Veeva Vault

A Risk-based Approach to Change Management of Validated GxP Systems

Position Paper

Contents

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

3 Background

In order to understand the proposed risk-based change approach, it is necessary to understand several perspectives that influenced the development of this paper. This section summarizes these perspectives.

3.1 Validated Environments

Operating in a validated environment requires clear delineation between changes/updates that require a traditional change management process, and those that do not. SOPs that describe how to change a validated system are commonly used as the method for addressing change management. However, increasingly companies also need to explain the impact of a change and why the change is acceptable to make. Simply documenting how to make a change is no longer sufficient.

There are also many human-use factors that complicate change management such as inadequate training that leads to a lack of understanding on the change process. As a result, overly complicated procedures that become daunting to follow for system owners, business administrators, and other support roles are very common. Cumbersome processes often impede system updates and changes that can benefit end users.

3.2 Cloud-Based GxP Applications

With cloud, there is a steady cadence of release updates, introducing more frequent system changes than what has been traditionally experienced in the past. As cloud solutions become more prevalent, required routine updates are expected. Adequate resources are required to keep current with updates, which may not exist in smaller organizations. For larger organizations, the comfort level with cloud applications may be incredibly low, presenting other challenges related to overall adoption and transformation of process. However, with the popularity of consumer web-based applications and smart devices, more users are ready to adopt cloud solutions.

A process to manage system changes from new release updates or business needs must be scalable to prevent compliance gaps and enable the customer to stay up-to-date. To effectively manage the change process for cloud-based GxP applications, organizations must mitigate unnecessary activities, while maintaining an adequate level of documentation to ultimately support and defend the changes.

The term “cloud” is often used to refer to any application that is located outside of an organization’s on-premise computing environment, and accessed across the Internet through a browser. While this is accurate, there are other characteristics of a “cloud” application that have significant impact on an organization’s validation and strategy for managing change. In general, there are two types of “cloud” applications – ‘hosted’ and ‘multi-tenant’. A fundamental difference between hosted and multi-tenant cloud applications lies in how their vendors manage and deliver new versions of their applications to customers.

3.2.1 Hosted Cloud

Hosted cloud applications provide new versions to customers using a traditional on-premise approach. The software vendor notifies customers when a new version is available. Customers decide if they want to upgrade, and when the vendor should perform the upgrade. The vendor upgrades a customer's application, and qualifies the installation (IQ) and operation (OQ) of the upgraded application on behalf of the customer. The customer qualifies the performance (PQ) of the application, and then deploys it for use. Not all customers upgrade to the latest version of a Hosted Cloud application at the same time, and some never upgrade. As a result, Hosted Cloud vendors must support multiple versions of their application.

3.2.2 Multi-tenant Cloud

Multi-tenant cloud applications deliver new versions to all customers at the same time based on a predefined schedule by the vendor. As a result, every customer is always on the latest version of the application and there are no old versions for the vendor to support. Customers are notified in advance when an upgrade will take place. The vendor qualifies the installation (IQ) and operation (OQ) of the application's new features, and the customer pre-qualifies the performance (PQ) of the application in a pre-release environment, prior to the upgrade.

Because multi-tenant applications require all customers to upgrade when a new release becomes available, new features are clearly categorized into two types:

- Automatically Enabled

Automatically enabled features are available for use the moment the upgrade is complete.

- Enabled through configuration

Features that require enablement through configuration can be turned on any time after the upgrade takes place, at the customer's discretion.

The multi-tenant model provides opportunities to assess the risk and impact of change on a validated system at the feature level, and the ability to clearly prioritize assessments based on whether features become available immediately upon upgrade – automatically enabled, or as needed – enabled through configuration.

3.3 Expectations of a Robust Change Process

A robust change process is necessary to efficiently navigate a GxP system through validation, implementation, and steady-state management. While the foundation of this paper is to propose a streamlined approach based on potential change impact, the objective is to facilitate a process whereby there is no compromise to the following:

- The quality of the system's "product"
- The underlying principles of an effective change management program

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.

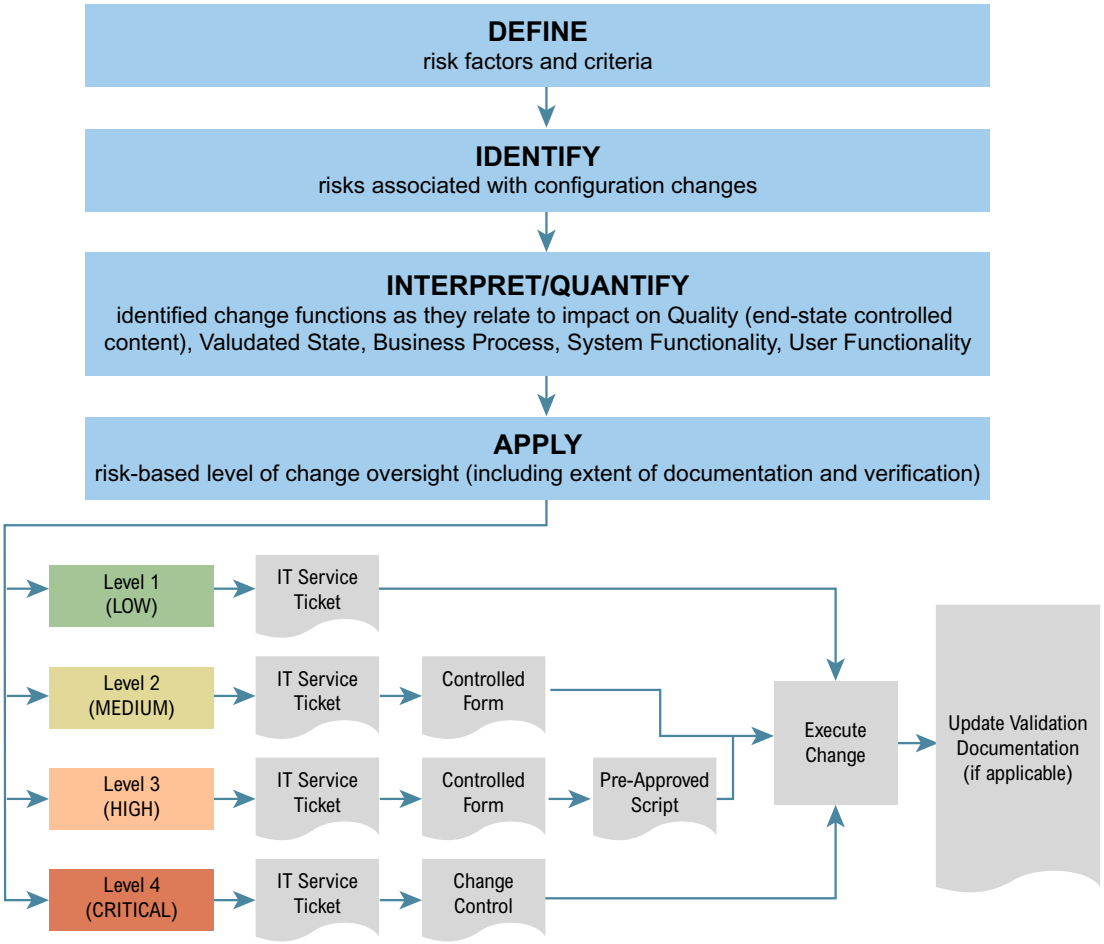
4 Applying a Practical Risk-Based Approach

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."

Figure 1 - Diagram of Risk-based Approach or Proposed Risk Process



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

Within the context of quality risk management there are an abundance of tools that can be leveraged to properly define, identify, interpret, and apply risk. For change management, the risk tool(s) must inclusively analyze: the potential effects of the change, the likelihood that the change is not executed as intended, and the potential the impact is not fully understood due to the complexity of the change. Thus, the ability to detect an unexpected result of a change, or a configuration error, is paramount to ensuring the risk-based process maintains a state of control and the validated state of the system is not compromised. To achieve this broad-spectrum analysis the recommended approach utilizes a failure mode and effects analysis (FMEA) to identify and interpret / quantify the risk associated with configuration changes.

4.2 Risk Framework

4.2.1 Establishment of a Scoring System

To enable risk identification of all potential system changes, a clear scoring process should be established that serves to guide risk determination. Development of scoring definitions specific to GxP systems is recommended to ensure a consistent and defendable approach. While the 'detectability' scores for the FMEA will be largely the same regardless of scope (i.e. drug product risk vs GxP system risk), the 'severity' and 'likelihood' definitions should be modified to fit the purpose:

Severity definitions relating to a GxP system should evaluate potential impact to the following:

- System validation and/or controlled content
- Established business process
- Configured system functionality
- Configured user functionality

Ultimately, the goal of the severity scoring must translate the risk of a configured change to the impact on the quality and compliance.

While the 'likelihood' scoring criteria may remain largely similar to scoring definitions found in traditional drug substance/product risk assessments, the overall scope of the definition should be altered to properly account for unexpected outcomes. In traditional FMEA assessments, the aim is to determine the potential frequency of an undesired event/outcome, whereas for the GxP system the event is being purposefully implemented. Thus the desired outcome and resulting effects are theoretically known. However, due to the complexity of GxP systems and the human element involved in enacting changes, the potential for errors and unexpected outcomes must be considered. Therefore, rather than scoring the likelihood of potential outcomes, the scoring is based on the likelihood for potential errors (i.e. misconfigurations) and misunderstood results; both of which are directly related to the complexity of the configured change.

Table 1 – Risk Rating: Example of a FMEA Scoring Table

Rating	SEVERITY of the effect of change	LIKELIHOOD of occurrence, or misconfiguration, or that change is not fully understood (directly corresponds to the complexity of the change)	DETECTION ability to detect the change
9	**Severe** – Change has potential to impact the validated state of the system and/or the controlled system output.	**Frequent** – Error is almost inevitable. Consistent issues observed	**Absolutely uncertain** – Existing controls cannot detect the change or change error. No controls are in place.
7	**Major** – Change impacts business process with potential impact to controlled system output or validation. Failure to comply with procedural requirements.	**Likely** – Error is likely and will occur in most circumstances. Repeated issues observed	**Remote** – Remote chance that controls will detect the change or change error. A control may be in place but is untested or unreliable
5	**Moderate** – Change has potential to impact system functionality without impact to system output or validation. Possible effect on intermediate stages of content without affect to overall workflows.	**Occasional** – Error is probable at some time and has been observed	**Moderate** – A moderate chance that the control will detect the change or change error.
3	**Minor** – Change has potential to affect user functionality without affect to overall system functionality.	**Unlikely** – Error could occur at some point. Only isolated incidents observed.	**High** – Very likely that the control will detect the change or change error.
1	**Insignificant**- No impact to system/ user functionality, business process, or system output.	**Remote** – Error is extremely unlikely. No incidents observed.	**Almost certain** – The control will detect the change or change error in almost every instance.

4.2.2 FMEA Analysis

Upon establishment of concrete risk definitions, risk identification and scoring can begin. The goal of the FMEA should be to create a full catalog of potential changes and thus a granular approach should be taken to evaluate all aspects of configuration. Cataloging the changes creates a scenario-based risk assessment to evaluate and quantify all associated risks, as well as incorporate the potential for the change to be misconfigured. While all potential areas that may be configured should be evaluated as part of the FMEA, each organization must determine whether the approach will be to evaluate all individual configuration changes within a given section, or if a worst-case approach will be implemented. The resulting analysis will allow for easy identification of risks for both customer-configured changes and changes resulting from system updates. Additionally, this approach will ensure a consistent evaluation of any given change made throughout the lifecycle of the product.

Table 2. Risk Classification: Example FMEA (Identify) of the Veeva Vault Application

S – Severity L – Likelihood D – Detectability

Change Input	Potential Failure Mode	Potential Failure Effects (or worst case scenario)	S	L	D	Risk Level
Create System notification	Notification not distributed to the proper user set	Users are not notified of assigned system tasks	5	3	3	Low
Update document status overlays	Wrong status overlaid on document	Wrong version of document used for controlled operations	7	3	3	Low
Update picklist entries	Wrong field entries added	Incorrect system metadata	5	3	3	Low
Update User security – Add setting to roles	Unintentional privileges added	Ability to progress input through intermediate stages of lifecycle that deviates from business process	7	3	5	Med
Create new system locations/folders	Location/Folder not given proper permissions	Samples/Outputs can't be added and workflow stops	5	5	5	Med
Entry criteria for deletion of minor versions	Minor versions not deleted upon approval	Versions available for viewing during inspections	5	3	5	Med
Create system action for 'Quarantine' state	Action (e.g. lock future tasks) not created with desired function	Intermediate stages of forward processing can occur	7	5	5	High
Create system job to establish automatic effective dates	Incorrect date established	Controlled content released on wrong date	7	5	5	High
Edit Workflow- State Change	Change state is configured incorrectly	Workflow does not proceed to intended state	7	3	7	High
Edit Existing workflow – Next Step	Workflow rules are altered and do not conform to GxP or procedural requirements	QA is potentially skipped as a required approver	9	7	7	Critical

4.2.3 Relating Risk to the System

To interpret risk is to classify the resulting risk scores into different categories requiring varying levels of control. As with the FMEA, the interpretation of risk should allow for a clear understanding of the resulting classification and consistent application. The goal should be to create an unambiguous correlation between the determined risk scores, the risk category, and ultimately the applied controls. For the purposes of the Veeva Vault application, a 4-tiered approach to risk-based control was determined to offer the most effective balance of risk and oversight. A risk categorization table was created to allow for easy translation of 'severity', 'likelihood', and 'detectability' scores into easily understandable categories of: low, medium, high, and critical. While calculation of a risk priority number utilizing the product of a set of risk scores is an equally acceptable method, a risk table was used for this assessment as it allows certain factors to be more heavily weighted, e.g. severity may be weighted more heavily than likelihood. Example of a GxP system risk categorization table is shown below.

Table 3 – Risk Classification (Interpret): Severity

	SEVERITY				
	1 – Insignificant	3 – Minor	5 – Moderate	7 – Major	9 – Severe
9 – Frequent	Medium	Medium	High	High	Critical
7 – Likely	Low	Medium	High	High	Critical
5 – Occasional	Low	Medium	Medium	High	High
3 – Unlikely	Low	Low	Medium	Medium	High
1 – Remote	Low	Low	Low	Low	Medium

Determine an interim result based on the criteria above and then utilize the following table to determine the risk classification.

Table 4 – Risk Classification (Interpret): Detection

	DETECTION				
	1 – Almost Certain	3 – High	5 – Moderate	7 – Remote	9 – Absolutely Uncertain
Critical	Medium	Medium	Critical	Critical	Critical
High	Low	Medium	High	High	High
Medium	Low	Low	Medium	High	High
Low	Low	Low	Low	Medium	Medium

4.2.3 Implementing a Risk-based approach

A primary goal of change management is to provide a high degree of assurance that the change was implemented as intended with no unexpected consequences. When executing risk-based change management, the level of the applied controls should correlate directly to the potential risk – i.e. the control should be sufficient to mitigate the risk, or if the risk has minimal impact on the resulting quality, an acceptable level of control may provide visibility without mitigation. Thus, the overall purpose of the risk assessment is to determine the configuration changes where a reduced level of control is justified based on the understood risk. To achieve this objective, the control methodologies should focus on application of the following aspects: visibility, verification, and qualification.

4.2.3.1 Visibility

Changes that have little to no potential impact on controlled state content or overall functionality (e.g. picklist updates) can be implemented without prior approval. The applied control around these configuration change types need only provide visibility to the change that was enacted.

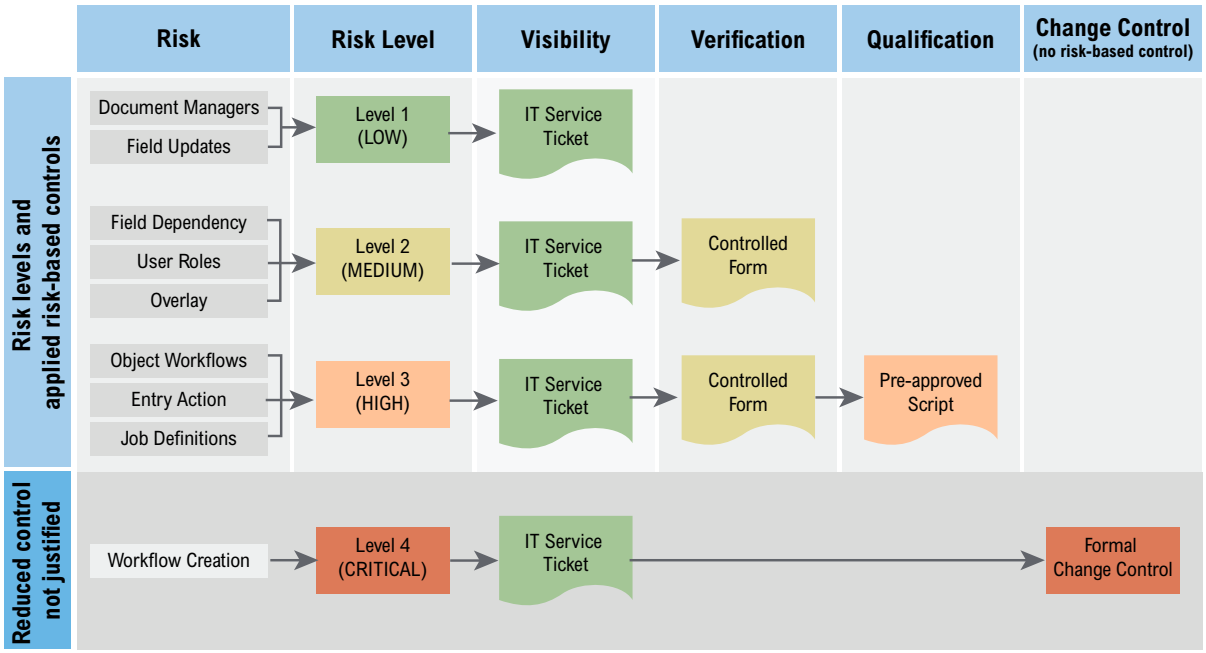
4.2.3.2 Verification

Changes with potential to affect various aspects of system functionality with little to moderate potential impact on controlled state content should add an additional ‘verification’ layer of control. In the context of this paper, the ‘verification’ level of control implies review of the configuration changes by a qualified SME, e.g. filling out a form(s) and / or screen shots, without the need for functionality confirmations.

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.

Figure 2 – Application of Risk-based Control (Apply) Example



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.

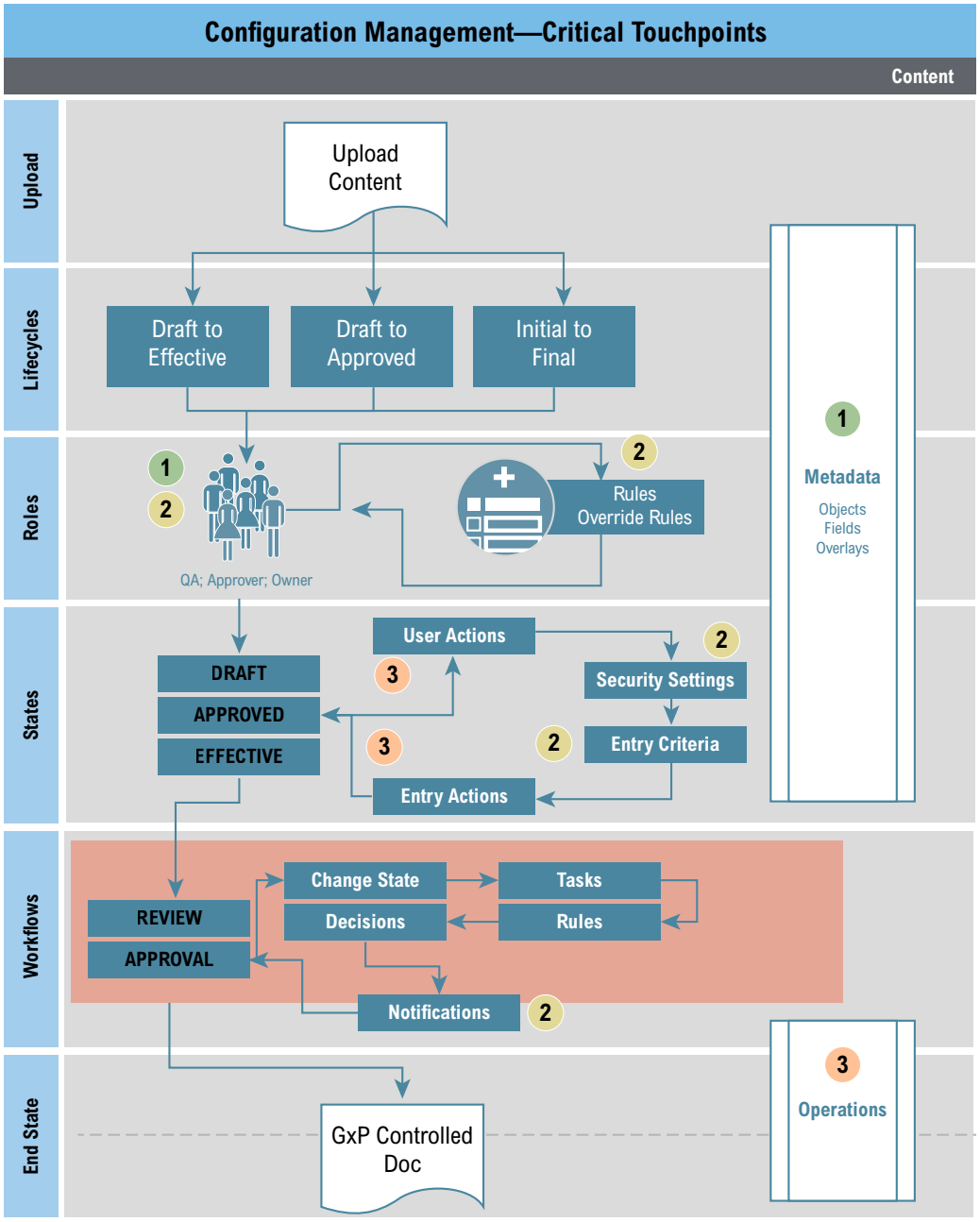
Table 5 – Change Matrix

Tab	Section	Menu	Setting	Input	Change	Change Level
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
	Templates	Overlays	Draft to Effective	N/A	Edit/Create	2
Users and Groups	Users 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 Workflow	N/A	Edit/Create	2
			With Workflow	N/A	Edit/Create	3
	Business Logic	Document Lifecycles: Draft to Effective	States - Draft	User Actions	Edit/Create	2
				Security Settings	Edit	2
				Entry Actions	Edit/Create	3
			Workflows	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.

Figure 3 – Critical Touch Points



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.

Appendix

LIST OF TABLES

LIST OF FIGURES

DEFINITIONS

COTS application
Commercial Off-The-Shelf application. Refers to a packaged IT application offered by a vendor to provide a solution for a specific business need.

Configuration
The process by which a customer makes changes to a COTS application's native features through its system administration capabilities.

Customization
The process by which a customer adds new features, or extends existing features, in a COTS application, through the use of custom code.

Change Management
Governing change through a quality management system/process.

Configuration Change Management
Process and oversight necessary to effectively manage changes to configuration elements of a validated system.

End-State Document Content
This refers to the "product" that results from using an Electronic Document Management System (EDMS). It is the approved, effective, final version of controlled documents.

General Release
The process by which Veeva introduces IQ and OQ qualified new features into customer Vault applications.

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 San Francisco Bay Area, with offices in Europe, Asia, and Latin America. For more information, visit **www.veeva.com/eu**.

+44 (0) 1865 398 190 | veeva.com/eu/contact | veeva.com