Audit and Monitor Vendors for CSV Compliance

John Lindahl for
IVT 18th Annual Computer and Software Validation
April 26, 2017, San Diego, CA
John Lindahl

Agilent Technologies
Santa Clara, CA
Software & Informatics Division
Customer Commitment Manager
john_lindahl@agilent.com
Experience with Vendor Audits?
Agenda

Background
On-boarding new vendors
Monitoring vendors
Vendor audits
Background
**Regulatory Expectation**

**General Principles of Software Validation;** Final Guidance for Industry and FDA Staff (January, 2002) [https://www.fda.gov/RegulatoryInformation/Guidances/ucm085281.htm](https://www.fda.gov/RegulatoryInformation/Guidances/ucm085281.htm)

“The **device manufacturer is responsible** for ensuring that the product development methodologies used by the OTS [off-the-shelf] software developer are appropriate and sufficient for the device manufacturer’s intended use of that OTS software.”

“The **audit should demonstrate that the vendor’s procedures** for and results of the verification and validation activities performed the OTS software are **appropriate and sufficient** for the safety and effectiveness requirements of the medical device to be produced using that software.”

Possible Outcomes

Vendor procedures satisfy all validation requirements and have been effectively implemented.

Vendor procedures partially satisfy the requirements.

Vendor procedures do not satisfy the requirements or vendor does not permit an audit.
On-boarding New Vendors
On-boarding New Vendors

Vendor selection
- Criticality classification
- Selection criteria based on classification
- Contract terms including software specification, services, support
- Initial information gathering
- Audit critical vendors

When vendor procedures are not sufficient
- Request improvement plan (audit findings)
- Identify risks and mitigate (i.e. do testing)
- Reject unqualified, uncooperative vendors
Monitoring Vendors
Monitoring Vendors

Approved Vendor List
Status for each vendor (approved, conditional, disapproved)
Prioritization of vendors needing observation
Re-evaluation schedule
Quality monitoring
  - Support tickets
  - Issues found in new software versions
Comparing Vendors

The four-fold problem

- Disparity
- Partiality
- Variability
- Legibility

Comparing Vendors: Disparity

Regulations specify “what” but infrequently “how”

There are many guidelines from both regulators and industry

Each company defines their own interpretation

The four-fold problem
- Disparity
- Partiality
- Variability
- Legibility
Comparing Vendors: Partiality

Audits are done by sampling and therefore incomplete

Reports focus on deficiencies and deviations

Findings vary from vendor to vendor

Findings vary over time for a single vendor

The four-fold problem
- Disparity
- Partiality
- Variability
- Legibility
Comparing Vendors: Variability

Auditors apply judgment of importance and severity

Audit teams vary in composition and focus

The four-fold problem
- Disparity
- Partiality
- Variability
- Legibility
Comparing Vendors: Legibility

Software architectures, tools, and technologies are numerous

High degree of technical jargon

Industries and vendors have their own jargon

Audits need to translate into the GxP data integrity requirements

The four-fold problem
- Disparity
- Partiality
- Variability
- Legibility
So what do you do?

Set up a system to make reporting as consistent as possible

Define an audit structure (“the six buckets”)

Work in teams and do peer reviews
Vendor Audits

The “six bucket” audit strategy
The six buckets

1. Procedures
2. Infrastructure
3. Training and personnel
4. Software development
5. Testing/validation
6. Quality management system
Procedures

1. Comprehensive
2. Clear / Detailed
3. Compliant
4. Controlled
5. Connected

The six buckets

1. Procedures
2. Infrastructure
3. Training and personnel
4. Software development
5. Testing/validation
6. Quality management system
Procedures: Comprehensive

Procedures are in place to define all activities associated with the design, development, testing and maintenance of software application.
Procedures: Clear / Detailed

Procedures are sufficiently detailed, clear and unambiguous to ensure that key processes are performed in a repeatable and consistent manner.
Procedures: Compliant

Procedures reflect industry best practices (e.g., IEEE, SEI) and reflect an understanding of the regulated environment.
Procedures: Controlled

Procedures are developed, reviewed, rolled-out, maintained and retired in a controlled manner.
Procedures: Connected

Related procedures (e.g., issues management, change control, CAPA) are well integrated and/or referenced to comprise a coherent system of interrelated processes.
Infrastructure

1. Server Room
2. Backup, DR, BC
3. Security (Logical / Physical)

The six buckets

1. Procedures
2. Infrastructure
3. Training and personnel
4. Software development
5. Testing/validation
6. Quality management system
Infrastructure: Server Room

Facility design meets industry expectations (e.g., raise flooring, fire suppression and environmental controls).

System hardware is maintained under acceptable conditions to safeguard applications and data.

System activity logs record excursions and events.
Infrastructure: Backup, DR, BC

Company has implemented appropriate processes to ensure the recoverability of data such as back up and recovery, business continuity/contingency planning and disaster recovery.
Infrastructure: Security (Logical / Physical)

Access to facility (including server room) is controlled and monitored.

Logical security processes (account management, encryption, authentication) have been implemented for key applications, in compliance with regulatory expectations (e.g., 21CFR11).
Training and personnel

1. Training Program
2. Training Records
3. Training on SOPs
4. Staffing
5. QA Independence

The six buckets

1. Procedures
2. Infrastructure
3. Training and personnel
4. Software development
5. Testing/validation
6. Quality management system
Training and Personnel: Training Program

The company maintains training records, job descriptions and resumes for all employees and contractors.

Training documentation clearly outlines requirements by job function.
Training and Personnel: Training Records

Training records are current, complete and accurate.

Training records cover both technical and regulatory requirements (awareness of Part 11).
Training and Personnel: Training on SOPs

Training documentation clearly demonstrated that individuals have read and understood the latest revision of procedures that impact their job function.
Training and Personnel: Staffing

Company has adequate resources for the development, testing, and/or operation and maintenance of HW/SW, including QA oversight of key processes.
Training and Personnel: QA Independence

The Quality Unit is sufficiently independent of operations to provide objective review of activities and deliverables.
Software development

1. SDLC
2. Requirements
3. Design Documentation
4. Configuration Management
5. Coding
6. Development Testing

The six buckets

1. Procedures
2. Infrastructure
3. Training and personnel
4. **Software development**
5. Testing/validation
6. Quality management system
Software development: SDLC

The company follows a formal development lifecycle methodology, one that clearly outlines development project deliverables, activities and quality gates.

The company can demonstrate, through documentation, that it adheres to these published standards.
Software development: Requirements

System requirements reflect application functions and features and regulatory expectations (e.g., Part 11) have been incorporated.

Both functional (intended use) and non-functional (operability, performance) requirements have been documented.

System requirements are clear, unambiguous, uniquely identified and testable.
Software development: Design Documentation

The application is well characterized to include a comprehensive set of design documents (FS functional specifications, DDS detailed design specifications).

Design documentation includes, as applicable,
• a) system and application component architecture,
• b) diagrams depicting the inter-relationships between presentation layer, application/business layer and data layer application,
• c) module level interdependencies,
• d) data flow diagram(s),
• e) application/module interfaces & I/O,
• f) database schema and stored procedures.
Software development: Configuration Management

Positive and correct correspondence among all approved versions of the specification documents, source code, and other software objects (manual, application platform, OS) has been established via a traceability matrix or other tool (Code control, Configuration Management).
Software development: Coding

Coding standards have been established for all languages used to ensure code consistency and compliance with good programming practices.

Code reviews are performed and documented.
Software development: Development Testing

Development testing is performed and documented, to include unit level testing, module integration, and regression tests (where applicable).

Testing adequately challenges boundary conditions, exceptions (error) handling, and module integration/communication.

Development testing adhere to the principles of independence of review.
Testing/validation

1. Test Plans
2. Test Case Design
3. Test Execution
4. Test Traceability
5. Test Summary

The six buckets

1. Procedures
2. Infrastructure
3. Training and personnel
4. Software development
5. **Testing/validation**
6. Quality management system
Testing/validation: Test Plans

Software testing is performed in accordance with pre-approved test plans that define the scope, approach, activities, deliverables, responsibilities and acceptance criteria for each phase of testing.

Testing rationale is explicit and considers such risk factors as function complexity and criticality, maturity of product/code, use history.

Test plans conform to company policies and procedures.
Testing/validation: Test Case Design

Test case design adheres to tenets of good software testing, which include documented test setup, clear and repeatable test instructions, and expected system response/results.
Testing/validation: Test Execution

Test execution conforms to the principles of Good Documentation Practice.

Sufficient objective evidence of testing (system response) is provided to permit an independent review of the test documentation.

A test deviation management process has been implemented.
Testing/validation: Test Traceability

All tests can be traced to requirements and specifications in order to demonstrate the completeness of the test coverage.
Testing/validation: Test Summary

A review of all testing is performed to document product quality and determine the releasability of the software candidate.

Summary reports clearly define the quality attributes and metrics for the release.

Deviations from testing, test plan, as well as product limitations, are documented.
Quality management system

1. Quality Audits
2. Change Management
3. CAPA
4. Issues Management
5. Release Management
6. Culture

The six buckets

1. Procedures
2. Infrastructure
3. Training and personnel
4. Software development
5. Testing/validation
6. Quality management system
Quality management system: Quality Audits

The company has established an internal quality audit program that periodically reviews all elements of computerized system development, testing, release, maintenance, and operations.

Internal audits are planned and performed at regular intervals.
Quality management system: Change Management

Changes to computerized systems/software are implemented after a comprehensive, formal, documented review and assessment of the change on the system as a whole (code, tests, design, manuals).

The impact assessment for code changes are clearly documented to inform the scope and level of testing required.
Quality management system: CAPA

A CAPA process has been instituted to address non-conforming product and processes.

The CAPA system is integrated with the issues management process, help desk, internal auditing, and process deviations/investigations to capture all events that may require corrective and preventive actions.

CAPAs are trended and periodically reviewed by management.
Quality management system: Issues Management

Issues encountered during all phases of the SDLC (development, testing, maintenance) are recorded, classified, tracked, trended, analyzed, and investigated (as appropriate for that phase of the lifecycle).

For critical process/product deficiencies, an analysis of root cause is performed to inform the CAPA process.
Quality management system: Release Management

Product release or release to GxP production use is contingent on process quality gates, that documented adherence to established SDLC processes.

Quality oversight is provided on all key activities and deliverables.
Quality management system: Culture

The company has demonstrated a culture of process improvement (evidenced through changes to procedures, CAPA, and/or attitude).
Summary

The regulated company is responsible for vendors

Objective comparison of vendors is difficult (“the four fold problem”)

Structured audits can improve consistency (“the six buckets”)
Additional Resources


purchase from ISPE.org
THANK YOU

john_lindahl@agilent.com