Template Revision History

Version	Date	Reason for Revision
1.0	January 11, 2026	First issue of the User Manual

AUTHORSHIP		
Name and Organization	**Email ID**	**Date**
Tushal Sajnani Novatio Solutions	Tushal.s@novatiosolutions.com	11-Jan-2026

Vendor Change Management Agent – User Manual

Contents

1. Introduction

Vendor Change Management is a structured and governed process that ensures vendor master data changes are reviewed, validated, approved, and implemented in a controlled manner. The process is designed to balance operational efficiency with strong governance by assessing the risk associated with each change request before execution.

Through intelligent evaluation of vendor-submitted requests, changes are categorized based on severity and business impact. Low-risk changes can be processed automatically to reduce manual effort and turnaround time, while medium- and high-risk changes are routed through defined approval workflows to ensure compliance, accuracy, and accountability. Throughout the process, every decision, approval, and system update is logged to maintain full auditability and traceability.

Overall, Vendor Change Management enables organizations to maintain accurate vendor data, minimize operational risk, and enforce consistent governance while scaling efficiently across large volumes of vendor updates.

2. Executive Summary

The Vendor Change Management Agent is an **agentic automation** that autonomously interprets, decides and acts on vendor master data change requests with embedded governance. The agent reasons over unstructured inputs, evaluates risk using AI Skills, dynamically selects tools, and invokes human oversight only when required.

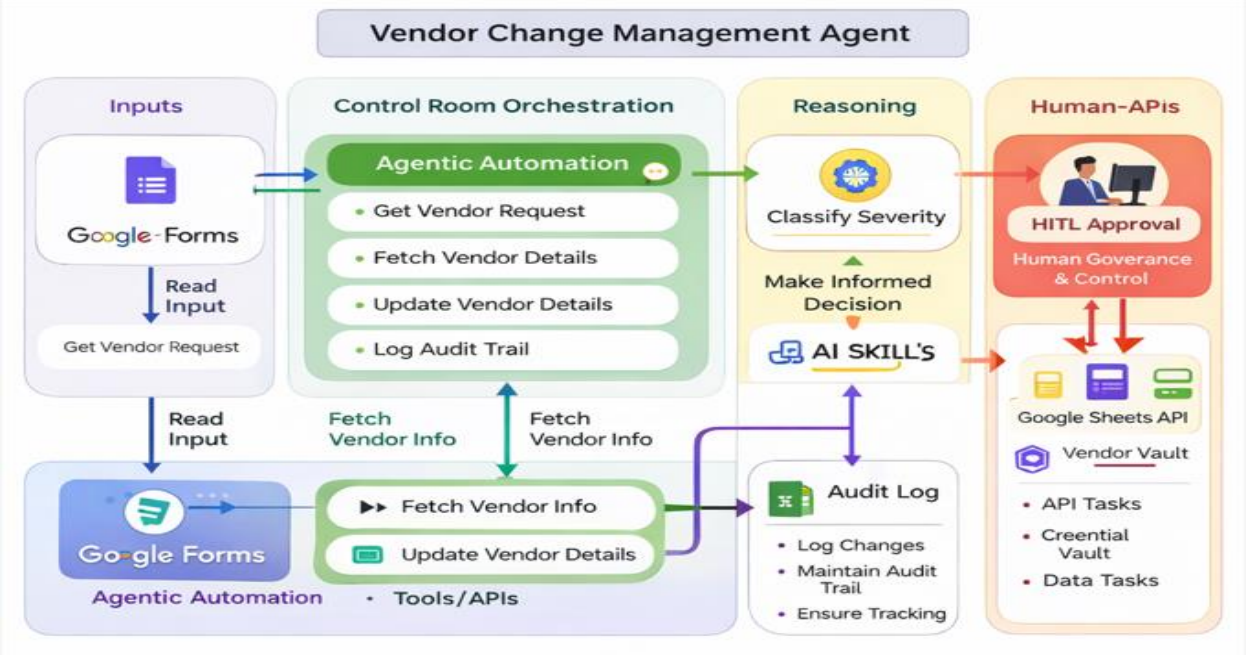
By combining AI-driven classification, conditional tool orchestration, and human-in-the-loop (HITL) approvals, the agent ensures **safe autonomy**: low-risk changes are executed end-to-end without intervention, while medium- and high-risk changes are escalated for human judgment. Every decision and action is auditable, deterministic, and repeatable.

3. Solution Overview

This solution demonstrates **true agentic behavior** using Automation Anywhere. Instead of a linear bot, an AI agent continuously reasons over incoming vendor change requests, decides the appropriate execution path, and dynamically invokes the right tools.

The agent: - Interprets unstructured vendor requests - Classifies risk using an AI Skill - Decides whether human approval is required - Generates context-aware API payloads - Executes partial updates using REST APIs - Logs outcomes for audit and compliance

The design follows an **Observe → Reason → Decide → Act → Learn (log)** pattern, making it scalable and enterprise ready.



4. Key Definitions

Terms	Definitions
Vendor Change Management	A governed process for reviewing, approving, and implementing changes to vendor master data to ensure data accuracy, compliance, and risk control.
Vendor Change Request	A request submitted by a vendor (or internal stakeholder) to update vendor master data such as banking details, contact information, tax data, or other critical attributes.
Vendor Master Data	The authoritative set of vendor-related information stored in enterprise systems and used across procurement, finance, and payment processes.
AI Agent (Agentic Automation)	An intelligent automation component that observes incoming requests, reasons over inputs, makes decisions based on defined rules and AI insights, and executes actions autonomously or with human oversight when required.
Severity Classification (Risk Level)	An AI-driven assessment that categorizes vendor change requests as **Low**, **Medium**, or **High** risk based on potential business, financial, or compliance impact.
Low Severity Change	A vendor change request with minimal risk that can be executed autonomously without human intervention.
Medium Severity Change	A vendor change request with moderate business impact that requires explicit human approval before execution.
High Severity Change	A vendor change request with significant financial, regulatory, or operational risk that mandates human review and approval prior to implementation.
Human-in-the-Loop (HITL)	A controlled approval mechanism where human reviewers validate or reject vendor change requests identified as Medium or High severity by the AI agent.
AI Skill	A reusable AI capability used by the agent to perform specific tasks such as severity classification or dynamic generation of API payloads.
JSON Payload	A structured data object generated by the AI Skill to represent approved vendor changes, used for partial updates through REST APIs.
Partial Update (PATCH Request)	An API-based update mechanism that modifies only approved and relevant vendor fields without impacting unchanged master data.
Audit Log / Traceability	A complete record of vendor requests, severity decisions, approvals, payloads, and execution outcomes maintained for compliance and audit

	purposes.

---

5. Key Benefits

- **AI-Driven Risk Classification**: Automatically evaluates vendor change requests and assigns severity levels.
- **Reduced Manual Effort**: Low-risk changes are processed automatically without human intervention.
- **Strong Governance**: Medium and high severity changes require explicit human approval.
- **Audit Readiness**: All requests, approvals, and updates are logged for traceability.
- **Scalable Design**: Supports multiple vendor requests processed sequentially without data conflicts.

---

6. Core Components

- **Google Forms Integration**
  Retrieves vendor change requests submitted by vendors.

- **AI Agent (Agentic Automation)**
  Orchestrates the workflow, tool execution, decision logic, and approvals.

- **AI Skill – Severity Classifier**
  Analyzes vendor change request text and classifies severity as Low, Medium, or High.

- **Human-in-the-Loop (HITL)**
  Captures approvals or rejections for medium and high severity requests.

- **AI Skill – JSON Payload Generator**
  Generates dynamic PATCH API request bodies for vendor updates.

- **Vendor Master API Integration**
  Applies approved updates to vendor records using REST APIs.

---

7. Agentic Process Flow

7.1 Pre-requisites

- Automation Anywhere Control Room access with Agentic Automation enabled
- AI Skills access
- Google Forms with vendor change request submissions
- Vendor Master system with REST API access
- Valid credentials for all integrated systems

7.2 Step-by-Step Workflow (Agent Reasoning)

The process follows a governed, step-by-step workflow ensuring data accuracy and compliance.

1. **Observe – Intake Vendor Request**
   The agent retrieves vendor change requests submitted via Google Forms using the *Get Vendor Request from Google Form Tool*.

2. **Reason – Risk Evaluation**
   Each request is analyzed by the *Classify Vendor Change Request Severity* AI Skill to determine business risk (Low / Medium / High).

3. **Decide – Governance Path Selection**

   - **Low Severity** → Autonomous execution

   - **Medium / High Severity** → Human-in-the-Loop approval required

4. **Act – Human Oversight (Conditional)**
   For Medium and High severity requests, the agent pauses execution and requests explicit approval or rejection via HITL.

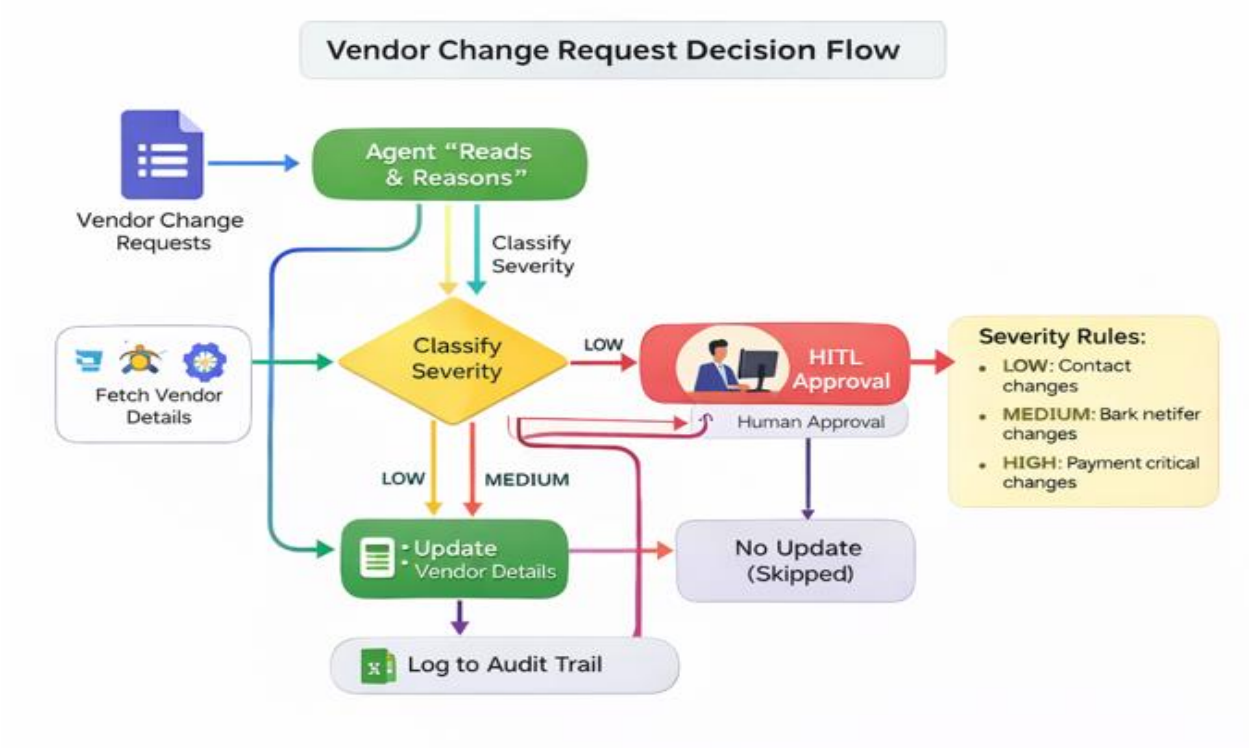
5. **Act – Data Context Retrieval**
   For approved requests, the agent retrieves vendor context (Vendor ID and master data) using the *Fetch Vendor Details Tool*.

6. **Reason – Payload Construction**
   The *Create JSON for Vendor Update* AI Skill dynamically generates a PATCH payload containing only approved and relevant fields.

7. **Act – System Update**
   The agent applies the update using the *Update Vendor Details Tool* via REST API.

8. **Learn (Log) – Audit & Traceability**
   The agent logs severity, approval decision, payload, and update status before

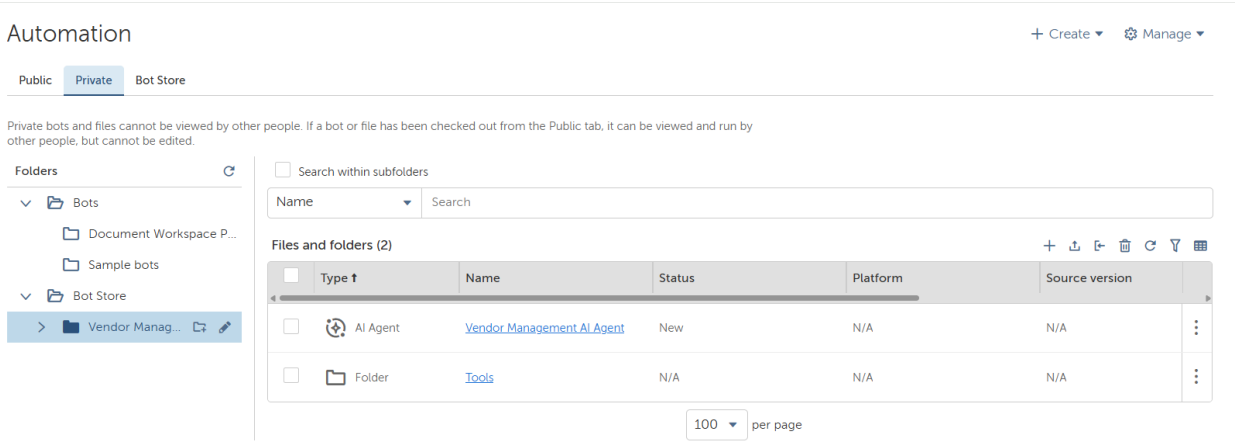
moving to the next request.



8. Usage Guide

8.1 AI Agent

The Vendor Change Management Agent coordinates the execution of tools, AI Skills, approval steps and decision logic. It ensures requests are processed sequentially to maintain data consistency.

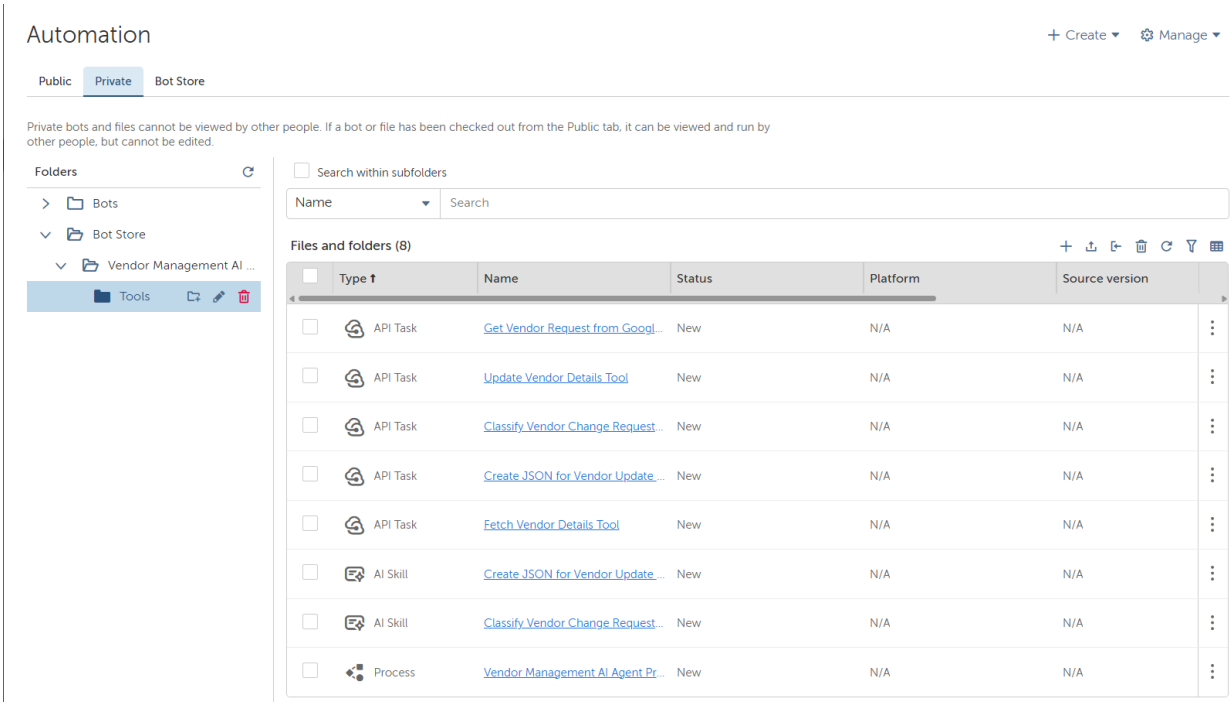


8.2 Tools

- Get Vendor Request from Google Form Tool
- Classify Vendor Change Request Severity Tool
- Fetch Vendor Details Tool
- Create JSON for Vendor Update Tool
- Update Vendor Details Tool
- Human-in-the-Loop Approval Tool

8.2.1 Table : Tool Details

Sr No	Tool Name	Description
1	Vendor Change Management Agent	End-to-end agent orchestrating the workflow
2	Get Vendor Request from Google Form Tool	Retrieves vendor change requests
3	Classify Vendor Change Request Severity Tool	AI Skill to classify severity
4	Fetch Vendor Details Tool	Retrieves vendor ID and master data
5	Create JSON for Vendor Update	AI Skill to generate PATCH payload
6	Update Vendor Details Tool	Apply vendor updates via API
7	HITL Approval Tool	Captures human approval decisions



8.3 How to Execute

- Execute the **Vendor Change Management Agent** process.
- Monitor execution via the Automation Anywhere Control Room.
- Provide approvals for Medium and High severity requests when prompted.
- Allow the agent to complete processing automatically.

---

9. Troubleshooting

Issue	Probable Cause	Agentic Resolution
Incorrect severity	Ambiguous request text	Refine AI Skill prompt or add examples
Approval not triggered	Severity misclassified	Review classification rules
API update failure	Invalid payload	Agent validates JSON before execution
Partial update missing	Field not approved	Agent omits unapproved fields

Issue	Probable Cause	Resolution
Vendor update failed	Invalid JSON payload	Validate AI Skill output before API call
Approval not triggered	Incorrect severity classification	Review AI Skill rules and prompts
API error	Credential or endpoint issue	Verify API credentials and endpoint URLs

---

10. Important Notes

- Credentials used in this solution are for demonstration purposes only.
- Ensure secure credential storage before using the solution in production.
- AI-generated outputs should be periodically reviewed to maintain data accuracy.