Veeva

WHITE PAPER

Veeva Professional Services Project Computer Systems Validation (CSV)

AUTHOR

Llinos Cooper | Veeva Systems, Services Lead, Validation Strategy

Executive summary

This white paper presents best practices for defining the approach to Computer Systems Validation (CSV) on Veeva Professional Services projects, focusing on configuration. This white paper is intended to complement and extend the Risk-based Approach to Change Management of GxP Systems white paper.

Validation | The process of establishing documentary evidence demonstrating that a procedure, process, or activity carried out in testing and then production maintains the desired level of compliance at all stages.

Validation Environments | Controlled environments that are used for initial project validation testing and later validation environments mirror production configuration for change testing.

GAMP 5 | (Good Automated Manufacturing Practice), a set of guidelines developed by the International Society for Pharmaceutical Engineering (ISPE). GAMP 5 provides a framework for ensuring that automated systems used in pharmaceutical manufacturing are properly validated and compliant with regulatory requirements, such as those from the FDA and EMA.

Contents

Veeva Vault validation

Veeva validation methodology overview

Veeva adheres to a robust validation methodology based on the principles of Computer Systems Validation (CSV). CSV involves establishing documented evidence that a computer system meets predefined requirements. This methodology ensures that Veeva Vault operates as intended and complies with relevant regulatory requirements.

Layered Approach: Veeva Vault employs a layered approach, consisting of:

- **Platform Layer:** This foundational layer provides the core infrastructure and functionalities upon which all Veeva Vault applications are built.
- **Core Application Layer:** This layer includes pre-built applications like QualityDocs or eTMF. These applications come with core requirements and functionalities that have been validated by Veeva.
- **Template Layer:** This layer includes starting point configuration for customer business process, this layer is not a validated starting point.
- **Configuration Layer:** Customers build their specific business processes and functionalities on top of the core applications through configurations.

Veeva's rigorous validation of the platform and core application layers ensures the underlying engine driving the template and customer configurations is reliable and compliant. This layered approach allows customers to focus their validation efforts on their unique configurations and business processes.

Veeva's Responsibility lies in the qualification of the hosted environments and the validity of the functionality of core software. This includes:

- **Installation Qualification (IQ):** Veeva performs IQ for the core system, including the operating system, software and security components. This ensures the proper installation and configuration of the underlying infrastructure.
- **Operational Qualification (OQ):** Veeva conducts OQ to verify that the core system functionalities meet the defined requirements. This encompasses functionalities like standard objects, lifecycles, and workflows, which are integral parts of the Veeva Vault platform and core application suite.

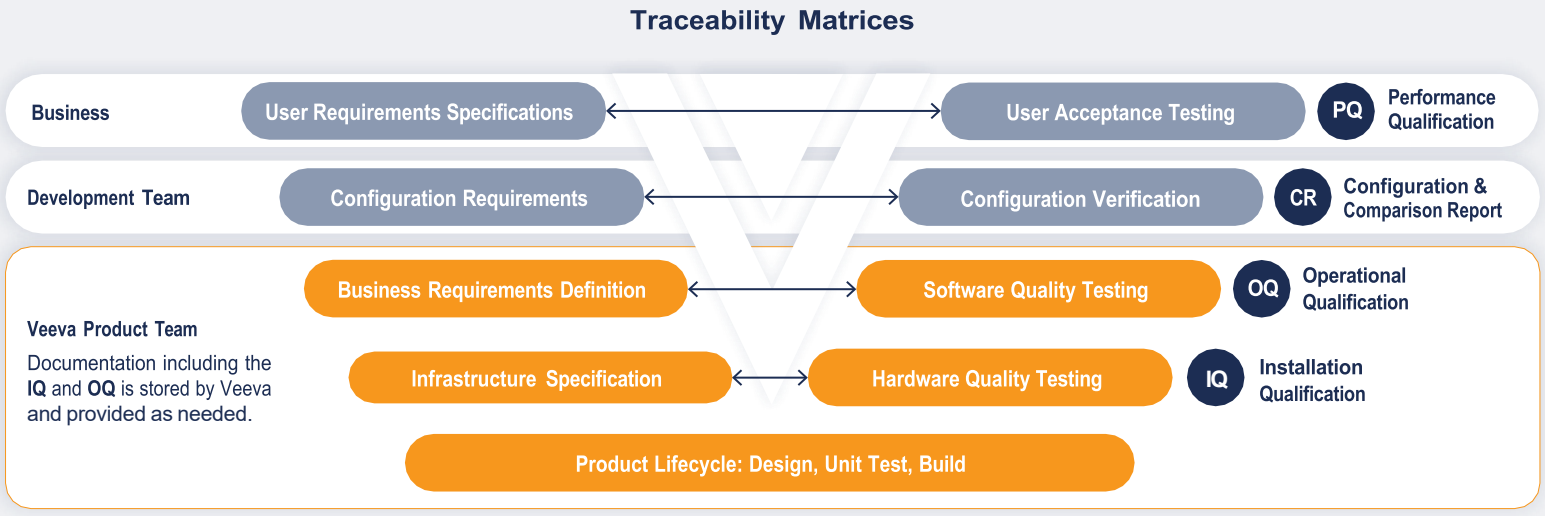
Customer's Responsibility lies in the validation of the specific configurations and integrations implemented within their Veeva Vault environments. This typically involves:

- **User Acceptance Testing (UAT):** UAT focuses on verifying that the system meets the user requirements and business processes per their approved system configuration.
- **Performance Qualification (PQ):** PQ assesses the system's performance under real-world conditions, ensuring it can handle the expected workload and maintain data integrity. Performance monitoring is managed by Veeva, with reports provided on a quarterly basis. These reports outline the performance metrics for Veeva Vault and are intended for customer review. Reports are available in ComplianceDocs. For instructions on how to access ComplianceDocs, please refer to page 7.

Risk-based approach to validation

GAMP 5 and Veeva Vault

Veeva's validation methodology aligns with the principles outlined in GAMP 5 (Good Automated Manufacturing Practice), a set of guidelines developed by the International Society for Pharmaceutical Engineering (ISPE). GAMP 5 provides a framework for ensuring that automated systems used in pharmaceutical manufacturing are properly validated and compliant with regulatory requirements, such as those from the FDA and EMA.



KEY ASPECTS OF GAMP 5

- **Risk-Based Approach:** Focuses validation efforts on critical system functionalities that impact product quality, patient safety, and data integrity. Identifies and mitigates risks by prioritizing areas of highest concern.
- **Lifecycle Approach:** GAMP 5 emphasizes the importance of validation throughout the entire system lifecycle. This encompasses initial implementation, ongoing changes and updates, and eventual retirement of the system.
- **Flexible Approach:** GAMP 5 recognizes that validation efforts should be proportional to the complexity and risk associated with the system. This means that less complex, lower-risk systems might require a streamlined validation approach, while more complex and higher-risk systems necessitate a more comprehensive validation strategy.
- **Supplier and Service Provider Involvement:** GAMP 5 acknowledges the crucial role of suppliers and service providers in providing evidence and documentation to support customer validation efforts.
- **Data Integrity:** GAMP 5 places significant emphasis on data integrity, ensuring that data is accurate, complete, consistent, attributable, available when needed, and protected from unauthorized alteration.

GAMP 5 CATEGORIES

GAMP 5 categorizes software based on its level of customization and associated risk:

- **CATEGORY 3 - Non-Configured Software:** This category comprises software that cannot be customized, such as commercially available applications like Microsoft Excel.
- **CATEGORY 4 - Configured Software:** This category includes software tailored to fit the specific needs of a process or system. Configuration might involve defining workflows, or configuring lifecycles within a document management system.
- **CATEGORY 5 - Custom/Bespoke Software:** This category encompasses software developed from scratch to fulfill unique business requirements. Custom software development poses a higher risk due to the complexity of the development lifecycle and the potential for introducing errors in the code.

VEEVA VAULT AS GAMP 5 CATEGORY 4

Veeva Vault falls under GAMP 5 Category 4, as it is a configured software system. The configurations applied to Veeva Vault do not involve writing custom code. They are implemented through a user-friendly interface that constrains options and enforces predefined rules, reducing the potential for errors.

LEVERAGING VEEVA DOCUMENTATION

As a GAMP 5 Category 4 software system, Veeva Vault allows customers to leverage Veeva's extensive documentation and verification activities to streamline their validation efforts. The Veeva validation team performs comprehensive testing and generates documentation that provides evidence of the system's functionality and compliance. Customers can utilize this documentation to support their own validation activities, focusing on verifying that their specific configurations meet their business requirements.

Veeva's compliance documentation which includes IQ and OQ is available in ComplianceDocs, see page 7 for further details.

Risk classification examples

A risk-based approach is essential for efficient and effective validation of Veeva Vault configurations. System changes vary in risk level, and identifying the associated risk ensures the appropriate level of validation rigor is applied.

FACTORS INFLUENCING RISK

Several factors contribute to the overall risk associated with a change in Veeva Vault. These may include:

- **GxP Impact:** Changes that directly impact GxP-regulated activities, such as data integrity, audit trails, electronic signatures, or security controls, pose a higher risk and require more stringent validation.
- **Impact on Core Functionality:** Changes affecting the core functionalities of Veeva Vault, including workflows, lifecycle management, document management, and security settings, are generally considered medium risk, requiring a thorough assessment and validation. In other words, changes in Vault related to a business process that alters Vault's behavior and logic when responding to inputs are considered medium risk.
- **Impact on Non-Core Functionality:** Changes impacting non-core aspects of the system, such as metadata fields, notifications, reports, user interface elements, or administrative functions not related to security or regulatory compliance, are typically deemed low risk.

EXAMPLES OF RISK CLASSIFICATION

The following table provides examples of how different areas within Veeva Vault could be classified based on their potential risk:

Risk Level	Veeva Vault Areas
High	Permissions, Login, Security Policies, Security Profiles, Audit Trail, eSignature, Document Change Control, DAC (Dynamic Access Control)
Medium	Creating, updating, deleting documents; Creating, updating, deleting objects; Workflow operations; Lifecycle operations; Check In/Check Out; Configuring reports; Versioning
Low	Document library, Creating/editing fields (fields that do not contain VQL/ constraints), Reporting and dashboards (where a quality decision is not made based on the results of these reports), Annotations, System Look & Feel (GUI), Localizations/translations, Labels, Exporting, Search, Field dependency, Breadcrumb navigation, Notifications, Managing data, Field level security

DOCUMENTING RISK DEFINITIONS

Organizations must clearly document their risk definitions, and the criteria used to classify changes within their Veeva Vault environments. This documentation should be included in their validation methodology, validation plans, or other relevant SOPs. A well-defined risk classification system enhances consistency and transparency in validation efforts.

Veeva resources

ComplianceDocs

ComplianceDocs is a repository designed to provide customers, prospective customers, and partners with access to a set of documents, including:

- Core Product Validation Documentation (Validation Plan, Impact Assessment, OQ, Trace Matrix, Validation Summary Report)
- Certificates and Attestations (ISO/SOC)
- Operational Reports (DR/Penetration Tests/Availability/Performance)
- White papers & Regulatory Compliance Assessments
- Standard Industry Assessments (SIG/CAIQ/GAMP)

Access can be requested via this link.

Veeva executed OQ test cases are available for consumption and can be used to supplement the customers Validation Package, the results of IQ can be found in the Validation Summary Report, the executed IQ test cases can only be viewed during scheduled audits.

The Validation Packages are organized in binders by suite and release, see page 9 for a list of the documentation provided in the binders.

Compliance assessments

Veeva provides several Compliance Assessments. The following assessments are available in ComplianceDocs and should be reviewed when defining the scope of UAT/PQ:

- **21 CFR 11 Compliance Assessment:** The purpose of this document is to provide interpretation, clarification and guidance regarding the applicability of the 21 CFR Part 11 requirements to Veeva products, processes, and personnel. This assessment is applicable to the regulated products, e.g., Development Cloud (Clinical, Regulatory, Safety, and CDMS Vaults), Quality Cloud and Commercial Cloud (Multichannel CRM, Network MDM, Commercial Vaults).
- **EU Annex 11 Compliance Assessment:** The purpose of this document is to provide interpretation, clarification and guidance regarding the applicability of the EU Computerized Systems Annex 11 requirements to Veeva products, processes, and personnel. This assessment is applicable to the regulated products, e.g., Development Cloud (Clinical, Regulatory, Safety, and CDMS Vaults), Quality Cloud and Commercial Cloud (Multichannel CRM, Network MDM, Commercial Vaults).
- **Japan ERES Compliance Assessment:** The purpose of this document is to provide clarification and guidance for customers regarding the applicability of the Japanese ERES (PFSB Notification, No. 0401022 April 2005) requirements as these apply to Veeva processes and products. The scope of this assessment includes only those ERES controls listed in Appendix A. This assessment is applicable to the regulated products, e.g., Development Cloud (Clinical, Regulatory, Safety, and CDMS Vaults), Quality Cloud and Commercial Cloud (Multichannel CRM, Network MDM, Commercial Vaults).
- **Detailed ERES Trace Assessment – Vault:** The objective of this Detailed Electronic Records/ Electronic Signatures (ERES) trace is to correlate the Vault ERES related features to their corresponding regulatory section in either FDA 21CFR11, EU GMP Annex 11, or Japan ERES regulations. This scope of this document is limited to features and functionality that are delivered as part of the Veeva platform, application specific supplements, and the processes that Veeva uses to comply with the development and validation aspects of these regulations as a supplier of product to regulated users in the Life Science industry.

Services project deliverables and responsibilities

Responsibilities

The figure below provides a suggested list of validation deliverables that may be leveraged or produced during a Veeva Professional Services Implementation Project and their corresponding responsibilities. The Validation Deliverables in orange are typically provided by Veeva and are available in ComplianceDocs.

The Validation Deliverables in blue are typical project deliverables, and with the exception of the Vault Configuration Report and Vault Compare Report, these are produced by the customer following the organizations CSV procedures which are documented in the organizations Quality Management System.

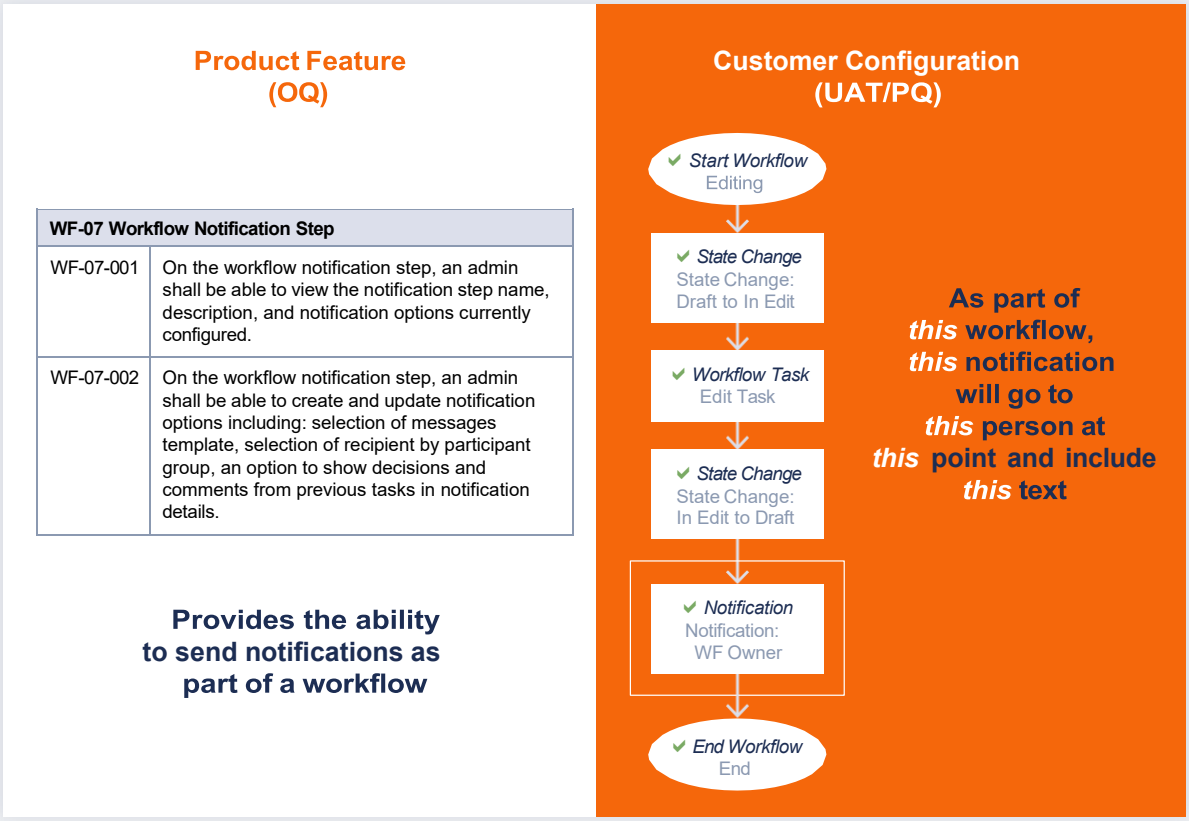
Project validation templates packages are available to be purchased for some core applications and can be used as a starting point for the customer's validation efforts. The customer is responsible for reviewing and updating the documentation in line with the customers validation SOP.

	Validation Deliverables	Veeva	Customer	Customer Action Required
Product	Validation Project Plan (VPP)	✔	N/A	
	Installation & Operational Qualification (IOQ) Protocol	✔	N/A	
	Validation Impact Assessment *(for each Vault release)*	✔	N/A	Reference executed documents provided by Veeva *(documents available via Veeva ComplianceDocs Vault)*
	Business Requirements Definitions (BRD)	✔	N/A	
	Executed OQ Test Scripts	✔	N/A	
	Trace Matrix (BRD <-> OQ)	✔	N/A	
	Validation Summary Report (VSR)	✔	N/A	
Project	Validation Master Plan	N/A	✔	Develop according to customer CSV SOP
	Vault Configuration Report	✔	N/A	Provided by Veeva Services *(Vault Auto-generated Document)*
	Vault Configuration Compare Report	✔	N/A	Provided by Veeva Services
	User Requirements Specification (URS)	N/A	✔	
	UAT/PQ Test Plan	N/A	✔	
	UAT/PQ Test Scripts	N/A	✔	Develop according to customer CSV SOP
	Traceability Matrix (URS <-> UAT/PQ)	N/A	✔	
	Validation Summary Report (VSR)	N/A	✔	

Operational Qualification versus User Acceptance Testing/Performance Qualification

An important concept to understand prior to defining the scope of UAT/PQ is the relationship between a Product Feature, which has already been validated by Veeva during OQ verses the customer's configuration applied during the Services project (UAT/PQ).

Below is an example of how this works for notifications.



The building blocks for notifications are verified through Veeva's OQ, ensuring that notifications can be sent as part of a workflow. The customer's UAT/PQ further validates the details, such as whether the notification triggered at the correct time and contained the expected text.

The same approach applies to workflows. The OQ layer verifies core functionality, such as sending workflow tasks and changing statuses based on predefined criteria. Specific statuses and criteria are configured during the Services Implementation project and may be included in UAT/PQ testing.

VAULT IS AN ADMIN AND USER APPLICATION – CONFIGURATION IS HIGHLY DEFINED AND CONSTRAINED TO REDUCE ERRORS

For 21 CFR Part 11 compliance, audit trail functionality is locked at the OQ layer, ensuring it cannot be modified by the Services Implementation team. The same applies to eSignatures, which are validated at the platform level. While the Services team can enable eSignatures at specific points in a business process and configure picklist values for meanings/capacity, they cannot alter the format or functionality. These elements are also covered in the Compliance Assessments.

Work products (validated and non-validated)

The following work products are typical deliverables for Veeva Services projects and can be used by an organization to build confidence in taking a risk-based approach to UAT/PQ.

VALIDATED TOOLS AND DOCUMENTS

- **Configuration Report:** A system export report in Microsoft Excel format containing configuration information and reference data used by components for a Vault. This report is useful for tracking and documenting a Vault's configuration at any time. This document can be saved and approved in the customer document management system; this may be used for traceability for lower risk items that are verified.
- **Compare Report:** Vault Compare allows you to compare the configuration of two Vaults. This can be helpful when building a Configuration Migration Package or validating that environments are synchronized after package deployment. The results are documented in a Microsoft Excel report which clearly highlights any differences between Vaults e.g., any differences between the Validation and Production environments.
- **Vault Clone/Sandbox Vaults:** Sandbox Vaults are copies of your production Vault, which your organization can use to develop and test configuration changes, data migrations, and integrations, without affecting your production Vault and users. Sandbox Vaults are critical to an effective change control process. Creating a sandbox for a new project and refreshing your sandboxes often will help your organization avoid issues and delays when deploying changes in production.

NON-VALIDATED WORK PRODUCTS

- **Role Definitions Matrix:** Spreadsheet documenting user access levels and controls.
- **Swim Lane Diagrams:** Visual representation of lifecycles of workflows.
- **RAID Log/Configuration log/User Stories:** Where project specific requirements are documented.

Defining the scope of UAT/PQ leveraging Veeva documentation

For organizations with multiple applications, Veeva recommends a cross-functional URS and Trace Matrix that documents the requirements that will apply to all applications e.g., eSignature, Audit Trail, Objects, Workflows, and Lifecycles. Most of this matrix will trace to the Veeva BRDs (Business Requirements Definitions) and therefore may not need to be included in UAT/PQ.

Another application specific URS & Trace Matrix documenting application-specific requirements is recommended. These items may need to be included in the UAT/PQ scripts or informally verified (dependent on risk).

- **Cross-functional URS & Trace Matrix** documenting the requirements that will apply to all applications e.g., eSignature, Audit Trail, Objects, Workflows, and Lifecycles. Most of this matrix will trace to our BRDs and therefore will not need to be included in UAT/PQ.
- **Application-specific URS & Trace Matrix** documenting application-specific requirements. These items will need to be included in the UAT/PQ scripts or informally verified (dependent on risk).

THE APPLICATION-SPECIFIC URS WOULD INCLUDE THE HIGH-LEVEL BUSINESS PROCESS FROM START TO FINISH ENSURING THAT THE END-TO-END BUSINESS PROCESS IS ACCOUNTED FOR.

Both trace matrices may trace to Veeva's BRDs (Business Requirements Definitions) with the addition of project-specific UAT/PQ test scripts for application-specific requirements. Lower risk requirements may be verified, and traceability can be achieved by tracing to the applicable Configuration Report tab.

How to stay compliant

Suggested documentation for implementing a risk-based approach

Organizations must maintain applicable documentation to demonstrate compliance with regulatory requirements and internal quality standards. The following documents/templates or their equivalents within the organization's quality system may be maintained to reflect the risk-based approach leveraging Vendor documentation

- Computer System Validation (CSV) Standard Operating Procedure
- Risk Calculation Work Instruction
- Validation Plan

- Test Plan
- User Requirements Specification
- Traceability Matrix
- Validation Summary Report

Additional Considerations

Administration: The organization will need to administrate the system, including account management, in accordance with your security policies.

Data Migration: Data migration tools need to be qualified, results need to be verified.

Integration: All application integrations need to be validated (IQ/OQ/PQ). If the configuration changes, the organization should assess the risk, and the integration(s) may need to be re-validated.

Key takeaways for success

- Define your risk-based approach leveraging the principles outlined in this white paper to define and implement a validation strategy that prioritizes critical risks.
- Leverage Veeva's vendor documentation. Not all configurations are impactful enough to warrant validation in addition to Veeva's.
- Decisions made during the Services Implementation project determine the level of validation required for each Veeva General Release and the customers operational releases.
- By implementing a well-defined process, maintaining thorough documentation, and leveraging vendor documentation, organizations can effectively validate Veeva Vault while maintaining compliance and optimizing performance.