Vol-4 Issue-1 2026
Scientific Research Journal of Science, Engineering and Technology
ISSN: 2584-0584, Peer Reviewed Journal

Integrating Computer Software Assurance into Existing Computer System Validation Programs: A Practical Risk-Based Framework

Birju Patel[1*] and **Jaymin Patel**[2]

[1] Manager, Validation Engineering, Anika Therapeutics (ORCID: 0009-0009-4015-7217)

[2] Sr. Manager, Analytical R&D, Amneal Pharmaceuticals (ORCID: 0009-0007-0914-9812)

*** Correspondence:** Birju Patel, Email: birju9586@gmail.com

Abstract

Background: The U.S. Food and Drug Administration (FDA) finalized its Computer Software Assurance (CSA) guidance in September 2025, signaling a paradigm shift from documentation-centric Computer System Validation (CSV) approaches toward risk-based, critical thinking-driven practices for production and quality system software in regulated life sciences industries. While the CSA framework offers significant benefits, including resource optimization and faster implementation cycles, many organizations struggle with practical integration into established CSV programs.

Methods: This article employs a structured analytical framework combining regulatory document analysis, industry literature review, and synthesis of implementation experience in pharmaceutical and medical device manufacturing environments. The integration methodology was developed by mapping CSA principles against established CSV lifecycle activities and identifying specific modification points within existing validation workflows.

Results: A phased integration strategy was developed, encompassing assessment, planning, and implementation stages. Key integration points include modifications to Computer System Risk Assessment (CSRA) procedures incorporating intended use analysis, requirement-level risk evaluations aligned with the CSA risk framework differentiating Critical Attributes from Business or Engineering Attributes, and differentiated testing strategies proportionate to risk. The framework demonstrates potential for substantial reduction in total validation effort for low and medium-risk systems while maintaining or enhancing rigor for high-risk functionality.

Conclusion: CSA implementation represents an evolution rather than a revolution of CSV practices. The integration framework presented enables organizations to adopt CSA principles systematically while maintaining regulatory compliance, achieving improved resource allocation, enhanced focus on critical functionality, and better alignment with modern software development methodologies. Successful implementation requires investment in critical thinking capability, structured change management, and robust documentation of risk-based rationale.

Keywords: Computer Software Assurance, Computer System Validation, Risk-Based Validation, GAMP 5, FDA Guidance, Quality System Software, Medical Device Manufacturing, Pharmaceutical Quality Systems, Critical Thinking, Intended Use

1 Introduction

1.1 Evolution of Computer System Validation

Computer System Validation (CSV) has been a cornerstone of quality assurance in pharmaceutical and medical device manufacturing for over three decades. The regulatory landscape governing computerized systems evolved significantly following the implementation of 21 CFR Part 11 in 1997, which established requirements for electronic records and electronic signatures [1]. Traditional CSV approaches, largely developed in the late 1990s and early 2000s, emphasized comprehensive documentation, extensive testing protocols, and rigorous verification activities to demonstrate that systems perform as intended and maintain data integrity throughout their lifecycle.

The International Society for Pharmaceutical Engineering (ISPE) Good Automated Manufacturing Practice (GAMP) guidelines have served as the primary industry framework for CSV since the early 1990s. The first edition of GAMP 5, published in 2008, introduced a risk-based approach to compliant GxP computerized systems, marking a significant advancement in validation philosophy [2]. Despite these improvements, many organizations implemented CSV programs that remained documentation-intensive, resource-heavy, and struggled to keep pace with rapid technological advancement [3]. Industry forecasts published in 2021 projected that revenue from cloud services in the medical devices sector would rise from approximately USD 2 billion in 2021 to USD 4.4 billion by 2024, reflecting a compound annual growth rate of roughly 17 percent and underscoring how rapidly digital infrastructure is being adopted in regulated environments where traditional validation approaches were not designed to accommodate such pace [4].

1.2 Challenges with Traditional CSV Approaches

Traditional CSV methodologies, while effective at ensuring compliance, have presented several persistent challenges for regulated manufacturers. The primary concerns include disproportionate resource allocation, with validation activities consuming significant time and budget that could otherwise support innovation and quality improvement initiatives. Industry observation has suggested that under conventional CSV practice, the bulk of effort tends to concentrate on documentation production and protocol execution, leaving comparatively little capacity for the assurance reasoning that the activities are intended to demonstrate [5]. This imbalance has led to widespread industry recognition that traditional approaches prioritize documentation volume over meaningful assurance of software fitness for use [6].

Additional challenges include difficulty validating cloud-based Software-as-a-Service (SaaS) applications, accumulation of technical debt from deferred system upgrades due to validation burden, and misalignment between traditional waterfall-based validation approaches and modern Agile software development methodologies [7]. Furthermore, the one-size-fits-all approach often applied to CSV results in excessive testing and documentation for low-risk systems while potentially under-emphasizing critical functionality assessment for high-risk applications [8]. Survey data reported by Wakeham, Vuolo-Schuessler, and Wyn from a March 2024 GAMP South Asia webinar with 71 respondents showed that only about 14 percent of attendees reported a strong understanding of CSA, 31 percent had no prior exposure to it, and the remaining 55 percent were uncertain about how CSA differs from CSV, indicating a substantial educational gap in the practitioner community [9].

1.3 The FDA Computer Software Assurance Initiative

On September 13, 2022, the FDA Center for Devices and Radiological Health (CDRH) and the Center for Biologics Evaluation and Research (CBER) issued a draft guidance titled “Computer Software Assurance for Production and Quality System Software” [10]. After an extensive three-year comment period incorporating stakeholder feedback, the FDA finalized this guidance on September 24, 2025, with an updated version issued on February 3, 2026 [11]. This guidance represents the FDA’s effort to modernize expectations for software validation while maintaining the fundamental requirement that computerized systems used in production or quality systems must be validated. The finalized CSA guidance supplements the FDA guidance “General Principles of Software Validation” issued in January 2002 [12], while superseding Section 6 of that earlier guidance document, which had addressed validation of automated process equipment and quality system software.

Computer Software Assurance is defined as a risk-based approach to establishing confidence that software is fit for its intended use [11]. The guidance emphasizes several key principles that differentiate CSA from traditional CSV practices. First, intended use determination serves as the foundation for risk assessment, focusing on how the software is actually used rather than its inherent capabilities. Second, critical thinking by knowledgeable subject matter experts should drive validation activities rather than rigid adherence to prescriptive procedures. Third, appropriate assurance activities should be proportionate to risk, with higher-risk functions receiving more rigorous testing and documentation. Fourth, organizations should leverage supplier documentation and testing evidence where appropriate, rather than duplicating effort [11].

An important concurrent regulatory development is that on February 2, 2024, the FDA issued a final rule amending 21 CFR Part 820 (the device Quality System Regulation) to align more closely with the international consensus

standard ISO 13485:2016, with the final rule taking effect on February 2, 2026 [13]. This harmonization further supports the risk-based computer software assurance approach and promotes international alignment. The FDA has indicated that the CSA guidance will be updated to ensure consistency with this new regulatory framework once it takes effect.

1.4 Alignment with GAMP 5 Second Edition

The July 2022 publication of ISPE GAMP 5 Second Edition provided complementary industry guidance that aligns closely with FDA's CSA principles [14]. The updated GAMP framework emphasizes critical thinking throughout the system lifecycle, supports both linear and iterative (Agile) development methodologies, and encourages leveraging supplier documentation and quality management systems. Key updates include expanded appendices addressing artificial intelligence and machine learning, cloud computing, and importantly, computer software assurance approaches [15].

GAMP 5 Second Edition maintains the established software categorization system (Categories 1, 3, 4, and 5) while clarifying how these categories inform risk-based validation strategies. The guidance explicitly states that validation activities should be scaled according to complexity, novelty, and criticality rather than applying uniform approaches across all system types [14]. The convergence of the FDA CSA guidance with GAMP 5 Second Edition creates a coherent regulatory and industry framework that supports modernized validation approaches.

1.5 Objectives and Scope

This article presents a practical framework for integrating CSA principles into established CSV programs, specifically targeting validation professionals, quality assurance personnel, and engineering managers in pharmaceutical and medical device manufacturing organizations. The integration approach described herein maintains compliance with existing regulatory requirements while realizing the efficiency and quality benefits offered by the CSA framework. The article is organized as follows: Section 2 describes the analytical methodology used to develop the integration framework; Section 3 presents the core findings including the CSA risk framework, a phased integration strategy with specific modifications to risk assessment and testing methodologies, practical implementation considerations, benefits, challenges, and recommendations; and Section 4 provides concluding observations.

2 Methodology

The integration framework presented in this article was developed through a structured analytical approach combining three complementary methods. First, comprehensive regulatory document analysis was conducted encompassing the FDA CSA final guidance [11], 21 CFR Part 11 [1], 21 CFR Part 820 [13], the FDA General Principles of Software Validation [12], and relevant European regulatory documents including EU Annex 11 [16]. Second, an industry literature review was performed covering ISPE GAMP 5 Second Edition [14], the ISPE GAMP Good Practice Guide on Enabling Innovation [8], peer-reviewed articles on CSA and critical thinking by Margolis and Gallagher [5] and by Wakeham and colleagues [9], published case studies and implementation reports from pharmaceutical and medical device organizations, and additional peer-reviewed articles addressing CSV modernization and risk-based validation approaches [7]. Third, the authors synthesized direct implementation experience from pharmaceutical and medical device manufacturing environments where CSA principles were applied to existing CSV programs.

The integration methodology was developed by mapping CSA principles against established CSV lifecycle activities and identifying specific modification points within existing validation workflows. Current-state assessment criteria were developed based on industry best practices, and gap analysis frameworks were constructed to enable systematic comparison of existing CSV practices against CSA expectations. The resulting phased integration strategy was refined through iterative application and review.

Risk assessment methodologies were evaluated by comparing the function-level CSA risk framework against traditional system-level approaches. Testing strategy alternatives, including unscripted exploratory testing, error guessing, and hybrid scripted/unscripted methods, were assessed against conventional protocol-driven approaches. Documentation optimization opportunities were identified by analyzing representative validation packages from multiple system types spanning GAMP Categories 1, 3, 4, and 5.

3 Results and Discussion

3.1 Core Principles of Computer Software Assurance

Analysis of the FDA CSA guidance reveals four core principles that distinguish it from traditional validation approaches while maintaining regulatory compliance objectives. Understanding these principles is essential for successful integration into existing CSV frameworks.

The first principle establishes intended use as the foundation for all assurance activities. CSA requires explicit determination of how software will actually be used in the production or quality system environment. This intended use directly drives risk assessment and validation activities. Unlike approaches that categorize entire systems uniformly, CSA recognizes that different functions within the same software may have vastly different risk profiles based on their specific application [11]. For example, a Laboratory Information Management System (LIMS) may contain both high-risk functions, such as raw data capture and calculations affecting product release decisions, and low-risk functions, such as report formatting or user preference settings.

The second principle emphasizes critical thinking and scientific judgment. The CSA guidance explicitly calls for critical thinking by knowledgeable and experienced personnel rather than rigid adherence to templates and checklists [11]. Margolis and Gallagher trace the formal use of this term in computerized systems guidance to ISPE's GAMP publications, where it appeared first in the GAMP Good Practice Guide on Enabling Innovation and was carried forward and elaborated in GAMP 5 Second Edition; in their account, the central purpose of critical thinking is to direct attention toward the validation considerations that conventional CSV practice tended to leave unexamined [5]. Applied in practice, this means that subject matter experts evaluate factors such as supplier quality management systems, software development practices, implementation complexity, and credible failure modes in order to determine which assurance activities are proportionate to the actual risk of the function under review [17].

The third principle mandates risk-based assurance activities proportionate to the potential consequences of software failure. High-risk functions warrant comprehensive testing with detailed documentation and full traceability, while low-risk functions may be adequately assured through less formal approaches such as unscripted testing or review of supplier testing evidence [11]. Notably, the final CSA guidance expanded upon the draft by allowing the possibility of using unscripted testing even for high-risk software features, functions, and operations when combined with scripted testing in a hybrid approach, representing a welcome evolution from the draft guidance's more restrictive position [18].

The fourth principle encourages leveraging existing evidence from suppliers. Rather than duplicating testing efforts, CSA supports appropriate reliance on supplier-generated documentation and testing artifacts when suppliers have adequate quality management systems and follow structured software development lifecycle practices [14]. The final guidance further encourages manufacturers to leverage vendor assessments, certifications such as ISO 13485, and digital records including system logs and audit trails to reduce manual documentation burden [11].

3.2 Comparative Analysis: CSA versus CSV

Table 1 presents a comprehensive comparison of traditional CSV and CSA-integrated approaches across key dimensions. It is critical to emphasize that CSA does not replace or eliminate CSV requirements; rather, it clarifies how to apply risk-based validation in a manner that optimizes resources while ensuring compliance.

Table 1: ***Comparison of Traditional CSV and CSA-Integrated Approaches***

Dimension	Traditional CSV	CSA-Integrated Approach
Primary Focus	Documentation completeness and protocol execution	Fitness for intended use and critical functionality
Risk Assessment	Often system-level or category-based	Function-level based on intended use

Dimension	Traditional CSV	CSA-Integrated Approach
Testing Strategy	Uniform, comprehensive testing regardless of risk	Risk-proportionate testing activities; scripted, unscripted, or hybrid
Documentation	Extensive, often duplicative protocols and reports	Appropriate, fit-for-purpose records proportionate to risk
Supplier Evidence	Limited acceptance; extensive internal retesting	Strategic leveraging when supplier QMS is adequate
Resource Allocation	Documentation and testing dominate effort; limited capacity for critical thinking [5]	Critical thinking and risk-based judgment lead; documentation is fit-for-purpose [5]
Change Management	Often triggers full revalidation	Risk-based assessment determines extent of revalidation
Development Alignment	Waterfall and stage-gate methodology	Supports Agile, iterative, and hybrid approaches
Regulatory Basis	21 CFR Part 820.70(i), Part 11, EU Annex 11	Same regulations; refined, risk-based interpretation
Quality Focus	Compliance demonstration	Patient safety and product quality assurance

The fundamental difference lies not in what must be validated, but rather in how validation is approached and documented. Both methodologies must satisfy the same regulatory requirements for establishing that computerized systems are fit for their intended use and maintain a validated state throughout their lifecycle. As the FDA states in the final guidance, "applying a risk-based approach to computer software used as part of production or the quality system would better focus manufacturers' assurance activities to help ensure product quality while helping to fulfill validation requirements" [11].

3.3 CSA Risk Framework and Categorization

The CSA guidance establishes a structured risk framework based on assessing potential consequences of software failure. The final guidance refined the risk terminology from the draft, categorizing software features, functions, or operations as posing either "high process risk" or "not high process risk" depending on whether failure could foreseeably compromise patient safety or result in a quality problem [11].

Per the FDA guidance, a software feature, function, or operation is considered high process risk when its failure to perform as intended "may result in a quality problem that could foreseeably compromise patient safety" [11]. In practical terms this category captures functions that control critical process parameters, perform calculations affecting product release decisions, or maintain electronic batch records. For high process risk items, the guidance recommends more rigorous assurance activities, including the use of scripted testing or a hybrid approach combining scripted and unscripted testing, scaled as appropriate to the function under review [11, 18].

Software features, functions, or operations that are not high process risk include those where failure would have minimal impact on product quality or patient safety, where redundant manual controls would readily detect errors, or where additional oversight mechanisms provide mitigation. For these items, less formal assurance approaches such as unscripted exploratory testing, system walkthroughs, or review of supplier testing evidence may be sufficient [11].

Multiple factors influence risk categorization. These include the severity of the consequence if the function fails, the likelihood that a failure would be detected, the complexity of the function, the novelty of the technology or

implementation, the maturity of the supplier's quality management system, the rigor of the software development lifecycle, the organization's prior history with similar systems, and the availability of alternate controls or independent verification mechanisms. The CSA framework emphasizes that risk should be assessed for specific functions or features in light of their intended use, rather than at an aggregated system level [11]. As a result, a single system may contain functions spanning both risk categories, warranting differentiated validation approaches.

3.4 Relationship to GAMP Software Categories

CSA risk assessment complements rather than replaces GAMP software categorization. GAMP categories provide an initial framework for understanding software type and complexity [14]: Category 1 encompasses infrastructure software such as operating systems and databases; Category 3 covers non-configured products, meaning commercial off-the-shelf software used as delivered; Category 4 addresses configured products, including configurable commercial software; and Category 5 applies to custom applications involving bespoke software development.

GAMP categories inform the starting point for the validation approach, particularly regarding emphasis on supplier assessment and documentation. CSA risk assessment then provides function-level granularity to determine specific testing and documentation requirements. For example, a Category 4 configured LIMS would undergo GAMP-informed supplier assessment, followed by function-level CSA risk assessment to differentiate validation activities for high process risk analytical calculations versus not high process risk report generation features.

3.5 Integration Strategy: A Phased Approach

3.5.1 Assessment Phase

Successful CSA integration begins with comprehensive assessment of the current validation program maturity and organizational readiness. This assessment phase typically requires four to eight weeks depending on organizational size and complexity. Organizations should conduct structured evaluations of existing CSV procedures, practices, and performance metrics. Key assessment areas include analysis of representative validation packages to identify documentation burden, redundancy, and value-added versus compliance-driven activities; quantification of effort distribution between risk assessment, testing, documentation, and review activities; measurement of time required for system implementation from concept through production release; categorization of existing validated systems by GAMP category, risk level, and validation approach applied; review of standard operating procedures for alignment with or barriers to CSA principles; and gathering perspectives from validation personnel, system owners, quality assurance staff, and end users regarding validation program effectiveness.

Gap analysis should compare current practices against CSA principles to identify specific opportunities for improvement. Critical comparison areas include risk assessment methodology (system-level versus function-level), testing strategy flexibility (uniform protocols versus risk-based approaches), supplier documentation leverage (extent of current utilization), critical thinking emphasis (documented rationale for validation decisions), and documentation practices (evidence of appropriate fit-for-purpose approaches). Organizations should also assess regulatory inspection history, inspector feedback regarding validation practices, and jurisdictional differences among regulatory authorities.

3.5.2 Planning Phase

Following assessment, the planning phase establishes the roadmap for CSA integration, typically spanning two to three months. Successful CSA integration requires engagement and participation from multiple organizational functions, including executive leadership to secure sponsorship and resource commitment, quality assurance to ensure alignment with quality system philosophy, validation and engineering teams to develop the technical implementation approach, IT and automation groups to address system and infrastructure considerations, regulatory affairs to confirm regulatory strategy and positioning, and system owners to engage end users in the risk assessment process.

Comprehensive training is essential to build organizational capability for critical thinking and risk-based decision making. Training should address CSA principles and FDA guidance interpretation, risk assessment methodologies and practical application, testing strategy selection based on risk, appropriate documentation practices, supplier assessment and evidence evaluation, and change management and continuous improvement. Quality system documents requiring revision include the Computer System Validation procedure, risk assessment procedure,

requirements management process, test strategy and execution guidance, supplier assessment procedures, change control process, and associated templates and forms.

Organizations should select two to three pilot systems representing different GAMP categories and risk profiles for initial CSA implementation. Pilot selection criteria should prioritize new system implementations to avoid revalidation burden, engaged system owners willing to participate, a range of risk levels to test different approaches, and manageable scope for learning and iteration.

3.5.3 Implementation Phase: Enhanced Risk Assessment

The implementation phase introduces specific modifications to existing validation practices, beginning with risk assessment methodology enhancements.

Integration Point 1: Enhanced Computer System Risk Assessment (CSRA). The Computer System Risk Assessment serves as the foundational activity for any GxP computerized system, determining overall validation strategy and resource allocation. CSA integration enhances CSRA by incorporating intended use analysis and the CSA risk framework while maintaining existing assessment elements. The enhanced CSRA contains six components: (1) GxP Applicability Determination, which remains unchanged from traditional CSV practice; (2) GAMP Categorization, which provides initial understanding of system complexity and supplier involvement; (3) Intended Use Analysis, a critical new CSA element that explicitly documents primary business processes supported, specific functions to be utilized, how the system fits within the overall process flow, key decisions driven by system output, interfaces with other systems, and user roles and responsibilities; (4) 21 CFR Part 11 Applicability assessment for electronic records and signatures [1]; (5) Overall System Risk Rating incorporating CSA risk factors; and (6) Validation Approach Determination documenting the high-level strategy including supplier assessment extent, testing framework, documentation deliverables, resource requirements, and quality assurance involvement level.

Figure 1 illustrates the integrated CSRA process flow incorporating both traditional CSV and new CSA elements.

Figure 1: Integrated Computer System Risk Assessment (CSRA) Process Flow

Integration Point 2: Requirement Risk Assessment Enhancement. Following system-level CSRA, requirement-level risk assessment provides function-specific risk determination that directly drives testing strategy. This assessment occurs during the specification phase once user requirements are defined. The requirement risk assessment process involves five steps. In Step 1, User Requirements Specifications (URS) or combined URS/Functional Requirements Specifications document system capabilities needed to support the intended use. In Step 2, each requirement is categorized as either a Critical Attribute (CA) or a Business or Engineering Attribute (BEA). Critical Attributes are requirements that directly impact product quality, patient safety, or data integrity, where failure could result in product non-conformance, patient harm, data integrity compromise, or inability to detect process failures. Business or Engineering Attributes are requirements that support business processes or system functionality but do not directly impact product quality or patient safety, including system performance features, user interface preferences, reporting functions, administrative capabilities, and backup and recovery. In Step 3, for requirements categorized as Critical Attributes, a risk level is assigned based on CSA risk framework criteria. In Step 4, risk level directly determines the appropriate testing approach. In Step 5, a Requirements Traceability Matrix maps each requirement to its risk categorization and testing approach, providing transparent documentation of the risk-based validation strategy.

Table 2: ***Testing Approach Matrix by Risk Level***

Risk Level	Testing Approach	Documentation Requirements
High Risk (CA)	Scripted test protocols or hybrid scripted/unscripted; formal review and approval	Detailed test protocols; comprehensive test results; deviation investigation; full test summary report
Medium Risk (CA)	Focused scripted or unscripted testing of key scenarios	Test plan or approach description; test results documentation; summary of testing performed
Low Risk (CA)	Unscripted exploratory testing; system walkthrough	Summary of testing approach; pass/fail documentation
BEA	Unscripted testing during training; user feedback during use; observation during go-live	Minimal formal documentation; may leverage training records; user feedback capture

3.5.4 Implementation Phase: Testing Strategy Evolution

CSA integration fundamentally changes testing strategies by introducing flexibility and risk-proportionate approaches while maintaining assurance of fitness for intended use.

Unscripted or exploratory testing involves structured evaluation of system functionality without predefined step-by-step protocols. This approach is appropriate for low-risk functions, business attributes, or functions with straightforward expected behavior. Unscripted testing focuses on user scenarios and real-world workflows, exercises system functionality through normal use, identifies usability issues and unexpected behaviors, captures pass/fail outcomes without detailed procedure documentation, and may be combined with user training activities. Documentation for unscripted testing should include the testing objective, general approach, systems and functions evaluated, tester identification, date performed, and overall result with any issues noted.

Error guessing and experience-based testing allows subject matter experts to apply knowledge of common failure modes, system behavior, and process risks to design targeted test scenarios. This technique is particularly valuable for medium-risk functions where comprehensive scenario coverage would be impractical. Testers deliberately attempt to create problematic scenarios based on experience and critical thinking [11].

When suppliers maintain adequate quality management systems and follow structured software development practices, organizations should evaluate supplier-generated testing evidence rather than duplicating effort. Acceptable supplier evidence may include software design specifications and verification records, unit and integration test results, system and user acceptance testing documentation, regression testing evidence for updates and patches, and validation certificates or attestations. Supplier evidence evaluation should consider the supplier's QMS certification (such as ISO 9001 or ISO 13485), software development lifecycle maturity, independence of testing from development, applicability to the organization's intended use, and currency and version alignment. Organizations should document their evaluation and determination that supplier evidence is adequate for the intended risk level [11, 14].

The CSA guidance also clarifies the distinction between repeatability testing (same user, same system, same conditions) and reproducibility testing (different users, systems, or conditions) [11]. High process risk functions may warrant reproducibility testing to ensure consistent performance across the intended use environment, while not high process risk functions may need only single-execution confirmation.

3.5.5 Implementation Phase: Documentation Optimization

CSA integration enables streamlined documentation practices aligned with risk-based principles while maintaining regulatory compliance. Rather than generating separate documents for each validation lifecycle phase, organizations may combine deliverables when appropriate to reduce redundancy and improve efficiency. Examples include combined URS and Functional Requirements Specifications, integrated Installation, Operational, and Performance

Qualification protocols, combined Validation Plan and Summary Report for low-risk systems, and single risk assessment documents incorporating system and requirement-level evaluation. The decision to combine documents should be documented in the Validation Plan with rationale.

The final CSA guidance encourages manufacturers to leverage digital records such as system logs and audit trails to reduce manual documentation burden, as opposed to paper documentation, screenshots, or duplicating results already digitally retained by the software [11]. Modern validation management systems and requirements management tools enable dynamic documentation approaches that maintain traceability while reducing paper-based processes. Electronic approaches may include requirements databases with integrated test case management, automated traceability matrices, electronic test execution with direct system evidence capture, digital approval workflows, and version control and configuration management integration. Electronic documentation should comply with 21 CFR Part 11 requirements where applicable [1]. The guiding principle is that documentation should be sufficient to reconstruct what was done, by whom, when, and with what result, but need not be excessive [11].

3.6 Supplier Assessment Integration

Enhanced supplier assessment practices enable appropriate leverage of supplier documentation and reduce duplicative testing effort. Comprehensive supplier evaluation should address four key domains. Quality Management System assessment should evaluate ISO 9001 or equivalent certification, quality procedures and organizational structure, management review and continuous improvement processes, document control and record keeping, and corrective and preventive action systems. Software Development Lifecycle assessment should evaluate development methodology (Waterfall, Agile, or hybrid), requirements management practices, design review and approval processes, code review and version control, testing approach and independence, and release and change management procedures. GxP Experience and Compliance assessment should evaluate experience with regulated industries, understanding of GxP requirements, previous regulatory inspections or observations, and training and competency programs. Documentation and Support assessment should evaluate availability of design and test documentation, user documentation completeness, technical support responsiveness, update and patch management process, and validation support services [11, 14].

Organizations may apply a streamlined supplier assessment for established, reputable suppliers with proven track records in regulated industries, provided the rationale is documented. The final CSA guidance explicitly encourages leveraging vendor assessments and certifications such as ISO 13485 as part of the overall assurance strategy [11].

3.7 Practical Implementation Considerations

3.7.1 Organizational Change Management

CSA implementation represents significant cultural and operational change requiring structured change management. All personnel involved in validation activities require training on CSA principles and application, and training effectiveness should be demonstrated through practical exercises, pilot project participation, and competency assessments. Clear, consistent communication prevents misunderstanding and builds confidence in the CSA approach.

Organizations may encounter resistance from personnel accustomed to traditional CSV approaches. Common concerns include questions about whether the approach will pass inspection, which should be addressed by referencing the FDA guidance, GAMP 5 alignment, and documented rationale approach; uncertainty about when documentation is sufficient, which can be resolved by providing clear criteria and examples tied to risk levels; recognition that CSA requires more judgment and responsibility, which should be acknowledged with emphasis on training and support availability; and attachment to established methods, which can be addressed by explaining industry evolution and regulatory modernization context.

3.7.2 Quality System Updates

CSA integration requires systematic updates to quality system documentation. Key procedures requiring update include the Computer System Validation SOP to incorporate CSA principles, risk framework, and flexible testing approaches; the Risk Assessment SOP to add function-level assessment methodology and CSA risk criteria; the Requirements Management SOP to include requirement categorization (CA versus BEA) process; the Test Strategy

and Execution SOP to document unscripted testing, supplier evidence use, and risk-based approaches; the Supplier Assessment SOP to enhance criteria for QMS and software development lifecycle evaluation; and the Change Control SOP to align change assessment with the CSA risk framework.

Updated templates and forms should reflect CSA integration, including enhanced Computer System Risk Assessment templates with intended use and CSA risk factors, Requirement Risk Assessment templates with CA/BEA categorization and testing strategy determination, streamlined validation planning templates with document combining options, unscripted test documentation templates, supplier assessment questionnaires aligned with CSA emphasis areas, and Requirements Traceability Matrix templates with risk-based approach columns. Approval requirements may also be modified based on risk, with high-risk systems maintaining robust multi-level approvals, medium-risk systems having streamlined approval with key stakeholders, and low-risk systems requiring minimal approval requirements.

3.7.3 Regulatory and Inspection Readiness

Preparation for regulatory inspection is essential to successfully demonstrate the validity of CSA implementation. The single most important element for inspection readiness is clear documentation of the rationale for risk-based decisions. For each system, validation packages should include intended use documentation explaining how the system is used in production or quality processes, risk assessment results with clear articulation of risk factors considered, testing strategy justification linked to risk assessment, supplier assessment results and determination regarding evidence acceptance, and approval of the risk-based approach by appropriate stakeholders.

Inspectors may be unfamiliar with CSA concepts or may question departures from traditional CSV. Organizations should proactively explain the CSA approach during opening meetings, provide FDA guidance and GAMP 5 references, walk through representative examples showing risk-based logic, demonstrate that critical functionality receives appropriate rigor, and show that the approach represents resource reallocation rather than reduction in assurance. Internal mock inspections following CSA implementation help identify documentation gaps or unclear rationale before regulatory scrutiny [3, 11].

3.8 Benefits Realized Through CSA Integration

Organizations implementing CSA-integrated validation programs report multiple tangible benefits. Resource optimization is among the most significant, with CSA enabling substantial reduction in validation effort for low and medium-risk systems while maintaining or enhancing focus on high-risk functionality. Industry practitioner reports describe meaningful efficiency improvements once CSA principles are operationalized, with several pharmaceutical organizations indicating that validation cycles for low and medium-risk systems can be shortened appreciably, freeing technical staff from documentation overhead and redirecting their effort toward innovation, process improvement, and higher-value assurance activities [19]. The magnitude of these gains varies by system type, baseline validation maturity, and the depth of CSA integration achieved, and quantitative reductions reported in industry literature should therefore be interpreted as illustrative rather than universally guaranteed outcomes.

Faster implementation cycles result from streamlined documentation, leveraged supplier evidence, and risk-appropriate testing. Several practitioner reports describe meaningful compression of release cycles after low-impact features are reclassified under CSA risk principles and testing effort is reallocated accordingly [9]. This agility supports business objectives and enables faster adoption of beneficial technologies. Enhanced critical functionality focus is achieved by eliminating unnecessary testing and documentation for low-risk functions, allowing validation personnel to devote more time and attention to comprehensive evaluation of critical functionality. This improved focus enhances overall product quality assurance and patient safety outcomes.

CSA principles also provide better alignment with modern software development methodologies, as they align naturally with Agile and iterative development approaches, enabling organizations to adopt modern software solutions that would be difficult to validate under traditional approaches. This includes SaaS applications with regular updates, AI and ML-based systems, and cloud-native platforms [14]. Furthermore, traditional CSV often creates backlogs of system updates and improvements due to validation burden. CSA's risk-based change assessment enables more frequent updates, patches, and enhancements, thereby reducing technical debt and improving system security and functionality [5]. Strategic leveraging of supplier documentation and testing also fosters improved supplier

relationships, where suppliers understand regulated customer needs and provide appropriate validation support rather than expecting customers to duplicate effort.

3.9 Common Challenges and Mitigation Strategies

Several challenges commonly arise during CSA integration and require proactive mitigation. Cultural resistance to change manifests when personnel comfortable with traditional CSV approaches resist new methods, citing inspection concerns or uncertainty about sufficiency of assurance. Mitigation strategies include providing comprehensive training emphasizing that CSA maintains compliance while improving efficiency, starting with pilot programs to demonstrate success before broad implementation, documenting inspection outcomes showing regulatory acceptance, and engaging quality champions who can advocate for the approach.

Developing critical thinking skills presents a challenge when personnel accustomed to template-based approaches struggle with risk assessment and judgment-based decision making. Mitigation includes providing practical training with realistic scenarios and case studies, establishing review and approval processes that mentor less experienced personnel, creating decision frameworks and tools that guide critical thinking, and documenting examples of effective risk assessments for reference [5, 17].

Defining documentation adequacy creates uncertainty, with a tendency to default to traditional comprehensive approaches. Organizations should develop clear documentation standards by risk level with examples, establish review checkpoints with experienced personnel, create templates that guide appropriate documentation, and iterate based on internal and external review feedback.

Regulatory inspector acceptance remains a concern, particularly with inspectors who may be unfamiliar with the CSA guidance. Organizations should proactively educate inspectors, provide guidance document references, document risk assessment rationale clearly and comprehensively, demonstrate that critical functionality receives appropriate rigor, and maintain a consistent approach across systems [3, 11].

Supplier assessment variability can create difficulty in obtaining adequate documentation or determining appropriate evidence acceptance criteria. Organizations should develop standardized supplier assessment questionnaires, establish clear acceptance criteria for different supplier types, build supplier assessment databases for reuse, and engage suppliers early in the procurement process. Finally, maintaining consistency across the organization requires clear procedures and decision frameworks, centralized oversight and quality review, regular calibration meetings among validation teams, sharing of examples and lessons learned, and monitoring of metrics for consistency.

3.10 Critical Success Factors and Recommendations

Based on analysis of implementation experience and industry literature, several factors are essential for successful CSA integration. Executive sponsorship providing visible leadership commitment enables necessary resource investment, cultural change, and prioritization. Comprehensive training programs build organizational capability and confidence and should be ongoing rather than one-time. A pilot program approach enables learning, iteration, and demonstration of success before broad deployment, with pilots representing diverse system types and risk levels. Clear documentation of rationale for risk-based decisions is the single most important element for sustainability and regulatory acceptance; organizations must develop discipline to document their reasoning in addition to their actions.

Quality system integration ensures that CSA principles are embedded in procedures, templates, and organizational culture rather than treated as exceptions. A continuous improvement mindset supports iterative refinement of the CSA approach based on experience, feedback, and evolving guidance. Cross-functional collaboration among validation, quality, engineering, IT, and business stakeholders ensures aligned understanding and support for risk-based approaches.

For organizations beginning CSA integration, the following sequence is recommended: conduct thorough current-state assessment before beginning implementation; secure executive sponsorship early; invest sufficiently in comprehensive training; initiate CSA approaches with new system implementations rather than retrofitting existing validated systems; establish organizational discipline for documenting risk-based decisions with clear rationale; utilize GAMP 5 Second Edition, the CSA guidance examples, and industry resources to inform implementation; plan for

multiple cycles of application, review, and refinement; communicate positive outcomes to build organizational confidence; monitor regulatory inspection trends and FDA statements regarding CSA acceptance; and foster a culture of critical thinking and risk-based decision making across the organization [3, 5, 11, 14].

4 Conclusion

Computer Software Assurance represents an evolution, not a revolution, in validation practices for pharmaceutical and medical device manufacturers. The FDA's finalization of the CSA guidance in September 2025, aligned with GAMP 5 Second Edition principles and supported by the ongoing harmonization of 21 CFR Part 820 with ISO 13485:2016, provides regulatory clarity and industry best practices for risk-based validation approaches that maintain patient safety and product quality while optimizing resource allocation and enabling adoption of modern technologies.

Successful CSA integration into existing CSV programs requires structured implementation addressing risk assessment methodology, testing strategy evolution, documentation optimization, and organizational change management. The phased approach presented in this article, encompassing assessment, planning, and implementation with specific enhancements to CSRA and requirement risk assessment processes, provides a practical framework that regulated organizations can adapt to their specific contexts.

Key integration points include enhanced computer system risk assessment incorporating intended use analysis and CSA risk factors, function-level requirement risk assessment driving differentiated testing strategies, appropriate leveraging of supplier documentation and testing evidence, and fit-for-purpose documentation practices. These modifications enable meaningful resource optimization for low and medium-risk systems, with practitioner reports describing improvements that range widely depending on baseline maturity and scope, while maintaining or enhancing focus on critical functionality affecting product quality and patient safety.

Implementation challenges, including cultural resistance, critical thinking skill development, and regulatory acceptance concerns, can be successfully mitigated through comprehensive training, pilot program approaches, clear documentation of rationale, and a continuous improvement mindset. Organizations that invest in building critical thinking capability and embed risk-based principles into quality system culture realize substantial benefits including faster implementation cycles, reduced technical debt, better alignment with modern software development practices, and enhanced regulatory posture.

As the life sciences industry continues evolving toward digital transformation, cloud computing, artificial intelligence and machine learning applications, and real-time manufacturing analytics, CSA principles provide the regulatory framework and practical methodology for validating these advanced technologies efficiently while ensuring product quality and patient safety remain paramount. The concurrent harmonization of the Quality System Regulation with ISO 13485:2016, effective February 2, 2026, further reinforces the global trajectory toward risk-based, outcomes-focused quality assurance approaches. Organizations that successfully integrate CSA into their validation programs position themselves for competitive advantage through accelerated innovation adoption, optimized resource utilization, and enhanced quality focus.

5 Conflict of Interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest. The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official positions of their respective employers.

6 Author Contributions

B.P. and J.P. contributed to the design and implementation of the research, to the analysis of the results and to the writing of the manuscript.

7 Funding

This research received no external funding.

8 Acknowledgments

The authors acknowledge the contributions of validation professionals, quality assurance personnel, and system subject matter experts whose practical experience informed the integration approaches described in this article.

9 Data Availability Statement

No new data were generated or analyzed in this study. All regulatory documents and industry guidance referenced are publicly available through the sources cited in the reference list.

10 References

[1] U.S. Food and Drug Administration. (1997). 21 CFR Part 11 - Electronic records; electronic signatures. Federal Register, 62(54), 13430–13466. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application

[2] International Society for Pharmaceutical Engineering. (2008). GAMP 5: A risk-based approach to compliant GxP computerized systems (1st ed.). ISPE. https://ispe.org/publications/guidance-documents/gamp-5

[3] Davidson, J. (2023). Advancing the transition to computer software assurance: Responding to the FDA draft guidance for production and quality system software. Food and Drug Law Institute Update, May–June, 24–31. https://www.fdli.org/2023/05/advancing-the-transition-to-computer-software-assurance/

[4] Medical Product Outsourcing. (2021, September 8). Medical device global cloud services to generate $4.4B in 2024 (GlobalData report citation). Medical Product Outsourcing. https://www.mpo-mag.com/contents/view_breaking-news/2021-09-08/medical-device-global-cloud-services-to-generate-44b-in-2024/

[5] Margolis, B., & Gallagher, S. (2024). Computer software assurance and the critical thinking approach. Pharmaceutical Engineering, 44(2), 42–49. https://ispe.org/pharmaceutical-engineering/march-april-2024/computer-software-assurance-and-critical-thinking

[6] Kallampunathil, R. (2023, September 20). CSA vs. CSV – FDA's computer software assurance draft guidance explained. MasterControl GxP Lifeline. https://www.mastercontrol.com/gxp-lifeline/csa-vs.-csv-fda-s-computer-software-assurance-draft-guidance-for-production-and-quality-system-software/

[7] Newton, M. E., Dern, M., & McDowall, R. D. (2023). What you need to know about GAMP 5 guide, 2nd edition. Pharmaceutical Engineering, 43(1), 26–35. https://ispe.org/pharmaceutical-engineering/january-february-2023/what-you-need-know-about-gampr-5-guide-2nd-edition

[8] International Society for Pharmaceutical Engineering. (2017). GAMP good practice guide: Enabling innovation. ISPE. https://ispe.org/publications/guidance-documents/gamp-good-practice-guide-enabling-innovation

[9] Wakeham, C., Vuolo-Schuessler, L., & Wyn, S. (2024). Finding the assurance in computer software assurance. Pharmaceutical Engineering, 44(5), September–October. International Society for Pharmaceutical Engineering. https://ispe.org/pharmaceutical-engineering/september-october-2024/finding-assurance-computer-software-assurance

[10] U.S. Food and Drug Administration. (2022, September 13). Computer software assurance for production and quality system software: Draft guidance for industry and Food and Drug Administration staff. FDA. https://www.fda.gov/media/161521/download

[11] U.S. Food and Drug Administration. (2025, September 24). Computer software assurance for production and quality system software: Guidance for industry and Food and Drug Administration staff. Federal Register, 90 FR 2025-18468. https://www.federalregister.gov/documents/2025/09/24/2025-18468/computer-software-assurance-for-production-and-quality-system-software-guidance-for-industry-and

[12] U.S. Food and Drug Administration. (2002). General principles of software validation: Final guidance for industry and FDA staff. FDA. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/general-principles-software-validation

[13] U.S. Food and Drug Administration. (2024, February 2). Quality management system regulation (QMSR): Final rule amending 21 CFR Part 820 to incorporate ISO 13485:2016. Federal Register. https://www.fda.gov/medical-devices/quality-management-system-qmsr

[14] International Society for Pharmaceutical Engineering. (2022). GAMP 5: A risk-based approach to compliant GxP computerized systems (2nd ed.). ISPE. https://ispe.org/publications/guidance-documents/gamp-5-guide-2nd-edition

[15] Wakeham, C., Vuolo-Schuessler, L., & Ferrell, S. (2022, November 24). ISPE GAMP 5 second edition: A risk-based approach to compliant GxP computerized systems. European Pharmaceutical Review. https://www.europeanpharmaceuticalreview.com/article/176422/ispe-gamp-5-second-edition-computerized-system-expectations/

[16] European Commission. (2011). EudraLex Volume 4, Annex 11: Computerised systems. https://health.ec.europa.eu/medicinal-products/eudralex/eudralex-volume-4_en

[17] International Council for Harmonisation. (2005). ICH Q9: Quality risk management. ICH. https://www.ich.org/page/quality-guidelines

[18] Birbal, S. (2026, January 28). Concluding Validation 4.0 with computer software assurance (CSA) and Annex 11 framework. ISPE Pharmaceutical Engineering iSpeak Blog. https://ispe.org/pharmaceutical-engineering/ispeak/concluding-validation-40-computer-software-assurance-csa-and

[19] Sware Technologies. (2025). CSA in the pharmaceutical industry: Should you implement it? https://www.sware.com/blog/csa-pharmaceutical-industry

[20] U.S. Food and Drug Administration. (2003). Guidance for industry: Part 11, electronic records; electronic signatures – Scope and application. FDA. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application