

THE SHIFT TO CLOUD MES: CSV AND VALIDATION PRACTICE

Rethinking validation design for the cloud era
through the lens of supplier–user responsibility





Agenda

1. Where Cloud Fits Within the Regulatory Landscape	3
2. What Actually Changes – The Shift in the Responsibility Model	3
3. Supplier-Side Qualification – From Development Through Release	5
3.1 Agile Development Under a Quality Management System	
3.2 Qualification: Supplier Verification of Standard Functionality	
3.3 A Risk-Based Approach to Qualification	
3.4 Combining Automated and Manual Testing	
4. Release and Upgrade Management	7
5. The User's Validation Strategy	7
6. Impact on Operational SOPs	8
7. Agile Development in Relation to Traditional Methods	8
8. Conclusion	9



Introduction

Across pharmaceutical, biotech, and cell and gene therapy (CGT) manufacturing, the migration of MES (Manufacturing Execution Systems) from on-premise infrastructure to the cloud and SaaS is accelerating. Yet it remains common for organizations to carry over a "1990s-style," on-premise validation playbook and apply it directly to cloud technology. Because the underlying system architecture of cloud and on-premise environments is fundamentally different, this direct carry-over simply does not work in practice. A successful migration to cloud MES depends on properly understanding how validation differs between on-premise and cloud environments, how responsibility should be divided between the parties involved, and what practical qualification and validation methods look like in this new context.

1. Where Cloud Fits Within the Regulatory Landscape

Practitioners often raise the question of whether cloud technology is even permissible from a regulatory standpoint. In fact, leading regulators such as the FDA have clearly encouraged the adoption of modern, innovative technologies, and this stance is strongly reflected in international discussions such as those under ICH. Regulation itself is therefore not the barrier to cloud adoption. Cloud and SaaS solutions have already gained wide traction globally within pharmaceutical manufacturing, including MES, and adoption across Asia, including Japan, is expected to continue expanding.

2. What Actually Changes — The Shift in the Responsibility Model

The most fundamental change brought about by cloud/SaaS adoption is in who is responsible for managing each layer of the system — networking, infrastructure, operating systems, middleware, and the application itself. On-premise, an in-house IT team builds, operates, and maintains all of these layers. In the cloud, much of this responsibility shifts to multiple third parties, such as cloud providers and MES suppliers.



Aspect	On-Premises	Cloud/SaaS
Building and maintaining infrastructure	In-house IT team	Cloud provider / supplier
Scope of IQ (Installation Qualification)	Performed in-house across every layer (large deployments can involve IQ documentation running to dozens of pages and more than ten physical servers)	Leverages the supplier's own qualification work; the user focuses on verifying configuration and confirming it meets requirements
Hardware investment	Required (procurement and maintenance costs are ongoing)	Generally not required
Backup / disaster recovery	Built and maintained in-house	Often provided redundantly by the cloud provider across multiple sites
Mechanism for managing responsibility	Internal policies and inter-departmental coordination	Quality agreements / service level agreements (SLAs), formalized in the validation plan and qualification plan

This shift is not itself a problem. What matters is clearly defining where each party's responsibility begins and ends, and formalizing that division in quality agreements, service level agreements (SLAs), and the validation and qualification plans. Even when responsibility is delegated to third parties, ultimate accountability still rests with the regulated user organization. As a result, supplier assessment — selecting the right partners — becomes an even more critical step than before.

Large-scale on-premise MES deployments commonly involve IQ documentation running to dozens of pages and require more than ten physical servers to run a reliable system. The procurement costs, documentation, review and approval burden, and the day-to-day operational maintenance that come with this are largely eliminated in the cloud. As a result, the role of the user organization shifts from doing and building everything itself to reviewing and approving the deliverables produced by its suppliers.

Validating a large on-premise MES frequently takes anywhere from several months to more than a year, and such projects are prone to running over both schedule and budget. By contrast, adopting cloud/SaaS solutions can shorten the validation timeline dramatically — in some cases down to a matter of weeks.



3. Supplier-Side Qualification — From Development Through Release

The lifecycle of developing and implementing a cloud MES divides broadly into supplier-side activities and user-side activities. Preceding the user's own validation are two supplier-side stages: design and development, and qualification.

3.1 Agile Development Under a Quality Management System

Modern MES development is largely built on agile methodologies and managed within the supplier's quality management system (QMS). Quality controls such as design reviews, risk assessments, and development-stage testing are built into the development process, ensuring that quality is designed into the product from the outset.

3.2 Qualification: Supplier Verification of Standard Functionality

During the qualification stage, the standard functions of the MES — data integrity controls, audit trails, recipe version control, electronic signatures, and the like — are verified against user requirements and a risk assessment to confirm they operate effectively. Qualification is not simply testing; it also involves compiling a complete set of documentation as evidence. Once qualified, the product is deployed to the user's environment on the cloud platform, at which point the platform configuration is also verified against user requirements.

One of the core principles underlying GAMP is to leverage the qualification work already performed by the supplier as fully as possible. Doing so not only supports compliance but also reduces the validation effort required on the user side — a consideration that is particularly important for GMP-critical systems such as cloud MES.

The main qualification deliverables can be summarized as follows. The qualification plan defines the team structure and division of roles the supplier will use to produce each deliverable, and shows how this is controlled within the supplier's QMS. Specification and design documentation, in an agile context, takes the form of epics and user stories rather than a traditional functional specification. For organizations accustomed to a functional-specification-based approach, this can feel like a significant departure, but industry guidance — including GAMP — formally accepts this agile approach. What matters is not the name or format of the documentation, but whether the right activities are being performed and whether they are reviewed and approved within an electronic system. Finally, once qualification testing is complete, a qualification report and a requirements traceability matrix are compiled and made available to the user.

Leverage supplier qualification work to reduce user-side validation effort.



3.3 A Risk-Based Approach to Qualification

Qualification is carried out on a risk basis. It begins with a process map that captures the system's workflows and data flows, and each process area is then assessed against criteria such as the maturity of the feature, its complexity (the level of development effort involved, or how configurable it is by users), and its GxP criticality (its potential impact on product quality and data integrity). These factors are scored in an electronic tool to calculate a qualification impact rating, which is used to focus qualification effort on the higher-risk areas.

Because risk assessment inherently involves an element of subjectivity, the supplier and the user do not always arrive at the same conclusion. In such cases, the supplier documents the rationale behind its own assessment, while the user can factor the qualification results into its own validation and apply its own independent judgment where appropriate.

3.4 Combining Automated and Manual Testing

Automated testing has become an efficient means of verification. For example, it is now common for a single process area — order management, say — to have more than a hundred test cases automated and run overnight as a batch job. Work that would take hours or even days to perform manually is completed in a fraction of the time, allowing defects to be caught earlier.

Automation does have its limits, however. Usability evaluation and integration testing with real equipment or external systems cannot be fully covered by automation alone and still require manual testing in an actual integrated environment. For this reason, a combination of scripted and unscripted testing (checklist-based, exploratory testing) is applied according to the results of the risk assessment. Unscripted testing avoids the effort of preparing detailed test scripts in advance, freeing testers to apply more creativity and flexibility and spend more of their time actually testing — an approach recognized as effective for catching defects earlier, and one that is accepted in both the FDA's Computer Software Assurance (CSA) guidance and GAMP. Even when unscripted, testing activities are still documented and reported.

The trustworthiness of this kind of automated testing rests on two factors: the testing tools themselves are not CSV-specific tools, but well-established software development lifecycle (SDLC) tools used broadly across every industry, and the results they produce are reviewed and approved on an ongoing basis rather than accepted blindly.

Once qualification is complete, a qualification report is compiled. It lists the deliverables and activities performed, summarizes the test results, and states a clear conclusion that the system is qualified and its functions are working effectively. This report serves as important supporting evidence for both the user's validation and any regulatory inspection.



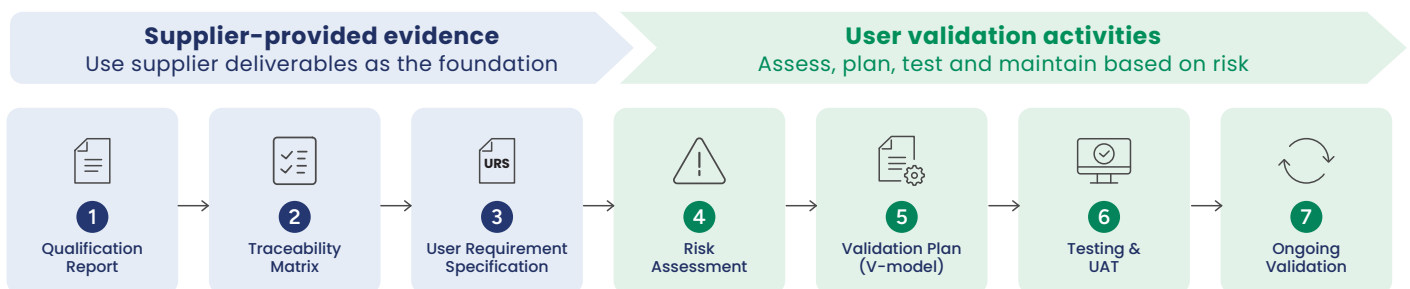
4. Release and Upgrade Management

A defining characteristic of cloud MES is the continuous stream of feature upgrades pushed out by the supplier. Unlike on-premise systems, these updates can arrive without waiting on the user's own timeline, which makes how they are managed particularly important.

For every upgrade, whether major or minor, the supplier performs its own qualification and provides supporting evidence to the user — release notes, deployment notifications, a traceability matrix, and deployment reports. In a cloud environment, a test environment and a production environment are typically kept separate, and an upgrade is deployed first to the test environment. At this stage, the user follows its own change control process, assesses the impact on its own operations based on the supplier's release notes, and decides whether any additional validation testing is required before deploying the upgrade to production. The release of an upgrade by the supplier does not automatically mean additional validation is required on the user's side.

5. The User's Validation Strategy

The basic principle behind the validation the user organization itself performs is to make full use, as a foundation, of the data integrity controls the supplier provides — security management, backup and restore, and failover, among others.



Many cloud providers offer multiple levels of backup, often replicated across more than one geographic location. Reputable providers also typically hold third-party certifications such as ISO 27001 and SOC reports, and publish guidance on how their infrastructure controls align with GMP expectations. Rather than verifying all of this from scratch, the user's role is to review the documentation and controls the provider makes available.

A validation strategy is typically built around a validation plan based on a V-model. This plan incorporates the qualification report and traceability matrix supplied by the supplier, together with a



high-level risk assessment specific to adopting a cloud MES — covering risks from both an infrastructure and a supporting-process perspective, such as business continuity in the event of a system outage. As for user requirement specifications (URS), it is acceptable from a compliance standpoint to make use of a URS provided by the supplier, provided the user reviews and formally approves its content. Ideally, the URS should be established before the project begins — that is, during supplier evaluation and selection.

Risk assessment within validation uses a process risk assessment methodology to evaluate data integrity gaps. Particular attention is paid to the source of the data: manually entered data is generally considered to carry a higher data integrity risk than data captured through equipment integration or generated by system calculations. Together with an assessment of how critical the data itself is, this process risk assessment drives the scope of the test plan and user acceptance testing (UAT), including the balance between scripted and unscripted testing.

6. Impact on Operational SOPs

Introducing a digital system such as an MES into a manufacturing environment requires a corresponding set of operational SOPs. Organizations that already have validated computerized systems in place can often extend existing CSV-related SOPs — change control and access control, for example — to cover the new system. One area specific to MES that deserves particular attention is the SOP governing recipe (master batch record) verification. It is worth developing a dedicated template to confirm that recipes are properly configured, reviewed, and tested.

7. Agile Development in Relation to Traditional Methods

The distinction between agile and waterfall development is another important consideration in understanding CSV for cloud MES. Where waterfall follows a V-model approach oriented toward a single, large release, agile development proceeds in smaller, more iterative increments and is managed through electronic SDLC tools. This is not a new concept confined to the pharmaceutical industry — it is a practice long established across modern software development generally, including at major technology companies — and it is explicitly recognized as best practice in both GAMP and ISPE guidance.



8. Conclusion

The essence of modern CSV for cloud MES is not about generating more paperwork; it is about smarter risk management. By making full use of the qualification work already performed by the supplier, the user organization can concentrate its own validation effort on what is specific to its infrastructure, network, and business processes.

What makes this possible is a trusted relationship with the supplier, together with contracts and plans that clearly document how responsibility is divided. The supplier is responsible for building quality and compliance into the system from the earliest stages of product development, while the user organization must manage this relationship as a long-term partnership — from supplier selection through ongoing operation and upgrade management. Cloud represents a compelling path forward for digitalizing the pharmaceutical industry, but realizing that potential requires meeting international regulatory expectations while maintaining an ongoing exchange of knowledge among all parties involved.

“Modern CSV for cloud MES is about smarter risk management — not generating more paperwork.”

Ready to rethink your approach to cloud MES validation?

Explore a practical approach to cloud MES validation.

Learn more about BatchLine's approach to qualification, validation, and ongoing compliance.

www.batchline.com/contact

BATCHLINE