Computer Systems Validation

But not as you know it

**SeerPharma**®
CONFIDENCE IN COMPLIANCE

Brief History of Computer Systems

- **2400 BCE** Abacus in Babylon

- **1185~1005 BCE** Abacus in Zhou Dynasty China

- **500 BCE** Abacus in Ancient India

- **1822** First mechanical computer – Charles Babbage England

- **1911** IBM founded from merger of several companies USA

- **1939** First electronic digital computer Atanasoff-Berry Computer (ABC) USA

- **1940** First programmable digital computer (Colossus) UK

- **1955** Computer Usage Company (CUC) first company to sell software USA

- **1972** SAP founded; 1975 Microsoft founded; 1976 Apple I built; 1977 Oracle developed; 1979 first spreadsheet

- **1989** Microsoft Office

- **1991** Linux; 1991 WWW; 1996 mini-computers; Nokia phone with internet

- **2000** Dot-Com burst; 2007 iPhone; 2007 Big Data; 2010 Tablet computing; 2012 Wearable Technology

- **2006** "Cloud computing" term introduced by Google in a modern context

- **2016** Intel: "The End of Moore's Law" (started 1970)

- **2018** To be landmark year for Augmented Reality

SeerPharma®
CONFIDENCE IN COMPLIANCE

Brief History of Computer Systems Validation

- **1983** – FDA first Guideline on CSV "Blue Book"

- **1991** - EU GMP Annex 11, FDA started on 21 CFR Part 11

- **1997** – FDA CFR Part 11 finalised

- **1998** – GAMP 3 released

- **2001** - FDA issue Part 11 Guidance on Validation, GAMP 4 released

- **2002** - FDA issue "General Principles of Software Validation" Guidance (commensurate with risk posed)

- **2003** - FDA issue Part 11 Guidance on Scope and Application

- **2007** – PIC/S Guidance Good Practices for Computerised Systems in Regulated "GXP" Environments

- **2008** – GAMP 5 released (risk based approach)

- **2011** - EU Annex 11 updated (risk management to be applied)

- **2016** – ISO 13485:2016 (new requirements specifically on software validation)

- **2018** – TGA adopt new PIC/S Annex 11 (better use of quality risk management principles)

- **2018** – ISPE and ISACA (collaboration on cybersecurity guidance – 'Security Categories')
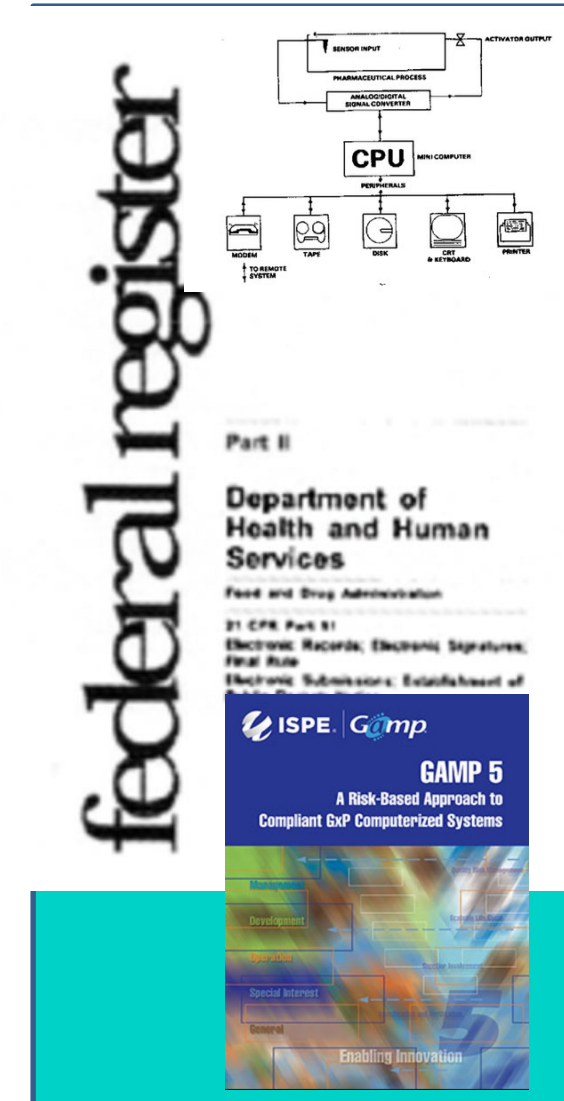
Computer Systems have been around a long time

**Computer Systems validation not really new requirement**

Validation activities should be commensurate with the complexity of the software design and **the risk associated with the use of the software for the specified purpose**

Validation Burden

- Software Validation can be a huge burden on companies

  - No manpower, no time, no experience

- Validation journey may appear to be a hard nut to crack

  - So we look to making the journey faster, less cumbersome, less expensive

- Our understanding of how to validate has been shaped by FDA CFR Part 11, Annex 11 and ISPE GAMP industry guidance

  - the 'traditional' approach

  - QA at ease with it

- GAMP 5: "A Risk-based Approach to Compliant GxP Systems" offers..

  - A good practice framework for demonstrating systems are "fit for intended use"
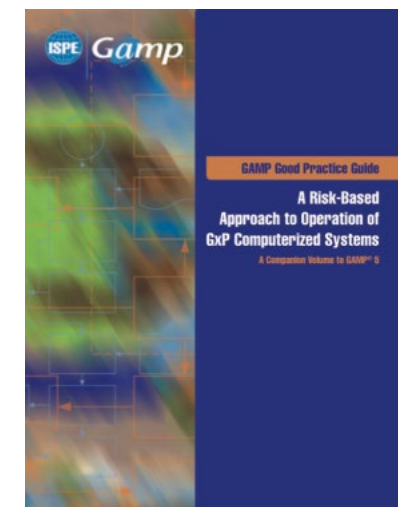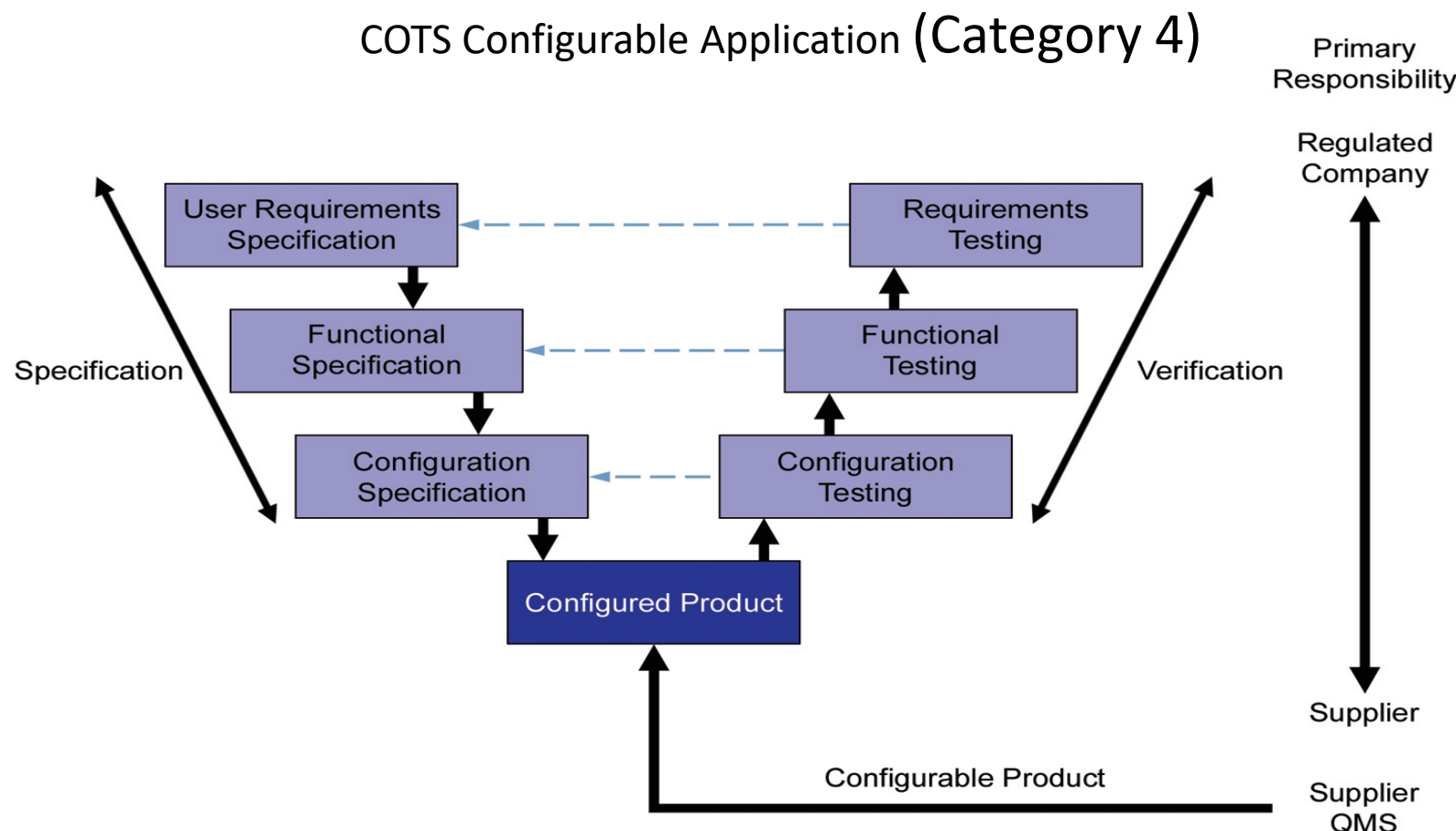
SeerPharma®
CONFIDENCE IN COMPLIANCE

The 'Traditional' Validation Approach

COTS Configurable Application (Category 4)

Source: Figure 4.3, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org.

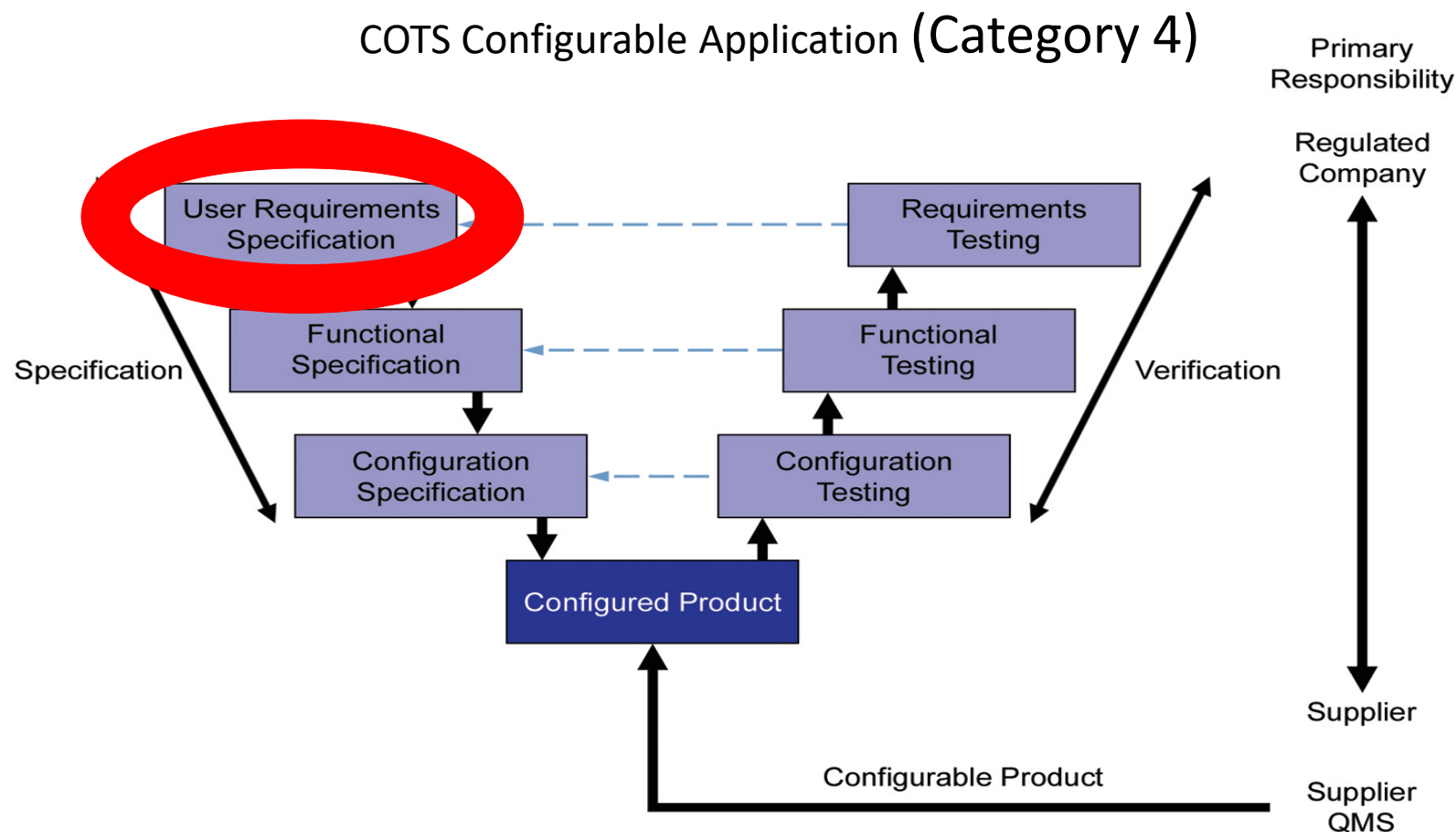# The 'Traditional' Validation Approach - Requirements

COTS Configurable Application (Category 4)

Source: Figure 4.3, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org.

User Requirements - background

- How many times have you seen projects in trouble with URS development?

- URS sent out as RFT

  - out of the box, configured, customized

- Recall additional effort and risk for validating customized systems

  - companies then refine requirements and plan to change their practices.

- Remember testing will be verified against requirements.

- Most test failures due to poor wording in test scripts

- Importance of URS being accurate

SeerPharma®
CONFIDENCE IN COMPLIANCE

User Requirement Specification

URS ID	Description	FRS Reference #
URS-EDMS-0012	The EDMS Interface shall have the provision for the capability for the control of user access / distribution to Work-In-Process (Draft), Approved (Released) and Inactive (Archived / Obsolete) metadata records within the systems application.	Portal v11.6x FRS • Section 4 • Section 8
URS-EDMS-0013	The EDMS Interface shall have the provision for approval of the new child revision /version and the automated replacement of the original parent version of the metadata record and associated file attachments as the main active distributed record. Inactive / Obsolete revisions shall be moved to an Archived status for purposes of viewing and storage access.	Portal v11.6x FRS • Section 8
URS-EDMS-0014	The EDMS Interface shall have the provision for moving out-of-date or obsolete metadata records into an archived status using a pre-defined approval routing workflow.	Documents v11.6x FRS • Section 2
URS-EDMS-0015	The EDMS Interface shall have the provision for escalating overdue tasking to assigned authorized users upon task timing expiration.	Documents v11.6x FRS • Section 2
URS-EDMS-0016	The EDMS Interface shall have the provision to track a metadata records status throughout the document lifecycle. This should include the data and status relating to creation, approval, editing, modification, change control actions, viewing actions, printing actions and record audit trail data.	Portal v11.6x FRS • Section 1
URS-EDMS-0017	The EDMS Interface shall have the provision for the capability to report the EDMS metadata including but not limited to: record action tracking, record approval history, user level approval report, record audit reporting, checked out record status, hard	Portal v11.6x FRS • Section 3 Analytics v11.6x FRS

URS to FRS Traceability

FRS ID	Description	Test Trace #	Feature Risk
5.3.1.2	A user can abort a form that they have launched as long as the form is still on the first step and no sign-off has occurred (either by another user or by the user signing off as work in process). They can abort directly from their My Tasks page.	PRC 6.1	
5.3.1.3	Users click on the data entry icon to complete a form or the approval icon to approve form data. PDF and HTML forms have unique data entry and approval icons. In the case of PDF forms, clicking on the data entry or approval icon launches either Adobe Reader or Acrobat (depending on what is installed on the user's machine). With HTML forms, clicking on either icon launches the form in the default browser.	PRC 6.1	
5.3.1.4	Auto-Save: When filling out an HTML form, the system will automatically save the data in accordance with the Autosave Interval selected in the route properties. A message box will appear indicating that the form has been auto-saved. In Tracking, an Auto-Save event will be shown with a status of Auto Save until the user signs off on the task.	PRC 3.1	
5.3.1.5	On HTML forms, a user is warned of potential data loss and the form lock is removed when navigating away from the form without initiating a signoff.	PRC 3.1	
5.3.2	Form Signoff		

URS ID	Description	FRS Reference #
URS-EDMS-0012	The EDMS Interface shall have the provision for the capability for the control of user access / distribution to Work-In-Process (Draft), Approved (Released) and Inactive (Archived / Obsolete) metadata records within the systems application.	Portal v11.6x FRS • Section 4 • Section 8
	The EDMS Interface shall have the provision for approval of the new child revision /version and the automated replacement of the original parent version of the metadata record and associated file attachments as the main active distributed record. Inactive / Obsolete revisions shall be moved to an Archived status for purposes of viewing and storage access.	Portal v11.6x FRS • Section 8
	The EDMS Interface shall have the provision for moving out-of-date or obsolete metadata records into an archived status using a pre-defined approval routing workflow.	Documents v11.6x FRS • Section 2
	[The] EDMS Interface shall have the provision for escalating overdue tasking to assigned [a]uthorized users upon task timing expiration.	Documents v11.6x FRS • Section 2
	[Th]e EDMS Interface shall have the provision to track a metadata records status [thro]ughout the document lifecycle. This should include the data and status relating to [crea]tion, approval, editing, modification, change control actions, viewing actions, [viewin]g actions and record audit trail data.	Portal v11.6x FRS • Section 1
	[ED]MS Interface shall have the provision for the capability to report the EDMS [da]ta including but not limited to: record action tracking, record approval history, [lev]el approval report, record audit reporting, checked out record status, hard	Portal v11.6x FRS • Section 3 Analytics v11.6x FRS

SeerPharma®
CONFIDENCE IN COMPLIANCE

The 'Traditional' Validation Approach - Testing

COTS Configurable Application (Category 4)

Source: Figure 4.3, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org.

Automated Test Results

FRS ID	Description	Test Trace #	Feature Risk
5.3.1.2	A user can abort a form that they have launched as long as the form is still on the first step and no sign-off has occurred (either by another user or by the user signing off as work in process). They can abort directly from their My Tasks page.	PRC 6.1	
5.3.1.3	Users click on the data entry icon to complete a form or the approval icon to approve form data. PDF and HTML forms have unique data entry and approval icons. In the case of PDF forms, clicking on the data entry or approval icon launches either Adobe Reader or Acrobat (depending on what is installed on the user's machine). With HTML forms, clicking on either icon launches the form in the default browser.	PRC 6.1	
5.3.1.4	Auto-Save: When filling out an HTML form, the system will automatically save the data in accordance with the Autosave Interval selected in the route properties. A message box will appear indicating that the form has been auto-saved. In Tracking, an Auto-Save event will be shown with a status of Auto Save until the user signs off on the task.	PRC 3.1	
5.3.1.5	On HTML forms, a user is warned of potential data loss and the form lock is removed when navigating away from the form without initiating a signoff.	PRC 3.1	
5.3.2	Form Signoff		

1 Failed Tests (0.33%)

Filter

Test Case & Workflow	Requirements	Test Details	Links
S-04304 - Test stamping document with multi select custom field data	18.4 The advanced document properties for the main file of InfoCards containing multi-select custom data fields display each of the chosen multi-selected values delimited by a comma.	Client: SQAVALID01 Date/Time of Results: 1 Jun 2018 12:33 AM VersionOne Defect: N/A Failure Status: Closed Failure Cause: Test Site Misconfigured Failure Resolution: Deleted the un-stamped version of the file on the client machine.	View Test Video View Change History

304 Passed Tests (99.67%)

Filter

Test Case & Workflow	Requirements	Test Details	Links
64135 - Test exporting infocard and folder with invalid windows file name characters in the names	9.33.7 When users export InfoCards with titles containing illegal Windows characters, the system replaces the illegal characters with a valid character.	Client: SQAVALID01 Date/Time of Results: 31 May 2018 5:22 AM	View Test Video

SeerPharma®
CONFIDENCE IN COMPLIANCE

Vendor has done good work – why not use it?

- Developer writes code and develops unit tests per defined specifications

- Developer peer code review

- Automated unit testing

- Unit integration testing

- End-to-end ("e2e") testing

  – Entire systems tested as a 'black box'

  – Simulated user in a 'sandbox' environment

- **Vendor may provide us with the equivalent of OQ testing and traceability to product and configuration testing**

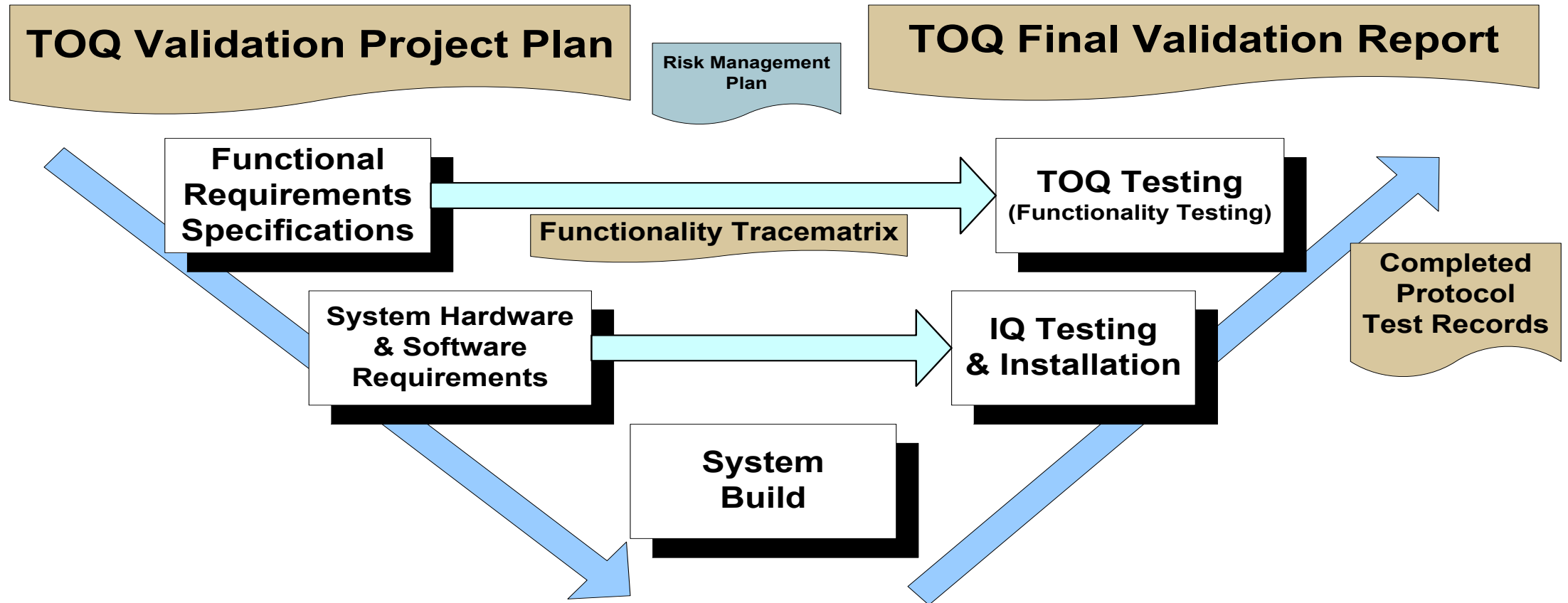- **No value is added by the user repeating this in their usage testing**

SeerPharma®
CONFIDENCE IN COMPLIANCE

Product and Configuration Validation

FRS ID	Description	Test #	Result
3.3	The native file for the document associated with a Line Item, can be viewed.	S-03648_23	PASS 6950, 7033
3.4	The InfoCard for the document associated with a Line Item, can be viewed.	S-03648_13	PASS 6950, 7033
3.5	Task Tracking for a document launched on a current task can be viewed.	S-02330	PASS 6950, 7033
3.6	Line Items configured for document upload allow users to browse to and upload a file.	S-03648_13	PASS 6950, 7033
4	**Line Item Tasks**	---	---
4.1	An Add Document task can be launched for an individual Line Item if the Line Item is configured for document upload.	S-03648_2	PASS 6950, 7033
4.2	Add Document tasks can be launched for a whole section at any level.	S-03648_27	PASS 6950, 7033
4.3	A task notification email is sent to the user assigned to the Line Item.	S-02489	PASS 6950, 7033
4.3.1	The link in the notification email opens the Line Item Detail view.	S-02489	PASS 6950, 7033
4.3.1.1	If the task is no longer valid, users are notified and cannot navigate to the Line Item Detail view.	S-03648_15	PASS 6950, 7033
4.4	Internal users receive Line Item tasks in My Tasks.	S-03648_2	PASS 6950, 7033
4.4.1	The task allows users to open the Line Item Detail view.	S-03648_2	PASS 6950, 7033
4.5	Internal users complete the task by uploading a file or linking an InfoCard for the Line Item.	S-03648_11	PASS 6950, 7033
4.6	External users complete the task by uploading a file.	S-03648_21	PASS 6950, 7033
	Tasks completed by a user other than the assignee are aborted.	S-03648_15	PASS 6950, 7033
4.6.1	Deleting a Line Item aborts any related tasks.	S-03648_9	PASS 6950, 7033
4.6.2	Changing the Assignee on a Line Item aborts any related tasks.	S-03648_19	PASS 6950, 7033
5	**Cloning Within a Checklist**	---	---
5.1	The Structure of any section can be cloned.	S-03648_7	PASS 6950, 7033
5.1.1	The Structure of an individual Line Item can be cloned.	S-03648_7	PASS 6950, 7033
5.1.2	When an item is cloned, the system creates a duplicate, consisting of all contained sections and Line Items.	S-03648_7	PASS 6950, 7033

SeerPharma®
CONFIDENCE IN COMPLIANCE

Some Definitions

- TOQ : An OQ conducted at the vendor site on a representative customer system. The TOQ is then **transferred** (the "T" part of the TOQ) to the customer's site using a **review and risk assessment** to identify the risk of any intended feature sets and determine if any further testing needed to ensure a valid transfer for the specific customer.

  - *OQ protocols are the "nitty gritty" functional testing (e.g. the save button saves and the cancel button cancels).*

- TPQ : A product that vendor produces that tests the best practice configuration usage scenarios for the standard configured modules.

Transfer OQ

TOQ Validation Project Plan

Risk Management Plan

TOQ Final Validation Report

Functional Requirements Specifications

Functionality Tracematrix

TOQ Testing
(Functionality Testing)

Completed Protocol Test Records

System Hardware & Software Requirements

IQ Testing & Installation

System Build

SeerPharma®
CONFIDENCE IN COMPLIANCE

Risk Assessment: MasterControl Example

- Regulators expect that the regulated client can explain the risk analysis and variables used

- *Initial Risk = Software Risk + Client Risk*

  - *Software Risk = (Conformance to Standard Configuration + Impact of Failure) – TOQ Testing*

  - *Client Risk = (Variation from Best Practice + Regulatory Impact + Client Assessment) – Usage (TPQ) Testing*

- If the system's risks are low, the recommendation is to leverage the MasterControl documentation of internal testing.

- If the risks are high, the recommendation will be to do additional client specific testing.

Risk Assessment: MasterControl Example

- **Client Risk Assessment** - How do you assess the risk of this component, given your configuration?

- **Impact of Failure** - To what degree would a failure of this component prevent standard usage of the system?

- **TOQ Testing** - To what degree was this component tested during MC System Functional Testing (TOQ)?

- **Conformance to Best Practices** - To what degree is this component included in the MC Best Practice (Standard) configurations?

- **Regulatory Sensitivity** - To what degree is the component used to comply with your regulatory requirements?

- **Software Risk** - What degree of risk does MC assess for the component from a software perspective?

- **TPQ Testing** - To what degree was this component tested during MC System Usage Testing (TPQ)?

- **Variation from Best Practices** - To what degree is your configuration of this component different from MC Best Practices?

SeerPharma®
CONFIDENCE IN COMPLIANCE

Risk Assessment: MasterControl Example

(Part of Best Practice + Impact of Failure) - (OQ Testing) = Software Risk

Low	(-3 - 1)
Med	(2 - 5)
High	(6 - 9)

(Regulatory Sensitivity + Variation from BP + Client Risk Assessment) - (TPQ Testing) = Client Risk

Low	(-2 - 3)
Med	(4 - 9)
High	(10-14)

Software Risk + Client Risk = Overall Risk Score

Score (-6 - 11)	No
Score (12-28)	Yes

SeerPharma®
CONFIDENCE IN COMPLIANCE

Component	Software Risk	Variation from Best Practices	Regulatory Sensitivity	Client Risk Assessment	Tested in TPQ	Client Risk Score	Overall Risk Score	Client Usage Testing Recommended
Approval Route	Med (5)	Low (2)	High (4)	Low (2)	High (5)	Low (3)	Low (8)	No
Change Request Step	Med (5)	Low (1)	Low (1)	Low (1)	High (5)	Low (-2)	Low (3)	No
Collaboration	Med (5)	Low (1)	Low (1)	Low (1)	High (5)	Low (-2)	Low (3)	No
Controlled Copies	Low (-1)	N/A (0)	N/A (0)	Low (1)	Low (1)	Low (0)	Low (-1)	No
Copies	Low (-1)	Low (1)	Low (1)	Low (1)	Low (1)	Low (2)	Low (1)	No
Document connections	Low (-3)	N/A (0)	N/A (0)	Low (1)	Low (1)	Low (0)	Low (-3)	No
Document connections email	Low (-3)	N/A (0)	N/A (0)	Low (1)	Low (1)	Low (0)	Low (-3)	No
Document Reports	Low (1)	Med (3)	Low (2)	Low (3)	Med (3)	Med (5)	Low (6)	No
Document Retention	Low (-3)	N/A (0)	N/A (0)	Low (1)	Low (1)	Low (0)	Low (-3)	No
Document Retention Configuration	Low (-1)	N/A (0)	N/A (0)	Low (1)	Low (1)	Low (0)	Low (-1)	No
Documents	Med (5)	Low (1)	Med (3)	Low (1)	High (5)	Low (0)	Low (5)	No

Best Practices

- Assess and accept your software supplier's documentation

- Include your supplier's testing in your validation package

- Follow the best practice configurations outlined by your supplier

- Assess your specific configuration for risk-based validation

- Focus on validating your critical business processes

- Establish a risk-based approach to your testing

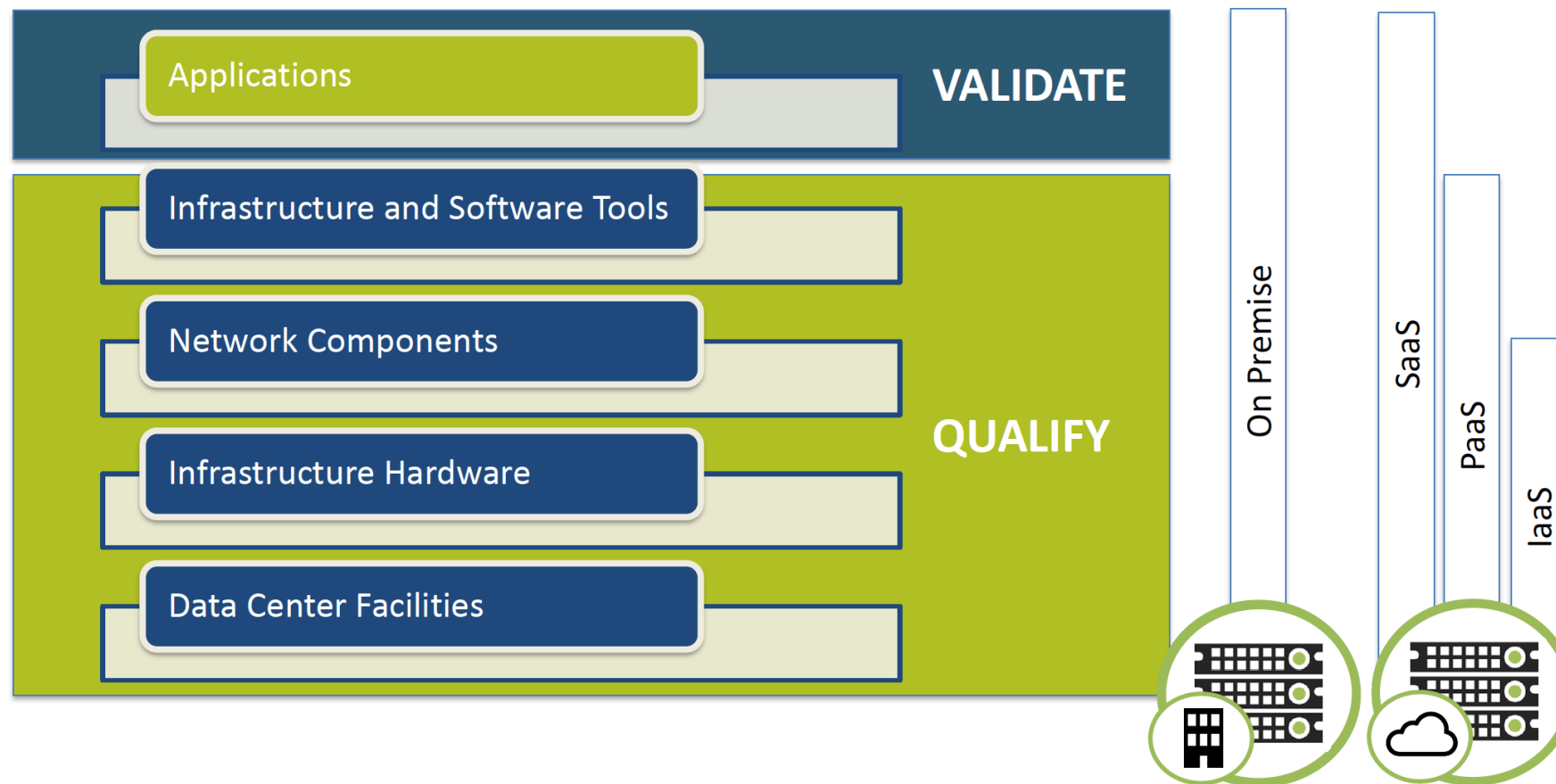# Cloud and Validation

Can Cloud Systems be Validated?

- Yes cloud applications can be validated

  - it is all about managing control and risk

  - However there are unique processes

  - Changes required to the *validation puzzle*

- Some companies are in a frozen state with an on premise system because of the cost of doing validation

- Cloud solutions come along with more regular updates and more frequent validation

- How to align these practices with the classical GAMP, FDA principles and PIC/S requirements?

SeerPharma®
CONFIDENCE IN COMPLIANCE

Validation in the Cloud

Applications

VALIDATE

Infrastructure and Software Tools

Network Components

QUALIFY

Infrastructure Hardware

Data Center Facilities

On Premise

SaaS

PaaS

IaaS

SeerPharma®
CONFIDENCE IN COMPLIANCE

We need to shift to Continuous Validation

Continuous Validation is …

- knowing the system state is up to date at all times without **Freezing** it in time

  – Reduces risks of data/privacy breach and cyber attacks

- **continuously testing**

  – with emphasis on high risks linked with interruption of services

  – (e.g. user access and audit trails)

- being proactive in relation to the upcoming changes from the cloud vendor

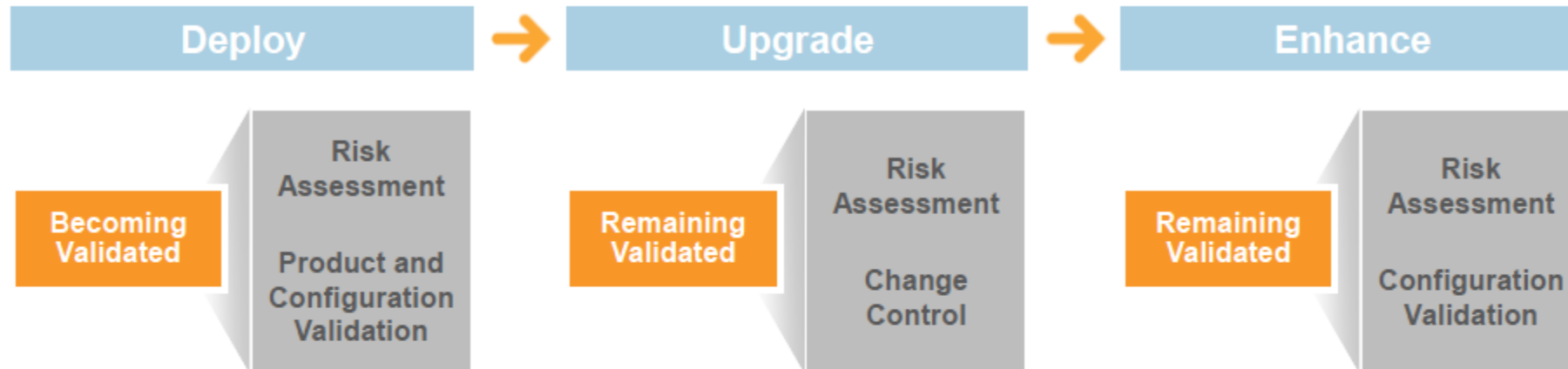- having the processes in place for system governance

Classic View
System Freeze
and Change
Control

Cloud View
Continuous
Change &
Improvements

SeerPharma®
CONFIDENCE IN COMPLIANCE

Phases in Validation of Cloud Systems

Deploy	→	Upgrade	→	Enhance

Deploy

| Becoming Validated	Risk Assessment Product and Configuration Validation

- Similar to traditional on-premise validation efforts
- Collaboration between vendor and customer required for success

Upgrade

Remaining Validated	Risk Assessment Change Control

- Biggest area of difference
- Vendor communication and maturity required for success

Enhance

Remaining Validated	Risk Assessment Configuration Validation

- Similar to traditional on-premise validation efforts
- Determined by customer requirements
- Implemented on customer schedule

SeerPharma®
CONFIDENCE IN COMPLIANCE

Cloud – Based Environment Management

Source: Microsoft Faculty Connection
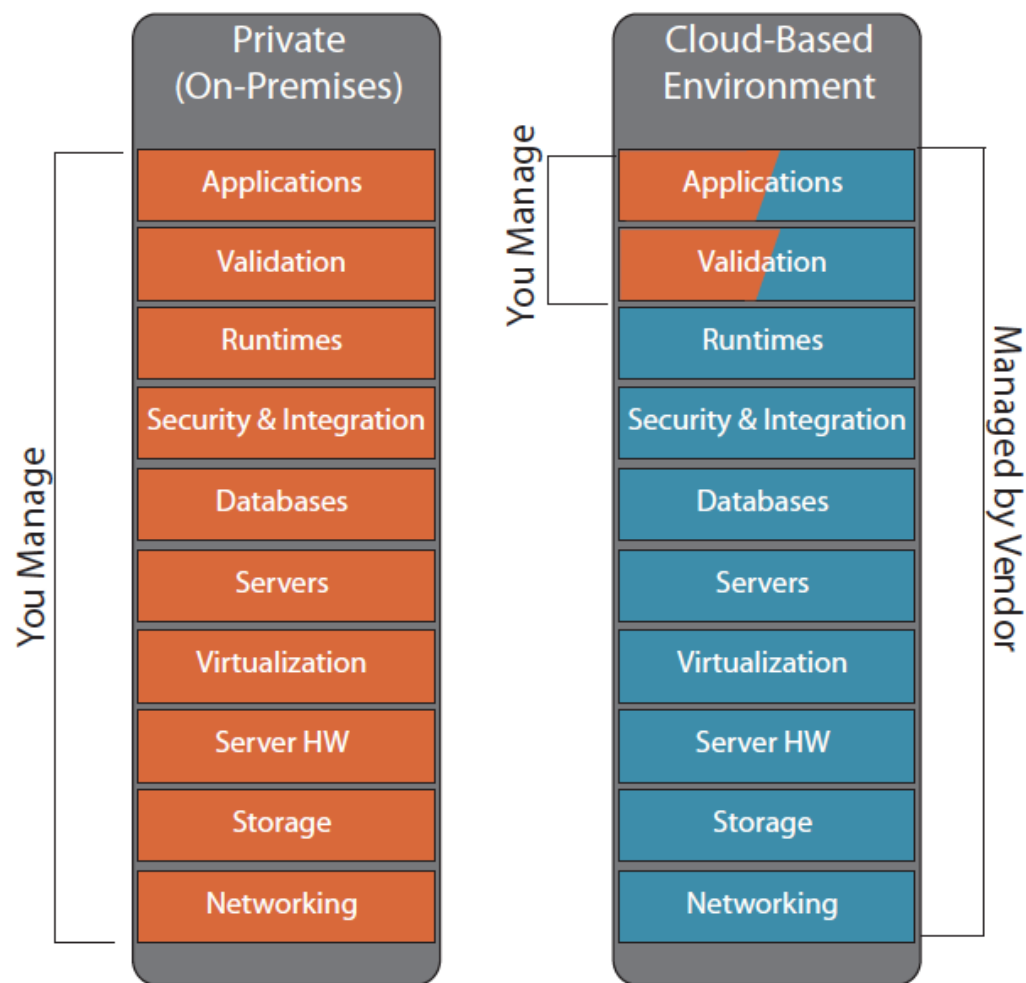
Evaluating a Cloud Provider

- Cloud uptime and performance

- Cloud Security and segregation of instances

- Notification processes and downtimes

- Data backup and recovery systems

- Business continuity systems (and testing of it)

- Controls to secure data between client and provider

- Network management

SeerPharma®
CONFIDENCE IN COMPLIANCE

Processes Required for Infrastructure Qualification
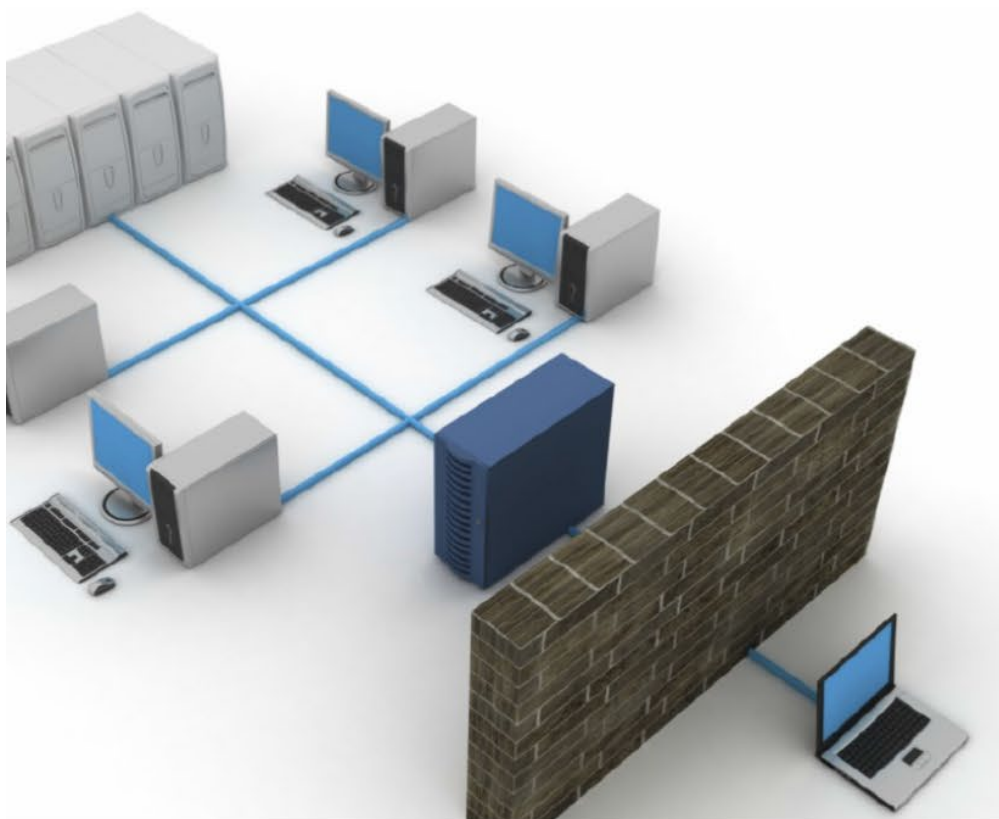
Change Management

Configuration Management

Security Management

Server Management

Client Management

Network Management

Problem Management

Help Desk (Service Desk ITIL)

Backup, Restore and Archiving

Disaster Recovery

Performance Monitoring

Supplier Management

SeerPharma®
CONFIDENCE IN COMPLIANCE

Do we Audit the Cloud Provider?

- It depends!

- Audit the software supplier and if they are using AWS or MS Azure then perform your own review of their information ISO/SOC Audit reports so you can say…

"Extensive controls that are implemented as part of internal Azure / AWS development, security, and quality practices help to ensure that the Azure / AWS platform meets its specifications and is maintained in a state of control and compliance. These processes and controls are audited and verified on a continuous basis by qualified third-party accredited assessors more versed in expertise that ACME could provide for vendor assurance".

Evaluating a Cloud Provider

- As part of their comprehensive compliance offering Microsoft Azure regularly undergoes independent audits performed by qualified third-party accredited assessors for :
  - ISO (27001, 27017, 27018 & 9001)
  - SOC (1, 2, 3)
  - Health Information Trust Alliance (HITRUST)
  - US Federal Risk and Authorization Management Program (FedRAMP)
  - Payment Card Industry (PCI)
- Although there are no certifications specifically for GxP compliance, the above certifications and attestations have many similarities with the controls required to meet regulatory requirements, such as those stipulated in the FDA's 21 CFR Part 11 and PIC/s Annex 11.

Microsoft Azure GxP Guidelines

Microsoft

SeerPharma®
CONFIDENCE IN COMPLIANCE

Processes Required for Infrastructure Qualification

FDA CFR Part 11

U.S. FDA 21 CFR Part 11	
Sec. 11.10 Controls for closed systems.	ACME / Microsoft responsibilities
11.10 (d) Limiting system access to authorized individuals.	ACME responsibilities Establish appropriate logical security processes governing the administration of system users/administrators to ensure segregation of duties and assignment of permissions according to the principle of least privilege. Verify control mechanisms for limiting access are properly configured. Implement periodic review of assigned access rights. Microsoft responsibilities Physical and logical security policies are in place to limit access to authorized individuals based on the individual's job duties. (Refer to SOC 2 Report Controls: CC5.1- CC5.8, CC6.2, DCS-02, IAM-01 to IAM-13, IVS-08, STA- 01).
11.10 (e) Use of secure, computer-generated time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	ACME responsibilities Verify that any GxP system generates secure audit trails as required by predicate rules for regulated electronic records. Implement appropriate security controls to restrict access to regulated audit trail data, for example, that audit trail functionality cannot be disabled. Ensure that data backup processes are in place and have been tested for applicable audit trail data. Establish record retention policies that include relevant audit trail data. Microsoft responsibilities Azure has established an Audit Log Management policy. Access to the log is restricted to authorized individuals (Refer to SOC 2 Report Controls: IVS-01). Security controls to protect cloud services and infrastructure are implemented (Refer to SOC 2 Report Controls: TVM-02). Controls are in place to oversee service of data backup or mirroring (Refer to SOC 2 Report Controls: CC5.5, CC5.7, A1.2, A1.3, PI1.1, PI1.4).
11.10 (f)	ACME responsibilities

SeerPharma®
CONFIDENCE IN COMPLIANCE

Processes Required for Infrastructure Qualification

PIC/S Annex 11

PIC/S Annex 11	
3. Suppliers and Service Providers	**ACME / Microsoft responsibilities**
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.	ACME responsibilities Review the most recent Microsoft Azure ISO and SOC audit reports produced by independent third-party organizations and document the results of the assessment as necessary based on internal processes. Ensure that supplier/vendor assessment information is available to inspectors when requested. Microsoft responsibilities Microsoft provides customers with access to audit information related to the internal quality system and secure development-related processes via the Service Trust Platform (STP) (Refer to SOC 2 Report Controls: AAC-01 – AAC-03)
4. Validation	
4.1 The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.	ACME responsibilities Implement a formal computer system validation policy or procedure that conforms to the specified requirements. Perform and document the qualification/validation of GxP system(s) hosted within Microsoft Azure based on a risk assessment. Microsoft responsibilities Procedures and controls are in place to ensure the Azure platform is developed and tested in accordance with industry best practices and standards (for example, ISO 9001 and ISO/IEC 27001) to ensure quality and security as well as consistent and reliable performance. (Refer to SOC 2 Report Controls: CC4.1, CCC-01, STA-03, CC7.1 to CC7.4). Risk management is incorporated into processes around the development and maintenance of the Microsoft Azure platform (Refer to SOC 2 Report Controls: CC1.2, CC3.1, CC3.2, BCR-06, BCR-09, DSI-02, CCC-05, GRM-02, GRM-04, GRM-08, GRM-10, GRM-11, HRS-02, IAM-05, IAM-07, IVS-04, STA-01, STA-05, STA-06, TVM-02).

SeerPharma®
CONFIDENCE IN COMPLIANCE

Summary

- Software validation historically been difficult and time intensive.

- New COTS – choose the supplier carefully

- Leverage software supplier documentation

  - OQ and maybe PQ with risk assessment

- Accept cloud supplier best practices in IS governance

- Have a strong SLA in place with cloud-provider

- Revise your CSVMP and SDLC procedures for the paradigm shift of classic to cloud validation

- You can adopt cloud solutions and upgrade frequently and lighten the validation load focussing attention on critical areas that can impact your software usage and regulatory requirements

SeerPharma®
CONFIDENCE IN COMPLIANCE

Summary

The cumbersome practices of "traditional" validation are not true traditions.

They are old habits that can be changed with the right mindset, tools and strategy.

SeerPharma®
CONFIDENCE IN COMPLIANCE