

## “Risk based validation in computer system validation and transition towards computer system Assurance”.

Aparna Pophale, Kailas Ganpati Rathod

*Department of Pharmaceutical Quality Assurance, Mangaldeep institute of Pharmacy, Chhatrapati sambhajinagar*

Date of Submission: 25-01-2026

Date of Acceptance: 05-02-2026

### ABSTRACT

Computerized systems are widely used in the pharmaceutical industry for manufacturing, quality control, laboratory operations, data management, and regulatory compliance. Since these systems directly impact product quality, patient safety, and data integrity, regulatory authorities mandate Computer System Validation (CSV). Traditional CSV approaches are largely documentation-driven and often result in excessive validation activities without proportional risk reduction.

To overcome these limitations, a risk-based validation approach has been introduced, focusing on system criticality and patient safety. Furthermore, regulatory agencies such as the US Food and Drug Administration (FDA) have proposed the concept of Computer System Assurance (CSA), which emphasizes critical thinking, assurance of system performance, and reduced documentation burden.

This review article discusses the principles of risk-based computer system validation, regulatory expectations, the GAMP 5 framework, and the lifecycle approach to CSV. Additionally, it explores the transition from traditional CSV to Computer System Assurance, highlighting its benefits, challenges, and future prospects in the pharmaceutical industry.

Risk management and risk assessment for computerized systems validation is a key regulatory issue following the Food and Drug Administration's (FDA) reassessment of the 21 Code of Federal Regulation (CFR) Part 11 regulations (Electronic Records and Electronic Signatures final rule).

**Keywords:** Computer System Validation, Risk-Based Validation, GAMP 5, Computer System Assurance, Data Integrity, Pharmaceutical Industry, Code of Federal Regulation (CFR), Food and Drug Administration's (FDA)

### I. INTRODUCTION

The pharmaceutical industry increasingly relies on computerized systems for various regulated activities such as production control, quality management, laboratory testing, electronic records, and reporting. These systems play a critical role in ensuring product quality, regulatory compliance, and patient safety. Any failure or malfunction of a computerized system may lead to data integrity issues, product quality defects, or regulatory non-compliance.

To mitigate these risks, regulatory authorities require pharmaceutical companies to implement Computer System Validation (CSV). CSV provides documented evidence that a computerized system consistently performs according to its intended use. However, traditional validation practices often involve extensive documentation and testing, even for low-risk systems, resulting in inefficiencies.

A risk-based approach to validation has been adopted to focus efforts on critical system functions. Recently, the concept of Computer System Assurance (CSA) has emerged as a modern approach that shifts focus from documentation to assurance of system performance. This review evaluates risk-based CSV practices and the transition towards CSA in the pharmaceutical industry

### Computer System Validation (CSV)

Computer System Validation is defined as the process of establishing documented evidence that a computerized system does what it purports to do in a consistent and reproducible manner. The primary objective of CSV is to ensure that systems supporting regulated activities are reliable, secure, and compliant with regulatory requirements. Validation is not a one-time event it's lifecycle-based.

CSV applies to various systems such as manufacturing execution systems (MES), laboratory information management systems

(LIMS), enterprise resource planning (ERP), quality management systems (QMS), and computerized laboratory instruments. Validation activities are performed throughout the system lifecycle, from planning and design to operation and retirement.

### Regulatory Requirements for CSV

Regulatory agencies have issued multiple guidelines governing the validation of computerized systems. The key regulatory requirements include:

- 21 CFR Part 11 (US FDA): Governs electronic records and electronic signatures.
- EU GMP Annex 11: Specifies requirements for computerized systems used in GMP environments.
- GAMP 5: promotes a risk-based approach and categorizes software systems based on complexity, such as configurable software and custom applications
- WHO Technical Report Series: Provides guidance on validation and data integrity.
- MHRA Data Integrity Guidance: Emphasizes data accuracy, completeness, and reliability.

These regulations highlight the importance of system validation, data integrity, audit trails, access control, and change management.

### Risk-Based Validation Approach

Risk-based validation is a structured approach that focuses validation efforts on system functions that have a direct impact on product quality, patient safety, and data integrity. Rather than validating all system features equally, risk-based validation prioritizes critical functionalities.

Risk assessment is typically performed using tools such as Failure Mode and Effects Analysis (FMEA) or impact assessment matrices. Based on risk classification (high, medium, or low), appropriate validation and testing strategies are defined. This approach reduces unnecessary documentation while ensuring compliance with regulatory expectations.

### GAMP 5 Framework

Good Automated Manufacturing Practice (GAMP 5) is a widely accepted guideline developed by ISPE for the validation of computerized systems.

Key principle of GAMP 5 is Risked based approach-

- More risk- more testing

- Less risk- Less testing

The framework emphasizes supplier assessment, lifecycle management, and leveraging vendor documentation where appropriate. GAMP 5 aligns well with regulatory expectations and supports efficient validation practices.

GAMP 5 promotes a risk-based approach and categorizes software systems based on complexity, such as configurable software and custom applications.

Key focus of GAMP 5:

- Patient safety
- Product quality
- Data integrity
- Risk-based validation approach

### GAMP 5 categorizes computerized systems based on:

- Complexity
- Configurability
- Impact on GxP processes

Categorization helps decide:

- i. Validation effort
- ii. Documentation level
- iii. Testing depth (IQ/OQ/PQ)

### GAMP 5 Categories

#### Category 1 – Infrastructure Software

Software that provides IT infrastructure and does not directly perform GxP functions.

Examples:

1. Operating systems (Windows Server, Linux)
2. Database software (Oracle, SQL Server)
3. Network components

Validation Approach:

- Vendor qualification
- Installation verification
- SOP control

Example in Pharma:

- Windows Server used to host a LIMS application.

#### Category 3 – Non-Configured Products

Standard, off-the-shelf software used as is, without configuration or customization.

Examples:

1. MS Excel (used only for calculations without macros)
2. PDF readers
3. Standard data viewers

**Validation Approach:**

- Intended use definition
- Functional verification
- SOP and user training

**Example in Pharma:**

Excel sheet used only for manual stability data trending (no macros, no formulas impacting decisions).

**Category 4 – Configured Products**

Standard software that is configured to meet user requirements without changing source code.

**Examples:**

1. LIMS
2. QMS (TrackWise, SimpliQ, Veeva QMS)
3. ERP systems (SAP – configured modules)

**Validation Approach:**

- URS
- Functional configuration specification (FCS)
- Risk assessment

- OQ & PQ focused on configured functions

**Category 5 – Custom Applications**

Software developed or customized specifically for a company's process.

**Examples:**

1. In-house developed batch record system
2. Custom laboratory data system
3. Tailor-made validation tools

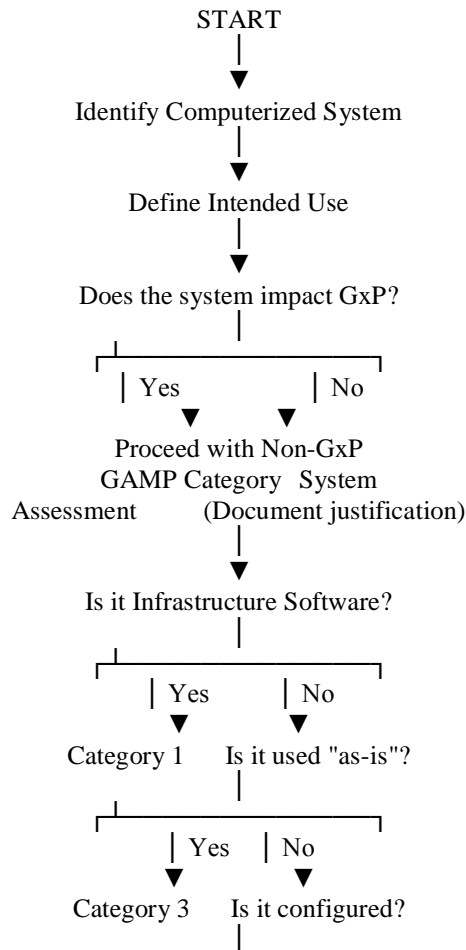
**Validation Approach:**

- Full SDLC
- URS → FRS → Design Specs
- Code review
- IQ, OQ, PQ
- Traceability matrix

**Example in Pharma:**

Custom-built electronic batch record (EBR) system developed internally.

**Categorizes computerized systems:**



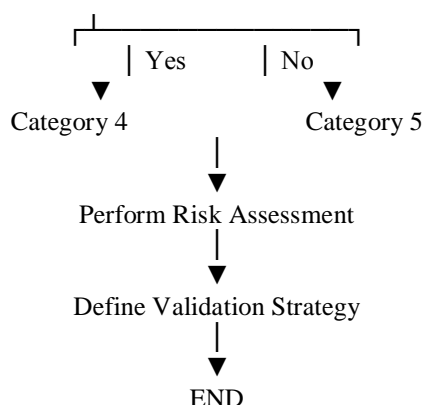


Figure: -GAMP 5 promotes a risk-based approach and categorizes software systems based on complexity, such as configurable software and custom applications.

### Data Integrity in Computerized Systems

Data integrity is a critical component of CSV and refers to the accuracy, completeness, and consistency of data throughout its lifecycle. Regulatory authorities emphasize the ALCOA+ principles, which state that data should be Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, and Available.

Key data integrity controls include audit trails, user access management, backup and recovery procedures, and system security measures.

### Computer System Validation Lifecycle

The goals of using a life cycle model for verification and validation align with those of a system architect. Controlling a system of defined elements, such as business or organizational functions, allows for efficient and cost-effective work processes and product.

The CSV Life Cycle is the full journey of a computerized system from initial idea through implementation, use, and eventual retirement with documented validation activities at each stage to ensure compliance, data integrity, and system quality.

It's based on lifecycle thinking (like that in GAMP 5), where validation is not a one-time event but an ongoing process integrated into the System Development Life Cycle (SDLC).

The system design phase is where computer systems are validated. It starts and proceeds through the whole SDLC. The following are the various phases of CSV .

#### 1. Concept / Initiation

- Define the business need and scope of the system.

- Determine whether validation is required (e.g., GxP impact on product quality, patient safety, or data integrity).
- High-level risk assessment and supplier/vendor evaluation.

#### 2. Planning & Requirements

- Develop a Validation Master Plan (VMP) that outlines strategy, responsibilities, and deliverables.
- Capture User Requirements Specification (URS) — what the system must do.
- Perform detailed risk assessment to tailor validation scope.

#### 3. Design & Development / Specification

- Translate user needs into design or functional specifications.
- Configure, code or customize the system as required by specifications.

#### 4. Qualification & Testing

This phase formally verifies that the system is built and operates correctly:

- Installation Qualification (IQ): Verifies correct installation.
- Operational Qualification (OQ): Ensures operation within expected ranges.
- Performance Qualification (PQ): Confirms performance under real-world conditions.
- Testing is documented and traceable often with a Requirements Traceability Matrix (RTM).

#### 5. Release & Go-Live

- Evaluate test results and produce a validation report.
- A summary report will be created based on the results obtained in the qualifications test

- Train users and transition system to production use.

### 6. Operation & Ongoing Maintenance

Once in production, the system must stay in a validated state throughout its operational life:

- Change control: Evaluate impact of upgrades or changes.
- Periodic reviews: Computerized systems ought to undergo regular assessments to ensure their continued validity and compliance with GMP . We regularly check the integrity of the computer-based system's validation status Concurrently with the change control procedure, we typically review all relevant validation records to determine the potential extent of revalidation. Reviews can occur more or less regularly, typically once a year, depending on the application. In addition to these evaluations, one can use internal audits to ensure proper protocol use and record control for validation support
- Incident, backup and security procedures to maintain integrity.

### 7. Retirement / Decommissioning

- When the system is no longer needed, plan its retirement.
- Safely archive or migrate data to meet regulatory record-keeping requirements.

### Key Principles of the CSV Life Cycle

- Lifecycle approach: Validation activities are planned and executed as part of the whole system life, not just at one point.
- Risk-based: The extent of validation effort should be commensurate with the system's impact on quality, safety, and compliance.
- Documentation: All validation actions must be documented and traceable to pass audits.
- Maintenance: Even after go-live, validation status must be maintained through controlled changes and periodic reviews.

### Computer System Assurance (CSA)

- Computer System Assurance is a modern approach proposed by the US FDA to improve the efficiency of computerized system oversight.
- CSA focuses on ensuring that systems perform as intended through critical thinking, risk-based testing, and continuous assurance rather than excessive documentation.
- CSA allows flexibility in testing methods, encourages leveraging automated testing tools, and reduces the burden of scripted testing for low-risk functions.
- The primary goal of CSA is to maintain compliance while improving system reliability and operational efficiency.

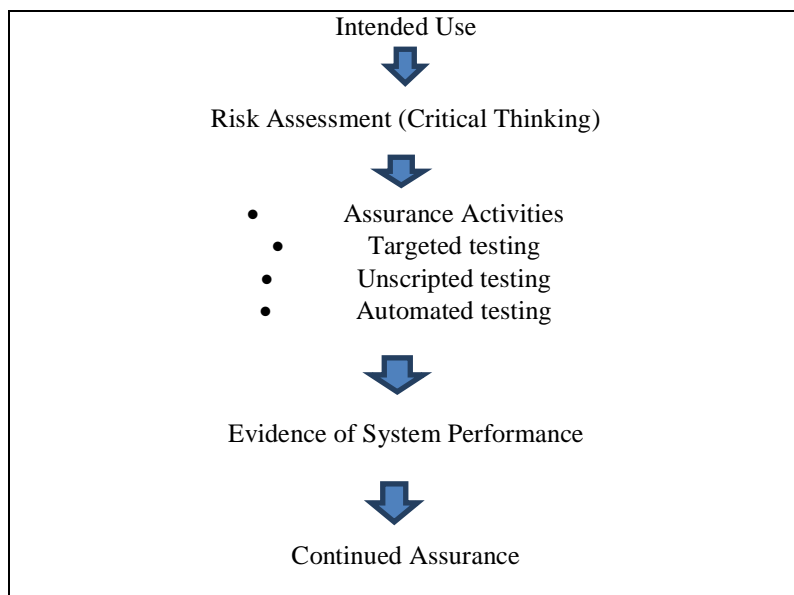


Figure: - Risk-Based Computer System Validation Lifecycle Showing the Transition toward Computer System Assurance

### Transition from CSV to CSA

Traditional CSV often creates a documentation burden that can slow innovation and consumes resources without always improving quality.

CSA supports modern software practices like cloud computing, Agile/DevOps, automated

testing, and exploratory testing — better suited to rapid software evolution.

Regulatory bodies (e.g., FDA) want to focus assurance where the risk actually lies, not on uniform validation of every function.

Aspect	CSV	CSA
Primary Focus	Compliance via documentation	Assurance via risk-based testing
Documentation	Extensive	Targeted and value-driven
Testing	Scripted, formal	Risk-based, includes unscripted/exploratory
Efficiency	Often slower	More efficient and scalable
Risk Handling	Uniform validation	Differentiated by risk impact
Supplier Documents	Less leveraged	Uses supplier evidence where appropriate

### CSV to CSA Transition Checklist

#### 1. Understand the Regulatory Context

- Review the FDA’s **Computer Software Assurance for Production and Quality System Software** guidance to understand scope and principles.
- Identify which systems are in scope (production/quality system software under 21 CFR Part 820).

#### 2. Establish Organizational CSA Readiness

- Form a **cross-functional team** (Quality, IT, QA, Compliance, and business owners).
- Conduct internal training on CSA principles — risk-based testing, exploratory testing, and rational evidence gathering.

#### 3. Revise Policies and SOPs

- Update validation procedures to reflect risk-based assurance (CSA), not purely documentation generation.
- Revise templates for risk assessments, test strategies, and evidence documentation to allow unscripted and exploratory testing where appropriate.

#### 4. Perform Risk Assessment

- Replace category-based risk thinking **with** intended use + impact on patient safety, product quality, or data integrity as the core risk drivers.
- Produce documented risk rationale for each system feature/test level.

#### 5. Define Testing Strategy Based on Risk

- High-risk features → structured/scripted testing.
- Medium/low-risk features → exploratory, scenario, unscripted testing documented with rationale.
- Leverage vendor/supplier evidence where credible, reducing internal test burden when possible.

#### 6. Update Validation Lifecycle Artifacts

- Ensure documentation reflects CSA practices:
- Risk assessment & risk rationale**
  - Test strategy & justification**
  - Assurance evidence**, including test notes, logs, and risk-based outcomes (not just screenshots)
  - Change control and training records**

#### 7. Pilot CSA on a System

- Start with one representative system (e.g., LIMS, QMS) to pilot the CSA approach.
- Assess how risk-based testing and unscripted validation work in practice.
- Gather lessons learned and refine procedures.

#### 8. Implement Continuous Assurance

- Embed CSA into your quality lifecycle: periodic review, change control, and ongoing risk reassessment.
- Use risk triggers (e.g., system changes) to determine when re-assessment or additional testing is needed.

**9. Train & Communicate Across Teams**

- Provide training for business owners, IT, QA, and auditors on:
  - Why CSA principles are used
  - How risk categories drive testing decisions
  - What evidence is acceptable for audit purposes

**10. Prepare for Inspections**

- Ensure documentation clearly articulates why each test was performed or not performed (risk rationale).
- Be ready to explain how risk assessments influenced test scope.

**Key Mindset Shifts (CSV → CSA)**

CSV (Old)	CSA (New)
Documentation heavy	Risk-based, critical thinking
Scripted testing only	Mix of scripted & exploratory testing
Test everything uniformly	Test based on potential impact
Screenshots as evidence	Evidence rationalized by risk
Compliance defense	Quality & safety assurance

**Challenges in Implementing CSA**

Despite its benefits, implementing CSA presents challenges such as lack of awareness, resistance to change, limited regulatory clarity in some regions, and the need for skilled professionals. Proper training, management support, and clear internal procedures are essential for successful adoption.

**Future Perspective**

The pharmaceutical industry is steadily moving toward digitalization, automation, and data-driven decision-making. CSA is expected to play a vital role in supporting advanced technologies such as artificial intelligence, cloud computing, and continuous manufacturing. Risk-based assurance models will become increasingly important to ensure compliance while maintaining efficiency.

**II. CONCLUSION**

Risk-based computer system validation is an essential regulatory requirement in the pharmaceutical industry to ensure product quality, patient safety, and data integrity. However, traditional CSV approaches often lead to excessive documentation without proportional benefit. The transition toward Computer System Assurance offers a modern, efficient, and compliance-driven approach that emphasizes system performance and critical thinking. Adoption of CSA can significantly enhance validation efficiency while meeting regulatory expectations.

**REFERENCES**

- [1]. US Food and Drug Administration. 21CFR Part11 Electronic Records; Electronic Signatures. FDA, USA.
- [2]. US Food and Drug Administration Computer Software Assurance for Production and Quality System Software – Draft Guidance for Industry FDA, 2022.
- [3]. European Commission. EudraLex, Volume EU Guidelines for Good Manufacturing Practice, Annex 11: Computerised Systems, 2011.
- [4]. World Health Organization. WHO Technical Report Series No. 996: Annex 5 – Guidance on Good Data and Record Management Practices, 2016.
- [5]. ISPE.GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems. International Society for Pharmaceutical Engineering, 2nd Edition, 2022.
- [6]. Bendale A, Patel N, Jadhav AG, et al.: Computer software validation in pharmaceuticals. Asian J Pharm Clin Res. 2011, 1:27-39.
- [7]. Hesham AM: Computerized systems validation (CSV) in biopharmaceutical industries . Open Access J Pharm Res. 2020, 4:1-15. 10.23880/oajpr-16000219 9. Pawar R, Kabra S, Bhushan B: Computer software validation: importance in pharma industry .Int J Pharm Res Appl. 2023, 8:620-6.
- [8]. Pedro F, Veiga F, Mascarenhas-Melo F: Impact of GAMP 5, data integrity and QbD on quality assurance in the pharmaceutical industry: how obvious is



- it?. Drug Discov Today. 2023, 28:103759.  
10.1016/j.drudis.2023.103759
- [9]. Uzzaman S: Computer systems validation: a systems engineering approach . Official J ISPE. 2003, 23:1-10.
- [10]. DilipPatil R, Pansare JJ: Computer system validation in the perspective of the medical field introduction .Int J Pharm Pharm Sci. 2022, 23:329-6.
- [11]. Savitha S, Kathiresan K: Computer system validation: a review .Int J Biol Pharm Allied Sci. 2022, 11:5256-66.  
10.31032/ijbpas/2022/11.11.6567
- [12]. Rusjan B: Computer system validation: example of quality management system design and of process implementation. J ContempManag Res. 2020, 25:1-23.  
10.30924/mjcmi.25.2.1
- [13]. Patel H V, Yogi RR, Narang E: A review on computer aided instrument validation . J Chem Pharm Res. 2011, 3:134-43.
- [14]. Jadhav SV, Waghchaure SS, Chemate SZ: Computer system validation in pharmaceutical industry .Int J Creat Res Thoughts. 2021, 9:2320-882.
- [15]. Vs T, Ks, D'souza P: Computerized system validation: introduction implementation and regulations - a review. Int J Pharm Res Scholars.2014, 3:122-31.