
Standard Operating Procedure

Risk-Based Validation of Laboratory Computer Systems



This is an example of a Standard Operating Procedure. It is a proposal and starting point only. The type and extent of documentation depends on the process environment. The proposed documentation should be adapted accordingly and should be based on individual risk assessments. There is no guarantee that this document will pass a regulatory inspection.

Publication from www.labcompliance.com

Global on-line resource for validation and compliance

Copyright by Labcompliance. This document may only be saved and viewed or printed for personal use. Users may not transmit or duplicate this document in whole or in part, in any medium. Additional copies and licenses for department, site or corporate use can be ordered from www.labcompliance.com/solutions.

While every effort has been made to ensure the accuracy of information contained in this document, Labcompliance accepts no responsibility for errors or omissions. No liability can be accepted in any way.

Labcompliance offers books, master plans, complete Quality Packages with validation procedures, scripts and examples, SOPs, publications, training and presentation material, user club membership with more than 300 downloads and audio/web seminars. For more information and ordering, visit www.labcompliance.com/solutions

Company Name:	
----------------------	---

Controls:	
Superseded Document	N/A, new
Reason for Revision	N/A
Effective Date	August 1, 2004

Signatures:	
Author	<p>I indicate that I have authored or updated this SOP according to applicable business requirements and our company procedure: Preparing and Updating Standard Operating Procedures.</p> <p>Name: _____</p> <p>Signature: _____</p> <p>Date: _____</p>
Approver	<p>I indicate that I have reviewed this SOP, and find it meets all applicable business requirements and that it reflects the procedure described. I approve it for use.</p> <p>Name: _____</p> <p>Signature: _____</p> <p>Date: _____</p>
Reviewer	<p>I indicate that I have reviewed this SOP and find that it meets all applicable quality requirements and company standards. I approve it for use.</p> <p>Name: _____</p> <p>Signature: _____</p> <p>Date: _____</p>

Risk-Based Validation of Laboratory Computer Systems**1. PURPOSE**

Laboratory computer systems should be validated for compliance and business reasons. The extent of validation depends on the risk the system can have on product quality and safety and on the complexity. This SOP gives guidelines on what the extent of validation should be for risk categories as defined by the SOP in Reference 4.2.

2. SCOPE

Risk-based validation of laboratory computer systems and other computer related GxP requirements such as limited access, system audits and change control.

3. GLOSSARY/DEFINITIONS

Item	Explanation
GAMP	Good Automated Manufacturing Practice (Forum). The GAMP Forum exists to promote the understanding of the regulation and use of computer and control systems within the pharmaceutical manufacturing industry.
GAMP Category 3	Standard software package. All applications problems are solved with standard functions. However, typically not all available functions are exercised by the user's application.
GAMP Category 4	Configurable software package. Provides standard interfaces and functions that enable configuration of user specific applications.
GAMP Category 5	Custom software package. Developed to meet specific needs of an application. Custom software may be a complete system or add on to a standard package. Custom software may be developed and supported in-house or by an external supplier.
Standard Function	Function that comes with software GAMP Category 3.
Critical Requirement	Requirement that the user determines to be critical for the effective use of the system.

Note: For other definitions, see www.labcompliance.com/glossary.

4. REFERENCE DOCUMENTS

- 4.1. GAMP 4 Guide: "Validation of Automated Systems", ISPE, Brussels, 2001
(order from www.ispe.org).
- 4.2. SOP S-519 "Risk Assessment for Laboratory Systems".
Available through www.labcompliance.com/solutions/sops
- 4.3. "Risk Management Master Plan".
Available through www.labcompliance.com/books/risk.

5. RESPONSIBILITIES

5.1. System Owner

- 5.1.1. Owns the process to define and document extent of validation for a specific system.
- 5.1.2. Drafts documentation.

5.2. Laboratory Manager

- 5.2.1. Reviews and approves documentation.

5.3. Quality Assurance

- 5.3.1. Advises on regulations and guidelines related to GxP and 21 CFR Part 11.
- 5.3.2. Reviews documentation for compliance with internal policies and guidelines.
- 5.3.3. Approves documentation.

6. FREQUENCY OF USE

Risk-Based Validation of Laboratory Computer Systems

- 6.1. Initially whenever equipment is qualified and software and computer systems are validated.
- 6.2. After system updates or other changes and the change indicates that the extent of qualification or validation may need to be changed.
- 6.3. Whenever system reviews indicate that the extent of qualification or validation may need to be changed.

7. PROCEDURE

7.1. System owner defines validation steps for life cycle phases and tasks using Tables 7.1.1 to 7.1.9 as guidelines.

7.1.1. Planning

Validation Steps – Planning			
System	GAMP 3	GAMP 4	GAMP 5
High Risk	Detailed validation plan with all activities, deliverables, owners, and timetables.	Detailed validation plan with all activities, deliverables, owners, and timetables.	Detailed validation plan with all activities, deliverables, owners, and timetables.
Medium Risk	High-level plan with key activities.	High-level plan with key activities.	High-level plan with key activities.
Low Risk	No specific plan.	High-level plan with key activities.	High-level plan with key activities.

7.1.2. Setting Specifications

Validation Steps – Setting Specifications			
System	GAMP 3	GAMP 4	GAMP 5
High Risk	Document all requirements. Uniquely number all requirements. Define critical vs. non-critical.	Document all requirements. Uniquely number all requirements. Define critical vs. non-critical.	Document all requirements. Uniquely number all requirements. Define critical vs. non-critical.
Medium Risk	Document all requirements.	Document all requirements. Uniquely number all requirements. Define critical vs. non-critical	Document all requirements. Uniquely number all requirements. Define critical vs. non-critical.
Low Risk	High-level system descriptions.	Define and document all non-standard requirements.	Define and document all non-standard requirements.

7.1.3. Vendor Assessment

Validation Steps – Vendor Assessment			
System	GAMP 3	GAMP 4	GAMP 5
High Risk	Review of vendor documentation.	Vendor audit.	Vendor audit.
Medium Risk	Document experience with vendor and system.	Review of vendor documentation.	Vendor audit.
Low Risk	None.	None.	None.

7.1.4. Installation

Validation Steps – Installation			
System	GAMP 3	GAMP 4	GAMP 5
High Risk	Verify correct software installation. Document system and all components and configurations. Document software versions.	Verify correct software installation. Document system and all components and configurations. Document software versions.	Verify correct software installation. Document system and all components and configurations. Document software versions.
Medium Risk	Document system and all components and configurations. Document software versions.	Document system and all components and configurations. Document software versions.	Document system and all components and configurations. Document software versions.
Low Risk	Document system and all components and configurations. Document software versions.	Document system and all components and configurations. Document software versions.	Document system and all components and configurations. Document software versions.

Risk-Based Validation of Laboratory Computer Systems

7.1.5. Functional Testing

Validation Steps – Functional Testing			
System	GAMP 3	GAMP 4	GAMP 5
High Risk	Test critical functions. Link tests to requirements.	Test critical standard functions. Test all non-standard functions. Link tests to requirements.	Test critical standard functions. Test all non-standard functions. Link tests to requirements.
Medium Risk	Test critical functions.	Test all critical standard and non-standard functions. Link tests to requirements.	Test critical standard functions. Test all non-standard functions. Link tests to requirements.
Low Risk	No testing.	Test critical non-standard functions.	Test critical non-standard functions.

7.1.6. Ongoing Maintenance and Performance Control

Validation Steps – Ongoing Control			
System	GAMP 3	GAMP 4	GAMP 5
High Risk	Regular virus check. Regular regression testing.	Regular virus check. Regular regression testing.	Regular virus check. Regular regression testing.
Medium Risk	Regular virus check.	Regular virus check. Regular regression testing.	Regular virus check. Regular regression testing.
Low Risk	Regular virus check.	Regular virus check.	Regular virus check.

Risk-Based Validation of Laboratory Computer Systems

7.1.7. Security Controls

Validation Steps – Security Controls			
System	GAMP 3	GAMP 4	GAMP 5
High Risk	Regular review of user access lists. Regular check of access controls.	Regular review of user access lists. Regular check of access controls.	Regular review of user access lists. Regular check of access controls.
Medium Risk	Regular review of user access lists.	Regular review of user access lists.	Regular review of user access lists.
Low Risk	Regular review of user access lists.	Regular review of user access lists.	Regular review of user access lists.

7.1.8. Change Control

Validation Steps – Change Control			
System	GAMP 3	GAMP 4	GAMP 5
High Risk	All changes approved by system owner and QA.	All changes approved by system owner and QA.	All changes approved by system owner and QA.
Medium Risk	All changes approved by system owner.	All changes approved by system owner.	All changes approved by system owner.
Low Risk	All changes documented by user.	All changes documented by user.	All changes documented by user.

7.1.9. Audits

Validation Steps – Audits			
System	GAMP 3	GAMP 4	GAMP 5
High Risk	Regular audit of system and subsystems. Regular review of the audit plan.	Regular audit of system and subsystems. Regular review of the audit plan.	Regular audit of system and subsystems. Regular review of the audit plan.
Medium Risk	“For cause” audits in case of problems.	“For cause” audits in case of problems.	“For cause” audits in case of problems.
Low Risk	None.	“For cause” audits in case of problems.	“For cause” audits in case of problems.

7.2. Review and Approval

7.2.1. The documents as developed in sections 7.1.1 to 7.1.9 are reviewed and approved by the laboratory manager for compliance with business practices.

7.2.2. The documents as developed in sections 7.1.1 to 7.1.9 are reviewed and approved by the QA management for compliance with regulations and internal standards and guidelines.

7.3. Regular Review and Updates

7.3.1. Definition of validation steps is an ongoing process. The system owner reviews Tables 7.1.1 to 7.1.9 every year and updates the tables, if necessary.

7.3.2. Updates from 7.3.1 are reviewed and approved following sections 7.2.1 and 7.2.2.