

## The Challenges of Computer System Validation in Growing Pharmaceutical Companies



Computer system validation in the pharmaceutical industry is a necessary but typically onerous, challenging, and expensive requirement. It is also a requirement that is often poorly defined in terms of methodologies, standards, and procedures. Optimising the validation process brings quality, compliance, cost, and productivity benefits, but to do that, it's important to first understand and address the challenges.

Computer system validation is necessary to ensure software applications and platforms consistently and reliably conform to both user needs and intended use.

This is a necessary requirement for all computer systems used in GxP environments.

Examples include [LIMS \(laboratory information management systems\)](#), [CDMS \(chromatography data management systems\)](#), and table top instrument connected systems in laboratories, as well as DMS (document management systems), MES (manufacturing execution systems), EMS (environmental management systems), and BMS (building management systems).

### The Main Challenges of Validating Computer Systems in Pharma Facilities

#### Time and Resources

Computer system validation has traditionally involved considerable time and a lot of resources. This particularly applies when a standard, prescriptive, largely box-ticking approach is taken to validation, where all computer systems are treated the same, regardless of the level of risk they pose.

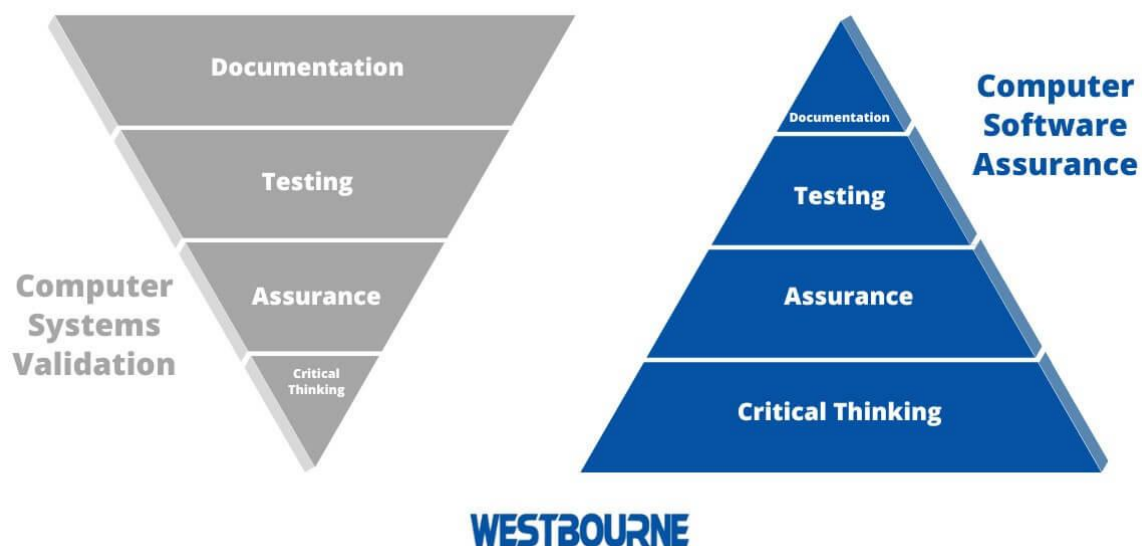
Taking a risk-based approach to computer system validation, however, reduces the amount of time and resources you need to allocate to the process, especially as there will be less of a requirement for testing and documentation, both of which are tedious processes. CSV engineers will also spend less time writing test scripts and more time on value-adding tasks.

Eliminating duplication of effort is also an important part of mitigating the time and resource challenges of computer system validation. Examples of duplicated efforts that can be eliminated include revalidating software that has already been validated by the vendor (providing the vendor's documentation is checked for adequacy and compliance) or developing a new SOP that shares substantial overlaps with existing SOPs.

### Understanding How Much Validation is Enough?

One of the big issues with computer system validation in the pharmaceutical industry is that the question of how is almost completely open to interpretation. For example, the FDA's 21 CFR Part 11 provides very high-level statements on what needs to be achieved in computer system validation, but it doesn't give guidance as to how. Even [GAMP 5 guidelines](#) are open to interpretation.

That said, the pharmaceutical industry is moving away from a one-size-fits-all computer system validation process. Pharma companies are instead moving to the risk-based approach mentioned in the previous point. A risk-based approach to computer system validation is advocated by regulators in many parts of the world, with the FDA, for example, encouraging the industry to move to a [CSA \(computer software assurance\) model of validation](#), with critical thinking rather than documentation at its core.



This move to a risk-based approach brings benefits, particularly as it switches the focus from compliance to quality, but it also presents a different challenge: how much validation is enough?

Auditing vendors and carrying out risk assessments on software applications help with answering this question, but it is also beneficial to engage a partner who has broad computer system validation experience.

At Westbourne IT, for example, we provide validation services to pharmaceutical laboratory operations in a range of different companies. We use this validation experience and expertise to optimise the validation process for our clients, including minimising validation costs, time, and resources.

## Governance

Who is responsible for ensuring computer systems in pharmaceutical operations are properly validated? What roles do different departments and individuals have when it comes to computer system validation, i.e., the laboratory team and quality control, manufacturing operations, IT teams, etc?

Centralised planning and monitoring alongside clearly defined goals help to overcome this challenge.

## Vendor Selection and Management

Pharmaceutical manufacturing and laboratory operations can have bespoke or customised software applications, but there is also considerable reliance on third-party platforms and systems.

This brings back into focus the risk-based approach to computer system validation, as off-the-shelf software generally doesn't need to be revalidated with a new set of documentation. Instead, you can use the vendor's documentation (functional specification, design specification, IQ, OQ, etc) provided you audit the vendor to ensure compliance with GAMP guidelines. How often audits should be conducted depends on a variety of factors, including the standard of the vendor's validation and quality practices and the level of risk posed to patient safety or product quality.

A subset of this challenge that deserves specific consideration is cloud-based computer systems. Cloud-based solutions are increasingly used in the pharmaceutical industry, but it is important to understand and define boundaries and responsibilities of validation. In doing this, it is important to keep in mind that it is pharmaceutical companies, not software or cloud platform vendors, that are ultimately responsible for ensuring computer systems remain in a validated state.

## Other Challenges of Computer System Validation

Some other challenges of computer system validation that are worth highlighting include:

- Regulatory landscape – regulations continuously evolve, plus there are differences depending on the marketplace.
- Technical complexity – the computer systems being deployed in pharmaceutical operations are increasing in technical complexity. This is only going to increase as technologies like AI become more widespread. This increase in complexity creates new validation challenges.
- Documentation – even though a risk-based approach to validation reduces documentation requirements, documentation remains an essential and ongoing part of the process.
- Data integrity – maintaining the integrity of data is essential. Specific challenges in relation to data integrity include the problems that occur with manual data as well as the sheer volume of data that needs to be managed and maintained.
- Cybersecurity – every new or expanded computer system in a pharmaceutical environment brings cybersecurity risks (such as ransomware attacks) that need to be understood and mitigated.

### Getting the Right Support

Getting the right validation support will help you overcome all the challenges in the above list as well as the main challenges outlined in this blog. With the right support, you will meet your regulatory obligations with a focus on product quality and patient safety, while reducing the resource, time, and cost burden of computer system validation. To find out more about the support we can offer at Westbourne IT, [please get in touch](#).