Steward Override and Approval Matrix for Security Data Corrections

Table of Contents

Introduction

This document delineates the procedures and approval matrices governing steward-initiated overrides on master data attributes within the Material Data Management (MDM) system. It is designed to guide authorized personnel through the steps required to request, approve, or reject override actions, ensuring compliance with governance standards. It also details the documentation standards for capturing the rationale behind overrides, attaching relevant supporting data, and maintaining data lineage integrity.

The purpose of this document is to facilitate accurate, auditable updates to

security-related master data, supporting data quality, integrity, and regulatory compliance. This is particularly vital for operations involving sensitive security data such as vendor taxonomies, sector classifications, and security identifiers.

Scope and Responsibilities

This procedure applies to all authorized stewards and data governance personnel responsible for maintaining master security data attributes. It encompasses:

- Requesting overrides for specific data attributes affected by discrepancies or updates.
- Approval workflows based on override impact, attribute criticality, and data sensitivity.
- Documentation and audit trailing of all override actions.

Responsibilities:

- **Stewards**: Initiate override requests with supporting documentation and comments.
- **Approvers**: Review override requests based on the approval matrix, approve or reject with documented rationale.
- **Data Governance Team**: Maintain the approval matrix, audit logs, and ensure compliance.

Overview of Master Data Overrides

Master data overrides are exceptional modifications to security data attributes that cannot be resolved via normal data update procedures. Such overrides may result from discrepancies identified during data reconciliation, vendor schema updates, or regulatory requirements.

These overrides impact modules such as:

- ADR (Authorized Data Reconciliation) Mapping
- ETF Constituents Reconciliation
- CUSIP/ISIN/SEDOL identifiers
- Lineage data updates
- Vendor taxonomy classifications

Proper handling ensures data consistency, auditability, and ensures

compliance with policies governing sensitive security information.

Override Types and Attributes

Override Types

Type	Description	Typical Use Cases
Data Attribute Override	Adjustment or correction of core data attribute values such as Security ID, Sector Code, or Vendor Taxonomy.	Correcting incorrect CUSIP entries, updating Moody's sector classifications, fixing vendor taxonomy mismatches.
Identifier Override	Override or correction of unique identifiers like ISIN, SEDOL, or Bloomberg suffix patterns.	Reconciliation after schema updates, vendor-supplied corrections, or duplicate entry resolution.
Lineage Override	Amendments to data lineage records to reflect updated source or transformation history.	Fixing lineage gaps detected during validation of master data flow.

Attributes Subject to Override

- Security Identifiers: CUSIP, ISIN, SEDOL
- Vendor Taxonomy Codes and Descriptions
- Sector and Industry Classifications
- Security Name and Description
- Data Lineage Fields

Approval Matrix for Overrides

Approval levels are determined by the override type, attribute impacted, and the severity of the impact. The following matrix provides guidance on approval requirements:

Override Type	Attribute	Impact Severity	Required Approval Level	Conditions

Data Attribute Override	CUSIP / SEDOL / ISIN	Low	Steward	Minor corrections, no impact on downstream modules
Data Attribute Override	Sector / Vendor Taxonomy	Medium	Senior Steward / Data Governance Lead	Impact on classification and reporting
Lineage Override	Lineage Records	High	Data Governance Director	Major process or source change
Identifier Override	Security Identifiers	Critical	Executive Approval	Potential regulatory compliance impact

Note: Override requests exceeding the thresholds require documentation and are logged for audit purposes.

Override Request Procedure

Prerequisites

- Access to the MDM override request portal or form
- Supporting documentation justifying the override (e.g., vendor correspondence, reconciliation reports)
- Clear description of the data discrepancy or correction necessary

Step-by-Step Process

1. **Initiate Request:** Fill out the override request form via the designated portal, specifying relevant details:
    - Override Type
    - Impacted Attribute(s)
    - Data Original Value(s)
    - Proposed New Value(s)
    - Supporting Documents (attach files or links)
    - Rationale for Override
2. **Submit for Review:** Submit the request, which triggers an automated

workflow routed to the appropriate approver based on the approval matrix.
3. **Approval Workflow:** Approvers review the request, evaluate supporting documents, and either approve or reject, including comments or conditions if rejected.
4. **Implementation:** Upon approval, the steward performs the override in the MDM system, documenting the override action in the system.
5. **Audit and Record:** All actions, comments, and supporting documents are logged for audit trailing.

Verification post-Override

Stewards must validate that the override has been correctly applied and that downstream modules reflect the changes. This includes executing validation checklists and cross-module reconciliation.

Documentation Standards for Overrides

Each override must be documented with comprehensive comments explaining the rationale, referencing supporting evidence, and attaching relevant supporting documentation. This ensures transparency and facilitates audits.

Comments Content Guidelines

- Explicit explanation of the discrepancy or reason for override
- Source references, such as vendor communication or reconciliation reports
- Impact assessment notes
- Follow-up instructions or conditions, if any

Supporting Documentation Standards

- Vendor letters, email correspondence
- Reconciliation reports or data extracts
- Regression test results

All attachments should be securely stored and linked within the override request system with proper access controls.

Supporting Documentation and Examples

Example: Vendor Taxonomy Update

A vendor reports a change in taxonomy code for a security asset, requiring an override:

- Original Vendor Taxonomy Code: VT-1234
- Updated Code Received from Vendor: VT-5678
- Supporting Document: Vendor Correspondence Email

Example: Correcting CUSIP

A reconciliation report indicates a mismatch in CUSIP entries for an asset ID, requiring override:

- Original CUSIP in System: 123456789
- Corrected CUSIP: 987654321
- Supporting Document: Reconciliation Log

FactSet Concordance Rule Example

Mapping rule for CUSIP/ISIN/SEDOL alignment: `IF CUSIP matches 123456789, THEN map to ISIN US1234567890 and SEDOL 1234567.`

Validation and Verification Procedures

Pre-Override Validation

- Check that the data discrepancy is valid and supported by documentation.
- Review the change impact on downstream systems, including reporting and trading modules.
- Confirm that the override aligns with regulatory requirements.

Post-Override Verification Checklist

Check Item	Verification Method	Status
Data Value Accuracy	Cross-check with source documents	
System Reflection	Query affected modules for updated values	

Downstream Impact	Run reconciliation reports	
Audit Trail Entry	Review system logs for override record	

Any anomalies identified during verification must be logged with corrective action plans.

Error Codes & Troubleshooting

Common Error Codes

Error Code	Symptom	Root Cause	Resolution Steps	Prevention Tips
MDM-ID-3102	Identifier conflict during override	Duplicate CUSIP or ISIN in system due to prior untracked override	Verify existing identifiers, resolve duplicates, and document the correction	Regular audits of identifier consistency and enforce validation rules
MDM-LIN-2207	Lineage gap detected	Missing source or transformation record	Revisit source data, re-run lineage tracing, and document correction	Implement lineage validation checkpoints during data loads
MDM-COM-1905	Comment required for override	Override lacks adequate rationale documentation	Prompt steward to provide detailed comments and supporting evidence	Mandatory comment entry in override request forms

Troubleshooting Flowchart

> **Step 1:** Encounter error during override submission
>
> **Step 2:** Review error code documentation

> **Step 3:** Follow resolution steps or escalate to Data Governance
>
> **Step 4:** Confirm resolution and re-submit request if applicable

Lineage Documentation Templates

Sample Lineage Document Structure

Section	Details
Source Data	Original source system, data extract timestamp, and source integrity checks
Transformation Details	Description of data transformations, validations, and rules applied</