Admin & Rule Management Module

Governance, Rule Lifecycle & Safety Controls (Compliance AI POC)

---

1. Purpose of This Module

This document defines **how compliance rules are created, modified, validated, and governed** in the Compliance AI Platform.

It focuses on: - Admin vs Super Admin responsibilities - Safe rule creation and modification - Prevention of duplicate or conflicting rules - Rule versioning, deletion, and auditability

This module is critical for **fintech-grade governance** and completes the compliance story of the POC.

---

2. Design Philosophy (Non-Negotiable)

The rule management system is designed with the following principles:

1. **Human Authority** – Only humans can create or approve rules
2. **AI Assistance, Not Control** – AI may suggest, never enforce
3. **Single Source of Truth** – SQL DB is authoritative
4. **No Silent Changes** – Every rule change is auditable
5. **Duplicate Prevention** – System actively prevents human error

---

3. User Roles & Permissions

3.1 Super Admin (Rule Authority)

Primary responsibility: Owns the rulebook

Capabilities - Create new compliance rules - Edit existing rules (text, severity, category) - Improve or refine rule wording over time - Activate / deactivate rules - Delete rules (with safeguards) - Upload regulatory documents for reference - Approve final rule versions

Super Admin actions are **high-impact and fully audited**.

3.2 Admin (Compliance Operations)

Primary responsibility: Operates within the rulebook

Capabilities - View all rules (read-only) - Enable / disable rules (if permitted) - Adjust severity thresholds (policy-controlled) - Monitor rule hit frequency - Review violations and trends

Admins **cannot create or delete legal rules**.

---

4. Rule Lifecycle (End-to-End)

```
Draft → Review → Active → Updated / Deprecated → Archived
```

Rules are never silently overwritten.

---

5. Rule Creation Workflow (Safe & Simple)

Step 1: Manual Rule Entry (Super Admin)

Super Admin enters: - Rule text (legal wording) - Category (IRDAI / Brand / SEO) - Severity (LOW / MEDIUM / HIGH) - Optional explanation

---

Step 2: Duplicate & Conflict Detection (Automatic)

Before saving, the system runs:

1. **Exact match check** (SQL)
2. **Semantic similarity check** (Vector DB)

If similarity exceeds threshold (e.g., 85%): - System blocks save - Shows existing rule - Requires explicit confirmation

This prevents **human duplication errors**.

Step 3: Rule Validation (Optional AI Assist)

AI may: - Flag ambiguous language - Highlight missing constraints - Suggest severity

AI suggestions are **non-binding**.

Step 4: Approval & Activation

Only after Super Admin approval: - Rule is saved in SQL DB - Version number assigned - Rule becomes enforceable

---

6. Rule Improvement & Modification

Rules evolve over time.

Supported Improvements

- Clarify wording
- Add exceptions
- Adjust severity
- Add examples or notes

How Updates Work

- Original rule remains immutable
- New version created (v2, v3, ...)
- Old version archived

Compliance results reference the **exact rule version used**.

---

7. Rule Deletion Strategy (Controlled)

Why Deletion Is Dangerous

- Breaks audit trails
- Invalidates past decisions

Safe Deletion Model

Instead of hard delete: - Rule is marked as **DEPRECATED** - Rule is set `is_active = false` - Rule remains in DB for audit

Hard deletion is: - Restricted - Requires justification - Logged permanently

---

8. Duplicate Rule Prevention (Critical Feature)

Why This Is Needed

Human admins may: - Re-enter similar rules - Use different wording - Forget existing rules

Prevention Mechanisms

Layer	Check
SQL	Exact text match

Layer	Check
Vector DB	Semantic similarity
UI	Warning + preview

This ensures **rule consistency at scale**.

---

9. Data Storage Responsibilities

SQL Database (Authoritative)

- Rule text
- Version history
- Severity & category
- Created / updated by
- Active / deprecated status

Vector Database (Supportive)

- Embeddings of rule explanations
- Clause-level regulatory text
- Used only for retrieval & similarity

Vector DB **never enforces rules**.

---

10. Audit & Compliance Guarantees

Every rule action records: - Who performed it - What changed - Previous vs new value - Timestamp - Reason (optional)

This satisfies: - Internal audits - Regulatory scrutiny - Legal review

---

11. Failure & Safety Scenarios

Scenario	System Behavior
Duplicate rule entered	Block + warn
Conflicting rule	Require manual override
Accidental delete	Soft-delete only
Admin misuse	Role-based restriction

---

12. What This Module Explicitly Does NOT Do

- Auto-scrape regulatory websites
- Auto-publish AI-generated rules
- Allow AI to delete or activate rules

Human control is mandatory.

---

13. Key Takeaway

> **Compliance rules are legal artifacts. This module ensures they are created, modified, and governed with the same rigor as financial policies—while still being easy for Super Admins to manage.**

This document defines the complete Admin & Rule Management workflow for the Compliance AI POC.