Design Once, Comply Twice: Computerized Systems Strategy as CSA and Annex 11 Modernize Together



A cGMP Consulting White Paper on Harmonized Control Design for FDA and EU-Inspected Operations – October 13, 2026

Computerized Systems | Data Integrity | Global Compliance | Annex 11

An educational resource for executive and technical leaders in FDA-regulated life sciences.

Executive Summary

Two major computerized systems frameworks are modernizing at once, on different clocks. In the United States, the FDA finalized its Computer Software Assurance guidance in September 2025 and updated it in February 2026 to align with the Quality Management System Regulation. In Europe, the Commission published a draft revision of EU GMP Annex 11 on July 7, 2025, alongside a new Annex 22 addressing artificial intelligence and a revised Chapter 4 on documentation. The Annex 11 consultation closed on October 7, 2025, and the final text is expected in mid-2026.

For an organization inspected by both authorities, the danger is not that either framework is unmanageable. It is that treating them as two sequential projects produces duplicated effort, conflicting controls, and remediation whiplash, where systems get rebuilt once for the American expectation and again for the European one. The scale of the Annex 11 change makes that expensive. The draft grows the annex from five pages to nineteen, restructured into seventeen sections plus a glossary, with substantially

expanded treatment of audit trails, supplier and service management, identity and access management, and, for the first time, cybersecurity as a core requirement.

The two frameworks share a direction and differ in emphasis. Both are risk-based and lifecycle-oriented. The FDA guidance is about proportioning assurance effort to intended use and risk of failure, cutting low-value documentation. The Annex 11 draft is more prescriptive about technical controls, with expectations including multi-factor authentication for electronic signatures, audit trails that capture data creation rather than only modification and deletion, and specified elements in supplier contracts. Here is the useful asymmetry: a control set designed to satisfy the more prescriptive framework will generally satisfy the more principles-based one. The reverse is not reliably true.

This paper compares the two frameworks, marks where they align and diverge, and lays out how to design a single harmonized control set instead of two. It covers the specific upgrades dual-jurisdiction organizations should prioritize, the sequencing that avoids rebuilding systems per regulator, and the governance multi-authority operations need. Design once and you absorb both changes at a fraction of what it costs the organizations that respond to each regulator in turn.

Introduction

Computerized systems have gone from supporting tools to core regulated assets. Manufacturing execution systems, laboratory systems, quality management platforms, and a growing pile of cloud services now hold the records product release depends on. Regulators responded by modernizing the frameworks that govern them, and 2025 and 2026 brought the most significant changes in over a decade on both sides of the Atlantic.

The timing is awkward. The FDA finalized Computer Software Assurance in September 2025 and refined it in February 2026. The European Commission published its Annex 11 draft in July 2025 with a consultation closing that October and final text expected mid-2026. So an organization inspected by both has been absorbing a settled American framework while a European one takes shape, and the natural move is to deal with the settled one first and the emerging one later.

That move is expensive. Remediate your computerized systems against the FDA framework, then discover that Annex 11 expects technical controls the American work never touched, and you rebuild the same systems twice. Worse, controls designed for one framework in isolation can fight the other, leaving you with a system that satisfies neither cleanly. The alternative is to design a target state informed by both frameworks from the start, take the more demanding expectation on each dimension, and implement once.

This paper is for the quality, validation, and technology leaders in organizations subject to both FDA and EU or PIC/S inspection, and for the executives funding the remediation. It focuses on how to design a harmonized control set and sequence the work so you are not doing it twice.

Industry Background

The current Annex 11 was published in June 2011 and has governed computerized systems in EU good manufacturing practice for well over a decade. It set out risk-based principles that fit the technology of its era, when systems were largely on-premises, deterministic, and stable. The years since brought cloud computing, software as a service, mobile applications, continuous delivery, and artificial intelligence, none of which the 2011 text contemplated in any detail.

The European Commission signaled the revision with a concept paper in November 2022, and the drafts landed on July 7, 2025. The package included the Annex 11 revision, a new Annex 22 addressing artificial intelligence, and a revised Chapter 4 on documentation that folds data integrity principles directly into the documentation chapter. Comments were accepted until October 7, 2025, and final publication is expected in mid-2026. Together, the three documents are the most substantial modernization of EU GMP digital compliance in fourteen years.

The American trajectory ran in parallel but started somewhere else. The FDA's Computer Software Assurance approach came out of the Case for Quality initiative within the Center for Devices and Radiological Health, aimed at the observation that validation practice had turned documentation-heavy in ways that burned resources without proportionate benefit. The guidance was finalized on September 24, 2025, and updated on February 3, 2026, to align with the Quality Management System Regulation and ISO 13485:2016.

Industry frameworks tracked both. The GAMP 5 second edition, published in July 2022, modernized the risk-based lifecycle approach, leaned on critical thinking by knowledgeable subject matter experts, and explicitly discussed the FDA's emerging Computer Software Assurance work. The ISPE GAMP Guide on Artificial Intelligence followed in July 2025. The convergence among the FDA guidance, the Annex 11 draft, and the GAMP framework is substantial, and the Annex 11 draft explicitly aligns with international frameworks including PIC/S, GAMP 5, ICH Q9, ICH Q10, 21 CFR Part 11, and ISO 27001.

Regulatory Landscape

Designing a harmonized control set means knowing exactly where the frameworks agree and where they differ in emphasis and prescription.

The FDA Framework

The Computer Software Assurance guidance addresses software used in production or the quality system, applying a four-step method: define intended use, assess the risk of failure, plan assurance activities proportionate to that risk, and document the basis for confidence. The February 2026 update aligned the guidance with the Quality Management System Regulation, adopted recognized cloud computing definitions for software as a service, platform as a service, and infrastructure as a service, addressed cybersecurity evidence, expanded vendor oversight recommendations, and stated explicitly that the approach applies to automation tools, data analytics tools, and artificial intelligence and machine learning tools used in production or the quality system. Underlying requirements including 21 CFR Part 11 for electronic records and signatures remain in force.

The Annex 11 Draft

The Annex 11 draft expands the annex from five pages to nineteen, restructured into seventeen chapters plus a glossary and organized around eight overarching principles. Where validation dominated the 2011 text, the draft shifts emphasis toward security, identity and access management, and audit trails. Notable expansions include ten subsections addressing audit trails, a security chapter running to roughly twenty subsections covering patching, penetration testing, firewalls, and removable media controls, expanded treatment of supplier and service management with specified mandatory contract elements, system alarms, and periodic review. The draft treats computerized systems as core GMP-controlled assets rather than supporting tools, and it aligns with ICH Q9, ICH Q10, and ISO 27001.

Where the Frameworks Diverge

Both are risk-based and lifecycle-oriented, but they differ in character. The FDA guidance is principles-based, focused on proportioning effort and documenting the basis for confidence. The Annex 11 draft is considerably more prescriptive about technical controls. Three divergences matter most in practice. First, the draft mandates multi-factor authentication for electronic signatures, with eIDAS-aligned trust services and time zone-aware timestamping, which exceeds what 21 CFR Part 11 requires explicitly. Second, the draft expands audit trail scope to capture data creation events, not only modification and deletion, with explicit immutability and periodic review obligations and ALCOA++ alignment. Third, the draft specifies mandatory elements in supplier contracts, where the FDA guidance recommends vendor oversight without prescribing contract content.

Annex 22 and Artificial Intelligence

The divergence is sharpest on artificial intelligence. The FDA's Computer Software Assurance guidance brings AI and machine learning tools within its risk-based scope, permitting their use in production and quality systems subject to appropriate assurance. The draft Annex 22 takes a more restrictive position, limiting artificial intelligence in GMP-critical applications to static, deterministic models, and excluding dynamic models, generative artificial intelligence, and large language models from critical use. For anyone deploying AI globally, that is a material difference: an application permissible under the American framework subject to assurance may be excluded from critical use under the European one. Track the final Annex 22 text closely, because this position directly constrains AI deployment strategy in EU-inspected operations.

Chapter 4 and the Data Integrity Foundation

The revised Chapter 4 on documentation folds data integrity principles in directly, substantially expanding the chapter and adding dedicated treatment of data governance and controls for computerized systems. This matters because it moves data integrity expectations from guidance into the body of the GMP guide itself, giving them a more binding character in the European framework than the guidance-based approach in the United States.

> *The practical design rule follows from the asymmetry. On each control dimension, the Annex 11 draft is generally the more prescriptive framework, and a control set built to its expectations will usually satisfy the FDA's risk-based approach. Building to the FDA framework alone will not reliably satisfy Annex 11, because the American guidance does not prescribe the technical controls the European draft mandates.*

Current Industry Challenges

The difficulties dual-jurisdiction organizations face are mostly problems of sequencing, ownership, and technical debt, not of understanding either framework.

Sequential Project Thinking

The dominant challenge is organizational. Because the FDA framework settled first, organizations naturally addressed it first, treating the European revision as a future project. That produces remediation designed against one framework in isolation, and when the second framework's expectations arrive, the same systems need a second pass. Beyond the duplicated cost, the second pass frequently reveals that the first pass made design choices you now have to reverse rather than extend.

The Multi-Factor Authentication Gap

The Annex 11 draft's requirement for multi-factor authentication on electronic signatures exposes a widespread technical gap. Plenty of GxP systems, older ones and standalone laboratory instruments especially, do not support multi-factor authentication natively. Retrofitting is not always technically feasible, and where it is, it may take a system upgrade or replacement rather than a configuration change. Discover this requirement late and you are looking at a remediation program with long lead times and potential capital implications.

Audit Trail Scope Expansion

Expanding audit trail scope to capture data creation, alongside immutability requirements and periodic review obligations, goes beyond how many systems are currently configured. Systems that log modifications and deletions but not creation events need configuration changes that may not be available, and the periodic review obligation adds a resource commitment many organizations have not staffed. Because audit trail review is already a common enforcement finding under existing expectations, organizations with an existing gap face a compounding problem.

Cybersecurity as a Quality Obligation

The Annex 11 draft treats cybersecurity as a core GMP requirement, with a substantial security chapter covering patching, penetration testing, firewalls, and removable media controls. The FDA guidance addresses cybersecurity evidence within software assurance. In most organizations, cybersecurity is owned by IT and GxP compliance is owned by quality, and nobody owns the intersection. The result is a control domain both frameworks now expect and no function currently manages end to end.

Supplier Contract Requirements

The Annex 11 draft specifies mandatory elements in supplier and service contracts, which means existing agreements with cloud and software vendors may be insufficient no matter how well the systems themselves are controlled. Contract renegotiation depends on vendor cooperation and commercial leverage, and it runs on timelines the organization does not fully control. Identify this requirement late and you may find you cannot remediate it quickly at any price.

Divergent AI Positions

The gap between the FDA's risk-based accommodation of AI and the draft Annex 22 restriction of GMP-critical applications to static, deterministic models is a genuine strategic conflict. Deploy dynamic or generative AI into critical quality workflows and you may satisfy American expectations while putting your European operations outside the permitted envelope. This is not a control design problem. It is a deployment strategy problem, and it needs a decision, not a technical fix.

Risks of Poor Implementation

The risks of treating these frameworks separately are mostly economic and operational, though they turn regulatory when remediation lags the final Annex 11 text.

Risk Category	Potential Consequence
Duplicated remediation	The same systems rebuilt twice, once against each framework, at multiples of the cost of a single harmonized program.
Conflicting controls	Design choices made for one framework that must be reversed for the other, producing rework rather than extension.
Long-lead technical gaps	Multi-factor authentication and audit trail scope gaps discovered late, requiring system upgrades or replacement with lead times measured in quarters.
Contractual exposure	Supplier agreements lacking mandated elements, remediable only through renegotiation on timelines the organization does not control.
Unowned cybersecurity	GxP system security falling between IT and quality, with neither function accountable for a domain both frameworks now expect.
AI strategy conflict	Artificial intelligence deployed under the American risk-based framework that falls outside the European position on GMP-critical applications.
Inspection findings	Gaps against the final Annex 11 text at EU or PIC/S inspection, in an area where audit trail and access control findings are already common.

The timing risk deserves emphasis. With the final Annex 11 text expected mid-2026, organizations that begin gap assessment only on publication will be remediating against a live expectation rather than a draft. And because the most consequential gaps, particularly multi-factor authentication and audit trail configuration, have long remediation lead times, an organization that starts late may simply be unable to close them before its next inspection no matter how many resources it throws at the problem. The draft

has been public since July 2025 and its direction is clear, which makes a late start a choice rather than a constraint.

Best Practices

The organizing principle is to design a single target state informed by both frameworks and implement once, taking the more demanding expectation on each dimension.

Design to the More Demanding Expectation

For each control dimension, figure out which framework sets the higher bar and design to it. Because the Annex 11 draft is generally more prescriptive on technical controls while the FDA guidance is more explicit about proportioning assurance effort, the harmonized target state typically adopts Annex 11 technical controls within an FDA-style risk-based assurance approach. That gives you a single control set that satisfies both, rather than a compromise that satisfies neither. Document the rationale, since the ability to explain why a control exists is itself an assurance artifact under the FDA framework.

Prioritize the Long-Lead Gaps

Multi-factor authentication and audit trail configuration are the gaps most likely to require system upgrades or replacement, and they should be assessed first regardless of where they land in a risk ranking, because their remediation lead times are the longest. Inventory which systems can support multi-factor authentication natively, which require upgrade, and which cannot support it at all, since that last category may force replacement decisions with capital and timeline implications leadership has to address early.

Assign Ownership of GxP Cybersecurity

Because both frameworks now expect cybersecurity evidence and the Annex 11 draft treats it as a core requirement, establish explicit ownership of GxP system security spanning the IT and quality functions. Define who is accountable for patching, penetration testing, access control, and incident response for regulated systems, and make sure security incidents affecting GxP systems are handled with awareness of their data integrity and regulatory reporting implications, not just their technical ones.

Address Supplier Contracts Early

Because contract remediation depends on vendor cooperation and runs on timelines outside your control, assess supplier agreements for critical computerized systems against the draft's specified elements early. Engage vendors about their plans to support the new requirements, since many will be addressing them for their broader customer base and may have roadmaps that inform your own sequencing.

Apply Risk-Based Assurance Within the Harmonized Control Set

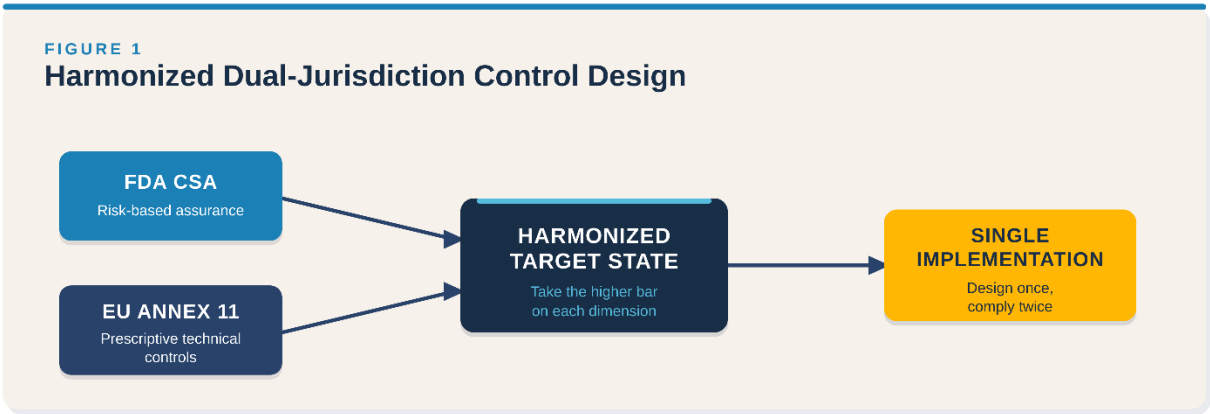
Adopting Annex 11 technical controls does not mean abandoning the efficiency the FDA framework enables. Proportion assurance effort to intended use and risk of failure, with scripted testing where risk justifies it and lighter methods elsewhere, and document the basis for confidence. The harmonized approach is Annex 11 controls implemented with CSA assurance discipline, which is both more compliant and less expensive than exhaustive validation of Annex 11 controls.

Decide the AI Position Deliberately

Given the divergence between the FDA's risk-based accommodation and the draft Annex 22 restriction, make an explicit decision about artificial intelligence in GMP-critical applications across your global operations, rather than letting deployment proceed under the more permissive framework and discovering the conflict later. Tracking the final Annex 22 text is essential, since the draft position, if retained, constrains AI strategy for any organization inspected in Europe.

Implementation Roadmap

The roadmap below builds a harmonized control set and sequences remediation so you are not rebuilding systems per regulator.



Step 1: Inventory and Assess

Inventory the computerized systems used in production and the quality system, and assess each against both frameworks rather than against one. The assessment should identify where current controls fall short of either expectation and, critically, which gaps require technical remediation with long lead times.

Step 2: Perform a Dual-Framework Gap Assessment

Map current controls against the FDA guidance and against the seventeen sections of the Annex 11 draft, identifying the higher bar on each dimension. Pay particular attention to multi-factor authentication, audit trail scope and review, security controls, and supplier contract elements, since these are where the draft most exceeds common current practice.

Step 3: Design the Harmonized Target State

Define a single control set that satisfies both frameworks, taking the more demanding expectation on each dimension and documenting the rationale. Establish how risk-based assurance will be applied within that control set, so the organization gets the FDA framework's efficiency while meeting the European draft's technical expectations.

Step 4: Sequence by Lead Time and Risk

Sequence remediation so that long-lead technical gaps begin first, even where a pure risk ranking would place them later. Systems requiring upgrade or replacement to support multi-factor authentication or expanded audit trails should be identified and funded early, since no amount of later effort compresses procurement and qualification timelines.

Step 5: Engage Suppliers

Assess supplier agreements against the draft's specified contract elements and engage vendors about their support plans. Prioritize agreements for systems whose failure would most affect product quality, and begin renegotiation early given the timelines involved.

Step 6: Establish GxP Cybersecurity Ownership

Define accountability for GxP system security across the IT and quality functions, covering patching, testing, access management, and incident response, and make sure incident response accounts for data integrity and regulatory obligations alongside technical remediation.

Step 7: Implement and Assure

Implement the harmonized control set, applying risk-based assurance proportionate to intended use and risk of failure, and documenting the basis for confidence. Implementing once against a dual-framework design is the point where the approach pays for itself.

Step 8: Govern Across Authorities and Track Final Texts

Establish governance that maintains the harmonized control set as both frameworks evolve, and track the final Annex 11 and Annex 22 texts expected in mid-2026. Where the final text differs from the draft, update the harmonized design deliberately rather than through a fresh remediation cycle.

Technology Considerations

The technical implications of the harmonized approach fall mainly on identity management, audit trail capability, security infrastructure, and cloud arrangements.

Identity and access management is where the technical consequences are greatest. The Annex 11 draft's expectation of multi-factor authentication for electronic signatures, with eIDAS-aligned trust services and time zone-aware timestamping, requires infrastructure many GxP environments lack. Assess whether enterprise identity platforms can extend to regulated systems, since a central capability generally beats system-by-system solutions, and identify systems that cannot support the requirement at all, because those present decisions rather than projects.

Audit trail capability is the second technical constraint. Capturing data creation events, ensuring immutability, and supporting periodic review require configuration some systems provide and others do not. Automated audit trail review tooling can make the periodic review obligation tractable at scale by surfacing the events that warrant human attention, which addresses the resource intensity that otherwise makes the expectation hard to meet consistently.

Cloud and software as a service arrangements sit at the intersection of both frameworks. The FDA guidance adopts recognized cloud definitions and addresses vendor oversight, while the Annex 11 draft specifies supplier contract elements and addresses qualification of cloud services. Shared-responsibility models have to be understood, documented, and reflected in agreements, with clarity about which party controls which controls. Evaluate cloud vendor contracts against data sovereignty, audit rights, service levels, and exit provisions, since the European draft's attention to supplier management makes these terms a compliance matter rather than solely a commercial one.

Future Outlook

The immediate horizon is the publication of the final Annex 11, Annex 22, and Chapter 4 texts, expected in mid-2026. Expect the direction established in the drafts to hold, since consultation refines rather than reverses packages like this, though specific provisions may shift. The prudent posture is to design against the draft while tracking the final text, rather than waiting for a certainty that will arrive too late to act on comfortably.

The longer trend is convergence. The Annex 11 draft explicitly aligns with PIC/S, GAMP 5, ICH Q9, ICH Q10, 21 CFR Part 11, and ISO 27001, and the FDA guidance aligns with the QMSR and ISO 13485. PIC/S participation in the Annex 11 revision means its expectations will propagate to member authorities beyond the European Union, extending the harmonized control set's value across additional jurisdictions. Design a coherent global control set and you are building toward where the frameworks are heading rather than where any single one currently sits.

Artificial intelligence is the exception to the convergence story, and the divergence between the American risk-based accommodation and the draft European restriction of GMP-critical applications to static, deterministic models is the most consequential open question. If that position holds in the final Annex 22, organizations operating globally will need a deliberate AI strategy that accounts for it, rather than assuming that satisfying one regulator satisfies both. This is the area dual-jurisdiction organizations should watch most closely.

How cGMP Consulting Can Help

Designing a computerized systems control set that satisfies both the FDA and European frameworks takes detailed knowledge of each and the judgment to see where they diverge and which expectation governs. cGMP Consulting helps dual-jurisdiction organizations design once and comply twice.

Our consultants perform dual-framework gap assessments, mapping current controls against the Computer Software Assurance guidance and against the Annex 11 draft's seventeen sections to identify the higher bar on each dimension. We help you design a harmonized target state, sequence remediation so that long-lead technical gaps including multi-factor authentication and audit trail configuration begin early, and apply risk-based assurance within that control set so compliance does not come at the cost of efficiency. We support supplier contract assessment against the draft's specified elements, help establish GxP cybersecurity ownership across the IT and quality functions, and advise on artificial intelligence deployment strategy given the divergence between the American and European positions.

Our approach is consultative and grounded in how computerized systems are examined by both authorities. We aim to leave you with a single coherent control set that absorbs both frameworks and adapts as the final texts arrive.

Conclusion

Two computerized systems frameworks are modernizing on different timelines, and the organizations inspected by both face a choice that decides what the change costs them. Treat the FDA guidance and the Annex 11 revision as sequential projects and you get duplicated remediation, conflicting controls, and rework, in an area where the most consequential gaps have the longest lead times.

The alternative is straightforward in principle. Assess against both frameworks, identify the more demanding expectation on each dimension, design a single harmonized control set, and implement once with risk-based assurance discipline. Because the Annex 11 draft is generally more prescriptive on technical controls while the FDA guidance is more explicit about proportioning effort, the harmonized state is typically Annex 11 controls implemented with CSA assurance thinking.

The timing favors deliberate action now. The Annex 11 draft has been public since July 2025 and its direction is clear; the final text is expected mid-2026. The gaps that take longest to close, multi-factor authentication, audit trail scope, and supplier contract terms, are exactly the ones you cannot close quickly once the expectation is live. Design once and you absorb both changes at a fraction of the cost paid by organizations that respond to each regulator in turn, and you will be better positioned as PIC/S propagates these expectations further.

> *If your organization is subject to inspection by both FDA and EU or PIC/S authorities and is planning its computerized systems strategy, the experienced consultants at cGMP Consulting can help assess your current state against both frameworks, identify gaps, and develop a harmonized approach tailored to your business objectives. To start a confidential conversation, complete the Contact Us form at* cgmpconsulting.com/contact-us*.*

References

European Commission. (2011). EudraLex Volume 4: EU guidelines for good manufacturing practice for medicinal products for human and veterinary use, Annex 11: Computerised systems. European Commission.

European Commission. (2022). Concept paper on the revision of Annex 11 of the guidelines on good manufacturing practice for medicinal products — Computerised systems. European Commission.

European Commission. (2025). EudraLex Volume 4: Annex 11 Computerised systems (Draft revision, published 7 July 2025). European Commission.

European Commission. (2025). EudraLex Volume 4: Annex 22 Artificial intelligence (Draft, published 7 July 2025). European Commission.

European Commission. (2025). EudraLex Volume 4: Chapter 4 Documentation (Draft revision, published 7 July 2025). European Commission.

International Council for Harmonisation. (2015). Q10 Pharmaceutical quality system. ICH.

International Council for Harmonisation. (2023). Q9(R1) Quality risk management. ICH.

International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO.

International Society for Pharmaceutical Engineering. (2022). GAMP 5: A risk-based approach to compliant GxP computerized systems (2nd ed.). ISPE.

International Society for Pharmaceutical Engineering. (2025). GAMP guide: Artificial intelligence. ISPE.

Pharmaceutical Inspection Co-operation Scheme. (2021). Good practices for data management and integrity in regulated GMP/GDP environments (PI 041-1). PIC/S.

U.S. Food and Drug Administration. (2025). Computer software assurance for production and quality system software: Guidance for industry and FDA staff (Finalized September 24, 2025). U.S. Department of Health and Human Services.

U.S. Food and Drug Administration. (2026). Computer software assurance for production and quality system software: Guidance for industry and FDA staff (Updated February 3, 2026). U.S. Department of Health and Human Services.

U.S. Food and Drug Administration. (2018). Data integrity and compliance with drug CGMP: Questions and answers; Guidance for industry. U.S. Department of Health and Human Services.

U.S. Government Publishing Office. (n.d.). Title 21 Code of Federal Regulations Part 11: Electronic records; Electronic signatures. Electronic Code of Federal Regulations.

European Parliament and Council. (2014). Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation). Official Journal of the European Union.