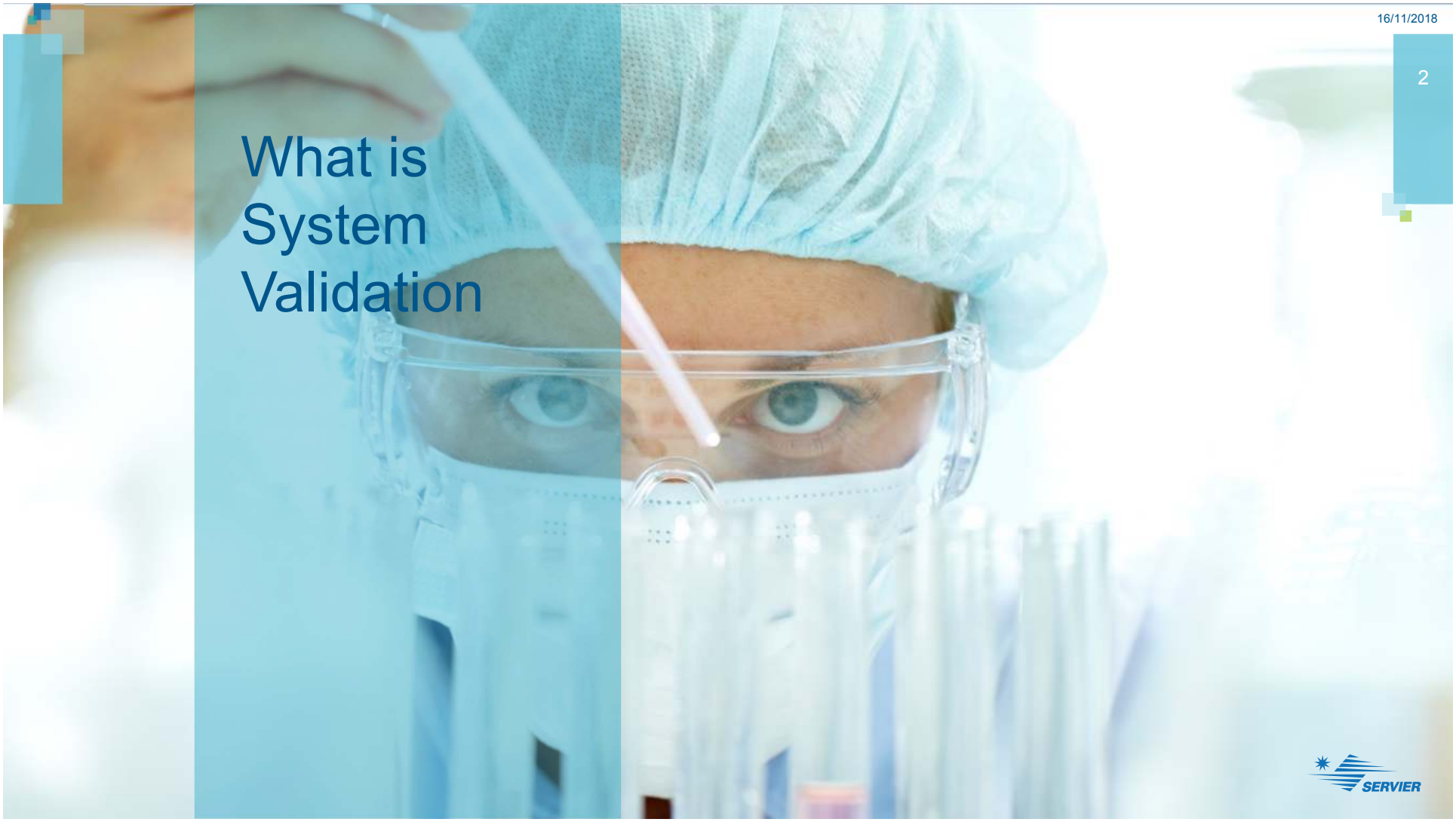
Validation of SaaS Systems (in the Cloud)

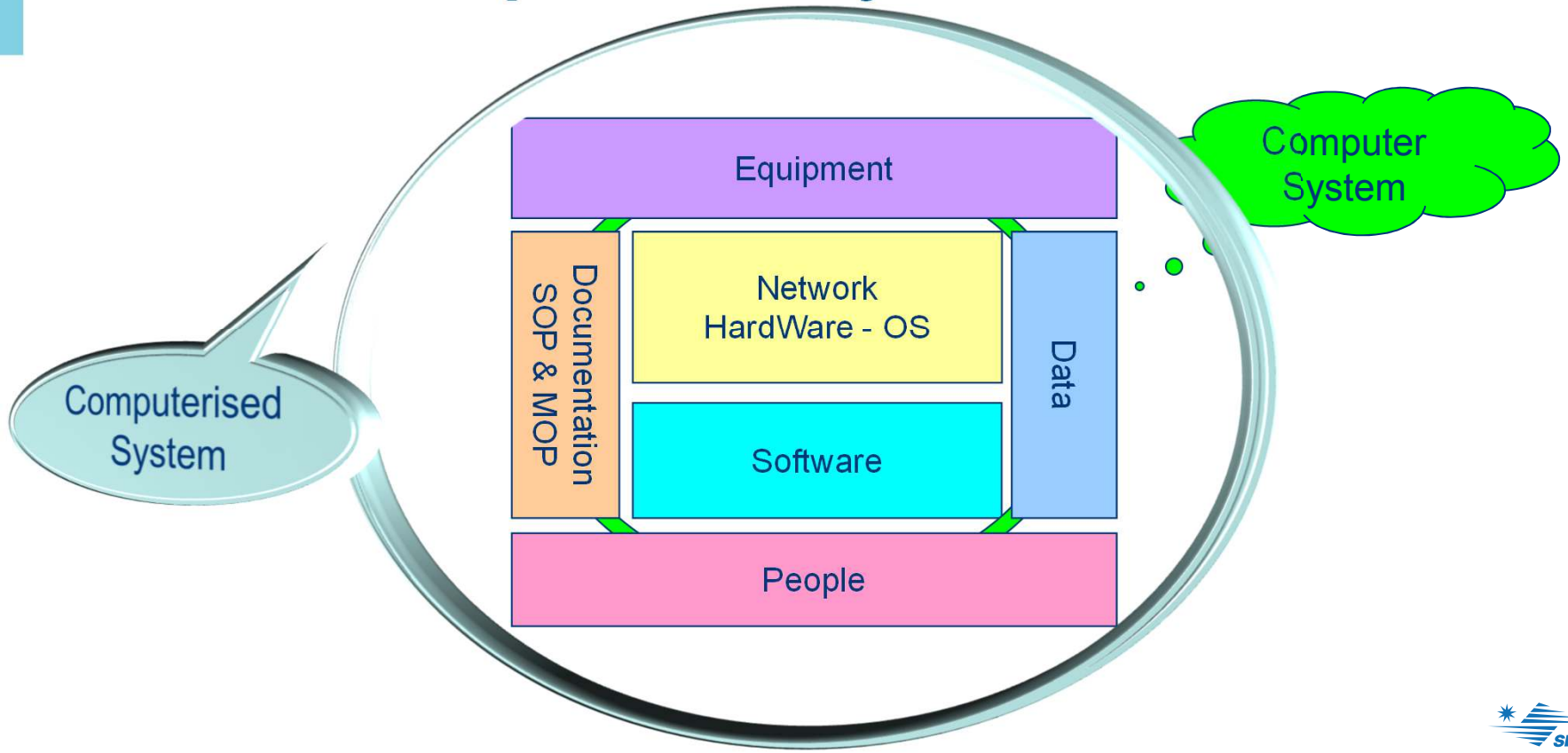
Nigel BONEHAM
Servier

13th November 2018

What is System Validation



What is a computerised system?



Validation for Reliability & Data Integrity, Risk-Based

- FDA 21 CFR Part 11, 1997

... Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

…The process of establishing **documented evidence**, that provides a **high degree of assurance**, that a CS consistently performs according to **predetermined specifications** and quality attributes

- FDA Computerized Systems Used in Clinical Investigations, Guidance, 1999

Software validation

Confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses and that the particular requirements implemented through the software can be consistently fulfilled.

- FDA 21 CFR Part 11 Scope and Application, 2003

Sponsors and other regulated entities should use a **risk-based approach** for validating electronic systems owned or managed by sponsors and other regulated entities

Validation for intended use, Risk-based

- ICH E6 R2 “Validation of Computerized Systems” (2017):

A process of establishing and documenting that the **specified requirements** of a computerized system **can be consistently fulfilled** from design until decommissioning of the system or transition to a new system.

The approach to validation should be **based on a risk assessment** that takes into consideration the **intended use** of the system and the potential of the system to affect human **subject protection** and **reliability of trial results**.

Regulatory implications on electronic data

- Limit access
- Prevent data modification

- Change control
- Link raw data and results

- Who did what, when and why?
- Previous entries must not be obscured

Trustworthiness of electronic records is ensured by appropriate measures for data security, data integrity and traceability

SERVIER

What is the Cloud?

What is Saas?

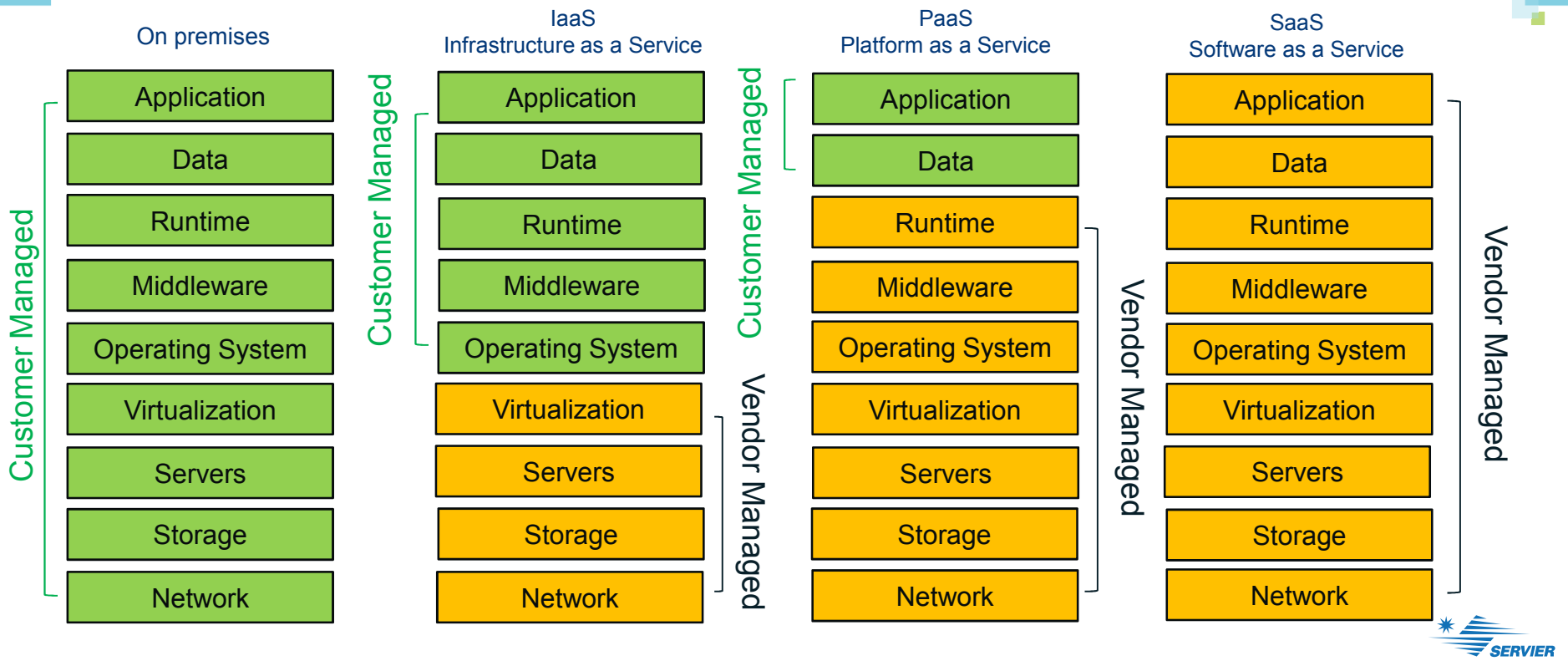
Cloud Computing

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

NIST (US National Institute of Standards and Technology)

SERVIER

IaaS, PaaS, SaaS



Service: are you buying a product or a service?

IaaS

- You buy computing power and storage volumes,
- Not servers etc.

PaaS

- You buy an available platform,
- Not an integrated set of software.

SaaS

- You buy access to computer functions, generally common to multiple clients, with configurability.
- Not software licences.

SERVIER

Some Regulatory Guidance for SaaS

FDA draft guidance for Outsourced Services processing regulated data

- It is ultimately the **responsibility of the sponsor** (or other regulated entity*) to **ensure that the service is validated as appropriate**.
- A **risk-based approach** to validation should be taken.
- Sponsors and other regulated entities should **obtain documentation from the Service Vendor** (SOPs, results of testing,...).

**clinical investigators, institutional review boards (IRBs), contract research organizations (CROs)*

FDA "Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 – Questions and Answers" (draft, 2017)

SERVIER

FDA draft guidance for Outsourced Services processing regulated data

Sponsors (and other regulated entities) should consider whether there are adequate controls in place to ensure data reliability and confidentiality:

- Validation documentation
- Ability to generate accurate and complete copies of records
- Availability and retention of records for FDA inspection for as long as required
- Access controls and authorization checks for users' actions
- Secure, computer-generated, time-stamped audit trails of users' actions and changes to data
- Encryption of data at rest and in transit
- Electronic signature controls

- Performance record of the electronic service vendor and the electronic service provided
- Ability to monitor the service vendor's compliance with security and data integrity controls

FDA may choose to inspect the electronic service vendors

FDA "Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 – Questions and Answers" (draft, 2017)

SERVIER

MHRA guidance concerning IT Suppliers and Service Providers (SaaS / PaaS / IaaS)

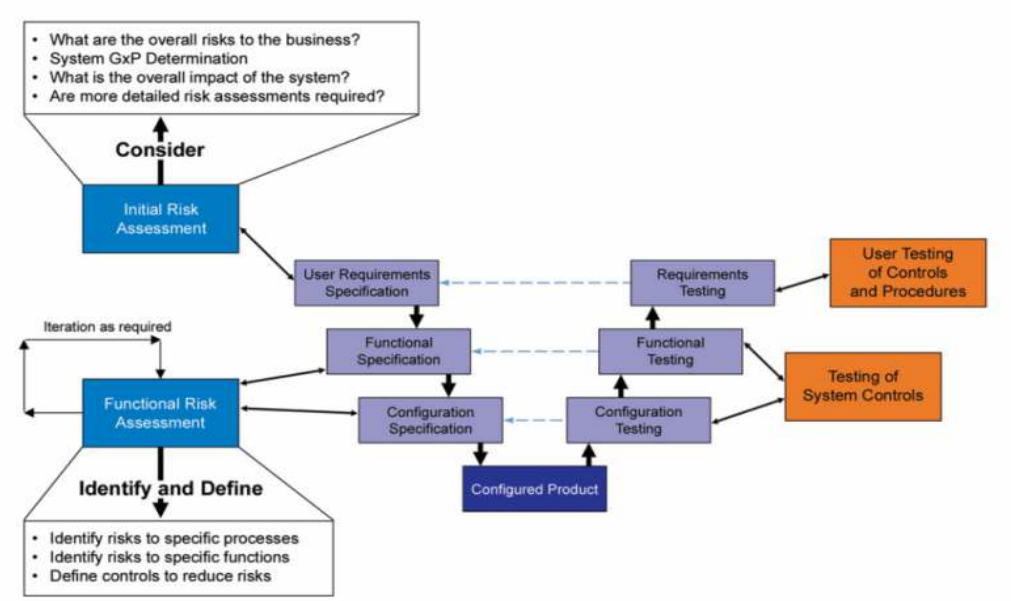
- Validation for intended purpose:
  - Requires an understanding of the computerised system's function within a process.
- Vendor-supplied validation in isolation of system configuration and intended use is not acceptable:
  - Vendor testing likely to be limited to functional verification only.
- Understand the service provided, ownership, retention and security of data.
- Consider physical location of data, including the impact of any laws applicable.
- Define responsibilities:
  - **Timely access to data** for the data owner and competent authorities.
  - **Archiving and continued readability** of the data throughout the retention period.
  - **Restoration** of the software/system.
  - **Business continuity** arrangements, including tests.
- Audit, dependent upon risk.

MHRA 'GxP' Data Integrity Guidance and Definitions (2018)

Suggestions for Validating SaaS systems

Use of a classic approach as the basis for validating SaaS

- Identify system in inventory & VMP
- Define URS
- Contracts & Due Diligence
- Audit Strategy
- Validation
- Change Control
- Periodic Review



Source: Figure M3.7, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org.

SERVIER

Validation by the Sponsor before Go Live

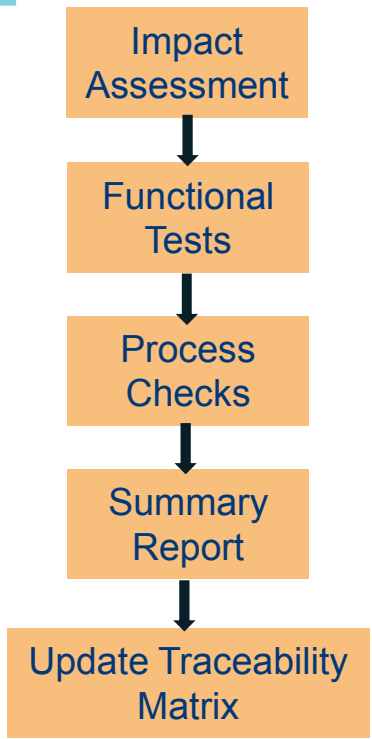
- Validation Plan:
  - Use risk assessment to justify scope and depth of activities
  - Take into account Vendor activities
  - Identify Sponsor activities
  - Show clearly the overall approach

- Include (depending on scope and risks):
  - User Testing (informal, formal)
  - Interfaces.
  - Documents to be provided by the Vendor (IQ…)
  - SOPs, User Guides, Training, Access, Configuration.
  - Process for Control of changes post Go Live…

Validation of Updates after Go Live

- Define the process well in advance.
- Get organized! Changes may be frequent, and timelines fixed.
- Sponsor effort will depend on:
  - Vendor maturity and effort (risk-based approach).
  - Impacts on user processes, data integrity & security.
  - May be adjusted as time goes on (hopefully reduced).
- Beware of interfaces

Example: Validation of Regular Updates after Go Live



- ⇒ Vendor document + user conclusion
  - ⇒ Needs for tests or updates to documentation, training,…
- ⇒ Reusable Regression Test Script & Tests of new/modified functions
  - ⇒ Possibility to automate regression tests…
- ⇒ Obtain documentation
  - ⇒ Vendor (Notification of Delivery, Validation,…)
  - ⇒ Users (Configuration Specs, User Guides,…)
- ⇒ Summarize the activities and anomalies in a Release Control Report
  - ⇒ Based on a Validation Report template.
- ⇒ After each cycle. Still a challenge without tools.

SERVIER

Contracts & Due Diligence

⇒ Evaluate and select electronic services:
- ⇒ Service vendor's ability to meet data security, protection & integrity requirements.
- ⇒ Whole life costs.
- ⇒ …

⇒ Establish contracts / service agreements:
- ⇒ Include data security, protection & integrity requirements.
- ⇒ Be clear who does what. Review all applicable requirements. Include end of contract terms.

⇒ Include everything needed for validation & compliance:
- ⇒ Access to, or recovery of, vendor documents (specs, validation, procedures, helpdesk records,…).
- ⇒ Notification of changes, delivery and incidents.
- ⇒ Impact assessments, Validation environments, Release delivery conditions.
- ⇒ Support in case of Inspection.
- ⇒ IaaS & Software Publisher requirements, even if subcontracted by a SaaS Vendor.
- ⇒ Oversight of the sub-contracted activity (your oversight, their oversight).

SERVIER

Thank you for your attention