Auditing Software Vendors

By Praxis Life Sciences
Auditing Software Vendors

© Copyright 2017 by Praxis Life Sciences. All rights reserved. No part of these materials may be reproduced or transmitted in any form without the written permission of Praxis.

Your Praxis Facilitator

- Debra Bartel, MBA, CQA, PMP
- Principal, Praxis Life Sciences
- 25+ years experience specializing in software quality assurance, validation and regulatory compliance, Information Systems project management, and process design.
- Prior to joining Praxis, held management positions in the pharmaceutical industry in both Quality Assurance and Information Systems organizations
- Active member of American Society for Quality (ASQ), Northeastern Illinois Section, Software Division
Intro to Praxis Life Sciences

Validation Center™

Consulting  Audit Services  Training  Library

Follow us!

Target Audience

Industries  • Pharmaceutical & Biologics  • Medical Device  • Clinical Studies  • Blood Products

Regions  • Operating in the US  • Selling to the US Market

Personnel  • IT Personnel and Managers  • Software Quality Personnel and Managers  • Auditors and Audit Managers
Webinar Outline

1. Audit Framework
2. Regulations & Guidance
3. Audit Methods
4. Audit Preparation
5. Audit Execution
6. Post Audit
7. Leveraging Audit Results
8. FDA Warning Examples

Audit Framework

Part 1
Part 1: Audit Framework

Section Overview
- Audit Terminology
- Audit Types
- Audit Roles
- Audit Process

Basic Terminology

<table>
<thead>
<tr>
<th>Audit</th>
<th>Assessment</th>
<th>Inspection</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Planned</td>
<td>1. Planned</td>
<td>1. Planned</td>
</tr>
<tr>
<td>2. Documented</td>
<td>2. Documented</td>
<td>2. Documented</td>
</tr>
</tbody>
</table>
### Basic Terminology

<table>
<thead>
<tr>
<th>Audit</th>
<th>Assessment</th>
<th>Inspection</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Planned</td>
<td>1. Planned</td>
<td>1. Planned</td>
</tr>
<tr>
<td>2. Documented</td>
<td>2. Documented</td>
<td>2. Documented</td>
</tr>
<tr>
<td>3. Determines whether or not requirements are met</td>
<td>3. Determines whether or not requirements are met</td>
<td>3. Determines whether or not product/service specifications are met</td>
</tr>
<tr>
<td>4. Outside the Production process</td>
<td>4. Outside the Production process</td>
<td>4. Part of the Production process</td>
</tr>
<tr>
<td>5. Performed by an Independent auditor</td>
<td>5. Performed by an Independent assessor</td>
<td>5. Performed by a company inspector</td>
</tr>
<tr>
<td>6. Formal</td>
<td>6. Less formal or less in depth</td>
<td></td>
</tr>
</tbody>
</table>

#### Audit Types

<table>
<thead>
<tr>
<th>Internal</th>
<th>Customer</th>
<th>Regulatory Agency</th>
<th>Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performed by personnel within the company</td>
<td>• Performed to determine suitability for business relations</td>
<td>• Performed to determine compliance with government requirements</td>
<td>• Performed to determine compliance with certification requirements</td>
</tr>
<tr>
<td>External</td>
<td></td>
<td>[e.g. FDA, DEA, EU Ministries of Health]</td>
<td>[e.g. ISO, Malcolm Baldrige National Quality Award]</td>
</tr>
</tbody>
</table>
Audit Types

- Audit of the final product or service
- Performed after producer’s final inspection
- Can be performed at producer’s or customer’s site

Audit Types

- Audit of conformance to standards, requirements, or procedures for specific process(es)
- Examples: Testing, Change Control, Incident Handling
Audit Types

- All Processes
- Execution of Quality Management Plans
- The effectiveness of the quality program

Basic Terminology

Audit Standard

Basis for the audit, for example:
- FDA Regulations
- Customer Contract
- Published Standards, e.g. PIC/S, ISO
- Internal company standards & best practices
Audit Standard

Evidence
Proof that the Audit Standard has (or has not) been met, for example:
• Procedures
• Records and documentation
• Observing work as it’s being done

Observation
Statement of fact recorded during an audit and supported by objective evidence
Basic Terminology

Audit Standard
Evidence
Observation
Finding
A conclusion based on one or more observations

FDA Warning Letter Example

Finding
Audit Standard
Observations
Audit Roles

Audit Sponsor

- Authorizes the Audit
- Determines the Audit Standard
- Identifies the Auditing Organization

Audit Sponsor

Audit Sponsor

Lead Auditor

Auditor Team

Auditors

- Communicates with the Audit Sponsor and Auditee
- Makes audit arrangements with Auditee
- Conducts Audits and Documents Results
- Reports results to Audit Sponsor
Audit Roles

- Audit Sponsor
  - Makes logistical arrangements
  - Escorts auditors
  - Provides information needed by auditors

- Auditor(s)

- Auditees

- Audit Facilitator

- Auditee Team

Vendor Audit Regulations & Guidance
Part 2
Part 2: Regulations and Guidance

Section Overview
- FDA Regulations & Guidance
- ICH Guidelines
- Eudralex Regulations

Context

ICH Guidelines

Regulations (Laws)
FDA 21 CFR ....
Eudralex Volume ...

Company policies & procedures

influences

FDA Guidance & Reference Documents
EMA Reflection Papers
PIC/S Guidance Documents
GAMP Guides (ISPE)
IEEE Guides etc.
Validation Center™ © 2017 Praxis Life Sciences

FDA: Software Validation

Guidance  General Principles of Software Validation

Quotes:

Where possible and depending upon the risk involved, the manufacturer should consider auditing the vendor’s design and development methodologies used in the construction of the OTS software and should assess the development and validation documentation generated for the OTS software.
### FDA: Software Validation

**Guidance**

**General Principles of Software Validation**

**Quotes:**

If the vendor can provide information about their system requirements, software requirements, validation process, and the results of their validation, the … manufacturer can use that information as a beginning point for their required validation documentation.

The vendor’s life cycle documentation, such as testing protocols and results, source code, design specification, and requirements specification, can be useful in establishing that the software has been validated.

### FDA: Pharmaceutical Manufacturing

**Reference**

FDA ORA Guide to Inspection of Computerized Systems in Drug Processing

**Quotes:**

- Although much of the software validation may be accomplished by outside firms, such as computer or software vendors, the ultimate responsibility for program suitability rests with the pharmaceutical manufacturer.
- Records of software validation should be maintained by the drug establishment, although when conducted by outside experts such records need not be voluminous but rather complete enough (including protocols and general results) to allow the drug manufacturer to assess the adequacy of the validation.
- Mere vendor certification of software suitability is inadequate.
FDA: Medical Device Manufacturing

21 CFR 820 Quality System Regulation

Quotes:

**Subpart E:** Each manufacturer shall establish and maintain procedures to ensure that all purchased or otherwise received product and services conform to specified requirements.

(a) ... Each manufacturer shall:

1. Evaluate and select potential suppliers, contractors, and consultants on the basis of their ability to meet specified requirements, including quality requirements. The evaluation shall be documented.

2. Define the type and extent of control to be exercised over the product, services, suppliers, contractors, and consultants, based on the evaluation results.

3. Establish and maintain records of acceptable suppliers, contractors, and consultants.

ICH Guidance: API Manufacturing

Guidance Good Manufacturing Practice Guide for Active Pharmaceutical Ingredients

Quotes:

5.41 Appropriate installation qualification and operational qualification should demonstrate the suitability of computer hardware and software to perform assigned tasks.

5.42 Commercially available software that has been qualified does not require the same level of testing.
3.2 The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for and audit should be based on a risk assessment.

4.5 The regulated user should take all reasonable steps to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.

3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.

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.
Part 3: Methods and Process

Section Overview
- Purpose & Timing
- Audit Methods
- General Audit Process
- Audit Process for each Method

Why Audit Vendors?

Regulatory Expectations

Safeguard Your Investment
- Are you buying a reliable, high-quality system?
- Will the vendor continue to support the system when it’s older?
- Will the vendor be around to support the system?

Utilize Vendor Documentation
- Requirements documentation
- Testing documentation
- Training materials ….
When Should you Audit Vendors?

- **Prior to Purchase**
  - Ensure investment quality

- **Prior to Validation**
  - Leverage vendor documentation

- **Other Timing ....**
  - Periodic Vendor Review
  - Follow-up to earlier audit
  - Investigation of issues

Audit & Assessment Methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>On Site Audit</strong></td>
<td>Company representatives conduct formal audit at vendor’s site</td>
</tr>
<tr>
<td><strong>Off Site Audit</strong></td>
<td>Company representatives conduct formal audit via online meeting</td>
</tr>
<tr>
<td><strong>Questionnaire</strong></td>
<td>Company representatives send a self-assessment to vendor and review responses</td>
</tr>
<tr>
<td><strong>Basic Assessment</strong></td>
<td>Company representatives investigate public domain information &amp; contact other users</td>
</tr>
</tbody>
</table>
### Audit & Assessment Methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>On Site Audit</strong></td>
<td>Company representatives conduct formal audit at vendor’s site</td>
<td>- Most thorough</td>
<td>- Most Time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Best method to review policies, procedures, and actual practices</td>
<td>- Most Expense</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Some vendors won’t agree to audit</td>
</tr>
</tbody>
</table>

- Traditional Approach
- Scope depends on intended use of vendor’s software and documentation
- Recommended for critical applications, especially when intending to leverage vendor’s documentation

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Off Site Audit</strong></td>
<td>Company representatives conduct formal audit via online meeting</td>
<td>- Less Time</td>
<td>- Less thorough</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Less Expense</td>
<td>- Some vendor’s won’t agree to audit</td>
</tr>
</tbody>
</table>

- Options
  - Online Meetings
  - Phone Interviews
  - Hybrid
  - Alternative to on site audits for less critical applications
### Audit & Assessment Methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Questionnaire</td>
<td>Company representatives send a self-assessment questionnaire or survey to vendor and reviews responses</td>
<td>- Little time</td>
<td>- No assurance of accurate responses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Little expense</td>
<td>- Some vendors won’t complete questionnaire</td>
</tr>
</tbody>
</table>

- Simple approach for non-critical applications and services
- No assurance of accurate responses

### Audit & Assessment Methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Assessment</td>
<td>Company representatives investigate public domain information &amp; contact other users</td>
<td>- Little time</td>
<td>- Surface evaluation only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Little expense</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Vendor’s can’t disagree to this Method</td>
<td></td>
</tr>
</tbody>
</table>

- Online information
  - Financial Ratings
  - Gartner vendor ratings

- User provided information
  - User groups
  - Contacts in similar companies
  - Prior experience
  - References (from vendor)

- Vendor provided information
  - Customer lists
  - Awards received
Vendor Audit Process

Step 1
Determine Audit Method

Step 2
Prepare for the Audit

Step 3
Conduct the Audit

Step 4
Post-Audit Activities

Vendor Audit Process – On Site

Step 1
Determine Audit Method

On Site Audit

Step 2
Prepare for the Audit

Planning
Notification
Team Selection
Document Reviews

Step 3
Conduct the Audit

Opening Meeting
Facility Tour
Discovery
Closing Meeting

Step 4
Post-Audit Activities

Vendor Rating
Audit Report
Audit Follow-up
Vendor Audit Process – Off-Site

Step 1 Determine Audit Method
Step 2 Prepare for the Audit
Step 3 Conduct the Audit
Step 4 Post-Audit Activities

Off Site Audit
Planning
Notification
Team Selection
Document Reviews
Opening Meeting
Facility Tour
Discovery
Closing Meeting
Vendor Rating
Audit Report
Audit Follow-up

Vendor Audit Process – Questionnaire

Step 1 Determine Audit Method
Step 2 Prepare for the Audit
Step 3 Conduct the Audit
Step 4 Post-Audit Activities

Questionnaire Assessment
Planning
Notification
Team Selection
Document Reviews
Opening Meeting
Facility Tour
Discovery
Closing Meeting
Vendor Rating
Audit Report
Audit Follow-up
**Vendor Audit Process – Basic Assessment**

1. **Step 1** Determine Audit Method
2. **Step 2** Prepare for the Audit
3. **Step 3** Conduct the Audit
4. **Step 4** Post-Audit Activities

**Factors:**

1. System criticality (risk to product quality and patient safety)
2. Degree of reliance on vendor deliverables
3. Experience with the vendor
### How do you select an audit method?

<table>
<thead>
<tr>
<th>System Criticality</th>
<th>Use of Vendor Documentation in Validation</th>
<th>1st Application from Vendor</th>
<th>Subsequent Application from Vendor *</th>
</tr>
</thead>
<tbody>
<tr>
<td>High: Direct impact on product quality or patient safety</td>
<td>Yes</td>
<td>On Site Audit</td>
<td>Off Site Audit</td>
</tr>
<tr>
<td>High: Direct impact on product quality or patient safety</td>
<td>No</td>
<td>On Site Audit</td>
<td>Off Site Audit</td>
</tr>
<tr>
<td>Medium: Indirect impact on product quality or patient safety</td>
<td>Yes</td>
<td>Off Site Audit</td>
<td>Questionnaire</td>
</tr>
<tr>
<td>Medium: Indirect impact on product quality or patient safety</td>
<td>No</td>
<td>Questionnaire</td>
<td>Questionnaire</td>
</tr>
<tr>
<td>Low: No impact on product quality or patient safety</td>
<td>Yes</td>
<td>Basic Assessment</td>
<td>None</td>
</tr>
<tr>
<td>Low: No impact on product quality or patient safety</td>
<td>No</td>
<td>Basic Assessment</td>
<td>None</td>
</tr>
</tbody>
</table>

* With acceptable past performance

---

### Audit Preparation

Part 4
Part 4: Audit Preparation

Section Overview
- Audit Notification
- Audit Arrangements
- Audit Team Selection
- Checklists
- Document Reviews

Prepare for the Audit

Step 1
Determine Audit Method

Step 2
Prepare for the Audit

On Site Audit
- Planning
- Notification
- Team Selection
- Document Reviews

Off Site Audit
- Planning
- Notification
- Team Selection
- Document Reviews

Questionnaire, Basic Assessment
- Planning
- Notification
- Team Selection
- Document Reviews
Audit Planning

- Review Results of Prior Audits
- Plan Details Regarding:
  - Audit Purpose & Scope
  - Audit Standard(s)
  - Audit Agenda & Schedule
  - Checklists
  - Proposed Date(s)
  - Number of Auditors

Vendor Notification & Arrangements

- Notify Vendor of Intent to Audit
- Provide Audit Plan Details Regarding:
  - Audit Purpose & Scope
  - Audit Standard(s)
  - Audit Agenda & Schedule
  - Checklists
  - Proposed Date(s)
  - Number of Auditors
- Reach agreement on audit dates and times
- Documents to Review in Advance
Audit Team Selections

- Number of auditors depends on scope
- Lead Auditor:
  - Overall responsibility for audit
  - Qualified & experienced
- Audit Team:
  - Specific expertise, such as system's technology or software validation
  - Train if new to auditing

Pre-Review Documentation

- Improve audit efficiency
- Ask better questions
- More accurate audit results
Common Audit Standards

ICH Guidelines

Regulations (Laws)
- FDA 21 CFR ....
- Eudralex Volume ...

Company policies & procedures

influences

FDA Guidance & Reference Documents
- EMA Reflection Papers
- PIC/S Guidance Documents
- GAMP Guides (ISPE)
- IEEE Guides
- etc.

Common FDA Audit Standards

<table>
<thead>
<tr>
<th>Audience</th>
<th>Type</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Regulation</td>
<td>21 CFR 11: Electronic Records, Electronic Signatures</td>
</tr>
<tr>
<td>General</td>
<td>Guidance</td>
<td>Part 11, Electronic Records, Electronic Signatures – Scope and Application</td>
</tr>
<tr>
<td>General</td>
<td>Guidance</td>
<td>General Principles of Software Validation</td>
</tr>
<tr>
<td>General</td>
<td>Reference</td>
<td>FDA Office of Regulatory Affairs Laboratory Manual</td>
</tr>
<tr>
<td>Drug</td>
<td>Regulation</td>
<td>21 CFR 211: Current Good Manufacturing Practice in Manufacturing, Processing, Packing, or Holding of Drugs; General</td>
</tr>
<tr>
<td>Drug</td>
<td>Regulation</td>
<td>Current Good Manufacturing Practice for Finished Pharmaceuticals</td>
</tr>
<tr>
<td>Drug</td>
<td>Reference</td>
<td>FDA ORA Guide to Inspection of Computerized Systems in Drug Processing</td>
</tr>
<tr>
<td>Biological</td>
<td>Regulation</td>
<td>21 CFR 600: Biological Products: General</td>
</tr>
<tr>
<td>Device</td>
<td>Regulation</td>
<td>21 CFR 820: Quality System Regulation</td>
</tr>
<tr>
<td>Device</td>
<td>Guidance</td>
<td>Off-The-Shelf Software Use in Medical Devices</td>
</tr>
<tr>
<td>Device</td>
<td>Guidance</td>
<td>Contents for Premarket Submissions for Software Contained in Medical Devices</td>
</tr>
<tr>
<td>Blood</td>
<td>Regulation</td>
<td>21 CFR 606: Current Good Manufacturing Practice for Blood and Blood Components</td>
</tr>
<tr>
<td>Clinical</td>
<td>Regulation</td>
<td>21 CFR 50: Protection of Human Subjects</td>
</tr>
<tr>
<td>Clinical</td>
<td>Regulation</td>
<td>21 CFR 56: Institutional Review Boards</td>
</tr>
<tr>
<td>Clinical</td>
<td>Guidance</td>
<td>Computerized Systems Used in Clinical Investigations</td>
</tr>
<tr>
<td>Lab</td>
<td>Regulation</td>
<td>21 CFR 58: Good Laboratory Practice for Nonclinical Laboratory Studies</td>
</tr>
</tbody>
</table>
### Audit Checklists

**Topic: Internal Audits**

<table>
<thead>
<tr>
<th>Question</th>
<th>Observation</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does the vendor require internal audits?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Are internal audit results reviewed with management?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Are quality improvements made as the result of internal audits?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Ratings**

1 = Acceptable  
2 = Partially Acceptable  
3 = Not Acceptable

### Common Checklist Questions

**General Topics**

<table>
<thead>
<tr>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. How long has the vendor been in business?</td>
</tr>
<tr>
<td>2. In what industry(ies) does the vendor focus its resources?</td>
</tr>
<tr>
<td>3. How long has the product of interest been on the market?</td>
</tr>
<tr>
<td>What companies are using the product of interest?</td>
</tr>
<tr>
<td>4. Is an independent financial rating available?</td>
</tr>
<tr>
<td>5. Does the vendor have any certifications, such as ISO, Malcolm Baldridge?</td>
</tr>
<tr>
<td>6. Does the vendor’s strategy, business outlook, and organizational structure suggest a long-term commitment to the product and industry?</td>
</tr>
</tbody>
</table>
## General Quality Topics

<table>
<thead>
<tr>
<th>Question</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  Is there an overall program to ensure software quality?</td>
<td>Quality Plan (QP) or Quality Assurance Plan (QAP)</td>
</tr>
<tr>
<td>Does the program include a software life cycle, testing practices, documentation requirements, and responsibilities?</td>
<td></td>
</tr>
<tr>
<td>2  Is the quality organization independent from the IT organization?</td>
<td>Organization Charts</td>
</tr>
<tr>
<td>3  Does QA have a role in the system life cycle – especially in testing and system release?</td>
<td>QA Job Description, QAP (responsibilities)</td>
</tr>
<tr>
<td>4  Does the Quality group perform periodic audits of system quality, documentation, and procedural compliance?</td>
<td>Audit SOP, Audit records</td>
</tr>
</tbody>
</table>

## System Life Cycle & Requirements

<table>
<thead>
<tr>
<th>Question</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  Is there a formal system/software life cycle</td>
<td>SLC (SDLC)</td>
</tr>
<tr>
<td>2  Are detailed functional requirements available to clearly define what the system needs to do?</td>
<td>Requirements documents (User, Functional, System…)</td>
</tr>
<tr>
<td>Are requirements approved?</td>
<td></td>
</tr>
<tr>
<td>Are requirement changes approved?</td>
<td></td>
</tr>
<tr>
<td>3  Are there adequate, independent quality assurance assessments throughout the software development process?</td>
<td>SOPs, Deliverables throughout the SDLC</td>
</tr>
<tr>
<td>4  Do requirements include regulatory requirements (e.g., 21 CFR Part 11)?</td>
<td>Requirements documents (User, Functional, System…)</td>
</tr>
</tbody>
</table>
### Design and Coding

<table>
<thead>
<tr>
<th>Question</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Do formal coding standards and/or guidelines exist? If yes, do they</td>
<td>SOP; Design Documents</td>
</tr>
<tr>
<td>contain requirements for entity naming conventions, revision level</td>
<td></td>
</tr>
<tr>
<td>notations, program descriptions, data flow diagrams, structured coding?</td>
<td></td>
</tr>
<tr>
<td>2. Do formal user interface standards and/or guidelines exist?</td>
<td>SOP; Design Documents</td>
</tr>
<tr>
<td>3. Do formal design documentation standards and/or exist? If yes,</td>
<td>SOP; Design Documents</td>
</tr>
<tr>
<td>review examples.</td>
<td></td>
</tr>
<tr>
<td>4. Are all standards under change control?</td>
<td>SOP</td>
</tr>
</tbody>
</table>

### Testing

<table>
<thead>
<tr>
<th>Question</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Is there a testing procedure? Does the testing process include</td>
<td>SOP</td>
</tr>
<tr>
<td>requirements for testing types (e.g. unit, system, integration),</td>
<td></td>
</tr>
<tr>
<td>documenting test results, comparison of results to acceptance criteria,</td>
<td></td>
</tr>
<tr>
<td>formal approvals, and ongoing evaluation?</td>
<td></td>
</tr>
<tr>
<td>2. Are Test Plans used? Do Test Plans defines the approaches, data,</td>
<td>Test Plans</td>
</tr>
<tr>
<td>scenarios, conditions, responsibilities, and documentation needed to</td>
<td></td>
</tr>
<tr>
<td>establish the adequate performance of the system?</td>
<td></td>
</tr>
<tr>
<td>3. Are Test Summaries available? Do Test Summaries summarize all the</td>
<td>Test Summary</td>
</tr>
<tr>
<td>system's test deliverables and activities, and provide evidence that</td>
<td></td>
</tr>
<tr>
<td>the system is fully tested?</td>
<td></td>
</tr>
</tbody>
</table>
## Common Checklist Questions

### Testing

<table>
<thead>
<tr>
<th>Question</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Are there test protocols and results?</td>
<td>Protocols</td>
</tr>
<tr>
<td>Were the tests protocols approved prior to execution?</td>
<td></td>
</tr>
<tr>
<td>Do tests include sufficient details, such as data checks, calculations, security?</td>
<td></td>
</tr>
<tr>
<td>Were the test results reviewed and approved?</td>
<td></td>
</tr>
<tr>
<td>5. Are there traceability matrices between specifications and programs?</td>
<td>Trace Matrices</td>
</tr>
<tr>
<td>Between specifications and tests?</td>
<td></td>
</tr>
<tr>
<td>6. Are system changes tested? Does testing include regression testing of unmodified functionality?</td>
<td>SOP Test Summary</td>
</tr>
</tbody>
</table>

### System Documentation

<table>
<thead>
<tr>
<th>Question</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does the system have up to date documentation, including data structures and flows, interactions with other systems, design &amp; architecture?</td>
<td>System design documents</td>
</tr>
<tr>
<td>2. Is the documentation updated each time a change is made?</td>
<td>System design documents</td>
</tr>
<tr>
<td>3. Is documentation managed using change control?</td>
<td>Document Management SOP; Document change records</td>
</tr>
<tr>
<td>4. What is the retention time period for all system related documentation?</td>
<td>SOP</td>
</tr>
<tr>
<td>5. How are paper records protected from loss?</td>
<td>SOP; review of retention areas</td>
</tr>
<tr>
<td>How are electronic records protected from loss?</td>
<td></td>
</tr>
</tbody>
</table>
### System Documentation

<table>
<thead>
<tr>
<th>Question</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>6  How are source code, programs, and configuration settings managed and protected? Who has access? Describe how the source code for a given release is controlled.</td>
<td>SOP; source code check-in/check-out records</td>
</tr>
<tr>
<td>7  Are back-ups retained in a separated, secure location? Are back-ups retained for the duration required?</td>
<td>Back-up SOP; back-up records</td>
</tr>
<tr>
<td>8  Is there a disaster recovery plan (DRP)? Has the plan been executed (tested)?</td>
<td>DRP; test protocol, results</td>
</tr>
</tbody>
</table>

### Security

<table>
<thead>
<tr>
<th>Question</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  Is there an adequate security system to prevent unauthorized modification of source code, builds, and distribution copies of software? What are the security measures?</td>
<td>SOP; source code check-in/check-out records</td>
</tr>
<tr>
<td>2  Are the development and manufacturing facilities adequately secured against unauthorized entry? Is there a documented authorization list? How is access authorized?</td>
<td>SOP; observation of practices</td>
</tr>
</tbody>
</table>
Common Checklist Questions

Procedures

<table>
<thead>
<tr>
<th>Question</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Is the system supported by approved procedures?</td>
<td>SOPs</td>
</tr>
<tr>
<td>Do procedures include disaster recovery, back up, maintenance (if hosted), information security, incident management, system change control, and configuration management?</td>
<td></td>
</tr>
<tr>
<td>2 Are procedures under change control?</td>
<td>Document Management SOP; Document change records</td>
</tr>
<tr>
<td>3 Are the procedures periodically reviewed?</td>
<td>SOP; Periodic Review Records</td>
</tr>
</tbody>
</table>

Change Management

<table>
<thead>
<tr>
<th>Question</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Are system changes documented? Are system changes approved?</td>
<td>System Change records</td>
</tr>
<tr>
<td>2 Are changes evaluated for the degree of testing needed?</td>
<td>Records of evaluations</td>
</tr>
<tr>
<td>3 Are configuration changes documented?</td>
<td>Configuration Change records</td>
</tr>
<tr>
<td>4 Is system documentation updated when changes are made</td>
<td>Updated documentation</td>
</tr>
<tr>
<td>5 Are users and support personnel retrained when changes are made?</td>
<td>Training records</td>
</tr>
</tbody>
</table>
### Support

<table>
<thead>
<tr>
<th>Question</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does the vendor utilize a maintenance/support agreement?</td>
<td>Standard agreement or template</td>
</tr>
<tr>
<td>If yes, what software product elements are maintained and supported?</td>
<td></td>
</tr>
<tr>
<td>2. Are prior releases adequately supported?</td>
<td>Policy of supporting prior releases</td>
</tr>
<tr>
<td>How long are prior releases supported?</td>
<td></td>
</tr>
<tr>
<td>3. Is the vendor’s help desk support function for software and hardware adequate?</td>
<td>Policy for help desk support</td>
</tr>
<tr>
<td>What is the availability of the help desk?</td>
<td></td>
</tr>
<tr>
<td>4. Does the documentation for new releases of the product provide enough information to allow the customer to determine the impact of every change in the release?</td>
<td>Example of release documentation sent to customers</td>
</tr>
</tbody>
</table>

### Incident Management

<table>
<thead>
<tr>
<th>Question</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Are system incidents documented?</td>
<td>Incident records</td>
</tr>
<tr>
<td>Are errors, bugs, and defects categorized by severity, urgency, and priority?</td>
<td></td>
</tr>
<tr>
<td>2. Are records maintained of all known problems for each revision?</td>
<td>Incident records</td>
</tr>
<tr>
<td>3. Are system incidents evaluated to determine correction and prevention activities?</td>
<td>Incident records; CAPA system</td>
</tr>
<tr>
<td>4. Are system users made aware of critical system defects? How quickly?</td>
<td>Notifications</td>
</tr>
<tr>
<td>5. Does the vendor have an effective program for resolving documented defects?</td>
<td>Incident records</td>
</tr>
</tbody>
</table>
### Data Integrity & Protection

<table>
<thead>
<tr>
<th>Question</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Is the system secured by unique user-ids and passwords</td>
<td>Requirements; test protocol, results</td>
</tr>
<tr>
<td>2 Are there controls to ensure that data can only be entered and changed by authorized personnel?</td>
<td>Requirements; test protocol, results</td>
</tr>
<tr>
<td>3 Is access to high levels of access (e.g., Super User) restricted.</td>
<td>Requirements; test protocol, results</td>
</tr>
<tr>
<td>4 Is critical data verified by a 2nd person, or by a validated electronic method?</td>
<td>Requirements; test protocol, results</td>
</tr>
</tbody>
</table>

### Audit Trails

<table>
<thead>
<tr>
<th>Question</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Is there an audit trail for critical data and activities?</td>
<td>Requirements; Test protocol, results</td>
</tr>
<tr>
<td>2 Does the audit trail include user, date, time?</td>
<td>Requirements; Test protocol, results</td>
</tr>
<tr>
<td>3 Can the audit trail be reviewed for irregularities?</td>
<td>Requirements; Test protocol, results</td>
</tr>
</tbody>
</table>
## Training & Personnel

<table>
<thead>
<tr>
<th>Question</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does the vendor have its own development staff? If so, how many?</td>
<td></td>
</tr>
<tr>
<td>What is the percentage of contract developers vs. Vendor employed developers?</td>
<td></td>
</tr>
<tr>
<td>What is the turnover rate?</td>
<td></td>
</tr>
<tr>
<td>2. Is there documentation on the qualifications and training background of personnel engaged in design, coding, testing, validation, installation, and operation of the systems?</td>
<td>Training requirements; Training records; Resumes</td>
</tr>
<tr>
<td>Does this include consultants and sub-contractors?</td>
<td></td>
</tr>
</tbody>
</table>

## Vendors (sub-contractors)

<table>
<thead>
<tr>
<th>Question</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Are there policies and procedures for assessing potential suppliers of hardware and software?</td>
<td>Vendor Assessment SOP; Assessment records</td>
</tr>
<tr>
<td>2. Is documentation provided by the vendor reviewed and approved internally?</td>
<td>Approvals</td>
</tr>
</tbody>
</table>
How is the vendor preparing for the audit?

Step 1. Review checklists and Audit Standards
Step 2. Determine which systems are in scope
Step 3. Staff the auditee team
Step 4. Locate documentation & procedures
Step 5. Conduct mock audit

Audit Execution

Part 5
Part 5: Audit Execution

Section Overview
- Opening Meeting & Tour
- Discovery
- Auditee and Auditor behavior
- Finding Categorization
- Closing Meeting

Conduct the Audit

Step 2 Prepare for the Audit

Step 3 Conduct the Audit

On Site Audit
- Opening Meeting
- Facility Tour
- Discovery
- Closing Meeting

Off Site Audit
- Opening Meeting
- Facility Tour
- Discovery
- Closing Meeting

Questionnaire, Basic Assessment
- Opening Meeting
- Facility Tour
- Discovery
- Closing Meeting
Opening Meeting

- Attendees:
  - Audit Team
  - Vendor management & audit team

- Agenda:
  - Introductions
  - Audit Schedule
  - Logistics
  - Company Overview

Facility Tour

<table>
<thead>
<tr>
<th>Areas to Observe</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑️ Are facilities neat and in good repair?</td>
</tr>
<tr>
<td>☑️ Are physical security practices followed?</td>
</tr>
<tr>
<td>☑️ Are data security practices followed?</td>
</tr>
<tr>
<td>☑️ Are documentation security practices followed?</td>
</tr>
</tbody>
</table>
Discovery

- The Main Event
- Logistics
- Coordinators
- Escorts

Any Topic:
- Are there documented policies and procedures?
- Are the policies and procedures followed?
- Are the policies and procedures effective?

Discovery Flow

Discovery Techniques

Interview
Observe
Auditor Approaches

- Sampling
- Trace Forward
- Trace Backwards
- Checklists

Auditor Techniques

<table>
<thead>
<tr>
<th>Interview and Observe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open ended questions</td>
</tr>
<tr>
<td>Paraphrasing</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Silence / Long Pause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Empathy</td>
</tr>
<tr>
<td>Aggression</td>
</tr>
<tr>
<td>Good Cop – Bad Cop</td>
</tr>
</tbody>
</table>
What If…

– The auditee doesn’t know the answer to the question being asked?

Accept the answer “I’ll get back to you”

Make a note

Follow-up later in the audit

What If…

– The vendor refuses to answer an audit question and states that it’s ‘confidential information’?

Be willing to sign a non-disclosure agreement in order to see the requested information

Or if a non-disclosure agreement is not utilized

In the audit report, note the information that was not reviewed.
What If…

– A deficiency is found?

Alert the vendor’s audit coordinator

Explain the deficiency vs. the audit standard

Note the deficiency in the audit report

If the deficiency is correct immediately…

Verify the correction

Note the correction in the audit report

Auditor Conduct

DO

• Professional
• Courteous
• Friendly
• Objective
• Accurate
• Calm

• Keep information confidential
• Ask for clarification
• Record interviewee names and positions, questions asked, answers provided, and evidence reviewed
Auditor Conduct

DON’T

• Argue or debate with the auditee team
• Act judgmental
• Use negative body language
• Waste auditees’ time
• Accept gifts or bribes

Watch Out For…

Antagonistic or Defensive Auditees

– Remain professional
– Stick to audit plan

Time Wasters

– Missing escort
– Late starts, long lunches
– MIA interviewees
– Extensive company overviews, tours
– Excessive socializing

Bribes

– Obvious
– Subtle
Categorize Audit Findings

Use a risk-based approach

<table>
<thead>
<tr>
<th>Category</th>
<th>Definition (example 1)</th>
<th>Category</th>
<th>Definition (example 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Vendor’s practice has compromised the quality of the product</td>
<td>Critical</td>
<td>Vendor’s practice deviates from regulation</td>
</tr>
<tr>
<td>Major</td>
<td>Vendor’s practice could potentially compromise the quality of the product</td>
<td>Major</td>
<td>Vendor’s practice deviates from regulatory guidance or industry standard</td>
</tr>
<tr>
<td>Minor</td>
<td>Vendor’s practice compromises non-essential attributes of the product</td>
<td>Minor</td>
<td>Vendor’s practice deviates from the auditing company’s view of best practices</td>
</tr>
</tbody>
</table>

Closing Meeting

- **Attendees:**
  - Audit Team
  - Vendor management & audit team

- **Agenda:**
  - Draft Audit Report
  - Findings and Observations
  - Corrective Action Requests
  - Timeline for final Audit Report
Post Audit

Part 6

Section Overview
- Vendor Rating
- Audit Report
- Corrective Action Requests
- Audit Follow-up
Post-Audit Activities

On Site Audit
- Vendor Rating
- Audit Report
- Audit Follow-up

Off Site Audit Questionnaire
- Vendor Rating
- Audit Report
- Audit Follow-up

Basic Assessment
- Vendor Rating
- Audit Report
- Audit Follow-up

Vendor Rating

Determine whether or not vendor is acceptable

<table>
<thead>
<tr>
<th>Rating</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Approval</td>
<td>Unrestricted approval is granted to the vendor.</td>
</tr>
<tr>
<td>Conditional Approval</td>
<td>Limited approval is granted to the vendor.</td>
</tr>
<tr>
<td></td>
<td>Document limitations, reasons for restrictions, and conditions for removal of restrictions in the Audit Report.</td>
</tr>
<tr>
<td>Not Approved</td>
<td>No approval is granted to the vendor.</td>
</tr>
<tr>
<td></td>
<td>Document reason(s) for disapproval and conditions for approval in the Audit Report.</td>
</tr>
</tbody>
</table>
Vendor Rating

Depending on scope of audit, rate vendor in multiple areas

<table>
<thead>
<tr>
<th>Vendor Product</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software</td>
<td>Full Approval</td>
</tr>
<tr>
<td>Validation Documentation</td>
<td>Conditional Approval</td>
</tr>
<tr>
<td>Training Services</td>
<td>Not Approved</td>
</tr>
</tbody>
</table>

Audit Report

- Introduction
  - Summary of the audit purpose, scope, dates, location, participants, audit standard

- Findings
  - Supporting Observations

- Approvals

- Corrective Action Requests (CARs)
Audit Report

**Introduction:**
- Audited Organization: _______________
- Auditing Organization: _______________
- Audit Date(s): _______________
- Location: _______________
- Scope (product, processes): _______________
- Audit Standard(s): _______________
- Audit Checklist(s): _______________

**Audit Team**

<table>
<thead>
<tr>
<th>Principle Contacts</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Audit Report**

**Findings:**

<table>
<thead>
<tr>
<th>#</th>
<th>Category</th>
<th>Finding Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Critical</td>
<td>Description of finding here</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Observation supporting finding here</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Observation supporting finding here</td>
</tr>
<tr>
<td>2</td>
<td>Major</td>
<td>Description of finding here</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Observation supporting finding here</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Observation supporting finding here</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Observation supporting finding here</td>
</tr>
</tbody>
</table>

Etc.
Audit Report

Audit Result:

_________________________________________________________________
_________________________________________________________________
_________________________________________________________________
_________________________________________________________________

Report Approval:

_____________________ _____________________
Lead Auditor              Head of Quality

What Not to Include

• Subjective Information, Opinions
• Trivial Items
• Recommendations
• Names of employees associated with findings
• Topics not discussed in the Closing Meeting
Corrective Action Request (CAR)

Corrective Action Request
The following condition is brought to your attention for corrective action

Discrepant Condition: ____________________________________________________________

________________________________________________________

________________________________________________________

Auditee Portion
Root Cause: ____________________________________________________________

Action to Correct: ____________________________________________________________

________________________________________________________

________________________________________________________

Scheduled Completion Date: _____ Signature/Date _____________

Follow-Up

Audit Report for Company XYZ

Yes

CARs

No

Response to Corrective Action Request

Verify Corrective Action Taken by Vendor

OK?

Yes

Modify Vendor Rating (opt.)

Close Audit Retain Records

Close Audit Retain Records

OK

Praxis Life Sciences | praxislifesciences.com
1925 West Field Court, Suite 125, Lake Forest, IL 60045 | +1 (847) 295-7160

Validation Center™ validationcenter.com
Leveraging Audit Results in a Risk-based Validation Approach

Part 7

Part 7: Leveraging Audit Results

Section Overview

- Using audit results as input to the Validation Plan
Scenario 1

Your Policy: Requirements & Test Protocols for validated systems
Vendor: Willing to provide requirements and validation protocols
Vendor Audit: Evaluated the vendor’s quality and procedures for requirements documentation and protocol development

Vendor Rating

Full Approval
- Use vendor’s requirements documentation & validation protocols as starting point
- Review and approve vendor-provided documents in-house

Not Approved
- Do not use vendor’s validation documentation
- Write in-house, as normal

Scenario 2

Your Policy: Comprehensive testing with 100% path coverage using multiple data scenarios for features of validated systems
Vendor: Does not provide protocols or results
Vendor Audit: Evaluated the vendor’s software quality & SDLC procedures

Vendor Rating

Full Approval
- Reduced path coverage and data scenarios, especially for less critical features

Not Approved
- Perform thorough testing with 100% path coverage using multiple data scenarios
Scenario 3

Your Policy: Validated systems must be hosted on qualified infrastructure
Vendor: Offers to host system on vendor's servers
Vendor Audit: Evaluated the vendor's infrastructure qualification practices and support procedures

Vendor Rating

- Full Approval
  - Allow vendor to host system
  - Periodically audit vendor's hosting service

- Not Approved
  - Do not allow vendor to host the validated system
  - Host in house, or on other qualified infrastructure

FDA Warning Examples

Part 8
FDA Warning Example

<table>
<thead>
<tr>
<th>Company Location</th>
<th>Germany</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Product</td>
<td>Endoscopic grasping/cutting instruments</td>
</tr>
<tr>
<td>Software Type</td>
<td>ERP / Inventory Control</td>
</tr>
</tbody>
</table>

Failure to establish and maintain adequate procedures to ensure that all purchased products and services conform to specified requirements.
- The procedure which addresses vendor selection qualification and requalification of suppliers, has not been not implemented. There is no documentation that the supplier of Majesty software, was qualified or re-qualified. The firm has been purchasing software from this vendor since 1996.
- The firm’s requirements to requalify vendors are not based on the vendor’s ability to meet specified requirements, including quality requirements. In addition, the criticality of the purchased product or service is not evaluated for determining the needs to requalify suppliers.

FDA Warning Examples

<table>
<thead>
<tr>
<th>Company Location</th>
<th>California, USA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Product</td>
<td>Foldable, implantable lenses for eyes</td>
</tr>
<tr>
<td>Software Type</td>
<td>Software used by surgeons to calculate proper lenses</td>
</tr>
</tbody>
</table>

Failure to establish procedures to ensure that all purchased products and services conform to specified requirements.
- A critical supplier, contractor and consultant of software has a pending status since 2007. This supplier has never been audited, provided a supplier questionnaire, or a Curriculum Vitae.

<table>
<thead>
<tr>
<th>Company Location</th>
<th>Illinois, USA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Business</td>
<td>Importer/distributor of diagnostic &amp; therapeutic devices</td>
</tr>
<tr>
<td>Software Type</td>
<td>Complaint System</td>
</tr>
</tbody>
</table>

Failure to adequately validate computer software used in an automated process for its intended use according to an established protocol.
- No person from your firm reviewed or approved the third party test results for the XXX Complaint System used in the firm’s quality system.
Firm fails to complete purchasing control activities according to the purchasing control procedure, CO-QA-056 Rev A, *Selection and Approval of Service Providers*, for software suppliers responsible for software development for the medical device.

Firm's SOP CO-QA-056 Rev B, *Purchasing Control for Outside Services*, does not assure that software suppliers complete both function and structural software testing.

### Need Help?

- [Vendor Assessment SOP and Checklist](ValidationCenter.com)
- [Online and Classroom CSV Training](ValidationCenter.com)
- [Validation Services](ValidationCenter.com)
- [3rd Party Vendor Audits](ValidationCenter.com)
Thank You!

Thanks for your interest in Auditing Software Vendors.

Any questions about what we have discussed today?
Please, feel free to call or e-mail me:

Deb Bartel
+1 (847) 295-7160
dbartel@PraxisLifeSciences.com

ValidationCenter.com | PraxisLifeSciences.com