Critical Thinking, Not Categorization

An explanation of GAMP® categories, the risk-based approach, critical thinking, and Computer Software Assurance (CSA) in the context of Computerized System Validation (CSV)

Charlie Wakeham, Waters APAC GxP Compliance Manager
Secretary, GAMP Global Steering Committee
Co-lead and contributing author of ISPE GAMP RDI Good Practice Guide: Data Integrity by Design

INTRODUCTION

As early as the 1970s the US FDA had begun to identify that an unvalidated computerized system presented a risk to patient safety, product quality, and data integrity, and had begun to formulate guidance on this topic (Wingate G. , 1995).

Regulatory requirements for CSV were formally introduced into European GMP EudraLex Volume 4, Annex 11 in 1992, with the requirement, "before a system using a computer is brought into use, it should be thoroughly tested and confirmed as being capable of achieving the desired results."

This was reflected in the US cGMP with the 1997 issuance of 21 CFR Part 11, which required "validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records."

GAMP GUIDANCE

Volunteer subject matter experts in the UK began writing industry guidances after a series of FDA inspection findings on their sites in 1991. This volunteer group published under the moniker "GAMP"* and later became a technical subcommittee of the International Society of Pharmaceutical Engineers (ISPE). Today, the ISPE GAMP guides are accepted globally by industry and regulators alike as setting the standard for life sciences good practices in GxP computerized systems and data integrity.

**Note - The name GAMP was created from an acronym, but the original acronym usage has been discontinued and GAMP is now a brand name trademarked by ISPE.*

In GAMP 4 (ISPE, 2001), the concept of Software and Hardware categories were introduced to provide a reference model to enable CSV practitioners to differentiate between systems of different complexity, including the extent of any customization, and to tailor the validation approach accordingly. The categories were:

- Software Category 1 – Infrastructure Software
- Software Category 2 – Firmware
- Software Category 3 – Non-configured Products
- Software Category 4 – Configured Products
- Software Category 5 – Custom Applications
- Hardware Category 1 – Standard Hardware Components
- Hardware Category 2 – Custom Built Hardware Components

KEY EVENTS BEHIND THE NEED FOR CSV AND THE DEVELOPMENT OF THE CSV PROCESS

- **1985–1987:** Patient deaths from a bug in the computerized system controlling the Therac 25 radiation therapy device
- **1988:** A bug in data management software controlling a blood bank could have led to the issue of AIDS-infected blood
- **1991:** FDA bans import of products based on computer systems' non-compliances found during inspections of several European manufacturing sites
- **1992:** Second Edition of EU GMP Guidelines includes Annex 11 on Computerized Systems

(continued)

KEY EVENTS BEHIND THE NEED FOR CSV AND THE DEVELOPMENT OF THE CSV PROCESS (CONTINUED)

- **1995:** Supplier Guide for Validation of Automated Systems in Pharmaceutical Manufacture ("GAMP 1") published
- **1996:** Supplier Guide for Validation of Automated Systems in Pharmaceutical Manufacture ("GAMP 2") published
- **1997:** 21 CFR Part 11 published
- **1998:** Guide for Validation of Automated Systems in Pharmaceutical Manufacture ("GAMP 3") published

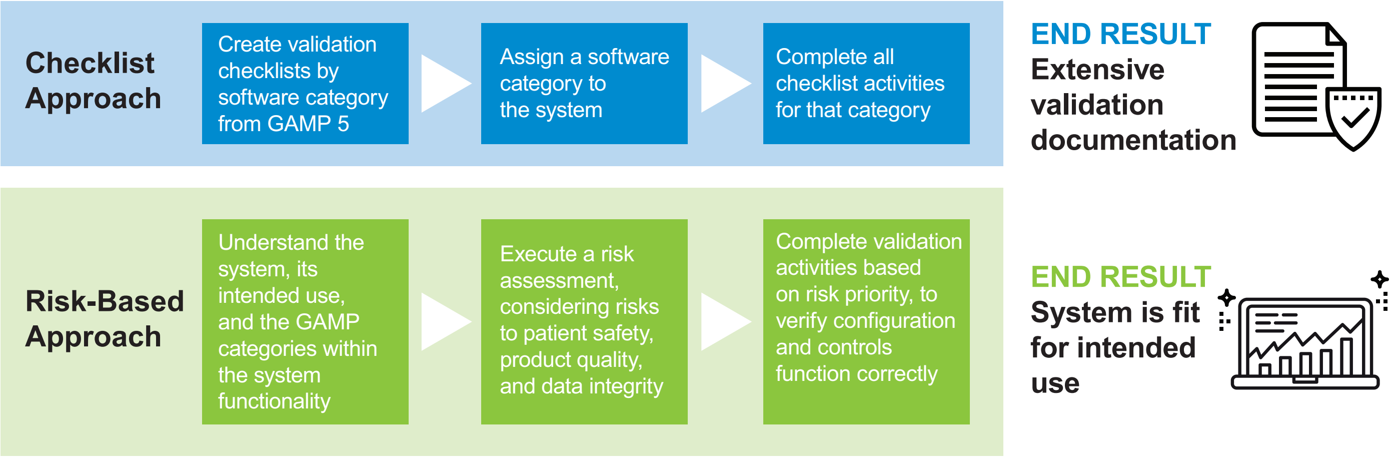
Configured products are defined as "stock programs that can be configured to specific user applications by 'filling in the blanks,' without altering the basic program" (Wingate, 1997), whereas a custom application involves creating bespoke code.

GAMP 4 was published around the same time that the US FDA began to formulate ideas around the need to consider a more risk-based approach to inspections, which they proposed in their 2002 document, "Pharmaceutical Current Good Manufacturing Practices (CGMPs) for the 21st Century", and formally endorsed in their 2004 Final Report, "Pharmaceutical CGMPs for the 21st Century – A Risk-Based Approach".

GAMP 5 (ISPE, 2008) was created in response to this FDA initiative, providing pragmatic guidance on how to apply the risk-based approach to CSV. Software Category 2 (firmware) was removed but the other categories remained, as many in the industry had based their CSV policies on these categories.

The presence of fixed categories in a risk-based approach can seem like a contradiction within GAMP 5. The risk-based approach is a continuum, a sliding scale of risk with mitigation and validation strategies designed to be commensurate with the assessed risk. The GAMP categories can encourage "silo-thinking", and indeed many CSV practitioners have erred this way. While GAMP 5 offers examples of activities that may be relevant for a particular category of software, such examples were never intended to be used as a checklist for compliance. Figure 1 shows shows a comparison of checklist vs. risk-based approaches, and the different end results from these approaches.

The aim of validation should always be to ensure that the system is fit for intended use and will safeguard patient safety, product quality, and data integrity. GAMP categories are best leveraged to help your understanding of the degree of configuration or customization within the system functionality that you will use, as this can impact the risks associated with the system.



Checklist Approach

Create validation checklists by software category from GAMP 5 → Assign a software category to the system → Complete all checklist activities for that category

END RESULT Extensive validation documentation

Risk-Based Approach

Understand the system, its intended use, and the GAMP categories within the system functionality → Execute a risk assessment, considering risks to patient safety, product quality, and data integrity → Complete validation activities based on risk priority, to verify configuration and controls function correctly

END RESULT System is fit for intended use

Figure 1. Comparison of Checklist vs. Risk-Based approaches.

MORE THAN A SINGLE CATEGORY

Few applications consist of a single category of software. There will be standard elements comprising the core functionality of the systems, configuration options applied by licensing to activate additional modules within the code or by configuring a workflow or signature routing, and most sophisticated applications will include some option for the user to easily create custom elements specific to their laboratory's intended use within the application. For example, a pH meter might be initially assumed to be Category 3 (non-configured product), but today's modern pH meters could also include a level of configuration, for example, configuring the serial output from the available options, which would introduce Category 4 elements.

The aim of validation should always be to ensure that the system is fit for intended use, and will safeguard patient safety, product quality, and data integrity. GAMP categories are best leveraged to help your understanding of the degree of configuration or customization within the system functionality that you will use, as this can impact the risks associated with the system.

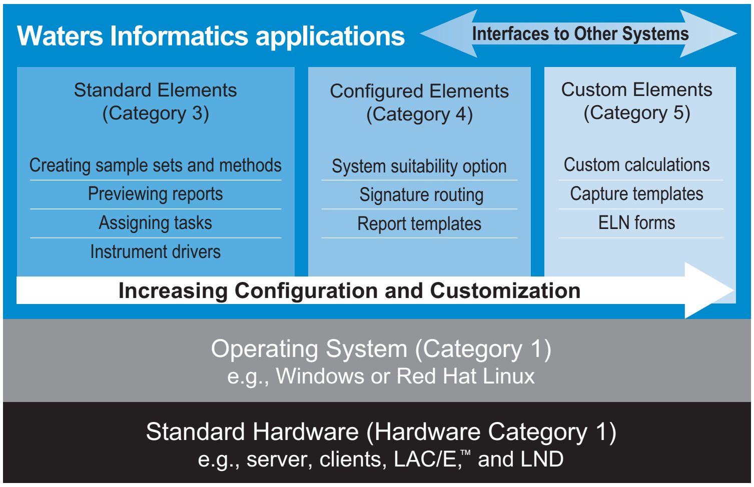

Waters Informatics applications
Interfaces to Other Systems
Standard Elements (Category 3)
Creating sample sets and methods
Previewing reports
Assigning tasks
Instrument drivers
Configured Elements (Category 4)
System suitability option
Signature routing
Report templates
Custom Elements (Category 5)
Custom calculations
Capture templates
ELN forms
Increasing Configuration and Customization
Operating System (Category 1)
e.g., Windows or Red Hat Linux
Standard Hardware (Hardware Category 1)
e.g., server, clients, LAC/E,™ and LND

Figure 2. Explanation of the structure of Waters Informatics applications.

Automated interfaces to other systems – essential for data integrity – can range from configurable through to fully customized, depending on the source and target systems and the available interfaces.

Figure 2 shows a typical structure for any of the Waters™ Informatics applications, such as the Waters Empower™ Chromatography Data System (CDS), NuGenesis™ Laboratory Management System, or UNIFI™ Scientific Management System.

All these Waters applications leverage hardware Category 1 and require software Category 1 operating systems to run.

An assessment of the applicable categories, based on an understanding of what functionality is intended to be used within the system, should be undertaken by the business process owner (typically the lab manager), IT, and the Quality unit. Vendor assistance can be beneficial in helping the assessment team understand what functionality will be used. For example, if custom calculations will not be used in your Empower CDS then potentially there may be no Category 5 elements within your intended use of Empower in your laboratory.

A skilled CSV practitioner who applies critical thinking will recognize and work with the multiple software categories within a single system.

There is no value in a fixed categorization statement provided by the vendor in isolation of your business's intended use. Such a categorization statement would be just as meaningless as a vendor claim that a system can be "prevalidated". The regulators make clear statements that validation must be based on your intended use, such as:

- **MHRA DI Definitions (MHRA, 2018) §6.19:** "The acceptance of vendor-supplied validation data in isolation of system configuration and users intended use is not acceptable"
- **FDA DI Guidance (FDA, 2018) §4:** "If you validate the computer system but you do not validate it for its intended use, you cannot know if your workflow runs correctly"

No vendor can know, in advance, how each regulated organization will implement, configure, and use their software, which makes this concept of "prevalidation" impossible. Validation has to be done for each organization individually, based on their unique intended use and their assessment of risk to their patient safety, product quality, and data integrity.

CATEGORY DOES NOT EQUAL RISK PRIORITY

The GAMP 5 risk assessment process (as defined in GAMP 5 Appendix M3) derives an overall risk priority based on the combination of three factors:

- **Severity of Harm** – what is the consequence to your patient safety, product quality, or data integrity if the function fails or the requirement is not met? Severity of Harm is typically inherent in the business process being supported by the system, and therefore unaffected by the system or its categories.
- **Probability of Occurrence** – how likely is the function to fail, or for the requirement not to be met? Probability of Occurrence can be impacted by the system and its categories, based on the premise that failures are increasingly likely to occur with increasing levels of configuration and customization.
- **Likelihood of Detection** – how reliably will the failure be detected? Likelihood of Detection will be impacted by the system and its categories if the detection mechanism relies on a system exception report or system alarm. Where the detection is achieved by human review or by other activities downstream of the system, the Likelihood of Detection is unaffected by the system and its categories.

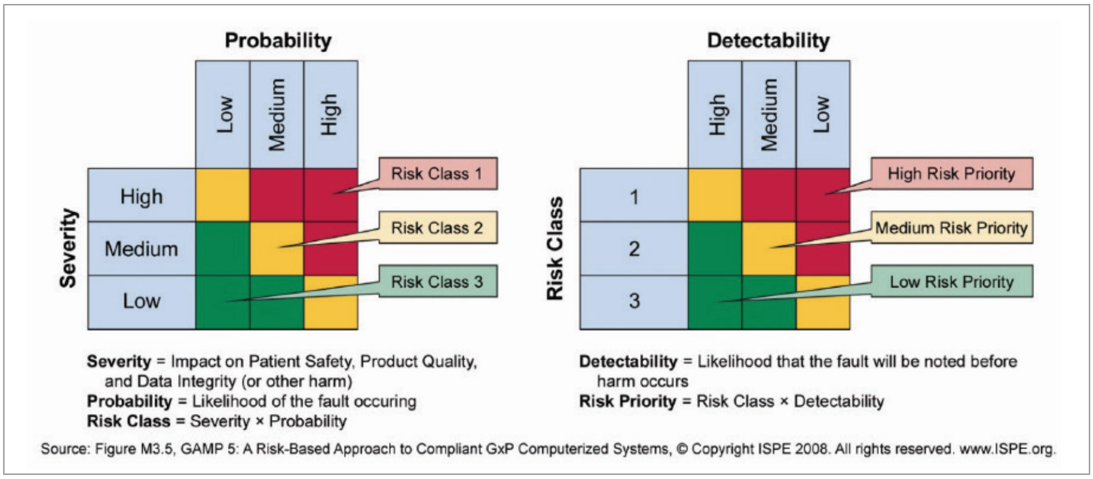
The GAMP methodology for combining those risk factors to generate an overall Risk Priority is shown in Figure 3.

Let's work through an example to understand these factors and how the software category can impact the risk. This example will focus on a requirement that "only authorized users can access the system" – this is a fundamental requirement derived from 21 CFR 211.68(b) in US cGMP. In this example, we will assume that the system under assessment creates, stores, or manages QC data and is therefore a critical GxP system.

Most, if not all, regulated companies would rate the Severity of Harm for this requirement as high. If the requirement is not met, an unauthorized person can access the regulated QC data.

Based on Figure 4, if the functionality addressing the requirement is based on standard functionality, then the project team may choose to assign a Low Probability of Occurrence (failure) – resulting in a Risk Class 2 interim rating.

When the requirement is met through configurable or customized functionality (that is, software categories 4 or 5), the Probability of Occurrence (failure) may be rated higher, resulting in a Risk Class 1 interim rating.



Severity = Impact on Patient Safety, Product Quality, and Data Integrity (or other harm)
Probability = Likelihood of the fault occuring
Risk Class = Severity × Probability

Detectability = Likelihood that the fault will be noted before harm occurs
Risk Priority = Risk Class × Detectability

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

Figure 3. Risk Assessment Method from GAMP 5 Appendix M3.

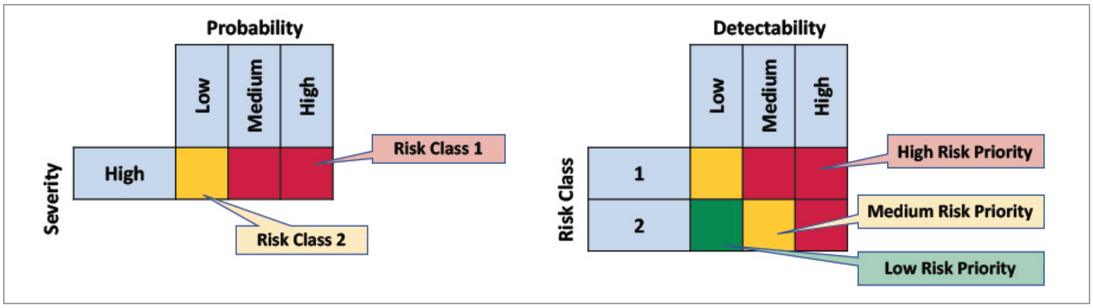


Figure 4. GAMP 5 Risk Assessment adapted and applied to the example requirement.

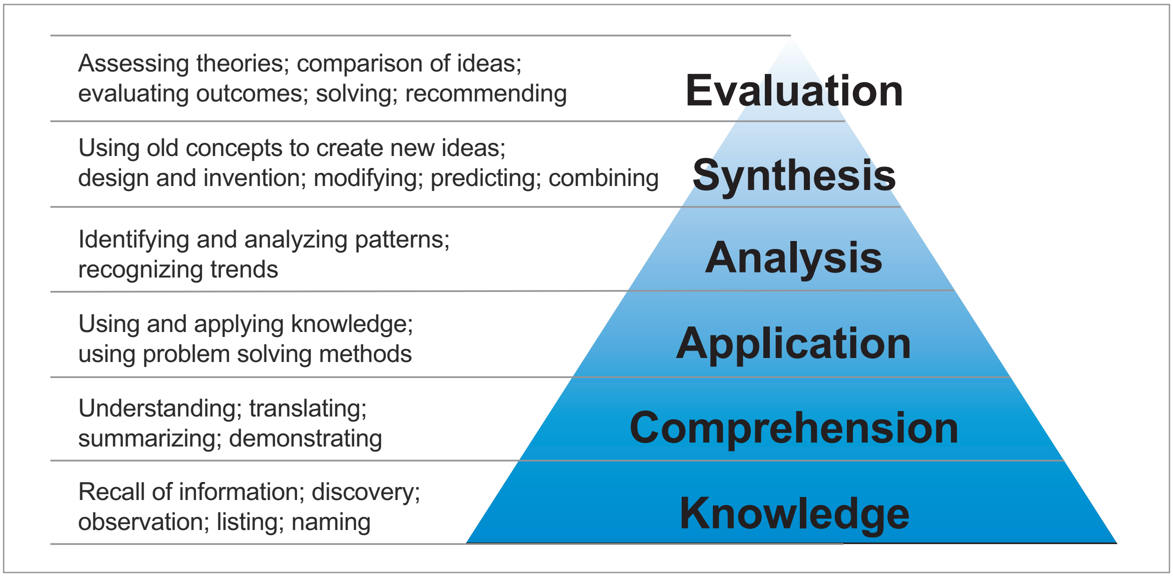

Assessing theories; comparison of ideas; evaluating outcomes; solving; recommending
Evaluation
Using old concepts to create new ideas; design and invention; modifying; predicting; combining
Synthesis
Identifying and analyzing patterns; recognizing trends
Analysis
Using and applying knowledge; using problem solving methods
Application
Understanding; translating; summarizing; demonstrating
Comprehension
Recall of information; discovery; observation; listing; naming
Knowledge

Figure 5. Bloom's Pyramid.

The final factor – Detectability (Likelihood of Detection) – may or may not depend on functionality from the system under assessment, as mentioned earlier. Depending on the Detectability, the overall Risk Priority could be high, medium, or low.

This example demonstrates that software category alone does not and cannot determine the Risk Priority. It is therefore illogical to base the validation approach on software category, as this is not in keeping with a risk-based approach.

APPLYING CRITICAL THINKING AND THE RISK-BASED APPROACH

Lessons learned since the publication of GAMP 5 have shown that the risk-based approach works best when combined with critical thinking.

In Figure 5, Bloom's Pyramid, critical thinking is achieved within the highest tiers of the pyramid. A skilled CSV practitioner is able to apply their combined knowledge, understanding, and experience analytically to more effectively evaluate new situations and propose solutions.

For example, consider the requirement that "a lab user must not be able to delete data", which the risk-assessment team rated as a High Risk Priority thus necessitating testing of the control functionality around deletion.

A moderately competent CSV practitioner can establish a basic test approach for this requirement using conventional thinking, as shown in Figure 6.

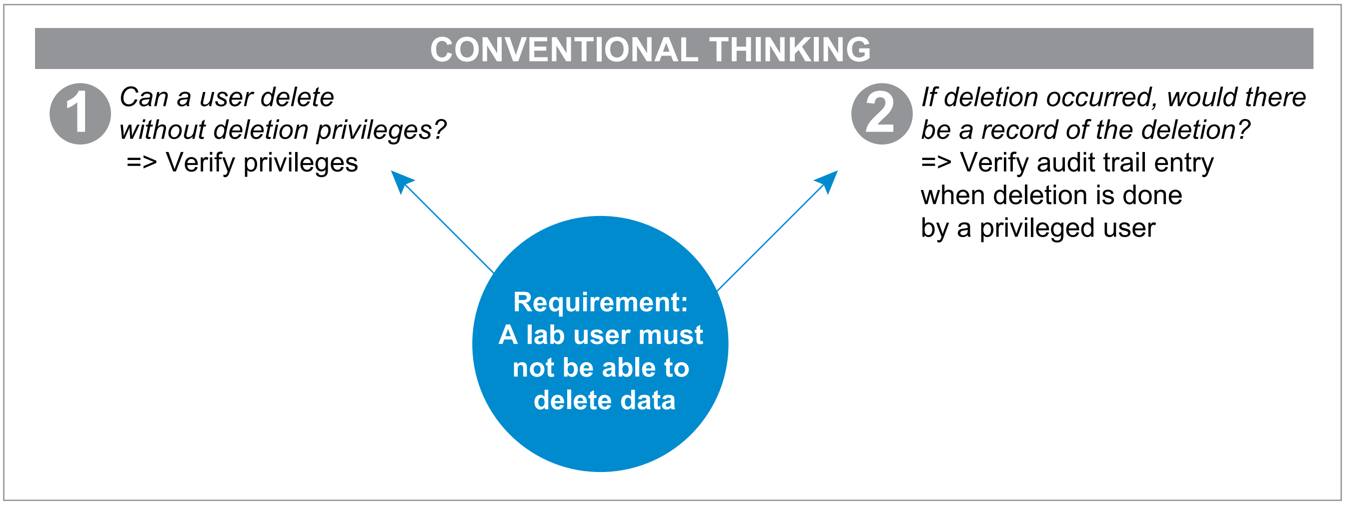

CONVENTIONAL THINKING
1
Can a user delete without deletion privileges?
=> Verify privileges
2
If deletion occurred, would there be a record of the deletion?
=> Verify audit trail entry when deletion is done by a privileged user
Requirement: A lab user must not be able to delete data

Figure 6. Applying conventional thinking to test planning.

A skilled CSV practitioner however – such as those in Waters Professional Services – would apply critical thinking, and identify further test cases to be included, as shown in Figure 7.

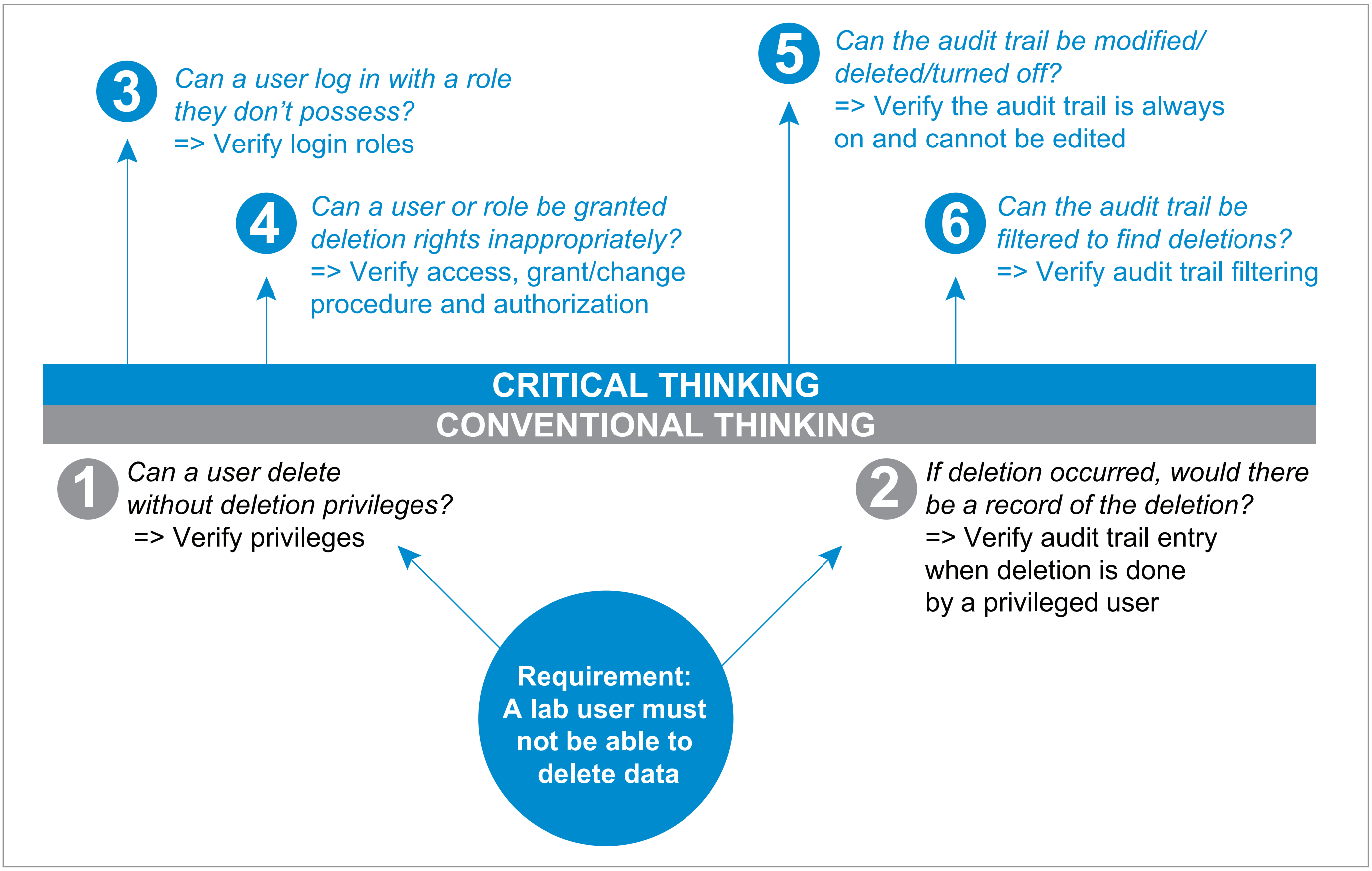

3
Can a user log in with a role they don't possess?
=> Verify login roles
4
Can a user or role be granted deletion rights inappropriately?
=> Verify access, grant/change procedure and authorization
5
Can the audit trail be modified/ deleted/turned off?
=> Verify the audit trail is always on and cannot be edited
6
Can the audit trail be filtered to find deletions?
=> Verify audit trail filtering
CRITICAL THINKING
CONVENTIONAL THINKING
1
Can a user delete without deletion privileges?
=> Verify privileges
2
If deletion occurred, would there be a record of the deletion?
=> Verify audit trail entry when deletion is done by a privileged user
Requirement: A lab user must not be able to delete data

Figure 7. Applying critical thinking to test planning.

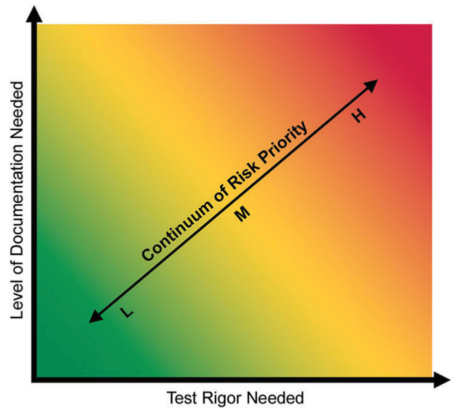
It should be noted that item 4 in Figure 7 is managed by a procedural control – it is important to realize that the scope of a computerized system includes more than just the software. A fully validated system operated by untrained users and lacking procedural operating controls poses just as high a risk to patient safety, product quality, and data integrity as the risk of using an unvalidated system.

ALIGNING WITH COMPUTER SOFTWARE ASSURANCE (CSA)

At the time of this white paper, the US FDA has further deferred the release of their draft guidance on Computer Software Assurance (CSA). ISPE GAMP however has published a new GAMP RDI Good Practice Guide: Data Integrity by Design (ISPE, 2020), which includes a detailed appendix written by the FDA - Industry CSA team (FICSA). This GAMP guide appendix provides the first formal guidance into the practical application of CSA in a regulated environment.

Critical thinking is inherent within CSA; it is foundational to the patient-safety focus promoted by FDA as part of CSA and their Case for Quality initiative. Critical thinking should be used during the initial project planning, during the requirements definition, within the risk assessment, as part of test planning, and during the scripting, execution, and reporting of the verification phase. Critical thinking involves looking beyond the obvious, to objectively assess potential root causes of failure and develop use cases, and to apply skill and knowledge effectively to improve the quality of the system implementation and operation.

CSA, while being discussed in internet forums as a new direction for computerized systems validation, is in fact simply the next step in the risk-based approach. In keeping with GAMP, it applies quality risk management principles based on the potential risk to patient safety, product quality, and data integrity. It promotes the risk-based approach to determine the scope and rigor of testing, but additionally leverages a risk-based approach to the extent of documentation of the testing, as shown in Figure 8.



Source: Figure 19.5 ISPE GAMP® Data Integrity by Design Guide, ©ISPE 2020. All rights reserved. www.ispe.org

Figure 8. Test rigor and level of documentation as a function of the risk continuum.

The risk-based approach to the documentation effort permits the use of unscripted and ad hoc testing in addition to the robust scripted testing traditionally used in CSV. The intent is that much of the effort previously invested in creating and checking test scripts is now redirected into challenging the software functionality to detect defects. The robust scripted testing is now reserved only for the highest Risk Priority requirements.

Note that, contrary to industry speculation, the FDA's use of the term "Computer Software" in place of "Computerized System" is not indicative of some reduction in scope. The aim of CSA, as with CSV, is to ensure the system – incorporating computer hardware and software, people, equipment, process, procedures, and operating environment – is fit for its intended use in the regulated company.

SUCCESSFUL, EFFECTIVE VALIDATION

Successful computerized systems validation needs:

- An organizational focus on quality culture and operational excellence
- An understanding of the business process involved, and how the system will support that process and its corresponding regulated data lifecycle
- Knowledge of GxP regulations and data integrity guidances
- The application of critical thinking throughout all phases of the CSV project by a skilled CSV practitioner
- Expert, detailed technical knowledge of the system
- A genuine desire for the system to protect patient safety, product quality, and data integrity

Waters has Professional Services teams around the world available to assist its customers with meeting their CSV obligations under the regulations. The Waters Professional Services CSV consultants are subject matter experts with years of experience in both CSV and in the Informatics software products being validated, allowing for delivery of a high-quality, risk-based approach in line with industry current good practices.

Table 1 outlines the key activities within a Waters CSV project, along with the objectives and focus of each activity, and highlights the primary influences on the activities (i.e., regulatory requirements and guidances, regulated companies' internal policies and working practices, industry good practices, and earlier activities within the GAMP 'V-model'). Note that some document names may differ regionally.

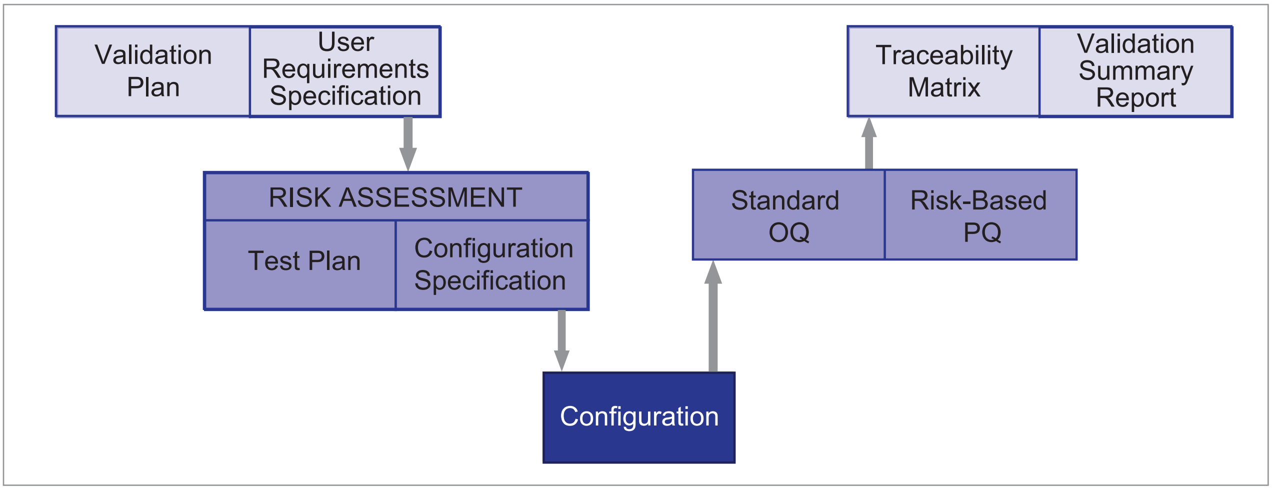


Figure 9. Waters V-model approach to CSV, adapted from ISPE GAMP 5 Figure 3.3.

Table 1. Understanding the objectives and influences on CSV activities.

CSV phases/ activities	Key objectives/focus	Influenced by
Planning: Validation Plan	Defining the rigor of validation required and the activities involved, based on the GxP impact of the system	▪ Applicable GxP Regulations ▪ Company Internal Policy ▪ Industry Good Practice
Planning: User Requirements Specification	Defining the functionality needed to support the business process (intended use), and the functionality/controls needed to ensure the integrity of the data within the system	▪ Business Process and Intended Use ▪ Other Systems Upstream/Downstream/Interfaces ▪ Vendor Assessment ▪ Record Retention Strategy ▪ Data Integrity Guidances
Specification: Risk Assessment	Identifying and assessing potential risk to patient safety, product quality, and data integrity if a function fails or a requirement is not met	▪ Severity of Harm is influenced by the GxP impact of the system and the particular requirement ▪ Probability of Occurrence may be influenced by the GAMP software categories of the chosen systems ▪ Likelihood of Detection will be influenced by the reliability of the detection controls – human, procedural, technical
Specification: Configuration Specification	Selecting system configuration settings and user privileges to configure the system to meet intended and mitigate data integrity risks	▪ Risk-Assessment ▪ Vendor Expertise and Support ▪ Data Integrity Guidances ▪ Regulatory Warning Letters and Non-Conformance Reports ▪ Laboratory Working Practices
Specification: Test Plan	Identifying the test cases needed to adequately verify how requirements with High and Medium Risk Priority are met	▪ Risk Assessment ▪ CSA Approaches ▪ Leveraging Vendor Testing and Standard OQ Test Coverage
Configuration: System Configuration	Applying the system configuration as documented in the Configuration Specification and activating Change Control from this point forward	▪ Configuration Specification
Verification: Standard OQ	Executing test cases against a Waters-provided test protocol to verify standard functionality commonly used	▪ Waters SDLC ▪ Data Integrity Guidances
Verification: Risk-Based PQ	Waters CSV consultants generate a tailored test protocol based on the Test Plan, intended to be executed by members of the regulated company	▪ Risk Assessment ▪ Test Plan ▪ CSA Approaches ▪ Standard OQ
Reporting: Requirements Traceability Matrix	Mapping User Requirements to Configuration Specification, Risk Priorities, Standard OQ and PQ test coverage to demonstrate the requirements have been met and verified using a risk-based approach	▪ User Requirement Specification ▪ Risk Assessment ▪ Configuration Specification ▪ Standard OQ ▪ Risk-Based PQ
Reporting: Validation Summary Report	Summarizing all of the CSV activities completed and any incidents or deviations. Confirming that the objectives of the Validation Plan have been met, and if the system is now validated for intended use. Identifies ongoing activities needed to maintain the validated state and operate the system in compliance	▪ Validation Plan ▪ User Requirement Specification ▪ Standard OQ ▪ Risk-Based PQ ▪ Requirements Traceability Matrix ▪ Data Integrity Guidances ▪ Regulated Company SOPs

CONCLUSION

GAMP categories are not a substitute for critical thinking and the risk-based approach. Asking for a Functional Specification from the vendor simply because GAMP 5 includes this in the list of documentation suggested for a software category 4 system does nothing to improve patient safety, product quality, or data integrity. Instead, use critical thinking to evaluate the risks inherent within the system and your business process, including other systems upstream and downstream of this step in the process. Assign categorization to the system based on an understanding of what functionality is needed to meet your unique intended use, and where that functionality would fit in the GAMP categories, remembering that each system is likely to encompass several categories. Leverage that categorization to identify the extent of configuration/customization needed to meet a particular user requirement, which in turn will help with rating the Probability of Occurrence of failure to meet the requirement. This approach strengthens your risk assessment process, which forms the basis for the extent and rigor of your validation activities.

Validation must take into account not just the computer hardware and software, but also any connected equipment, the underlying business process, and the people and procedures supporting the system's operation. Safeguard your end patients, your product, your data, and your company's reputation by focusing your validation efforts to truly assure the system is fit for your intended use.

Related Reading

- FDA. (2018). Data Integrity and Compliance With Drug CGMP; Questions and Answers Guidance for Industry. FDA.
- ISPE. (2001). GAMP Guide for Validation of Automated Systems (GAMP 4). ISPE.
- ISPE. (2008). GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems. ISPE.
- ISPE. (2020). ISPE GAMP RDI Good Practice Guide: Data Integrity by Design. ISPE.
- MHRA. (2018). 'GXP' Data Integrity Guidance and Definitions. MHRA.
- Wingate, G. (1995). Computer Systems Validation: A Historical Perspective. ISPE Pharmaceutical Engineering, Vol. 15 No. 4 July/August.
- Wingate, G. (1997). Validating Automated Manufacturing and Laboratory Applications. CRC Press.

All GAMP figures used by permission of ISPE. GAMP is a trademark of ISPE.

Waters

THE SCIENCE OF WHAT'S POSSIBLE.™

Waters Corporation
34 Maple Street
Milford, MA 01757 U.S.A.
T: 1 508 478 2000
F: 1 508 872 1990
waters.com