

# A Complete Guide to Computer System Validation



Computer System Validation, or CSV, is a modern, risk-based methodology that confirms software used in pharmaceutical operations functions as intended. The risk-based approach is based on critical thinking.

CSV has applied to the pharmaceutical industry for many decades, but the guidelines have been updated by the FDA in recent years with the introduction of CSA – Computer Software Assurance. European regulators and regulators in other jurisdictions have introduced similar guidelines that align with CSA.

CSA modernizes software validation processes in the pharmaceutical industry to make them more relevant to the digitalized nature of workflows and processes as well as the way in which modern software applications are developed.


Looking back, the traditional CSV approach was prescriptive, with all software treated in the same way. Validation processes were test and document-heavy and often amounted to a box-ticking exercise aimed at satisfying compliance inspectors.

[Software validation using CSA principles](#) requires risk analysis and critical thinking to ensure the majority of the validation effort targets the applications that pose the most risk to patients, product quality, and data integrity.

This CSV guide focuses on modern methods of computer system validation, with the objectives of traditional CSV but using modern CSA methodologies.

## Infographic: Traditional CSV vs Modern CSV Based on CSA Methodologies

CSV Utilizing CSA Methodologies & Principles	
Traditional CSV	CSV based on CSA
✗ Barrier to innovation and digitalization	✓ Risk-based approach breaks down barriers
✗ All software validated using the same process	✓ Validation effort is based on risk
✗ Focus: providing evidence to regulators	✓ Focus: patient safety, quality, & data integrity
✗ Vendor documentation & testing is duplicated	✓ Vendor documentation and testing is utilized

 **WESTBOURNE**  
Global IT Solutions

### Transitioning to CSV Based on CSA Methodologies

While the traditional CSV approach to software validation continues to exist in the pharmaceutical industry, regulators are recommending a shift to more modern CSA methodologies.

As mentioned previously, traditional CSV focuses largely on compliance. The outworking of this is that many pharmaceutical organizations continue to retain manual processes or legacy systems that have already been validated. The perception is often

that the validation burden is too heavy when implementing new technologies, resulting in delays and stalled modernization programs.

This is a sub-optimal situation as new technologies offer a range of safety and quality benefits, including significantly reducing the risk of human error.

CSA aims to move the dial by using a risk-based approach to validation based on critical thinking. CSV principles still apply, but the focus is no longer on testing and documenting each system the same way.

Validation processes under CSA are instead based on risk. This risk-based approach usually means you don't automatically test and document software that has already been tested and documented by the vendor. You can instead use the vendor's documentation, allowing you to concentrate your validation efforts on other elements, including those assessed to be high-risk to patient safety.

When taking this approach, it is also important to ensure vendor documentation is verified for completeness, traceability, and relevance to your intended use. Regulatory inspectors may request objective evidence that vendor materials were assessed and deemed sufficient.

The summary, however, is that the validation effort you deploy should match the level of risk.

# Traditional CSV vs Modern CSV/CSA

## Traditional CSV



## CSV Based on CSA



**WESTBOURNE**  
Global IT Solutions

With this updated approach to computer system validation, pharmaceutical organizations are replacing manual processes with digitalized solutions. They are also updating legacy platforms and outdated applications with modern versions.

## The Objectives of Computer System Validation

CSV is about proving that computer systems are fit for their intended use. CSV also demonstrates that computer systems comply with regulations (including 21 CFR Part 11) and adhere to GxP, including good manufacturing practice (GMP) and good laboratory practice (GLP).

This approach aligns with global regulatory frameworks, including ICH Q9 for Quality Risk Management, EU Annex 11 for computerized systems, and ALCOA+ principles for ensuring data integrity.

An essential objective is to demonstrate that computer systems can perform consistently and reproducibly.

With a risk-based approach to CSV, there are three core areas of priority:

- Patient safety
- Product quality
- Data integrity

CSV is becoming increasingly important as pharmaceutical organizations continue to implement business process automation and digital transformation initiatives.

## Computerized Systems Explained

CSV usually concerns the validation of software used in pharmaceutical organizations. However, the term “computerized systems” has a broad definition that includes the combination of hardware, software, and processes that are part of the **manufacturing and quality control of pharmaceutical products**.

Examples include:

- SCADA, PLCs, controllers, and HMIs
- Computers and laptops
- Edge devices
- Commercial off-the-shelf software, sometimes referred to as COTS
- Custom software

Within the above list, there are a lot of variables. For example, commercial off-the-shelf software can include operating systems such as Windows 11. It can also include pharmaceutical industry-specific software such as Chromatography Data Systems (CDS), Laboratory Information Management Systems (LIMS), and Document Management Systems (DMS). And it can include software that is important but not unique to the pharmaceutical sector, such as Manufacturing Execution Systems (MES) and Enterprise Resource Planning (ERP) software.

Even within commercial off-the-shelf software, there are different types:

- Software with very limited scope for configuration.
- Software that is highly configurable.
- Software that is customizable as well as configurable.

Then there is custom software designed for a specific purpose that is often also facility-specific.

## Varied Validation Requirements

The main point when considering software system types is that the amount of work required will vary depending on:

- a. Risk to patient safety, product quality, and data integrity
- b. Validation work already completed by the software vendor

An operating system, for example, is likely to be deemed low risk, so validation is implied via upstream processes, i.e., when validating a CDS application, validation of the operating system it is running on is implied.

A CDS is another good example, as it will be in a higher-risk category. That said, there is no need to recreate work done by the vendor, so vendor validation documentation can be used, reducing the validation effort that is required.

A highly customized MES or a completely custom application, on the other hand, is likely to require the highest level of validation, especially if it is deemed to be high risk.

It's also important to note that there are types of software applications not included in the above lists. Examples are accounting software or CRM systems – customer relationship management systems. Software systems like this don't fall within the CSV remit as they are not involved in the manufacture or quality control of pharmaceutical products.

## Categorizing Software Applications

GAMP5 presents four categories of computerized systems that can be helpful guides in determining the amount of validation testing that is required for a software application. The infographic below provides a broad outline of these categories (NB: there is no category 2 as it is no longer applicable in modern software environments).

# GAMP5 Computerized System Categorization

Category	Description	Validation Action
1	Infrastructure software such as operating systems and MS Word	Generally only tested indirectly when testing computerized systems in the other three categories
3	Non-configured systems purchased off the shelf that offer very limited scope for configuration	Simple validation is usually only required to verify the software meets user requirements
4	Configured systems such as customizable software applications	More detailed validation steps are required for this type of computerized system
5	Fully custom systems require the highest level of testing and control to properly validate	Comprehensive testing and validation of all code, features, and functions



## CSV Considerations for Cloud-Based and SaaS Systems

As pharmaceutical organizations increasingly adopt cloud-based platforms and Software-as-a-Service (SaaS) solutions, the CSV approach must adapt accordingly. While vendors manage core infrastructure, security, and some aspects of validation, the regulated company remains responsible for validating intended use, configuration settings, access control, and data integrity.

A shared responsibility model applies, meaning that:

- Vendor audits or questionnaires should assess cloud provider capabilities and data controls.
- Risk-based assessments are still needed to determine the validation scope.
- Configuration and integration points must be validated by the customer.

It is also important to ensure SOPs (standard operating procedures) and quality systems address cloud-specific considerations such as data residency, periodic backups, disaster recovery, and change management.

## Essential Elements for Effective Computer System Validation

### Risk Assessments

A core component of CSV is to identify the risks associated with computerized system failures, defects, and deviations from their intended use.

The focus of risk assessments should be on patient safety, product quality, and data integrity, i.e., what is the level of risk to patient safety, product quality, and/or data integrity if there are defects, deviations, or failures in a computerized system?

The next steps in the CSV process are determined by the assessed risk level. The greater the risks, the greater the validation effort that is required. Where there are risks to patient safety, product quality, and/or data integrity, effective controls must be identified, implemented, verified, and monitored.

### Supplier Qualification

For commercial off-the-shelf software, supplier qualification rather than system testing and documentation is usually the recommended approach. In other words, you can use the vendor's own testing and documentation to assess their ability to provide you with a product that meets the objectives of CSV.

Vendor assessments as part of a supplier qualification process can include vendor-supplied documentation and quality systems, the service level agreement you have with the vendor, and the vendor's reputation and past history for quality.

Importantly, features or components of the commercial software that you have customized will require ad hoc testing and documentation.

### Testing

For elements deemed to be high risk and/or where there is no suitable documentation from the vendor, it is essential to create and implement a testing strategy. The entire process must be documented. This includes documenting what you tested, how you tested it, who did the testing, and when it was performed. The documentation should also include the results of the tests.



If the tests produced defects or deviations, these must also be documented in addition to what you did to deal with them, i.e., the controls that you designed, verified, and implemented.

## Change Control

A robust change control process must be in place to ensure changes, such as software updates, are documented and validated. Again, the goal is to ensure the computer system performs as intended and doesn't increase patient safety, product quality, or data integrity risks.

## Training

Individuals involved with the computerized system, including users and operators, must be properly trained as part of the CSV process.

## Periodic Review

Validated systems must be periodically reviewed to confirm they remain in a controlled and validated state.

## CSV Support

CSV often requires expert support from experienced resources. You should consider hiring CSV expert support in the following situations:

- Implementing a new computerized system, such as a new software application.
- Upgrading an existing system to a new version, especially when significant changes are involved.
- Changing or reconfiguring an existing system.
- As a response to an inspection or audit where issues are identified.
- Where your team would benefit from CSV training.
- Where you need a new or updated Validation Master Plan
- When you have resource gaps in your in-house team
- In preparation for a regulatory inspection.

## CSV Support from Westbourne

At Westbourne, [we have extensive CSV experience](#) with skilled resources on our team who have [supported pharmaceutical industry customers](#) in all the situations highlighted above. Whether you need support to augment your existing team or you need CSV

project leaders, we can provide a custom solution that will meet your business and compliance needs. [Contact us](#) today to arrange a consultation.