Data Integrity and Quality Culture Virtual Symposium 21st May 2020

Data Integrity - Will the Cloud Reign?

Paul Kerr
Partner

SeerPharma®
CONFIDENCE IN COMPLIANCE

Agenda

- Setting the context
- Cloud put simply
- DI and the cloud
- Cloud Deployment
- Risks, Responsibilities and Controls
- Myths and Reality
- Validation – change approach?
- Auditing Cloud Providers
- Wrap-up and Q&A

In The Beginning…

- **2400 BCE** Abacus in Babylon
- **1822** First mechanical computer – Charles Babbage England
- **1911** IBM founded from merger of several companies USA
- **1940** First programmable digital computer (Colossus) UK
- **1955** Computer Usage Company first company to sell software
- **1972** SAP founded; 1975 Microsoft founded; 1976 Apple I built; 1977 Oracle developed; 1979 first spreadsheet
- **1989** Microsoft Office
- **1991** WWW; 1996 mini-computers
- **2006** “Cloud computing” term introduced by Google in a modern context
- **2007** iPhone; 2010 Tablet computing; 2012 Wearable Technology
- **2020** To be landmark year for Augmented Reality

What Is Cloud Computing?

“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

NIST SP-800-145

Or put simply, Cloud Computing is …
a utility purchased to deliver computing and storage resources **As A Service** to end-users over a network

Cloud Adoption Since 2006

- Despite promises of efficiencies and flexibility there is slow adoption of cloud solutions in our regulated space.
- Why? The dilemma of innovation versus compliance (FUD factor).
- Our understanding of how to operate has been shaped in the past based on FDA CFR Part 11 and EU or PIC/S Annex 11
- Outcome was that with a very conservative mindset and historically risk-adverse culture, the adoption in ‘our’ space was slow.
- However adoption rate of Cloud solutions in the life sciences has seen a rapid increase since 2015.

How many companies here today are running GXP solutions in the Cloud?

Evolution of Data Integrity regulations and guidelines

- Data Integrity is not a new concept. It has been around since paper and ink were the only ways of doing business, but Regulators have become increasingly prescriptive in their requirements.

- We know how the well-understood requirements for paper data integrity should be translated to apply to electronic records and computer systems.

- Since 2015, the FDA, EMA, MHRA, WHO, PIC/S and other associations (PDA, ISPE) have been publishing Data Integrity guidelines to increase the industry's understanding of the expectations for compliance.

Where are we with e-compliance with Suppliers?

- Many guidelines, articles, conferences and trainings, the maturity level of many Suppliers remains low.

- Rapidly evolving technology disrupts and challenges the required compliant handling of electronic records throughout the record retention period.

- **Solution providers** are typically too far from the regulated user's operating environment.

- **Regulated users** are not able to clearly define requirements or expectations regarding e-compliance.

Where are we with e-compliance with Regulators?

- Many software applications are widely used in laboratories, offices and manufacturing that are under the regulator’s watchful eyes.

- Regulations such as FDA's GxPs, 21 CFR Part 11 and the EU or PIC/S Annex 11 require users of software and computer systems to demonstrate and document data accuracy, **data integrity** and confidentiality.

- Regulators specifically cite missing validation and other **data integrity controls, such as access security**.

- Many applications have not been designed for regulated environments… **and now there is the cloud.**

Now There Is Cloud Computing

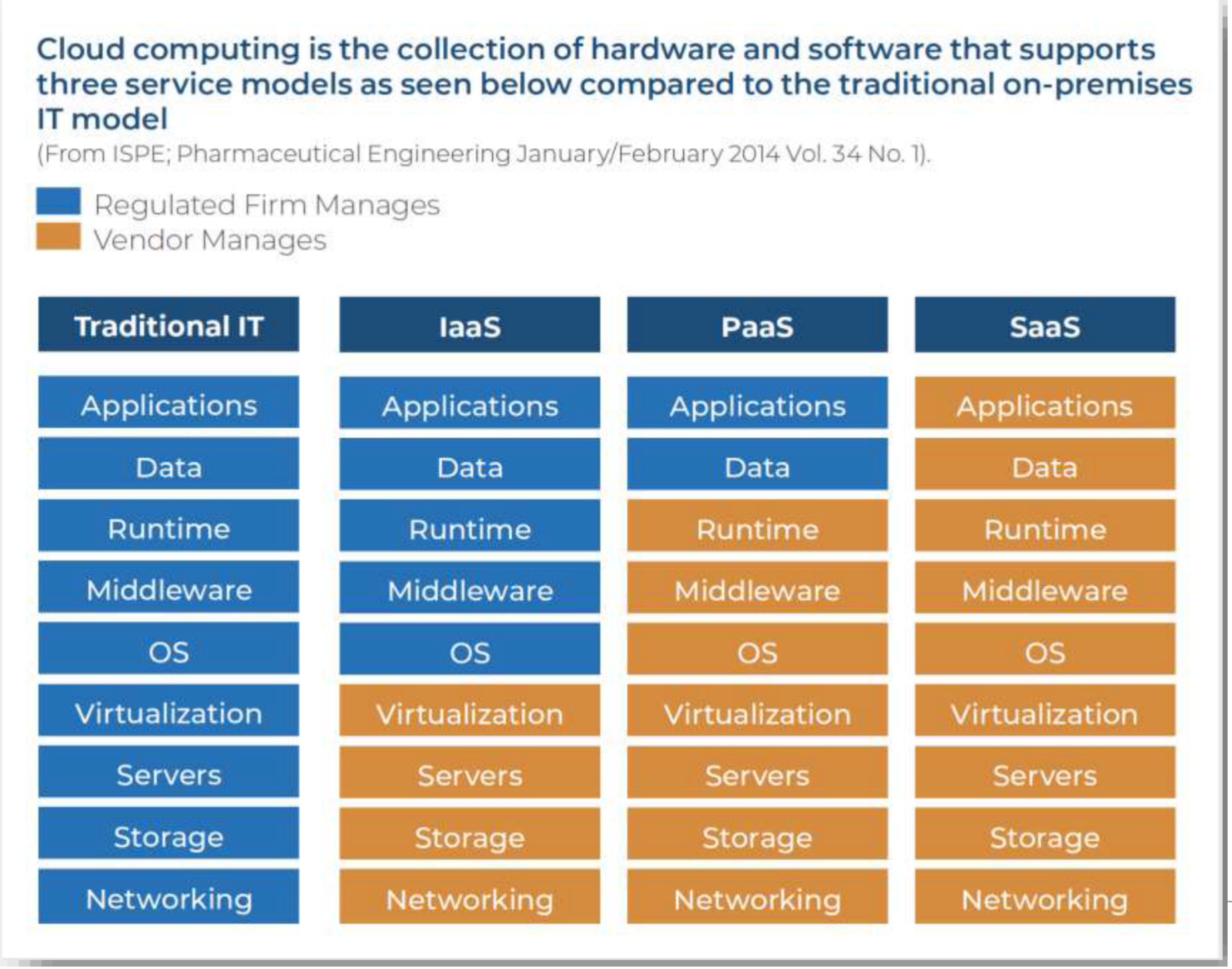
The current developments of new approaches with cloud computing emphasise once again the poor understanding of regulatory requirements by regulated companies, particularly in terms of **control, data integrity, security, and privacy.**

Cloud Service (XaaS) Analogy – a rental apartment

IaaS:
You pay a monthly fee for power, water and gas

PaaS:
You pay a monthly fee for power, water, gas, cable tv, building manager, garden you maintain – grow produce

SaaS:
You pay a monthly fee for power, water, gas, cable tv, building manager, shared kitchen/garden/parking area with neighbours which is yours on an as needed basis. Landlord ensures enough shared resource for everyone.



Cloud computing is the collection of hardware and software that supports three service models as seen below compared to the traditional on-premises IT model

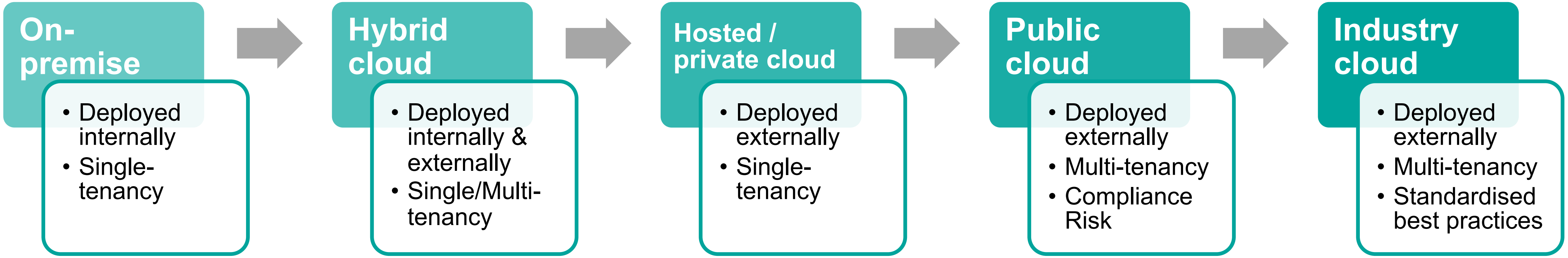
(From ISPE; Pharmaceutical Engineering January/February 2014 Vol. 34 No. 1).

🟦 Regulated Firm Manages

🟧 Vendor Manages

Traditional IT	IaaS	PaaS	SaaS
🟦 Applications	🟦 Applications	🟦 Applications	🟧 Applications
🟦 Data	🟦 Data	🟦 Data	🟧 Data
🟦 Runtime	🟦 Runtime	🟧 Runtime	🟧 Runtime
🟦 Middleware	🟦 Middleware	🟧 Middleware	🟧 Middleware
🟦 OS	🟦 OS	🟧 OS	🟧 OS
🟦 Virtualization	🟧 Virtualization	🟧 Virtualization	🟧 Virtualization
🟦 Servers	🟧 Servers	🟧 Servers	🟧 Servers
🟦 Storage	🟧 Storage	🟧 Storage	🟧 Storage
🟦 Networking	🟧 Networking	🟧 Networking	🟧 Networking

Cloud Deployment



On-premise
- Deployed internally
- Single-tenancy

Hybrid cloud
- Deployed internally & externally
- Single/Multi-tenancy

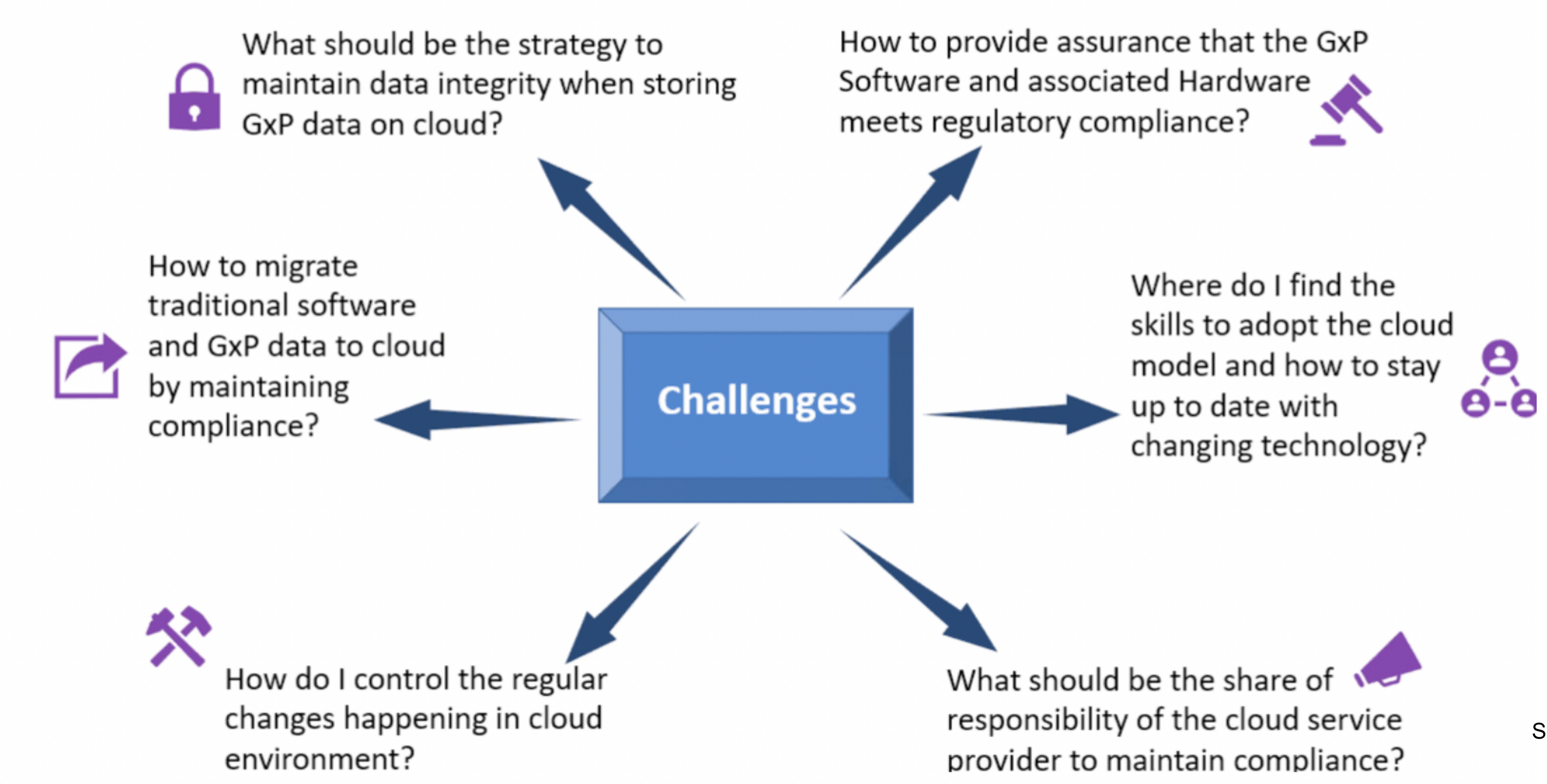
Hosted / private cloud
- Deployed externally
- Single-tenancy

Public cloud
- Deployed externally
- Multi-tenancy
- Compliance Risk

Industry cloud
- Deployed externally
- Multi-tenancy
- Standardised best practices

Challenges and Risks

Challenges In GxP Regulated Industries



Challenges

What should be the strategy to maintain data integrity when storing GxP data on cloud?

How to provide assurance that the GxP Software and associated Hardware meets regulatory compliance?

How to migrate traditional software and GxP data to cloud by maintaining compliance?

Where do I find the skills to adopt the cloud model and how to stay up to date with changing technology?

How do I control the regular changes happening in cloud environment?

What should be the share of responsibility of the cloud service provider to maintain compliance?

Source ISPE

Risks With Cloud Computing

Governance

- Lack of control over how cloud provider operates
- Lack of visibility/communication of infrastructure changes

Security

- Shared responsibility over data security
- Must trust cloud provider’s security architecture
- Cloud provider has privileged access to cloud consumer data
- Security incidents may spill over to multiple cloud tenants

Business Continuity

- Poorly defined SLAs for system recovery
- Differing government / industry regulations for data privacy and storage policy

Legal and Compliance

- Vendor reluctance to accommodate audits or to invest in necessary controls
- Migration of platform, software or data to another cloud provider/environment
- Legal definitions for government access to data may conflict by country

Cloud and Data Integrity and ALCOA+

													R
	A												E
	T												G
	T											C	U
	R											O	L
C	I									A	C	M	A
L	B	C					C			C	O	P	T
O	U	O			O		O		L	C	N	L	O
U	T	N			R	E	N	R	E	U	S	E	R
D	**A**	**T**	**A**		**I**	**N**	**T**	**E**	**G**	**R**	**I**	**T**	**Y**
	B	R	V		G	D	E	L	I	A	S	E	
	L	O	A		I	U	M	I	B	T	T		
	E	L	I		N	R	P	A	L	E	E		
			L		A	I	O	B	E		N		
			A		L	N	R	L			T		
			B			G	A	E					
			L				N						
			E				E						
							O						
							U						
							S						

CONNECTING PEOPLE SCIENCE AND REGULATION®

Validation

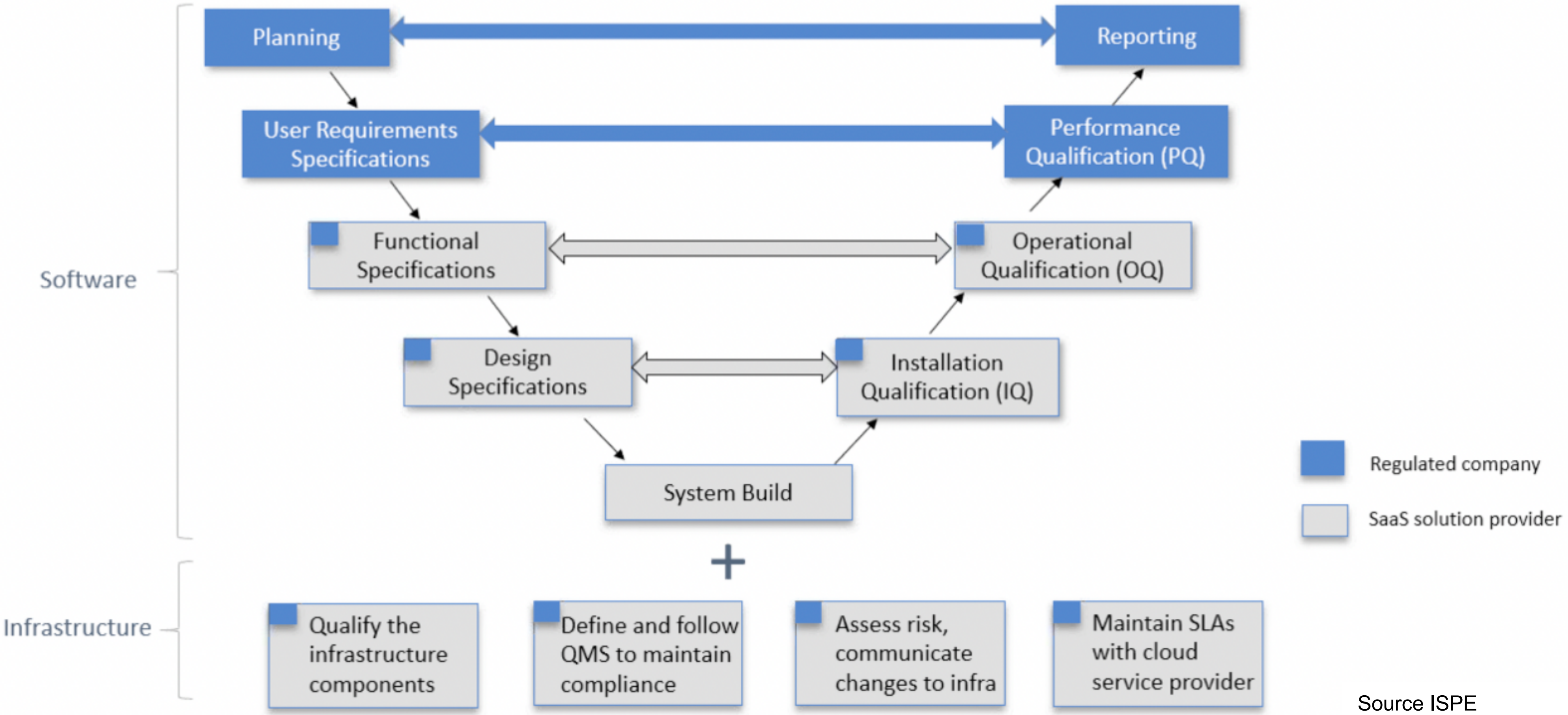
How Cloud Computing (SaaS) Impacts Validation Approach

- **For conventional on-premise software implementation**
  - well-known and understood
  - follows a risk-based approach that focuses on product quality and data integrity

- **For SaaS implementation – need to accommodate**
  - out-sourcing concern
  - not wanting to give up control
  - issue deviating from rigid validation procedures
  - a culture change required to accept out-of-the-box configuration to then leverage provider's validation documentation

- How does the **Validation puzzle** change from the traditional way we do it with on-premise systems?

SaaS Provider Validation Leverage (IQ,OQ)



Software

Planning

Reporting

User Requirements Specifications

Performance Qualification (PQ)

Functional Specifications

Operational Qualification (OQ)

Design Specifications

Installation Qualification (IQ)

System Build

+

Infrastructure

Qualify the infrastructure components

Define and follow QMS to maintain compliance

Assess risk, communicate changes to infra

Maintain SLAs with cloud service provider

🟦 Regulated company

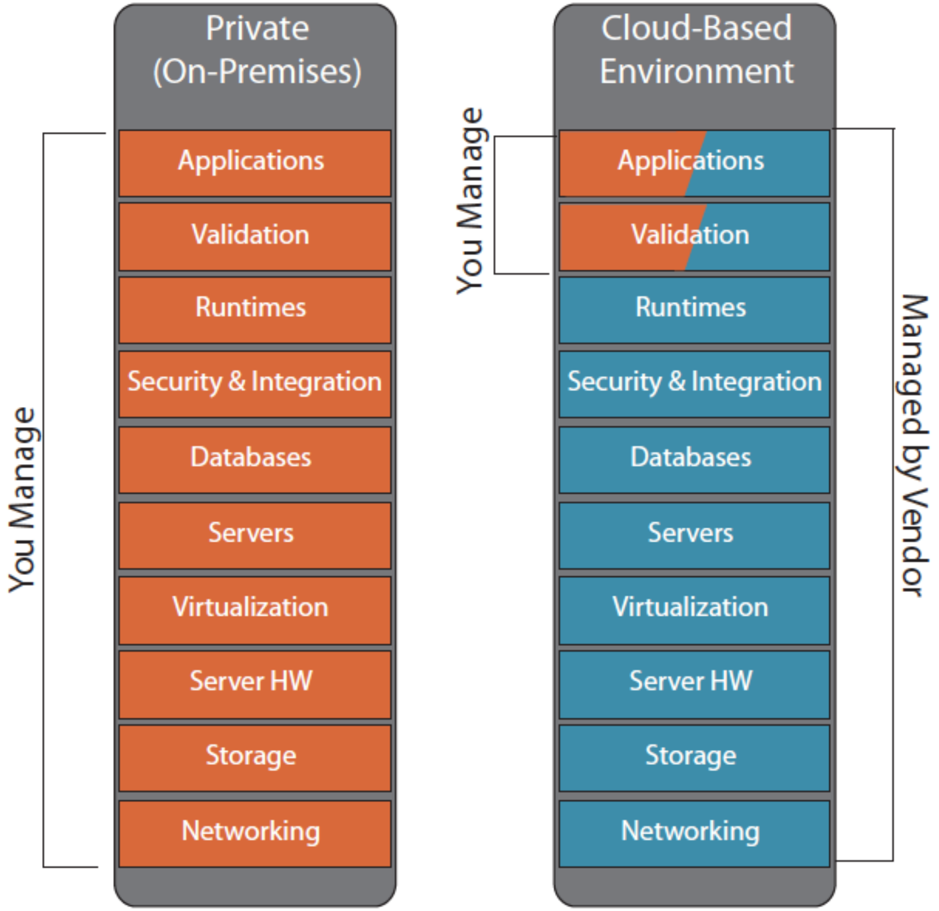
⬜ SaaS solution provider

Source ISPE

Validation Assistance Tools

Cloud Service Provider Validation Tools

- Managing specification and validation docs
- Risk management of release analysis
  - Internal risk score of software features
  - How you use the software
  - Variation from best practices
  - Determines additional validation



Source: Microsoft Faculty Connection

SaaS Validation Approach - Summarised

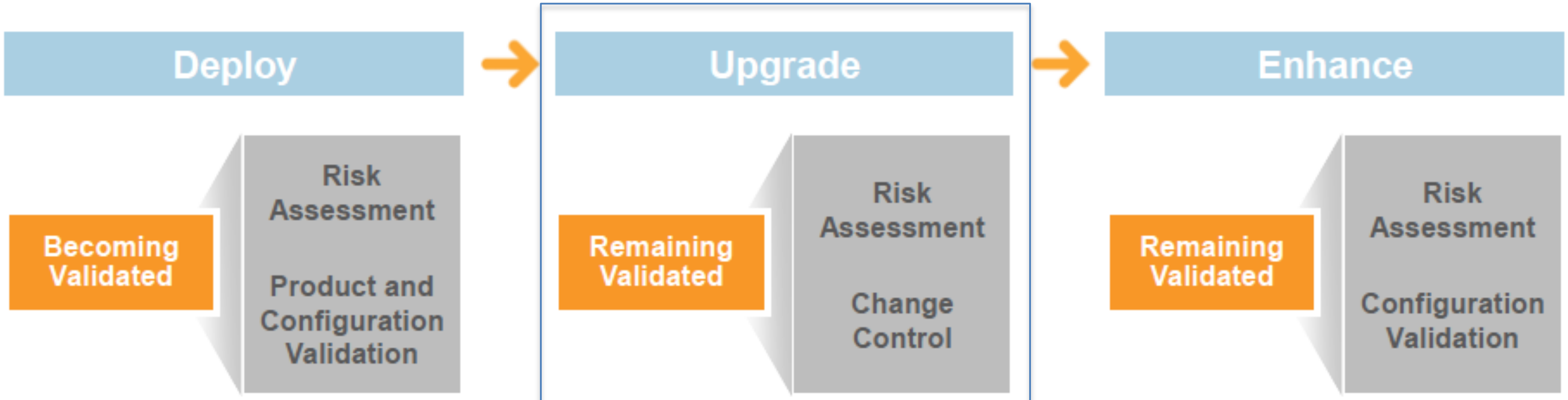
- Assess and accept your software supplier’s documentation and templates.
- Include your supplier’s usage testing in your validation package.
- Follow the best-practice configurations outlined by your supplier.
- Assess your specific configuration and usage for risk-based validation.
- Focus on validating your critical business processes (CBPs).
- Follow a risk-based approach in software validation.

How Cloud Computing (SaaS) Impacts Validation Approach

Computer System Validation Master Plan

- Add section to existing CSVMP for Cloud
- Update Risk Management Section
- Update Responsibilities Section
- Validation Activity Triggers
- Periodic Review Requirements
- Vendor Management
- SLA

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

Continuous Validation

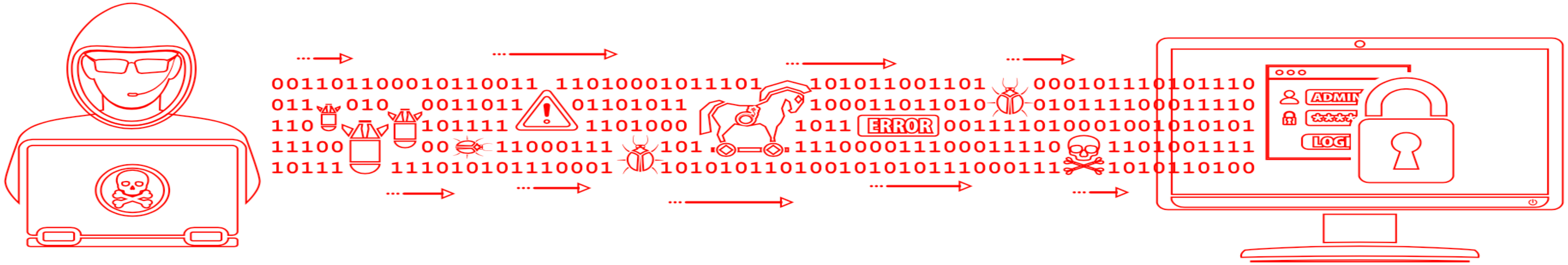
- Perhaps the **most significant concern** regarding the validation and ongoing maintenance of SaaS systems are **software updates**.
- SaaS suppliers commonly perform periodic small software updates at specified times.
- Be aware of the timeframe maintained by your CSP between releasing the upgrade in the test environment and production environment.
- It should be a relatively short process that checks any potential impact on functionality from the previous version
- Keeping the system up to date with security updates and business features reduces risks of data/privacy breach and cyber attacks

Cybersecurity

- One area that is not usually considered for data integrity is cybersecurity.
- Cyber attacks take two forms, one form is extortion, where data is encrypted until the victim pays to get it back, and the other is targeted attacks focused on damaging data.
- Our industry has encountered that with
  - Merck 2017 **lost access to batch data** as a result of a cyber attack
    - (ALCOA: Available, Complete, Enduring, Control, ..)
  - Caused extensive shutdown of systems, data loss and cost the over $1 billion to resolve (many recalls, and couldn’t make Gardisil)

Cybersecurity

- The main motivation for going to the cloud originally was not security, but now?
- The key to dealing with ransomware is limiting exposure and mitigating the risk. For instance, limiting data access rights within an organization reduces exposure
- Established cloud vendors like Microsoft, Amazon and Google, have put eye-watering investments into the security of their infrastructure



Auditing Cloud Suppliers

Auditing The SaaS Vendor

- A common practice among regulated companies is to perform an audit of the potential supplier’s quality systems prior to the selection of a software system for traditional implementation (Annex 11-3.1, 11-3.3, 11-4.5).
- **Pre-selection** and **ongoing** audits are of greater significance to SaaS suppliers than conventional software vendors.
  - greater reliance is placed on a SaaS supplier’s quality systems.
  - focus on SaaS supplier on-going IT governance.
  - how do we assure *Data Integrity is* maintained throughout the data life cycle?
  - **have we the skills to perform the audits?**

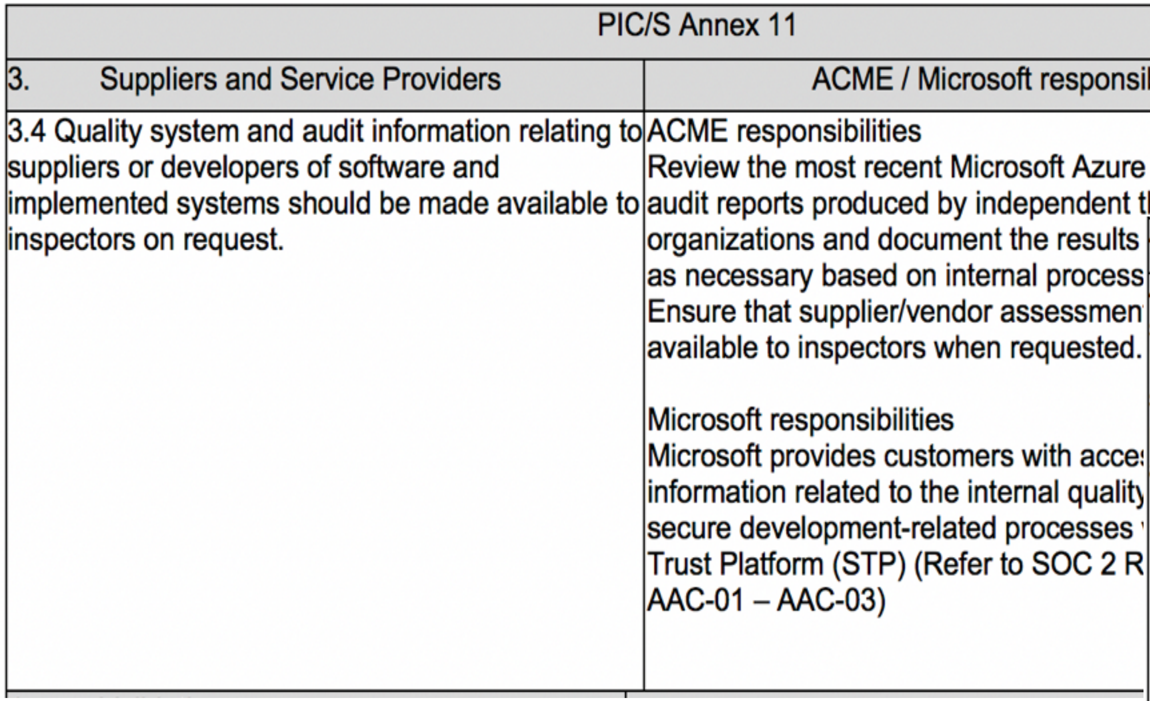
Auditing The SaaS Vendor

- **Audit should be directed to areas in which the SaaS supplier maintains control of specific processes, such as**
  - Location and control of data centres used to store the software and client data.
  - Change control of hardware and software for ongoing updates or upgrades.
  - Communication methods and timelines for customer notification of software updates or upgrades.
  - Physical and logical security, such as user identification, passwords, and roles and privileges.
  - Backup and recovery.
  - Data security and privacy.

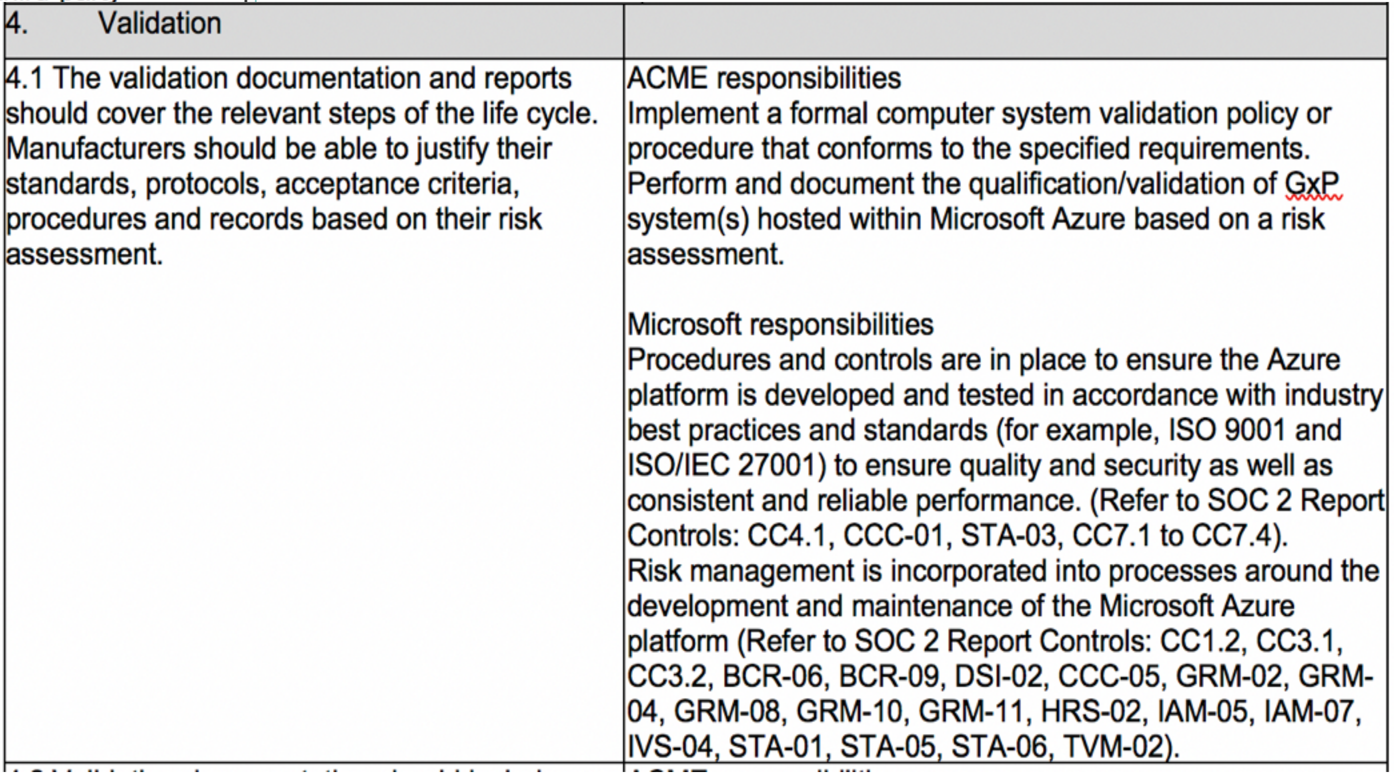
Auditing The SaaS Vendor

- Many CSPs regularly undergo independent audits performed by qualified third-party accredited assessors for :
  - ISO (27001, 27017, 27018) - IT security
  - ISO 9001
  - SOC 1, 2 (Type I and II) System and Organisation Controls
  - Health Information Trust Alliance (HITRUST)
  - US Federal Risk and Authorization Management Program (FedRAMP)
  - Payment Card Industry (PCI)
  - HIPAA
  - GDPR
- CSPs willingly grant access to independent third party audit reports.

PIC/S Annex 11 – MS Azure



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 as necessary based on internal process Ensure that supplier/vendor assessmen available to inspectors when requested. Microsoft responsibilities Microsoft provides customers with acce information related to the internal quality secure development-related processes Trust Platform (STP) (Refer to SOC 2 R AAC-01 – AAC-03)



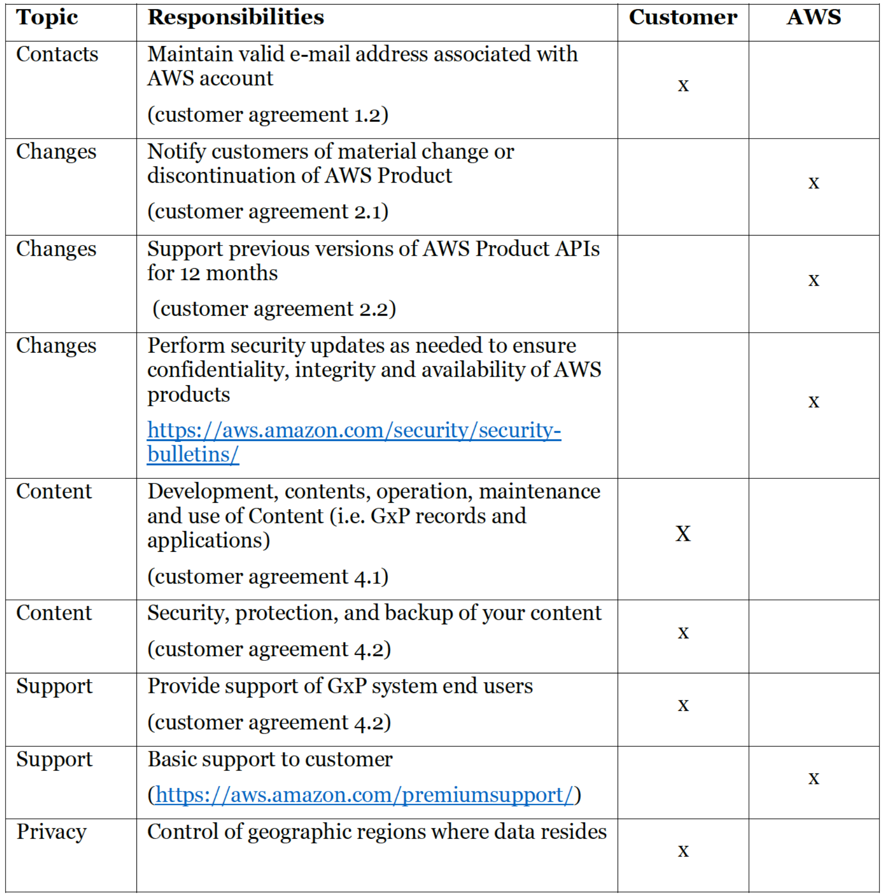
4. Validation	
4.1 The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.	ACME responsibilities Implement a formal computer 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).

Formal Agreement for Service Providers

Annex 11 subpart 3.1 on Suppliers and Service Providers:

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

Example of using AWS in GXP Solutions



Topic	Responsibilities	Customer	AWS
Contacts	Maintain valid e-mail address associated with AWS account (customer agreement 1.2)	x	
Changes	Notify customers of material change or discontinuation of AWS Product (customer agreement 2.1)		x
Changes	Support previous versions of AWS Product APIs for 12 months (customer agreement 2.2)		x
Changes	Perform security updates as needed to ensure confidentiality, integrity and availability of AWS products https://aws.amazon.com/security/security-bulletins/		x
Content	Development, contents, operation, maintenance and use of Content (i.e. GxP records and applications) (customer agreement 4.1)	X	
Content	Security, protection, and backup of your content (customer agreement 4.2)	x	
Support	Provide support of GxP system end users (customer agreement 4.2)	x	
Support	Basic support to customer (https://aws.amazon.com/premiumsupport/)		x
Privacy	Control of geographic regions where data resides	x	

Summary of responsibilities found in AWS standard agreements. It relies on agreeing the responsibilities in an SLA between AWS customers and their end users.

Adapting For The Future

- SaaS Cloud solutions are here to stay.
- This means **providers** to our regulated industries will **need to understand regulatory requirements (and data integrity concerns)** and take the proper steps to ensure compliance.
- **Our regulated companies** must expand our computer systems and validation perspectives beyond conventional applications to include management of SaaS vendors.
- **Monitor life sciences industry trends** with regard to Cloud Computing.
  - Monitor FDA and other regulators activities, statements, and regulatory actions in order to understand their interpretation and expectations.
  - It is unlikely that regulations will change to accommodate Cloud Computing, but the interpretation of how data integrity controls and validation requirements should be applied to these environments is likely to evolve as they become more popular.

Summary

The cumbersome practices of “traditional” data integrity compliance management and validation with on-premise IT systems are not true traditions.

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

Maybe the Cloud will reign.