Contents

3.2

Executive Summary

Validation of GxP systems is required to assure they are fit for intended use and compliant with applicable regulations. However, the same rigor is often applied to all system changes—regardless of potential impact. This stifles change and culminates in stagnant systems and a growing gap between what the solution delivers and the needs of the users or business.

With cloud solutions requiring more frequent, mandatory updates, a streamlined change management process is essential. This position paper proposes a risk-based approach to manage GxP system configuration changes and release updates without compromising the quality of the "system product" or the integrity of the validated state, and is developed to align with ICH Q7, ICH Q9, ICH Q10, and GAMP 5. While the scope of the paper was developed specifically for Veeva Vault configuration changes and release management, the principles and methodology can be applied to a wide range of GxP systems.

1 Introduction

The evolving nature of the life sciences industry requires a nimble approach to the steady state management of validated systems. Validation of GxP systems is required to assure they are fit for intended use and compliant with applicable regulations. However, the inherent nature of validation poses significant challenges when systems are faced with potential changes. Configuration changes and new software releases can alter qualified workflows and affect the validated state of a system.

Often, the same rigor is applied to all system changes – regardless of potential impact. If a universal change management approach is applied to all configuration changes for a validated system, it will likely stifle system change with over-engineered, cumbersome processes. The process for managing the change is usually more involved than implementing the change itself, resulting in systems consistently lagging user needs. Without costly resources and time dedicated to steady state management, solutions usually become stagnant – stuck on older software versions, or creating a growing gap between business needs and what the solution can deliver.

We can better ensure a change process that embraces system updates, and continuously meets end-user requirements by reducing the redundant, extraneous, and non-value added change requirements that also pose no compromise to the following:

- The quality of the "system product"
- The integrity of the application's validated state

Regulators are increasingly expecting risk-based decision-making is incorporated into all facets of business processes throughout the product lifecycle. Appropriate controls should be implemented to manage risk and validate GxP systems for their intended use.

This position paper is developed in alignment with the following guidelines: ICH Q7, ICH Q9, ICH Q10, and GAMP 5, and proposes a risk-based approach to manage Veeva Vault system configuration changes and general releases – without compromising the quality of the end-state content maintained in Veeva Vault. The proposed proactive approach aligns with the principles conveyed in:

- ICH Q9, where the rigor of change oversight, including the extent of documentation and verification, is based on the risk and complexity of the change
- ICH Q10, where a change management system is a driver for continual improvement, and risk management is utilized in the evaluation of proposed changes
- GAMP 5, where "Quality risk management should be based on clear process understanding and potential impact on patient safety, product quality, and data integrity" and "application of quality risk management enables effort to be focused on critical aspects of a computerized system in a controlled and justified manner"

The methodology also leverages ICH Q7, where it provides guidelines for changes to computerized systems.

The benefits of the proposed risk-based process include:

- A consistent and repeatable approach to Veeva Vault change management
- Timely alignment between user expectations and Veeva Vault performance and capabilities
- Reduced time and effort planning and managing Veeva Vault changes and releases
- Agility to scale for increased demand by the business or as the user needs grows, while ensuring the system remains fit for purpose

2 Scope

This paper provides principles to implement a risk-based process to more effectively and efficiently manage changes to a GxP system. While the examples presented here are developed specifically for Veeva Vault configuration change and release management, the risk-based approach can be applied to a wide range of GxP systems.

The proposed risk-based approach to Veeva Vault system configuration changes and release management does not compromise the following:

- The quality of the "system product" such as end-state document content
- The integrity of the Veeva Vault application's validated state

One effective measure of a risk-based approach is how well the process meets the established standards/ requirements of a formal change within the context of a quality management system. Change management ensures that the impact of a proposed change is fully understood and allows an organization to take a proactive approach to mitigation and control. There is a wide range of change management processes, from capturing a revision history to overarching management within a formal change system. The level of oversight for GxP system configuration changes should embrace the following ICH Q10 concepts:

- "To manage changes based on knowledge and information accumulated" – in configuration and steady state use
- "To evaluate the impact of changes on the availability of the final product" – i.e. evaluate impact of change on controlled content
- "To evaluate the impact on product quality changes to the facility, equipment, material, manufacturing process or technical transfers" – how does the change impact controlled content in addition to the validated state, business process, system functionality, and user functionality
- "To determine appropriate actions preceding the implementation of a change" – e.g. additional testing, (re) qualification, (re) validation, or communication with regulators

Ultimately, change management will allow for proper evaluation and implementation of change drivers with "a high degree of assurance there are no unintended consequences of the change (ICH Q10)." A highly functioning change management process for GxP systems should include the following principles:

- Leverage quality risk management (QRM) to evaluate proposed changes and determine a level of change effort appropriate to the level of determined risk
- Evaluate proposed changes as they relate to the validated status of the system
- Include evaluation by system and business experts that have an understanding of the true impact resulting from a proposed change
- Provide confirmation / documentation that the change was completed as expected, and provide assurance that there will be no unexpected impact on system quality
- Allow for low impact / low risk changes to proceed without extraneous documentation

3.3.1 Impact

Consistency in the interpretation of 'impact' proves challenging when the roles of those defining impact are always evolving and evaluations can be made in a vacuum. A consistent interpretation / definition is difficult to maintain without constantly reviewing all impact assessments in previous records. Creating a single source of truth as it relates to the definition of impact provides a robust strategy for managing change in a consistent and effective manner. As regulations or business needs change, the guiding document can be updated to always reflect the current definition.

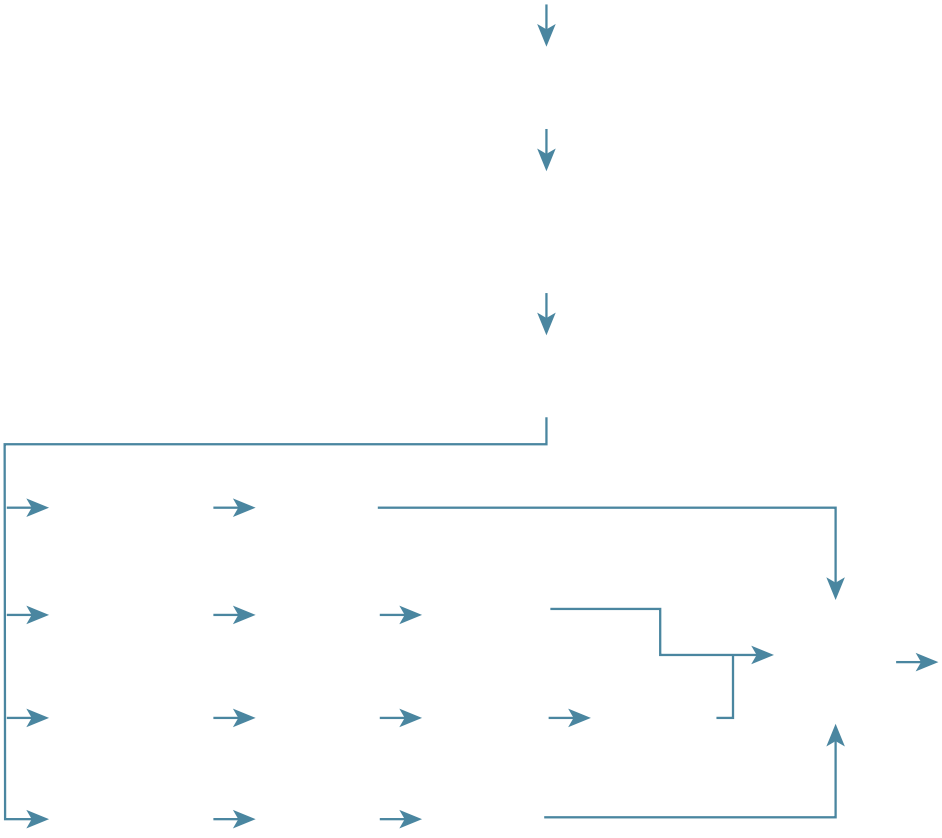
4 Applying a Practical Risk-Based Approach

4.1 Methodology

Successful implementation of a risk-based approach to configuration change management is highly dependent upon having a well-defined methodology in place to ensure the depth and breadth of potential changes are well understood. Risk evaluation must consider potential impact on: the system, the product / output, and the end-users, in addition to employing a multi-faceted approach to control. The overarching process should allow for scalability across most GxP systems and applied consistently for a particular GxP application.

To meet the tenets of risk-based ICH guidance, the proposed methodology for risk analysis targets four (4) main categories of risk evaluation: define, identify, interpret / quantify, and apply. Employing the proposed methodology will allow for both an understanding of potential risks associated with GxP configuration changes, and the establishment of a catalogue of system changes with varying levels of risk-based control. The following figure presents an overview of the proposed risk-based approach based on this methodology. Subsequent sections describe how the methodology was applied to arrive at this approach."

F 1-D R- A P R P



4.1.1 Define Risk

Defining risk is integral to application of a quality risk management program and is a crucial first step prior to starting specific change analysis. GAMP 5 declares, “Quality risk management should be based on clear process understanding and potential impact on patient safety, product quality, and data integrity.” For the purposes of this paper, the scope of product quality refers to the controlled output of the system, or more specifically to the quality/integrity of the end-state content in the Veeva Vault application.

4.1.2 Identify Risk(s)

GAMP 5 states “application of quality risk management enables effort to be focused on critical aspects of a computerized system in a controlled and justified manner.” To achieve this objective, risk identification involves completing a granular look at all potential changes, and developing a full catalog of these potential changes based on established risk definitions. The more comprehensive the approach employed for this step, the greater the consistency and realized benefits will be for continual application of risk-based control.

4.1.3 Interpret / Quantify Risks

After risks are appropriately defined and identified, they must be translated into easily understood categories that facilitate risk-based application. In regards to risk interpretation, ICH Q9 states, “the evaluation of the risk to quality should be based on scientific knowledge and ultimately link to the protection of the patient.” Applying to GxP systems, this can be interpreted as ‘evaluation of the risk to quality / compliance should be based on subject matter expertise and ultimately link to the integrity of the controlled end-state content.’ Proper risk quantification must be made by trained staff that understands the administrative aspects of the system including, but not limited to, lifecycles, workflows, security settings, Part 11 controls, system operations, and data analysis. Where possible, expertise from the application vendor should be leveraged.

4.1.4 Apply an Appropriate Level of Risk Control

The level of control must not compromise the visibility of the inherent risk, or the quality / compliance of the system. While maintaining quality is paramount, the applied approach must be scalable and facilitate a proactive and real-time approach to configuration change management. The concept of applied risk from ICH Q9 states, “the level of effort, formality, and documentation of the quality risk management process should be commensurate with the level of risk.” To apply this concept for change oversight of GxP configuration management, the level amount of visibility, confirmation, and qualification varies based on the risk the potential change poses to the system and system product.

4.1.5 Selecting the Right Tool

T 1 R R : E FMEA S T

Y	of the effect of change		

T 2. R C : E FMEA (I) A
S S

4.2.3.3 Qualification

Lastly, changes with potential to impact the validated state of the system and/or end-state controlled content should employ a more robust ‘qualification’ level of control. In the context of this paper, qualification refers to thorough ‘verification of functionality and impact’ with a pre-approved test script. The identified levels of control above allow for a risk-based approach that scales to the complexity of the change.

F 2 A R - C (A) E

4.3 Example of a Change Matrix

Below is a sample change matrix for the Veeva Vault application developed with the risk-based approach for change management.

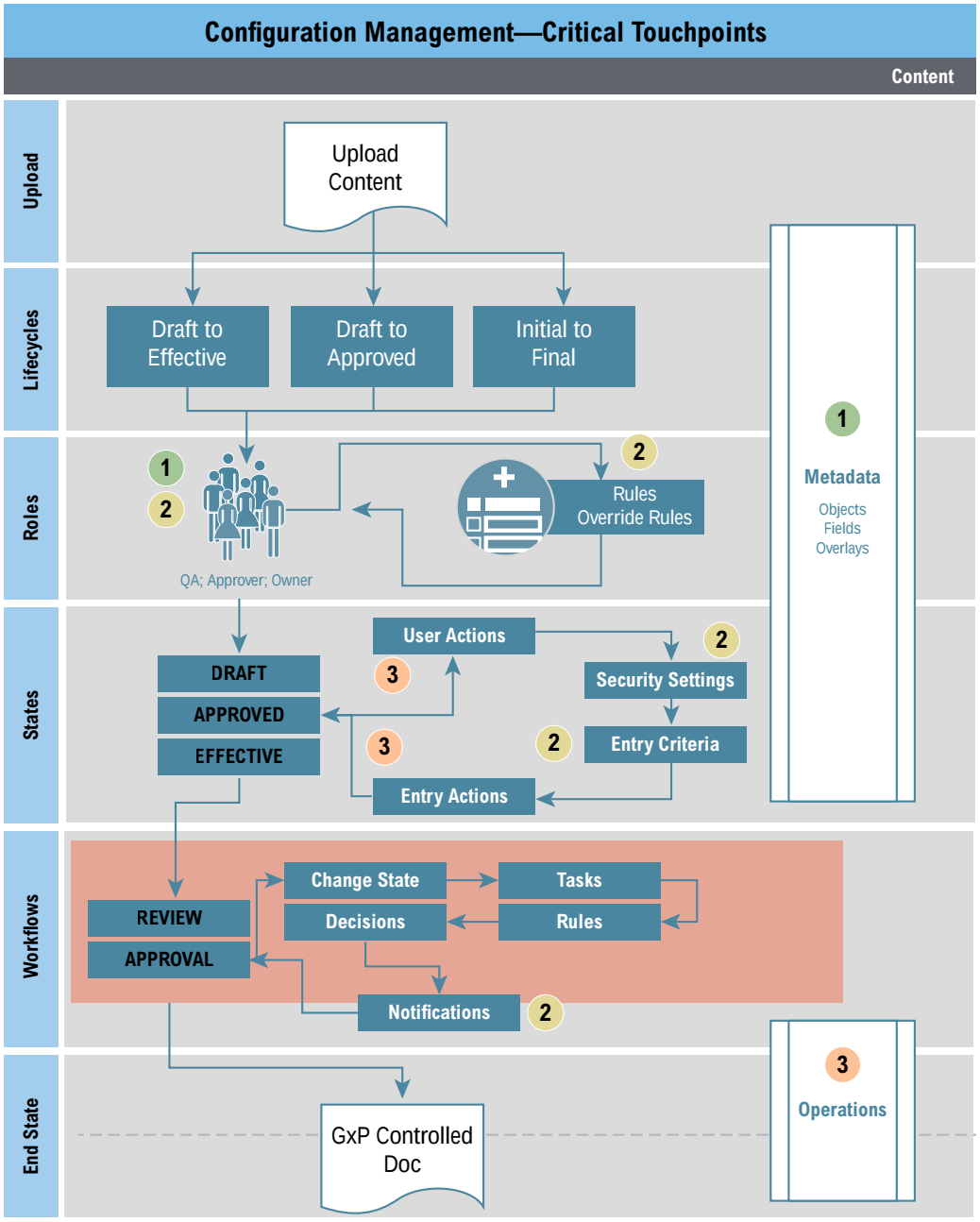
T 5 C M

Business Administration	Application Setup	Facilities	N/A	N/A	Edit/Create	1
		Application Roles	N/A	N/A	Create	1
			Approver	N/A	Edit	2
	emplates	Overlays	Draft to Effective	N/A	Edit/Create	2
Users and Groups	sers and Groups	Groups	Members	N/A	Edit	1
			N/A	N/A	Create	2
		Security Profiles	System Administrator	Members	Edit/Create	2
Configuration	Document Setup	Document Types	Quality	General	Edit	2
				Security	Edit	3
		Document Fields	QA Not Required	N/A	Add/Delete	2
			All Other Fields	N/A	Add/Delete	1
		Field Dependencies	N/A	N/A	Edit/Create	2
	Object Setup	Objects	No orkflow	N/A	Edit/Create	2
			ith orkflow	N/A	Edit/Create	3
	Business Logic	Document Lifecycles: Draft to Effective	States - Draft	ser Actions	Edit/Create	2
				Security Settings	Edit	2
				Entry Actions	Edit/Create	3
			orkflows	Approval	Edit/Create	4
					Capacity	1
Operations	Jobs	Job Definitions	Make Document Effective	N/A	Edit	3
			N/A	N/A	Create	3

5 Critical Touch Points

When identifying areas of risk, it is important to understand all the critical touch points. Developing a diagram enables a more complete understand of impact. In figure below, the area shaded in red shows where a comprehensive change management process is required due to potential high impact.

F 3 C T P



6 Summary

With a well-defined methodology that ensures the depth and breadth of potential configuration changes are well understood, companies reduce the overall time and resources needed to plan, manage, and execute changes and gain a consistent and repeatable process that is defendable in audits and inspections. The guiding document—similar to SOPs—must also be periodically reviewed and updated to reflect new requirements, as regulations or business needs change.

Adopting a risk-based approach to configuration change management enables companies to efficiently keep systems up-to-date, leverage new functionality, and continuously meet business and end-user requirements.

About Veeva Systems

Veeva Systems Inc. is a leader in cloud-based software for the global life sciences industry. Committed to innovation, product excellence, and customer success, Veeva has more than 950 customers, ranging from the world's largest pharmaceutical companies to emerging biotechs. Veeva is headquartered in the < ع ﻍ rea ¡ á ith A Ê s in < urB ∫ ¡ ia ¡ þ M