Collaborative Authoring with Microsoft Office
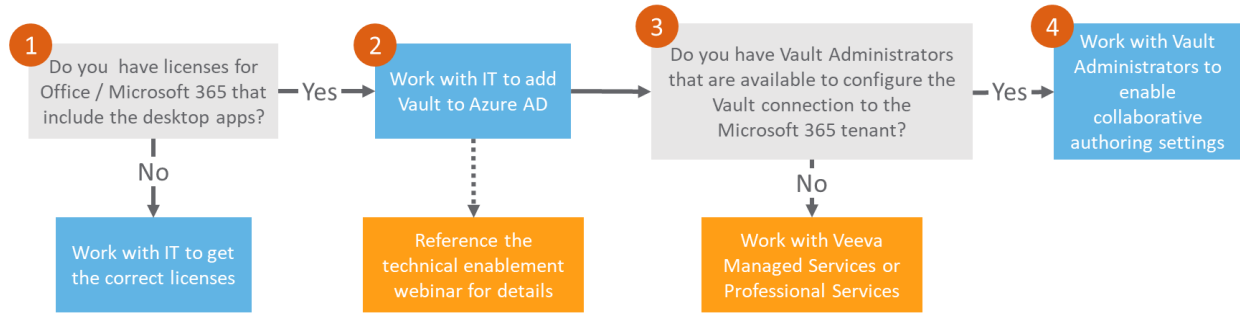## Quick Reference Guide

Collaborative authoring with Microsoft Office™ is available for all Veeva Vault users, but there are several steps to consider before getting started. Use this quick reference guide to understand the technical and business process requirements, as well as which teams to work with to get ready for implementation.

Technical Self-Assessment

1 Do you have licenses for Office / Microsoft 365 that include the desktop apps? — Yes →

2 Work with IT to add Vault to Azure AD →

3 Do you have Vault Administrators that are available to configure the Vault connection to the Microsoft 365 tenant? — Yes →

4 Work with Vault Administrators to enable collaborative authoring settings

- 1 → No → Work with IT to get the correct licenses
- 2 → Reference the technical enablement webinar for details
- 3 → No → Work with Veeva Managed Services or Professional Services

Business Self-Assessment

1 Do all potential authors/reviewers have access to Vault? — Yes →

2 Do you have external partners that help author or edit documents? — Yes →

2a Do they have the correct Office 365 license type? — Yes →

2b Do they have access to Vault? — Yes →

3 Are you using authoring workflows in Vault today? — Yes →

4 Are the existing workflows suitable for collaborative authoring? — Yes →

5 Are you using templates to create the source content and initiate the authoring process? — Yes →

6 Are your templates enabled in Vault? — Yes →

7 Will you need to update the current authoring SOPs and work instructions to account for collaborative authoring in the defined processes and use cases? →

8 Do you have resources available to validate changes to Vault once collaborative authoring and workflows have been updated? — No →

- 2 → No → (to step 3)
- 1 → No → Work with your Account Executive → Train new users on Vault and update security permissions as needed
- 2a → No → Work with IT to acquire the correct licenses
- 2a → Yes → Add them to Azure
- 2b → No → Work with Veeva Account Executive and update security permissions as needed
- 3 → No → Leverage the delivered application authoring workflow, which may require user training
- 4 → No → Consider making updates
- 5 → No → Consider how the workflow initiator will source the content consistently
- 6 → No → Work with IT to enable them
- 7 → Yes → Update SOPs and work instructions
- 8 → No → Identify resources to validate changes after updates

Legend:
- Work with Veeva
- Work with Internal Teams