Reliable Context

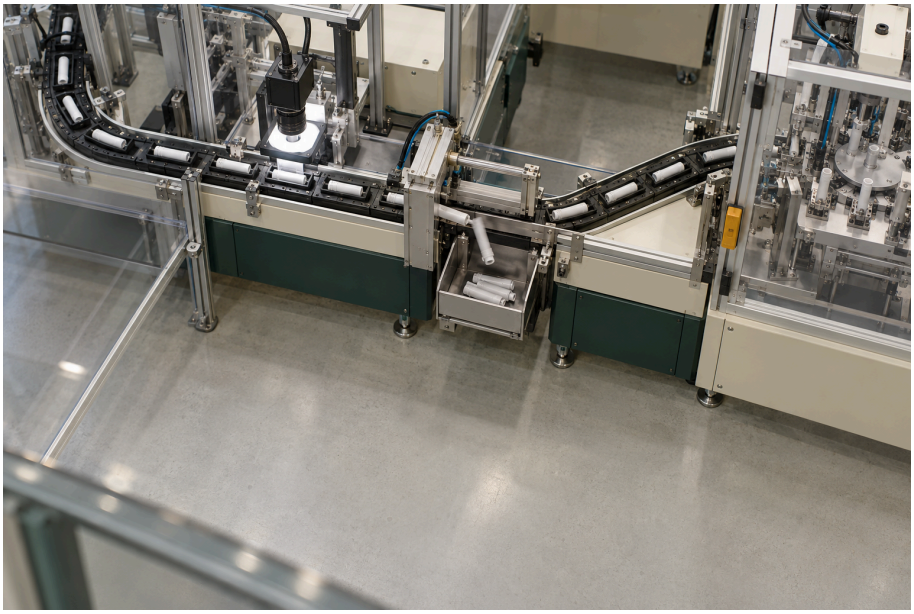
RELIABLE CONTEXT / RESEARCH & PRACTICAL GUIDANCE

Computer Software Assurance vs CSV: GAMP 5 and Annex 11

> Reliable Context is a kernel of truth: a system of record for organizations that fuse private and public information and must defend every value they act on. One canonical record per real thing, a cited source and an observation date behind every value, unknowns declared rather than left blank, and any past state of the record reproducible.

Published by Reliable Context · 2026-10-29 · computer software assurance · gamp 5 · computer system validation · csv vs csa · fda csa guidance

Original article: https://reliablecontext.com/articles/gxp-computerized-system-validation-gamp-5-and-fda-csa



In this article

1. Why validate at all
2. GAMP 5: categories and critical thinking
3. Annex 11: suppliers, validation, change and periodic evaluation
4. FDA Computer Software Assurance
5. CSV versus CSA
6. Validating AI-enabled components
7. Worked example (fictional)
8. The evidence package
9. Common over-documentation traps
10. Checklist
11. Sources

Why validate at all

Computerized system validation (CSV) is the documented demonstration that a computerized system does what its regulated use requires, and keeps doing so after changes. The obligation is old; what has changed is how much paper regulators expect it to generate.

In the European Union, EU GMP Annex 11 says of computerised systems used in GMP-regulated activities: "The application should be validated; IT infrastructure should be qualified." In the United States, FDA's Computer Software Assurance guidance treats validation of device production and quality management system software as a requirement of the device Quality Management System Regulation.

Both texts tie the depth of validation to risk. Annex 11 clause 1 says "decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment." ICH Q9(R1), adopted on 18 January 2023, states the underlying principle: "The level of effort, formality and documentation of the quality risk management process should be commensurate with the level of risk."

For a team running data systems (LIMS, MES, eQMS, analytics), that becomes one question per function: what goes wrong if this fails, and how much evidence does that failure justify?

GAMP 5: categories and critical thinking

ISPE published GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems (Second Edition) in July 2022. Its public page states that the second edition maintains "the principles and framework of the first edition", adds discussion of FDA's Computer Software Assurance work, expands appendices to AI/ML, cloud computing, blockchain and open-source software, and highlights "critical thinking" by knowledgeable subject matter experts (SMEs) in choosing an approach.

As described by R.D. McDowall in a 2009 analysis of the first edition's software categories:

- **Category 1, infrastructure software** (operating systems and broader infrastructure layers), which is qualified rather than validated.

- **Category 2, firmware**, which GAMP 5 dropped; firmware is accommodated in the other categories according to its nature.
- **Category 3, non-configured products**: software used as supplied, configured only for its run-time environment.
- **Category 4, configured products**: software whose functions can be modified to match a business process, which "triggers increased validation effort".
- **Category 5, custom applications**: the highest-risk category, because the code may be unique.

McDowall stresses that categories 3 to 5 are "a continuum rather than discrete silos". Treat the category as one input to effort, not a lookup table of deliverables; ICH Q9(R1) likewise calls formality "not a binary concept".

Annex 11: suppliers, validation, change and periodic evaluation

Annex 11 is EU GMP guidance in EudraLex Volume 4, in operation since 30 June 2011. Four clauses carry most of the validation workload.

Clause 3, suppliers and service providers. Where third parties provide, configure, validate, maintain or host a system, "formal agreements must exist" with clear statements of the third party's responsibilities (3.1). "The need for an audit should be based on a risk assessment" (3.2). Documentation supplied with commercial off-the-shelf products "should be reviewed by regulated users to check that user requirements are fulfilled" (3.3), and supplier quality and audit information should be available to inspectors on request (3.4).

Clause 4, validation. Validation documentation should cover the relevant life-cycle steps, and manufacturers "should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment" (4.1). It also asks for a system inventory (4.3), risk-based, traceable user requirements (4.4), tests covering parameter limits, data limits and error handling (4.7), and checks that migrated data are "not altered in value and/or meaning" (4.8).

Clause 10, change and configuration management. Any change, including configuration changes, "should only be made in a controlled manner in accordance with a defined procedure."

Clause 11, periodic evaluation. Systems "should be periodically evaluated to confirm that they remain in a valid state", considering deviations, incidents, upgrade history, performance, security and validation status, among other inputs.

Status of the revision. Drafts of a revised Annex 11, a revised Chapter 4 and a new Annex 22 on artificial intelligence went to a joint European Commission and PIC/S stakeholder consultation that opened on 7 July 2025 and closed on 7 October 2025. On 28 October 2026 the EudraLex Volume 4 page still lists "Annex 11 Computerised Systems (revision January 2011)" and lists no Annex 22. The 2011 text remains in force; the drafts show direction, not obligation.

FDA Computer Software Assurance

History and current title

The guidance has had three published versions, all under docket FDA-2022-D-0795:

Version	Date	Title	Status
Draft	13 September 2022 (87 FR 56059)	Computer Software Assurance for Production and Quality System Software	Superseded
Final	24 September 2025	Computer Software Assurance for Production and Quality System Software	Superseded
Final, revised	3 February 2026	Computer Software Assurance for Production and Quality Management System Software	Current

The renaming follows the device rule. FDA published the Quality System Regulation amendments on 2 February 2024 (89 FR 7496), effective 2 February 2026. The rule incorporated ISO 13485:2016 by reference and removed most former Part 820 text, including 820.70; the February 2026 guidance therefore cites ISO 13485 subclauses 4.1.6, 7.5.6 and 7.6 as the validation requirements.

Scope, as written

The guidance "provides recommendations regarding computer software assurance for computers or automated data processing systems used as part of production or the quality management system for medical devices." It does not cover design verification or validation of device software functions. It was issued by CDRH and CBER (CDER was consulted). A drug manufacturer under 21 CFR Part 211 can read it as FDA thinking on risk-based assurance, not as guidance written for its regulation.

It defines computer software assurance as "a risk-based approach for establishing and maintaining confidence that software is fit for its intended use", following "a least-burdensome approach". Software outside validation requirements includes email, accounting, networking, user authentication, and backup and restore.

The risk framework

FDA presents process risk "in a binary manner, 'high process risk' and 'not high process risk.'" A feature, function or operation is **high process risk** "when its failure to perform as intended may result in a quality problem that foreseeably compromises safety, meaning a medical device risk." It is **not high process risk** "when its failure to perform as intended would not result in a quality problem that foreseeably compromises safety." Examples of high process risk include functions that "measure, inspect, analyze and/or determine acceptability of product or process with limited or no additional human awareness or review." Not high examples include CAPA routing, complaint logging, and functions that "manage data (process, store, and/or organize data)". Finer grades are allowed; anything below high counts as "not high".

Assurance activities, as written

The guidance lists testing types "including, but not limited to":

- **Unscripted testing**: "Dynamic testing in which the tester's actions are not prescribed by written instructions in a test case." It includes **scenario testing**, which the guidance says is "Also referred to as Ad-Hoc Testing", and experience-based testing such as **error guessing** and **exploratory testing**, "in which the tester spontaneously designs and executes tests based on the tester's existing relevant knowledge, prior exploration of the test item (including results from previous tests), and heuristic 'rules of thumb'".
- **Scripted testing**: "Testing in which test cases are recorded (e.g., document in a test management tool or in a spreadsheet) and can then be executed manually or executed automatically using an automated testing tool." Its Table 1 distinguishes robust from limited scripted testing.

For high process risk, manufacturers "may choose to consider more rigor such as the use of scripted testing or a hybrid approach"; otherwise unscripted methods may suffice. The reverse is explicitly allowed where it works better, and vendor work, downstream process controls and monitoring data can reduce effort.

CSV versus CSA

CSA does not replace validation; it describes methods that "provide objective evidence to fulfill regulatory requirements, such as computer software validation requirements". The contrast is between document-heavy practice and the guidance.

Dimension	Document-heavy CSV practice	FDA CSA guidance (Feb 2026)
Unit of analysis	Whole system	Each feature, function or operation, by intended use
Risk model	Often multi-level scoring per system	Binary: high process risk or not
Default test method	Step-by-step scripts with expected results	Risk-based choice of unscripted, limited scripted or robust scripted testing
Vendor work	Repeated in-house	Leveraged via purchasing controls and vendor assessment
Evidence form	Paper, signatures per step, screenshots	Digital records, logs and audit trails, "as opposed to paper documentation, screenshots"
Volume of record	As much as can be produced	"need not include more evidence than necessary" for the risk identified
After go-live	Revalidation on change	Validated state maintained with monitoring, iterative testing and change assessment

Validating AI-enabled components

CSA states that its risk framework can be applied to "artificial intelligence/machine learning tools" used as part of production or the quality management system. Two non-final texts add AI-specific expectations.

FDA's draft guidance on AI to support regulatory decision-making for drug and biological products (January 2025, docket FDA-2024-D-4689) was still labelled draft on fda.gov on 28 October 2026. Its draft text proposes a seven-step credibility assessment for a model's context of use, defines model risk as a combination of

"model influence" and "decision consequence", and excludes drug discovery and "operational efficiencies" that do not affect patient safety, drug quality or study reliability.

The EU draft Annex 22 covers AI models in critical GMP applications. As drafted, it applies only to static models with deterministic output, and says generative AI and large language models "should not be used in critical GMP applications". It asks for an SME-approved intended use, acceptance criteria "at least as high as the performance of the process it replaces", independent test data under access control and audit trail, recorded confidence scores, change and configuration control, and drift monitoring.

The common core: a defined intended use, a pre-approved performance threshold, independent test evidence, and monitoring after release.

Worked example (fictional)

Halden Therapeutics AG (fictional) makes drug product at an EU GMP site; its US subsidiary Halden Devices Inc. (fictional) assembles a pen-injector under the device QMSR. Both use one cloud MES. At Halden Devices, the CSV lead splits it into functions:

MES function	Intended use	Risk call (CSA)	Assurance chosen
Material restocking; operator checks material before use	Supports production	Not high: wrong material is caught by a qualified person	Vendor assessment, configuration record, scenario testing
Automated camera inspection that rejects or releases components with no human review	Direct: determines acceptability	High: failure may release defective components	Robust scripted tests on rejection limits plus exploratory testing of edge images
Batch genealogy report used in trending	Direct: manages data	Not high	Exploratory testing of report filters; rely on system logs as evidence

At the EU site, the supplier relationship falls under Annex 11 clause 3: a formal agreement, a risk-based audit decision, and review of supplier documentation against user requirements. The system sits in the clause 4.3 inventory, releases go through clause 10 change control, and a clause 11 periodic evaluation reads incidents, deviations and upgrade history. Retraining the camera model would be a change under draft Annex 22 requiring a documented retest decision; under CSA it stays high process risk.

The evidence package

CSA lists what each function's record should hold; Annex 11 adds system-level items.

Evidence item	What it demonstrates	Basis
Intended use per feature, function or operation	Why the function is in scope	CSA V.A.1 and V.A.6
Risk-based analysis and its result	Why this level of rigor	CSA V.A.2; Annex 11 cl. 1; ICH Q9(R1)
Supplier assessment and agreement	What vendor work is relied on	CSA V.A.5; Annex 11 cl. 3

Evidence item	What it demonstrates	Basis
Description of testing, issues found, conclusion of acceptability	That the function performs as intended	CSA V.A.6, Table 1; Annex 11 cl. 4.7
Who tested, when; approval where appropriate	Attribution	CSA V.A.6
System inventory and, for critical systems, system description	What exists and how data flow	Annex 11 cl. 4.3
Migration checks	Data not altered in value or meaning	Annex 11 cl. 4.8
Change records and periodic evaluation reports	That the validated state persists	Annex 11 cl. 10 and 11; CSA V

Each item should be retrievable as it stood on a given date: "what was the validated state before the March release?" is a point-in-time question. System-generated records such as an audit trail count as CSA evidence; reviewing them is a separate topic.

Common over-documentation traps

1. **Screenshots of what the system already logs.** CSA recommends digital records over "paper documentation, screenshots, or duplicating results already digitally retained by the software".
2. **One risk rating for a whole system.** A single high rating drags low-risk functions into full scripting; CSA rates functions separately.
3. **Step-by-step scripts for not-high-risk functions.** Exploratory or scenario testing with a summary record is a listed option.
4. **Re-executing the vendor's tests.** CSA treats vendor work as a starting point; Annex 11 3.3 asks users to review it against requirements.
5. **Validating tools outside the regulated process.** In CSA's debugger example, a least-burdensome check suffices.
6. **Treating every log as a Part 11 record.** CSA's example: routine activity logs not needed to support a validated state are outside Part 11.
7. **Stand-alone risk reports for low-risk decisions.** ICH Q9(R1) allows lower-formality risk work embedded in the quality system.

The opposite failure is real: ICH Q9(R1) says "Resource constraints should not be used to justify the use of lower levels of formality."

Checklist

- Is each function's intended use written down, and is it inside or outside validation scope?
- Is each function rated high or not high process risk, with the reason?
- Does the chosen test type match the risk, and is vendor evidence used where it exists?
- Do records rely on system-generated evidence rather than copies of it?
- Are inventory, supplier agreement, change control and periodic evaluation current (EU sites)?

- For AI components: is there an intended use, a pre-approved acceptance threshold, independent test data and drift monitoring?
- Which sites fall under EU GMP, the US device QMSR or US drug CGMP?

This article is educational and is not legal or regulatory advice; confirm obligations with your quality and regulatory functions for each jurisdiction. For quality data in pharmaceutical settings, Reliable Context keeps one canonical record per real thing, with a cited, dated source behind every value, unknowns declared and any past state reproducible, inside the customer's perimeter.

Sources

1. Computer Software Assurance for Production and Quality Management System Software, FDA guidance page, February 2026 — title, date, docket, supersession.
2. Computer Software Assurance for Production and Quality Management System Software, FDA guidance PDF, 3 February 2026 — scope, risk framework, testing types, records, QMSR footnote.
3. Notice of availability, final CSA guidance, Federal Register, 24 September 2025 — 2025 final and 2022 draft dates.
4. Medical Devices; Quality System Regulation Amendments, 89 FR 7496, Federal Register, 2 February 2024 — QMSR dates.
5. GAMP 5 Guide, 2nd Edition, ISPE, July 2022 — publication date, public summary.
6. Understanding and Interpreting the New GAMP 5 Software Categories, R.D. McDowall, Spectroscopy, June 2009 — software categories.
7. EudraLex Volume 4, Annex 11: Computerised Systems, European Commission, 2011 — clauses 1, 3, 4, 10 and 11.
8. EudraLex Volume 4, European Commission — current Annex 11 revision; no Annex 22.
9. Stakeholders' Consultation on Chapter 4, Annex 11 and New Annex 22, European Commission, 2025 — consultation dates and status.
10. Joint stakeholders consultation on Chapter 4, Annex 11 and Annex 22, PIC/S, 7 July 2025 — joint consultation.
11. Draft Annex 22: Artificial Intelligence, European Commission consultation document, July 2025 — draft scope and requirements.
12. ICH Q9(R1) Quality Risk Management, ICH, adopted 18 January 2023 — principles, formality.
13. Considerations for the Use of AI to Support Regulatory Decision-Making for Drug and Biological Products, FDA draft guidance page, January 2025 — draft status.
14. Same draft guidance, FDA PDF, January 2025 — scope, steps, model risk.

Source links

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

1. https://health.ec.europa.eu/system/files/2016-11/annex11_01-2011_en_0.pdf
2. https://www.fda.gov/media/188844/download
3. https://database.ich.org/sites/default/files/ICH_Q9%28R1%29_Guideline_Step4_2022_1219.pdf

4. https://ispe.org/publications/guidance-documents/gamp-5-guide-2nd-edition
5. https://spectroscopyonline.com/understanding-and-interpreting-new-gamp-5-software-categories
6. https://health.ec.europa.eu/medicinal-products/eudralex/eudralex-volume-4_en
7. https://health.ec.europa.eu/consultations/stakeholders-consultation-eudralex-volume-4-good-manufacturing-practice-guidelines-chapter-4-annex_en
8. https://picscheme.org/en/news/joint-stakeholders-consultation-on-the-revision-of-chapter-4
9. https://www.federalregister.gov/documents/2022/09/13/2022-19763/computer-software-assurance-for-production-and-quality-system-software-draft-guidance-for-industry
10. https://www.federalregister.gov/documents/2025/09/24/2025-18468/computer-software-assurance-for-production-and-quality-system-software-guidance-for-industry-and
11. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/computer-software-assurance-production-and-quality-management-system-software
12. https://www.federalregister.gov/documents/2024/02/02/2024-01709/medical-devices-quality-system-regulation-amendments
13. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/considerations-use-artificial-intelligence-support-regulatory-decision-making-drug-and-biological
14. https://www.fda.gov/media/184830/download
15. https://health.ec.europa.eu/document/download/5f38a92d-bb8e-4264-8898-ea076e926db6_en?filename=mp_vol4_chap4_annex22_consultation_guideline_en.pdf

THE PUBLISHER

About Reliable Context

Reliable Context is a system of record for organizations that fuse private and public information and must defend every value they act on.

The guarantees

One canonical record per real thing: duplicates resolve by rule, ambiguity is shown rather than hidden, and related organizations relate without ever being merged. A verbatim, cited source and an observation date sit behind every value. Unknowns are declared as not found, blocked or not applicable with a reason, never left as an empty cell. Any past state of the record is reproducible, together with what changed since.

Where it runs

It runs inside the customer's perimeter, one database per organization. Permitted sources, model routing, reader clearance and retention are set as the customer's own policies, and every value is exportable with its chain of custody for an auditor or regulator.

What it is not

It is not a vector database or a RAG framework, not a data catalog, MDM or data-quality suite, not a CRM or data-enrichment vendor, and not a chatbot or AI assistant. Where a reader needs one of those, the honest answer is to say so and point them there.

Visit

See Reliable Context.

Reliable Context is in production use in two sectors; more than six thousand of its identity decisions were made by rule and none has been reversed. Articles published here explain general practice, cite their primary and academic sources, and name the jurisdiction of any regulatory rule they describe. They are not legal, regulatory or compliance advice for a specific organization, and requirements change.

Website: https://reliablecontext.com

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.