



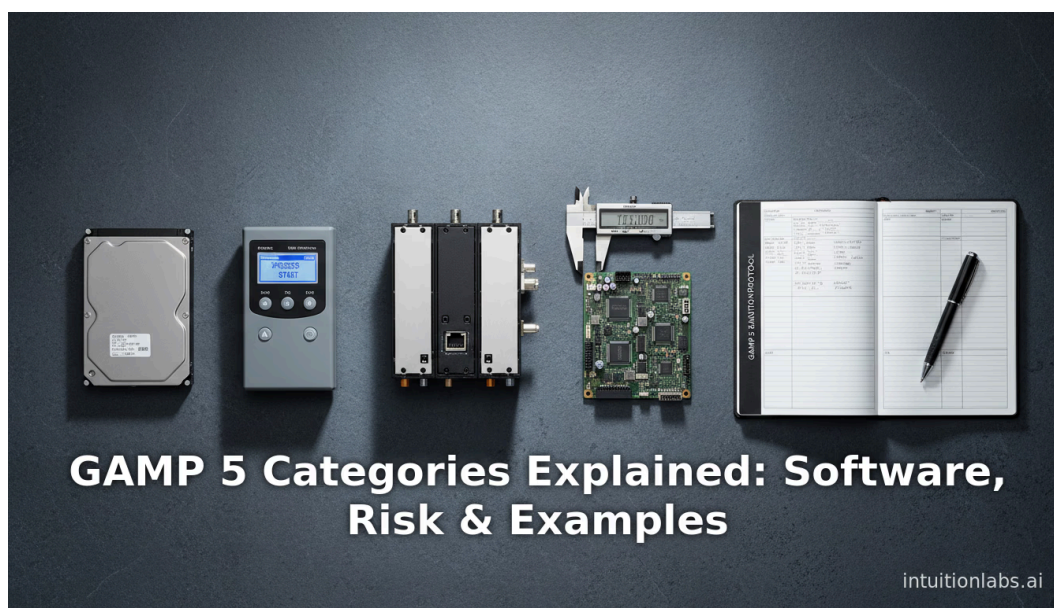
INTUITIONLABS / RESEARCH & PRACTICAL GUIDANCE

GAMP 5 Categories Explained: Software, Risk & Examples

Build practical AI for pharma and biotech with IntuitionLabs. We help life-science teams turn complex information and workflows into useful software, governed knowledge systems and AI tools.

Published by IntuitionLabs · 2025-10-16 · gamp 5 · computer system validation · gxp · risk-based approach · ispe · software validation · pharmaceutical compliance

Original article: <https://intuitionlabs.ai/articles/gamp-5-categories-explained>



In this article

1. [GAMP 5 Categories Explained: Software, Risk & Examples](#)
 2. [Executive Summary](#)
 3. [Introduction](#)
 4. [Overview of GAMP 5 Life Cycles and Categories](#)
 5. [Historical Numbered Categories](#)
 6. [Software vs. Hardware Categories \(Continua\)](#)
 7. [Implementation Strategies and Case Examples](#)
 8. [Risk Considerations and Regulatory Views](#)
 9. [Data Analysis and Evidence-Based Points](#)
 10. [Future Trends and Implications](#)
 11. [Conclusion](#)
-

GAMP 5 Categories Explained: Software, Risk & Examples

[Revised October 10, 2026]

Executive Summary

Good Automated Manufacturing Practice (GAMP) 5 is a globally recognized guideline for validating computerized systems in regulated industries, especially pharmaceuticals and biotechnology. Published by the International Society for Pharmaceutical Engineering (ISPE) in 2008 (with a second edition in 2022), GAMP 5 introduced a **risk-based approach** to prioritize validation efforts. A core part of GAMP 5 is the **categorization of software and hardware**. These categories describe component types and development approaches; they are not a fixed scale of increasing system risk. For example, operating systems, databases, and office tools (Category 1) are treated with minimal validation, whereas bespoke, in-house developed software (Category 5) requires rigorous control (www.spectroscopyonline.com) (kneat.com). Hardware is also split into “standard” and “custom” types (pmc.ncbi.nlm.nih.gov) (qualio.com).

Adopting GAMP 5’s classification helps companies apply **“fit-for-use”** validation: focusing resources on high-risk systems and relying on foundational quality for common tools (www.ptc.com) (www.ptc.com). In practice, organizations range from spreadsheet-dependent small firms to large enterprises with fully integrated systems (qualio.com). GAMP 5’s contemporary updates (Second Edition, 2022) explicitly view categories as a continuum and emphasize that other factors (system criticality, complexity, novelty) also drive risk-based test planning (xevalics.com) (xevalics.com). Expert sources note that this continuum view discourages rigid “checklist” validation purely by category (xevalics.com).

This report provides a comprehensive overview of GAMP 5 categories, detailing component definitions, examples, and risk-based validation-planning considerations. It contrasts GAMP 5 with earlier GAMP versions, illustrates how classification underpins a scaled life-cycle approach, and discusses practical implications.

Multiple expert perspectives and case example scenarios (e.g., laboratory systems, manufacturing control) are provided, and numerous authoritative sources (ISPE, industry publications, validation guides) are cited. The report concludes with implications for future trends (e.g. cloud and [AI in GxP systems](#)) and recommendations for continuous improvement in computerized system validation.

Introduction

Historical Background

Validated computerized systems have been critical in pharmaceuticals since the 1990s. FDA 21 CFR Part 11, issued in 1997, establishes requirements for electronic records and electronic signatures. The current European Commission GMP Annex 11, *Computerised Systems*, is revision January 2011 and addresses computerized systems in the GMP context. In response, industry professionals developed supplemental best practices like GAMP. GAMP originated in 1991 as an initiative by pharmaceutical industry professionals, specifically to address computerized system compliance needs; its guidance is now published by ISPE (International Society for Pharmaceutical Engineering) (www.ptc.com). Early GAMP guides (Versions 1–4) used a single V-model lifecycle for all systems, which often proved too rigid for diverse computer-based tools. In 2008, recognizing the need for flexibility, GAMP 5 was introduced with a **risk-based, flexible life cycle approach** (www.spectroscopyonline.com) (www.ptc.com). The second edition of GAMP 5 (2022) further modernized guidance to address new technologies (cloud, AI, service providers) and explicitly emphasized critical thinking by experienced SMEs (guidance-docs.ispe.org) (xevalics.com).

GAMP is **not a regulation**; rather, it is a consensus standard. As the PTC whitepaper notes, “rather than being a regulation, GAMP® 5 is a set of principles and procedures created to help validate automated computer systems” (www.ptc.com). Adhering to GAMP 5 supports compliance with FDA 21 CFR 11, EU Annex 11, and other regulatory frameworks by providing a structured, quality-based approach (www.ptc.com). Many regulated companies and their suppliers worldwide rely on GAMP 5 as a **common language and framework**, enabling efficient auditing and reducing duplicate effort (www.ptc.com) (www.ptc.com).

The Risk-Based Philosophy

GAMP 5’s central tenet is “**fit for intended use**”, which calls for validating a system only to the extent needed to ensure quality and compliance (www.ptc.com). This is achieved through *quality risk management* (aligned with ICH Q9 principles), i.e. using risk analysis to determine the breadth and depth of validation (kneat.com) (xevalics.com). High-risk systems (those affecting patient safety or product quality) get the most validation rigor, while low-risk, standard systems (like an OS or commercial word processor) receive minimal formal testing (www.spectroscopyonline.com) (www.ptc.com). As one industry report emphasizes, “using a risk-based approach encourages... focusing on areas of high risk and avoiding duplicate activities” (www.ptc.com). Categorization can inform the assessment of the likelihood of residual defects in individual components, but it does not determine system risk or validation effort by category number. Those activities should be scaled to the overall GxP impact and identified risks. (www.spectroscopyonline.com) (kneat.com)

ICH Q9 and FDA guidance on risk management are integral to this approach. Indeed, GAMP 5 explicitly references a science-based quality risk process and leverages standards like ISO 14971 (risk mgmt for [medical devices](#)) ([ispe.org](#)). In practice, a GAMP-based strategy asks two key questions: *Do I need to validate this system at all?* and *How much validation work is enough?* ([www.researchgate.net](#)). Systems with minimal GxP impact (e.g. marketing tools) may even be excluded from the scope of GAMP validation. But for all regulated systems, GAMP 5 promotes continuous risk evaluation throughout the life cycle (planning, development, testing, operation, changes) to keep resource spending commensurate with risk ([xevalics.com](#)) ([ispe.org](#)).

Overview of GAMP 5 Life Cycles and Categories

GAMP 5 replaced the one-size-fits-all V-model with multiple tailored life-cycle models and a suite of appendices, central among them **Appendix M4** on Categories. GAMP 5 (Second Ed.) itself explains that **“computerized systems are generally made up of a combination of components from different categories; the categories should be viewed as a continuum”** ([xevalics.com](#)). In other words, a single application may include both standard and custom components, and the validation strategy should be adapted holistically, not slavishly by category number. This second-edition emphasis ensures that companies don’t simply follow a rote checklist but apply critical thinking: “categorization is not intended to provide a checklist approach to validation,” warns Xevalics Consulting ([xevalics.com](#)).

Nevertheless, category assignment serves as an initial stratifier for validation. The **five main principles of GAMP 5’s risk-based approach** (from the PTC blog interpretation) are: (1) understand the product and process; (2) manage the system life cycle within a quality management system; (3) make life-cycle activities scalable; (4) ensure the approach to risk management is science-based; (5) leverage supplier involvement throughout the system life cycle ([www.ptc.com](#)). Within this framework, Appendix M4 defines **software categories** (1, 3, 4, 5) and **hardware types** (1, 2) to guide the validation planning. (GAMP 5 no longer uses “Category 2” for software; firmware, which can range from simple to custom software, is now accommodated in the other categories depending on its nature ([www.spectroscopyonline.com](#)).) The table below summarizes common software-category terminology with descriptions and examples. Category is one input to validation planning; it is not a fixed relative-risk scale.

Software Category	Description	Example Systems/Software	Validation-planning considerations
Category 1: Infrastructure Software	Core/plumbing software providing hosting environment. Generally not modifiable by end users.	Operating systems (Windows, Linux), Database management systems (Oracle, SQL Server), Programming languages, Office suites (Word, Excel), Statistical tools, Middleware (www.spectroscopyonline.com) (kneat.com).	Assess its services and interfaces in the context of intended use. Supplier evidence, installation checks, and system-level testing may be leveraged as appropriate.

Software Category	Description	Example Systems/Software	Validation-planning considerations
Category 3: Nonconfigured Products	Off-the-shelf software used “as installed,” without customization beyond default settings. Entering parameters is allowed but code itself is fixed.	Lab instruments’ embedded software (e.g. GC/HPLC software), Commercial “as-is” applications with no code changes (e.g. pure COTS packages used without config) (www.ptc.com) (kneat.com).	Supplier assessment, confirmation of the installed version, and risk-based testing of the functions and parameters actually used (for example, IQ/OQ), scaled to intended use and GxP impact (kneat.com) (pmc.ncbi.nlm.nih.gov).
Category 4: Configured Products	Commercial or open-source software products that are configured (via configuration settings, business rules, or workflows) to meet user needs; custom scripts or macros added to them are treated as Category 5 components. No changes to underlying code.	Highly configurable systems like Laboratory Information Management Systems (LIMS), Manufacturing Execution Systems (MES), SCADA, DCS, Warehouse Management, ERP, Building Management (BMS) (www.ptc.com) (pmc.ncbi.nlm.nih.gov).	Risk-based supplier assessment plus verification of the configuration and of the application within the business process; effort scales with complexity, novelty, and GxP impact. GAMP 4 Class 4 listed MES, ERP, SCADA, and DCS as typical examples (gmpua.com) (pmc.ncbi.nlm.nih.gov).
Category 5: Custom Applications and Components	Software or code developed for the specific application, including custom extensions, scripts, macros, and heavily modified open-source software.	In-house LIMS written from scratch, custom data analysis software, laboratory-information interfaces, extensions or heavily modified plugins, and Excel spreadsheets with custom VBA macros.	Apply lifecycle controls and verification scaled to the component’s complexity, novelty, intended use, supplier evidence, and identified risks; custom code does not by itself establish the system’s risk level.

Table 1. GAMP 5 software categories, descriptions, examples, and planning considerations. [Sources: ISPE GAMP 5 guidance (kneat.com) (qualio.com), PTC blog (www.ptc.com) (www.ptc.com), Cureus review (pmc.ncbi.nlm.nih.gov) (pmc.ncbi.nlm.nih.gov), GAMP 4 for context (gmpua.com).]

Categories are not fixed risk levels. They group components with similar creation attributes and can help assess the likely presence of residual defects, but a complex configured component may warrant more verification than a simple custom component. The applicable life-cycle activities depend on the overall GxP impact, complexity, novelty, supplier assessment, and identified risk scenarios. (kneat.com) (www.ptc.com) Category 2 (Firmware) was from GAMP4 and is now **unused** in GAMP5 (www.spectroscopyonline.com) (kneat.com). The examples in the table above illustrate each category: for instance, a vendor-supplied nuclear magnetic resonance (NMR) spectrometer is Category 3 if used “as installed,” but if the vendor provides configuration options (methods, workflows), it may edge into Category 4 territory (www.spectroscopyonline.com) (pmc.ncbi.nlm.nih.gov). Conversely, a routine office spreadsheet is Category 1, but if users develop complex macros in it, that spreadsheet could become a Category 5 “application” due to custom code (www.spectroscopyonline.com) (www.ptc.com).

GAMP 5 hardware types describe the nature of individual hardware components; their type alone does not establish GxP risk or the required verification effort.

Hardware Type	Description	Example Systems	Validation-planning considerations
Type 1 (Standard Hardware)	Off-the-shelf, generic hardware components. No custom electronics. Document model, version, vendor; qualified by inventory/config control.	Standard servers, workstations, network devices; PLCs and controllers purchased off-the-shelf (with vendor FW) (pmc.ncbi.nlm.nih.gov) (qualio.com).	Determine installation, configuration, and verification activities from the component's intended use, interfaces, supplier evidence, and identified risks.
Type 2 (Custom Hardware)	Custom-built or custom-assembled hardware. Requires detailed design documentation and acceptance testing.	Custom circuit boards, proprietary lab instruments built in-house, or systems pieced together from various specialized components (pmc.ncbi.nlm.nih.gov) (qualio.com).	Plan design evidence, acceptance activities, and testing according to the hardware's intended use, complexity, novelty, supplier evidence, and identified risks.

Table 2. GAMP 5 hardware types. Hardware evidence and verification should be appropriate to the component's role in the computerized system and the identified risk scenarios; type is one input, not a substitute for that assessment. (qualio.com) ([pmc.ncbi.nlm.nih.gov](https://pubmed.ncbi.nlm.nih.gov/))

Historical Numbered Categories

The following subsections explain commonly used Category 1, 3, 4, and 5 terminology. In the Second Edition, this terminology remains useful for describing components, but categories 3–5 are viewed as a continuum and are only one factor in a risk-based approach; they are not fixed validation-risk levels.

Category 1: Infrastructure Software

Definition: Category 1 encompasses generic, widely used *infrastructure software*. This includes operating systems, database servers, programming languages/interpreters, middleware, and even office suite applications. These products are *not designed specifically for GxP tasks* but provide a platform. GAMP 5 broadened Category 1 significantly compared to earlier versions (www.spectroscopyonline.com): it now includes everything from Linux/Windows OS to statistical programming tools and spreadsheet packages such as Excel. Importantly, office tools (Excel, Word, PowerPoint) are Category 1 *unless* used to create specialized data-tracking applications (www.spectroscopyonline.com).

Validation Approach: Category 1 software is “validated” largely by acknowledging the vendor’s established qualification processes. One should document the software name, version, and where it’s installed (www.spectroscopyonline.com) (qualio.com). Change control is applied (patches, upgrades), but minimal testing is done. For example, confirming that the OS boots correctly, or that an antivirus (in Cat 1) is up-to-date, suffices. As one author notes, “operating system is implicitly tested... since all higher functions rely on this functioning flawlessly,” requiring only documentation of its use (gmpua.com) (www.spectroscopyonline.com).

Examples:

- A standard Microsoft Windows or Linux server used to host laboratory applications.
- A commercial SQL database (Oracle, MySQL) pre-installed for lab data management (www.spectroscopyonline.com).

- A network monitoring tool or spreadsheet software.
- A drug company's standard VPN software and anti-virus system.

A Category 1 classification does not by itself establish low GxP risk; assess the component in the context of its intended use and risk scenarios. However, misuse can raise category: e.g., writing data-processing macros in Excel turns it into a higher category (treated as custom development) (www.spectroscopyonline.com).

Category 3: Nonconfigured Products

Definition: Category 3 covers software *used out-of-the-box with minimal or no configuration*. These are off-the-shelf applications that meet the business needs without code changes. According to PTC, Cat 3 includes “software which can meet the requirements... without modification (‘used as installed’), as well as configurable software used only with its default settings” (www.ptc.com). In practice, Category 3 includes laboratory instrument software, firmware in instruments that only allow setting run parameters, or commercial software run with only initial user input (but no tailoring of functions).

Validation Approach: For Cat 3, the validation approach is mostly supplier-driven. The steps often include obtaining a User Requirements Specification (URS) to justify need, confirming the version/vendor, installation checks, and performing risk-based testing of critical functions (pmc.ncbi.nlm.nih.gov) (www.ptc.com). One may use a simplified life cycle (focused on IQ/OQ) and supplier documentation in lieu of full design specs (pmc.ncbi.nlm.nih.gov). As GMPUA notes, COTS Category 3 usually needs only documenting version and testing essential functionality during qualification (gmpua.com) (kneat.com). In high-risk cases (e.g. a lab instrument controlling a critical process), additional measures like vendor audit may be warranted.

Examples:

- A laboratory gas chromatograph's control software (as supplied by the GC vendor) and its firmware.
- Commercial data analysis tools or chromatography processing programs used “as is”.
- A stand-alone PC application that simply runs standard reports without user customization.

Category 3 does not establish a fixed risk level. Its use as a standard component can inform the assessment of residual-defect likelihood, while the required assurance depends on the intended use, GxP impact, supplier evidence, and identified risk scenarios. (kneat.com) Companies typically ensure traceability from URS through testing (OQ) for Category 3, but may not require full design documents or code review (as per Cat 5).

Category 4: Configured Products

Definition: Category 4 refers to **commercial or open-source software that is configurable to meet user needs**, without altering the source code. This is the broadest and most complex category. Examples include LIMS, MES, SCADA/DCS, ERP, CRM, electronic batch record systems, or any vendor system where administrators set up workflows, business rules, or parameters. PTC notes that Cat 4 systems “are configured to meet user-specific business needs” and lists LIMS, SCADA, DCS as examples (www.ptc.com). GAMP 4's Class 4 also cited MES, ERP, SCADA and DCS as typical Category 4 (gmpua.com). Notably, if macros or custom scripts are added to these systems, those extensions may be treated as Category 5 (custom) even though the base product is Category 4 (gmpua.com) (kneat.com).

Validation Approach: Category 4 systems demand a comprehensive validation strategy scaled by risk. Activities normally include: writing formal functional specifications and design specifications (often involving both the vendor and the user); supplier assessment of the vendor's quality system; User Requirement Specification; mapping to functional OQ tests; and a full testing phase of configurations. Because Cat 4 systems are “highly complex” ([pmc.ncbi.nlm.nih.gov](https://pubmed.ncbi.nlm.nih.gov/)), risk-based prioritization is key: focus testing on critical functionality and key configurations. Traceability matrices linking requirements to tests are typical. If the software is heavily used in critical processes (e.g., batch release), auditors often expect Supplier Qualification and configuration management evidence (gmpua.com).

Examples:

- A LIMS system configured for the lab's specific workflows and instruments.
- An ERP finance module set up for GxP compliance but “as delivered” without code changes.
- A building-management/BMS system customized with control rules for cleanroom pressurization.
- Any COTS process-control system (SCADA/DCS) where engineers parameterize control loops.

Category 4 components often need substantial verification because of their size and configurability, but the category does not by itself set their risk level. Common pitfalls include failure to retest after configuration changes, or underestimating the validation needed for interfaces. Because the underlying code is vendor-provided, Category 4 work typically combines supplier evidence with user verification of the configuration (kneat.com).

A notable point: GAMP 5 (and GAMP 4) stress that Category 4 validation relies on both **supplier documentation** and user testing. As one source states, “an approach to supplier assessment that is based on risk shows that the supplier has a sufficient quality management system” and then “risk-based testing to show that the application functions within the business process as intended” ([pmc.ncbi.nlm.nih.gov](https://pubmed.ncbi.nlm.nih.gov/)). In other words, a competent vendor and thorough IQ/OQ/PQ build confidence.

Category 5: Custom Applications

Definition: Category 5 includes software that is **custom-developed** for a specific business need. This can be either: (a) *in-house developed* code, or (b) *outsourced bespoke software projects*. Even if built from open-source frameworks, if the organization develops new features or rewrites significant portions, it is Cat 5. The distinguishing feature is that code is created or materially changed for the specific application; the classification can inform assessment of residual-defect likelihood, not establish the system's risk level. GAMP 4's Class 5 likewise defined “customer-specific software” where “an application is programmed for an individual application” (gmpua.com). Any macros, scripts, or pieces of custom code in other categories are also classified as Cat 5.

Validation Approach: Custom components may require lifecycle controls such as requirements, design evidence, reviews, version control, and verification, but the activities and their rigor should be selected and scaled to the component's intended use, complexity, novelty, supplier evidence, overall GxP impact, and identified risks. Custom code alone does not establish the system's risk level or mandate a uniform SDLC, test method, supplier audit, or source-code escrow arrangement. ([ISPE](https://ispe.org/))

Examples:

- A biotechnology firm's lab instruments interfacing software written in-house.
- Custom database applications (e.g. a new computerized maintenance management system) built by third-party contract developers.
- An audit trail and reporting feature coded by a CRO for a clinical trial.
- Any bespoke data analysis pipeline (e.g. an in-house pharmacokinetic model runner).

Custom components require lifecycle controls and evidence appropriate to their intended use and identified risks. Requirements, reviews, testing, and change control should be planned using that assessment; no general percentage increase in validation effort can be supported without a defined study context.

Software vs. Hardware Categories (Continua)

Modern computerized systems often integrate hardware and software components with different characteristics. A PLC-based automation system, for example, may contain infrastructure software, standard or configured components, and custom code. GAMP 5's second edition treats categories as a continuum rather than isolated whole-system labels. The validation strategy should assess each relevant component and the integrated system in the context of intended use, interfaces, and risk scenarios; custom macros or scripts are custom components.

From a practical standpoint, when classifying a system, companies often consider the highest applicable category. For example, in the pharma manufacturing context, an entire batch control system might be labeled "Category 4" if it is primarily a configurable MES, even though its OS and some modules are Cat 1. However, tasks like change control will note that upgrades to the OS (Cat 1) or custom plugins (Cat 5) are subject to their own requirements within the overall project. A recent consulting note cautions against "rigidly stick[ing] a computerized system into a single category" without thinking critically ([xevalidics.com](https://www.xevalidics.com)).

On the hardware side, similar logic applies. A validated instrument may have standard (Type 1) circuitry but a custom sensor (Type 2). Assembled systems that combine custom hardware from different sources need verification that the interconnected hardware components are compatible (qualio.com). In practice, this means treating the custom portion as Type 2: providing a hardware design spec and performing acceptance tests for the custom part, while treating the standard components by inventory/documentation (qualio.com) (pmc.ncbi.nlm.nih.gov).

Implementation Strategies and Case Examples

In applying GAMP 5, companies first assess the system's GxP impact, intended use, components, suppliers, and risk scenarios, then scale life-cycle activities accordingly. Categorization can support assessment of individual components and supplier assessment, but it does not prescribe validation effort or a whole-system test protocol. For example, a data-collection instrument and an automated packaging line each require assurance activities appropriate to their actual functions and identified risks.

Case Example: Laboratory Information Management System (LIMS). Consider a mid-size biotech adopting a new LIMS. The LIMS may contain configured components, while any custom extensions require separate component assessment. The company would likely perform a supplier audit of the LIMS provider, develop a

URS specifying how samples/results should be handled, and map to test scripts. All custom configurations (workflows, data fields, reports) get OQ testing. The OS and database beneath the LIMS (Category 1) might only be installation-qualified (e.g. confirming correct software version and licenses), per Table 1 guidelines. This approach is consistent with industry best practice: focusing validation on the configurable aspects and relying on vendor trust for infrastructure (www.ptc.com) (kneat.com).

Case Example: Custom Lab Instrument Software. A research lab develops in-house software to control a novel analytical device. The custom software component requires lifecycle controls and verification appropriate to its intended use, complexity, novelty, and identified risks. They define detailed specs, review code for data integrity, perform unit testing on modules, then integration testing on the full system. They also validate the PC and OS (Cat 1) on which it runs (e.g. ensuring the operating system patches are up to date, documentation of version). If during use they find a bug in their software, they update via strict change control (new code version, regression test) before re-release.

Case Example: Spreadsheet Use. Per GAMP 5, generic spreadsheets (Excel) can fall into different categories. For example, an Excel file used solely for simple arithmetic checks might be Cat 1 (infrastructure). But when a lab creates a complex Excel-based calculation system (with multi-sheet links, macros, and templates), it becomes a Category 3, 4, or 5 application depending on its complexity, and any macros are Category 5 components (www.spectroscopyonline.com). The difference is risk: the latter requires validation steps (testing formulas, protecting macros) whereas the former does not. Auditors often check this: if critical processes rely on a spreadsheet, it is validated as software (Category 3, 4, or 5) rather than ignored as Cat 1.

Industry Survey Insight: Industry benchmarking reports highlight that smaller pharmas tend to be **spreadsheet-dependent**, whereas large enterprises use integrated validation tools and dedicated software (qualio.com). This underscores how GAMP 5's flexible approach applies differently by context. FDA's CSA guidance for medical-device production and quality system software (final in September 2025, revised February 2026) further motivates risk-based approaches, as it recommends that manufacturers consider unscripted testing for features, functions, and operations that are not high process risk (nsf.org). For a small firm, a part-time QA might use GAMP categories to justify validating only the minimum (e.g. treating many tools as low-risk). In contrast, a top-tier pharma provides validated templates for each category and invests in computerized validation management systems.

Risk Considerations and Regulatory Views

Regulators expect that systems affecting GMP-critical quality attributes (CQAs) are validated sufficiently. GAMP 5 dovetails with concepts in FDA guidance and EU Annex 11. For example, FDA's Computer Software Assurance guidance for medical-device production and quality management system software (issued February 3, 2026) supersedes Section 6 of FDA's 2002 General Principles of Software Validation and recommends scaling assurance activities, including the choice between scripted and unscripted testing, to process risk (fda.gov). This parallels GAMP's scaled approach (kneat.com). Both FDA and EMA emphasize focusing on patient/product quality risks (www.ptc.com). In the EU, Annex 11 explicitly calls for risk management in computerized systems. GAMP 5 mirrors these by adopting a science- and risk-based rationale.

From a regulatory perspective, basing validation on GAMP 5 categories is acceptable **provided it is justified**. ISPE and auditors warn that justification (or “fit-for-use” documentation) is key whenever deviating from a full waterfall approach (www.spectroscopyonline.com) (www.ptc.com). In practice, during an inspection, companies present their classification (e.g., “this system is Cat 4 due to its configurability”) and demonstrate that accordingly they performed appropriate tests. If a Category 1 component, such as a spreadsheet, directly feeds data into a GxP process, additional verification may be prudent (www.spectroscopyonline.com). The emphasis is always on **logic and documentation**.

Expert publications stress that GAMP 5 is a **guide, not a bind**. As one author quips, it allows deviations so long as “thought and intelligence coupled with effective risk management” are applied (www.spectroscopyonline.com). Therefore, savvy quality managers use categories as a starting point but tailor their protocol to actual risk: e.g. a critical infusion pump embedded software (Cat 3) might be tested more rigorously than typical if it poses patient hazards.

Data Analysis and Evidence-Based Points

Quantitative data on GAMP usage is scarce in open literature. However, some evidence-based claims can be made:

- A 2024 academic review notes that CSV (computer system validation) is **essential to maintain data integrity and product quality**, and that GAMP 5 is the core framework for it ([pmc.ncbi.nlm.nih.gov](https://pubmed.ncbi.nlm.nih.gov/41888888/)) ([pmc.ncbi.nlm.nih.gov](https://pubmed.ncbi.nlm.nih.gov/41888888/)). The review cites that failing validation can lead to serious compliance breaches.
- Industry benchmarking underscores a **market need for modern CSV tools**, with surveys where companies report pain points in audit readiness and data integrity (qualio.com). While not GAMP-specific, this reinforces why structured practices (like GAMP 5) remain critical.
- A 2005 review of risk management options for CSV (McDowall, *The Quality Assurance Journal*) concluded that no single risk analysis methodology fits every situation and proposed a single integrated document as an alternative to a full V-model for lower-risk systems, one way risk-based CSV **reduces unnecessary work** ([www.researchgate.net](https://www.researchgate.net/publication/228111111)).

In summary, though direct statistics are limited, the sources reviewed support applying structured, risk-based frameworks such as GAMP 5 rather than uniform full-lifecycle validation for every system ([www.researchgate.net](https://www.researchgate.net/publication/228111111)) ([pmc.ncbi.nlm.nih.gov](https://pubmed.ncbi.nlm.nih.gov/41888888/)). The 2024 review likewise treats validation as central to maintaining data integrity and meeting GxP requirements ([pmc.ncbi.nlm.nih.gov](https://pubmed.ncbi.nlm.nih.gov/41888888/)).

Future Trends and Implications

GAMP 5 continues to evolve with technology. The Second Edition (2022) already foreshadowed this: its expanded appendices cover topics such as **cloud computing, AI/machine learning, blockchain, and open-source software**, with Appendix D11 addressing AI/ML ([ispe.org](https://www.ispe.org)). Medical device industries also widely apply GAMP 5 now ([ispe.org](https://www.ispe.org)), bridging to standards like IEC 62304.

A major milestone arrived in **July 2025** with the publication of the **ISPE GAMP Guide: Artificial Intelligence**, a standalone 290-page guide. It provides a framework for developing and using AI-enabled computerized systems in GxP areas, covering risk management, scalable life-cycle activities, supplier collaboration, data and model governance, and monitoring and maintenance during operation (ispe.org) (ispe.org). It is designed as a stand-alone guide to be used in parallel with GAMP 5 Second Edition.

On the regulatory front, FDA issued final Computer Software Assurance (CSA) guidance in September 2025 and revised it in February 2026 to align with the Quality Management System Regulation (fda.gov). The guidance covers computers and automated data-processing systems used in medical-device production or quality management systems and recommends a risk-based approach to establish confidence in automation. It does not establish GAMP software categories or prescribe assurance solely by a category label. FDA's Quality Management System Regulation amendments to 21 CFR Part 820 took effect on February 2, 2026 (fda.gov). Together, CSA and GAMP 5 support risk-based assurance when applied within their respective scopes.

In the EU, the European Commission ran a stakeholder consultation from 7 July to 7 October 2025 on a revised Annex 11 (Computerised Systems), a revised Chapter 4 (Documentation) and a new Annex 22 on artificial intelligence, drafted by the EMA GMDP Inspectors Working Group in cooperation with PIC/S (health.ec.europa.eu). As of October 10, 2026, the Commission's EudraLex Volume 4 page still lists the January 2011 revision of Annex 11 and has not added an Annex 22 (health.ec.europa.eu).

Looking forward, as pharmaceutical manufacturing adopts Industry 4.0 elements (IoT devices, digital twins, continuous manufacturing), organizations should assess the components, intended use, suppliers, and risk scenarios of these novel systems. A cloud-based LIMS may include configured and custom components, while connectivity can introduce additional considerations such as cybersecurity and data-location controls. Experts recommend integrating **cybersecurity risk assessments** into the GAMP process when cloud or IoT is involved. Additionally, with accelerated development methods (agile/DevOps), lifecycle activities may overlap; GAMP 5 2nd ed supports iterative approaches over the old waterfall model.

Implications for organizations include ongoing training and updating CSV/CSA procedures. Some contract research organizations (CROs) now expect outsourcing partners (e.g. LIMS vendors or service providers) to adhere or align with GAMP 5 principles, since supplier data or services impact GxP compliance.

On balance, the **future direction** is that GAMP 5's flexible, risk-based paradigm, now reinforced by the FDA's CSA framework and ISPE's dedicated AI guide, can support the adoption of new technology while maintaining a risk-based compliance posture. Companies are encouraged to update their validation master plans accordingly, use GAMP categories thoughtfully (with the continuum concept), and leverage more automated validation tools. ISPE describes GAMP 5 Second Edition as promoting "increased use of software tools and automation to achieve greater control, higher quality, and lower risks throughout the life cycle" (ispe.org) (guidance-docs.ispe.org).

Conclusion

GAMP 5's category framework is a cornerstone of modern computerized system validation. By classifying software and hardware components according to how they are built and supplied, it helps companies **prioritize validation effort** and ensure "fitness for use". As summarized in this report, Category 1

infrastructure software typically needs the least product-specific verification and Category 5 custom software typically needs the most lifecycle control, although overall effort follows GxP impact and identified risks rather than the category number (www.spectroscopyonline.com) (www.ptc.com). Hardware components likewise fall into standard and custom types (qualio.com) (pmc.ncbi.nlm.nih.gov). Adopting these categories properly (along with critical thought) supports alignment with regulatory expectations such as 21 CFR Part 11 and EU Annex 11 and can help avoid unnecessary over-validation.

This research has examined GAMP 5 categories through multiple sources: ISPE publications, industry analyses, and expert commentaries. Throughout, claims are linked to the sources consulted. When applied judiciously, GAMP 5's risk-based approach can help focus lifecycle and assurance activities on identified risks; the magnitude of any efficiency benefit depends on the system context. With the 2025 publication of the ISPE GAMP AI Guide and FDA's revised February 2026 CSA guidance for medical-device production and quality-management-system software, the regulatory landscape continues to emphasize risk-based assurance. As pharmaceutical and biotech industries advance, the GAMP 5 categories approach will continue evolving, but its core principle, to **validate based on risk and intended use**, remains essential (www.ptc.com) (xevalics.com).

References: Authoritative sources cited above include official ISPE guidelines (GAMP 5 Second Edition and the 2025 GAMP AI Guide) (guidance-docs.ispe.org) (ispe.org) (ispe.org), regulatory guidance (FDA CSA, issued 2025 and revised 2026; Annex 11 summaries) (nsf.org) (www.ptc.com), and industry whitepapers and journals (www.spectroscopyonline.com) (www.ptc.com) (pmc.ncbi.nlm.nih.gov). Factual statements and examples are linked to the published references consulted. These span peer-reviewed articles (pmc.ncbi.nlm.nih.gov), technical magazines (www.spectroscopyonline.com), and lifecycle guides (www.ptc.com), ensuring a balanced, evidence-based report.

Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. <https://intuitionlabs.ai/articles/gamp-5-guidelines-system-validation>
2. <https://www.spectroscopyonline.com/view/understanding-and-interpreting-new-gamp-5-software-categories>
3. <https://kneat.com/article/what-is-gamp-5/>
4. <https://pmc.ncbi.nlm.nih.gov/articles/PMC11416705/>
5. <https://www.qualio.com/blog/complete-guide-to-computer-system-validation>
6. <https://www.ptc.com/en/blogs/alm/gamp-5-guide-categories-requirements-and-validation>
7. <https://xevalics.com/gamp5-2nd-edition-you-categories-of-software-hardware/>
8. <https://intuitionlabs.ai/articles/ai-biopharma-regulation-2025>
9. <https://guidance-docs.ispe.org/doi/book/10.1002/9781946964571?nl0Jcb92=18LgdwoT2QF>
10. <https://intuitionlabs.ai/articles/samd-definition-and-scope>
11. <https://ispe.org/pharmaceutical-engineering/january-february-2024/leveraging-gampr-5-second-edition-medical-devices>
12. https://www.researchgate.net/publication/229903668_Effective_and_practical_risk_management_options_for_computerised_system_validation
13. <https://gmpua.com/World/Ma/09/d.htm>

14. <https://ispe.org/pharmaceutical-engineering/january-february-2026/when-category-not-category>
15. <https://www.nsf.org/life-science-regulatory-news/fda-final-guidance-computer-software-assurance-csa>
16. <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/computer-software-assurance-production-and-quality-management-system-software>
17. <https://ispe.org/publications/guidance-documents/gamp-5-guide-2nd-edition>
18. <https://ispe.org/pharmaceutical-engineering/ispeak/new-gamprguide-provides-framework-achieve-high-quality-ai-enabled>
19. <https://ispe.org/publications/guidance-documents/gamp-guide-artificial-intelligence>
20. <https://www.fda.gov/medical-devices/postmarket-requirements-devices/quality-management-system-regulation-qmsr>
21. https://health.ec.europa.eu/consultations/stakeholders-consultation-eudralex-volume-4-good-manufacturing-practice-guidelines-chapter-4-annex_en
22. https://health.ec.europa.eu/medicinal-products/eudralex/eudralex-volume-4_en

THE PUBLISHER

About IntuitionLabs

IntuitionLabs is an AI consulting, custom software development and data engineering firm serving pharmaceutical, biotechnology, medical-device and other life-science organizations. We work with clinical, regulatory, medical-affairs, commercial, quality and IT teams to connect technology decisions with the work people need to accomplish.

AI consulting and adoption

Our AI enablement services cover readiness assessments, use-case selection, governance and policies, team workshops, adoption measurement and ongoing advisory support. We help organizations structure the information layer behind AI: source material, context, permissions and maintained knowledge that make generated answers useful and reviewable. Private LLM inference and hosted AI options support teams evaluating how to operate AI with appropriate control over their data and infrastructure.

Software, data and life-science workflows

IntuitionLabs develops custom software for pharma and biotech, integrates enterprise systems, and builds data engineering and business intelligence solutions. Areas of focus include AI agents, regulatory research, medical writing, medical affairs, CMC information, competitive intelligence and clinical-document workflows. Our eTMF intelligence work includes cross-system reconciliation and inspection-readiness support.

Enterprise platforms and regulated delivery

We provide Veeva services, application support, managed services, integrations and custom applications, alongside enterprise content work involving platforms such as Egnyte. For regulated workflows, our services include GxP enablement, computer-system validation and software development addressing 21 CFR Part 11 requirements. The applicable controls, validation responsibilities and acceptance criteria are defined for each engagement.

Work with IntuitionLabs

Explore [AI enablement](#), [pharma and biotech software development](#), [data engineering and BI](#), and [Veeva services](#). [Contact IntuitionLabs](#) to discuss your workflow, information sources and implementation needs.

IntuitionLabs publishes educational research to help life-science teams make informed technology decisions. Coverage of a product or organization does not imply a client relationship, endorsement or partnership.

Website: <https://intuitionlabs.ai>

This article is educational. Verify consequential medical, legal, financial, regulatory and technical decisions with appropriate professionals and the cited primary sources. Company services are described separately from the article's research findings.