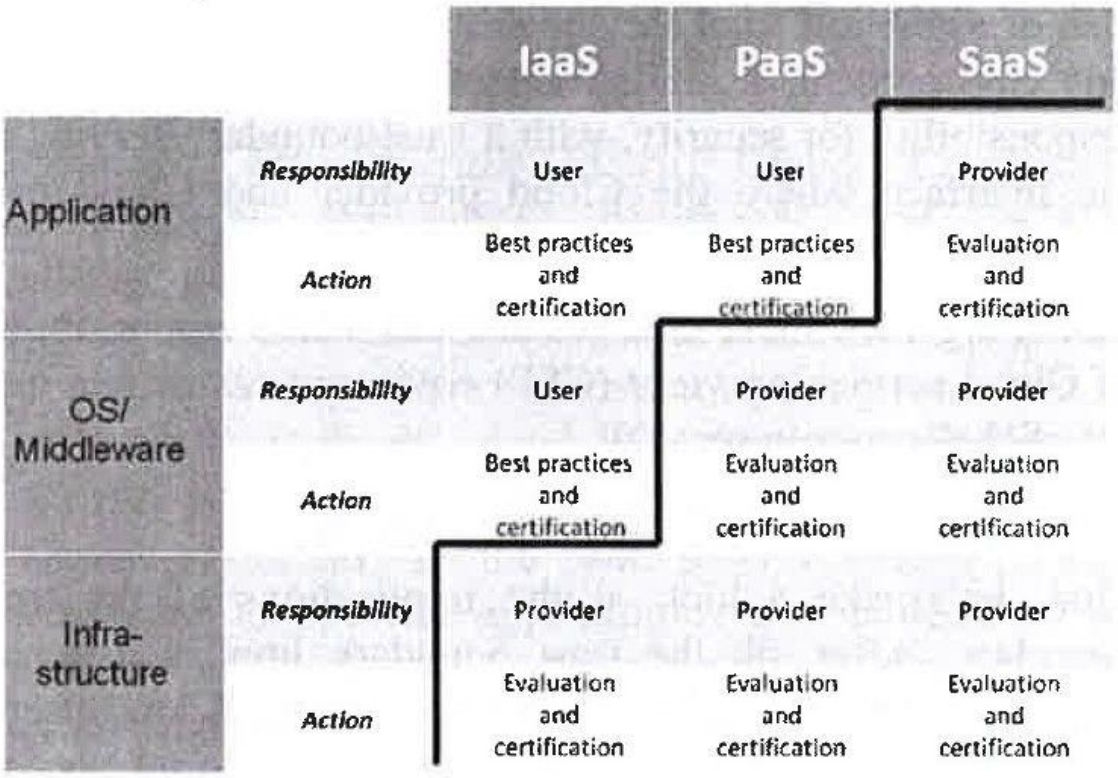

Figure 5 – Trust boundary (Carstensen et al. 2012).

Also the question of public or private clouds must be evaluated - is the platform private or public? Who is in charge or security administration for the cloud?

It has been recommended that in a phased approach model provider's responsibilities (in IaaS) to be limited below operating system level because

> *Providers often implement the appropriate security and data protection controls, but FDA requirements for formal qualification, training, and documentation are unlikely to be met. Risks can be minimized by keeping the responsibilities for the standard Operating System, middleware, and applications in house (Gorban 2012)*

5.4 Agreements and accountability

Formal agreements are mandatory between customer and service providers. This requirement is defined in Annex 11

> *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 computerised 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 (EC 2011).*

According to Stokes (2012, 5) regulated company is always accountable to the regulatory authorities for

> *- The appropriate control and compliance of their IT infrastructure (IaaS and PaaS)*
> *- The validation of the GxP significant applications (SaaS)*

However, “day to day” responsibilities can be outsourced.

5.5 Vendor audits

Pharmaceutical companies must assess supplier for adherence to regulatory and business requirements. It is the responsibility of pharmaceutical company to make sure their service provider meet the appropriate compliance standards. With regards to service provider assessment approach Annex 11 state

> *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 (EC 2011).*

Supplier assessment can be done by questionnaires (offline, online or assisted), performing an on-site audit (data center, support office) or by using a 3rd party assistance with an auditing standard such as SAS 70 or SSAE-16. Once a supplier has been accepted there might become need to do re-evaluation at some point. GxP compliance issue or a system upgrade could indicate a need to re-assess the supplier.

Questionnaire for hosting and managed services apply, some additional cloud specific questions and explanation requests should be included. In the following examples of such questions have been listed:

- *Issues of access via uncontrolled networks*
- *Need to qualify and validate for a broad range of client devices*
- *The uncontrolled nature of "self-service" (process owners provisioning inappropriately qualified, validated or controlled it infrastructure, platform's or applications)*
- *Resource pooling (shared access) erodes one or more layer of security controls*
- *Location independence may not be bounded*
- *Rapid elasticity may undermine necessary change controls (Stokes 2012, 32)*

In addition questions like these may be relevant for pharmaceutical industry:

- Application can move inside a datacenter but what about between the datacenters?
- Where does the data physically reside?
- How can I make electronic copies of my regulatory critical records?
- How is my data backed up?
- What kind of disaster recovery arranagement are in place?
- If I make a mistake can you restore just my data?
- How can I remove/get back my data if I choose to de-cloud?

5.6 Validation and qualification

It is important to recognize the difference between validation and qualification because regulations refer to both terms. EudraLex Volume 4 Annex 11 states "The application should be validated; IT infrastructure should be qualified." (EC 2011)

Rajinderkaur (2008) describes the difference of validation and qualification;

> *Qualification is a process of assurance that the specific system, premises or equipment are able to achieve the predetermined acceptance criteria to confirm the attributes what it purports to do.*

> *Validation is establishing a documented evidence to provide a high degree of assurance that a specific system, process or facility will consistently produce a product meeting its predetermined specifications and quality attributes.*
>
> *Things are qualified: equipments, systems etc.*
> *Process/Procedures (the way we use things) are validated.*

Requirements for application validation in cloud based applications do not differ from standard networks. Decision of software validation will have to be made through appropriate frameworks and regulatory guidelines.

Karamanova (2012, 19) advices to create a checklist with questions on the impact of computerized systems to drug product quality. Validation is required if at least one answer is yes on the checklist.

5.7 Sector targeted cloud solutions

IT infrastructure qualification, application validation requirements and other requirements set by various regulations may lead into cumbersome scenarios when a pharmaceutical company seeks a cloud based solution for their GMP significant applications. For example lack of audit trails or forced application upgrades on SaaS may come as a surprise if the requirement has not been noted in the evaluation phase. Therefore cloud computing industry has shown signs of waking up to the sector specific needs.

There are cloud solutions available targeted directly to pharmaceutical and life sciences industry which provide compliant platforms. One example is Compliance Cloud by NextDocs Corporation. Traditional SaaS platform offers a multi-tenancy on the application layer whereas Compliance Cloud provides multi-tenancy on the infrastructure level. “Each customer gets a fully logically isolated environment consisting of dedicated virtual web, application and database servers” (NextDocs 2012). Virtual servers, databases, network and resources is said to provide isolation from other customers and enable freedom in application upgrades – upgrades are not mandatory. Company claims regulatory compliance and validation readiness

> *The NextDocs Compliance Cloud was designed and implemented to be validation ready. Each customer environment includes Development, QA and Production environments in support of Change Control practices. Our operational and support processes are implemented to be compliant with regulations and optimized to follow industry best practices. We recognize the complexities of compliance in the cloud and have addressed those challenges in the architecture of the NextDocs Compliance Cloud, in the NextDocs products, and in our operational and support processes. (Nextdocs 2012)*

Another example of sector targeted product is EMC Cloud Computing Solutions for Life Sciences consultancy and regulation compliant systems based on a private cloud.

> *EMC Consulting will enable you to build a qualified infrastructure, validate your applications, and develop a risk management strategy to ensure you can use private cloud to support and enable your regulated applications. We start by determining which aspects of the IT Infrastructure to qualify and the required extent of that qualification. We then validate applications using established and enforced corporate policies to define the overall approach to computerized system quality and compliance (EMC 2011).*

5.8 Where to start – support documentation

The following organizations have prepared documents and guidelines to assist in the cloud decision making and vendor evaluation process.

5.8.1 CSA

Cloud Security Alliance (CSA) is a not-for-profit organization consisting of cloud key stakeholders that promotes the use of best security practices within cloud computing. CSA has published two publicly available documents that any organization approaching cloud based solutions may find useful

- Consensus Assessments Initiative Questionnaire
- Cloud Controls Matrix Framework

5.8.2 ENISA

European Union Agency for Network and Information Security (ENISA) is responsible for cyber security issues affecting to EU. Organization's goal is to achieve good quality of network and information security within EU. ENISA has published on their web site a lot of documentation that can help in the decision making process such as

- Reports on cloud computing
- Cloud computing information assurance framework
- Cloud computing risk assessment

5.8.3 NIST

National Institute of Standards and Technology (NIST) is an US based federal agency to promote US industrial competitiveness. Cloud computing relevant material include

- NIST Special publication 500-293, US Government Cloud Computing Technology Roadmap, Release 1.0 Volume 1 and Release 1.0 Volume 2

5.8.4 ISACA

ISACA is a nonprofit global association to promote knowledge and practices for information systems. They have release the following documents which may be useful in the cloud computing evaluation process

- Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives
- IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud

5.9 Block level approach

If a pharmaceutical company selects for instance IaaS as their base model for implementing cloud services there are usually many options of approaching the question of responsibility depending on the application configuration. Application can be made available for example using following methods

1. *Internal application hosted on IaaS (VMware or Amazon etc.)*
2. *External application hosted on third party IaaS*
3. *External application hosted on application providers own infrastructure*
4. *True multi-tenant application (shared dbase etc.) hosted on third party IaaS*
5. *True multi-tenant application hosted on providers own infrastructure (Appendix 1)*

These different configurations can be broken into blocks and understand where the different layers of responsibilities are. For example IaaS border is located at the operating system level and therefore question of validation may become obsolete as GAMP4 and GAMP5 guides categorization classifies operating systems on software category 1. Instead a platform qualification is expected.

5.10 EudraLex 4 Annex 11 cloud computing specific clauses

Eudralex 4 Annex 11 has seventeen clauses. In addition of previously mentioned application validation, infrastructure qualification and vendor audit requirements there are several others that need to be taken into account during cloud computing evaluation. In table 1 most relevant ones to cloud computing have been handpicked.

TABLE 1. EudraLex 4 Annex 11 cloud computing specific clauses (EudraLex 2011)

Annex 11 clause	**Requirement**
1. Principle	1. The application should be validated; IT infrastructure should be qualified.

2. Personnel	2. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.
3. Supplier and service provider	3.1 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 computerised 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. 3.2 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.
7. Data storage	7.1 Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. 7.2 Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.
9. Audit trails	9. Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly

	reviewed.
10. Change and configuration management	10. Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.
12. Security	12.1 Physical and/or logical controls should be in place to restrict access to computerized system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.
13. Incident management	13. All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.
16. Business continuity	16. For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.

5.11 Summary

Cloud computing in pharmaceutical industry is not a simple topic due to complexity of different cloud deployment models and layers of responsibilities. It is important to identify GMP significant features of operations as per Eudralex 4 Annex 11. Therefore the sector specific cloud solutions may become more popular among industry. The subject of vendor assessment can be approached block by block using the assistance of documents released by various organizations such as CSA.

6 SECURITY

6.1 Security issues

Survey after surveys among information technology management shows security being top issue preventing larger scale utilization of cloud computing. In a survey among CIOs (Cloud Adoption Study: Cloud computing is gaining momentum 2011) insufficient data security was ranked number one reason for not adopting cloud computing.

Security as a term can for example include elements of application, network, data, service or instance security.

By definition of Wikipedia (Cloud computing security 2013) security issues associated with cloud computing can be split into two categories;

1. Security issues faced by cloud providers
2. Security issues faced by their customers

According to Wikipedia (Cloud computing security 2013), in most of the cases it is the responsibility of the service provider to secure their infrastructure among end-user data. It is the responsibility of customer to ensure that service provider has implemented the proper security measures.

Wang (2009) evaluates cloud security from three aspects;

1. Security and privacy (i.e. disaster recovery)
2. Compliance (i.e. proper handling of audit trails)
3. Legal and contractual issues (i.e. liabilities)

6.2 Security controls

For cloud service providers to manage security issues proper security controls need to be in place. Francis (2013) lists four categories with examples for cloud security controls;

1. deterrent (i.e. logon warnings to advice users of rights to enter system)
2. preventative (i.e. installing a proxy server)

3. corrective (i.e. quick change of passwords after an incident)
4. detective (i.e. testing unlawfully access to information)

6.3 Security assessment

As a part of vendor assessment a security assessment may be performed to document what security controls are in place in a cloud platform. As a template, a questionnaire titled “Consensus Assessments Initiative Questionnaire” (2011) has been released by the Cloud Security Alliance for the use of cloud auditors and customers. The purpose of the questionnaire is to provide more transparency within industry. Each question has a framework of certain regulations (i.e. ISO27001) in which they refer to. For example questionnaire item DG-07.1 about information leakage in a multi-tenant environment refers to sections A.10.6.2 and A.12.5.4 of ISO27001 and may be directly suitable in use of multi-tenant pharmaceutical SaaS software evaluation.

6.4 Securing the data

Anytime when data moves outside of the traditional IT infrastructure there is a potential risk of jeopardizing sensitive content. Why not use best possible cryptography technology at every node? Usually there might be performance issues if data is being encrypted at rest, in process and in motion.

Cloud Security Alliance lists three options for securing the data transmission; Client/Application encryption, Link/Network encryption and proxy-based encryption. CSA recommends of encrypting data at the network level on every deployment models. CAS also documents how data can be encrypted in different cloud deployment models (Security Guidance for Critical Areas of Focus in Cloud Computing 2011)

According to HIPAA § 164.312 data encryption when handling regulated data in transit is mandatory.

> *Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. (HIPAA Technical Safeguards)*

Vendors like Symantec providing cloud based products have addressed to the sector specific requirements explaining how their online backup product complies with HIPAA regulations.

> *While there is no standard HIPAA certificate of compliance for online backup services, Symantec Protection Network (SPN) enables HIPAA defined covered entities that must store &protect electronic patient data comply with HIPAA security and privacy rules by:*
>
> - *Encrypting data at the point of origin, during the backup process, using 256-bit AES (approved by the NSA for encrypting U.S. classified data up to and including Top Secret).*
> - *Encryption key is private which only the originator (not even Symantec) has access*
> - *All information is sent through a secure 128-bit SSL tunnel to one of the Symantec datacenters.*
> - *Symantec data centers and operations are SAS-70 Type II certified. Additionally SPN follows an ISO 17799 / 27002 security framework and ITIL Service Management framework.*
>
> *(Is Symantec Online Storage HIPAA Compliant? 2008)*

6.5 Risks

Cloud computing in itself does not differ from traditional computing from risk point of view. There are some unique risks however. For instance access to computerized systems via uncontrolled networks and using resource pooling are unique compared to traditional computing. Also the type of chosen cloud platform together with chosen deployment model gives different risk variables. Therefore extra attention is required in risk assessment and mitigation.

Carstensen et al. (2012, 39) describes a method to understand interaction between risk, security and compliance in cloud based environment. An important thing to notice is that in the areas of compliance and security cloud user and cloud provider both have some of the responsibility. In the area of risk there is not usually similar boundary because of wide utilization of asymmetric risk arrangements in the agreements. Risk of lack of application

availability for instance results usually to financial penalties but only in limited amount.

IT risk measurement has been defined by Wikipedia (IT risk management 2013) *"The measure of a IT risk can be determined as a product of threat, vulnerability and asset values: Risk = Threat * Vulnerability * Asset"*

6.5.1 Cloud model risks

Selected cloud computing model also has an important part in the evaluation. According to Stokes (Figure 6) private IaaS cloud deployed on-premises has far less variables and connection points through uncontrolled networks compared to public SaaS cloud deployed off-premises. This of course depends on the implementation of the system; it may become useful to classify risks into three categories of acceptable, controllable and unacceptable (Stokes 2012, 33).

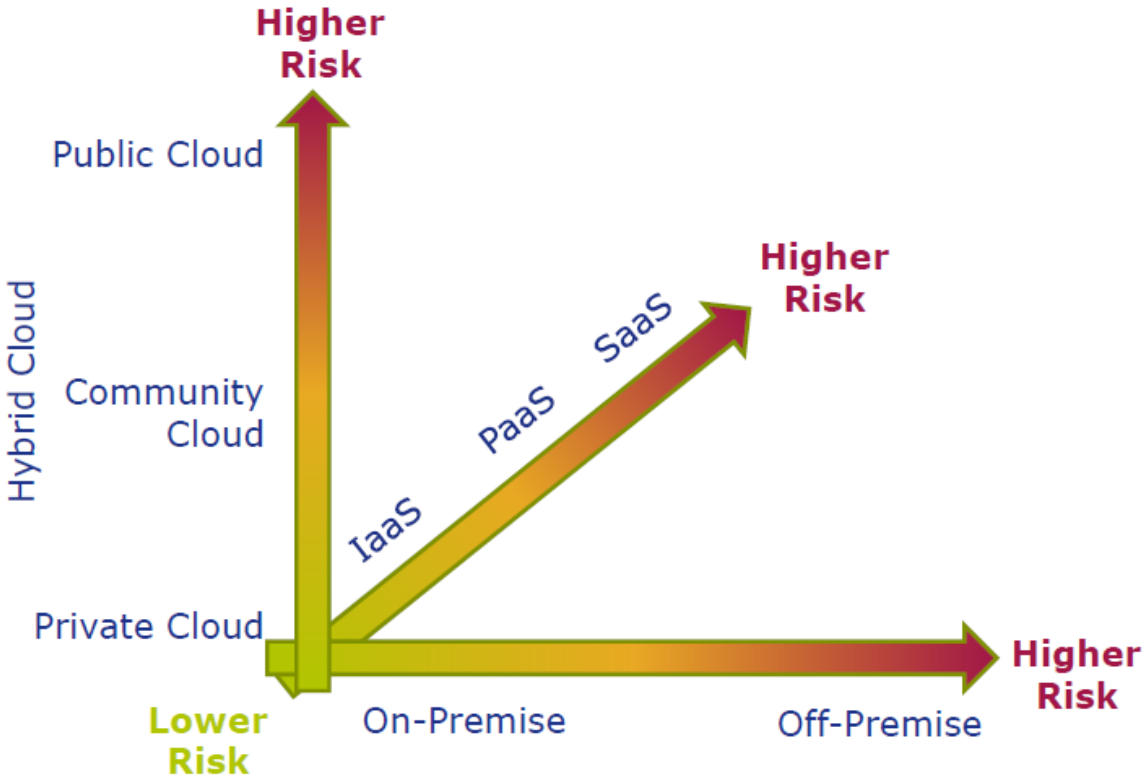

Figure 6 – Risk continuum dimensions (Stokes 2012, 34)

The risk can also be mitigated by having a fully test disaster recovery plan and procedures in place.

6.6 Risk assessment

Risk assessment is mandatory by many (Pharmaceutical) compliance standards such as EudraLex Volume 4 Annex 11, PCI DSS requirement 12.1.12, HIPAA section 164.308(a) (1) and ISO27001 Clause 4.1. If risk assessment is not mandatory from compliance point of view it is still considered to be good business practice and there are business rationales that benefit from risk assessment.

Before starting the risk assessment the business model company or organization currently has should be identified first. This context establishment is used as an input for risk analysis.

There are various methodologies like “NIST SP 800-30” or “Octave” for performing a structured risk assessment. One possible risk assessment option in evaluating cloud computing systems is the “ISO27005:2011 Information security risk management” standard. It has three steps: identification, estimation and evaluation of risks.

1. According to Wikipedia (IT risk management 2013) ISO27005 advices to identify in risk identification phase the following list of causes of a potential loss: Assets, threats, security measures (existing and planned), vulnerabilities, consequences and related business processes.
2. Risk estimation phase specifies the measure of risk: quantitative (mathematically calculated) and qualitative approach (evaluation from low to very high). Risk estimation produces a list of risks with values which can be formatted into a risk list.
3. Risk evaluation phase prioritizes and compares the identified risks based on risk evaluation and acceptance criteria.

6.7 Risk mitigation

Risks in IT are part of normal business operations. It is impractical and extremely expensive to eliminate all risks. However it is usually possible to

reduce risks. If risk assessment process reveals major findings then risk mitigation should to be implemented. Different tools can be used in assistance to mitigate the risks. A failure mode and effect analysis (FMEA) is a common tool that uses risk assessment - or similar analysis - as an input and generates either risk severity reduction or lowering the probability of the risk.

> *A successful FMEA activity helps to identify potential failure modes based on past experience with similar products and processes or based on common failure mechanism logic. It is widely used in development and manufacturing industries in various phases of the product life cycle (Failure mode and effects analysis 2013)*

Organization can be highly affected if the chosen cloud platform is not accessible. This risk can be mitigated by selecting correct service level agreement (SLA) with appropriate uptime category. So called class of 9s is widely used in the SLAs where 90% equals to maximum of 36,5 days of downtime in a year, 99,99999% maximum of 3,15 seconds of downtime in a year.

6.8 Summary

The elimination of all risks is expensive and very impractical. Cloud computing is not an exception and has risks which needs to be addressed adequately. There are also risks explicit to cloud computing. Vendors have started to release documentation to support decision making by showing how their products are compatible with various regulations.

7 RISK BASED APPROACH MODEL

7.1 Background

In order to achieve fuller understanding of regulations and cloud computing in pharmaceutical industry a risk based approach model has been generated to show real-life connections between the good manufacturing practices, regulations and technology.

In the previous chapters the terminology for cloud computing has been introduced together with relative ISO/IEC standards, general EU directives, security issues, sector specific regulations and other guidelines.

This risk based approach model has been based on pharmaceutical company point of view. It can be utilized as a case study template for companies seeking for cloud computing solutions.

7.2 Introduction

As learned in previous chapters it is vital for pharmaceutical companies to identify computerized operations within organizations that may have GMP significance. It is also required to act on findings with appropriate actions to mitigate the risks. Failing to do so may result failures in audits, official warning letters, financial penalties and even seizures of operations.

Even if GMP significant features mentioned in the EudraLex Volume 4 Annex 11 of software or a system have been recognized earlier it may be useful to revisit those findings especially if any cloud based solution models are in consideration. Also as personnel may have changed over the years and change logs do not necessarily provide accurate information whether any custom modification has been made to standard off-the-shelf type of software application.

7.3 Risk based approach model

In this model there are six steps starting from gathering operational data and identifying GMP significant features and resulting in decision on cloud suitability for selected application.

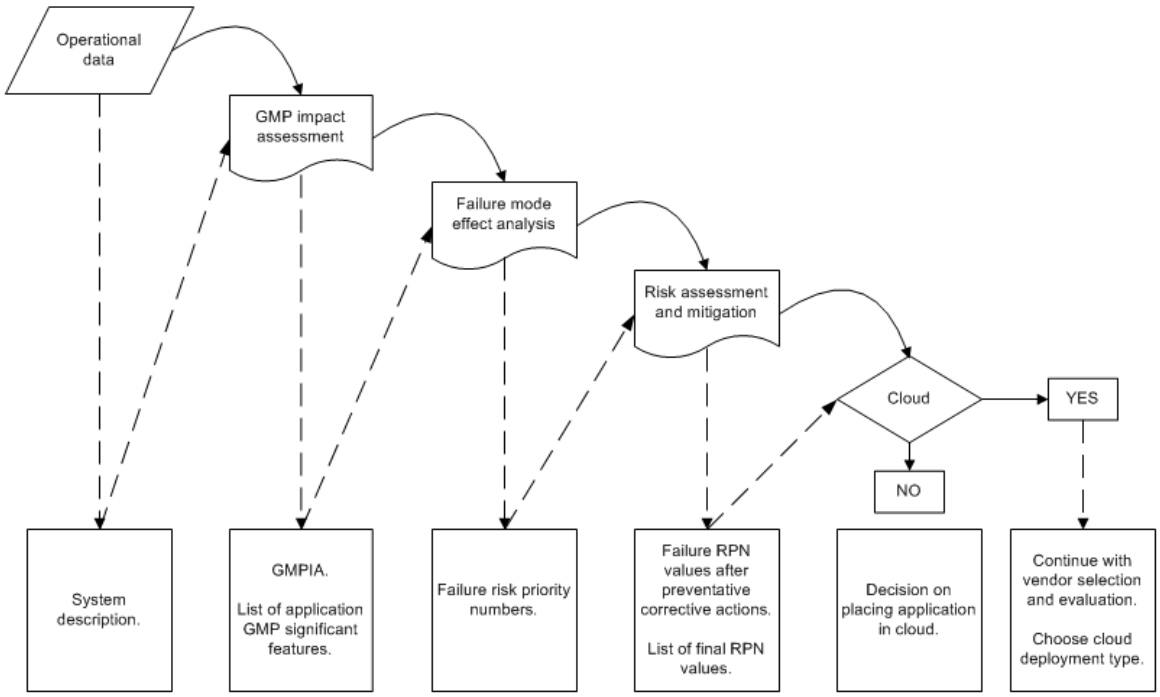

Figure 7 – Risk based approach model steps

The following steps have been identified as required steps based on risk management approaches on GAMP 5, ICH Q9 and ISO 14971 guidance.

1. **Gather operational data**
    - Input: Interviews, User requirement specifications (URS)
    - Output: System description (SD)

2. **Identify GMP significant features of software application**
    - Input: SD, regulations and guidelines
    - Output: GMP impact assessment (GMPIA)

3. **Calculate risk priority numbers for GMP significant features**
    - Input: GMPIA

- Output: Failure mode effect analysis (FMEA)

4. **Mitigate high risk priority number (RPN) risks**
   - Input: FMEA
   - Output: Updated FMEA

5. **Evaluate the risks whether they excess limits**
   - Input: Updated FMEA
   - Output: Risk assessment (RA) summary
   - Output: Data for cloud computing decision making

6. **Decision making**
   - Input: RA summary
   - Output: Final decision and path of proceeding

Framework in table 2 reflects these six steps with relevant sections of GAMP 5, ICH Q9 and ISO 14971 processes.

TABLE 2. Risk based approach model framework

Step	GAMP 5	ICH Q9	ISO 14971
Gather operational data	Step 1	Initiate QRM process	-
Identify GMP significant features of software application	Step 2	Risk identification	Risk analysis
Calculate risk priority numbers for GMP significant features	Step 3	Risk analysis and evaluation	Risk evaluation
Mitigate risks with high risk priority numbers (RPN)	Step 3	Risk reduction	Risk control
Evaluate the risks whether they excess limits	Step 4	Risk acceptance	Evaluation of overall residual risk acceptability
Decision making	Step 5	Risk communication Review events	Post production information

7.3.1 System description (SD)

System description is a document describing main features of a system and how they are utilized in practice. The format of the document can be created

to fulfill the specific needs or to follow possible corporate layout template. In general the contents vary depending on what is appropriate. In this example it is necessary to list main modules of the ERP software and modifications to these modules to-date.

An example of modifications made to the software code in a module:

Stock items can be receipted into the company against an approved purchase order. The user will check that the delivery meets the order conditions, recording the receipt in ERP and assigning a batch number and expiry date (if required). If required labels and a material reception and release form are printed. Stock items are receipted into the quarantine location.

The following modifications have been made:

- *Add two fields on the PO line receipt form that requires a user to denote whether a batch certificate has been received with the order and whether it complies with the order requirements. These are only displayed if the 'PO Manuf. batch certificate fields req, flag is set on the company card.*
- *Print storage temperature from item card on receipt labels and material reception & release form.*

An example of no software modifications applied in a module:

The Company card holds system wide information that is used throughout the modules (Company name, address, financial info etc.).

The following modifications have been made: - NONE.

7.3.2 GMP impact assessment (GMPIA)

GMP impact assessment should be generated to identify software application features that may have GMP significance. The layout of the document is free and it may include elements such as list of software features and their GMP significance. An example of a GMPIA document template has been attached as per appendix two.

In general high GMP impact systems typically include those that:
- Generate, manipulate, or control data supporting regulatory safety and efficacy submissions
- Control critical parameters or data used at any stage; clinical, development and manufacture
- Control or provide data for product release
- Control data required in case of product recall
- Control adverse event or complaint recording or reporting
- Support pharmacovigilance

7.3.3 Failure mode effect analysis (FMEA)

Using tool such as FMEA or similar, the value of a risk can be mathematically calculated and evaluated further. It may become useful to analyze different "what if" –scenarios if applications and functionalities are actually being placed in a cloud service.

FMEA is a subjective screening tool to calculate risk priority numbers with highest number of having the biggest risk. Risk priority number can be calculated with a formula of RPN = Severity (on a scale of 1 to 10) * Occurrence (on a scale of 1 to 10) * Detection (on a scale of 10 to 1). An example FMEA template can be found from Appendix 3.

7.3.4 Risk assessment summary

High risks with GMP significance identified with FMEA can be mitigated by elimination, reducing to suitable level or by demonstrating that the levels are suitable with an extended review. In the risk assessment the high risks are being addressed using preventative corrective actions and the RPN numbers for the risks are recalculated.

Risk assessment summary document summarizes GMPIA and FMEA findings, preventative risk mitigation actions and lists final RPN numbers.

Document gives data for cloud computing decision making on systems that have GMP significance.

7.4 Summary

Risk based approach model was created as an example due to various similarities in GAMP 5, ICH Q9 and ISO/IEC 14971 guidelines. This approach model can be used as a template for any company seeking for a cloud based solution.

8 CONCLUSION AND RECOMMENDATIONS

Pharmaceutical companies need to follow regulatory guidelines, most importantly in Europe EudraLex Volume 4 Annex 11. This directive clearly states that the software should be validated and IT infrastructure should be qualified.

Therefore regulated companies need to validate their GMP significant applications whether they are based on their own server infrastructure, on or off premise cloud platform or otherwise outsourced. Using public cloud based software applications that are not GMP significant is more of a business decision and should involve all the relevant stakeholders. This category may include for example communication software.

The qualification of the IT infrastructure is mandatory regardless of chosen service deployment model. Qualification needs to be documented.

However, as long as certain expectations are fulfilled cloud computing should be an acceptable solution from regulatory point of view also for GMP significant applications. Before moving to public cloud the following steps need to be completed on satisfactory level:

- Review applicable regulations
- Determine cloud service type
- Determine cloud deployment model
- Perform application and data classification
- Do vendor audits and qualifications
- Perform risk assessments and mitigate risks
- Review data security requirements
- Perform infrastructure qualifications
- Perform software validations
- Start with least critical systems
- Have fallback models in case of “de-clouding” at some point

There are different approach models. One, a phased risk based approach model was created in this thesis in chapter 7. It can be used to identify GMP significant features in software applications and in risk identification and mitigation processes.

In conclusion private cloud and public IaaS are easiest to tackle from pharmaceutical regulatory point of view. Applications can be validated and infrastructure qualification performed as required.

Off-premise SaaS, PaaS, community cloud and other “higher altitude of cloud” solutions like multi-tenant applications are a possibility but depending on implementation method they may not be in compliance with the regulations. Aspects like continuous software upgrades which affect application validation status or lack of audit trail could be directly against regulations. They may also require much more thoroughly vendor assessment and heavier risk assessment processes than simpler IaaS platforms.

There have been some signs of cloud service industry waking up to the situation (Chapter 5.7.) and a few sector specific compliance cloud types of products have been rolling onto the market. If the cloud infrastructure in itself would be qualification ready (or pre-qualified) and applications could be validated it should lower the bar for pharmaceutical industry to enter the cloud era also in SaaS solutions.

APPENDICES

Appendix 1

An interview with N.N., Director of Sales EMEA at N.N. This interview was done via Linkedin social networking site using send and receive messages function in October 2012.

To: N.N.
Date: October 15, 2012

Hi N.,

I'm doing my thesis work on Cloud computing in Pharmaceutical industry and pretty confused at the moment. I have a couple of tough questions on the matter - could I please use your expertise?

To: Ville Harjulampi
Date: October 15, 2012

Hi Ville,

No problem, I'll do my best to give you an answer! The pharmaceutical industry is quite confused on the subject at the moment but in reality it's all quite simple. Just send the questions across.

To: N.N.
Date: October 15, 2012

Hi N.,

thanks. I am familiar with the old school "server/client" type of network and application validation requirements. Especially if the software is standard off the shelf type. (Create URS, VP, protocols, validate and that's it!) Virtualization and cloud based thinking are not in itself giving me hard time - I do know the technical concepts of resources pooling, cloud service layers and how different cloud types differ. I've also been playing around with Hyper-V and VMWare solutions.

How on earth should we tackle the challange of combining GMP regulated activities, regulations and cloud computing? For instance EudraLex Vol 4 Annex 11 lists quite a few things to be taken into consideration starting from the principle "The application should be validated; IT infrastructure should be qualified".

If a pharmaceutical company would like to use outsourced, let's say ERP system which has several GMP regulated activities what would be the correct marching order? How would it document and verity compliance with Vol. 11 requirements?

Vendor assessments may bit a bit difficult to perform as well as knocking on the door of a datacenter (if you even know what's the right continent :)

Would it be the way of creating Risk Assessments, FMEAs, Impact Assessments etc. and documenting that using this and this application from cloud using a chosen service provider doesn't increase the overall risk compared to the current server/client model?

To: Ville Harjulampi
Date: October 15, 2012

Hi Ville,

This is a question that we are all trying to understand still! There are a few different ways of looking at it.

If you break down the cloud layers into IaaS, PaaS and SaaS that is the easiest method.

We then generally see a few different combinations of these in delivering services.

For example:

Internal application now hosted on IaaS (VMware or Amazon etc)
External application hosted on third party IaaS
External application hosted on application providers own infrastructure
True multi-tennant application (shared dbase etc) hosted on third party IaaS
True multi-tenant application hosted on providers own infrastructure
External application developed on PaaS (Force.com etc) where data center location is now known.

The key thing is to try and break these all down into blocks and understand where the different layers of responsibility are.

For example IaaS stops at the OS level so you would not expect to validate anything at IaaS but qualify it.

The big thing that is happening in the market at the moment is whether for example an IaaS provide qualifies the infrastructure themselves. This would great reduce the costs if there was a standardised qualification for example across all vmware IaaS providers. This would also be greatly beneficial to the Pharma companies as most of the qualification work is already done.

Providers who are looking to provide to the Pharma market understand that where the data resides is also key and that they may have to start opening the doors of thei datacenters (we do and also ensure that the data only resides in these legal jurisdictions). What we may see happening though is cloud environments becoming more expensive for specific vertical markets if for example Pharma want the cloud providers to maintain large documented audit requirements (IQ/OQ and the rest of the quality/validation docs etc.

You could write a whole these on this...

To: N.N.
Date: October 17, 2012

Hi N.,

thank you for your response. This is a very helpful view. I like the idea of breaking down to blocks and defining different responsibility layers.

I think cloud service providers have seen the need to "endorse" their platforms from regulatory point of view. For instance Microsoft claims to be in compliance with following standards and regulations for their Dynamics CRM cloud product: Safe Harbor, ISO 27001, SAS70 Type II and FISMA.

http://www.microsoft.com/online/legal/v2/?docid=27

One thing I've been thinking to evaluate a cloud service provider is the Cloud Controls Matrix (CCM) framework provided by Cloud security alliance. You may have heard about the framework which can be downloaded from their web page:
https://cloudsecurityalliance.org/research/ccm/

Microsoft has done fantastic job in evaluating their Azure against the CCM matrix requirements. They've released a document on the subject (DOC, 4MB)

http://download.microsoft.com/download/7/4/9/749DF9E9-4357-4A73-8FD8-9602B1F7A2E1/StandardResponsetoRequestforInformationWindowsAzureSecurityPrivacy.docx

Like said this is a massively big area to investigate and I hope you don't mind if I come back on the subject at some point.

To: Ville Harjulampi
Date: October 18, 2012
Hi Ville,

The main problem is that the majority of the current certs don't transfer to Pharma very well. SAS70 is just a financial snapshot and doesn't really mean anything, Safe Harbor is really about protecting against the Patriot Act but again it's just a registration process and the Patriot Act itself is a bit of a red herring.

ISO27001 one is a different standard again but it's really just procedural.

You also have the G-Cloud intiative by the UK government and the Cloud Security Alliance as you mention.

Really there needs to be a better standard for the Pharma industry to understand or a set of documents that shows the delta between the different standards.

I'll see if I can find some of the presentations from the GAMP forum event a few weeks ago. There’s some interesting info in there.

One other thing to think about is what is actually being protected. Clinical trials for example will now have people entering data in IPADS across the globe. The data is being sent across multiple network connections and geographies and there's no way to avoid this. But the data doesn't really mean anything to the end user, the value is when the data is collated and the algorithms applied. So really the only concern is at the point of computation in this case.

So if that's a central data center/cloud provider in a known location it becomes a lot easier to control.

The other key is that the cloud platforms themselves are becoming more standardised. In IaaS there is really only Xen based (Amazon), Vmware based (vCloud/vSphere) and Hyper-V (Azure). IN our area with Vmware all service providers have to adhere to the same stack build in order to be accredited by vmware to deliver the services and to ensure that the VMs can move from on premise to the vCloud seemlessly. As this becomes more standardised it is going to be a lot easier for providers to adhere to simplified "qualification" processes for their platforms. For example if you developed a set of documents that qualified our platforms they could equally be used by all other vmware vCloud providers as they use the same stack. There's a nice opportunity out there for someone to do this!

Appendix 2

This GMPIA document template represents a way of listing features of a systems´ potential GMP impact.

Finance

Function	Description	Documentation	Regulation reference	GMP impact (Yes/No)	Notes

Procurement

Function	Description	Documentation	Regulation reference	GMP impact (Yes/No)	Notes

Function	Description	Documentation	Regulation reference	GMP impact (Yes/No)	Notes

Quality Control

Function	Description	Documentation	Regulation reference	GMP impact (Yes/No)	Notes

Stock Control

Function	Description	Documentation	Regulation reference	GMP impact (Yes/No)	Notes

Function	Description	Documentation	Regulation reference	GMP impact (Yes/No)	Notes

Other Functions

Function	Description	Documentation	Regulation reference	GMP impact (yes/No)	Notes

Appendix 3

This FMEA document template represents a way of documenting mitigation of GMP significant features.

Item	Step	Acceptance criteria / range of parameter values	Failure	Cause	Effect	Controls and Detection mechanism
1						
2						
3						

Item	Severity	Occurrence	Detection	RPN	Preventative Corrective Actions	Severity	Occurrence	Detection	FINAL RPN	Notes
1										
2										
3										

REFERENCES

Assuring Life sciences compliance in the private cloud. 2011. Accessed on 22.9.2013. http://www.emc.com/collateral/software/service-overview/h7217-compliant-life-science-svo.pdf

Bittman, T. 2012. Top Five Private Cloud Computing Trends, 2012. 22.3.2012. Accessed on
22.9.2013. http://blogs.gartner.com/thomas_bittman/2012/03/22/top-five-private-cloud-computing-trends-2012/

Carstensen J., Golden, B., Morgenthal, JP. 2012. Cloud Computing, Assessing the Risks. United Kingdom: IT Governance Publishing.

Cloud Adoption Study: Cloud computing is gaining momentum. 2011. CIOnet and Deloitte. Accessed on 12.11.2013.
http://webserver2.deloitte.com.co/Consultoria/Cloud Adoption Survey.pdf

Cloud computing. 22.9.2013. An article on Wikipedia. Accessed on 22.9.2013.
http://en.wikipedia.org/wiki/Cloud_computing

Cloud computing security. 26.8.2013. Accessed on 22.9.2013.
http://en.wikipedia.org/wiki/Cloud_computing_security

Commission Decision 2000/520/EY 32000D0520. 2000. European Commission. 25.8.2000. Accessed on 22.9.2013. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML

Consensus Assessments Initiative Questionnaire. 9.1.2011. Accessed on 22.9.2013. https://cloudsecurityalliance.org/research/cai/

Cox, P. n.d. Securing data in the cloud. Accessed on 22.9.2013.
http://www.emacromall.com/techpapers/Is%20Your%20Data%20Safe%20in%20the%20Cloud.pdf

Directive 95/46/EC. 1995. European Commission. Accessed on

22.9.2013. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Essers, L. 2013. European companies should stop sending data to the US, German privacy officials say. 25.7.2013. Accessed on 22.9.2013. http://www.pcworld.idg.com.au/article/521980/european_companies_should_stop_sending_data_us_german_privacy_officials_say/

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. 2011. European Commission.

Failure mode and effects analysis. 19.9.2013. An article on Wikipedia. Accessed on 22.9.2013. http://en.wikipedia.org/wiki/Failure_mode_and_effects_analysis

Francis, S. 2013. Cloud Storage Security Controls. 25.3.2013. Accessed on 22.9.2013. http://www.cloudtweaks.com/2013/03/cloud-storage-security-controls/

Gartner outlines cloud computing strategy shapers. 2.4.2012. Accessed on 22.9.2013. http://www.cloudcow.com/content/gartner-outlines-cloud-computing-strategy-shapers

General Data Protection Regulation Proposal. 2012. European Commission. 25.1.2012 Accessed on 22.9.2013. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Gorban, A. 2013. Phased Approach to Compliant Cloud Computing. 5.6.2013. Accessed on 22.9.2013. http://www.pharmacompliancemonitor.com/phased-approach-to-compliant-cloud-computing/4987/

HIPAA Technical Safeguards. n.d. Accessed on 22.9.2013.

http://www.hipaasurvivalguide.com/hipaa-regulations/164-312.php

International Register of ISMS Certificates. 2012. ISMS International User Group. Accessed on 22.9.2013. http://www.iso27001certificates.com/

Is Symantec Online Storage HIPAA Compliant? Forum post. 12.11.2008. Accessed on 22.9.2013. http://www.symantec.com/connect/forums/symantec-online-storage-hipaa-compliant

ISO27001 Security. 2013. ISO/IEC 27002. Accessed on 22.9.2013. http://www.iso27001security.com/html/27002.html

IT risk management. 27.8.2013. An article on Wikipedia. Accessed on 22.9.2013. http://en.wikipedia.org/wiki/IT_risk_management

Karamnova, L. 13.11.2012. Software-as-a-Service Validation. PDF-document from IVT conference held on 13.11.2012.

Lassila, A. 2012. EU:n työryhmä: Pilvipalveluiden tietosuojariskit selvitettävä huolella. Helsingin Sanomat 28.8.2012.

Ludwig, S. 2011. Cloud 101: What the heck do IaaS, PaaS and SaaS companies do? 14.11.2011. Accessed on 22.9.2013. http://venturebeat.com/2011/11/14/cloud-iaas-paas-saas/

Martin, K., Perez, A. 2008. GAMP 5 Quality Risk Management Approach. Pharmaceutical Engineering May/June 2008, Vol. 28 No. 3.

Mell, B. 2011. The NIST Definition of Cloud Computing (Draft): Special Publication 800-145. Recommendations of the National Institute of Standards and Technology.

Mitchell, C. Standardizing. n.d. Privacy and security for the cloud. Accessed on 22.9.2013. http://www.chrismitchell.net/Talks/111101.pdf

New draft European data protection regime. 2012. M Patent Group. 2.2.2012. Accessed on
22.9.2013. http://www.mlawgroup.de/news/publications/detail.php?we_objectID=227

NextDocs Compliance Cloud White Paper. 2012. Accessed on 22.9.2013.
http://www.nextdocs.com/en-us/White%20Papers/Compliance%20Cloud.pdf

Rajinderkaur. 2008. Qualification Vs Validation. Forum post. 24.7.2008.
http://www.askaboutvalidation.com/forum/showthread.php?979-Qualification-Vs-Validation

Security Guidance for Critical Areas of Focus in Cloud Computing.
14.11.2011. Accessed on
22.9.2013. https://cloudsecurityalliance.org/research/security-guidance/

Sourya, B. 2011. A History of Cloud Computing. 9.2.2011. Accessed on
22.9.2013. http://www.cloudtweaks.com/2011/02/a-history-of-cloud-computing/

Stokes, D. 2012. Selecting, Qualifying and Validating Cloud Applications.
PDF-document from IVT conference held on 13.11.2012.

Top 10 cloud computing providers of 2012. 24.4.2012. Accessed 22.9.2013.
http://searchcloudcomputing.techtarget.com/photostory/2240149038/Top-10-cloud-providers-of-2012/1/Introduction

Turunen, I. 2011. Deploying FreeNEST Project Platform to an OpenStack based cloud platform: A pragmatic study into an emerging technology. B.Sc. thesis work. Jyväskylä University of Applied Sciences, Degree Programme in Software Engineering Technology, ICT. Accessed on 1.9.2012.

U.S.-EU Safe Harbor homepage. n.d. Accessed 22.9.2013. http://export.gov/safeharbor/eu/index.asp

Wang, C. 2009. Cloud Security Front And Center. 18.11.2009. Accessed on 22.9.2013. http://blogs.forrester.com/security_and_risk/2009/11/cloud-security-front-and-center.html