The Cloud, Infrastructure, Compliance and Security

Keith Williams November 13th 2014

Research Quality Association Conference
Brighton, November 2014

Formpipe.GxP Simply Compliant

RQA Research Quality Association

Agenda

- Annex 11 how do we achieve compliance?
- How do we ensure our Cloud Service Provider's adherence to the regulations?
- Web services, can we control them?
- How safe is our data?
- Some examples

What Is The Cloud?- Recap

Formpipe.GxP
Simply Compliant

- Distributed and flexible computing over a network
  - Provides the ability to run an application on many connected computers simultaneously
  - Allows Software, Platforms and Infrastructure to be sold as a service and separately dependent on need
  - Offers cost savings in hardware and infrastructure components because of scale

RQA Research Quality Association

Microsoft Partner
Gold Collaboration and Content
Gold Application Development
Gold Digital Advertising

Formpipe.GxP
Simply Compliant

RQA Research Quality Association

Annex 11, how do we achieve compliance?

What Is Annex 11?

- Eudralex, The Rules Governing Medicinal Products in the European Union, Volume 4, Good Manufacturing Practice, Medicinal Products for Human and Vetinary Use, Annex 11: Computerised Systems
  - Annex 11 of the EU GMP defines terms of reference for computerised systems used in the pharmaceutical industry.
  - Annex 11 is a checklist of non-prescriptive requirements that was adopted by the EU GMP to establish the requirements for computerised systems used in the production and distribution of medicinal products.

Annex 11 Structure

- Annex 11 consists of three sections
  - General
  - Project Phase
  - Operational Phase
- Each of these phases are further broken down into 17 sub phases- some of which will look at in detail

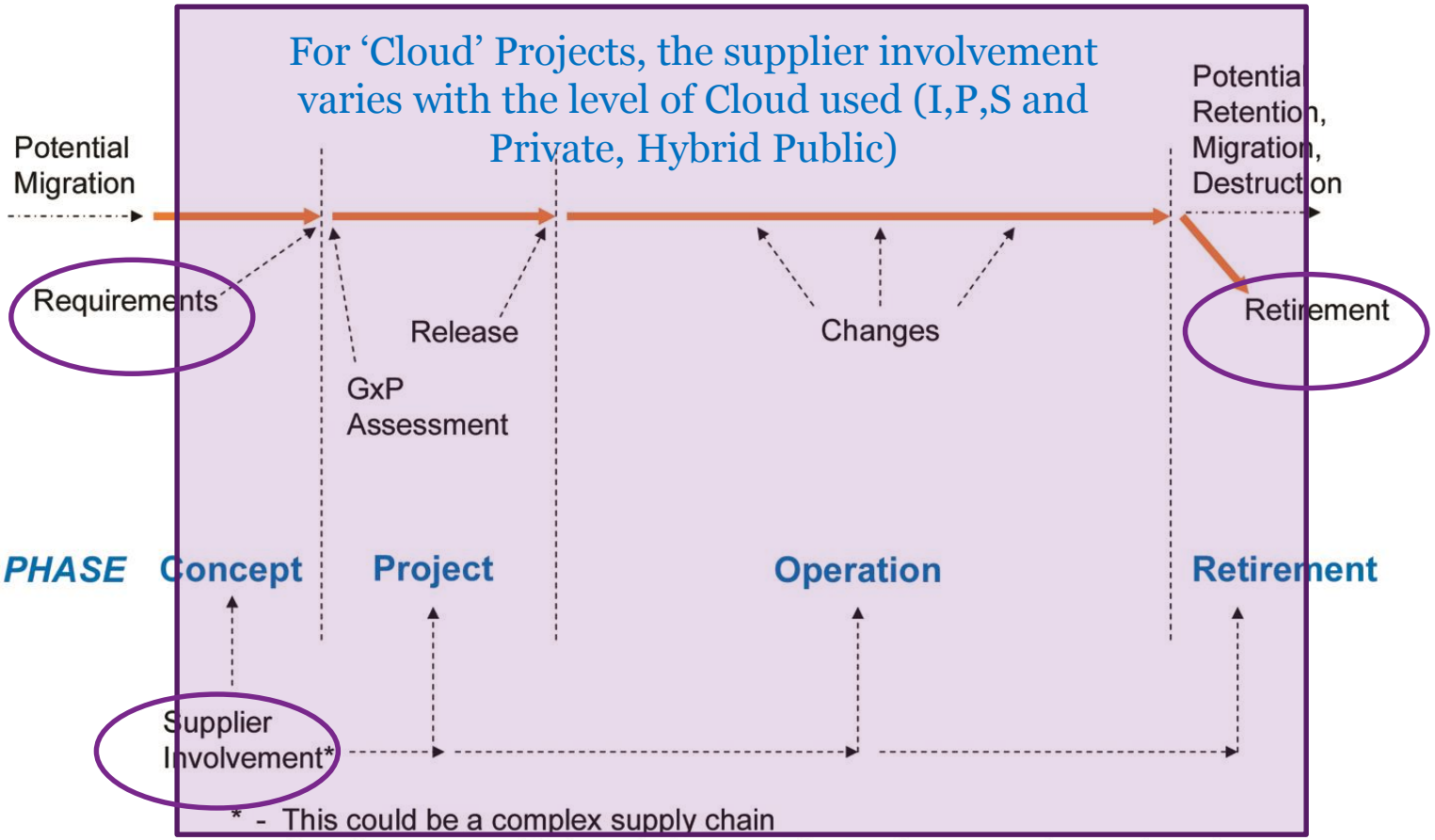
General Phase

- The General Phase contains the following sub phases:
  - Risk Management
  - Personnel
  - Suppliers and Service Providers

Project Phase

- The Project Phase contains the following sub phase:
  - Validation

Using GAMP as a structure



Source: Figure 3.2, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org.

Operational Phase

- The Operational Phase contains the following sub phases:
  - Data
  - Accuracy Checks
  - Data Storage
  - Printouts
  - Audit Trails
  - Change and Configuration Management

Operational Phase Ctd.

- The Operational Phase contains the following additional sub phases:
  - Periodic Evaluation
  - Security
  - Incident Management
  - Electronic Signature
  - Batch Release
  - Business Continuity
  - Archiving

How Do We Rationalise Annex 11 and Cloud?

- Step 1 Categorise Annex 11
  - Review the categories and sub categories in light of the following stages:
    - Vendor Selection
    - Validation & Qualification
    - Ongoing Compliance
  - This allows the requirements to be approached in manageable pieces

Step 1 Example

Formpipe.GxP Simply Compliant

Section	Subsection No	Title	Content	Cloud Control
Principle	N/A	N/A	The application should be validated; IT infrastructure should be qualified	
General	1	Risk Management	Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.	Risk Assessment to be carried out as part of selection criteria
	2	Personnel	There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.	Training records for CSPs, SLAs in place, as part of selection criteria
	3	Suppliers and Service Providers		
	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.	SLAs in place and escalation processes, including Roles and Responsibilities Ongoing Compliance
	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.	Audit based on Infrastructure GPG and CSA info Selection
	3.3		Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.	Part of application validation
	3.4		Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.	CSP should adhere to a QMS, as should the client, this will be backed up by the audit findings selection

RQA Research Quality Association

Microsoft Partner
Gold Collaboration and Content
Gold Application Development
Gold Digital Advertising

Step 2 Address the Requirements Against Annex 11

- Split the Responsibilities
  - Determine whether the Cloud Service Provider or the Cloud Customer is responsible for each requirement:

Section	Subsection No	Title	Content	Cloud Control	Customer Responsibility	CSP Responsibility
General	3.3	Suppliers and Service Providers	Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.	Part of application validation	***Implementing controls which ensure the review of documentation related to commercial off-the-self applications supporting GxP activities to verify that the system meets user requirements.*** 1 Ensuring that a procedure exists for selecting and deploying off the shelf software solutions and services which includes the verification of supplied documentation to ensure these meet user requirements.	**Ensuring the provision to the customer of sufficient documentation to allow the customer to meet this requirement.**

What is the your Cloud Service Partner Providing?

Formpipe.GxP
Simply Compliant

RQA Research Quality Association

Microsoft Partner
Gold Collaboration and Content
Gold Application Development
Gold Digital Advertising

Matrix of Split Responsibilities (partial example)

Activities: / Organisations:	Regulated Company	Software Developer	SaaS Provider	IaaS Provider
Validation Plan & Report	✓			
User Requirements & Acceptance Testing	✓			
Functional & Design Documentation		✓		
Installation Qualification			✓	
Incident Management			✓	✓
Infrastructure Qualification				✓
Operational Change Control	✓	✓	✓	✓
Periodic Review	✓			

NB: Can use separate matrices for “Project” and “Service”

Reasonable Expectations of Providers

Reasonable Expectations of Providers

- Effective Security Systems *e.g. Certified in Information Security (e.g. ISO 27001)*
- A Basic Quality System including; Change Control / Incident Management and Training. *e.g. ISO9001 is a standard for QMS.*
- Installation / Operational Qualification
- Asset Inventory
- Audit (levels involved maybe outside standard experience)

Formpipe.GxP
Simply Compliant

RQA Research Quality Association

Web services, can we control them?

How Can we secure Our Web Services?

- Because of its nature (loosely coupled connections) and its use of open access (mainly HTTP), Web services add a new set of requirements to the security landscape
- Web services security needs to include several aspects:
  - Authentication
  - Authorisation (Access Control)
  - Confidentiality (Privacy)
  - Integrity (Non Repudiation)

Web Services Credentials

- Web services security requirements must also utilise:
  - Credential mediation (Exchange of security token in a trusted environment)
  - Service Capabilities (What a Web service can and cannot do)
  - The use of Public Key Infrastructure (PKI)
  - The use of Transport Level Security to protect the communication between the Web service user and the Web service provider
  - Message Level Security to ensure confidentiality by digitally encrypting messages, and using digital signatures

Formpipe.GxP
Simply Compliant

RQA Research Quality Association

How safe is our data?

How Safe is Our Data?

Formpipe.GxP
Simply Compliant

- When data is stored in the cloud, we need to be aware of:
  - Data Location
  - Co-mingled data
  - Data ownership
  - Audit record protection
  - Data erasure
  - Data modification of quality records

RQA Research Quality Association

Microsoft Partner
Gold Collaboration and Content
Gold Application Development
Gold Digital Advertising

How Safe is Our Data? (cont)

- Data Location
  - Do you know where your data is?
  - Have you control over it ?
- Co-Mingled Data
  - Are you sharing resources with other customers?
  - Can other customers access or manipulate your data?

Conclusions

- We have covered:
  - Compliance with Annex 11
  - Cloud providers responsibilities and expectations of them
  - Web service controls
  - Data security
- This can all be achieved, by due Diligence (Audit), the CSP and customer interaction, and the use of managing the CSP on an ongoing basis
- Now a couple of examples

Formpipe.GxP
Simply Compliant

RQA Research Quality Association

Some real examples of Regulated Companies in the cloud

Example 1

- New “virtual” Pharma company using hosted SaaS for document management.
- Software Product highly configurable (as distinct from customisable) to meet client requirements
- Specialised software developer / SaaS provider with auditable development documentation ready for Pharma clients.
- Extensive auditing carried out
- IaaS provider used for actual hosting, audited by the SaaS provider

Example 1- Lessons Learned

- Niche service providers do understand needs of Pharma Clients, and expect to be audited as part of supplier selection.
- SaaS provider can take on responsibility to audit and manage the IaaS provider, including Infrastructure and Installation Qualification.
- Suppliers need to be pragmatic when faced with multiple opinions on compliance details from different clients.
- Configuration needs to be managed carefully by the SaaS provider, with maximum input from actual users.

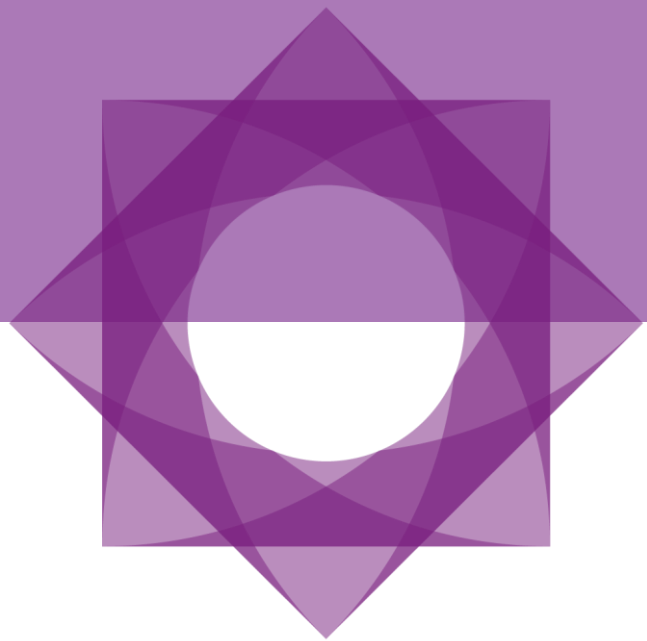
Example 2

- Large Pharma Company using new software from developer new to Pharma industry.
- System not required to hold GxP data now, but could do so in future, hence agreed to validate.
- Potentially includes intellectually property data
- Software Developer offering SaaS, via a separate IaaS provider.
- Small number of users, but global, web-based access required.
- Both suppliers were audited by the Regulated Company

Example 2 Lessons Learned

- The developer / SaaS provider needed educating e.g. in how to write Test Plan and Test Scripts, but were keen to learn.
- The IaaS provider were not eager to produce e.g. IQ documentation, due to small volume of data / business as seen from their viewpoint
- Performance Testing proved difficult – e.g. “it’s running slowly”, but whose responsibility is it to determine where the problem lies, and to resolve it?
- Security aspects were addressed well by the Regulated Company via in-house knowledge, included “ethical hacking”.

Thank you for listening.



Formpipe.GxP
Simply Compliant