



INSIGHTS

Compliance Challenges with Enterprise Application Integration

By Jason Ward, Vinay Jain, and Tim Bartel

January 2004

Executive Summary

Enterprise Application Integration (EAI) implementations can provide enormous benefits to organizations that run multiple computer-based systems in regulated environments. The ability to have information seamlessly flow from the source of data collection [for example, a Laboratory Information Management System (LIMS), or an Enterprise Resource Planning (ERP) System], to other systems that may use that information, can improve cycle-time of decision-making, and reduce costs in data maintenance. However, when these systems house data that falls under regulations such as 21 CFR Part 11, the challenge of achieving, and demonstrating, that the systems meet the requirements of the regulation can be daunting. The purpose of this white paper is to discuss challenges and recommendations in working to meet compliance with 21 CFR Part 11, specifically around computer systems validation as it relates to EAI solutions.

The implementation of an EAI tool to enable the integration of multiple systems poses some very unique challenges to the validation effort for the project. When a specific system is implemented, the boundary of validation should be established to verify processes and data that are either within the system, or input to or output from the system. But when the purpose of the tool itself

is not to create data, but to correctly and efficiently pass it from one system to another, where do you draw the line with the effort to validate the system implemented? And what additional steps must be taken to ensure the integrity and traceability of regulated data as it is passed and manipulated between multiple systems? These are two of the biggest challenges facing organizations that implement EAI in a regulated environment.

A third major challenge exists around the approach utilized for implementation. Typically, EAI implementations are completed in phases, or waves. An initial phase may integrate an ERP and LIMS system, for example, to reduce cycle-time on inspection and release of product. A contract compliance system may then be integrated in a second phase to improve customer responsiveness and compliance. To add to the challenge, business requirements typically evolve during the implementation time-frame. An efficient yet effective approach to validation will allow the completion of phases in a timely manner.

Drawing the Line on Validation

There is much confusion in the validation arena about what must be validated versus what is acceptable to simply test. There is so much confusion that some in the industry have begun to simply validate everything so as to

(continued)

eliminate risk. While this does eliminate risk, it elevates cost, creates unnecessary paperwork, and ties up resources that could be used on more lucrative tasks. Another common mistake is that validation is not approached in a modular fashion, thereby making change and additions to the system very slow and expensive. The common mistake that we see repeatedly is when organizations develop a validation approach that “ties their hands,” thereby making simple changes in the future a daunting task, and thus making the organization go without necessary system changes because of the huge validation impact. By following some general guidelines and developing a structured approach, it is possible to eliminate risk by validating the necessary areas only, thus freeing up organizational resources by not performing unnecessary validation.

The Challenge

Knowing where to draw the line in integration validation is two-fold:

- **Different types of transactions (both GMP and non-GMP) can be processed through the same integration tool.** Properly identifying the appropriate transactions will help determine the success of the validation effort.
- **Identifying what vendor components must be validated and what is covered with a vendor audit.** Correctly identifying components from an integration vendor that can be covered by a simple vendor audit will help save time and money in the validation process.

Recommendation

Tough FDA restrictions have caused many organizations to become very skitish about validation. However, organizations can be much better served if they perform thorough analyses to determine what systems and data are GMP-relevant, and document the reasoning behind their decision-making. Systems and data are determined to be GMP-relevant by evaluating the processes supported by the system to the predicate rules. Likewise, an analysis and determination of the applicability of Part 11 should be completed at the same time. It is important that individuals from the Quality Assurance and/or regulatory compliance areas be included in this determination.

The extra effort required to perform a thorough analysis of what transactions are worthy of validation is much more cost-effective than to just validate everything.

The extra effort required to perform a thorough analysis of what transactions are worthy of validation is much more cost-effective than to just validate everything. For example, if an organization is integrating a LIMS, ERP, and production planning system, they may determine that the data being passed from the LIMS to the ERP system is GMP-relevant, but that the data passed from the ERP to the planning system

(continued)

is not. Historically, the FDA has shown that if an organization can 1) perform a thorough analysis of all transactions for GMP-applicability, 2) illustrate how this analysis was conducted, and 3) document the results of this analysis, then there is no need for organizations to perform the additional burden of validating non-GMP transactions “just to be safe.” In the above example, validation would be performed on the ERP-LIMS integration, but not on the ERP-Planning integration.

Vendor audits should be performed to ease validation efforts of integration tool components. By performing audits of the vendor’s software development lifecycle, you can minimize the amount of validation that must be performed on-site for custom coding and data integrity checking.

For example, let’s assume that you are purchasing an integration tool with an out-of-the-box connection to an ERP system. Rather than validating that the connection “works” every time it is used, a vendor audit conducted once of the development practices used can cover the connection.

By validating that the software development practices of the vendor are sufficient, we can assume that the out-of-the-box connections will work appropriately. We do not have to prove that they work every time that we use them; a test case executed during system testing is sufficient. This basic connection validation is not only helpful, but also essential to surviving a validation effort. Spending time validating out-of-the-box components will make the validation effort insurmountable. Some larger vendors have audits available for purchase through industry organizations in order to simplify even further. If one of these pre-packaged audits is available, it is recommended that you save time and purchase the audit.

Vendor audits should be performed to ease validation efforts of integration tool components.

Having said that, a vendor audit is essential to a successful validation effort. The next question that you might be asking is, What am I looking for in a vendor audit? Does the vendor need to be ISO-9000 compliant? Should they follow the Capability Maturity Model (CMM)? A simple answer is, yes and no. Having a certification from an outside source certainly illustrates that the vendor has repeatable processes; however, your organization will be ultimately responsible, so you should take these certifications at face-value. While a certification by itself may not be sufficient for a vendor audit, it certainly is a nice addition to any verification that your organization performs. A vendor audit should produce results that prove that the vendor follows processes that would result in producing a consistent final product.

It is important to note that a vendor audit is just one important component of the validation package. In addition to the audit, the following are required to demonstrate proper validation:

(continued)

- A validation master plan
- A document summarizing the GMP assessment of what needs to be validated
- Installation qualifications, operational qualifications, and performance qualifications
- Change control processes

We highly recommended that organizations perform vendor audits prior to the purchase of software solutions to better understand the validation requirements and features that the solutions may offer to address FDA requirements.

Data Integrity and Traceability

Integration, by nature, provides a seamless way for data to be passed and utilized by multiple systems. However, a potential harmful side effect of programs manipulating data between systems is that data can be changed from its original content. In the wake of the FDA's 21CFR part 11 regulations, the importance of data integrity and traceability has acquired increased significance. This provision requires the organization to have the ability to generate accurate and complete copies of records in both human readable and electronic forms suitable for inspection, review, and copying by the agency. This becomes especially important in an environment with integrated systems because the source system of the data may not be the system where decisions are made regarding that data. An organization needs to demonstrate control of all systems in which GMP data resides. In the case of an adverse event, an organization will need to be able to demonstrate that it was not caused by systems that created, stored, or reproduced faulty data.

The Challenge

Before we discuss the challenges around data integrity and traceability, let us first understand their definitions.

- **Data Integrity** – A condition existing when data is unchanged from its source, and has not been accidentally or maliciously modified, altered, or destroyed.¹
- **Traceability** – The property of the result of a measurement whereby it can be related to appropriate standards (generally international or national standards) through an unbroken chain of comparisons.² It is also defined as “The ability to trace the history, application or location of an item or activity by means of recorded identification.”³

(continued)

As part of good business practices, and also required by the FDA, data integrity and traceability are key requirements for all GMP information related to equipment and computer systems. Organizations must ensure that data is secure and traceable for all systems (automated or procedural) that were used to create the test, or create data verifying who created it and the date and time of creation. Software must also prevent uncontrolled and undocumented changes to the records or data at a later stage. These records or data should be able to be retrieved by FDA inspectors, as needed, for up to ten years in most cases, and maybe more in some. Non-compliance with 21 CFR Part 11 can be very costly as it may lead to delays in product launches, compromised product quality, fines, sanctions, imprisonment, or complete shut down of a manufacturing facility. For integration validation, mistakes that we have seen include not testing data integrity from initial source through the final destination, not building or demonstrating audit trails in the integration software itself, and not completing tests that demonstrate that all 21 CFR Part 11 requirements are met.

As part of good business practices, and also required by the FDA, data integrity and traceability are key requirements for all GMP information related to equipment and computer systems.

Recommendations

One of the first items that must be accomplished is to complete data flow diagrams that document the source and flow of data between all systems that will be integrated. Similar to drawing the line on validation, a GMP analysis should then be completed to determine which data is regulated. It is important to check that non-GMP modules or data, such as a forecast, does not affect GMP data; if it does, it could change the determination. This analysis will determine the end-to-end tests that must be completed. This will be directly used by the validation master plan to determine the scope of validation. It is not uncommon to find that a system that is being integrated will require some retrospective validation along with the integration software itself.

Another critical step is to complete a 21 CFR Part 11 assessment of the integration tool itself to determine how audit trail and security requirements will be met and proved via testing. For example, if the integration tool has a workflow component that is utilized for approval of batch data as it moves from a source system to a repository, it needs to be demonstrated that audit trails exist for the approval, and that the appropriate security verification of the electronic signature was done at the time of approval.

Thorough Yet Modular System Testing

Both the data flow and 21 CFR part 11 analyses will produce areas of focus for testing. This input should then be used when developing the Operational Qualification (OQ) and Performance Qualification (PQ) plans. The OQ should address

(continued)

both unit and integration testing so that data integrity and traceability can be thoroughly demonstrated at both levels. In an integration project, this is one of the critical success factors simply because there are more integration points and objects.⁴ Data integrity and traceability between these objects is of utmost concern since an integration tool⁵ is used to flow data from one object to another, which may or may not be cGMP-compliant.⁵

Testing should not be specific to a software component or an application. It should cover all software, integration points and objects, servers, connections between multiple applications, and accuracy of data flow. However, tests should be designed in a modular approach so that, in future phases, regression testing can be made as manageable as possible. As a part of thorough testing, tests must confirm

that everything works as designed (positive testing), and negative testing must be performed, whereby scenarios are run to try to break functionality, e.g., accept values that are not valid or do not fall within expected ranges and tolerances.

The testing process should be covered in both an OQ and PQ. The OQ should cover both reliability testing,

which is mainly done by developers to see if the source code works, and functional testing to ensure that the application does what the business requires. The PQ should cover load and stress testing, which simulate the scale of operational use once it is handed over to the users. Whenever changes are made, regression testing is carried out to ensure that the application is still performing as expected. There are automated testing tools that may also be used to reduce the cycle time for testing.

Testing should not be specific to a software component or an application. It should cover all software, integration points and objects, servers, connections between multiple applications, and accuracy of data flow.

Multi-Phased Implementations

Due to the complexity, risk, and resources required to implement EAI solutions across the organization, multi-phased implementations are typically planned and executed. After the initial phase is live in a production environment, adding additional functionality to the production system carries its own set of validation challenges

The Challenge

A great deal of time and resources were invested to validate the initial phase of the project. A completed validation package containing plans, protocols, and summary reports has been signed and archived. Production change control is now in force. The next phase of implementation, however, will cause some changes to the production system, and add a whole new set of data most likely flowing through the same integration objects. During the first phase, no atten-

(continued)

tion had to be paid to making changes to code until OQ testing started. In future phases, the fact that a validated system is already in production will need to be factored into any plans going forward. What approach can be taken to complete the next phase without having to re-work all of the validation deliverables that has been completed?

Recommendation

Similar to the recommended approach described for ‘drawing the line’ on the upfront validation effort, a thorough analysis should be completed that examines the extent of change. This analysis needs to encompass not only what may be changing in the integration tool, but also what may affect any systems that utilize the tool as an integration technology. Questions such as the following need to be considered:

- What new data is passing through the system, and is it GMP-relevant?
- What current production objects will be affected?
- Will there be any changes to the standard integration tool itself?
- What effect will a newly integrated system have on those systems already integrated?
- Will new integration points change any of the GMP relevancies of existing integration points?

After completing this analysis, the scope of the validation effort can then be determined by focusing on those areas where regulated data is being affected and assessing the risk of change. Not everything will need to be revalidated. Best practice dictates that the focus of the validation effort is applied to only those areas in which change carries a risk; by using this approach, an efficient yet effective validation approach can be utilized on the subsequent phases of the project. As the business changes, this same approach can also be applied to changing business requirements.

Through our client experience, we have found the following to be key characteristics of organizations that maintain and expand upon existing systems efficiently:

- **Efficient Change Control** – A well-defined and practiced change control process is essential to the on-going development and compliance of computer systems.
- **QA/IT/Business Alignment** – It is critical to have QA, IT, and business users of the systems working very closely in a well-defined process to ensure that business needs are prioritized and met in a timely fashion while not compromising compliance and requirements of other system users.

(continued)

- **Comprehensive Quality System** – A completely defined, executed, and well-educated system of SOPs and guidelines covering the assessment, completion, and maintenance of validation efforts.

Choosing the Right Solution Partner

For the long-term success of your integration project and to mitigate the risks associated with rapid industry changes and consolidation, it is important that you partner with a vendor with a track record of auditable success and long-term viability.

EAI is a rapidly evolving industry. Many vendors are consolidating or forging an alliance with other industry leaders to stay competitive and survive in this quick-paced industry. For the long-term success of your integration project and to mitigate the risks associated with rapid industry changes and consolidation, it is important that you partner with a vendor with a track record of auditable success and long-term viability. Many research firms can provide a comparison of these vendors. You can also partner with a services firm that has specialized knowledge of these vendors and can complete an unbiased analysis based on their integration experience, industry trends, and their experience in your legacy host systems. When deciding on the right EAI partner for you, keep in mind how well they address some important validation issues like data integrity, data security, and traceability.

Conclusion

Enterprise Application Integration (EAI) implementations can provide enormous benefits if implemented in a timely and efficient manner. Implementing EAI solutions in a regulated environment should not hamper the benefits that EAI can bring to the table. With a well-defined approach to validation, a thorough analysis and understanding of the data and systems, and a chosen software tool from a vendor with auditable development methods, integration in a regulated environment can become a very successful investment.

About the Authors

Mr. Jason Ward and Mr. Vinay Jain are Senior Consultants in Clarkston Consulting's Life Sciences Practice. Jason brings over eight years experience, and Vinay over five years of industry experience to their clients.

(continued)

Notes

1. www.atis.org
2. <http://www.nist.gov/traceability>
3. www.isoeasy.org
4. Objects can be an array of multiple systems like LIMS, ERP, Transportation System, WMS, Production Planning System, CRM System, or any Legacy Systems.
5. Integration tools can be a middleware product such as Vitria, Webmethods, Mercator, TIBCO, etc.

About Clarkston Consulting

Clarkston Consulting is a nationally recognized management and technology consulting firm that provide validation, compliance and implementation services to address issues that its clients face in FDA-regulated environments. Nearly half of the top 50 pharmaceutical companies in the world have worked with Clarkston's consultants, who deliver award winning expertise and exceptional customer satisfaction. Clarkston Consulting's approach focuses on the key business drivers aimed to improve productivity of product development pipelines; communications between sales, marketing, and customers; and business processes centered on new product launches. To learn more about Clarkston Consulting, visit www.clarkstonconsulting.com/whitepapers.



Copyright © 2004, Clarkston Consulting. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without prior written permission.