

Functional Specification Document (FSD) - Model Risk Management (MRM) MRM Vault

AMENDMENT HISTORY				
VERSION	EFFECTIVE DATE	CREATED BY	REVIEWED BY	APPROVED BY
1.0	08-October-2025	Harsha B	Gaurav K	Prithivi P
1.1	27-October-2025	Harsha B	Gaurav K	Prithivi P

Table of Contents

1	Purpose.....	3
1.1	Purpose.....	3
1.2	Scope	3
1.3	References.....	3
2	Solution Overview.....	3
2.1	Business Problem Statement.....	3
2.2	High-Level Architecture of MRM Vault.....	4
	MRM Vault – Three-Tier Architecture.....	4
2.3	Stakeholders & Personas	5
3	Approach	7
	Requirement:.....	7
4	Business Requirements.....	9
4.1	Functional Requirements.....	11
4.1.1	Roles.....	11
4.1.2	Attributes	15
4.1.3	Form Templates	20
4.1.4	Configuration Table	26
4.1.5	Workflows.....	31
4.1.6	Emails	38
4.1.7	Notifications	44
4.1.8	Reports.....	49
4.1.9	Dashboards	53
4.1.10	Attestation Process.....	66
4.1.11	Change Management	68
4.1.11	Migration.....	80
4.1.13	Archival and Retention	83
4.1.14	Audit and Logging	86
4.1.15	External Approval Process	91
4.2	Non-Functional Requirements.....	93
5	Project-Level Assumptions	96
6	Key Dependencies	97

1 Purpose

1.1 Purpose

- The purpose of this Functional Specification Document (FSD) is to define how the MRM Vault platform will be configured, customized, and implemented to operationalize HDFC Bank's Model Risk Management (MRM) Governance and Model Inventory Framework as outlined in the approved Business Requirement Document (BRD) and accompanying annexures as shared for 'Sprint 1'.
- This document provides a detailed configuration blueprint translating the Bank's MRM Policy, governance principles, and process requirements into system design elements within MRM Vault. It specifies the functional and non-functional configurations/enhancements needed to enable structured model registration, lifecycle governance, validation tracking, change management, monitoring, and decommissioning, all within a single, auditable, and role-driven digital environment.
- Through this implementation, MRM Vault will become HDFC's centralized system of record for all models, providing end-to-end transparency, automated workflow controls, versioned audit trails, and regulatory-grade compliance. The configuration ensures alignment with HDFC Bank's internal risk-governance standards, enterprise security requirements, and supervisory expectations, thereby strengthening governance integrity, operational efficiency, and regulatory defensibility across the model lifecycle.

1.2 Scope

- In scope: Model registration workflow, model inventory workflow, notifications, TAT/SLAs, inventory, reports, roles/RBAC, integrations (SSO/LDAP/Power BI).
- Out of scope: Custom code, non-agreed integrations, bespoke regulatory packs, data science model training, PDV & Monitoring Satellite processes.

1.3 References

- REF-01: BRD_Main.docx
- REF-02: Attribute_List.xlsx
- REF-03: Workflow_Images.zip
- REF-04: Reporting_Requirements.xlsx
- REF-05: TAT_SLA_Rules.xlsx

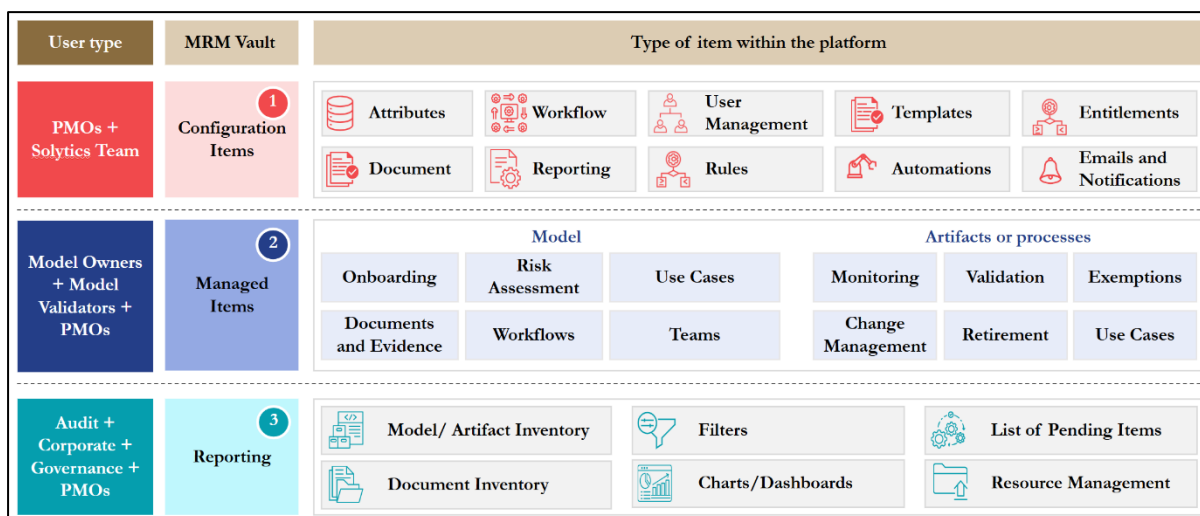
2 Solution Overview

2.1 Business Problem Statement

- HDFC Bank currently manages its model inventory and related governance processes using decentralized, Excel-based repositories and manual workflows distributed across multiple business units. This fragmented operating model has led to data inconsistencies, limited traceability, delayed validations, and governance blind spots, making it difficult to demonstrate comprehensive lifecycle control and compliance with regulatory expectations under the MRM Policy.

- The absence of a centralized, auditable, and role-governed system of record has increased operational effort and dependency on manual coordination between teams. Model approvals, validations, monitoring, and change management activities are tracked in isolation, often through email-based exchanges, which limits oversight and creates challenges in maintaining timely updates, evidence retention, and version-controlled audit trails.
- To address these gaps, MRM Vault will be implemented & configured by Solytics Partners with the help of HDFC Bank stakeholders. MRM Vault is a centralized Governance and Model Inventory Management platform designed to provide full lifecycle oversight of models by capturing all model-related data, documentation, validation records, governance actions, and performance metrics in a unified, configurable, and fully auditable environment. The new system - MRM Vault - will provide HDFC with a single source of truth for model inventory and lifecycle management, enabling automation of workflows, real-time dashboards for oversight, consistent policy enforcement, and regulatory-grade traceability. This transformation will significantly enhance governance integrity, operational transparency, and regulatory defensibility across the model lifecycle.

2.2 High-Level Architecture of MRM Vault



MRM Vault – Three-Tier Architecture

MRM Vault follows a **three-tier architecture** designed to segregate responsibilities, maintain governance integrity, and ensure end-to-end traceability across the model lifecycle.

- **Tier 1 – Configuration Layer (Config Admins):** Managed by configuration administrators, PMOs, this layer defines the system backbone — setting up attributes, workflows, templates, rules, automations, user roles, and reporting structures. It provides the foundational governance framework upon which all model lifecycle processes operate.

- **Tier 2 – Model Lifecycle Layer (FLOD/SLOD Users):** This is the operational core where **First Line and Second Line of Defense users** manage actual model creation and its subprocesses across the lifecycle — from onboarding, risk assessment, validation, monitoring, and change management to retirement. It represents day-to-day model governance and execution activities.
- **Tier 3 – Oversight and Reporting Layer (Audit, Corporate Governance, PMO, Management):** Focused on transparency and assurance, this layer enables governance teams, audit functions, and senior management to monitor model inventory, review lifecycle statuses, analyze risk exposures, and generate dashboards and reports for oversight and regulatory compliance.

Together, these tiers establish a **controlled yet flexible governance architecture**, ensuring configurability at the foundation, structured model management at the core, and continuous oversight at the top.

2.3 Stakeholders & Personas

Category	Stakeholder / Persona	Primary Responsibilities in MRM Vault
Business Stakeholders	Model Owners / Model Developers	Responsible for initiating model registration, completing metadata, uploading supporting documentation, and submitting models for validation and governance review.
	Business Unit Heads / Sponsors	Provide business justification and oversight for models developed within their units; approve submissions and ensure governance compliance.
Governance Stakeholders	MRM Oversight / Governance Team	Administers workflows, templates, and attributes. Reviews change requests, manages attestations, monitors SLA adherence, and ensures compliance with the Bank's MRM Policy.
	Model Risk Committee (MRC)	Provides final sign-offs and governance approvals for model lifecycle transitions, decommissioning, and exceptions.
Validation Stakeholders	Model Validators / Independent Validation Team (IVU)	Conduct pre-deployment validations (PDV), review model performance, record validation findings, and upload reports and evidence to MRM Vault.

	Validation Head / Validation Committee	Approves validation outcomes, manages exceptions, and ensures adherence to validation SLAs.
Monitoring & Performance Stakeholders	Monitoring Analysts / Risk Analytics Team	Upload periodic monitoring reports, record exceptions, and track remediation progress within the platform.
	Business Risk Teams	Review monitoring results and assess material impacts, ensuring corrective measures are initiated.
Change Management Stakeholders	Change Request Initiators (Business or Risk Users)	Raise model or attribute-level change requests and provide impact details and supporting documentation.
	Governance Approvers	Review, approve, or reject change requests and ensure all changes follow defined governance and audit protocols.
Technical & Support Stakeholders	System Administrators (MRM Admins)	Manage platform configuration, user access, and parameter tables. Maintain templates, workflows, and dashboards per governance-approved structures.
	HDFC IT / Enterprise Architecture (EA) / ISD	Ensure the system meets enterprise security, infrastructure, and information security standards. Responsible for hosting, VPN, SFTP, and related infrastructure approvals.
Project Governance	HDFC PMO / Program Sponsors	Provide project-level oversight, approve FSDs and Go-Live milestones, and ensure alignment with overall MRM transformation objectives.
End-Users	All Authorized Users (Viewers, Contributors, Reviewers)	Access dashboards, reports, and lifecycle status information relevant to their assigned roles and permissions.

3 Approach

Requirement:

The approach for implementing this framework is twofold:

- System-enabled Sequential Workflow, and
- Inventory update through Non-Sequential Workflow.

This is required to ensure that the MRM system can support both governed, rule-driven model lifecycle transitions and flexible inventory management operations without compromising auditability or data integrity.

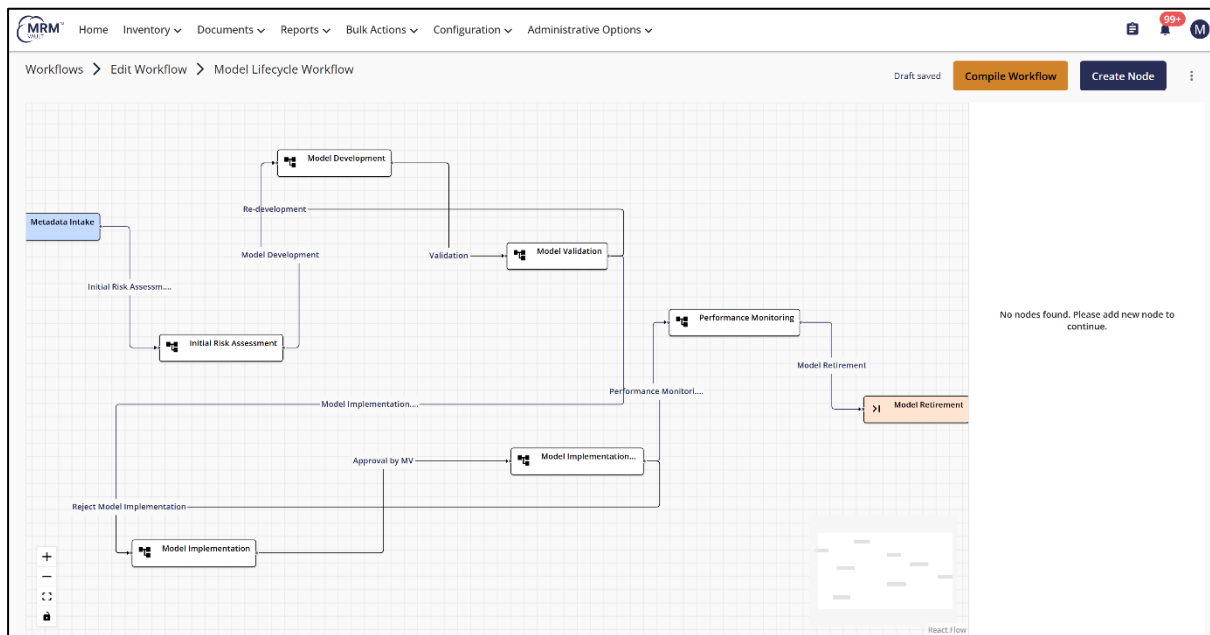
Our Understanding:

expects the system to manage models using two complementary modes of operation:

- Sequential (Governed) Workflow: A structured, rule-based progression through predefined model lifecycle stages such as Registration → PDV → Deployment → PTT → Monitoring → Mitigation → Decommission, with approval gates and validations at each transition.
- Non-Sequential (Inventory Update) Workflow: Controlled flexibility for direct updates or bulk uploads to inventory metadata, used in scenarios like model onboarding, metadata corrections, or regulatory reconciliations. Both flows must maintain full audit trails, access control, and data consistency.

Solytics Response:

Requirement	How MRM Vault Handles This	Status
System-Enabled Sequential Workflow	MRM Vault provides a configurable workflow designer to define model lifecycle stages, transitions, roles, and approval rules. Each model follows the configured sequential path, ensuring governance alignment. Pre-conditions, validations, and maker-checker approvals are enforced at every transition. All stage movements and decisions are logged in the audit trail with timestamp, user, and comments.	Configuration Required
Inventory update through Non-Sequential Workflow.	The Bulk Upload feature in MRM Vault enables authorized users to create or update multiple models or lifecycle stages simultaneously using Excel templates . These templates can be directly downloaded from the Bulk Upload interface for the selected model types, updated with required details, and re-uploaded into MRM Vault for processing. The platform supports bulk model upload, update, and lifecycle transition for Individual or large number of Models. MRM Vault ensures that all related metadata, ownership assignments, and governance attributes are updated consistently and accurately across models, enabling efficient large-scale data management without IT dependency.	Configuration Required



Reference Image 1: Sequential workflow: Workflow starts at Metadata Intake and ends with Model Retirement, processed in a sequential manner through different user roles.

Bulk Transition

Search

Bulk Action **Bulk Transition History**

<input type="checkbox"/> SELECT ALL	Unique ID	Entity Name	entity type	template name	workflow name	current state	CREATED ON	entity alias	entity code	Request Type
<input checked="" type="checkbox"/>	CR-373	Mitigation Email U	ModelInventory	Change Request	Change Request	Closed	10/26/2025	Mitigation Email U	373	ModelRequest
<input checked="" type="checkbox"/>	CR-372	Monitoring Attribu	ModelInventory	Change Request	Change Request	Change Execution	10/26/2025	Monitoring Attribu	372	ModelRequest
<input checked="" type="checkbox"/>	CR-371	Retirement Templ	ModelInventory	Change Request	Change Request	Review	10/26/2025	Retirement Templ	371	ModelRequest
<input checked="" type="checkbox"/>	CR-370	Workflow Enhance	ModelInventory	Change Request	Change Request	Approved	10/26/2025	Workflow Enhance	370	ModelRequest
<input type="checkbox"/>	MIT-364	Liquidity Risk Asse	ModelInventory	Model Identificat	Model Identificat	MO to start model	09/19/2025	Liquidity Risk Asse	364	ModelRequest
<input type="checkbox"/>	EUA-343	Loan Default Prob	ModelInventory	EUC Candidate an	EUC Registration a	EUC Registration	09/17/2025	Loan Default Prob	343	ModelRequest
<input type="checkbox"/>	EUA-333	EUC Assessment fr	ModelInventory	EUC Candidate an	EUC Registration a	EUC Registration	09/17/2025	EUC Assessment fr	333	ModelRequest
<input type="checkbox"/>	EUF-323	EUCs due for Q4 C	ModelInventory	EUC Control Form	EUC Control Form	Control Review Lai	09/16/2025	EUCs due for Q4 C	323	ModelRequest

Select models

Search

Bulk Transition

<input checked="" type="checkbox"/> SELECT ALL	UNIQUE ID	MODEL NAME	WORKFLOW NAME	CURRENT STATE	NEXT STATE
<input checked="" type="checkbox"/>	CR-373	Mitigation Email Updatio	Change Request	Closed	Change Execution
<input checked="" type="checkbox"/>	CR-372	Monitoring Attribute Ch	Change Request	Change Execution	Closed
<input checked="" type="checkbox"/>	CR-371	Retirement Template Ad	Change Request	Review	Initiation Draft
<input checked="" type="checkbox"/>	CR-370	Workflow Enhancement	Change Request	Approved	Change Execution

Show: 5 rows 1-4 of 4 < 1 >

Action name: Enter action name **NEXT**

Reference images 2 & 3: Bulk Transition; Authorized users can select multiple models/lifecycle events and transition them non-sequentially or sequentially to any stage in the workflow for quick and efficient Inventory management.

4 Business Requirements

Requirement:

The Inventory Workflow is designed to capture, manage, and govern all models that fall within the scope of the Model Risk Management (MRM) Policy.

It must ensure:

- Structured registration, versioning, and updates for all models.
- Controlled workflows for pre-development validation (PDV), deployment, post-implementation testing (PIT), monitoring, mitigation, and decommissioning.
- Centralized governance, transparency, and auditability.
- Role-driven access ensuring secure model data management.
- Full adherence to internal governance and compliance standards.

Note: Artifacts/Satellite workflows and the connected requirements are to be further developed based on BRDs for Sprint 2 and will be addressed in response of FSD for the same, for PDV on 31st Oct & Monitoring on 7th Oct.

The overall objective is to create a centralized, transparent, and auditable system of record that maintains model lifecycle integrity and enables traceability from inception to retirement.

Our Understanding:

The client requires an end-to-end inventory governance framework that manages all models and related artifacts in a structured and compliant manner throughout their lifecycle.

The system must:

- Serve as the single source of truth for all model metadata, documentation, and approvals.
- Support workflow-driven governance aligned with the MRM Policy — from registration to decommissioning.
- Maintain full traceability, auditability and transparency for each lifecycle stage.
- Provide role-based visibility and control over model activities, ensuring segregation of duties (e.g., Maker, Checker, Approver).
- Offer complete auditability of model actions, status changes, validations, and approvals.
- Uphold information security and regulatory compliance across all modules.

The workflow thus forms the governance backbone of the MRM framework — ensuring consistency, accountability, and defensibility across the model lifecycle.

Solytics Response:

Requirement	How MRM Vault Handles This	Status
Centralized Model Inventory	MRM Vault serves as a single, centralized repository for all models governed under the MRM Policy. Each model record captures structured	Out of the Box

	metadata (e.g., model type, owner, materiality, risk tier, intended use), ownership lineage, and linked documentation (methodology note, validation report, approval artifacts, etc.). Governance enforcement is achieved via mandatory field validation and workflow-based review and approval checkpoints.	
End-to-End Lifecycle Governance	The platform enables configurable, workflow-driven governance across all lifecycle stages, from registration and PDV through deployment, PIT, monitoring, mitigation, and decommissioning. Each workflow enforces stage-specific validations, maker-checker reviews, and approval of checkpoints. Traceability is maintained across model versions, linked artifacts (validation cycles, monitoring cycles), and approvals via immutable audit trails.	Configuration Required
Structured Registration & Versioning	Models are created using predefined, configurable templates based on model category (statistical, AI/ML, vendor, etc.), ensuring standardized metadata capture. Version control is system-managed; each update is automatically versioned with timestamps, user IDs, and approval references, ensuring complete historical traceability.	Out of the Box
Governance & Compliance Alignment	The lifecycle workflows and metadata configurations are designed to align with the Bank's MRM Policy and regulatory expectations, ensuring all models undergo required validations and reviews.	Configuration Required
Role-Based Workflow Execution	MRM Vault's Role-Based Access Control (RBAC) ensures segregation of duties by assigning granular permissions for model owners, validators, reviewers, and oversight users. Role assignments are dynamic (based on model ownership or workflow stage). Approval gates are enforced via workflow configuration.	Out of the Box
Transparency & Auditability	Each model's metadata, lifecycle transitions, and document uploads are logged with timestamps and user IDs, ensuring a complete audit trail accessible for governance and regulatory reviews through the dedicated logs added in configuration menu for metadata, templates, workflows, automations, email templates and user access management.	Out of the Box
Secure Model Data Management	All model-related data and documents are encrypted (AES-256), access-controlled, and	Out of the Box

	governed by enterprise-grade security aligned with ISO 27001 and SOC2 standards. Role-based permissions prevent unauthorized modification or download.	
Reporting & Visibility	Configurable dashboards and reports provide real-time visibility into inventory composition, lifecycle progress, validation and monitoring status, ownership, and governance KPIs. Users can customize filters, date ranges, and risk indicators to align with internal reporting and audit requirements.	Configuration Required

4.1 Functional Requirements

4.1.1 Roles

Requirements:

The MRM system must embed a clear, consistent, and regulator-aligned role framework to ensure accountability, segregation of duties, and transparency across the model lifecycle. Roles must define responsibilities, authorities, and access rights (read, write, approve, administer), be applied consistently across all lifecycle stages, and support auditability, configurability, and regulatory defensibility.

Our Understanding:

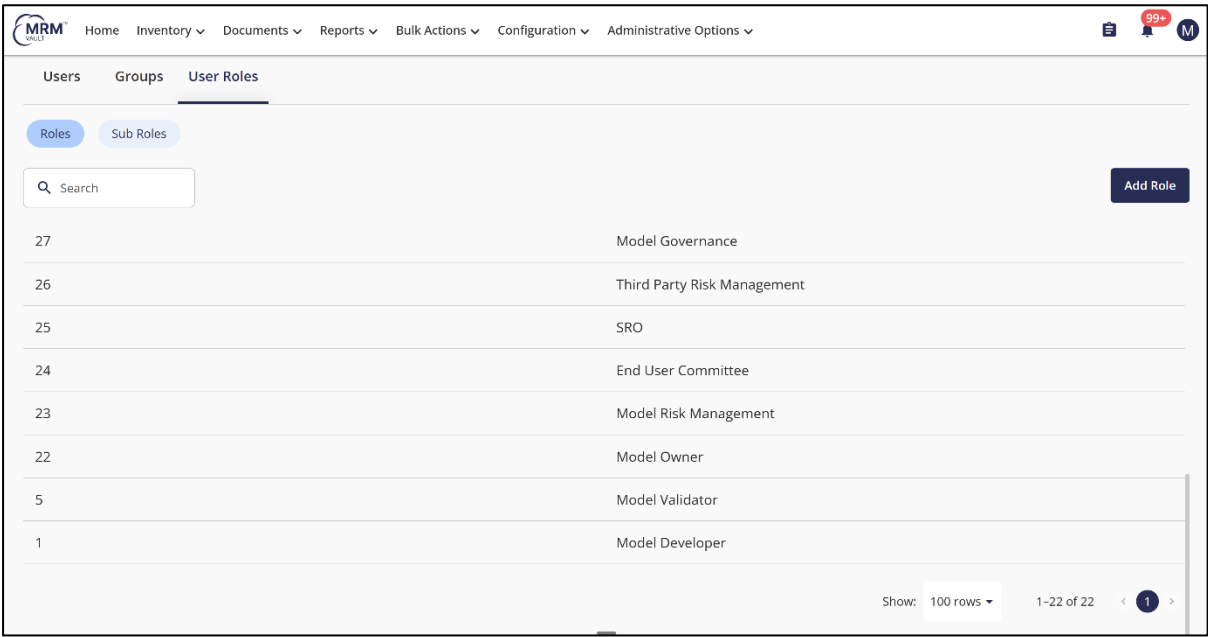
Roles must be centrally defined and mapped to responsibilities across the lifecycle stages of registration, validation, monitoring, change management, and decommissioning. Role-based permissions should be granular and enforce segregation of duties, ensuring no overlaps or conflicts. The framework must support flexible updates to adapt to governance or organizational changes, while maintaining audit trails and compliance with regulatory requirements.

Solytics Response:

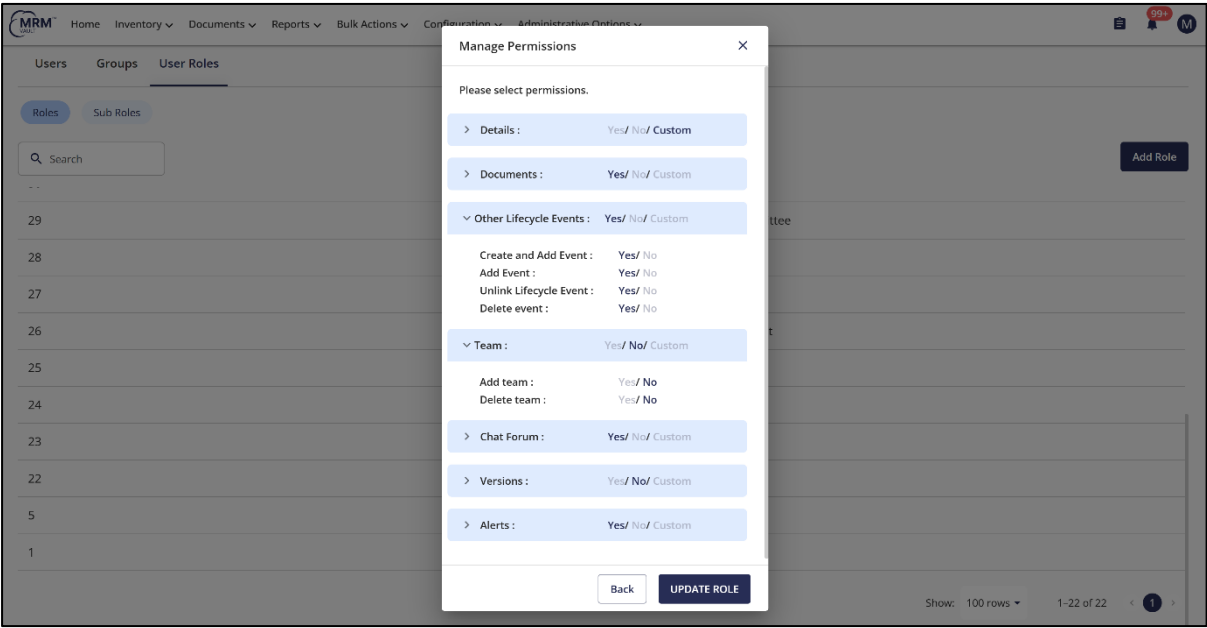
Requirement	How MRM Vault Handles This	Status
Clear Accountability	MRM Vault enforces mandatory role assignments through system-level validations that prevent workflow progression without a defined role owner. Each role (e.g., Model Owner, Validator) is pre-mapped to workflow stages with corresponding responsibilities and privileges. Audit logs maintain a continuous trace of ownership and approvals from model creation to decommissioning. (Configuration involves mapping role templates to bank-specific workflow stages.	Configuration Required

Role-Based Access Control (RBAC)	The User Management module empowers administrators to define user roles and assign granular permissions across both module and model levels. These permissions include actions such as View, Edit, Approve, and Manage Templates. To ensure robust governance, the system also supports maker-checker alerts, which prevent users from approving their own actions, thereby enforcing proper separation of duties.	Configuration Required
Flexibility & Configurability	MRM Vault supports self-service role administration for authorized MRM Admins, enabling creation, modification, or retirement of roles without technical intervention. Changes to critical roles trigger approval from Super Admins. The system supports hierarchical role structures, allowing governance bodies (e.g., AI Governance Committee, Model Risk Council) to inherit relevant privileges while maintaining audit visibility.	Out of the Box
Consistency Across Lifecycle	MRM Vault enforces consistent role and permission application across all lifecycle workflows through standardized workflow templates. Each stage (registration → validation → monitoring → mitigation → decommissioning) references the same role mapping library to ensure consistent accountability and segregation of duties across processes.	Configuration Required
Transparency & Auditability	MRM Vault logs every role-based action (who, what, when) in an immutable audit trail accessible via dashboards and exportable reports. SLA and approval tracking dashboards can be customized by role type (e.g., Validator view vs. Oversight view) for transparency and operational control.	Out of the Box
Alignment with Governance	MRM Vault enables governance alignment through configurable role-policy mappings that link internal governance functions (e.g., Risk Oversight, Validation Committee) to workflow checkpoints. Roles can be embedded in approval hierarchies and policy-driven task sequencing to ensure compliance with the Bank's governance charter.	Configuration Required
Regulatory Defensibility	The system provides regulator-ready audit trails capturing all role-based actions, ensuring traceability for internal and external audits. Oversight roles can monitor breaches or exceptions through automated alerts, generate compliance reports, and trigger	Out of the Box

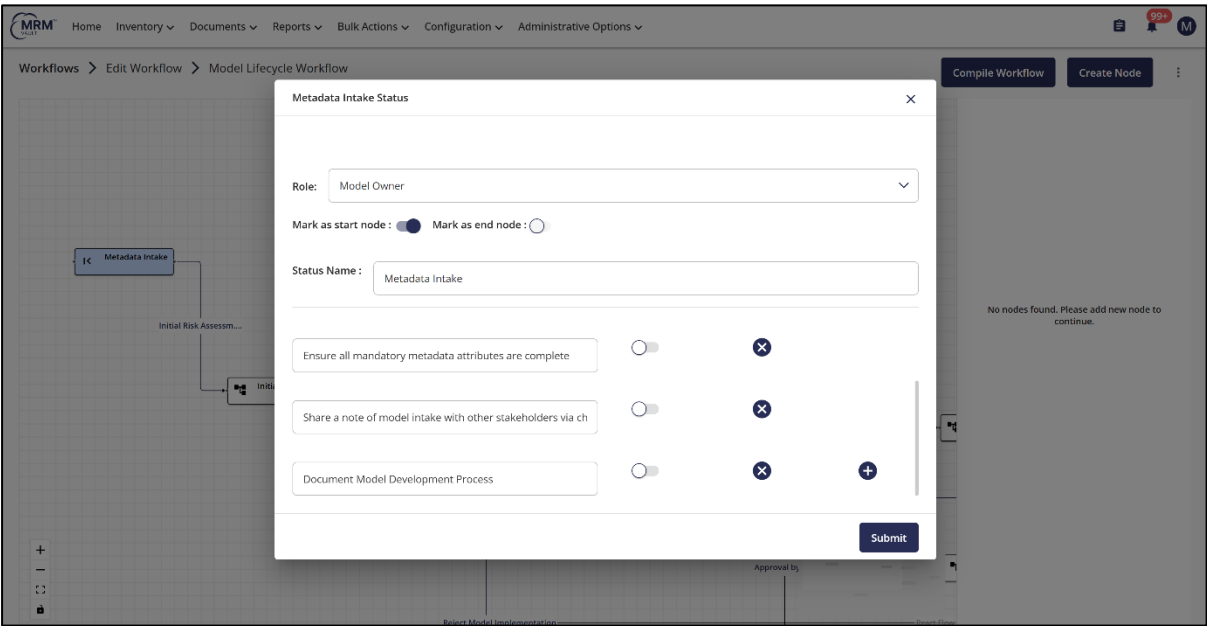
	predefined mitigations (e.g., revoking user access or escalating to MRM Admin).	
Tiered Administration	<div>MRM Vault supports multi-tiered administration:</div> <ul style="list-style-type: none">• Super Admin: Enterprise-wide privileges for configuration and global policies.• Admin: Delegated authority limited to attributes, templates, notifications, and reports within assigned business areas.	Configuration Required



Reference Image 1: User Roles List; Enables administrators to create, retire, or modify permissions for user roles.



Reference Image 2: Model-Level User Role Permissions; Define and manage role-based access to all model elements, such as details, documents, teams, lifecycle events, workflows, chat forums, alerts, and related modules.



Reference Image 3: Workflow State Role Assignment; Define which model roles have access to or responsibilities at each stage of the workflow process.

MRM Vault

DashboardInventoryModel ArtifactsDocumentsRules & ReportsBulk ActionsConfigurationAdmin Options

User Management

UserGroupsRoles

RolesLogs

Q Search

User2024-11-082024-12-23Log ActionAttributesState

FIELD NAME	ACTION	PERFORMED BY	DATE	CURRENT VALUE	PREVIOUS VALUE
Model Owner	Created	MRM Admin	09/06/2025, 11:15:22 am	Active	-
Model Validator	Created	MRM Admin	09/08/2025, 02:30:45 pm	Active	-
Model Risk Analyst	Created	MRM Admin	09/10/2025, 07:50:10 am	Active	-
Model Governance Lead	Created	MRM Admin	09/12/2025, 03:12:33 pm	Active	-
Model Performance Monitor	Created	MRM Admin	09/14/2025, 04:25:15 pm	Active	-
Model Compliance Officer	Created	MRM Admin	09/16/2025, 12:05:58 pm	Active	-
Model Development Lead	Created	MRM Admin	09/18/2025, 09:45:01 am	Active	-

Showing 1 - 5 out of 100

<123...8910>

Show : 5 rows

Reference Image 4: User Role Logs; Creation/edit/deletion of user roles in MRM Vault with log metadata like date, user who did the action.

4.1.2 Attributes

Requirement:

The system must capture, manage, and maintain standardized attributes for every model in the inventory. Attributes must ensure unique identification, consistency, lifecycle coverage, auditability, configurability without IT dependency, backward compatibility, role-based access, and scalability for future requirements.

Our Understanding:

Each attribute must have an immutable system ID, distinct from display labels, and remain constant across all workflows and reports. Administrators should be able to configure and manage attributes directly without IT intervention, while changes must be logged, version-controlled, and backward compatible. Role-based visibility and edit rights should be enforced, and the framework must support evolving business and regulatory metadata needs.

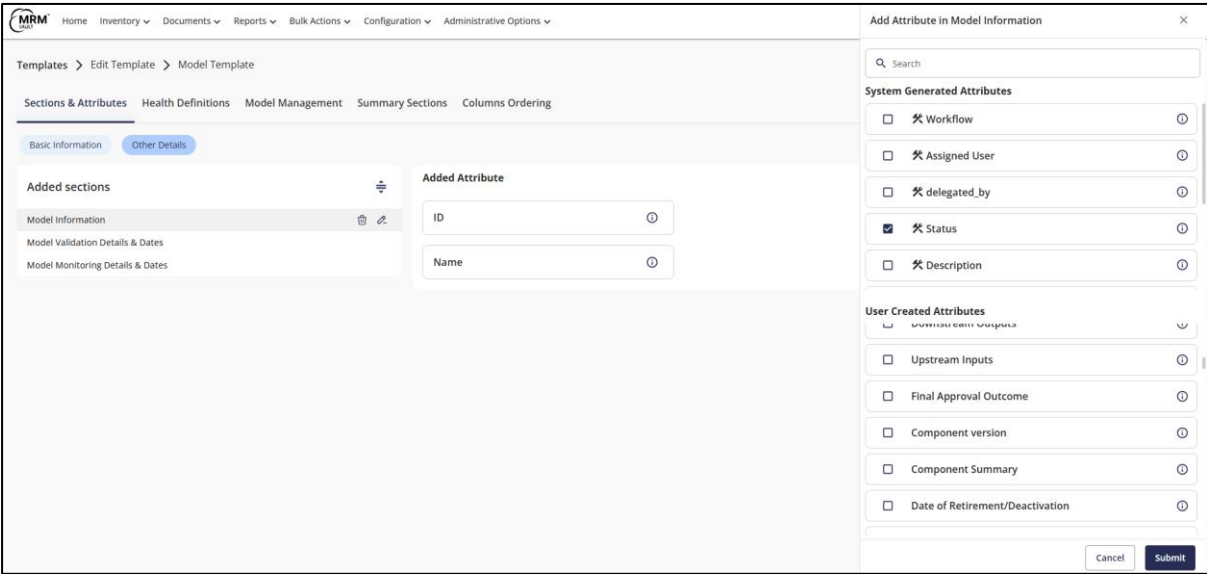
Solytics Response:

Requirement	How MRM Vault Handles This	Status
Unique Identification	MRM Vault automatically generates a unique, immutable system ID for each attribute at creation. This ID remains constant across template versions, lifecycle stages, and model migrations, ensuring traceability and consistency across all workflows and reports	Out of the Box
Standardization	Attribute definitions, permissible values, and formats are governed by a centralized attribute library. Standardization is enforced via controlled vocabulary and validation rules that prevent free-text deviation. Attribute templates are reusable across business units to ensure uniformity.	Out of the Box
Lifecycle Coverage	MRM Vault attributes are designed to capture all necessary metadata across the lifecycle stages of a model. These attributes are organized into templates, which map relevant metadata to each specific stage of the lifecycle. Templates are integrated with workflows that enable permissioned users and user roles to update attribute values. This ensures that all required metadata is accurately captured and maintained throughout the model's lifecycle, in alignment with the bank's governance policies.	Configuration Required
Auditability	MRM Vault maintains an immutable audit trail for every attribute change, whether it is a creation, modification, or retirement. These logs are embedded within templates for entities such as models, assessments, artifacts, lifecycle events, and use cases. Each log entry includes: <ul style="list-style-type: none"> Change details: The specific attribute values before and after the change Timestamp: The exact date and time of the change User information: The identity of the permissioned user who made the change The comprehensive audit logs enable full traceability and compliance with the bank's governance standards.	Out of the Box
Flexibility & Configurability	Authorized administrators can create, edit, or deactivate attributes via a self-service UI, without IT involvement. <ul style="list-style-type: none"> Allowed changes: display names, dropdown values, descriptions. Restricted changes: data type or ID structure (to maintain backward compatibility). 	Configuration Required

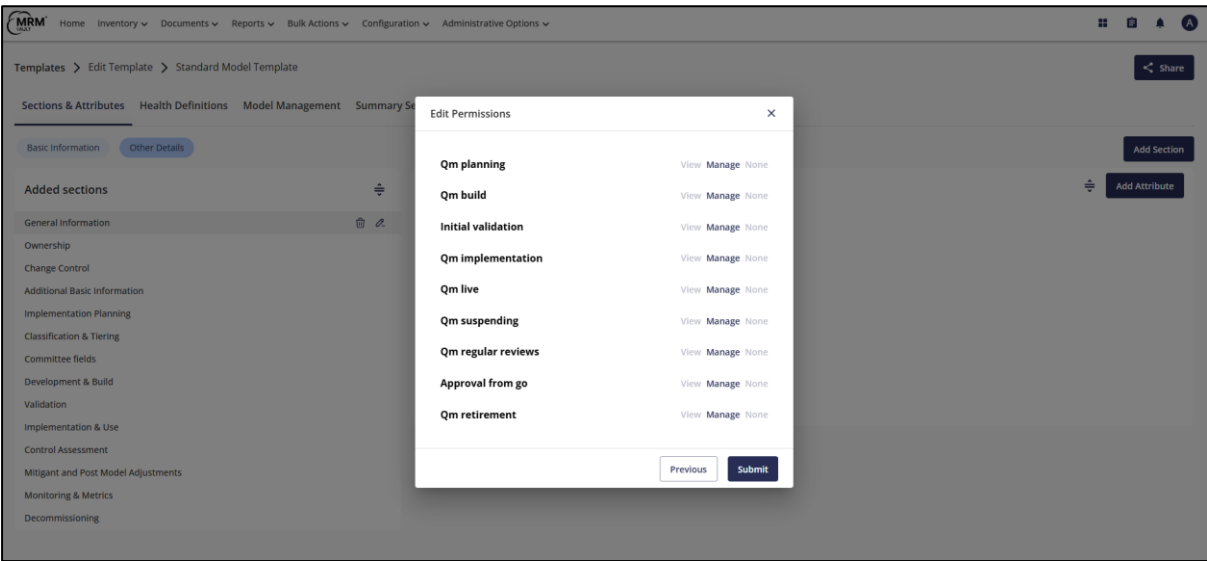
	<ul style="list-style-type: none"> All changes are version-controlled and logged with approval-based governance. 	
Non-Disruptive Changes	MRM Vault ensures that all attribute modifications preserve prior versions, which are archived in the audit trail. Historical attribute values remain fully retrievable through the attribute history view or exported reports, ensuring no data loss or overwriting.	Out of the Box
Role-Based Control	<p>Attribute permissions are governed by RBAC integrated with template-level access settings.</p> <ul style="list-style-type: none"> Each section (e.g., Model Metadata, Validation, Monitoring) can be configured to restrict edit or view access to specific roles. For example, Model Owners can edit registration attributes, while Validators can only view or update validation-related fields. 	Configuration Required
Extensibility	<p>The attribute framework is inherently extensible — administrators can introduce new regulatory, business, or model-type-specific attributes through the centralized attribute library.</p> <p>New attributes automatically inherit role-based permissions and audit properties, ensuring seamless integration with existing workflows.</p>	Out of the Box

ATTRIBUTE ID	ATTRIBUTE NAME	ATTRIBUTE DISPLAY NAME	DATA TYPE	IS DERIVED	TEMPLATE USAGE
562	CAP Evidence	CAP Evidence	Hyperlink	No	MRM Finding
561	PMA Applied	PMA Applied	Single Select	No	MRM Finding
560	PMA Count	PMA Count	Integer	No	MRM Finding
559	PMA Comments	PMA Comments	Text	No	MRM Finding
558	PMA Details	PMA Details	Text	No	MRM Finding
557	Mitigant Status	Mitigant Status	Text	No	MRM Finding
556	Mitigant Due	Mitigant Due	Text	No	MRM Finding
555	Mitigant Owner	Mitigant Owner	Text	No	MRM Finding
554	Mitigant Action	Mitigant Action	Text	No	MRM Finding
553	CAP Status	CAP Status	Text	No	MRM Finding
552	CAP Due Date	CAP Due Date	Date	No	MRM Finding

Reference Image 1: Central Attribute Library; A single place to manage all system attributes, create, update, or delete them easily.



Reference Image 2: Template & Attributes; Attributes are sourced and placed into templates from the Central Attribute Library for consistency and reuse.



Reference Image 3: Section-Level Permissions; Define and manage permissions for attribute sections at each stage of the workflow.

MRM

HomeInventoryDocumentsReportsBulk ActionsConfigurationAdministrative Options

99%

ModelsAIM-M045

Logs

Search

UserFrom dateMM/DD/YYYYTo dateMM/DD/YYYYLog ActionsAttributesState

ACTION	RESPONSIBLE USER	CHANGED DATE	CHANGED FIELD	WORKFLOW STATE	PREVIOUS VALUE	CURRENT VALUE
Updated Attribute	mrm_admin	08/26/2025, 9:45:02 pm	Complexity	Model Development	Moderate	High
Updated Attribute	mrm_admin	08/26/2025, 9:45:02 pm	Expected Life of Model	Model Development	-	1-2 Years
Updated Attribute	mrm_admin	08/26/2025, 9:44:32 pm	Expected Life of Model	Model Development	5 Years	1-2 Years
Updated Attribute	brian	08/26/2025, 4:26:30 pm	Model Risk Tier	MV to review Risk Assessment	Tier 3	Tier 2
Updated Attribute	brian	08/26/2025, 4:26:30 pm	Expected Life of Model	MV to review Risk Assessment	-	5 Years
Updated Attribute	brian	08/26/2025, 4:26:29 pm	Complexity	MV to review Risk Assessment	Moderate	High
Updated Attribute	brian	08/26/2025, 4:24:47 pm	Model Risk Tier	MV to review Risk Assessment	Tier 2	Tier 3
Updated Attribute	brian	08/26/2025, 4:24:46 pm	Complexity	MV to review Risk Assessment	High	Moderate
Updated Attribute	brian	08/26/2025, 4:24:43 pm	Complexity	MV to review Risk Assessment	High	Moderate
Updated Attribute	brian	08/26/2025, 4:24:41 pm	Model Risk Tier	MV to review Risk Assessment	Tier 3	Tier 2
Updated Attribute	brian	08/26/2025, 4:24:40 pm	Model Risk Tier	MV to review Risk Assessment	Tier 2	Tier 3

Reference Image 4: Model Attribute Audit Log; Records every modification to attribute values, ensuring traceability and accountability.

MRM

DashboardInventoryModel ArtifactsDocumentsRules & ReportsBulk ActionsConfigurationAdmin Options

99%

Configuration > Templates > Edit Sections & attributes

DetailsSections & AttributesSettingsVersionsLogs

VERSION	ENTITIES CONNECTED	CREATED DATE	CREATED BY
V 1.1	2 Models	10/07/2025	MRM_Admin
Test Temp 02 Default	1 Model	10/07/2025	MRM_Admin
TESTING -TRP	No Models	10/07/2025	MRM_Admin
Temp_dev	142 Models	10/07/2025	MRM_Admin
Test Template V1.1	10/07/2025	10/07/2025	MRM_Admin

Publish to Template

View Version

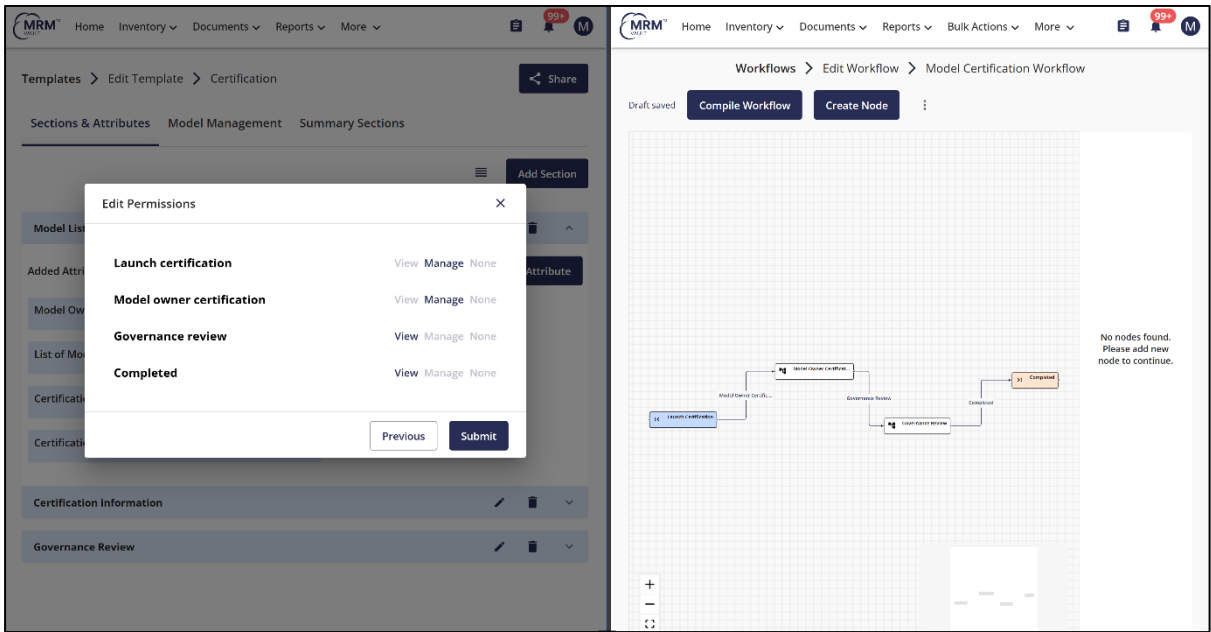
Compare Versions

Use as Default

Delete

Show: 5 rows < 1 2 3 4 ... 10 >

Reference Image 5: Template & Attribute Audit Log; Records every modification to attribute values, ensuring traceability and accountability.



Reference Image 6: Template & Workflow permissions; Setup the permission to View/Manage/None sections or attributes depending upon the workflow state and mapped user role.

4.1.3 Form Templates

Requirement:

Form templates must serve as standardized, configurable collections of attributes required for model lifecycle processes (e.g., Registration, Validation, Monitoring, Decommissioning). They must ensure consistency, auditability, and flexibility while supporting role-based controls, configurability without IT dependency, and backward compatibility.

Our Understanding:

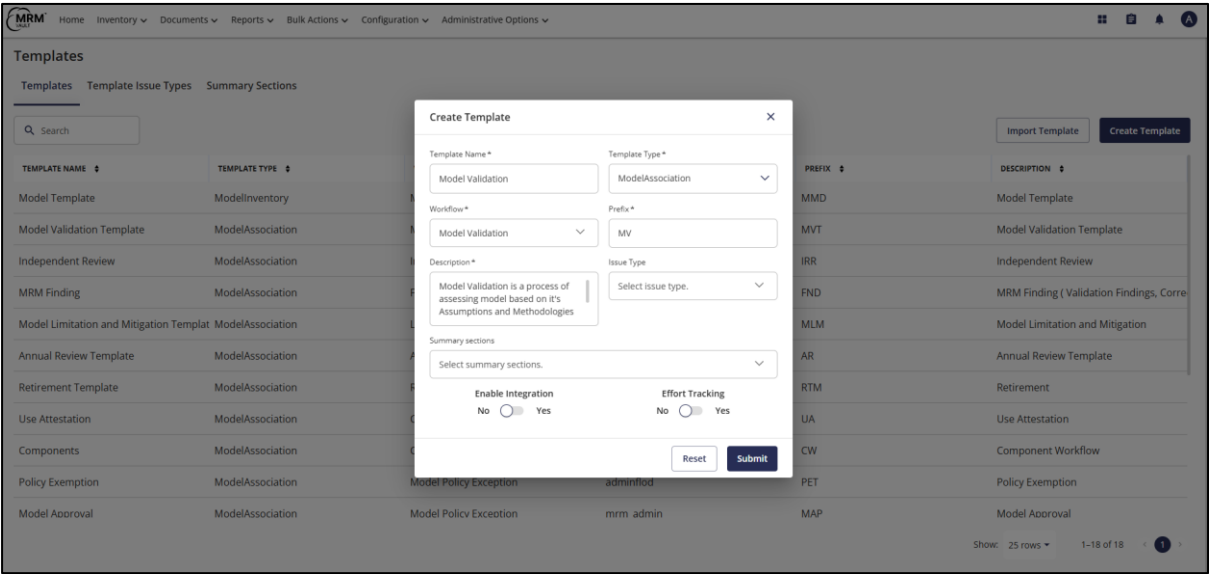
Templates/ Form should be centrally created from the Attribute Library, consistently reused across lifecycle stages, and managed only by authorized roles. They must be version-controlled, auditable, flexible enough to support new regulatory or business requirements, and designed to preserve historical submissions.

Solytics Response:

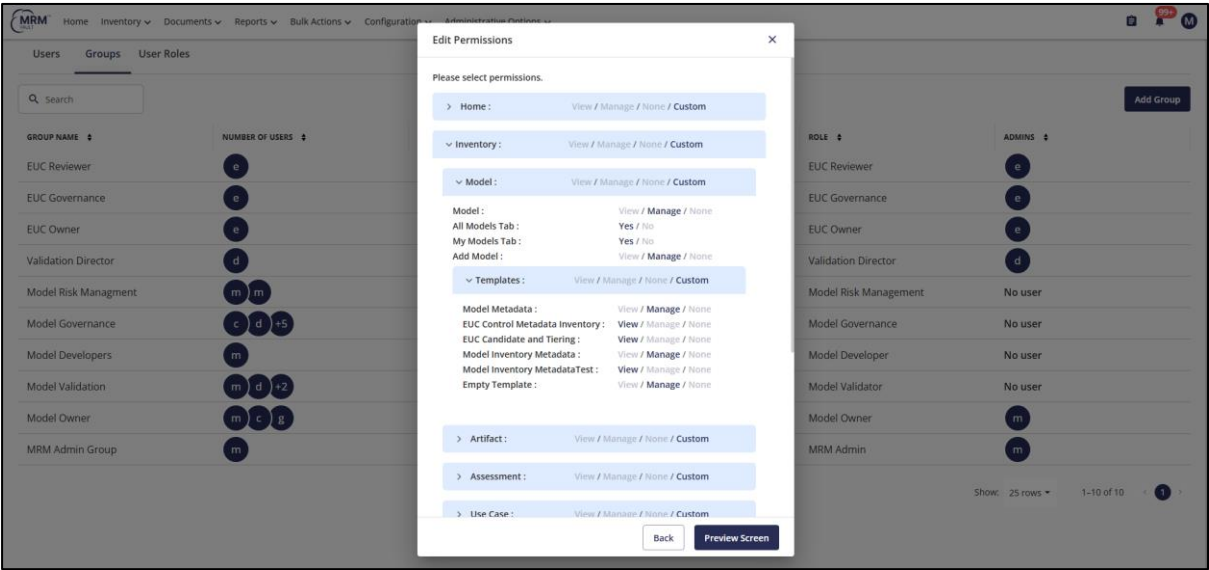
Requirement	How MRM Vault Handles This	Status
Standardization Across Lifecycle	MRM Vault provides administrators with configurable base templates for key lifecycle stages (Registration, PDV, Monitoring, Change Management, Decommissioning). These can be customized using the centralized attribute library. Configuration involves mapping each template to the corresponding lifecycle workflow and defining mandatory attributes and role ownership per stage.	Configuration Required

Role-Based Creation & Ownership	Template creation and modification are restricted to authorized roles (MRM Admins, Function Heads) under RBAC controls. Each template change triggers a workflow requiring review and approval by an oversight role. All actions, creation, modification, deactivation — are logged with user IDs, timestamps, and approval references to ensure governance alignment.	Configuration Required
Configurability Without IT	MRM Vault provides a user-friendly interface for administrators to add, remove, or update attributes in Templates/Form without IT support. Attributes are selected from the Centralized Attribute Library and arranged as needed. Fields can be defined as mandatory or optional, with mandatory ones clearly marked, ensuring process integrity, data completeness, and compliance consistency across workflows.	Out of the Box
Version Control & Auditability	<p>MRM Vault automatically assigns each template or forms a unique identifier based on its name, increment for new version created, and maintains a complete version history for every change—such as attribute additions, removals, or configuration updates.</p> <p>Each update is logged with:</p> <ul style="list-style-type: none"> • User details: Who made the change • Timestamp: When the change occurred • Approval for change: When was the template change approved <p>To ensure full auditability and traceability, the platform also supports version rollbacks, allowing administrators to revert to previous versions when needed—preserving historical consistency and reducing operational risk.</p> <p>Additionally, users can now perform an impact assessment when updating templates are initiated. This allows them to choose whether the changes:</p> <ul style="list-style-type: none"> • Apply retroactively to existing inventory already mapped to the template • Apply prospectively only to new items mapped going forward <p>This flexibility ensures that updates are aligned with governance requirements and operational priorities, giving users full control over how changes affect their data landscape.</p>	Out of the Box
Flexibility	Authorized administrators can create new templates or deactivate existing ones anytime. Deactivated templates remain available in a read-only mode for historical records	Out of the Box

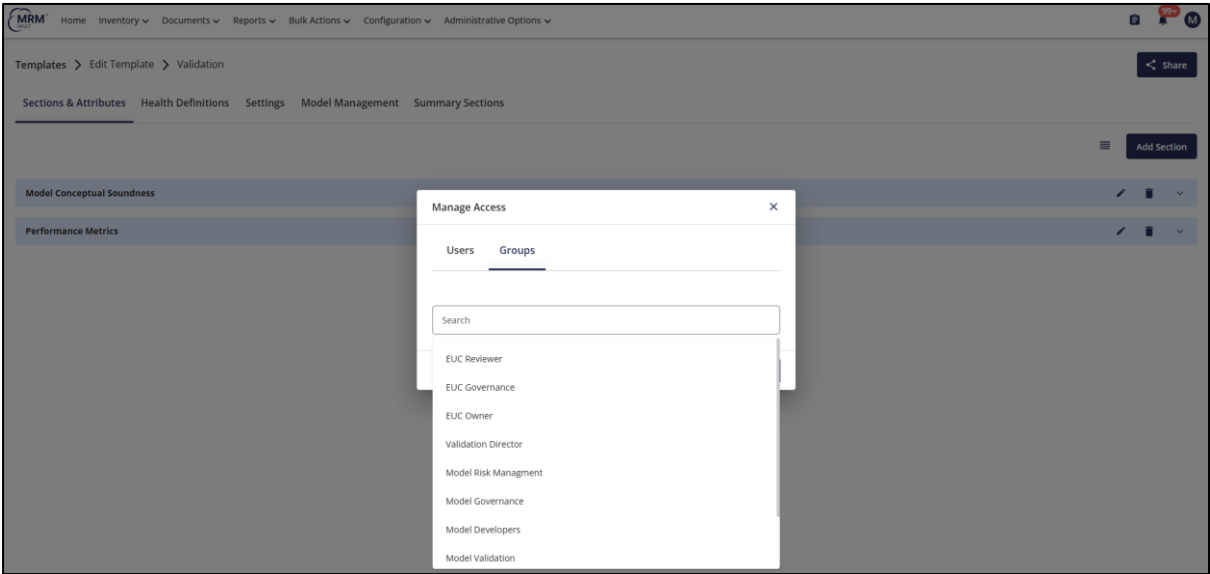
	and reports but cannot be used for new submissions. Dependency checks prevent deactivation of templates currently in active workflows, ensuring lifecycle integrity.	
Non-Disruptive Updates	Template updates are applied prospectively, ensuring historical submissions remain unchanged. Each update creates a new version entry within the audit log, preserving complete traceability for prior data and reports.	Out of the Box
Inter-Linkages	MRM Vault allows templates to be interlinked across lifecycle stages through configuration mapping. Each stage (Registration, PDV, Monitoring, etc.) references relevant template sections dynamically, ensuring that users view only stage-relevant data. Visibility rules and section dependencies are controlled by workflow configuration, eliminating duplication and ensuring data continuity.	Configuration Required
Usability & Accessibility	MRM Vault structures template / form into logical sections, enforce role-based visibility, and provide inline guidance to improve data accuracy.	Out of the Box
Submitter & Approver Views	<p>MRM Vault supports a Maker-Checker control mechanism that enforces review and approval before any workflow stage transition. At each stage of the workflow, the maker (submitter) enters or updates the required information and submits it for review. The checker (approver) then reviews the submission and can either:</p> <ul style="list-style-type: none"> • Approve – allowing the model to progress to the next workflow stage, or • Reject/Send Back – returning the model to the maker with comments for revision. <p>The maker can then modify the inputs based on feedback and resubmit for approval. Once corrections are made, the maker can resubmit; system automatically re-initiates approval routing.</p> <p>All Maker-Checker actions are logged with timestamps and user IDs, ensuring accountability and auditability.</p>	Configuration Required



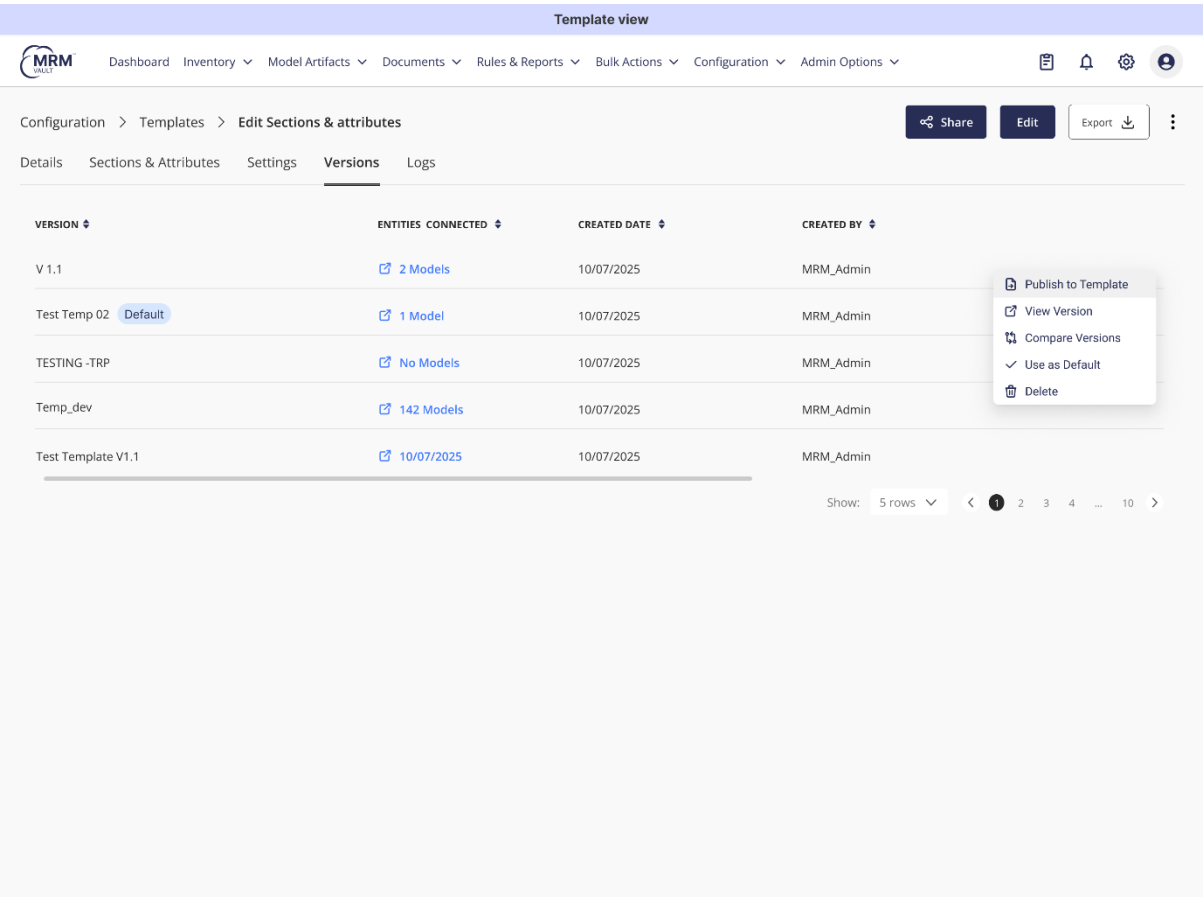
Reference Image 1: Template-to-Workflow Mapping; Link each template to its corresponding workflow for process alignment.



Reference Image 2: Template Permissions Management; Enables administrators to grant or modify template permissions for specific user groups via the Group Permissions section.



Reference Image 3: Direct Template Permission Assignment; Administrators can grant template permissions to specific users or roles directly from the template.



Reference Image 4: Template Version page; Create/Edit/Publish template versions with option to compare, apply to inventory or only new models

MRM

DashboardInventoryModel ArtifactsDocumentsRules & ReportsBulk ActionsConfigurationAdmin Options

Configuration > Templates > Edit Sections & attributes

ShareEditExport

DetailsHealth DefinitionsModel ManagementSummary SectionsVersionsLogs

Q Search

User

2024-11-08 → 2024-12-23

Log Action

Attributes

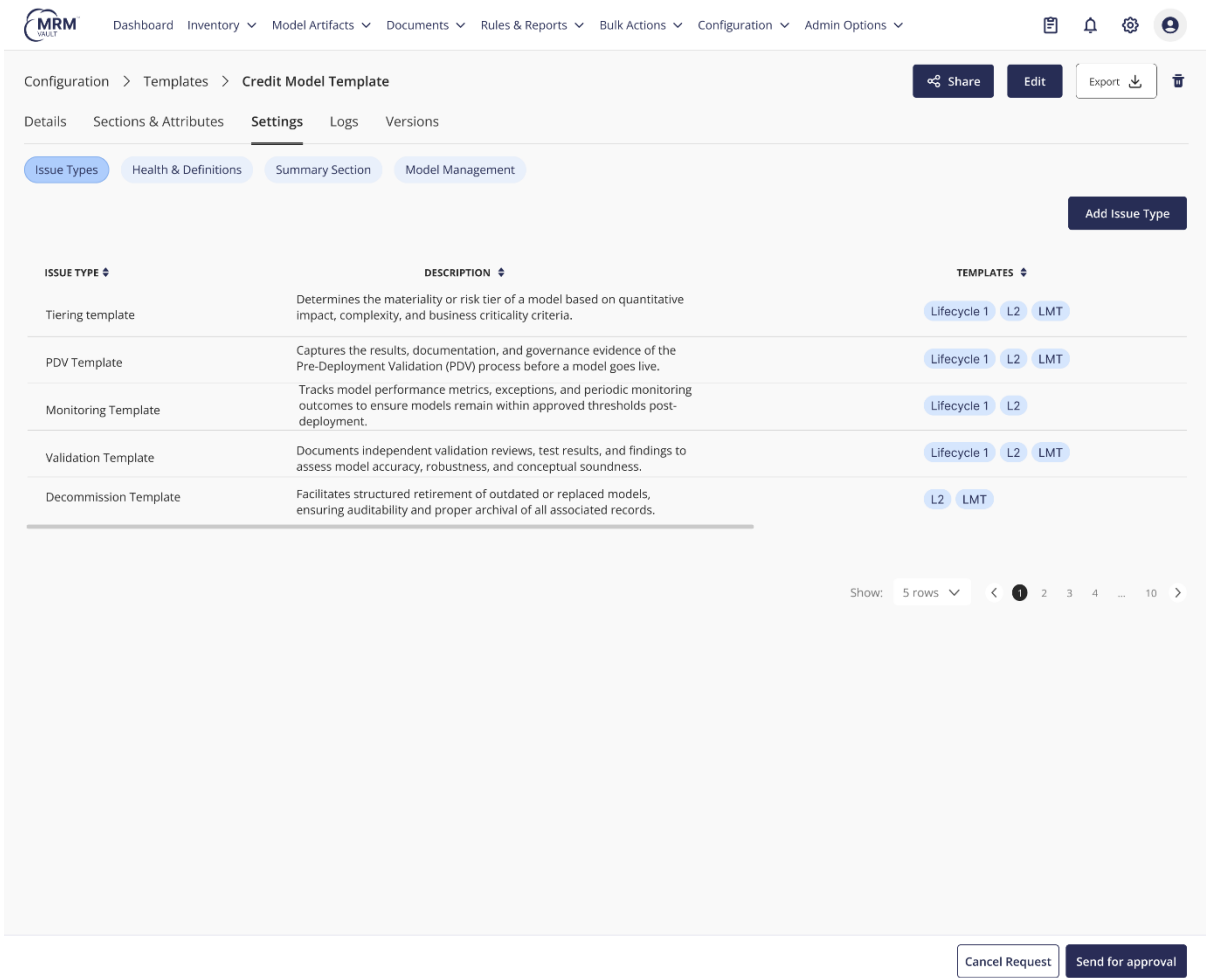
State

ACTION	RESPONSIBLE USER	CHANGED DATE	CHANGED FIELD	PREVIOUS VALUE	CURRENT VALUE
Attribute rename	Asimov	12/01/2024, 03:22:11 pm	Risk Tier	T2	T3
Section deleted	Verne	12/05/2024, 09:15:52 am	Model details	Model details	-
Attribute added	Verne	12/11/2024, 11:59:01 pm	Model Use	-	Insurance sector
Attribute added	Verne	12/18/2024, 07:34:28 am	Business Unit	-	CRAIN
Attribute added	Asimov	12/22/2024, 01:08:45 pm	Materiality	-	High

Show: 5 rows < 1 2 3 4 ... 10 >

Cancel RequestSend for approval

Reference Image 5: Template Logs; View all changes made to the current version of template



Reference Image 6: Template Issue Types; Authorized users can associate the Credit Model Template with other templates—such as the Tiering Template—to establish a connection between the model and a corresponding lifecycle event (e.g., Tiering). This linkage mechanism is extensible across all templates and lifecycle events. In this setup, the Issue Type functions as a bridge, enabling seamless mapping between templates and their lifecycle events.

4.1.4 Configuration Table

Requirement:

The system must provide a centralized Configuration Table to govern model lifecycle behavior. This includes a Parameter Table for lifecycle rules (e.g., stage visibility, TATs, role assignments, escalation paths) and a User Access Management (UAM) Table for managing user roles, groups, and permissions. These tables must be configurable without IT intervention, support change control, preserve audit trails, and ensure scalability across business areas and model types.

Our Understanding:

The Parameter Table acts as the active “rulebook” for models’ journey through it’s lifecycle, defining lifecycle stage requirements, ownership, deadlines, and escalation logic. The UAM Table provides control over visibility of attribute(s) across different stages of lifecycle workflow, applicability of stages of the workflow, roles, TAT, escalation etc. ensuring RBAC is enforced

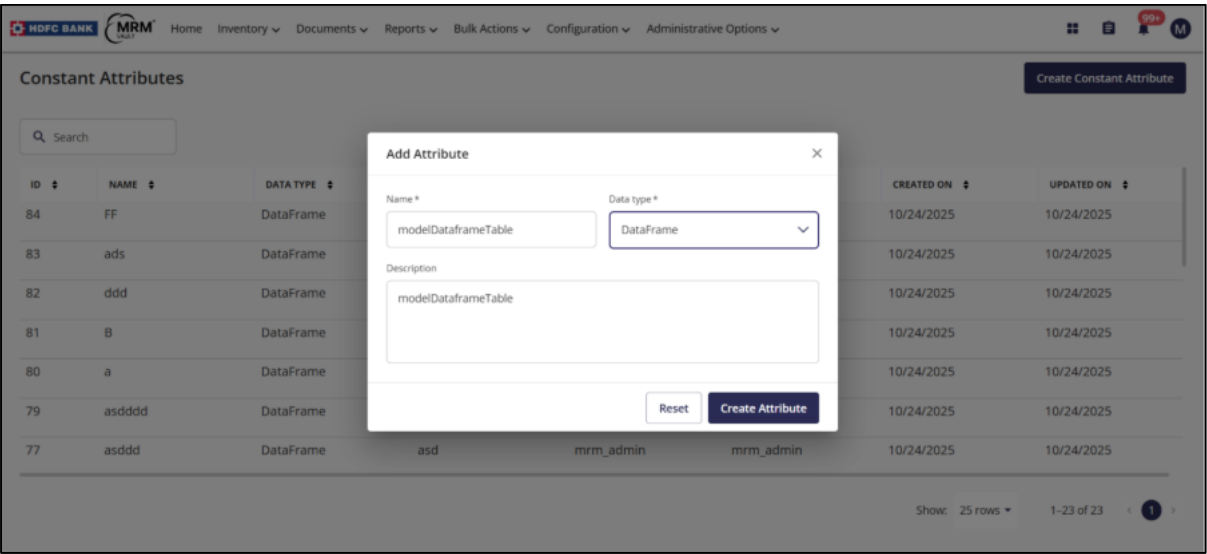
consistently across workflows. The parameter table must be configurable from the UI without need for any kind of tech intervention, centrally owned by oversight teams, auditable, and aligned with regulatory expectations.

Solytics Response:

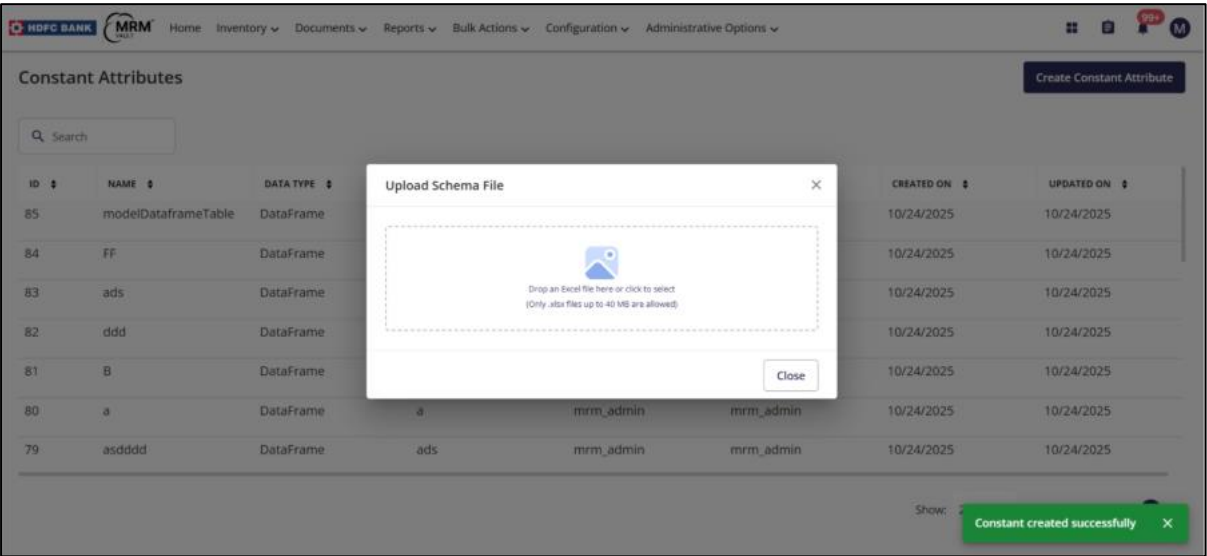
Requirement	How MRM Vault Handles This	Status
Single Source of Control	<p>The Parameter Table in MRM Vault acts as the central configuration layer that governs workflows, forms, SLAs, and escalation logic across the model lifecycle.</p> <ul style="list-style-type: none"> It is implemented as a Constant Attribute, where administrators upload an Excel/CSV file defining combinations of model characteristics (e.g., Model Area, Business Unit, Model Type, Risk Tier) and their corresponding configurations (e.g., applicable forms, workflows, timelines, escalation paths). At runtime, MRM Vault performs a lookup against parameter table based on the model's metadata to determine the correct lifecycle behavior. This design ensures an auditable single source of truth for governance - maintained centrally, applied dynamically, and traceable end to end. 	Out of the Box
Parameter-Driven Lifecycle Rules	<p>MRM Vault dynamically determines each model's lifecycle flow using the Parameter Table as its configuration source.</p> <ul style="list-style-type: none"> For every model metadata combination (e.g., Model Area, Business Unit, Model Type, Risk Tier), the Parameter Table specifies applicable stages, responsible owners, approvers, SLAs, and escalation paths. At runtime, MRM Vault performs a metadata-based lookup against this table to automatically activate the correct workflow sequence and associated configurations. This parameter-driven orchestration eliminates hardcoded logic, ensuring lifecycle behavior remains consistent, configurable, and easily adaptable across all model categories. 	Configuration Required
Stage Skipping & Dynamic Display	<p>MRM Vault uses conditional rules from the Parameter Table to control which workflow stages, forms, or sections are displayed for a given model.</p> <ul style="list-style-type: none"> At runtime, the system evaluates key metadata (e.g., Materiality, Model Type, Risk Tier) and, based on matching configuration entries, automatically shows or skips specific stages. 	Configuration Required

	<ul style="list-style-type: none"> For instance, if <i>Materiality</i> = <i>Low</i>, the PDV stage is excluded from the workflow. This ensures each model follows only its relevant governance path, enhancing accuracy, reducing manual intervention, and streamlining the user experience. 	
TAT & Escalation	<p>TATs and escalation rules are configuration-driven through the Parameter Table.</p> <ul style="list-style-type: none"> For each workflow stage, the table defines the standard duration and escalation hierarchy. At runtime, Vault calculates the due date automatically, issues pre-expiry alerts, and triggers auto-escalation if timelines are breached. All reminders, escalations, and ownership transitions are executed as per the configuration matrix, allowing administrators to modify SLAs directly through the UI or Excel upload of Parameter table without any code change or IT intervention. 	Configuration Required
Change Control & Auditability	<p>All Parameter Table modifications are governed through Vault's Change Management workflow to maintain strict control and traceability.</p> <ul style="list-style-type: none"> Each action in change request workflow is audit logged with action details, user details, time stamp etc. Each approved update to the parameter table is immutably audit logged, ensuring complete version history, regulatory defensibility and prevention of unauthorized configuration changes. 	Out of the Box
Granularity & Coverage	<p>Each entry in the Parameter Table represents a specific configuration rule based on model attributes such as Model Area, Business Unit, or Risk Tier.</p> <p>MRM Vault allows rules to be defined at multiple levels such as – model lifecycle workflow, subprocess workflows etc. All rules can be viewed and edited through the UI, ensuring complete coverage of all model types and clear governance control across the organization.</p>	Configuration Required
Scalability & Extensibility	<ul style="list-style-type: none"> The Parameter Table is built to scale without requiring code changes. New model types, business units, or workflows - can be added directly through the UI CSV/XLSX upload. MRM Vault automatically applies existing baseline rules such as permissions, SLAs, and lifecycle templates to new entries, ensuring consistent governance and quick rollout across expanding model inventories. 	Configuration Required

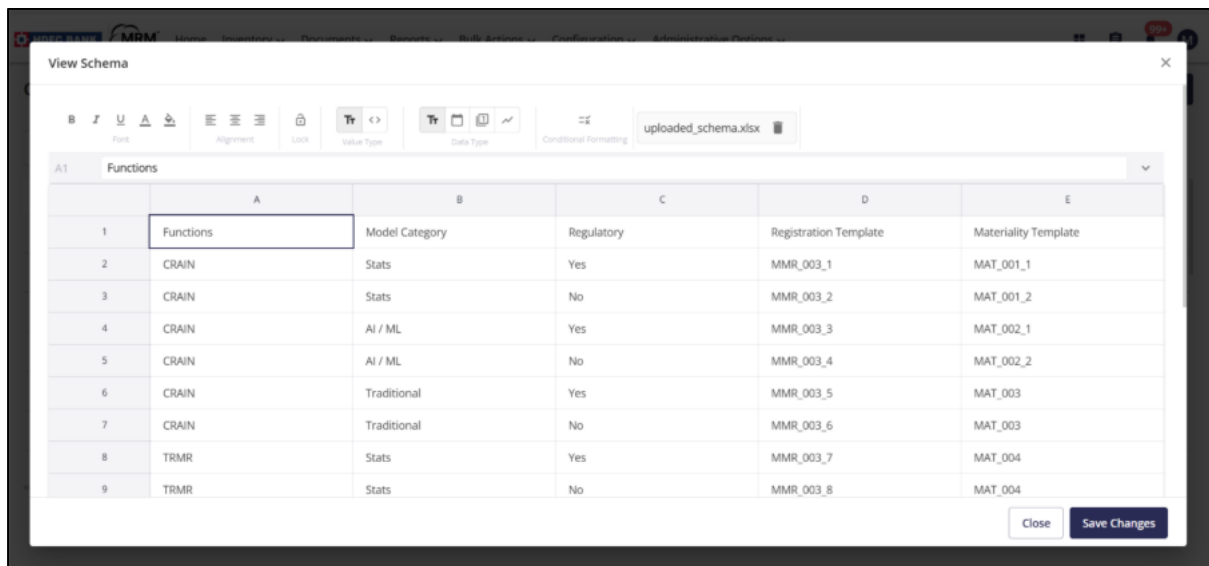
UAM Role– Model Permissions	<p>Role-Model permissions in MRM Vault define granular access rights for each role at model and sub-process level.</p> <p>Administrators can specify permissions for a role such as (View, Edit, Approve, None) for different actions at model or lifecycle-stage level. Actions such as editing metadata, attaching document, adding comments in chat-forum, accessing logs, transitioning a model etc.</p> <p>At runtime, MRM Vault evaluates these rules dynamically to restrict user actions within authorized boundaries, basis Role – Model permission configuration.</p> <p>Any role or mapping change instantly recalibrates access rights and generates audit logs—ensuring compliance with segregation of duties and traceable access control.</p>	Configuration Required
UAM Group– Feature Permissions	<p>Feature-level permissions govern access to specific platform actions such as <i>Create Model</i>, <i>Edit Workflow</i>, or <i>Manage Templates</i>.</p> <ul style="list-style-type: none"> Each group or role can have defined rights for these actions, enforced through real-time authorization checks during execution. Sensitive actions prompt confirmation dialogs, and all permission changes are UI-based and audit logged. This framework ensures precise control, prevents unauthorized configuration changes, and maintains operational integrity. 	Configuration Required
Central Oversight	<p>Parameter Table and UAM configurations are centrally managed by oversight roles such as configuration admins, project management etc. The allocation of responsibility to manage and own config table is configurable. These roles can have exclusive edit rights, while others have view-only access. All updates generate audit logs automatically.</p> <p>This oversight model enforces segregation of duties, prevents unauthorized edits, and maintains governance alignment across business functions.</p>	Configuration Required
Regulatory Defensibility	<p>Immutable audit logs and version histories can be exported in CSV/PDF format for regulatory or internal audit use. Reports show full traceability of configuration changes, updates, approvals, and actions decisions across the MRM Vault ecosystem.</p>	Out of the Box



Reference Image 1: System Hosts a configurable attribute called 'Constant Attribute' which can host parameter table for model or it's subprocesses.

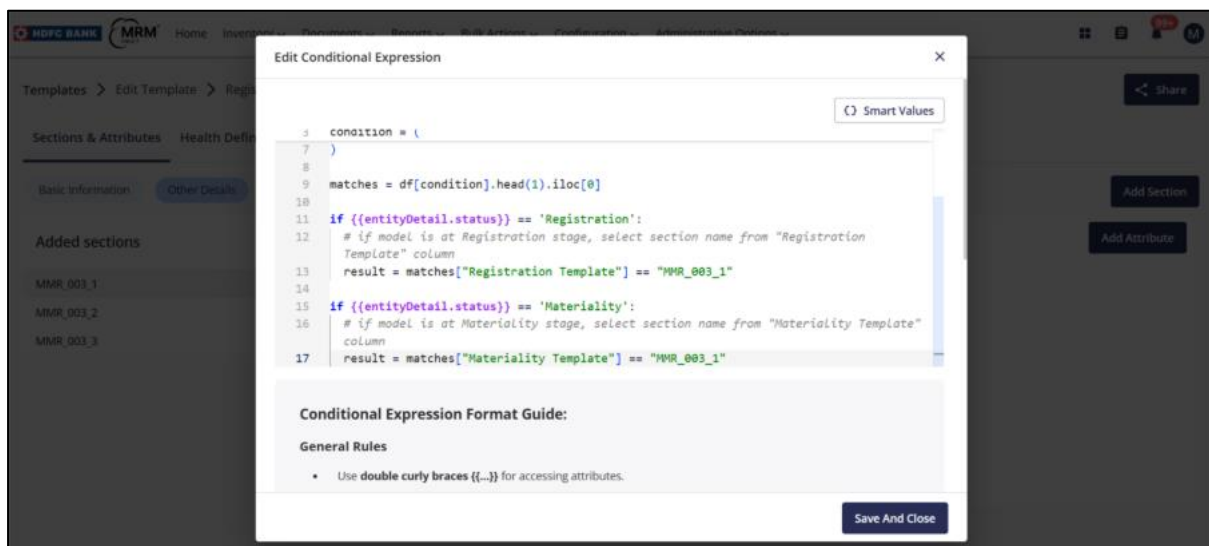


Reference Image 2: User to prepare parameter table in an excel file (csv/xlsx) and upload to a constant attribute.



	A	B	C	D	E
1	Functions	Model Category	Regulatory	Registration Template	Materiality Template
2	CRAIN	Stats	Yes	MMR_003_1	MAT_001_1
3	CRAIN	Stats	No	MMR_003_2	MAT_001_2
4	CRAIN	AI / ML	Yes	MMR_003_3	MAT_002_1
5	CRAIN	AI / ML	No	MMR_003_4	MAT_002_2
6	CRAIN	Traditional	Yes	MMR_003_5	MAT_003
7	CRAIN	Traditional	No	MMR_003_6	MAT_003
8	TRMR	Stats	Yes	MMR_003_7	MAT_004
9	TRMR	Stats	No	MMR_003_8	MAT_004

Reference Image 3: User can view/edit uploaded parameter table schema in MRM Vault UI.



Reference Image 4: Conditional expression added into relevant metadata attribute forms; Conditional expressions are embedded within relevant metadata attribute forms to enable automatic system lookups against the parameter table. Based on predefined rules and configurations, the system dynamically populates metadata attributes, ensuring consistency and automation. A built-in guide supports users through an intuitive process for constructing conditional logic, streamlining setup and reducing manual effort.

4.1.5 Workflows

Requirement:

The system must support configurable workflows to govern every stage of the model lifecycle (Registration → Validation → Deployment → Monitoring → Mitigation → Decommissioning). Workflows must enforce role-based approvals, support conditional routing, automate task

assignments, provide return/review paths, maintain full auditability, and align with governance policies and regulatory requirements.

Our Understanding:

Workflows should be configurable through a no-code visual designer, allowing administrators to map lifecycle stages, assign roles, embed approval steps, and apply conditional logic (e.g., high-risk vs. low-risk models, AI/ML vs. statistical). The system must ensure segregation of duties, automate escalations and notifications, preserve historical workflow records, and provide complete traceability of all actions.

Solytics Response:

Requirement	How MRM Vault Handles This	Status
Configurable Workflow Designer	MRM Vault provides a no-code Visual Workflow Designer with drag-and-drop stage blocks and rule panels. Administrators can create or modify lifecycle workflows, define dependencies, assign actions, and version-control all changes. Workflows are validated before publication, ensuring only approved versions go live.	Out of the Box
Role-Based Stage Ownership	Each workflow stage enforces mandatory role ownership before activation. Roles such as Model Owner, Validator, or Governance Committee are mapped at design-time and can be reassigned through controlled change workflows with audit logging. Stages cannot progress without completion of the assigned role's approval.	Configuration Required
Conditional Routing	MRM Vault supports conditional logic branches in workflows , administrators can define logic (e.g., IF Model Type = AI AND Materiality = High → route to Independent Validation) using the workflow designer. The engine dynamically routes submissions to the correct branch at runtime, eliminating manual intervention.	Configuration Required
Return & Review Paths	Return loops are configurable for each stage (e.g., Validator → Model Owner → Validator). The system logs each return with reason, comments, and timestamp. Limits on review iterations can be configured to prevent process cycling. All revisions remain auditable in the workflow history.	Configuration Required
Stage-Specific Permissions	Each stage inherits role-based permissions from RBAC but can override them for granular control. Example: Validators can approve PDV while Oversight can close Monitoring. Permissions are defined within the workflow designer and validated against segregation-of-duties rules.	Configuration Required

Audit Trail & Versioning	Every workflow transaction (submit, approve, reject, return) is immutably logged with user, timestamp, and role. Prior versions remain retrievable and exportable as PDF or CSV for audit. Administrators can view version diffs and roll back if needed.	Out of the Box
Notifications & Escalations	<p>MRM Vault workflows support configurable notifications and escalations to ensure timely and coordinated execution of activities. Each workflow state can be assigned a turnaround time, defining the expected duration for transitioning to the next state. If this turnaround time is breached, automated escalations are triggered to alert relevant stakeholders. .</p> <ul style="list-style-type: none"> • Notifications are sent during every workflow transition, including alerts to Checkers when approvals are requested by Makers • Each workflow state has configurable TAT and escalation settings. Automated reminders and multi-level escalations trigger based on breach of defined time thresholds (e.g., Level 1 after 3 days, Level 2 after 7 days) • Email and in-app notifications use templated messages that pull metadata (Model ID, Stage, Owner) and can be customized per workflow stage and recipient group. 	Configuration Required
Alignment with Policy	<p>Workflows are configurable to replicate the bank's governance hierarchy, including approval committees, escalation groups, and attestation steps.</p> <p>Governance mappings can be imported from the Parameter Table to ensure alignment with policy changes without manual re-design.</p>	Configuration Required
Flexibility & Scalability	New workflows or variants (for AI, Vendor, Market-Risk models, etc.) can be created by cloning existing ones, preserving baseline logic while allowing customization of roles, approvals, and TATs. Changes do not impact existing workflows in production.	Out of the Box
Decommissioning Coverage	Dedicated Decommissioning workflows capture retirement justifications, final approvals, and archival confirmation. Upon completion, models are moved to the archive repository with metadata and audit logs retained for the regulatory period (e.g., 7 years).	Configuration Required

MRM

HomeInventory▼Documents▼Reports▼Bulk Actions▼Configuration▼Administrative Options▼

Workflows

Create Workflow

Search

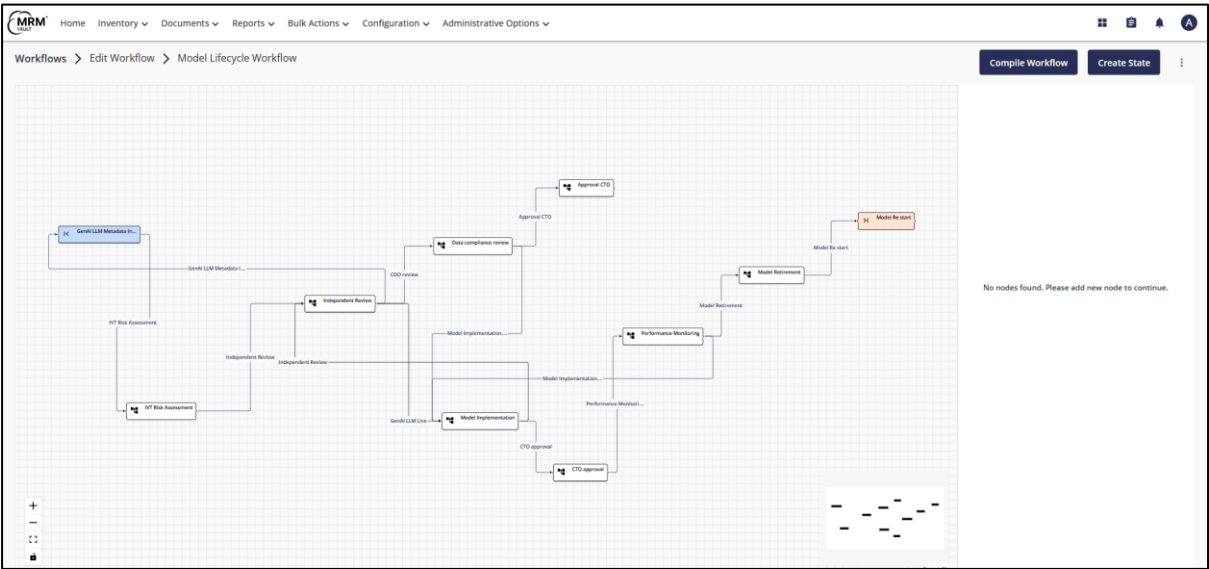
ID	WORKFLOW NAME	CREATED BY	DESCRIPTION	WORKFLOW TYPE
24	Findings Remediation Workflow	adminflod	Findings Remediation Workflow	Published
23	Outcome	mrm_admin	Outcome	Draft
22	Mitigant	mrm_admin	Corrective Action Plan Workflow	Draft
21	Corrective Action Plan Workflow	mrm_admin	Corrective Action Plan Workflow	Draft
20	Validation Findings	mrm_admin	Validation Findings	Draft
19	Model Performance Monitoring	mrm_admin	Performance Monitoring Workflow	Draft
18	Component Workflow	mrm_admin	Component Workflow	Published
17	Annual Review	mrm_admin	Annual Review	Published
16	Limitations and Mitigation	mrm_admin	Limitations and Mitigation	Published
15	Retirement	mrm_admin	Retirement	Published
14	Certification	mrm_admin	Certification	Published
13	Model Validation	mrm_admin	Model Validation	Published

Show: 25 rows

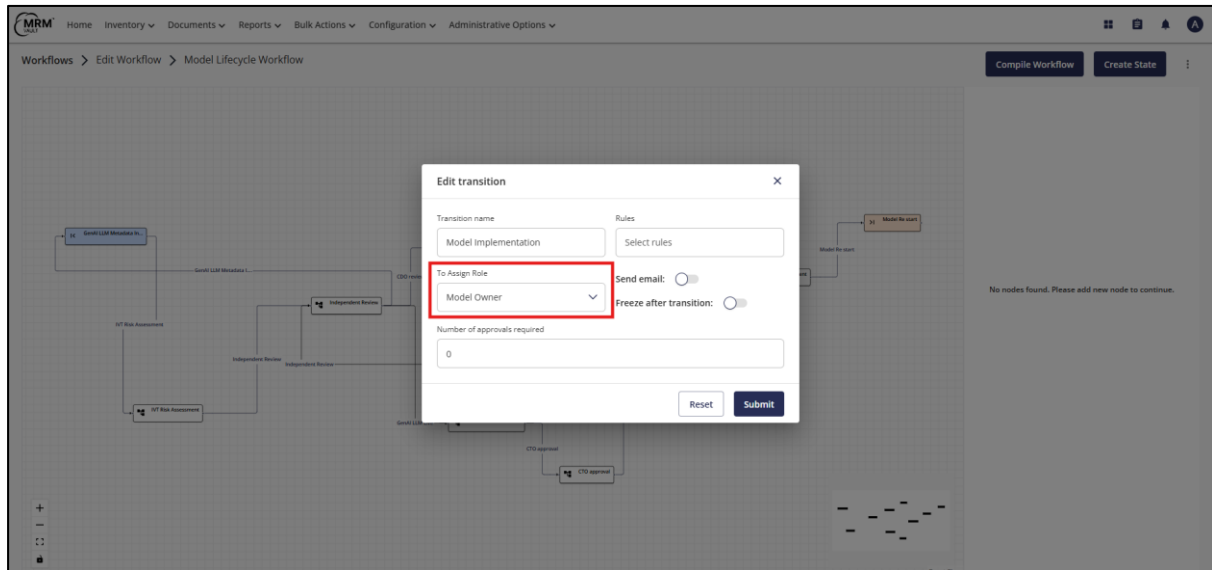
1-23 of 23

1

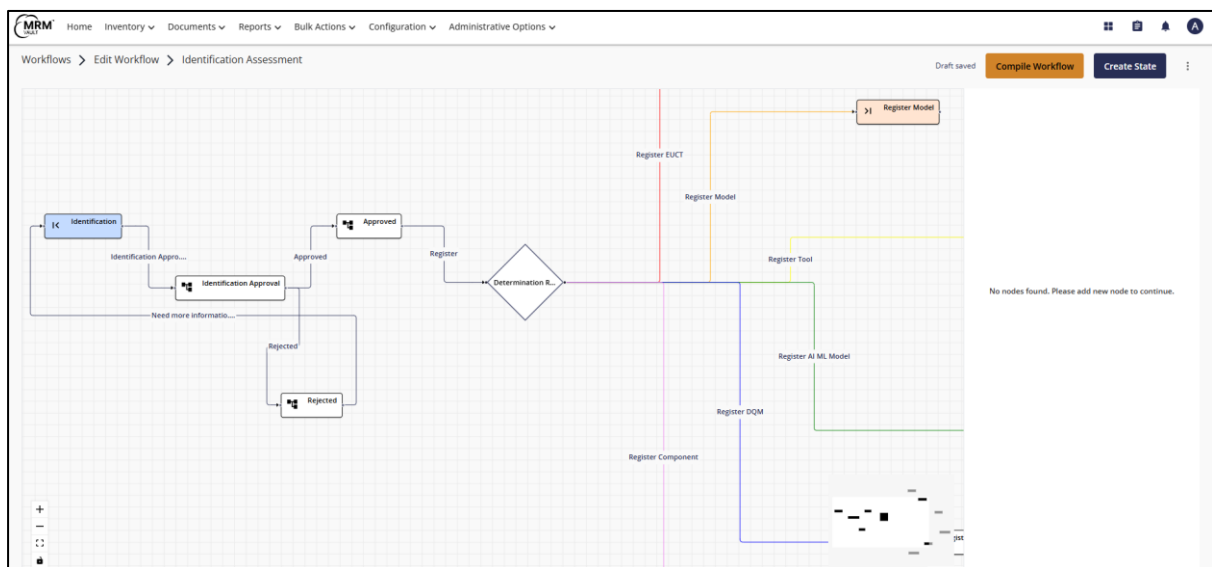
Reference Image 1: Workflow Inventory; A centralized library of all workflows in the system. Administrators can create, edit, or delete workflows.



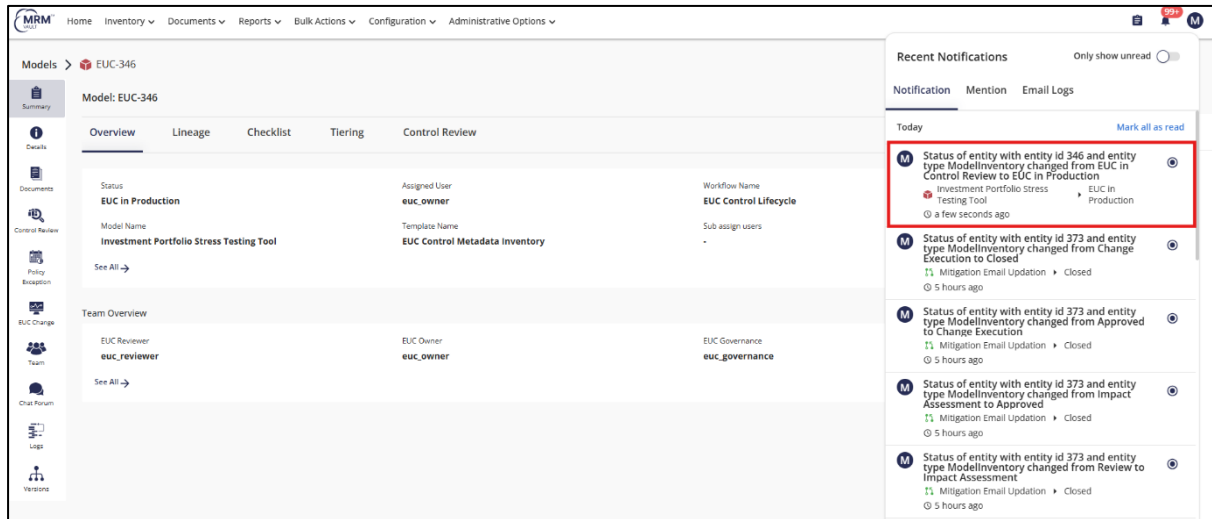
Reference Image 2: Workflow Designer; Define workflow processes, including start and end points, routing, and loops.



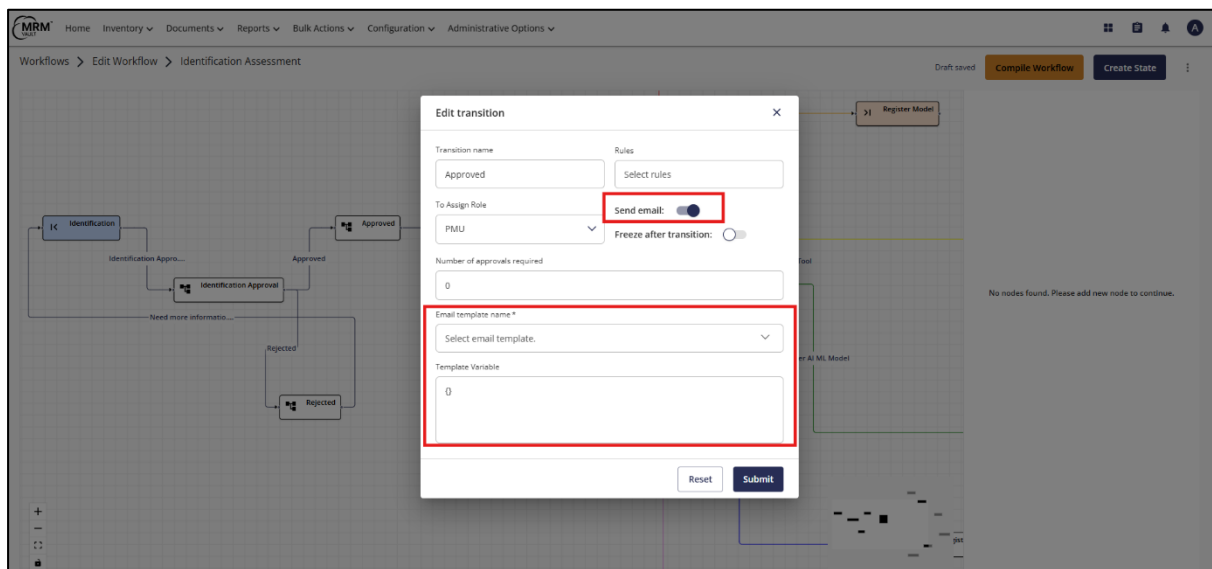
Reference Image 3: Assign Role on Transition; Assign a role to a workflow transition so that when a model reaches that stage, all models at that stage inherit the role's permissions.



Reference Image 4: Conditional Node & Node Loop back; conditional nodes to change the route of a model based on conditions, and loop-backs to previous stages also possible to configure.



Reference Image 5: Stage Transition Notification; Notifications to alert users when a model or artifact moves to another workflow stage.



Reference Image 6: Option Of Email Notification on Nodes; Administrator can select emails from email template which should be sent model transition happens

MRM

DashboardInventoryModel ArtifactsDocumentsRules & ReportsBulk ActionsConfigurationAdmin Options

Workflow Inventory

WorkflowsLogs

Q Search

User2024-11-08 → 2024-12-23Log ActionWorkflowState

ACTION	RESPONSIBLE USER	CHANGE DATE	CHANGE DETAIL	PREVIOUS DETAIL	CURRENT DETAIL
Published Workflow	Galileo Galilei	09/05/2025, 11:47:40 am	Workflow ID/Name	-	Retirement Workflow
Published Workflow	Aryabhata	09/05/2025, 11:47:40 am	Workflow ID/Name	-	Monitoring Workflow
Published Workflow	Johannes Kepler	09/05/2025, 11:47:40 am	Workflow ID/Name	-	PDV Workflow
Updated Workflow	C.V. Raman	09/05/2025, 11:47:40 am	Added Node	-	Registration Workflow (→ Duplication Check)
Updated Workflow	Carl Sagan	09/05/2025, 11:47:40 am	Added Node	-	Inventory Workflow (→ PIT)

Showing 1 - 5 out of 100

<123...8910>

Show : 5 rows

Reference image 7: Workflow Inventory Logs; Changes to workflows like publishing new/updating are captured along with metadata like user who made the change and when.

The screenshot displays the 'Create Automation' page in the MRM Vault system. The interface includes a top navigation bar with links to Home, Inventory, Documents, Reports, Bulk Actions, and More. A 'Create Automation' button is located in the top right corner. The main section is titled 'Automation > Create Automation'.

The 'Automation name*' field contains the text 'Automated model implementation workflow start'. To the right of this field is a toggle switch labeled 'Disabled' and 'Enabled', currently set to 'Disabled'.

The workflow diagram on the left shows a sequence of steps: 'When: TimeBased' followed by 'Then: Entity Transition'. Below the diagram is an 'Add Component' button.

The 'Entity Transition' configuration panel on the right provides details for the action. It includes a description: 'This action executes when the value of the fields selected below changes.' The configuration fields are:

- Relation:** A dropdown menu set to 'Downstream'.
- Template type:** A dropdown menu set to 'ModelAssociation'.
- Template Name:** A dropdown menu set to 'Model Implementation'.
- To State:** A dropdown menu with the placeholder text 'Select destination state'. A list of options is shown below the dropdown: 'Initiate implementation', 'Deploy in production', 'Testing', and 'Implementation Completed'. A 'Submit' button is located to the right of the dropdown.

Reference Image 8: Automation for workflow; In the image above, based on a set duration of time period, the model implementation workflow can be transition into the different states shown as options in the drop-down menu

4.1.6 Emails

Requirement:

Email notifications must be automatically triggered during key model lifecycle actions such as submission, approval, and return.

Notifications should be fully configurable, allowing administrators to:

- Create and edit email templates;
- Define recipient lists based on user roles and workflow actions;
- Customize email content with dynamic fields (e.g., Model ID, stage, owner);
- Support role-based delivery, timely alerts, escalation for overdue tasks; and

- Maintain a complete audit trail of all emails sent.

Administrators must be able to easily enable/disable alerts and modify recipients without IT dependency

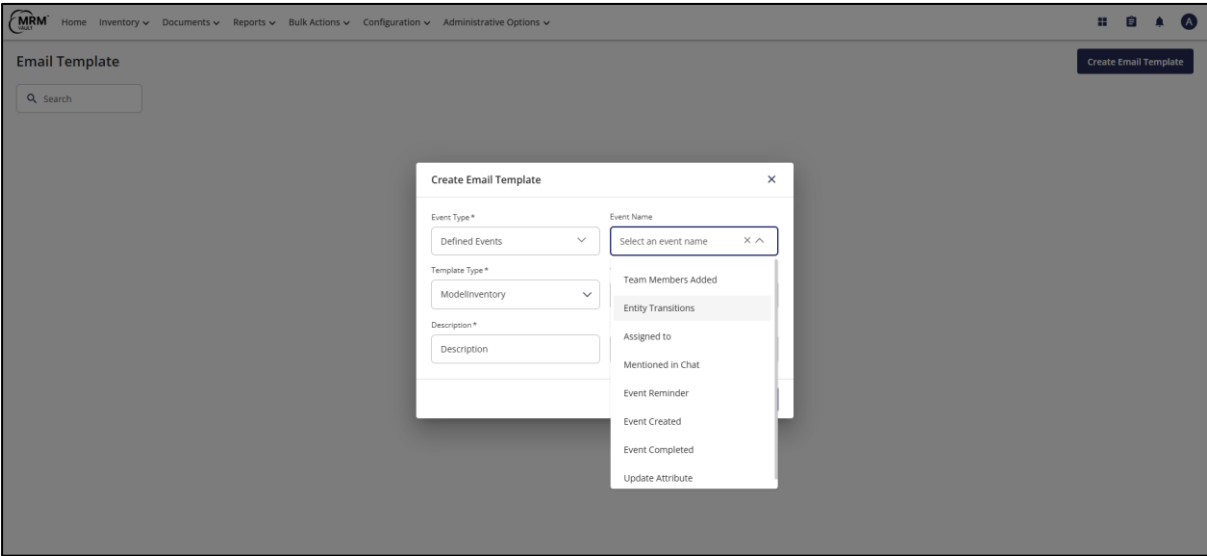
Our Understanding:

The client expects the MRM system to offer a comprehensive and configurable notification framework that aligns with model governance workflows. Email alerts should ensure that all relevant stakeholders (e.g., Model Owner, Validator, Governance Team) are promptly informed of lifecycle events and pending actions. The notification system should be modular supporting dynamic field insertion, configurable templates, role-based routing, and auditability of notification history to ensure transparency, accountability, and timely communication.

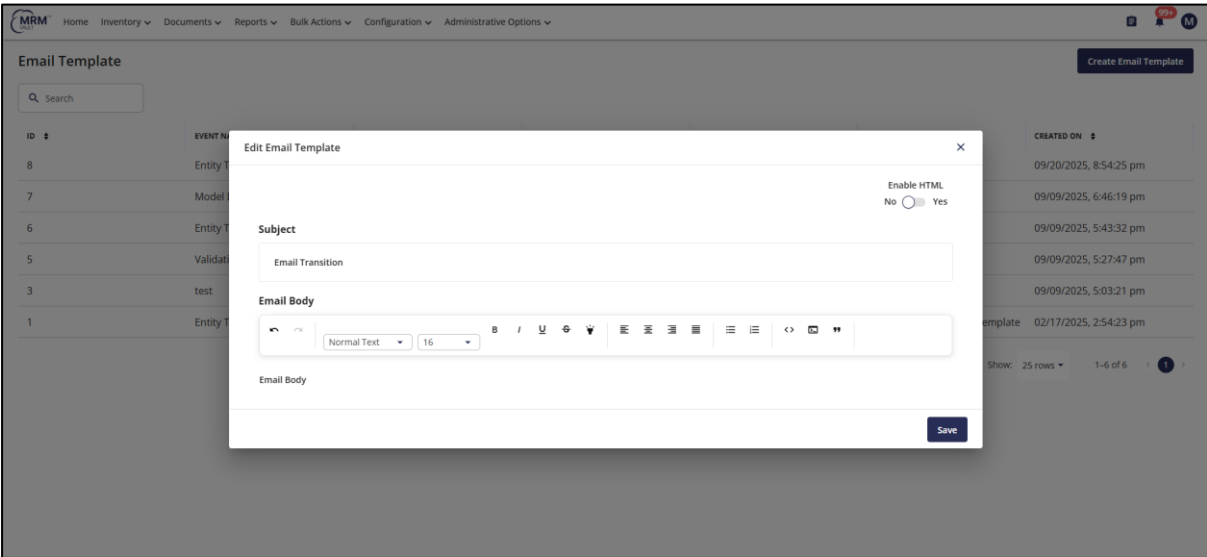
Solytics Response -:

Requirement	How MRM Vault Handles This	Status
Automated Email Notifications	<p>MRM Vault automatically triggers email notifications for lifecycle events (submission, approval, return) through predefined notification templates.</p> <ul style="list-style-type: none"> • Administrators can link additional notification rules to workflows through the no-code configuration UI, defining the event trigger (e.g., approval, SLA breach) and corresponding recipients • Configuration involves mapping triggers to workflows — no code required. 	Configuration Required
Configurable Templates	<p>Email templates are fully configurable and can be defined at an Inventory level through automation triggers or workflow-specific level. Templates support placeholders for Model ID, Model Name, Owner, and Stage, ensuring consistency across notifications. All templates are stored in a centralized repository with version control and audit logs.</p>	Configuration Required
Recipient & Role Mapping	<p>Recipient lists are dynamically derived from workflow roles (Model Owner, Validator, Reviewer, Oversight Committee).</p> <p>Administrators can define one-to-many mappings — for example, Model Owner + Risk Oversight receive submission alerts for high-risk models. Conditional mapping is supported (e.g., AI/ML model → AI Governance Committee).</p>	Configuration Required
Administrator Control	<p>Authorized administrators can add, modify, or deactivate notification rules through the</p>	Out of the Box

	<p>configuration interface without IT support.</p> <p>Bulk management actions (e.g., enabling bulk workflow actions, updates which trigger emails) are supported, ensuring centralized control and operational efficiency.</p>	
Dynamic Fields & Customization	<p>Templates support dynamic placeholders (e.g., {{Model_ID}}, {{Stage_Name}}, {{Owner}}, {{Submission_Date}}).</p> <p>These tags auto-populate during email generation, ensuring context-rich communication aligned with workflow data.</p>	Configuration Required
Escalation & Overdue Alerts	<p>Escalation notifications are configurable at multiple levels e.g., first escalation after 3 days of inactivity, second after 7 days.</p> <ul style="list-style-type: none"> Overdue alerts automatically trigger when SLA thresholds are breached. Notifications can be customized per workflow stage and role, ensuring prompt action and visibility for pending approvals. 	Configuration Required
Enable/Disable Alerts	<p>Administrators can enable or disable notification rules or recipients in real time.</p> <p>Deactivation does not delete history; all previously triggered emails remain stored in audit logs for governance traceability.</p>	Configuration Required
Audit Trail of Emails	<p>All outbound emails are logged with sender, recipient, timestamp, subject, and trigger event.</p> <ul style="list-style-type: none"> Email audit logs are accessible through the “Notification History” dashboard and exportable in CSV/PDF format for compliance or audit reporting Logs cannot be modified or deleted. 	Configuration Required
Ease of Maintenance	<p>Email configurations are managed via the admin UI using simple point-and-click options.</p> <p>Changes to global templates or escalation rules follow an optional review workflow before deployment, ensuring governance oversight and reducing dependency on IT teams.</p>	Configuration Required



Reference Image 1: Email Configurability; Emails for different actions in Model



Reference Image 2: Email Subject and Body; Define the email subject and body content for notifications to be sent during workflow events.

MRM Vault

DashboardInventoryModel ArtifactsDocumentsRules & ReportsBulk ActionsConfigurationAdmin Options

Email Template Inventory

Email TemplatesLogs

Q Search

User2024-11-082024-12-23Log ActionWorkflowState

EMAIL SUBJECT	STATUS	DATE SENT	RECIPIENT	ERROR MESSAGE
Model Risk Assessment	Sent	11/2/2024 2:30 PM	bob.ross@solytics.com	jane.doe@solytics.com
Regulatory Compliance Review	Sent	11/2/2024 2:30 PM	alice.smith@solytics.com	charlie.brown@solytics.com
Quantitative Model Validation	Sent	11/2/2024 2:30 PM	david.jones@solytics.com	emily.davis@solytics.com
Model Governance Framework	Sent	11/2/2024 2:30 PM	frank.white@solytics.com	grace.lee@solytics.com
Risk Appetite Statement	Sent	11/1/2024 10:00 AM	hannah.martin@solytics.com	ian.thomas@solytics.com
Model Inventory Management	Sent	11/1/2024 10:00 AM	julia.clark@solytics.com	kevin.wilson@solytics.com
Stress Testing Procedures	Sent	11/1/2024 10:00 AM	lisa.miller@solytics.com	mike.hall@solytics.com
Model Performance Monitoring	Sent	10/31/2024 4:15 PM	nancy.roberts@solytics.com	oliver.kelly@solytics.com
Model Development Standards	Sent	10/31/2024 4:15 PM	paul.adams@solytics.com	quincy.james@solytics.com
Scenario Analysis Techniques	Sent	10/31/2024 4:15 PM	rachel.walker@solytics.com	steve.harris@solytics.com
Model Documentation Requirements	Sent	10/30/2024 11:59 AM	tina.allen@solytics.com	uma.scott@solytics.com
Independent Validation Process	Sent	10/30/2024 11:59 AM	vicky.green@solytics.com	will.morris@solytics.com
Data Quality Assessment	Sent	10/30/2024 11:59 AM	xander.thompson@solytics.com	yara.baker@solytics.com

Showing 1 - 5 out of 100<123...8910>Show : 5 rows

Reference image 2: Email Logs; Emails dispatched from MRM Vault are fully traceable via detailed logs. Each log entry captures the email subject, delivery status, date and timestamp, and associated metadata, ensuring transparency and auditability.

MRM™
VAULT

HomeInventory ▾Documents ▾Reports ▾More ▾

99+

M

Automation > Update Automation

Save Automation

Automation name *

Validation Type Email Trigger

Disabled ☐ Enabled ☒

⌚ When: Update Attribute

⚡ Then: Send Mail

Add Component

⌚ Update Attribute

This rule will trigger when the value of the fields selected below changes.

Select field type *

Global Attributes ▾

Template type *

ModelAssociation ▾

Template Name *

Validation ▾

Attribute to monitor for change *

Validation type ▾

Submit

Reference Image 3: Emails notification using Automation; Emails can be triggered using automations

Reference Image 4: Emails notification using dynamic templates; Automated email notifications can be triggered using dynamic templates. These templates leverage metadata such as model attribute values and users associated with specific roles to personalize and contextualize the message. This setup enables scalable, role-based communication tailored to the lifecycle or state of the model.

4.1.7 Notifications

Requirement:

Provide an in-built notifications functionality (bell icon in the UI) that acts as a central, real-time task and alert inbox for users.

This functionality should ensure users are promptly informed of key lifecycle events/activities (e.g., task assignment, submission, approval, return, and status changes) and can take timely action directly from the application interface.

Our Understanding:

A UI-based notification center that functions as an internal alert hub within MRM Vault, complementing email notifications.

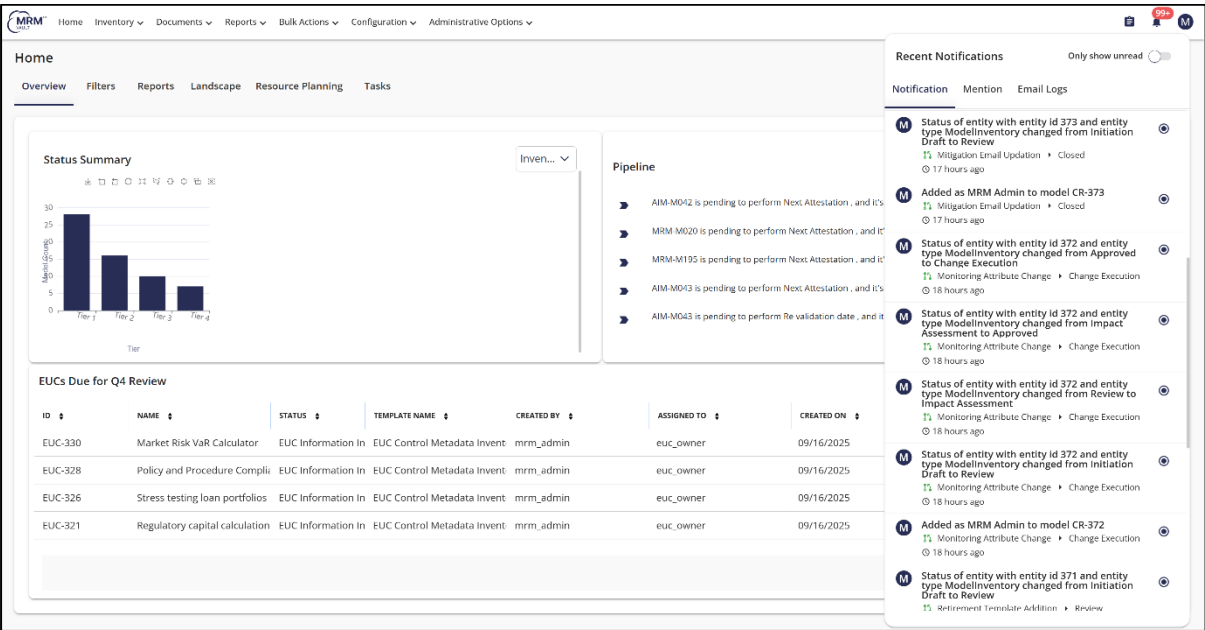
The feature should:

- Display real-time updates triggered by workflow events.
- Serve as a centralized inbox for tasks and alerts relevant to the logged-in user.
- Support clickable notifications for quick navigation to the related record or task.

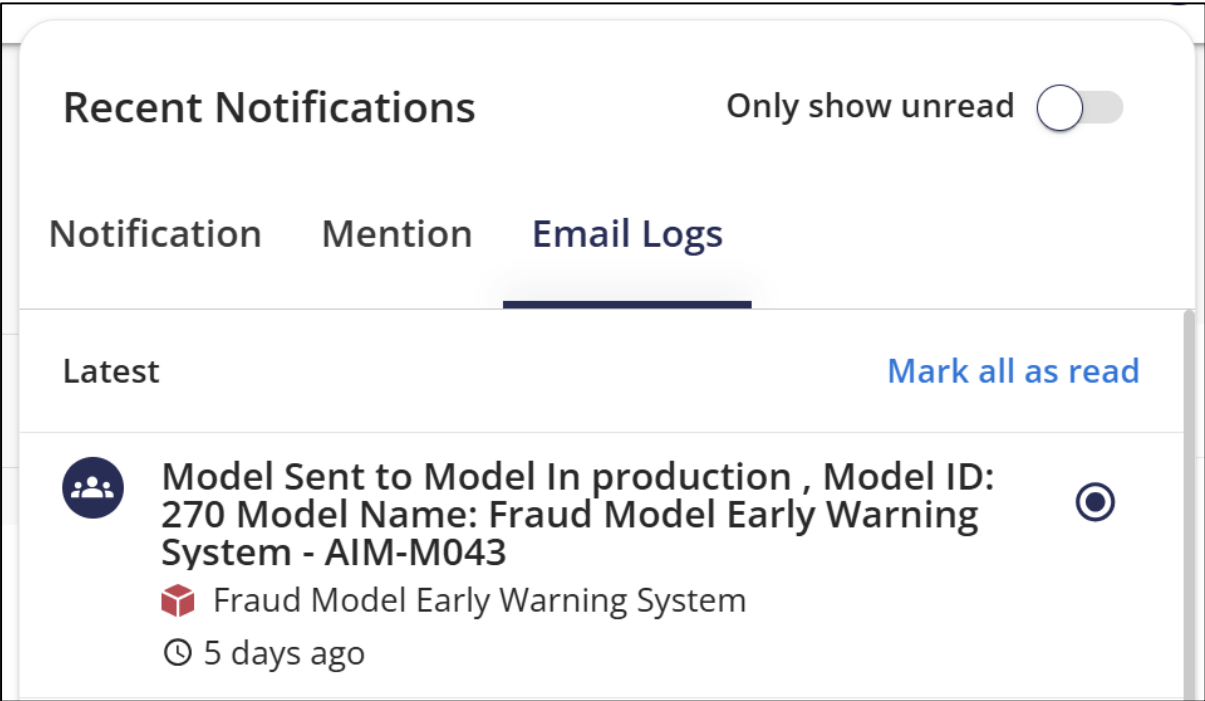
- Maintain read/unread status, timestamp, and contextual message details.
- Improve user responsiveness by minimizing dependency on email alerts for time-sensitive actions.

Solytics Response:

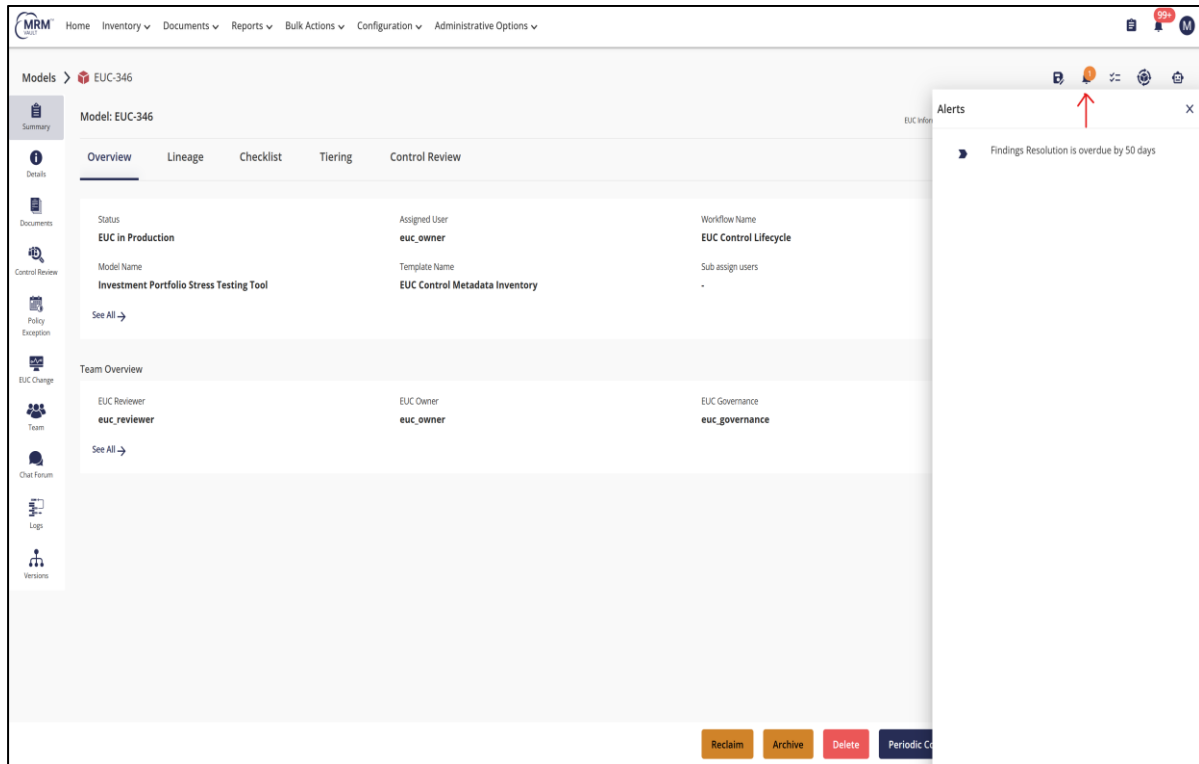
Requirement	How MRM Vault Handles This	Status
In-Built Notification Center (Bell Icon)	MRM Vault includes a real-time notification hub accessible via the bell icon in the header UI. It displays count badges, read/unread status, and supports filtering by event type (e.g., submission, approval). Users can access their centralized alert inbox to track pending actions and recently completed items. This includes mentions in chats, emails sent to the user.	Out of the Box
Real-Time Updates	Notifications are generated instantly upon workflow-triggered events (e.g., submission, reassignment, return) using MRM Vault's event-driven push architecture. The system updates the user's alert inbox in real time without page refresh, ensuring immediate visibility of critical actions.	Out of the Box
Actionable Alerts	Each in-app alert is actionable users can click directly to open the related record (model form, validation task, approval screen). <ul style="list-style-type: none"> • Access is permission-controlled, ensuring users are routed to view-only or edit mode based on RBAC rights. • This design minimizes navigation friction and speeds up task resolution. 	Configuration Required
Role-Based Visibility	MRM Vault dynamically filters alerts based on the user's active role and access permissions at runtime. Only alerts for workflows or records the user can act upon are displayed. Role reassignment automatically updates the visibility scope to ensure segregation of duties.	Configuration Required
User Experience	Notifications display a concise message summary, timestamp, and event type. Users can mark alerts as read/unread, view hover previews, and group alerts by model or workflow stage for easier prioritization.	Out of the Box
Audit & Traceability	All notifications are logged for traceability, ensuring audit readiness. This enables review of which alerts were triggered, viewed, or acted upon.	Out of the Box
Integration with Workflow Events	MRM Vault's notification system is tightly integrated with its Workflow Designer. Each workflow transition (submission, approval, reassignment, closure) automatically triggers a relevant in-app alert.	Configuration Required



Reference Image 1: Notifications pre-configured in MRM Vault; The screenshot covers notifications for model status updated via workflows, role assignments in models.



Reference Image 2: Email Logs; High level summary of trigger and connected model for which an email will be sent, with timestamp, option to mark notification as read/unread.



Reference Image 3: Model level notifications; MRM Vault support notifications at platform level and granular level in a model to enable effective MRM Operations.

Core Requirement for Notification

Requirement:

Implement a Real-Time In-App Notification Framework that provides users with immediate, contextual alerts for key lifecycle events (e.g., registration submitted, validation assigned, SLA breach).

The feature must support:

- Centralized visibility through a notification panel with unread counts.
- Role-based targeting to ensure relevant delivery.
- Configurable triggers managed by MRM Oversight without IT support.
- Priority levels, escalation, and persistence for critical alerts.
- Workflow integration for clickable, actionable notifications.
- Full audit trail, consistency with email alerts, and customizable content accessible across devices.

Our Understanding:

A comprehensive in-system notification hub that acts as a real-time governance cockpit for users. The goal is to ensure that users (Model Owners, Validators, Oversight, etc.) are informed instantly of model lifecycle events, SLA breaches, or pending approvals through a non-intrusive,

interactive bell icon panel in the UI. Notifications must be configurable, auditable, and synchronized with email alerts to maintain uniformity and ensure timely action.

Requirement	How MRM Vault Handles This	Status
Real-Time Alerts	MRM Vault pushes instant alerts for key events (e.g., submission, validation, SLA breach) via the workflow engine. Notifications appear immediately in the user's in-app panel.	Configuration Required
Centralized Visibility	A unified notification hub (bell icon) aggregates all alerts with unread counts, allowing users to view and act on pending items from a single interface.	Configuration Required
Role-Based Targeting	Notifications are filtered dynamically using role and ownership mappings so users only see alerts relevant to their assigned models or responsibilities.	Configuration Required
Configurable Triggers	MRM Oversight can configure event triggers (e.g., submission, approval, return, SLA breach) via admin UI without IT dependency. Any triggered event also generates a linked in-app notification.	Configuration Required
Escalation & Prioritization	Notifications highlight critical or overdue tasks based on workflow transitions and SLA breaches, enabling early detection and timely escalation.	Out of the Box
Workflow Integration	Each alert includes a clickable deep link that opens the related model, form, or task directly, enabling immediate follow-up.	Out of the Box
Persistence & Tracking	Notifications remain until the task is completed or acknowledged. A detailed log (event, timestamp, recipient, action) is retained for audit.	Out of the Box
Consistency with Emails	All lifecycle events that trigger emails also generate corresponding in-app alerts, ensuring uniformity across communication channels.	Out of the Box
User Experience	Users access updates via a panel with three tabs: Notifications, Mentions, and Email Logs. <ul style="list-style-type: none"> Notifications show workflow alerts (e.g., role changes, status updates) with details like entity ID, role assigned, and workflow transitions (e.g., "Initiation of Identification" → "MRG Review"). 	Out of the Box

	<ul style="list-style-type: none"> Filters allow users to view only unread items, helping prioritize tasks and stay informed. Mentions list chat tags; Email Logs track all sent emails. 	
Administration & Editability	Admins can create or modify triggers and enable/disable alerts directly from the workflow configuration UI without IT support.	Configuration Required
Trigger Types	Supports both user-initiated (e.g., submission) and system-triggered actions (e.g., SLA breach, reassignment) for comprehensive coverage.	Configuration Required

4.1.8 Reports

For detailed mockups/designs on reporting & dashboard requirements, Refer to: **MRM Vault_ Solytics Partners_Reporting Process Design.docx** located in - [HDFC FSD 1 Reference Documents](#) , for detailed mockups and reporting design workflows.
Access Password: hdfc@FSD2025

Requirement:

Inventory Reporting (Point-in-Time Snapshot) — The system must provide static reports showing the state of the model inventory as of a specific date or period (weekly, monthly, quarterly, yearly).

Reports should display:

- Overall model count by use case, materiality (High/Medium/Low), and scope (In-Scope/Out-of-Scope).
- Distribution by lifecycle status (Registered, Under Development, Under PDV, Under PIT, Active, Retired).
- Ability to view portfolio composition at a given point in time for management and regulatory reporting.

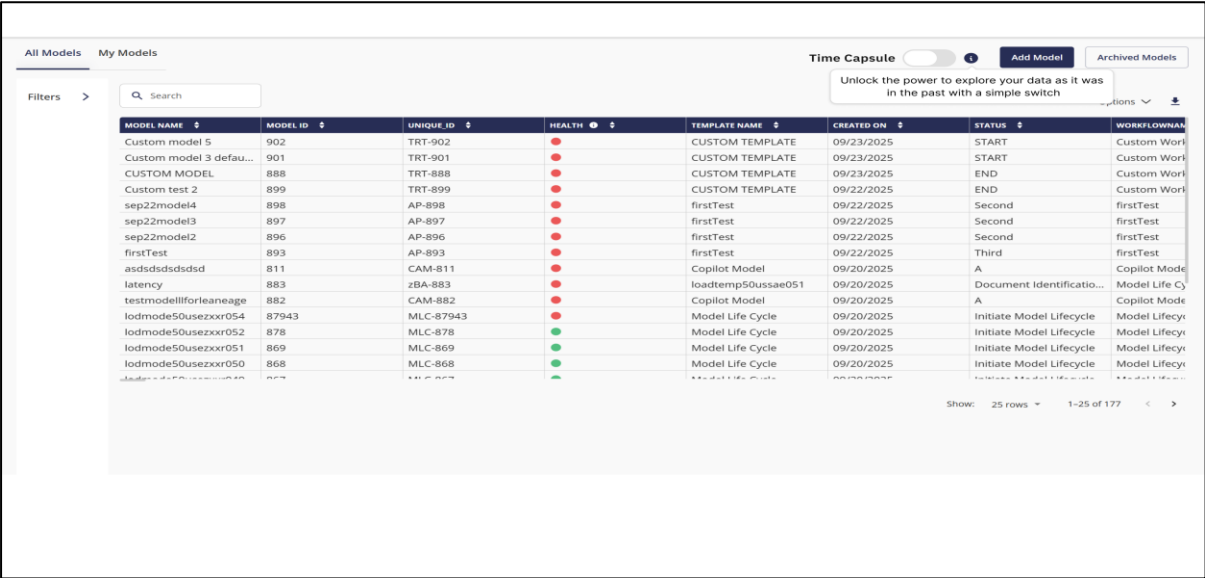
Our Understanding:

The client requires the capability to generate time-bound, point-in-time snapshots of the model inventory for management and regulatory reporting purposes. These reports should allow governance users to understand the current composition and distribution of the inventory based on various parameters use case, materiality, scope, and lifecycle stage and observe changes over time. Snapshots should be static (non-editable once generated), timestamped, and retrievable later for reference, enabling consistent portfolio monitoring and audit support.

Solytics Response:

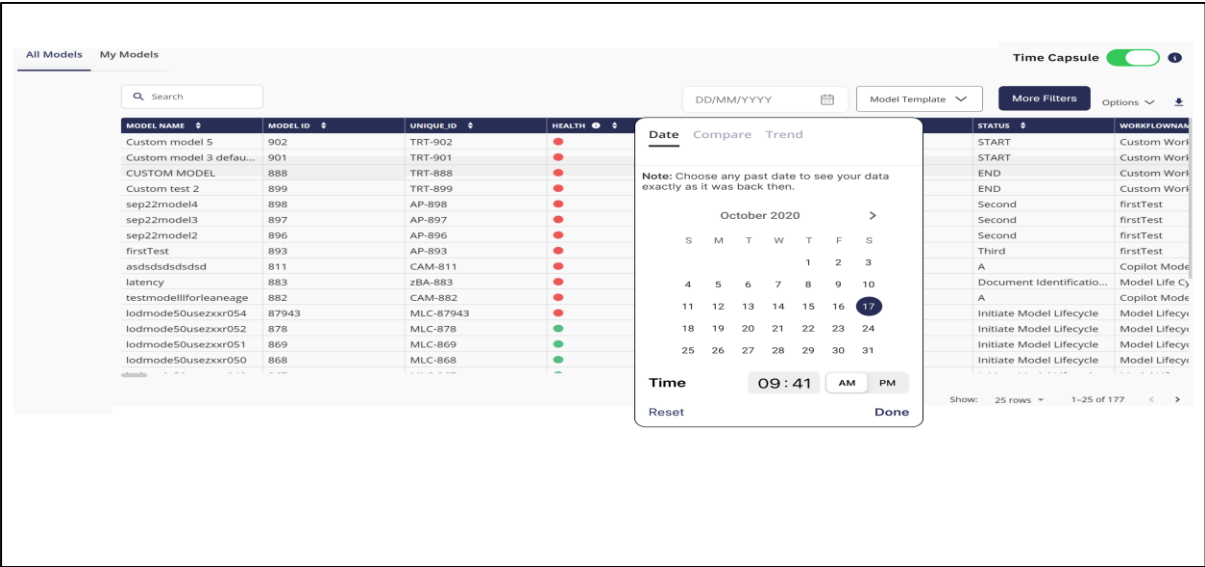
Requirement	How MRM Vault Handles This	Status
Point-in-Time Inventory Snapshot	<p>MRM Vault enables authorized users (e.g., MRM Admins, Oversight) to generate or schedule snapshot-based inventory reports that capture the entire model portfolio as of a selected date or reporting frequency (weekly, monthly, quarterly, yearly), this can be done using “Time Capsule” toggle in the Model Inventory page.</p> <p>Once generated, each snapshot is versioned, timestamped, and immutable, ensuring consistent audit references and preventing overwrites.</p>	Configuration Required
Model Count by Dimensions	<p>Reports include total model counts grouped by multiple dimensions, such as use case, materiality (High/Medium/Low), and scope (In-Scope/Out-of-Scope).</p> <p>Users can filter, sort, and aggregate these views or export them to Excel/PDF for further analysis</p>	Configuration Required
Lifecycle Status Distribution	Inventory snapshots automatically categorize models by lifecycle stages (Registered, Under Development, Under PDV, Under PIT, Active, Retired). Lifecycle stages are configurable to align with the Bank’s governance policy.	Out of the Box
Trend and Movement Tracking	MRM Vault enables users to select data points like models or attribute values and compare movement of data based on the time period or value changes to determine trends.	Configuration Required
Historical Reporting and Retention	All generated snapshots are archived and retrievable as per SLA & policies setup, this data can always be analyzed and are retained as per SLAs.	Out of the Box
Regulatory and Management Reporting Utility	<p>Reports support both management and regulatory needs by presenting summarized data and visual insights (charts, trend indicators).</p> <p>They can be directly embedded into management dashboards or exported as formatted outputs for regulatory submissions.</p>	Out of the Box
Governance Insights	The platform includes governance indicators that automatically flag delayed validations, overdue monitoring, or approval bottlenecks based on SLA parameters stored in the configuration table – enabled	Configuration Required

	through Tasks Tab and automated notifications for upcoming activities as well as delayed activities. Trend data can be filtered by area, owner, or model type to identify recurring governance risks.	
Ease of Access & Export	Reports are exportable in multiple formats (PDF, CSV) for data matching criteria like date, trend and comparison of values.	Configuration Required



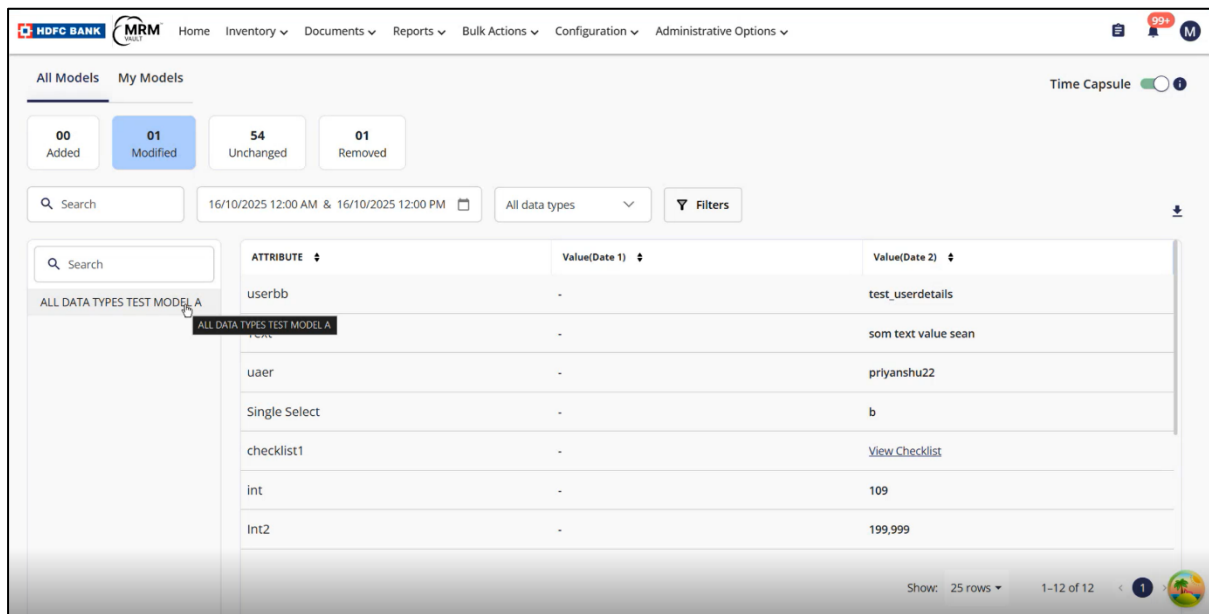
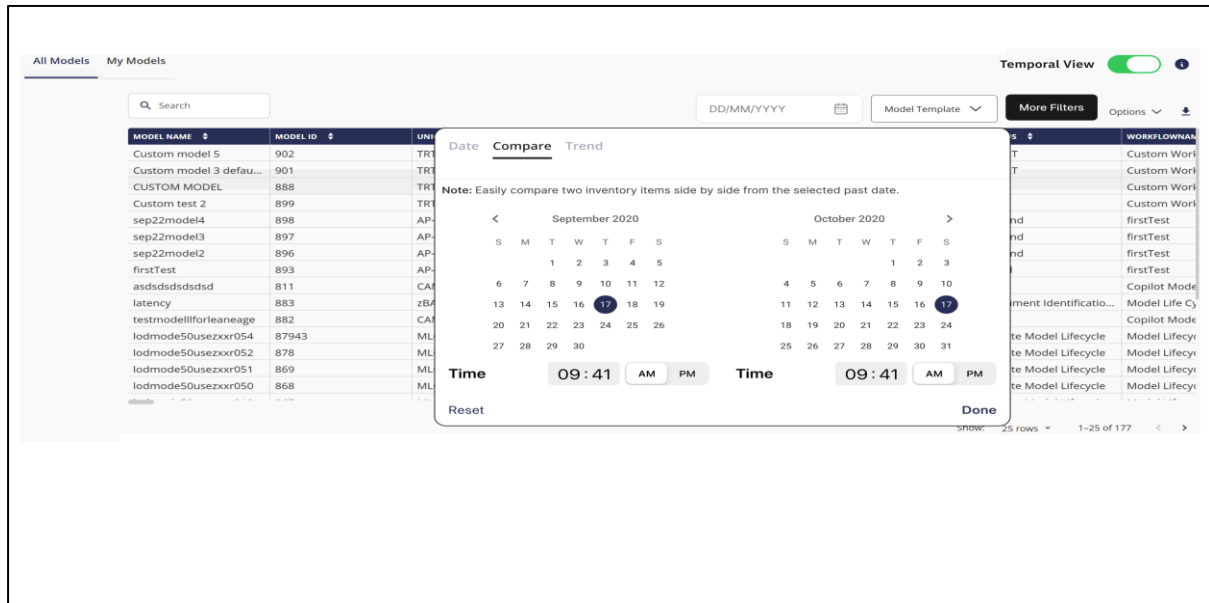
MODEL NAME	MODEL ID	UNIQUE_ID	HEALTH	TEMPLATE NAME	CREATED ON	STATUS	WORKFLOWNAME
Custom model 5	902	TRT-902	●	CUSTOM TEMPLATE	09/23/2025	START	Custom Work
Custom model 3 default	901	TRT-901	●	CUSTOM TEMPLATE	09/23/2025	START	Custom Work
CUSTOM MODEL	888	TRT-888	●	CUSTOM TEMPLATE	09/23/2025	END	Custom Work
Custom test 2	899	TRT-899	●	CUSTOM TEMPLATE	09/22/2025	END	Custom Work
sep22model4	898	AP-898	●	firstTest	09/22/2025	Second	firstTest
sep22model3	897	AP-897	●	firstTest	09/22/2025	Second	firstTest
sep22model2	896	AP-896	●	firstTest	09/22/2025	Second	firstTest
firstTest	893	AP-893	●	firstTest	09/22/2025	Third	firstTest
asdsdsdsdsdsd	811	CAM-811	●	Copilot Model	09/20/2025	A	Copilot Mode
latency	883	zBA-883	●	loadtemp50ussae051	09/20/2025	Document Identification...	Model Life Cy
testmodellforleaneage	882	CAM-882	●	Copilot Model	09/20/2025	A	Copilot Mode
lodmode50usezxr054	87943	MLC-87943	●	Model Life Cycle	09/20/2025	Initiate Model Lifecycle	Model Lifecy
lodmode50usezxr052	878	MLC-878	●	Model Life Cycle	09/20/2025	Initiate Model Lifecycle	Model Lifecy
lodmode50usezxr051	869	MLC-869	●	Model Life Cycle	09/20/2025	Initiate Model Lifecycle	Model Lifecy
lodmode50usezxr050	868	MLC-868	●	Model Life Cycle	09/20/2025	Initiate Model Lifecycle	Model Lifecy

Reference Image 1: Time Capsule; Authorized users can enable Time Capsule to select Date for which data has to be investigated.



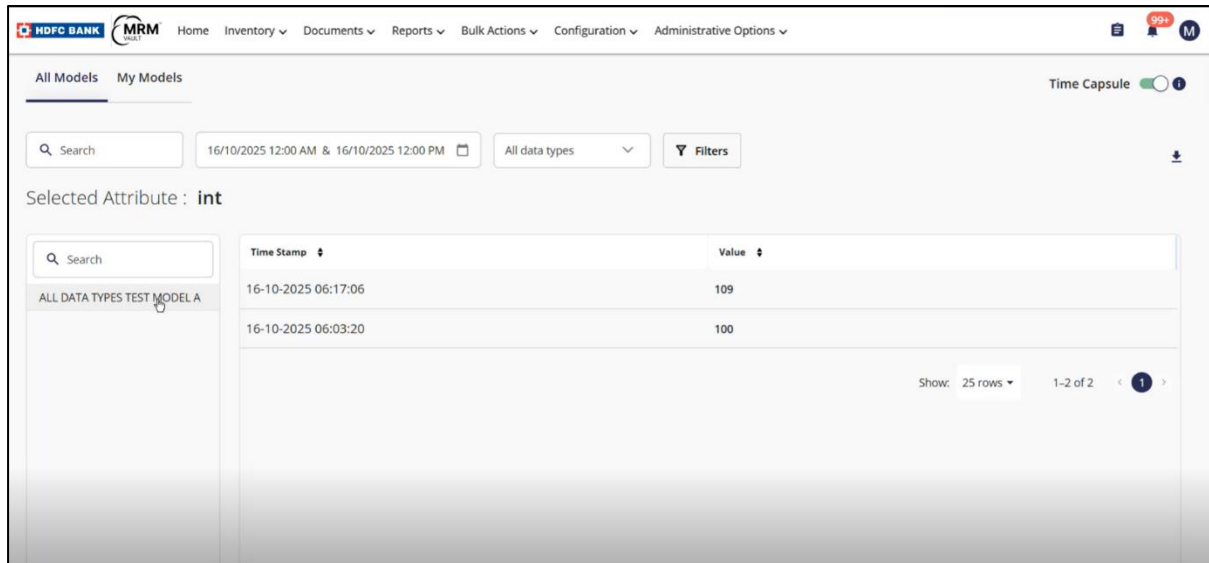
MODEL NAME	MODEL ID	UNIQUE_ID	HEALTH	STATUS	WORKFLOWNAME
Custom model 5	902	TRT-902	●	START	Custom Work
Custom model 3 default	901	TRT-901	●	START	Custom Work
CUSTOM MODEL	888	TRT-888	●	END	Custom Work
Custom test 2	899	TRT-899	●	END	Custom Work
sep22model4	898	AP-898	●	Second	firstTest
sep22model3	897	AP-897	●	Second	firstTest
sep22model2	896	AP-896	●	Second	firstTest
firstTest	893	AP-893	●	Third	firstTest
asdsdsdsdsdsd	811	CAM-811	●	A	Copilot Mode
latency	883	zBA-883	●	Document Identification...	Model Life Cy
testmodellforleaneage	882	CAM-882	●	A	Copilot Mode
lodmode50usezxr054	87943	MLC-87943	●	Initiate Model Lifecycle	Model Lifecy
lodmode50usezxr052	878	MLC-878	●	Initiate Model Lifecycle	Model Lifecy
lodmode50usezxr051	869	MLC-869	●	Initiate Model Lifecycle	Model Lifecy
lodmode50usezxr050	868	MLC-868	●	Initiate Model Lifecycle	Model Lifecy

Reference Image 2: Time Capsule date selector.



Reference Image 3 & 4: Time Capsule data comparison selector & view with summary of changes for selected date range in attribute values.

Note: Time capsule enables user to analyze inventory data based on temporal view i.e. basis inventory snapshot in the past.



Reference Image 5: Time Capsule trend view; Attribute value change trend shown with timestamp of when the value was updated.

4.1.9 Dashboards

Requirement:

The Model Risk Management (MRM) system must provide comprehensive, role-based dashboards to enable stakeholders to monitor, manage, and oversee model lifecycle activities effectively.

Dashboards should serve as the single source of truth for real-time insights into:

- Model inventory composition and lifecycle progress,
- Validation and review statuses,
- Governance activities and attestation timelines, and
- Regulatory compliance metrics.

Dashboards must support multiple stakeholder views — including Business Model Owners, Validators, Risk Oversight, Governance Committees, Senior Management, and Regulators — while ensuring role-appropriate access and strict data security through RBAC enforcement.

Our Understanding:

MRM Vault must provide dynamic and role-specific dashboards that consolidate all relevant model risk management information into a single, unified interface.

Each user role should see a customized dashboard aligned with their responsibilities — for instance:

- Model Owners: lifecycle progress, upcoming submissions, pending validations;
- Validators: models due for validation, SLA compliance;
- Governance Teams: approvals, exceptions, attestations;

- Senior Management: aggregate metrics, portfolio health, regulatory alignment.

Dashboards should provide real-time, accurate data sourced from the centralized model inventory, eliminating the need for manual reconciliation and ensuring consistent reporting across the organization.

Solytics Response:

Requirement	How MRM Vault Handles This	Status
Real-Time Data Source (Single Source of Truth)	<p>All dashboards in MRM Vault are sourced directly from the centralized model inventory database, ensuring near real-time synchronization across modules (Models, Validations, Workflows, and Documents).</p> <p>Data refresh frequency is configurable to balance performance and accuracy, maintaining consistency across all reporting and visualization layers.</p>	Out of the Box
Role-Based Dashboards	<p>MRM Vault applies granular Role-Based Access Control (RBAC) to dashboard views.</p> <ul style="list-style-type: none"> • Each user automatically receives dashboards aligned to their active roles (e.g., Owner, Validator, Oversight, or Senior Management). • Users with multiple roles can toggle between role-specific views as permitted under RBAC configurations. 	Configuration Required
Lifecycle & Validation Monitoring	<p>Dashboards display lifecycle and validation metrics such as model count by stage (Registered, PDV, PIT, Active, Retired) and real-time validation statuses (Due, In Progress, Completed, Overdue). Validation timelines and SLA compliance are dynamically tracked to support governance review.</p>	Out of the Box
Governance & Compliance Tracking	<p>Governance dashboards display KPIs related to approvals, exceptions, attestations, and compliance metrics.</p> <p>These KPIs are automatically derived from workflow events and attestation submissions, allowing Governance and Oversight teams to identify overdue items and track policy adherence.</p>	Configuration Required
Portfolio Composition & KPIs	<p>Dashboards visualize model composition by parameters such as use case, business line, materiality, and risk tier.</p>	Configuration Required

	<ul style="list-style-type: none"> Trend indicators highlight concentration risks, overdue validations, or materiality changes. KPI widgets can be customized by Admins to align with internal governance and risk frameworks. 	
Data Security & Access Control	<p>RBAC restricts data visibility based on user role and access rights.</p> <ul style="list-style-type: none"> Sensitive attributes (e.g., risk ratings, validator comments) are masked for unauthorized users. All access attempts and visibility changes are logged for audit trail and regulatory compliance. 	Configuration Required
Customizable Views	<p>Admin and authorized users can create or rearrange dashboard widgets using a drag-and-drop interface.</p> <ul style="list-style-type: none"> Custom views can be saved at user or global level and persist across sessions. Visualization types (charts, tables, heatmaps) and filters are configurable without IT dependency. 	Configuration Required
Export & Reporting Integration	<p>Dashboards can be exported to Excel/PDF while preserving applied filters and date ranges. They can also be scheduled for automated distribution or integrated with reporting workflows for periodic management reviews and regulatory submissions.</p>	Out of the Box
Performance & Scalability	<p>Dashboards are performance-optimized to handle large inventories (tested up to thousands of models) with minimal load time. Users can drill down from portfolio summaries into model-level or validation-level detail while maintaining context and data lineage.</p>	Out of the Box

A. Inventory & Governance Dashboards

Requirement:

The system must provide Inventory & Governance Dashboards displaying:

- Total models in inventory, categorized by risk tier, business unit, and model type (AI/ML, statistical, vendor, etc.).
- Registration and lifecycle status (newly registered, pending approval, in-progress, etc.).
- Ownership and accountability views (by Model Owner, Validator, Committee).
- Governance workflow metrics, including pending approvals, escalations, and overdue actions.

These dashboards should give governance stakeholders a unified operational view of model inventory composition and governance health at any point in time.

Our Understanding:

The client expects a real-time operational dashboard that consolidates inventory and governance data into actionable, role-specific insights.

The dashboards must:

- Pull data directly from the central model inventory and workflow engine.
- Reflect real-time model counts and governance statuses.
- Support filtering by business unit, tier, model type, owner, and validator.
- Enable governance monitoring by tracking approvals, escalations, and overdue tasks; and
- Serve as a decision-support tool for both operational and management-level stakeholders.

Solytics Response:

Requirement	How MRM Vault Handles This	Status
Inventory Breakdown (Risk Tier, Business Unit, Model Type)	The dashboard displays a summary view of total models with segmentation by risk tier (High/Medium/Low), business unit, and model type (AI/ML, Statistical, Vendor). Widgets are configurable for bar, pie, or tabular visualization.	Configuration Required
Registration & Lifecycle Status Tracking	MRM Vault provides real-time counts of models by registration and workflow status — e.g., <i>Newly Registered</i> , <i>Pending Approval</i> , <i>Under Validation</i> , <i>Active</i> , <i>Retired</i> . Users can drill into Inventory filters for model status and in models for the detailed breakdown.	Configuration Required
Ownership & Accountability View	Dashboards group and filter data by ownership roles (Model Owner, Validator, Governance Committee). <ul style="list-style-type: none"> • Each view highlights model counts, pending actions, and SLA status per role, ensuring accountability and enabling balanced workload distribution. • Escalation metrics can be configured to display by department or reviewer hierarchy. 	Configuration Required
Governance Workflow Status	Governance dashboards display key workflow indicators, including pending approvals, SLA breaches, escalations, and overdue validations.	Configuration Required

	<ul style="list-style-type: none"> SLA thresholds and escalation rules are configurable by Admin users within workflow setup. Widgets dynamically update based on workflow events (submission, review, approval) for near real-time monitoring. 	
Interactive Filters & Drill-Down	<p>MRM Vault allows interactive filtering by business unit, tier, owner, or workflow state.</p> <ul style="list-style-type: none"> Each widget supports drill-down to record-level detail (read-only view) for root cause or task-level analysis. Filters can be saved per session or globally for recurring analysis. 	Configuration Required
Role-Based Views	<p>Dashboard access and data visibility are governed by RBAC.</p> <ul style="list-style-type: none"> Users only view data relevant to their assigned models or roles (Owner, Validator, Governance). Users with multiple roles can toggle between role views while maintaining data segregation and access controls. 	Configuration Required
Visualization & Export Options	<p>Dashboards support multiple visual formats (bar, donut, trendline) and export options (Excel/PDF).</p> <ul style="list-style-type: none"> Exported views preserve applied filters and parameters. Admins can schedule exports for recurring governance or management reports. 	Configuration Required
Data Refresh & Integrity	<p>All metrics are dynamically sourced from the centralized model inventory, updating at configurable refresh intervals to ensure near real-time accuracy.</p> <ul style="list-style-type: none"> Dashboard data refreshes are logged, ensuring audit traceability and preventing manual reconciliation errors. 	Out of the Box

B. Validation & Monitoring Dashboards

Requirements:

The dashboards must provide real-time visibility into the Validation and Monitoring processes, offering detailed operational and analytical insights.

They should include:

- Validation Pipeline: models awaiting validation, in progress, or overdue.

- Pre-Deployment & Periodic Validation (PDV) Status: PDV outcomes, 2nd PDV, and revalidations.
- Validation findings: Whether open, closed, or overdue, are captured as part of PDV and monitoring activities. These findings are managed through the Query module, which enables structured tracking and resolution.
- Performance Monitoring: exceptions logged and remediation tracking.
- Outcome Distribution: insights by model type, risk tier, validation/monitoring TAT, outcome, and analyst performance.

Note: Certain reports, visualizations, and dashboards pertaining to Pre-Deployment Validation (PDV) and Monitoring will be made available in Sprint 2. This is because the dedicated configuration of the PDV and Monitoring satellite processes is planned for Sprint 2 as part of the phased implementation approach.

Our Understanding:

The client expects role-based, real-time dashboards that provide a holistic view of validation lifecycle and monitoring effectiveness.

The dashboard should:

- Reflect validation workloads and SLA adherence (e.g., models awaiting validation or overdue).
- Track PDV and periodic validation outcomes with stage-wise statuses.
- Display findings and exceptions logged during validation and monitoring, with closure tracking.
- Provide analytical views to assess validation throughput, turnaround times, and performance distribution by risk tier, model type, and analyst.

The dashboard must directly source data from the centralized inventory, validation workflow, and findings (query tracking) modules to ensure data integrity and timeliness.

Solytics Response:

Requirement	How MRM Vault Handles This	Status
Validation Pipeline Overview	<p>Dashboards present a near real-time pipeline of models under validation, segmented by stage — Awaiting Validation, In Progress, or Overdue.</p> <ul style="list-style-type: none">• Data refreshes automatically at configured intervals.• Access is role-based (Validators see assigned models; Governance and Oversight see aggregate status and SLA adherence).	Configuration Required

PDV & Periodic Validation Status	<p>PDV dashboards summarize Pre-Deployment and Periodic Validation outcomes, including 2nd PDVs and Re-validations.</p> <ul style="list-style-type: none"> • Widgets flag overdue PDVs based on configurable SLA rules and next review date. • Users can filter by model stage, validation type, outcome, or upcoming due date. 	Configuration Required
Validation Findings Management	<p>MRM Vault dashboards will integrate the Query Tracking module (Sprint 2) to display validation and monitoring findings along with query owner, due date, remediation status, and closure timelines.</p> <p>Users will be able to view and update remediation status (where permitted), ensuring timely resolution and audit-ready visibility of open findings.</p>	Enhancement Required (post-query tracking integration)
Performance Monitoring Metrics	<p>Monitoring dashboards track exceptions (e.g., missed validation turnarounds, pending remediations) and closure timelines by model or business unit.</p> <p>KPIs such as average TAT, SLA breach count, and remediation completion rate are auto-calculated and visualized for trend comparison</p>	Configuration Required
Outcome Distribution Analytics	<p>Dashboards present breakdowns of validation and monitoring outcomes by model type, risk tier, and analyst performance.</p> <ul style="list-style-type: none"> • Visuals include trend lines for TAT, overdue ratios, and validation frequency. • Data is pulled from validation workflow and performance modules to enable benchmarking and resource planning. 	Configuration Required
Role-Based Dashboard Views	<p>Validators, Risk Oversight, and Governance teams access role-specific dashboards.</p> <ul style="list-style-type: none"> • Validators view assigned models and open findings; Oversight monitors SLA breaches and trends; Governance reviews portfolio-level health. • Multi-role users can toggle views through RBAC without data overlap. 	Configuration Required
Visualization & Drill-Down	<p>Interactive widgets (bar chart, table, heatmap) allow filtering and drill-down to model record or</p>	Configuration Required

	validation finding. Each visual element links to the underlying record in read-only mode for contextual review and audit reference.	
Real-Time Data Sourcing	Data is sourced directly from the centralized inventory, validation, and findings modules. Dashboards update at configurable intervals to ensure near real-time accuracy and data integrity while maintaining performance efficiency.	Out of the Box
Export & Reporting Capability	Dashboards are exportable to Excel and PDF formats for management and regulatory reporting. Each export is timestamped and logged for audit traceability and consistency across governance reviews.	Out of the Box

C. Change Management Dashboards

Requirement:

The system must provide Change Management Dashboards that visualize:

- The change request pipeline (initiated, pending approval, implemented),
- The impact of approved changes on related models, validations, and governance activities, and
- The version history of affected models for transparency and audit readiness.

Dashboards should support real-time insights into change activities, ensuring governance teams can monitor workflow progress, assess downstream effects, and maintain version control integrity.

Our Understanding:

The client expects a dedicated change management dashboard within MRM Vault that consolidates all change-related information into an interactive, role-based view.

This dashboard should:

- Provide real-time visibility of all active and completed change requests;
- Allow governance teams to track progress and approvals across the change lifecycle;
- Quantify the impact of changes (e.g., models requiring revalidation, updated metadata fields);
- Display version comparisons and maintain a traceable log of model revisions; and Support decision-making and regulatory attestation through transparent change tracking and auditability.

Solytics Response:

Requirement	How MRM Vault Handles This	Status
Change Request Pipeline	<p>Dashboards present a real-time pipeline of change requests segmented by status (Initiated, Pending Approval, Approved, Implemented, Rejected).</p> <ul style="list-style-type: none"> Users can filter by date, owner, change type, or impacted entity (model / artifact / workflow). SLA-based color cues highlight overdue approvals to help governance teams prioritize actions. 	Configuration Required
Impact Assessment	<p>MRM Vault maintains a structured Change Log capturing every modification to attributes, templates, workflows, and entities (models, assessments, artifacts, use cases).</p> <ul style="list-style-type: none"> Dashboards summarize the nature of each change (metadata update, revalidation trigger, ownership change) and its downstream impact (e.g., models requiring PDV re-run or attestation update). Users can filter changes by type, entity, or approval date, enabling transparency across the model ecosystem. 	Enhancement Required
Version History Visualization	<p>Dashboards integrate with the Vault's Versioning Engine to display attribute-level differences between pre- and post-change versions of model records and documents.</p> <ul style="list-style-type: none"> Users can view, compare, or download version snapshots for audit evidence. Visual diffs highlight updated fields, timestamp, and change owner for full traceability. 	Configuration Required
Workflow Integration	<p>Dashboard data syncs continuously with the Change Management workflow and Audit Log modules.</p> <ul style="list-style-type: none"> Approvals, rejections, and comments update in near real-time (typically within minutes of action). The integration ensures one-to-one traceability between workflow activity and dashboard entries. 	Configuration Required
Governance Oversight Metrics	<p>Governance dashboards track key KPIs — change volume, average approval turnaround time, pending approvals, and recurring change categories.</p>	Configuration Required

	<ul style="list-style-type: none"> SLA thresholds and aging bands (0–7 days, 8–14 days, 15+ days) can be configured to highlight bottlenecks. Trends help identify frequent update areas and inform process improvement. 	
Auditability & Traceability	<p>Each change is automatically logged with timestamp, user, change type, reason, and approval history.</p> <ul style="list-style-type: none"> Dashboards pull this data for audit readiness and export it to Excel or PDF for evidence submission. Audit entries are immutable and linked to the associated model version for end-to-end traceability. 	Out of the Box
Role-Based Access	<p>Dashboard access is governed by RBAC at both module and record levels.</p> <ul style="list-style-type: none"> Users see only changes related to their business unit or assigned models. Multi-role users (e.g., Validator + Governance) can toggle views without cross-access to restricted data. 	Configuration Required
Visualization & Exports	<p>Dashboards offer bar, donut, and trendline charts for change volume and turnaround times.</p> <ul style="list-style-type: none"> All visuals can be exported to Excel or PDF for regulatory submissions or internal attestation. Exports retain filters and metadata (e.g., date range, status, approver) for audit consistency. 	Configuration Required

D. MIS & Executive Dashboards

Requirement:

The system must provide strategic, high-level dashboards for MIS and Executive stakeholders, offering a top-down view of the model landscape to support decision-making, planning, and regulatory reporting.

Dashboards should include:

- Heatmaps showing distribution of models across key dimensions (e.g., Business Unit vs. Risk Tier).
- Population Trends track inventory growth, retirements, and rebuilds over time.
- Resource Allocation Insights highlighting validation workload vs. available capacity.

These dashboards should help senior management and governance leaders monitor portfolio evolution, assess capacity utilization, and identify emerging model risk patterns.

Our Understanding:

The client requires a Board-level management information system (MIS) dashboard suite that consolidates high-level analytics across the model lifecycle.

These dashboards should:

- Aggregate data from the entire model inventory and validation pipelines;
- Provide visual and trend-based summaries rather than operational details;
- Enable executive-level insights into risk exposure, resource utilization, and governance performance;
- Support strategic decision-making through dynamic, visualized KPIs (heatmaps, time trends, workload vs. capacity).

The focus is on aggregation, visualization, and interpretability, ensuring senior management receives concise and data-driven insights.

Requirement	How MRM Vault Handles This	Status
Aggregated Executive View	<p>Dashboards aggregate data from Model Inventory, Validation, and Governance modules into a unified executive view.</p> <ul style="list-style-type: none"> • Insights are refreshed at configurable intervals (daily/weekly snapshots) to ensure accuracy and audit stability. • This consolidated layer supports strategic decision-making by summarizing lifecycle health, SLA adherence, and governance posture. 	Configuration Required
Heatmaps	<p>Interactive heatmaps visualize model concentration across Business Unit, Risk Tier, and Model Type. Users can hover or filter to view counts and risk exposure by segment. Persistent filters enable consistent board-level reviews.</p>	Configuration Required
Population Trends	<p>MRM Vault's trend charts illustrate model population movements, new registrations, retirements, and rebuilds over time. Helps management understand portfolio evolution and growth rates.</p>	Configuration Required
Resource Allocation Insights	<p>Dashboards compare validator workload (by model count or effort hours) against available capacity.</p> <ul style="list-style-type: none"> • Governance teams can identify imbalances and plan reallocation. • Charts auto-update with workflow completion data to reflect real-time validator utilization. 	Configuration Required

Portfolio Composition Metrics	<p>Displays total model count segmented by Type (AI/ML, Statistical, Vendor) and Materiality (High/Medium/Low).</p> <ul style="list-style-type: none"> Aggregated risk exposure metrics (e.g., percentage of High-risk models) are auto-calculated to inform portfolio health. 	Configuration Required
Regulatory & Governance KPIs	<p>Executive dashboards track compliance KPIs including % models validated within SLA, % overdue validations, attestation timeliness, and validation closure rate.</p> <ul style="list-style-type: none"> All KPIs auto-refresh from underlying workflow data and display color-coded risk thresholds (R/A/G). 	Configuration Required
Visualization & Presentation	<p>Dashboards feature interactive visualizations (heatmaps, trend lines, scorecards) and summary tables for Board presentation.</p> <ul style="list-style-type: none"> Views can be exported to Excel/PDF while preserving filters and metadata. Reports can contain tables, visualization, pivots with templates for common exports. 	Out of the Box
Role-Based Access	<p>RBAC ensures only senior management, risk heads, and governance officers can access MIS dashboards. Aggregated summaries mask model-level identifiers to prevent sensitive exposure while still enabling full portfolio oversight</p>	Configuration Required
Performance & Scalability	<p>Dashboards are optimized for enterprise portfolios with rapid rendering (<10 seconds for aggregated visuals based on network latency). The architecture supports high-volume analytics with zero data duplication and stable concurrency handling.</p>	Out of the Box

E. Reporting & Extract Requirements

Requirement:

The system must enable users to export reports and dashboards and support automated, scheduled distribution of these reports to designated stakeholders.

Reports should be exportable in standard formats (e.g., Excel, PDF) and automatically generated and shared at defined intervals (e.g., weekly, monthly, quarterly) for governance committees and regulatory submissions.

Our Understanding:

The client expects the MRM system to provide both manual and automated reporting capabilities to support periodic governance reviews, internal reporting, and regulatory submissions.

This includes:

- The ability for users to export dashboards and reports on demand in common formats (Excel, PDF).
- A scheduler utility that automates recurring report generation and email distribution.
- Configuration flexibility so that business or governance users can set frequency, format, recipients, and filters without requiring IT intervention.
- Full auditability of scheduled runs and sent reports to maintain traceability.

Requirement	How MRM Vault Handles This	Status
Report & Dashboard Export	Users can export any report or dashboard to Excel (.xlsx) or PDF (.pdf) with all applied filters, column selections, and visual configurations intact. Each export carries a timestamp and report-ID for audit reference.	Configuration Required
Automated Scheduling	<p>A built-in Scheduler module lets authorized users create recurring jobs for report generation.</p> <ul style="list-style-type: none"> • Users can define frequency (daily/weekly/monthly), start date, and recipients through a no-code interface. • Each scheduled job is logged with execution status (success/failure) and error details. 	Configuration Required
Automated Distribution via Email	<p>MRM Vault's generated reports can be automatically emailed to predefined stakeholder groups (e.g., Governance Committee, Risk Oversight, Validation Leads) at scheduled times, ensuring timely dissemination.</p> <p>Emails are sent via secure SMTP.</p>	Configuration Required
Configuration Flexibility	<ul style="list-style-type: none"> • Business and governance users can configure report templates without technical assistance by selecting fields, filters, and output formats. • Enhanced filters and no-code data segmentation tools (Planned Sprint 2) will enable intuitive ad-hoc report creation. • This reduces IT dependency and increases agility in governance reporting. 	Configuration Required

Audit Trail of Distributed Reports	<ul style="list-style-type: none"> Every scheduled and manual report generation is logged with timestamp, initiating user, recipients, report type, and delivery status. Audit records are immutable and retained for a minimum of 3 years (or client-defined period) to ensure regulatory readiness, can be increased as per user requirement. 	Configuration Required
Use Cases Supported	<ul style="list-style-type: none"> Reporting framework supports periodic regulatory submissions, executive MIS dashboards, and committee pack generation. Templates for standard governance cycles (e.g., Quarterly Validation Review, Annual Model Attestation) can be pre-configured. 	Configuration Required
Security & Role-Based Access	<ul style="list-style-type: none"> RBAC ensures only authorized users can configure or receive specific reports. Role-based filters automatically exclude data outside a user's privilege scope (e.g., validator views own models only). Audit logs capture access to report exports and downloads to preserve traceability. 	Configuration Required

4.1.10 Attestation Process

For detailed mockups/designs on attestation process requirements, Refer to: 'MRM Vault_Solytics Partners_Attestation Process Design.docx' located in – Click here: [HDFC FSD 1 Reference Documents](#) for detailed screenshots and guide.
Access Password: hdfc@FSD2025

Requirement:

The MRM system must support multi-level attestations, bulk approvals, automated scheduling, full audit logging, and easy configuration all backed by clear dashboards and reporting tools for governance visibility. The functionality should enable governance teams to efficiently manage attestation cycles, track progress, and ensure accountability and regulatory compliance across multiple models simultaneously.

Our Understanding:

The client requires an attestation framework within the MRM platform that allows for:

- Multi-Level Attestations: Sequential or parallel approvals from multiple stakeholders (e.g., Model Owner → Validator → Governance Committee).

- **Bulk Approvals:** The ability to approve or attest multiple models simultaneously to improve operational efficiency.
- **Automated Scheduling:** Configurable scheduling of attestation cycles and reminder alerts (e.g., 1 week, 5 days, or same-day notifications).
- **Full Audit Logging:** Each attestation action should be logged with date, time, user, and comments.
- **Configuration Flexibility:** Admin users should be able to define attestation workflows, schedules, and checklists without IT dependency.
- **Governance Dashboards & Reporting:** Real-time dashboards and reports providing visibility into attestation status, overdue attestations, and completion rates for internal and regulatory reviews.

Solytics Response

Requirement	How MRM Vault Handles This	Status
Multi-Level Attestations	MRM Vault supports both sequential and parallel multi-level attestations configured through workflow logic. Approver hierarchies (e.g., Model Owner → Validator → Governance Committee) can be defined by role or business unit. Completion at each level automatically triggers the next stage.	Configuration Required
Bulk Approvals	MRM Vault enables users to perform bulk attestations, approving or rejecting multiple models in a single action. Each bulk transaction is individually recorded in the audit log of the attestation assessment with model ID and approver details, ensuring traceability while improving operational efficiency.	Configuration Required
Automated Scheduling	Attestation cycles can be scheduled automatically using date-based or SLA-based triggers (e.g., annual attestations, 30-day reviews). Notifications and alerts can be sent 7 days, 3 days, or 1 day before the due date. These configurations can be managed directly through the admin interface.	Configuration Required
Alerting Mechanism	MRM Vault's attestation alert framework allows admins to configure rule-based alerts for upcoming or overdue attestations. Alerts can be triggered by due dates, pending approver actions, or incomplete bulk approvals. Notifications are sent via both in-app alerts and email.	Configuration Required
Audit Logging	Every attestation action, manual, bulk, or automated, is recorded in the Audit Log with timestamp, model ID, user, action type, and comments. Logs can be exported	Out of the Box

	to Excel or PDF for internal or regulatory audit purposes.	
Ease of Configuration	Administrators can configure attestation workflows, schedules, checklists, and approver roles through an intuitive UI. Existing attestation templates can be cloned or reused across business units to streamline setup.	Configuration Required
Dashboards & Reporting	Dashboards display attestation progress by business unit, owner, and due date. KPIs include completion %, overdue counts, SLA adherence, and average attestation turnaround time.	Configuration Required/ Enhancement (for advanced analytics)
Governance Oversight	Governance dashboards provide a portfolio-level view of attestation compliance, including pending approvals, overdue attestations, and bottlenecks by stakeholder. Oversight users can intervene directly by reassigning attestations, triggering reminders, or downloading compliance summaries for reporting.	Configuration Required

4.1.11 Change Management

For detailed mockups/designs on how change management process is facilitated in MRM Vault, Refer to: 'MRM Vault_Solytics Partners_Change Management Process Design.docx' located in - Click here: [HDFC FSD 1 Reference Documents](#) , for detailed screenshots/mockups.
Access Password: hdfc@FSD2025

Requirement:

The MRM system should support a complete Change Management Workflow, covering the full process from raising a change request to implementation and archival.

It must ensure standardization, traceability, and governance alignment, addressing the following key requirements:

Initiation

- Users can raise a formal change request with details (reason, requester, impacted models).
- System auto-generates a unique Change Request ID.

Impact Assessment

- Ability to document expected impacts and dependencies.
- Link changes to monitoring results (e.g., threshold breaches).

Validation & Review

- Requests routed to validators as per rules.
- Validation scope varies by change type (major/minor) with results recorded.

Approvals

- Role-based approvals involving Model Owner, Validator, Risk/Oversight.
- SLA tracking for timely reviews.

Implementation

- Track implementation progress and notify impacted users.
- Manage communications related to deployment or cutover.

Version Control & Archival

- Auto-update of model version and effective date.
- Retain all past versions and supporting documents for audit.

Core Principles:

- End-to-end lifecycle coverage.
- Consistent workflow for all models.
- Clear roles and responsibilities.
- Complete audit trail.
- Impact and risk awareness.
- Integration with validation, monitoring, and reporting.
- Visibility via dashboards and reports.

Our Understanding:

The client requires a standardized, configurable, and auditable change management framework within MRM Vault that governs every change to models, templates, or metadata attributes.

This workflow should:

- Ensure traceability from initiation to archival;
 - Support impact linkage with monitoring results and validations;
 - Route requests dynamically based on change type and roles;
 - Provide automated version updates upon implementation;
 - Maintain full audit trails and documentation history; and
 - Offer real-time dashboards and reports for governance visibility.
- The system must operate without manual intervention or IT dependency, ensuring transparency and regulatory compliance.

Solytics Response:

Requirement	How MRM Vault Handles This	Status
Initiation	Users can raise formal Change Requests via a standardized form capturing requester details, reason for change, impacted models, and supporting attachments. The system auto-generates a unique	Configuration Required

	Change Request ID to maintain traceability across the change lifecycle.	
Impact Assessment	Impact Assessment forms capture the expected impact, dependencies, and linked monitoring outcomes (e.g., threshold breaches). Each request maintains a structured record linking changes to underlying validation or monitoring observations, supporting risk-based prioritization and governance review.	Configuration Required
Validation & Review	Based on change type (Major, Minor, or Administrative), MRM Vault automatically routes the request to assigned validators. Validation outcomes (Approved / Rejected / Conditional) and evidence are captured within the system, with scope rules configurable by change type.	Configuration Required
Approvals & SLA Tracking	Role-based approval routing ensures that Model Owners, Validators, and Oversight Committees review and sign off on each change. SLA timers track pending approvals, highlight overdue cases in dashboards, and trigger automated reminders or escalations to governance users.	Configuration Required
Implementation Tracking	Once a change is approved, implementation tasks are automatically created and tracked in the system. Notifications are sent to impacted users, and dashboards display progress, dependencies, and completion status. Communication logs maintain transparency during deployment or cutover.	Configuration Required
Version Control & Archival	Upon closure of a Change Request, MRM Vault automatically increments the model version, updates the effective date, and maintains lineage between prior and updated versions. All historical metadata, attachments, and documents are archived and retrievable for audit and regulatory inspection.	Out of the Box
Audit Logging	All change-related actions creation, edit, validation, approval, and implementation — are logged in the centralized Audit Log with timestamp, user, and action details. Audit entries are immutable and exportable for internal or regulatory reporting.	Out of the Box
Governance Dashboards & Reporting	Governance dashboards visualize the full Change Management pipeline with metrics for pending approvals, SLA adherence, and impact category (Major/Minor). Users can filter by business unit, change type, or requester, and drill down to individual Change Request records for investigation or follow-up.	Configuration Required

Integration with Other Modules	The Change Management module integrates seamlessly with Validation, Monitoring, and Inventory modules through data mapping and workflow automations. Approved changes automatically update model metadata and trigger necessary revalidations or monitoring refreshes to maintain lifecycle continuity.	Configuration Required
Ease of Configuration	All workflow stages, roles, checklists, and SLA parameters are configurable by administrators using the Workflow Designer UI. No code changes are required to modify approval hierarchies or attestation dependencies.	Configuration Required

A. Change Management for Roles

Requirement:

The system must support role and responsibility changes for users involved in the model lifecycle to ensure governance alignment with organizational changes.

This includes scenarios such as employee transfers, exits, team restructuring, or policy revisions, with the following core capabilities and process requirements:

System Capabilities:

- Allow authorized users (e.g., MRM Oversight) to create, update, or deactivate roles and reassign responsibilities without coding.
- Support dynamic updates to user groups (e.g., business units, teams, regions).
- Align role-based access with enterprise IAM standards.
- Enable dual approvals for critical role changes.
- Enforce periodic access reviews to maintain compliance.

Process Flow Requirements:

- Trigger Identification: Changes may originate from employee movements, exits, or policy/regulatory updates.
- Change Request Initiation: A formal change request should capture impacted role/person, reason, new rights, and effective date.
- Review & Approval: Governance review for compliance and policy alignment.
- System Update & Communication: Access matrix updates post-approval, automatic stakeholder notification, and change logging.
- Audit & Recordkeeping: All role changes logged in a register with full audit trail.

Our Understanding:

The client requires a role governance framework embedded within MRM Vault to ensure that all role and access updates are systematically reviewed, approved, executed, and auditable.

Key expectations include:

- Administrative self-service: MRM Oversight should manage roles, user groups, and responsibilities via the UI without IT involvement.
- Maker–Checker governance: Critical access changes must undergo review and approval before taking effect.
- Alignment with enterprise IAM standards: Role-based controls must map to organizational hierarchies and policies.
- Audit readiness: Every role modification must be fully logged and reportable for compliance and regulatory inspection.
- Automation: Notifications and access updates should be system-driven, reducing dependency on manual processes.

Solytics Response:

Requirement	How MRM Vault Handles This	Status
Role Creation & Updates	Authorized users (e.g., MRM Oversight or Admin) can create, modify, or deactivate user roles directly through the UI without coding. Each role change is subject to approval workflow and allows upload of justification or supporting documentation.	Configuration Required
Dynamic User Group Management	Dynamic updates to user groups (e.g., Business Units, Regions, or Teams) are supported. Role assignments cascade automatically to all dependent users and systems based on configured inheritance rules, ensuring consistency across the organization.	Configuration Required
Role-Based Access Alignment (IAM Integration)	MRM Vault’s RBAC framework aligns with enterprise IAM standards through optional integration with LDAP/AD or SSO connectors. Each role defines permissions across workflow actions (view, edit, approve) and module access, ensuring compliance with organizational access hierarchies.	Configuration Required/ Enhancement (for IAM connector)
Dual Approval for Role Changes	Maker–Checker controls ensure dual approval for critical access modifications. A role change is only activated once validated by an independent approver. Escalation rules can be configured for pending approvals nearing SLA breaches.	Configuration Required
Access Review Mechanism	Scheduled and ad-hoc access reviews allow MRM Oversight to verify role-to-user mappings and compliance with internal and regulatory policies. Automated reminders are sent for overdue reviews, and completion metrics are displayed on dashboards.	Configuration Required/ Enhancement (for automated reminders)

Change Request Process (Initiation to Closure)	The role change workflow follows a standardized path — Request → Review → Approval → Update → Notification → Audit Logging. Each request is tracked through a unique Change ID with a complete record of comments, approvals, and evidence attachments.	Configuration Required
System Update & Notifications	Upon approval, MRM Vault automatically updates the access matrix and sends configurable notifications (email/in-app) to stakeholders. Notification templates can be customized by recipient group (e.g., approvers, governance committee).	Out of the Box / Configuration Required
Audit Trail & Register	All role changes are captured in the centralized Audit Log with timestamp, initiator, approver, change type, and effective date. The system maintains a Role Change Register that can be exported to Excel/PDF and retained per organizational retention policy.	Out of the Box
Governance Dashboards	Dashboards display real-time KPIs such as active roles, pending change requests, access review completion %, and SLA breaches. Visuals include bar charts for role distribution and trendlines for periodic reviews, enabling governance oversight and proactive compliance tracking.	Configuration Required

B. Change Management for Attributes

Requirement:

The MRM system must support full change management for attributes in a controlled and auditable manner. Attribute changes such as addition, modification (e.g., name, format, visibility, mandatory status), or retirement should be managed by Admin users through a configuration interface, without IT intervention or database redevelopment.

Administrators must also be able to maintain parameter tables (e.g., risk scoring thresholds, SLA timelines, escalation triggers, role mappings, PDV requirements, monitoring mappings, and in-scope area additions) via front-end configuration or uploads.

The system should support the creation of new rule sets or conditional logic through configuration, along with a simulation (“what-if”) mode to test rule impacts before going live.

Key governance expectations include:

- Controlled Access – Only Admin users can modify attributes.
- Governance & Notification – Governance team must be automatically notified of attribute-level changes.

- Impact Assessment – System must check and warn for linked dependencies before applying changes.
- Audit Trail – All attribute changes must be logged, versioned, and retrievable.

Our Understanding:

The client requires an enhanced Attribute Configuration and Governance module in MRM Vault that allows for complete attribute lifecycle management—from creation to deactivation—without backend dependency.

Key expectations include:

- Front-end configurability: Admin users should manage attributes, templates, and parameter tables directly through the UI or upload utility.
- Automated dependency checks: Before applying changes, the system should identify linked entities (forms, workflows, reports).
- Governance visibility: Each attribute change should generate automated alerts to the governance team with full details.
- Auditability and traceability: All attribute changes must be logged for audit and regulatory inspection.
- Simulation capability: Ability to preview or test rule/attribute changes in a non-production mode before making them live.

This feature requires product enhancement to strengthen MRM Vault's configuration governance and introduce simulation and parameter maintenance capabilities.

Solytics Response:

Requirement	How MRM Vault Handles This	Status
Controlled Access	Only authorized Admin users can modify attributes through the Attribute Configuration interface. Users can add, edit, or retire attributes, and adjust parameters (label, format, mandatory status, visibility). All configurations are version-controlled, ensuring rollback or reactivation if required. Role-based permissions restrict all other users from altering attribute settings.	Configuration Required
Governance & Notification	As part of the maker-checker workflow, MRM Vault automatically notifies the Governance team whenever an attribute is created, modified, or retired. Notifications include change metadata (attribute name, change type, initiator, impacted entities, and effective date). Governance approval is	Configuration

	mandatory before activation, ensuring oversight and controlled implementation.	
Impact Assessment	Before applying changes, the system performs an automated dependency check to identify links to forms, templates, workflows, or reports. If dependencies exist, the Admin receives a warning with impacted entities listed. The system requires explicit confirmation or Governance approval before proceeding, ensuring that no dependent process is unintentionally disrupted.	Out of the Box
Audit Trail	All attribute modifications (create/edit/retire) are logged in a centralized Audit Log with timestamp, user, old vs. new values, and impacted modules. Each change generates a unique version ID, allowing rollback to prior configurations if needed. The Audit Log is searchable and exportable for compliance and governance review.	Out of the Box
Parameter Table Management	Admin users can manage parameter tables (e.g., risk thresholds, SLA timelines, escalation triggers, PDV mappings, etc.) directly via the front-end interface or Excel upload. Each update is version-controlled, logged, and optionally routed for Governance review before activation.	Configuration Required
Conditional Logic Configuration	MRM Vault allows creation of conditional logic using attribute-value combinations to automate actions such as email alerts, task triggers, or report generation. Each rule undergoes validation to detect logical conflicts or missing dependencies before activation. This ensures automation remains consistent and aligned with governance controls.	Configuration Required
Simulation (“What-if”) Mode	MRM Vault currently supports impact analysis for changes made to template metadata or settings. When a change is initiated, the platform presents a clear summary of its potential impact such as affected models or workflows and prompts the user for confirmation and approval through the maker-checker process before implementation. As part of the product roadmap, this capability will be extended to other modules across the platform. Future enhancements will include visual simulations and downstream impact previews, helping users	Out of the Box

	better understand how their changes may affect related entities and processes before finalizing them	
Governance Visibility (Dashboards & Reports)	<p>MRM Vault provides governance dashboards summarizing attribute change activity, including metrics such as number of attribute updates, change type (add/edit/retire), pending approvals, and average approval time.</p> <p>All metadata changes across attributes, templates, or configurations are tracked in queryable, exportable logs. Governance users can filter by user, entity, or time range and generate on-demand reports for audits or regulatory submissions</p>	Configuration Required

C. Change Management for email & notification

Requirement:

The MRM system must ensure that all email and notification templates follow a structured change management process to maintain consistency, traceability, and governance. These templates are essential for communication, approval tracking, and auditability; hence, their creation, modification, or deactivation must be controlled, versioned, and fully auditable.

Our Understanding:

Emails and notifications are critical communication tools in model governance workflows, ensuring timely alerts to stakeholders such as Model Owners, Validators, and Governance Teams. However, MRM Vault does **not** have a centralized “notification center.”

Instead, all notifications (email or in-app) are **configured using automation rules** linked to workflow events or lifecycle stages.

Changes to email templates, notification triggers, or recipients must be authorized, version-controlled, and logged to maintain governance and compliance.

Solytics Response:

Section	How MRM Vault Handles This	Status
Ownership & Access	MRM Vault restricts configuration and deployment of email or notification templates to MRM Admins under Role-Based Access Control (RBAC). Configuration changes are performed via the Automation Engine. Business users (e.g., MOA, MOTL, MRMA, MRMTL) have view-only access to notification templates. Only designated Admins can deploy template or trigger	Configuration Required

	updates after successful testing in a sandbox environment.	
Scope of Change	<p>Authorized Admins can use the Automation Engine to:</p> <ul style="list-style-type: none"> • Create or edit templates tied to specific lifecycle events (e.g., validation completion, PDV initiation). • Modify notification triggers linked to workflow actions (e.g., overdue validations, rejected approvals). • Deactivate obsolete or redundant templates. <p>All changes undergo version control and pre-deployment validation in a sandbox environment to verify formatting, recipients, and event linkage before being promoted to production. Rollback to prior versions is supported in case of configuration errors.</p>	Configuration Required
Governance Process	<p>MRM Vault enforces a structured change management process for notification of templates. Each modification begins with a Change Request (CR) raised by Admin or Governance users. The system performs an impact assessment to identify dependencies (workflow IDs, automation rules, and recipient lists).</p> <p>Critical changes require dual-level approval (MRMA and MRMTL) and are version-controlled with timestamp, initiator, and approval trail. Upon deployment, a confirmation email is automatically sent to Governance users, verifying the updated template version and affected workflows.</p>	Configuration Required
Audit & Logging	<p>MRM Vault maintains an immutable Audit Log capturing every template-related action (Add/Edit/Deactivate) with the following details:</p> <ul style="list-style-type: none"> • Template ID and Version Number • Type of Action (Create/Edit/Remove) • Initiator and Approver details • Timestamp and deployment confirmation <p>Historical versions are preserved, searchable, and exportable for audit or regulatory inspection. The system maintains lineage between template versions for traceability.</p>	Out of the Box

D. Change Management for templates

Requirement:

MRM Vault must support configurable and controlled management of form templates used throughout the model lifecycle.

These templates are critical for capturing governance and regulatory data and must be flexible to accommodate ongoing policy, regulatory, or business process changes.

Key expectations include:

1. Template Configuration & Workflow Logic:
 - a. Admins must modify form and sub-template structures without coding.
 - b. Add/remove fields, reorder workflow steps, define conditional logic, and assign approval roles.
 - c. Enable version control so older model records retain their original structure after updates.
2. Scope of Editable Elements:
 - a. Template/sub-template structure, field-level attributes, dropdown lists, permissions, and workflow associations.
 - b. Attribute-level changes follow separate governance handled under the Attribute Change Management module.
3. Change Triggers:
 - a. Regulatory updates, new product types or risk areas, internal process changes, or user feedback.
4. Governance Workflow:
 - a. Change request initiation, review by governance team, escalation to committees if required, and final approval before implementation.
5. System Update & Audit:
 - a. Approved changes must update live workflows automatically.
 - b. Notifications sent to impacted users.
 - c. Full change history maintained in a Template Change Register with auditability of all versions.

Our Understanding:

The requirement is for a centralized, governed, and configuration-based framework for managing form templates and their lifecycle.

The feature must:

- Allow non-technical administrators to configure Forms and Sub-templates (Templates and Sections) via the front-end.
- Ensure strict control and versioning, where previously completed model records are not impacted by new Template/Form structures.

- Provide workflow-integrated notifications and audit trail logging for all Template/Forms edits.
- Support conditional logic, dropdown configuration, and permission mapping through the UI.
- Maintain a Template/Form Change Register with visibility into who made what changes and when, ensuring full traceability during audits.

This functionality will require enhancement in MRM Vault's current configuration framework to strengthen governance control and version management.

Solytics Response:

Requirement	How MRM Vault Handles This	Status
Form & Sub-Template (Template & Section) Configuration	Authorized Admins can create, modify, or deactivate Templates and Sub-templates directly via the UI. Changes such as adding/removing fields, defining conditional logic (e.g., "Mandatory if Risk Tier = High"), or updating workflow sequences are supported without coding. Before deployment, new or modified templates can be previewed and validated in a sandbox environment, with rollback to prior versions available if errors are identified.	Configuration Required
Version Control	Each update to a Template or Form generates a new version while preserving prior structures for audit and data consistency. The system allows rollback to previous versions and maintains retention of historical templates per governance retention policy.	Out of the Box
Editable Elements Scope	Admins can edit form structure, dropdown lists, access roles, workflow associations, and permissions. Attribute-level edits (e.g., field name, format, mandatory flag) are managed under the Attribute Change Management module with maker-checker control. MRM Vault ensures dependency mapping, changes affecting conditional fields or risk-tier logic are validated before finalization.	Configuration Required
Change Request Workflow	Template change requests can be raised by Admin, Business, or Governance users. Each request includes Template ID, reason, impacted entities, and effective date. The system automatically generates a dependency summary identifying linked workflows, dashboards, or reports. Requests follow a review-approval workflow before implementation, ensuring traceability and accountability.	Configuration Required

Governance Review & Approval	Governance teams review and approve template modifications for consistency and compliance. MRM Vault supports dual-level approvals (Admin + Governance Lead). Each change request undergoes automated impact analysis showing affected workflows, forms, and dependent logic before approval. Critical or regulatory-impacting changes can be escalated to committees for sign-off.	Configuration Required
System Update & Notifications	Upon approval, MRM Vault automatically updates live workflows, sends notifications to impacted users, and records deployment confirmation in the Audit Log. Notifications include version ID, approval timestamp, and approver details to ensure traceability.	Configuration Required
Audit Logging & Template Change Register	All modifications are logged in a Template Change Register capturing Template ID, type of change, initiator, approver, timestamp, and old vs new structure. The system also tracks version lineage (parent-child relationship) for backward traceability. Audit logs are exportable for regulatory inspection.	Out of the Box
Regulatory & Business Adaptability	MRM Vault templates can adapt dynamically to regulatory or governance updates. Retrospective changes apply only to future records without altering historical submissions, while prospective changes can be configured to update ongoing processes. This dual-mode capability ensures compliance with continuity and operational flexibility.	Configuration Required
Dashboards & Reporting	Dashboards display active templates, pending change requests, version counts, change turnaround time, and approval status distribution. Governance teams can view trendlines for configuration activity and export reports for committee review or audit reporting.	Configuration Required

4.1.11 Migration

Requirement:

The migration requirements captured in this document pertain exclusively to Model Inventory Migration. Migration requirements related to PDV and Monitoring will be addressed separately in their respective requirement documents.

HDFC's existing model inventory is maintained in Excel spreadsheets across multiple business units. For MRM Vault to function as the single source of truth, the inventory must be migrated, standardized, validated, and reconciled within the centralized workflow.

The migration is a one-time exercise during implementation but must ensure:

- Completeness – All models and relevant metadata are migrated.
- Accuracy – Data integrity is preserved.
- Transparency – Migration steps and mapping are fully documented.
- Regulatory defensibility – Audit trail of all migration activities maintained.

Our Understanding:

The client's primary objective is to transition from a decentralized Excel-based inventory to a centralized, workflow-driven system (MRM Vault) that serves as the single source of record for all model-related metadata.

The migration process must:

- Standardize legacy metadata for consistency (naming conventions, ownership, validation status).
- Cleanse and harmonize data prior to upload.
- Map legacy attributes to MRM Vault's metadata model and workflows.
- Validate migrated records against source data for accuracy.
- Maintain comprehensive migration logs for audit and regulatory purposes.
- Be executed as a one-time controlled exercise during implementation; all future updates will occur directly in MRM Vault.

This ensures that post-migration, MRM Vault becomes the system of record, eliminating dependency on spreadsheets and ensuring governance, auditability, and completeness.

Solytics Response:

Requirement	How MRM Vault Handles This	Responsibility	Status
Standardization	All metadata fields (e.g., Model Name, Owner, Business Unit, Classification, Validation Status) must be standardized prior to upload to align with MRM Vault's attribute library. Solytics will provide pre-validated upload templates and data-type rules to ensure consistency across all business units.	Client	Enabled
Data Cleansing	Duplicate, incomplete, or inconsistent records in legacy Excel sheets must be remediated before upload. Solytics will provide validation scripts to identify anomalies (missing mandatory	Client	Enabled

	fields, duplicate Model IDs, invalid formats). Clean datasets will be uploaded only after meeting validation thresholds defined jointly by HDFC and Solytics.		
Mapping to MRM Vault Structure	MRM Vault maps legacy model data to the centralized schema aligned with metadata fields (Materiality, Model Tier, Lifecycle Status, Validation Frequency, etc.). Solytics will configure mapping logic and conduct dry-run uploads to validate structural compatibility.	Solytics	Enabled
Validation & Reconciliation	Uploaded data will be validated against source files to confirm completeness and accuracy. Reconciliation reports will highlight record counts, exceptions, and mismatch summaries. HDFC will review and provide written sign-off upon successful validation.	Solytics + HDFC	Enabled
Audit Trail & Traceability	MRM Vault captures all migration activity logs with timestamp, record count, validation summary, and error corrections. Each log entry is uniquely identifiable for traceability. The migration log supports rollback and re-execution in case of validation failure, ensuring regulatory defensibility.	Solytics	Enabled
One-Time Migration (Implementation Phase)	During Sprint-1 implementation, Solytics and HDFC will perform a single controlled migration of all legacy model records into MRM Vault. This activity will be governed through predefined control gates, Data Readiness Validation, Dry-Run Verification, and Final Upload Approval, marking the initial population of the centralized inventory.	Solytics + HDFC	Enabled
Ongoing Migration (Post-Cutover)	Post go-live, all model creation and updates will occur directly within MRM Vault through governed workflows. Uploads or migrations	HDFC	Enabled

	outside the system are disabled to prevent data silos. Ongoing model onboarding will leverage automated data-validation and approval rules, ensuring continuity of data quality.		
Transparency & Documentation	All migration steps, including mapping logic, validation outcomes, and reconciliation sign-offs, will be documented in a Migration Logbook. Solytics will deliver a Migration Completion Report summarizing data accuracy, exceptions resolved, and final confirmation of upload completion.	Solytics	Enabled

4.1.13 Archival and Retention

Requirement:

The system shall allow archival of retired or decommissioned models while retaining all model-related data, metadata, and supporting documentation for full auditability and regulatory compliance.

Archived models must:

- Remain searchable and retrievable within the system.
- Be clearly distinguished from active models through a status flag or segregation mechanism.
- Preserve all historical records, approvals, and attachments for future inspection or audit reference.

Our Understanding:

The client expects the MRM system to include a controlled archival process that ensures decommissioned or retired models are not deleted but are securely stored with their full audit history intact.

The archival function must:

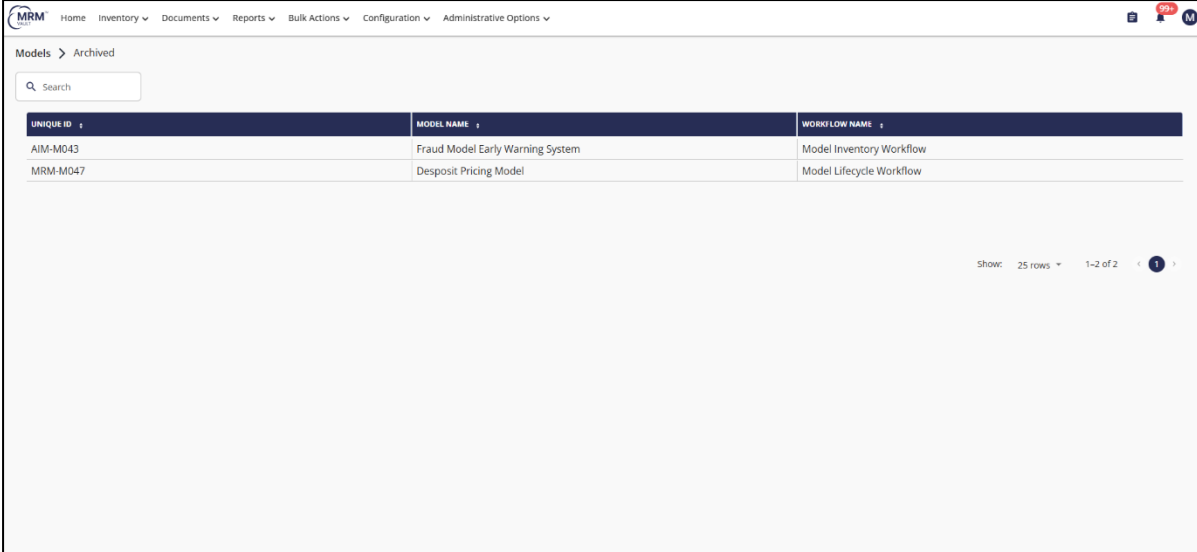
- Trigger automatically upon completion of the decommissioning workflow;
- Retain all metadata, documents, workflow actions, and historical logs associated with the model;
- Maintain read-only access to ensure the integrity of archived data;
- Keep archived models searchable and referenceable, with a clear status identifier;
- Serve regulatory, internal audit, and governance review purposes without reactivation risks.

This process ensures data preservation, transparency, and regulatory defensibility while maintaining system performance and governance compliance.

Solytics Response:

Requirement	How MRM Vault Handles This	Status
Archival of Decommissioned Models	MRM Vault automatically archives models once their lifecycle reaches the Decommissioned or Retired state. The archival trigger is workflow-based and executed via automation rules; no manual intervention required. Archived models are securely stored in a logically segregated repository, maintaining data integrity and retrievability.	Configuration Required
Retention of Data & Documents	MRM Vault retains all metadata, documents, workflow logs, approvals, attachments, and historical records associated with the model in perpetuity or as per configurable retention policy (e.g., 7–10 years, or as required by local regulatory guidelines). Archived content remains immutable, ensuring authenticity and audit readiness.	Out of the Box
Search & Accessibility	Archived models remain fully searchable in the “Archived Inventory” view. Each record is marked with a distinct Archived/Decommissioned flag and supports filtered searches by lifecycle stage, owner, or model type. Advanced search allows comparison between active and archived models for governance analytics.	Out of the Box
Access & Permissions	Archived records are automatically switched to read-only mode for all users. Access is restricted to authorized Oversight, Governance, and Audit personnel. Any attempt to access, export, or restore archived data is logged with timestamp and user ID, ensuring traceability and access control compliance.	Out of the Box
Archival Repository View	Archived models are displayed under a dedicated “Archived Inventory” tab within the Model Inventory module. This segregated view maintains centralized visibility while ensuring archived models are excluded from active operational workflows. The repository supports metadata filters and export capabilities for governance and regulatory inspections.	Out of the Box
Audit Trail Preservation	Each archived model retains its complete audit history, including workflow transitions, user actions, validations, and approvals. These audit trails are immutable and stored in encrypted form to ensure data integrity and non-repudiation. Historical logs remain	Out of the Box

	accessible through the Audit Log viewer for compliance review.	
Compliance & Governance Reporting	Archived models are automatically included in lifecycle completeness reports and regulatory dashboards. MRM Vault enables governance teams to demonstrate compliance with retention policies, audit reviews, and model decommissioning controls. Reports can filter active vs. archived inventories for regulatory submissions.	Configuration Required

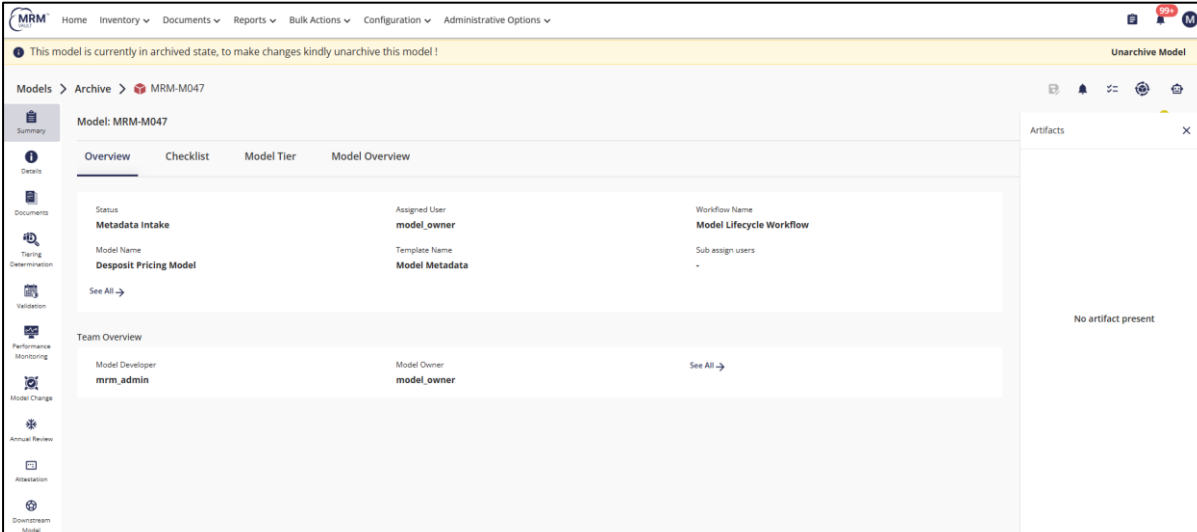


The screenshot shows the 'Archived' tab in the MRM Vault interface. It displays a table with three columns: 'UNIQUE ID', 'MODEL NAME', and 'WORKFLOW NAME'. The table contains two rows of data.

UNIQUE ID	MODEL NAME	WORKFLOW NAME
AIM-M043	Fraud Model Early Warning System	Model Inventory Workflow
MRM-M047	Deposit Pricing Model	Model Lifecycle Workflow

At the bottom right of the table, there is a pagination control showing 'Show: 25 rows' and '1-2 of 2'.

Reference Image 1: Collection of archived models in a dedicated Archive tab.



The screenshot shows the 'Archive' tab in the MRM Vault interface, specifically the details for model MRM-M047. The interface includes a navigation sidebar on the left with various icons for different model lifecycle stages. The main content area is divided into sections for 'Overview', 'Checklist', 'Model Tier', and 'Model Overview'. The 'Overview' section is currently selected and displays details for the 'Deposit Pricing Model'.

Status	Assigned User	Workflow Name
Metadata intake	model_owner	Model Lifecycle Workflow
Model Name	Template Name	Sub assign users
Deposit Pricing Model	Model Metadata	

Below the 'Overview' section, there is a 'Team Overview' section showing the 'Model Developer' as 'mrm_admin' and the 'Model Owner' as 'model_owner'.

Reference Image 2: An archived model where data/information cannot be altered by any user except the user with permission to do it, managed through user role permission module.

4.1.14 Audit and Logging

Requirement:

The MRM system must provide comprehensive audit and logging capabilities to ensure that all user actions, system events, and workflow activities are captured, immutable, time-stamped, and retrievable for governance, audit, and regulatory purposes.

Core Principles:

- **Comprehensive Coverage:** Every material user action and system event must be logged.
- **Immutability:** Logs must be tamper-proof, append-only, and protected from modification or deletion.
- **Traceability:** Must provide end-to-end traceability across the model lifecycle.
- **Accountability:** Logs must capture who, what, when, where for each activity.
- **Transparency:** Logs must be easily retrievable for internal and external audits.
- **Integration:** Logging must be linked with dashboards, reporting, and archival functions.
- **Compliance:** Audit framework must align with regulatory expectations for defensibility.

Scope of Audit Logs:

Audit logging must cover the full model lifecycle — from registration through validation, monitoring, change management, migration, archival, and decommissioning, including:

- All user actions and metadata updates.
- Additions, modifications, and exclusions to the Master Attributes List.
- Changes to Form Templates, Email Templates, Notification Triggers, and any linked dependencies across lifecycle workflows.

Our Understanding:

The client requires an enterprise-grade audit logging framework within MRM Vault that ensures full traceability, transparency, and immutability across all governance functions.

The system should:

- Automatically log all user and system actions, with relevant metadata.
- Maintain immutable, append-only audit logs resistant to tampering or deletion.
- Support querying, filtering, and exporting audit records for audit and regulatory reviews.
- Maintain coverage across all modules (Inventory, Validation, Monitoring, Change Management, Attribute, and Template Management, etc.).
- Integrate reporting and dashboards to provide real-time visibility into governance activities.

- Store all records in compliance with regulatory data retention policies and information security standards.

This ensures full audit readiness, lifecycle traceability, and defensibility before regulators or internal audit bodies.

Solytics Response:

Requirement	How MRM Vault Handles This	Status
Comprehensive Coverage	MRM Vault maintains a unified audit trail capturing every material system event and user action across all lifecycle modules — including model creation, validation outcomes, approvals, evidence uploads, configuration edits, communications, and archival actions. Logs extend to attribute, template, email, and notification changes, ensuring holistic traceability.	Out of the Box
Immutability & Tamper-Proofing	Audit logs are system-generated, immutable, and stored in append-only format using write-once-read-many (WORM) principles. Entries are cryptographically hashed and timestamped to prevent alteration or deletion. Even system administrators cannot edit or purge audit entries directly.	Out of the Box
Traceability	Each log record captures the full who-what-when-where-how chain, including user ID, action type, entity affected, timestamp (UTC synchronized), and originating workflow. This ensures end-to-end lineage and accountability across all governance activities.	Out of the Box
Audit Metadata Captured	Every audit event records user identity, role, timestamp, entity name, field modified, old and new values, action type, workflow ID, and approval context. Audit entries are linked to model IDs for hierarchical traceability, enabling drill-down and cross-reference with validation or change events.	Out of the Box
Lifecycle-Wide Logging	Audit coverage spans the complete lifecycle, Model Registration, PDV, Monitoring, Change Management, Migration, Archival, and Decommissioning. Cross-module consistency ensures uniform data lineage even when models transition across stages or ownership groups.	Out of the Box

Attribute & Template Governance	All modifications in Master Attributes, Form Templates, Email Templates, and Notification Rules are automatically logged with version history, approver ID, and change reason. This guarantees traceability between configuration governance and lifecycle outcomes.	Out of the Box
Integration with Dashboards & Reporting	MRM Vault integrates audit data into governance dashboards, presenting key KPIs such as number of configuration changes, audit exceptions, and module activity by user. Interactive filters allow Governance teams to view, export, and analyze logs by category (validation, change management, archival). Anomaly alerts can flag missing or delayed audit entries.	Configuration Required
Record Retention & Compliance	MRM Vault enforces configurable data retention for audit logs based on institutional or regulatory requirements (e.g., 7–10 years). Logs are automatically archived post-expiry and securely purged only after dual-level approval. Audit data remains encrypted at rest and in transit, meeting data security standards.	Configuration Required
Audit Log Accessibility	Access to audit logs is restricted through RBAC. Authorized Governance and Oversight users can query, filter, and export logs by module, user, action, or timeframe. All log exports are recorded as secondary audit events, ensuring meta-audit traceability (“audit of audit”).	Configuration Required
Transparency & Regulatory Defensibility	MRM Vault’s immutable audit framework ensures defensibility before internal audit, risk committees, and regulators. Logs demonstrate model lifecycle completeness, control adherence, and accountability, satisfying governance expectations under frameworks like SR 11-7, SS 1/23, and MMS MMG.	Out of the Box

MRM

HomeInventoryDocumentsReportsBulk ActionsConfigurationAdministrative Options

2024M

ModelsAIM-M166

SummaryDetailsDocumentsTiering DeterminationValidationPerformance MonitoringModel Change

Logs

Search

User

From dateMM/DD/YYYYTo dateMM/DD/YYYY

Log Actions

Attributes

State

ACTION	RESPONSIBLE USER	CHANGED DATE	CHANGED FIELD	WORKFLOW STATE	PREVIOUS VALUE	CURRENT
Updated Attribute	mrm_admin	09/11/2025, 5:51:03 pm	TEST	Model Implementation	-	-
Updated Attribute	michael	09/05/2025, 8:43:29 pm	Model Attestation	Model Implementation	False	True
Updated Attribute	mrm_admin	09/05/2025, 1:23:32 pm	Max Effort in Weeks	Model Implementation	-	-
Updated Attribute	mrm_admin	09/05/2025, 11:51:27 am	Validation table	Model Implementation	-	-
Updated Attribute	mrm_admin	09/04/2025, 8:23:48 pm	Date of Next Annual ...	Model Implementation	-	-
Updated Attribute	mrm_admin	09/04/2025, 8:23:47 pm	Date of Next Annual ...	Model Implementation	-	-

ReclaimArchiveDeleteApproval By MV

Reference Image 1: Model level comprehensive logs with search, filter and export functionality.

MRM

DashboardInventoryModel ArtifactsDocumentsRules & ReportsBulk ActionsConfigurationAdmin Options

2024-11-082024-12-23

WorkflowChange Request Workflow

DetailsLogs

Search

User

2024-11-08 → 2024-12-23

Log Action

State

ACTION	RESPONSIBLE USER	CHANGE DATE	CHANGE DETAIL	PREVIOUS DETAIL	CURRENT DETAIL
Added Node	User 2	09/05/2025, 11:47:40 am	Node ID	-	Approved
Deleted Node	User 2	09/05/2025, 11:47:40 am	Node ID	Execution Review	-
Assigned User Role	User 2	09/05/2025, 11:47:40 am	Node Role ID	-	Reviewer
Added Checklist Point	User 2	09/05/2025, 11:47:40 am	Checklist Point ID	-	Attach Impact Assessment
Added Node	User 2	09/05/2025, 11:47:40 am	Node ID	-	Review
Added Node	User 2	09/05/2025, 11:47:40 am	Node ID	-	Request Initiation

Showing 1 - 5 out of 100

<123...8910>

Show : 5 rows

Reference Image 2: Individual Control Level Logs, depicting history of changes to any control such as – workflows, attributes, template etc.

MRM

HomeInventory▼Documents▼Reports▼Bulk Actions▼Configuration▼Administrative Options▼

99+

M

Reports

1

Conne...

Report

3

Activity

Report

Generate Report

ID	NAME	ATTRIBUTE REPORT TYPE	CREATED AT	STATUS
159	Inventory Configuration Changes Log: 08/01/2025 - 08/01/2025	Configuration	2025-09-29	Done
158	Mail Report: 09/01/25 - 09/29/25	Email	2025-09-29	Done
151	Account access report: 09/01/25 - 09/26/25	Logging	2025-09-26	Done

Show: 10 rows1-3 of 31

Reference Image 3: Logs of all platform level actions - changes in controls - workflows, attributes, templates, user management etc.

MRM

DashboardInventory▼Model Artifacts▼Documents▼Rules & Reports▼Bulk Actions▼Configuration▼Admin Options▼

Email Template Inventory

Email TemplatesLogs

Q Search

User

2024-11-08 → 2024-12-23

Log Action

Workflow

State

EMAIL SUBJECT	STATUS	DATE SENT	RECIPIENT	ERROR MESSAGE
Model Risk Assessment	Sent	11/2/2024 2:30 PM	bob.ross@solytics.com	jane.doe@solytics.com
Regulatory Compliance Review	Sent	11/2/2024 2:30 PM	alice.smith@solytics.com	charlie.brown@solytics.com
Quantitative Model Validation	Sent	11/2/2024 2:30 PM	david.jones@solytics.com	emily.davis@solytics.com
Model Governance Framework	Sent	11/2/2024 2:30 PM	frank.white@solytics.com	grace.lee@solytics.com
Risk Appetite Statement	Sent	11/1/2024 10:00 AM	hannah.martin@solytics.com	ian.thomas@solytics.com
Model Inventory Management	Sent	11/1/2024 10:00 AM	julia.clark@solytics.com	kevin.wilson@solytics.com
Stress Testing Procedures	Sent	11/1/2024 10:00 AM	lisa.miller@solytics.com	mike.hall@solytics.com
Model Performance Monitoring	Sent	10/31/2024 4:15 PM	nancy.roberts@solytics.com	oliver.kelly@solytics.com
Model Development Standards	Sent	10/31/2024 4:15 PM	paul.adams@solytics.com	quincy.james@solytics.com
Scenario Analysis Techniques	Sent	10/31/2024 4:15 PM	rachel.walker@solytics.com	steve.harris@solytics.com
Model Documentation Requirements	Sent	10/30/2024 11:59 AM	tina.allen@solytics.com	uma.scott@solytics.com
Independent Validation Process	Sent	10/30/2024 11:59 AM	vicky.green@solytics.com	will.morris@solytics.com
Data Quality Assessment	Sent	10/30/2024 11:59 AM	xander.thompson@solytics.com	yara.baker@solytics.com

Showing 1 - 5 out of 100

<123...8910>

Show: 5 rows

Reference Image 4: Logs for email notifications triggered from the platform.

4.1.15 External Approval Process

Requirement:

The MRM system must support an External Approval Process (End-to-End Lifecycle Coverage: Registration → PDV → Deployment/PIT → Monitoring → Decommissioning), wherein governance reviews and sign-offs occur outside the system (via manual or email-driven workflows), but the system acts as the single centralized repository for all approved records, supporting documents, and lifecycle evidence.

The system must:

- Capture structured metadata (e.g., model name, owner, purpose, tier, business unit).
- Require upload of supporting approval documents (signed forms, scanned memos, or email confirmations).
- Enforce completeness checks before lifecycle progression.
- Maintain full audit trails, timestamps, and version control of approvals.
- Trigger notifications and alerts for key lifecycle events and overdue actions.
- Ensure that all evidence is securely stored and accessible for regulatory, governance, and audit purposes.

Our Understanding:

HDfC expects MRM Vault to function as the single source of truth for all model-related approvals and supporting evidence — even when approvals are conducted offline or via email, this will be enabled through workflow mapped to users, alerts & automations, audit trails & inventory wide reporting.

MRM Vault must:

- Capture all mandatory metadata fields and supporting documents per lifecycle stage (Registration, PDV, Deployment, Monitoring, Decommissioning).
- Enforce mandatory checklists to ensure no transition occurs without complete documentation and approvals.
- Allow attachment of approval documents directly through document-type attributes or document sections.
- Trigger automated email notifications upon stage completion or when SLA breaches occur.
- Maintain full audit logs for all uploads, transitions, and approvals for regulatory defensibility.

This approach combines external approval workflows with MRM Vault's governance enforcement and evidence management, ensuring traceability and completeness without altering existing organizational processes.

Solytics Response:

Requirement	How MRM Vault Handles This	Status
1. External Approval Framework (General)	MRM Vault enables governance workflows for model management by supporting actions that are tracked and documented. Features like checklists, alerts, notifications, and document attributes ensure all changes are logged with supporting documentation, promoting transparency and accountability.	Configuration Required
2. Metadata Capture & Structured Registration	During Model Registration, users must capture required metadata (e.g., model name, business unit, type, purpose, owner, materiality tier). System-defined templates enforce completeness through checklist and validation checks, ensuring no record progress without all mandatory metadata fields populated and verified.	Configuration Required
3. Approval Document Uploads	Each lifecycle stage includes document-type attributes for uploading approval evidence, signed memos, validation reports, or committee minutes. Version control ensures only the latest approved document is active, while historical versions remain archived for traceability. Digital signature or email confirmation metadata (date, approver name, designation) is captured for authenticity.	Configuration Required
4. Pre-Deployment Validation (PDV)	At the PDV stage, MRM Vault enforces upload of validation results, governance committee sign-offs, and closure evidence before allowing deployment. PDV approval is linked to validation cycle ID and version, ensuring governance traceability. The system automatically flags missing approvals or incomplete reports.	Configuration Required
5. Deployment & Post-Implementation Testing (PIT)	During deployment, users can attach PIT results, final deployment sign-offs, and go-live approvals. MRM Vault compares PIT completion timelines against SLA parameters, triggering automated escalation alerts for overdue or non-compliant activities.	Configuration Required
6. Monitoring Stage	At the monitoring stage, users upload both interim and final monitoring reports tagged as "Satisfactory," "Action Required," or "Under Review." The system triggers reminders for	Configuration Required

	upcoming monitoring cycles and escalates overdue reviews as per governance matrix.	
7. Decommissioning & Archival	Authorized users initiate model closure requests, validated by governance reviewers. The system verifies that all preceding lifecycle stages (PDV, Deployment, Monitoring, Mitigation) are complete with evidence before enabling archival. The final decommissioning approval is logged and archived immutably.	Configuration Required
8. Mandatory Checklists & Lifecycle Gate Controls	Each lifecycle stage includes configurable checklists enforcing field-level and document-level completeness. Transitions between stages are blocked until all mandatory metadata fields and approvals are verified. System logs every approval gate pass/fail event for auditability.	Configuration Required
9. Notifications & Escalations	MRM Vault auto-triggers email and in-app notifications upon lifecycle transitions or SLA breaches. Alerts are routed to predefined user groups (Governance, Risk, Oversight). Multi-level escalation rules ensure senior visibility when deadlines lapse or approvals are missing.	Configuration Required
10. Audit Trail & Traceability	Every lifecycle event, approval upload, metadata change, status transition, is audit-logged with timestamp, user ID, and version context. The immutable log enables governance teams to reconstruct the full approval lineage for any model.	Out of the Box
11. Governance & Reporting Visibility	Dashboards display real-time status of pending approvals, overdue validations, and SLA adherence. Reports provide a 360° view of model approval completeness across all business units and lifecycle stages, ensuring early identification of process bottlenecks.	Configuration Required

4.2 Non-Functional Requirements

Requirement:

In addition to the functional requirements, the Model Inventory Workflow must comply with defined Non-Functional Requirements (NFRs) to ensure reliability, governance integrity, and long-term sustainability.

These requirements cover:

- Performance & Timeliness – Real-time or near-real-time reflection of model inventory updates; timely notification and escalation mechanisms.

- Scalability & Flexibility – Capability to handle growing model volumes and to incorporate new lifecycle stages or governance checkpoints.
- Security & Confidentiality – Strict role-based access control aligned with enterprise information security standards.
- Auditability & Traceability – Comprehensive logging of all actions and historical retrievability for regulatory audit.
- Compliance – Adherence to internal model-governance frameworks and external supervisory expectations.
- Usability & Clarity – Structured, intuitive interface ensuring standardization and transparency of information.

Our Understanding:

The client requires the MRM Vault inventory framework to demonstrate not only strong functionality but also operational resilience and compliance assurance.

Specifically:

- Inventory updates, lifecycle transitions, and notifications must occur within governance-defined turnaround times.
- The solution must be scaled to support thousands of models without performance degradation.
- The access model must strictly follow RBAC and enterprise security frameworks.
- All activities — from registration to archival — must be auditable and time-stamped, providing evidence of compliance.
- The system should remain user-friendly, standardized, and transparent, minimizing manual dependency and ensuring clear accountability across stakeholders.
- These capabilities collectively ensure that the solution is future-proof, regulator-ready, and aligned with enterprise technology standards.

Solytics Response:

Non-Functional Requirement	How MRM Vault Handles This	Status
Performance & Timeliness	MRM Vault provides real-time synchronization for model updates and workflow transitions, reflecting status changes within seconds. The Notification Engine triggers alerts, reminders, and escalations automatically based on SLA parameters. System benchmarks ensure an average API response time under 2 seconds and notification dispatch within 60 seconds of event trigger.	Out of the Box
Scalability & Flexibility	MRM Vault's microservice-based architecture supports horizontal scaling to handle 5,000 + models and concurrent multi-user activity without latency. Configuration-driven design enables the addition of new lifecycle stages or approval	Out of the Box

	checkpoints without code modifications, ensuring agility as governance frameworks evolve.	
Security & Confidentiality	MRM Vault enforces strict Role-Based Access Control (RBAC) and Attribute-Level Permissions. All data is encrypted in transit (TLS 1.3) and at rest (AES-256). The platform complies with enterprise InfoSec, ISO 27001, and GDPR data protection policies. Audit logs of access attempts and failed logins are maintained for security review.	Out of the Box
Auditability & Traceability	Every model activity—creation, modification, approval, or archival—is logged with timestamp, user ID, and workflow context in an immutable audit trail. Logs are query able within 3 seconds and exportable for internal or regulatory audits. Historical records remain retained as per the organization’s retention policy (e.g., 7 years).	Out of the Box
Compliance Alignment	MRM Vault’s compliance module produces regulator-ready evidence demonstrating adherence to internal frameworks and supervisory guidelines (RBI MRM, CBUAE MMS MMG, PRA SS1/23). Retention and archival policies ensure defensibility during inspections. Regulatory reporting templates can be configured per jurisdiction	Configuration Required
Usability & Clarity	MRM Vault provides an intuitive, standardized interface with context-sensitive tooltips, dynamic forms, and pre-validated dropdowns. Visual cues minimize user error, while embedded Help & Support guides promote self-service learning. Logical layout ensures traceable navigation across lifecycle stages.	Out of the Box
System Monitoring & Reliability	The system continuously monitors uptime, latency, and health metrics via its Ops Dashboard, maintaining 99.9% availability. Automated alerts notify administrators of anomalies. Scheduled maintenance and feature deployments are communicated through in-app banners and emails to prevent disruption.	Out of the Box
Change Adaptability	MRM Vault’s configuration-first design enables adaptation to policy or regulatory changes (e.g., new validation checkpoints, metadata attributes) without code intervention. System behavior can be adjusted via admin configuration panels, ensuring sustainability and agility.	Configuration Required

5 Project-Level Assumptions

Document & Governance Alignment

- HDFC will share all finalized Requirement Documents (RDs) and governance workflows before FSD sign-off to ensure accurate scope definition and alignment with regulatory expectations.
- Each Functional Specification Document (FSD) will be reviewed and formally approved by relevant stakeholders — Business, IT, EA, ISD, and PMO — prior to configuration initiation.
- Any subsequent changes to requirements or workflows post-FSD approval will follow the Change Control Process (CCP), requiring written approval and impact assessment.

Architecture, Security & Infrastructure

- HDFC's Enterprise Architecture (EA) and Information Security Department (ISD) teams will review and approve the MRM Vault architecture to ensure compliance with enterprise security, data privacy, and InfoSec policies prior to deployment.
- All required infrastructure components — including VMs, servers, databases, storage, and network access — will be provisioned by HDFC as per mutually agreed technical specifications and timelines.
- HDFC will provide secure connectivity credentials (VPN, SFTP, firewall whitelisting) and network clearance to facilitate product installation, configuration, and testing.
- Infrastructure readiness, including SSL certificates and backup policies, will be validated by HDFC before initiating UAT.

Data Migration & Configuration Prerequisites

- HDFC will share clean, validated, and structured model inventory data aligned to the agreed attribute templates for ingestion into MRM Vault.
- Solytics will proceed with data migration activities only after receiving client approval on data completeness and accuracy.
- All workflows, role hierarchies, access matrices, and lifecycle configurations must be finalized and approved by HDFC before system setup.
- HDFC will provide access credentials and API tokens (if applicable) for integration with internal systems or data sources required for automation or migration.

Communication & Notifications

- HDFC will provide the required email server credentials, SMTP details, and notification gateway parameters to enable automated communication and alerts.
- Notification templates and escalation matrices will be finalized during the configuration phase and approved by the governance team.

Testing, UAT & Go-Live

- HDFC will nominate User Acceptance Testers (UAT) and SPOCs from both Business and IT teams for each sprint, ensuring timely validation and feedback closure.

- UAT observations will be tracked through a shared tracker, and closure sign-off will be required for every sprint before progression to the next phase.
- Final UAT sign-off and Go-Live approval will be provided by HDFC PMO upon successful completion of all planned test scenarios and resolution of identified issues.
- Go-Live readiness will include verification of infrastructure stability, data validation completion, and access control testing.

User Access Management (UAM)

- MRM Vault's User Access Management (UAM) module has been designed and configured specifically for HDFC's organizational structure.
- A separate FSD has been provided for this module, detailing access roles, approval workflows, and audit controls.
- UAM configuration will be subject to HDFC's internal security validation and approval before activation in the production environment.

General Project Conditions

- Any dependencies on external systems, data sources, or third-party tools (e.g., SFTP, SharePoint, AD integration) must be communicated and provisioned by HDFC prior to the start of the respective sprint.
- Delays in approvals, infrastructure readiness, or data sharing from HDFC may impact project timelines and will require mutually agreed schedule adjustments.
- Both Solytics and HDFC teams will maintain shared responsibility for adherence to the agreed Project Plan, Testing Schedule, and Issue Resolution SLAs.

6 Key Dependencies

Infrastructure Provisioning

- Servers, VPN access, SSL certificates, and database environments must be provisioned, configured, and validated by HDFC's IT/Infrastructure team as per the agreed specifications.
- Network connectivity (VPN/SFTP/Firewall whitelisting) must be in place prior to installation and configuration.
- Database and server readiness confirmation must be formally communicated before initiating deployment activities.
- Any delay in infrastructure provisioning may impact the sprint timelines and Go-Live plan.

Approvals

- Approvals from HDFC's Enterprise Architecture (EA), Information Security Department (ISD), and Project Management Office (PMO) are mandatory prior to environmental deployment and production migration.
- Solytics will proceed with deployment only after receiving written approval via HDFC's internal governance process.

- Any design change post-approval will follow the formal Change Control Process (CCP).

Requirements & Workflows

- All finalized Requirement Documents (RDs), workflows, templates, and attribute libraries must be provided and approved by HDFC's Business / MRM Governance team before configuration begins.
- Any updates to process flow or attributes post-sign-off will require mutual review and impact assessment.
- Workflow dependencies (e.g., between Registration, PDV, and Monitoring) must be validated by the governance team.

Data Migration

- Clean, structured, and validated model inventory data aligned to the agreed attribute templates must be provided by HDFC's Data / Model Governance team.
- Solytics will not modify client data; cleansing and deduplication will be the responsibility of HDFC prior to migration.
- Data mapping and migration testing will occur only after HDFC's written confirmation of data completeness.

UAT Execution

- User Acceptance Testing (UAT) will be coordinated by HDFC's Business and QA teams with support from Solytics.
- HDFC will nominate UAT testers and SPOCs to execute test cases and validate sprint deliverables.
- Feedback incorporation and UAT closure will be tracked in a shared log and formally approved before Go-Live.

Go-Live Readiness

- Production deployment, communication, and Go-Live approval will be coordinated by HDFC's PMO and Risk Governance committees.
- Go-Live readiness will include confirmation of data migration success, UAT closure, infrastructure stability, and user access validation.
- Final sign-off from the PMO and Governance Lead is required before production release.

Security & Access Credentials

- HDFC will provide secure credentials (VPN, SFTP, SMTP, and role-based access tokens) and ensure compliance with internal InfoSec controls.
- Solytics will not store or retain credentials beyond the project lifecycle.
- Connectivity testing and credential validation must be completed before initiating configuration activities.

Communication & Escalation

- Both Solytics and HDFC will maintain a mutually agreed communication and escalation matrix throughout the project.
- All key dependencies, blockers, or delays will be logged and reviewed weekly during governance meetings.
- Escalations will follow the defined project RACI for timely resolution.

About Solytics Partners

Solytics Partners is a global services and solutions provider in the area of Risk, Compliance, Analytics and Technology. We bring a unique ecosystem of deep domain expertise, along with advanced analytics and new age technology to accelerate value creation for our clients. Our regulatory and industry best practices compliant services and technology solutions enable leading corporations and institutions worldwide to create and sustain competitive advantage.

Solytics Partners Privacy Notice

Solytics Partners is committed to respecting your privacy and choices. We may collect, store and use your contact information, such as your name, email id and address to fulfil your request or to provide you additional information.

Disclaimer

This document is the proprietary property of Solytics Partners, all its legal entities and affiliates (the “Company”) and is strictly confidential. It contains information intended only for the person to whom it is transmitted. With receipt of this information, recipient acknowledges and agrees that: (i) this document is not intended to be distributed, and if distributed inadvertently, will be returned to the Company as soon as possible; (ii) the recipient will not copy, fax, reproduce, divulge, or distribute this confidential information, in whole or in part, without the express written consent of the Company; (iii) all of the information herein will be treated as confidential material with no less care than that afforded to its own confidential material.

The information provided in this document is for informational purposes only. It is not offered as advice on a particular matter and should not be relied upon as such and Solytics Partners disclaims any liability arising out of the use of the information for any purpose whatsoever. Solytics Partners makes every reasonable effort to present current and accurate information. However, Solytics Partners makes no guarantee of any kind with respect to accuracy or otherwise. Solytics Partners reserves the right to modify the content of this document at any time without prior notice.

The details given in the document, including the employees’ profiles and pricing information are only indicative. The actual profiles and pricing (if any) may vary depending on the scope of work and other applicable factors. Exchange of information through this document does not constitute a legal contract or consulting relationship with any person or entity.