RiskaVaire User Manual

This user manual is designed to help users understand and navigate the platform effectively. It covers all essential modules and functionalities, including login, profile management, role-based access control, policy management, compliance workflows, audits, incident handling, and risk management.

Unlock Strategic Control with RiskaVaire

In today's dynamic business environment, effective Governance, Risk, and Compliance (GRC) are not just about meeting obligations—they're about building a foundation for resilience and growth. The Vardaan's GRC Platform RiskaVaire is your comprehensive, intuitive solution designed to integrate these critical functions seamlessly, transforming complexity into clarity.

Core Capabilities at Your Fingertips:

The platform provides role-based dashboards tailored to different users—whether risk owners, auditors, compliance officers, or business users—ensuring that each individual sees only the information and actions relevant to their responsibilities. Its advanced analytics and reporting capabilities give management a clear view of organizational performance, policy adoption, compliance maturity, audit effectiveness, and risk exposure, empowering data-driven decisions at every level.

Users benefit from features such as policy creation and versioning, compliance mapping and tailoring, audit planning and evidence tracking, incident escalation and resolution workflows, and structured risk assessment and scoring. Interactive dashboards, KPI analysis, and real-time notifications ensure that users remain aligned with organizational goals while responding quickly to emerging issues.

By integrating automation, secure access controls, and intuitive navigation, the Vardaan's GRC Platform RiskaVaire reduces complexity and ensures accountability across teams. It supports both day-to-day operational needs and long-term strategic oversight, making it an indispensable tool for organizations seeking to strengthen resilience, maintain regulatory alignment, and foster a culture of proactive risk management.

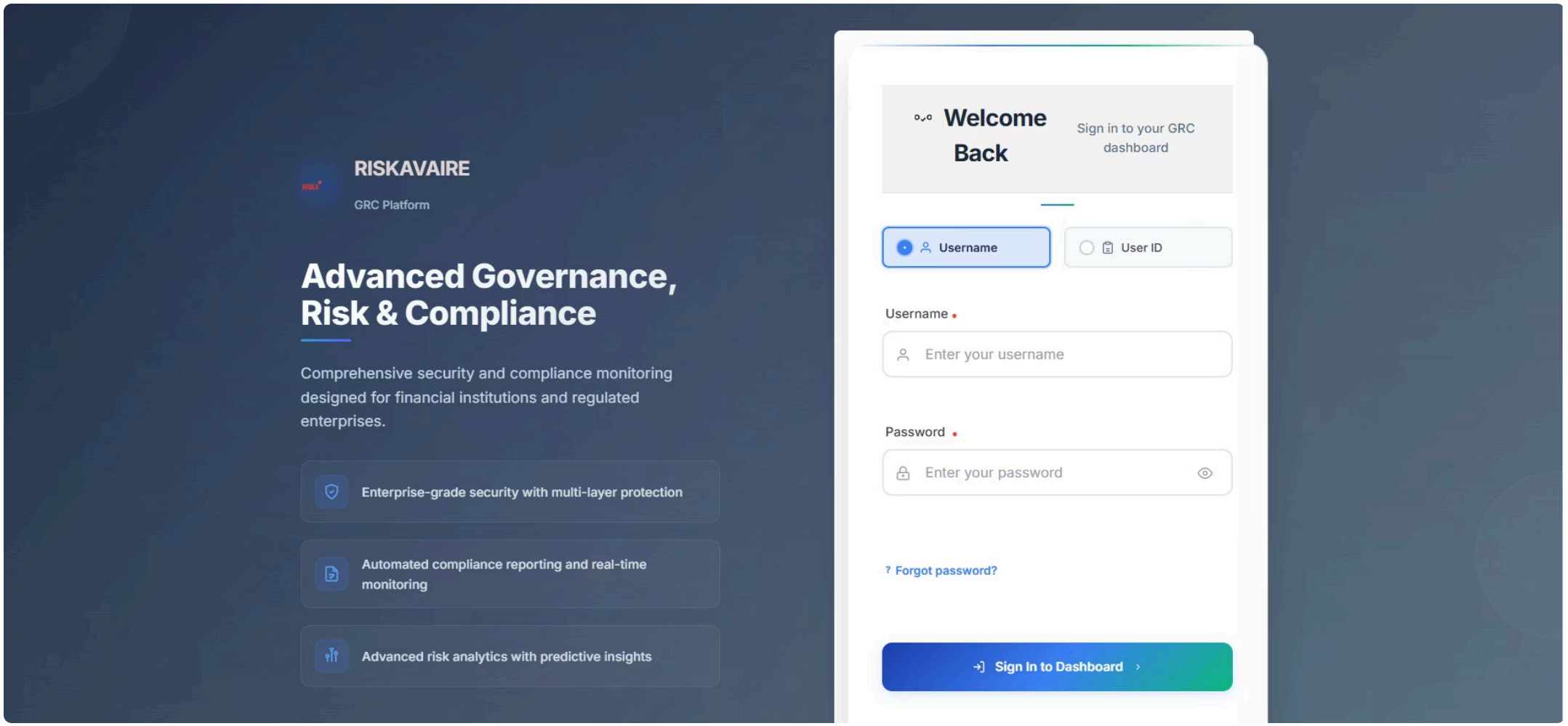
Table of Contents

Getting Started and User Settings

This section will walk you through the core navigation and user account functionalities, helping you understand how to effectively use the system.

Login Process

- Log in using either your User ID or Username
- Enter your credentials in the respective fields
- Click "Sign in to Dashboard" to proceed
- Complete Multi-Factor Authentication (MFA) if enabled
- Use "Forgot Password" option if needed to reset your password
- **Note:** Users will receive their initial login credentials from the Administrator via email. These credentials should be used for the first login. During the first-time login, users will be prompted to complete a consent form, where they must review and accept the Terms and Conditions, End User License Agreement (EULA), and the Privacy & Security Policy to proceed.



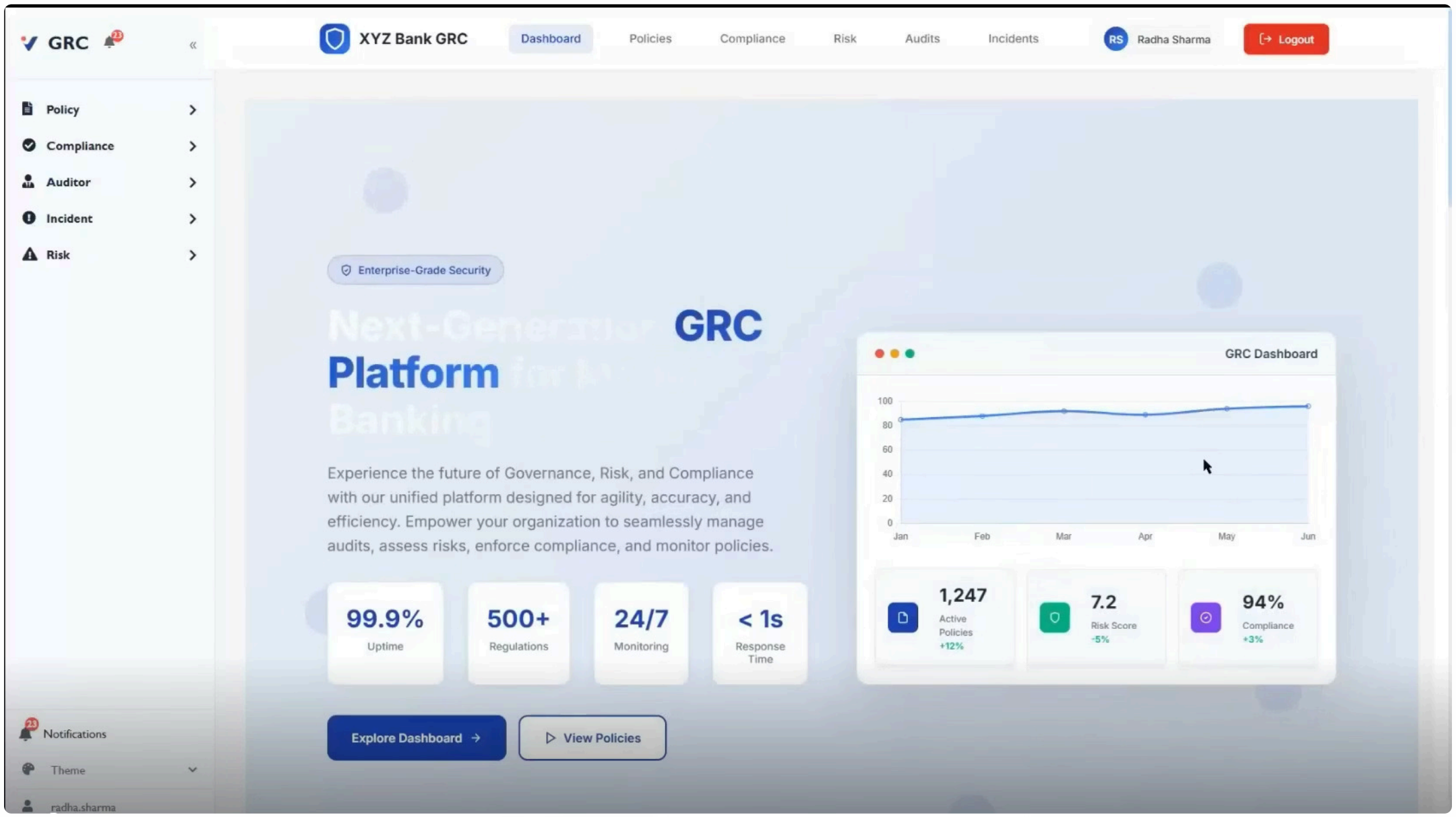
Dashboard Overview

Upon logging in, you'll see a dashboard tailored to your specific role—whether you're a Risk Owner, Auditor, or Admin—ensuring you only access relevant modules.

The dashboard displays statistics relevant to your role, including:

- Total number of Policies
- Regulations
- Uptime
- Response Time

Quick access options are available to View Dashboard and View Policies.



Navigation System

Left Navigation Bar

The left navigation bar provides quick access to key modules: Policy, Compliance, Audit, Incident, and Risk. Selecting any module will reveal its associated submodules.

Notifications and Theme options are conveniently located at the bottom.

Top Bar

The top bar offers essential navigational tools, including a logout option positioned on the far right.

Further down the page, you'll find detailed module descriptions and access to the Advanced Analytics and Reporting section.

Notifications Management

The Notifications page allows you to stay updated with all system alerts and messages.

Accessing Notifications

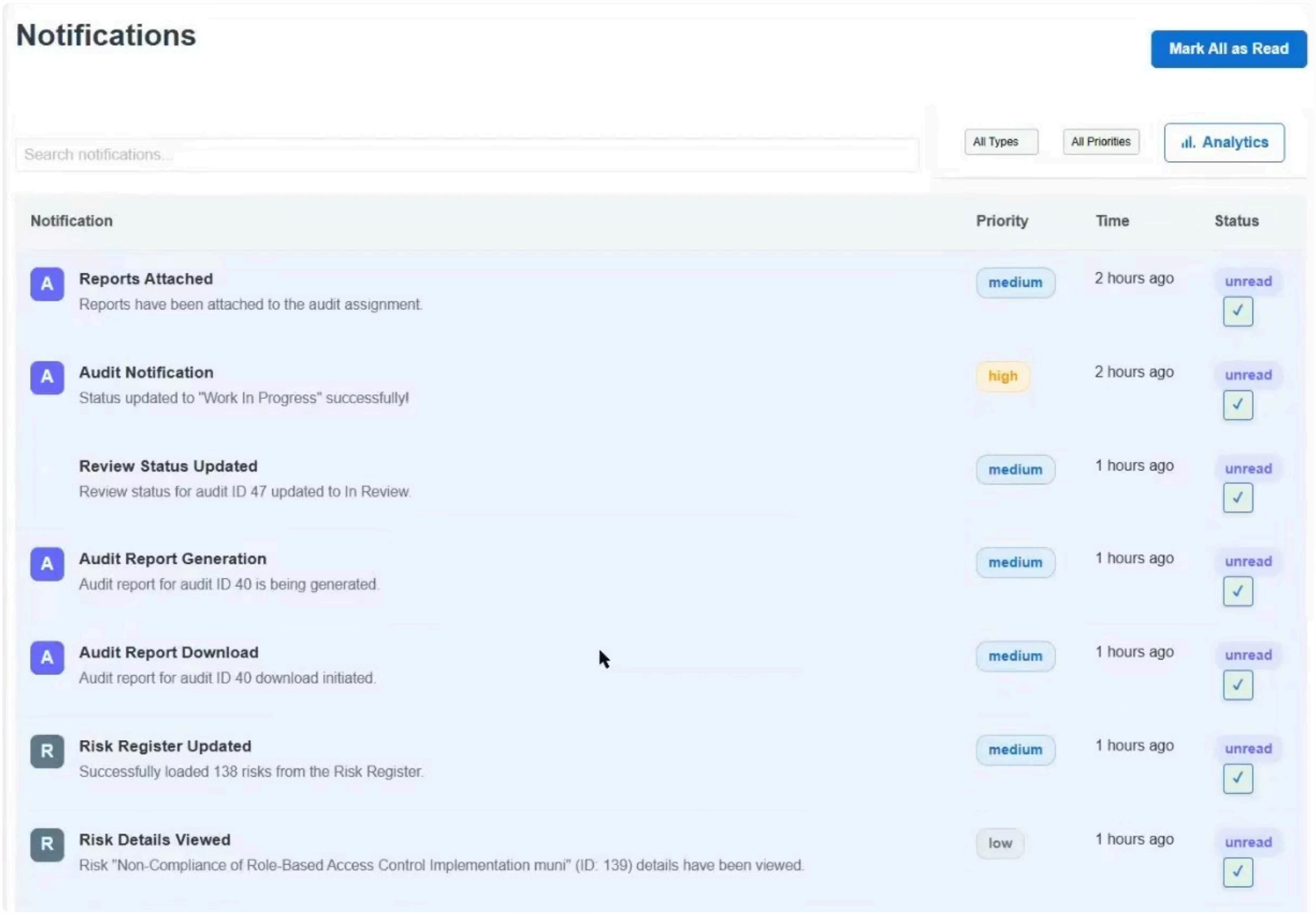
Click "Notifications" on the left navigation bar to open the Notifications page

Managing Notifications

Mark notifications as Read individually or all at once

Filtering Options

Filter notifications based on Topic and Priority to find relevant information quickly

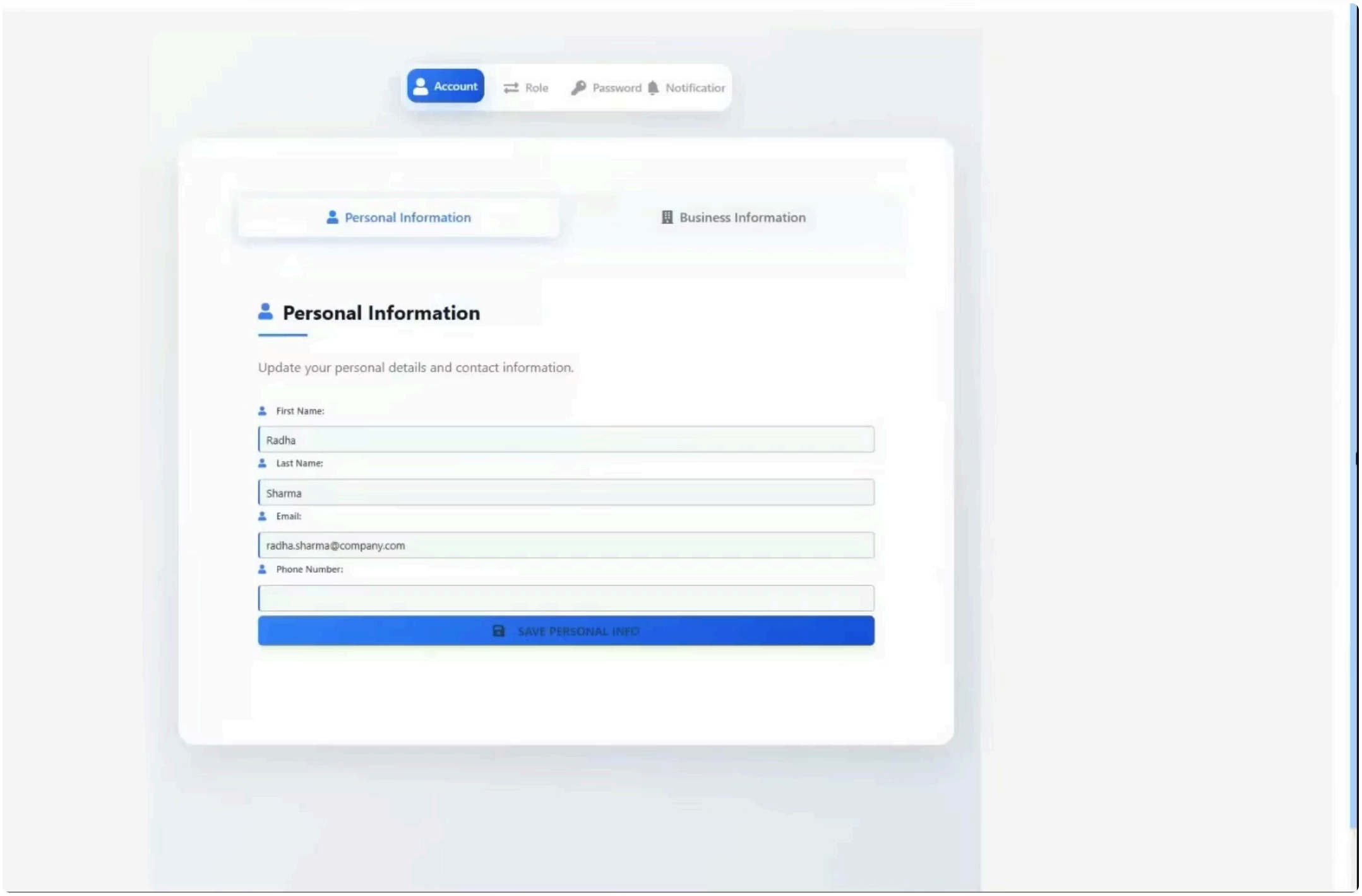


Profile Management

Access your profile by clicking the Profile icon at the end of the left navigation bar. The Profile page contains four main tabs:

- **Account** (default view) - Manage personal and business information
- **Role** - Request role changes
- **Password** - Update your password
- **Notifications** - Configure notification preferences

In the Account section, you can update your Personal Information (name, email, phone) and Business Information (department, business unit, entity, location, department head).



Role-Based Access Control

The system implements a comprehensive role-based access control mechanism to ensure appropriate permissions across the platform.

Role Assignment

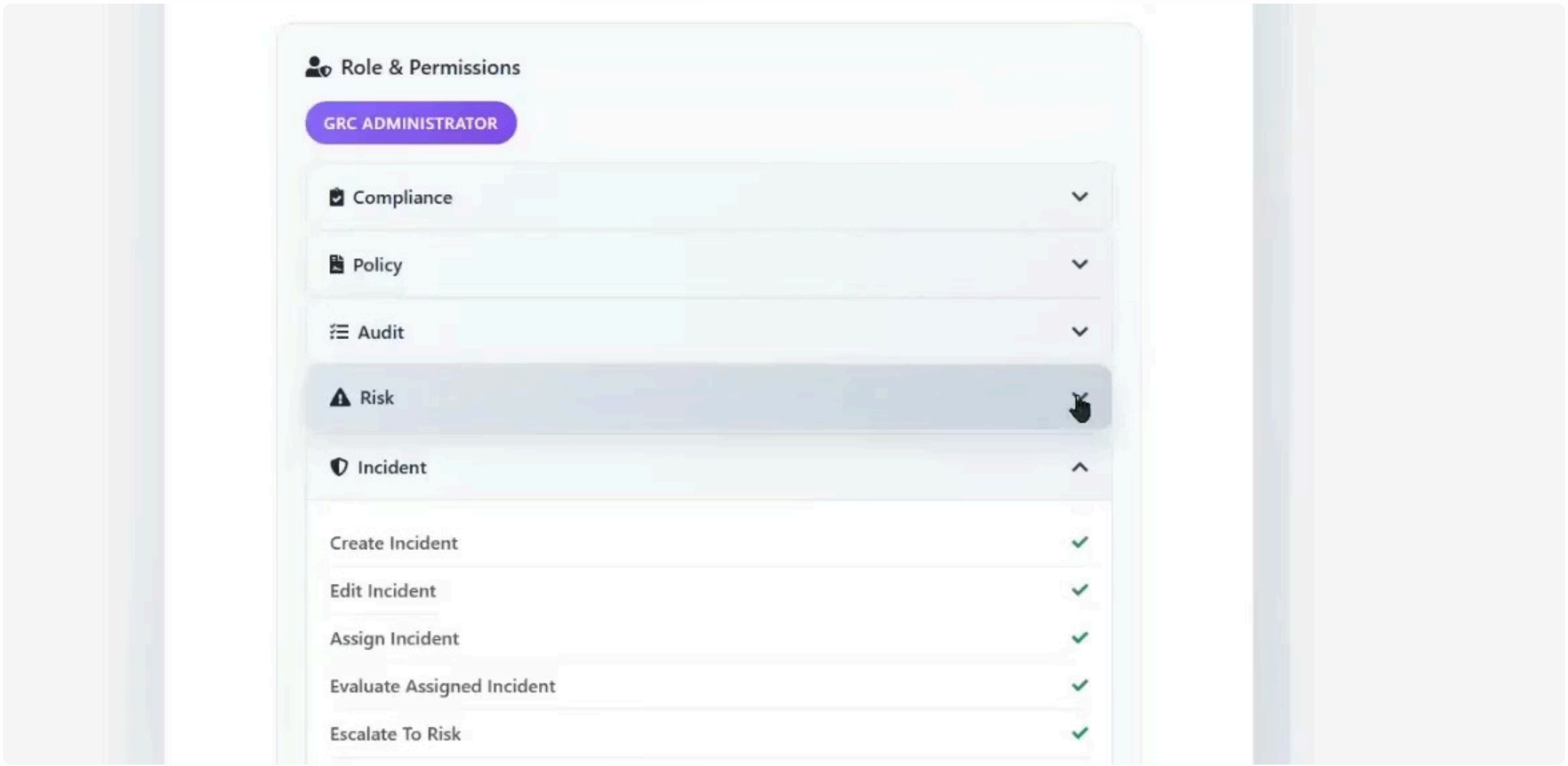
Administrators can assign roles such as ISO Officer, Control Owner, Risk Manager and more

Predefined Permissions

Each role has predefined permissions, ensuring least-privilege access across the system

Customization

The system includes 22 predefined roles, with options to create additional roles and assign different modules and permissions



Requesting Role Changes

Users can request changes to their system role through a simple process:

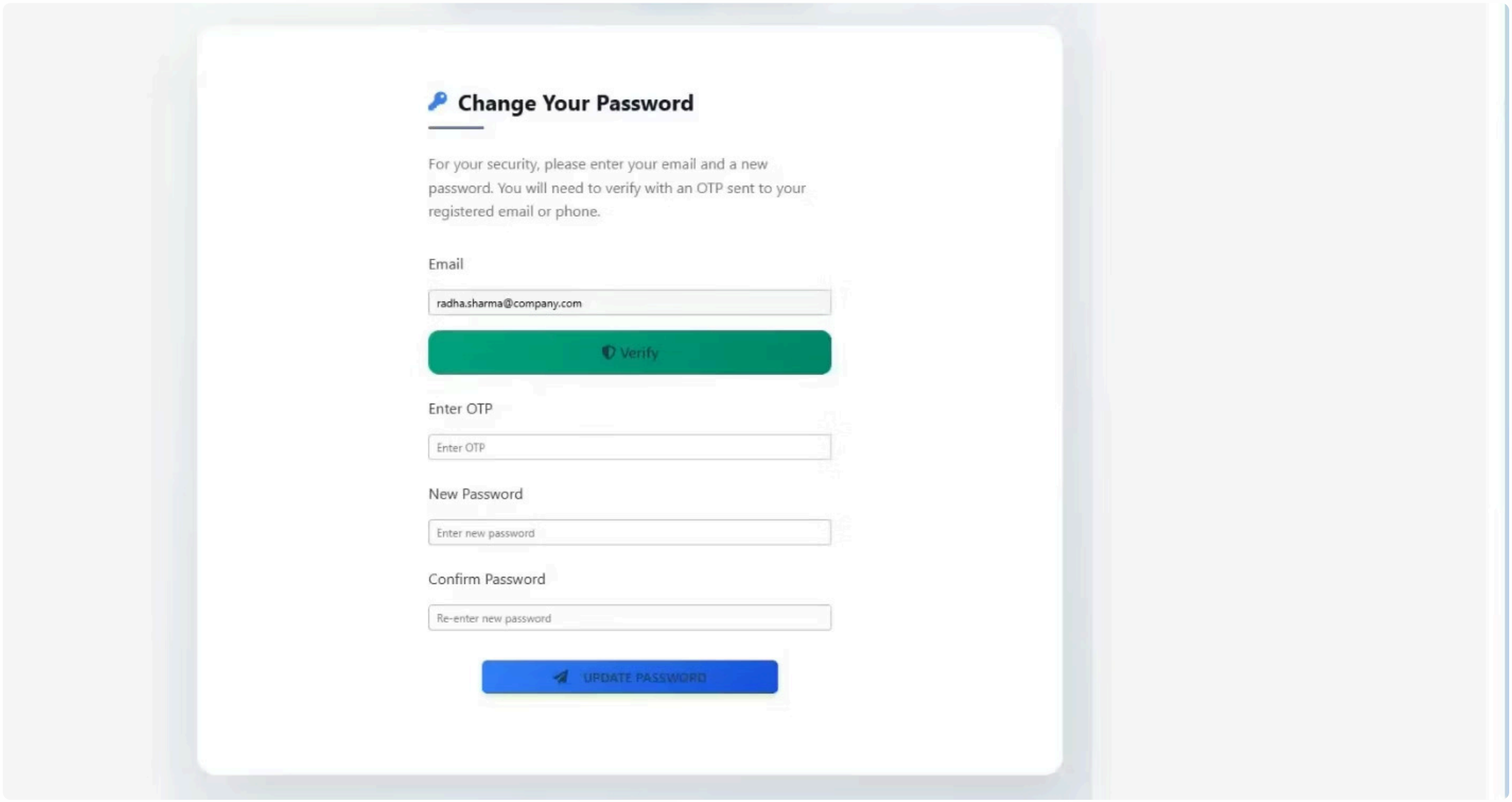
1. Navigate to the Profile section
2. Select the Role tab
3. Enter your Username
4. Select the Role you want access to from the dropdown
5. Click "Request Role Change"

Once your request is approved by an administrator, you will gain access to the modules and actions associated with the requested role.

Password Management

Secure password management is essential for maintaining account security. To change your password:

1. Navigate to the Profile section
2. Select the Password tab
3. Verify your Email ID
4. Enter the OTP received in your email
5. Enter your New Password and confirm it
6. Click "Update Password" to apply the change



Notification Preferences

Customize how you receive system notifications to stay informed about important updates:

- Navigate to the Profile section
- Select the Notifications tab
- Choose your preferred notification channels:
  - Email notifications
  - WhatsApp notifications
  - On-platform alerts
- Enable or disable each channel using the toggle buttons
- Click "Save" to apply your preferences

Policy Module

The Policy Module serves as the central hub for creating, managing, and monitoring organizational policies within the Vardaan GRC Platform. It enables users to build new frameworks and policies, organize them into structured hierarchies, and visualize relationships through an intuitive policy tree. With features such as tailoring, templating, versioning, and AI-assisted framework uploads, the module ensures policies remain accurate, up to date, and aligned with compliance requirements. Integrated approval workflows, metadata tracking, and performance dashboards provide transparency and accountability at every stage, while KPI analysis helps measure adoption, coverage, and effectiveness across the organization.

1

Policy Creation

Create Policy, Upload Framework, Tailoring and Templating, Versioning

2

Policy List

All Policies, Policy Tree

3

Framework Management

Framework Explorer, Framework Approval

4

Approval & Analysis

Policy Approval, Status Change Requests, Performance Analysis

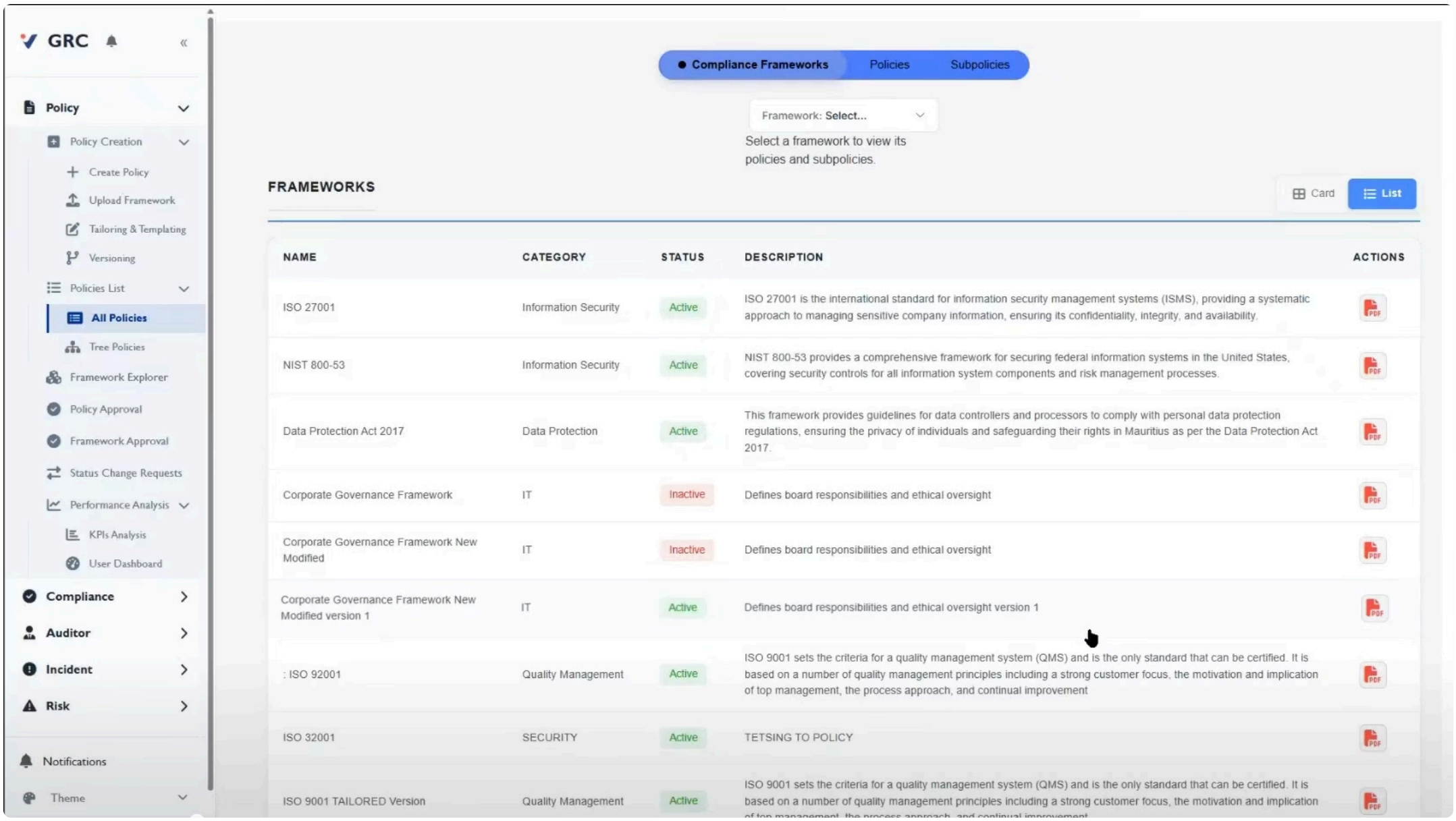
Role-Specific Permissions

Role	View	Create	Edit	Approve	Delete
System Admin	✅	✅	✅	✅	✅
Policy Owner	✅	✅	✅	✅	❌
Compliance Officer	✅	✅	✅	✅	❌
Business User	✅	❌	❌	❌	❌

All Policies View

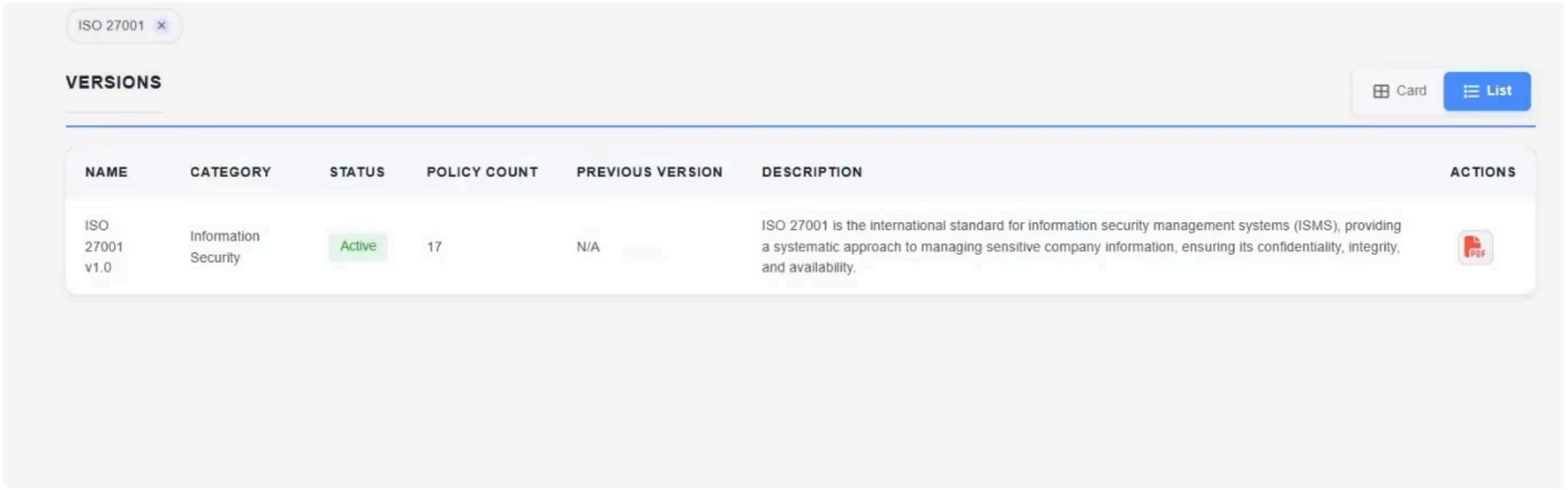
The All Policies view provides a comprehensive overview of all available frameworks, policies, and sub-policies in the system.

- Access this view by clicking "All Policies" in the left navigation bar
- Switch between list view and card view using the view selector in the top-right corner
- Click on any framework to view its versions and details
- Navigate through the hierarchy to explore policies and sub-policies
- View metadata by clicking the PDF icon next to any item

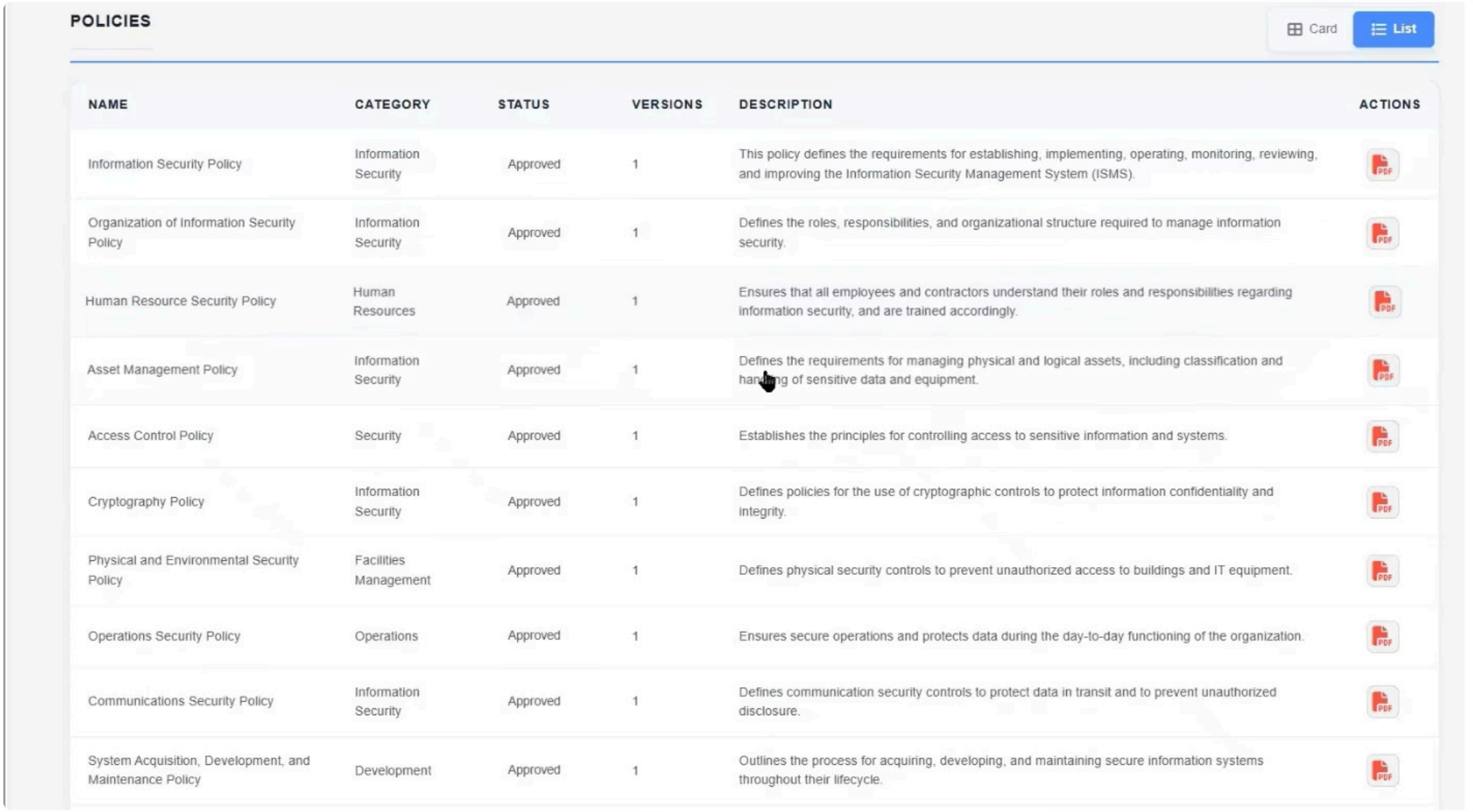


Policy Hierarchy Navigation

Framework Versions page shows Name, Category, Status, Policy Count, Previous Version, and Description



Clicking a version displays all policies associated with that framework version, showing Category, Status, Version Number, and Description

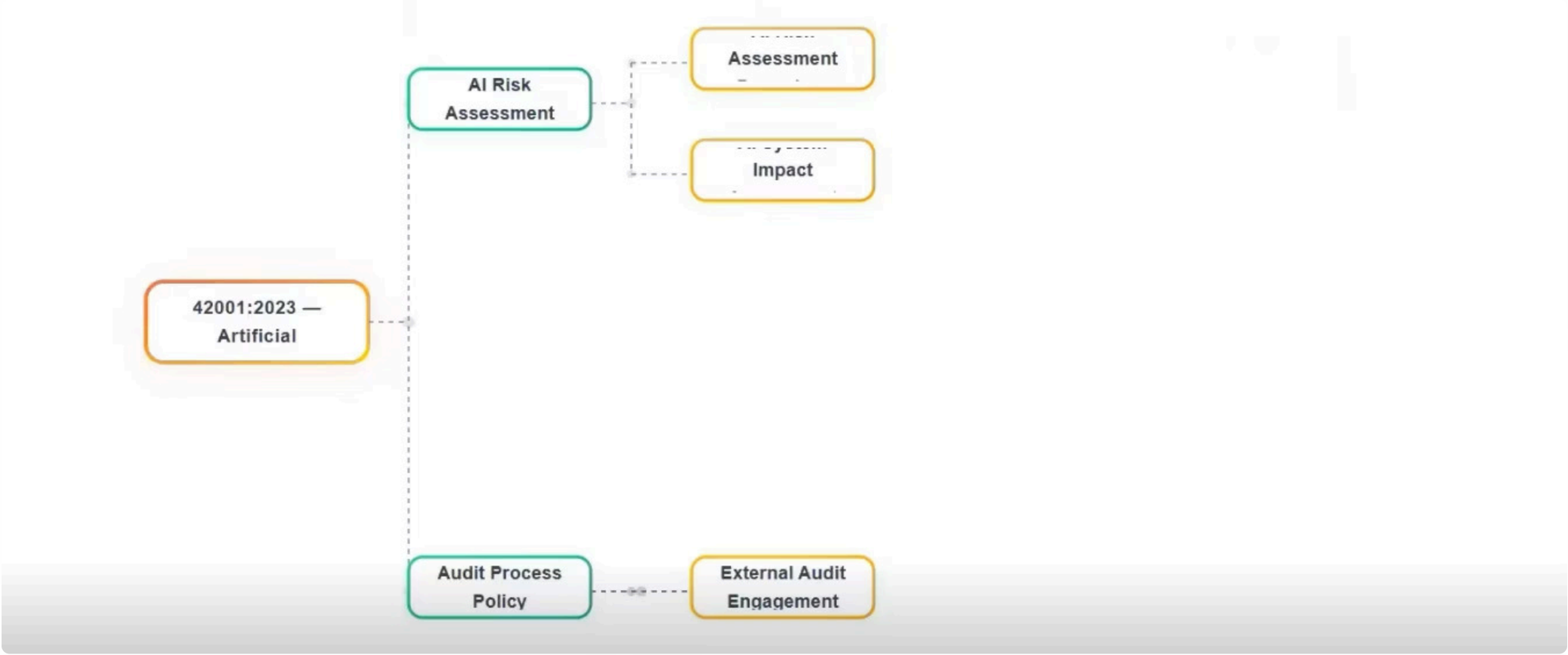


Continue drilling down to view policy versions and sub-policies by clicking on the desired items in each level of the hierarchy.

Policy Tree Visualization

The Policy Tree provides a visual representation of the hierarchical relationship between frameworks, policies, and sub-policies.

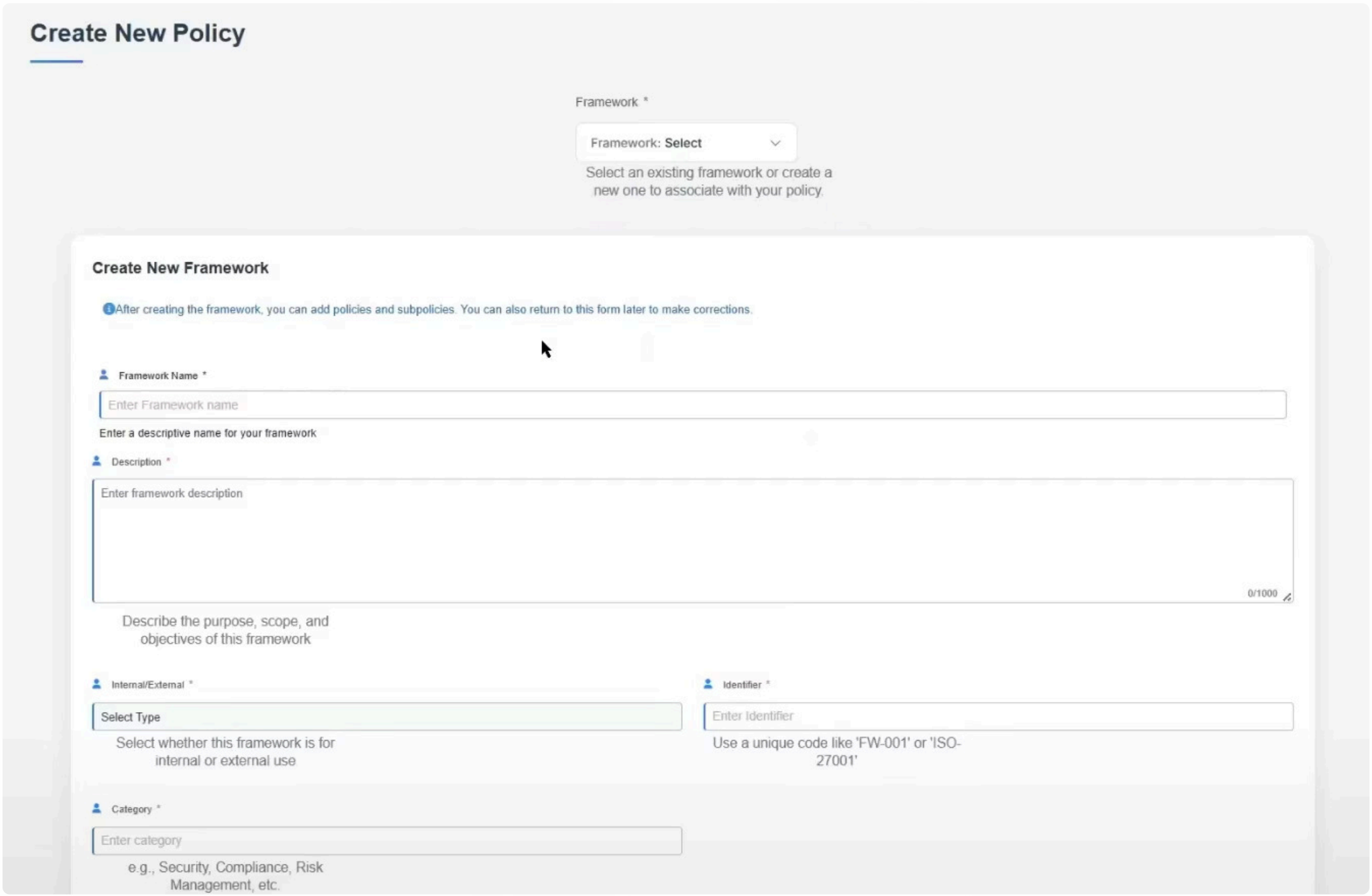
- Access by clicking "Policy Tree" in the left navigation
- Switch between different frameworks using the dropdown selector
- Use the "Expand All" option to view all sub-policies in the hierarchy
- Visualize the complete policy structure in an intuitive tree format
- Quickly identify relationships between different policy components



Creating a New Framework

To create a new framework:

1. Click "Policy Creation" from the left navigation
2. Click "Create New Framework" to open the Framework Creation page
3. Enter the framework details:
    - Framework Name
    - Description
    - Type (Internal or External)
    - Identifier (unique)
    - Category
    - Reference Documents (upload supporting files)
    - Effective Start Date and End Date
4. Click "Continue to Policies" to proceed to the Policy Creation page



Creating a New Policy

Once a framework is created, you can add policies under it by providing comprehensive details:

Basic Information

- Policy Name
- Policy Identifier
- Description
- Scope

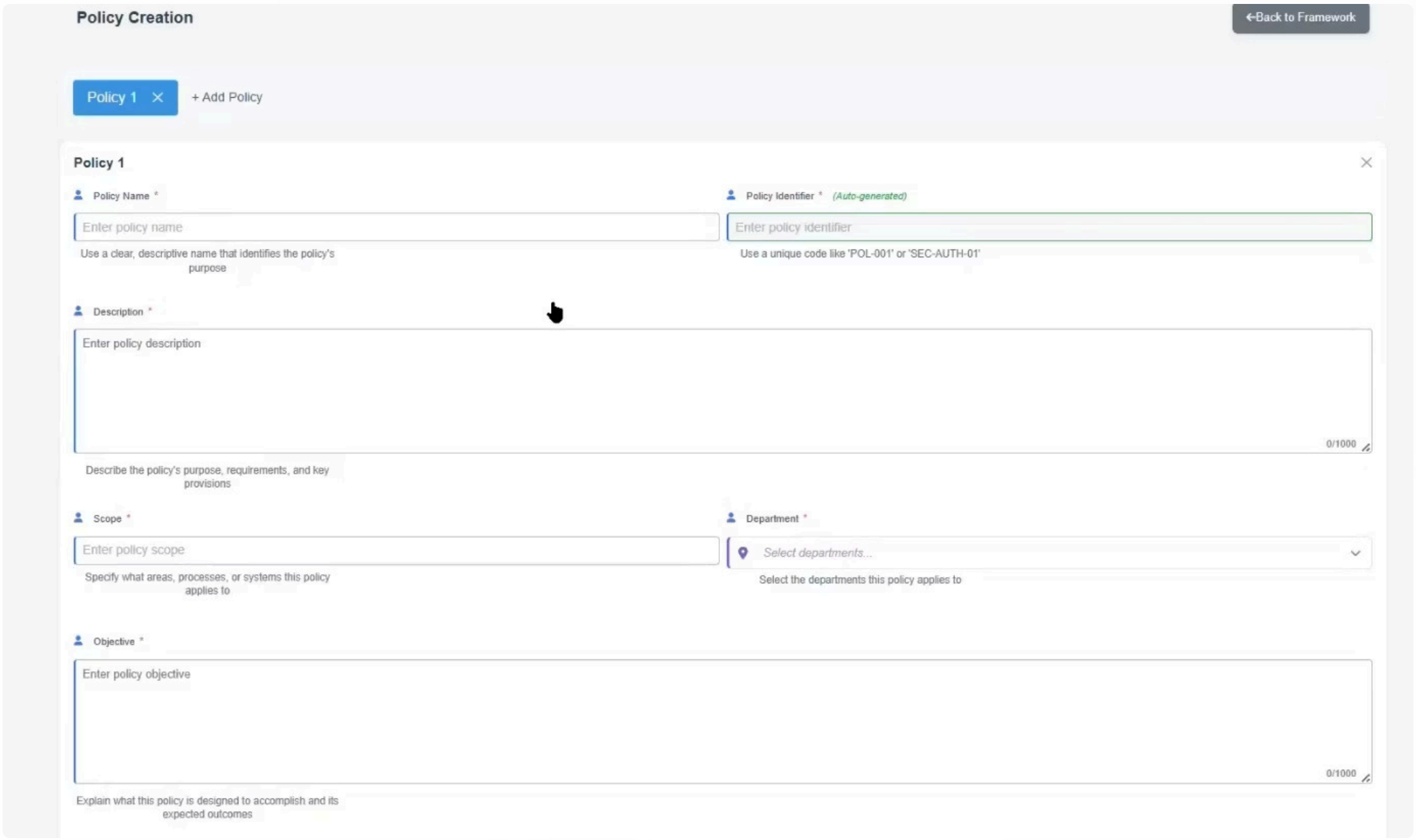
Classification

- Departments
- Policy Type
- Category
- Sub-Category

Implementation

- Objectives
- Coverage
- Applicability
- Applicable Entities

After filling in these details, you can proceed to add Sub-Policies.

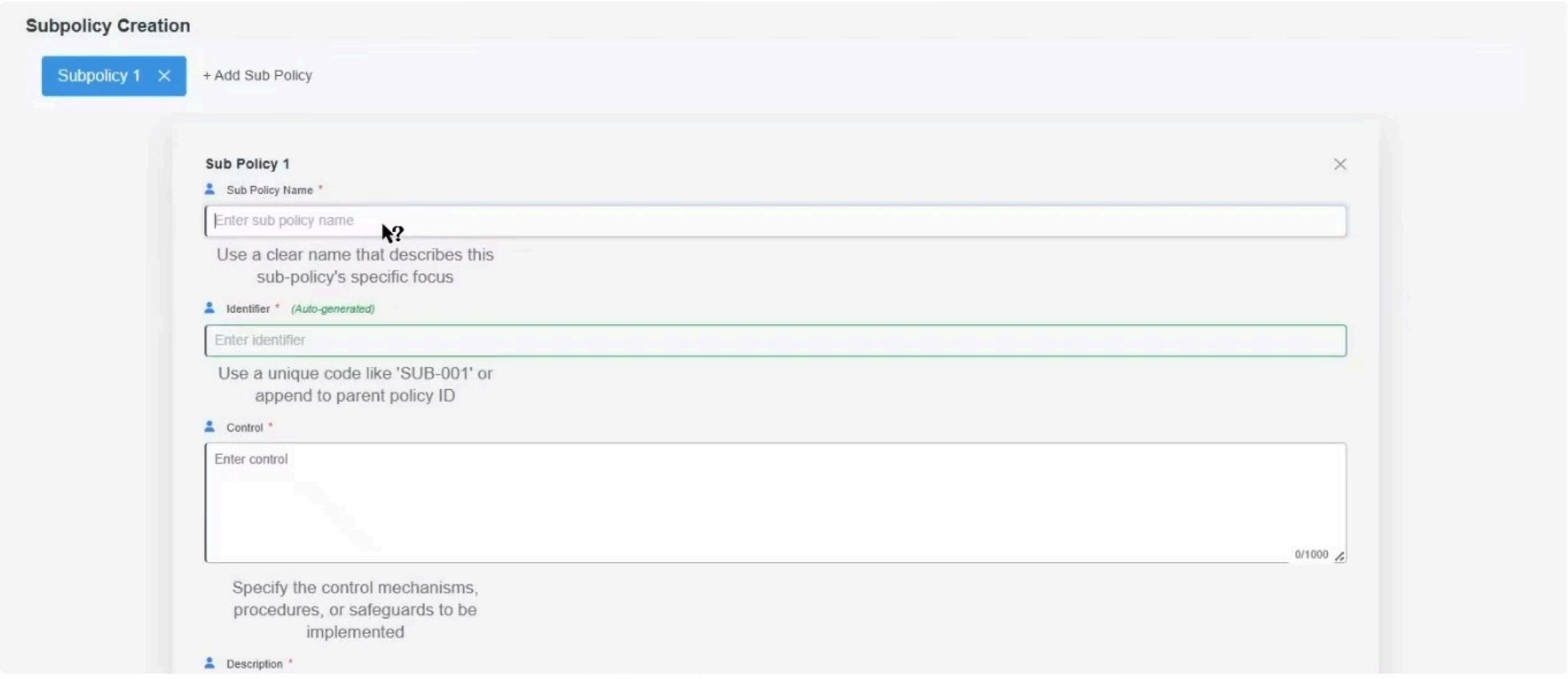


Creating Sub-Policies

Sub-policies provide more detailed guidelines under a main policy. To create a sub-policy:

1. Enter Sub-Policy Name
2. Provide a unique Sub-Policy Identifier
3. Define Controls (mechanisms, procedures, and safeguards)
4. Add a detailed Description (purpose, scope, and specific requirements)

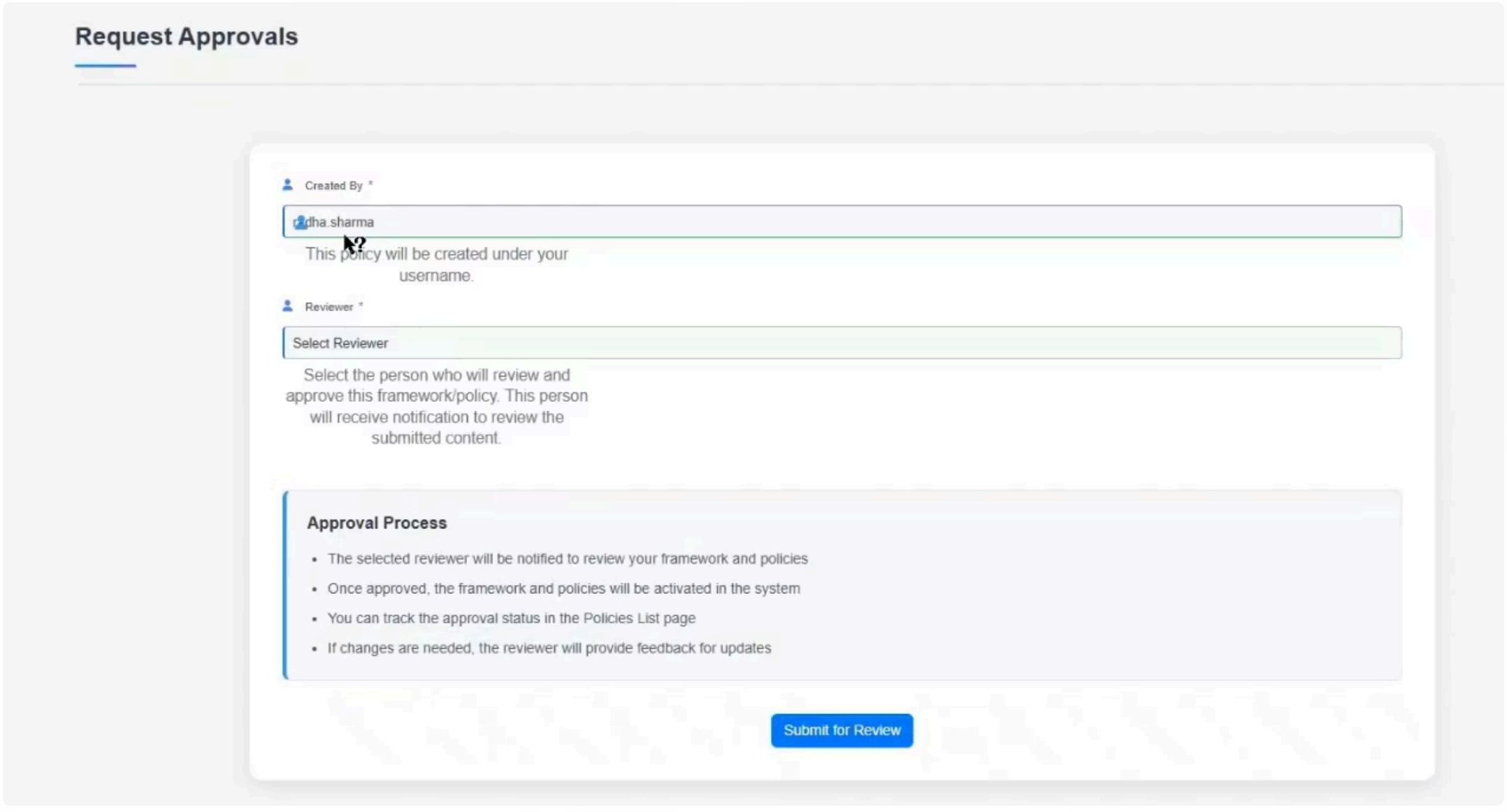
Once all required details are entered in both the Policy and Sub-Policy sections, click the "Submit" button to proceed to the Approvals page.



Policy Approval Process

After creating a policy or framework, it must go through an approval process:

1. On the Approvals page, enter:
    - Created By - Your username
    - Receiver Name - The reviewer/approver who will validate the policy
2. The receiver will be notified about the pending approval
3. Once approved, the policy becomes active in the system
4. Track approval status from the Policy List page
5. If changes are required, the approver can add comments requesting modifications



Reviewer Approval Workflow

Approvers follow a structured workflow to review and approve policies:

Access Pending Approvals

Navigate to the appropriate Approval section and select "Reviewer Tasks" to view assigned items

Review Details

Click "View Details" to examine the policy or framework information in a pop-up window

Make Decision

Choose to Approve or Reject based on the review, or request modifications with feedback

Finalize

For frameworks, approve all associated policies and sub-policies, then click "Submit Review"

Tailoring and Templating

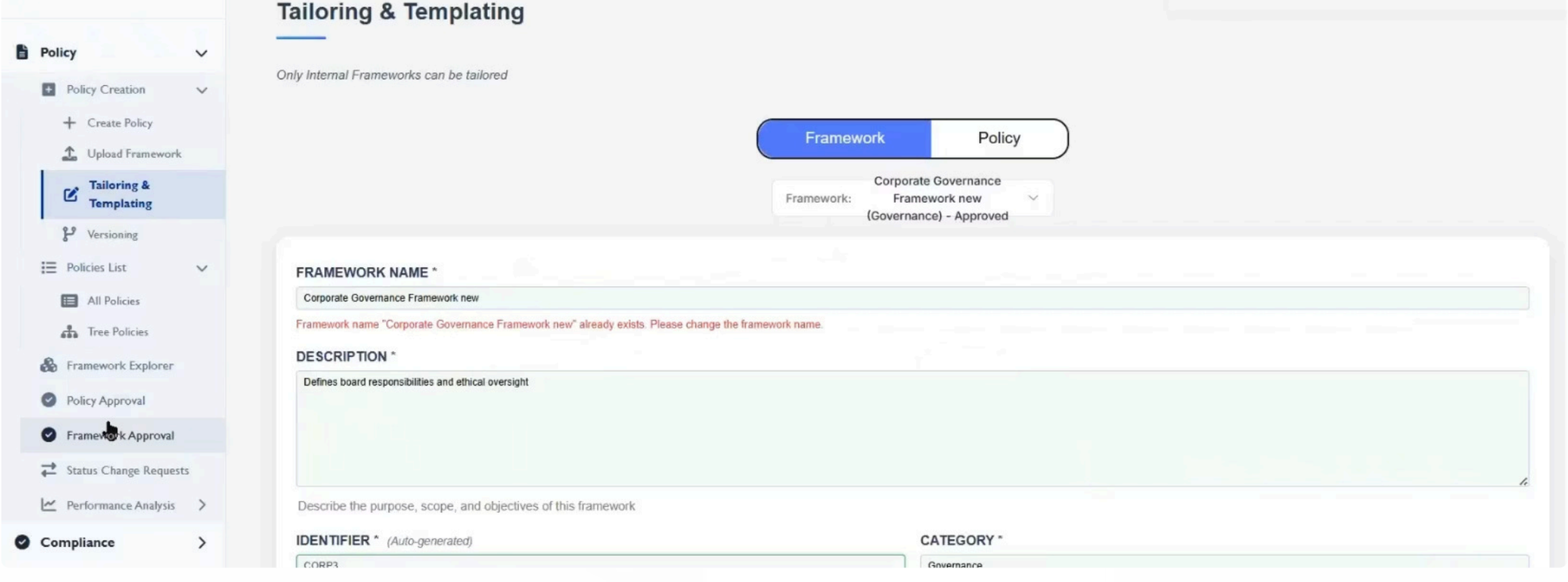
The Tailoring and Templating feature allows you to customize existing frameworks and policies to meet specific organizational needs:

Framework Tailoring

1. Navigate to Policy Creation > Tailoring and Templating
2. Select an internal framework to view its details
3. Modify the framework details as required
4. Submit for approval

Policy Tailoring

1. Navigate to the Policy tab at the top of the page
2. First select the framework
3. Then select the policy to tailor
4. Make necessary modifications
5. Submit for approval



Versioning Policies and Frameworks

The Versioning feature allows you to create new versions of existing frameworks or policies while maintaining a history of changes:

Select Item

Navigate to the desired framework or policy that needs updating

Modify

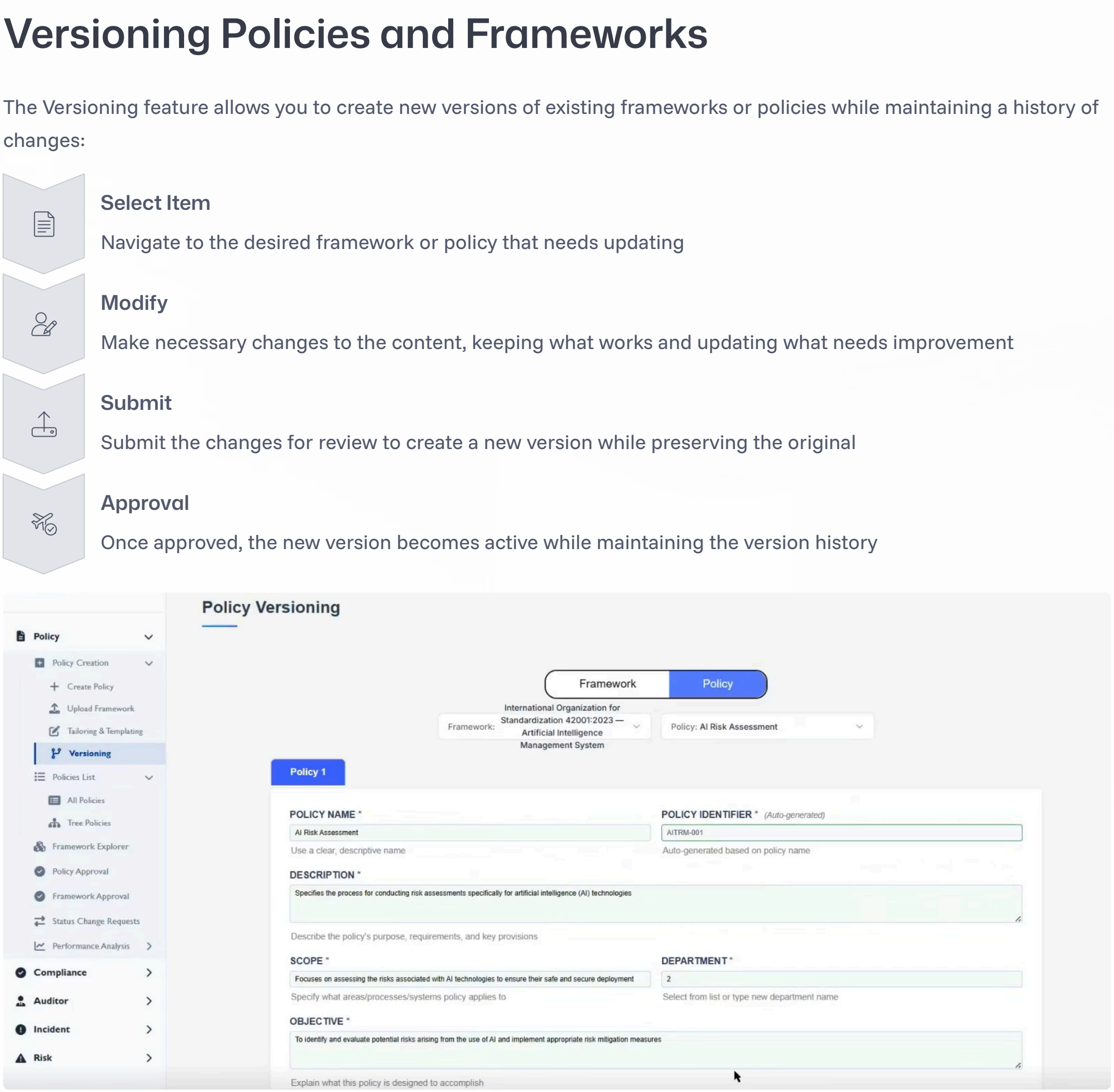
Make necessary changes to the content, keeping what works and updating what needs improvement

Submit

Submit the changes for review to create a new version while preserving the original

Approval

Once approved, the new version becomes active while maintaining the version history

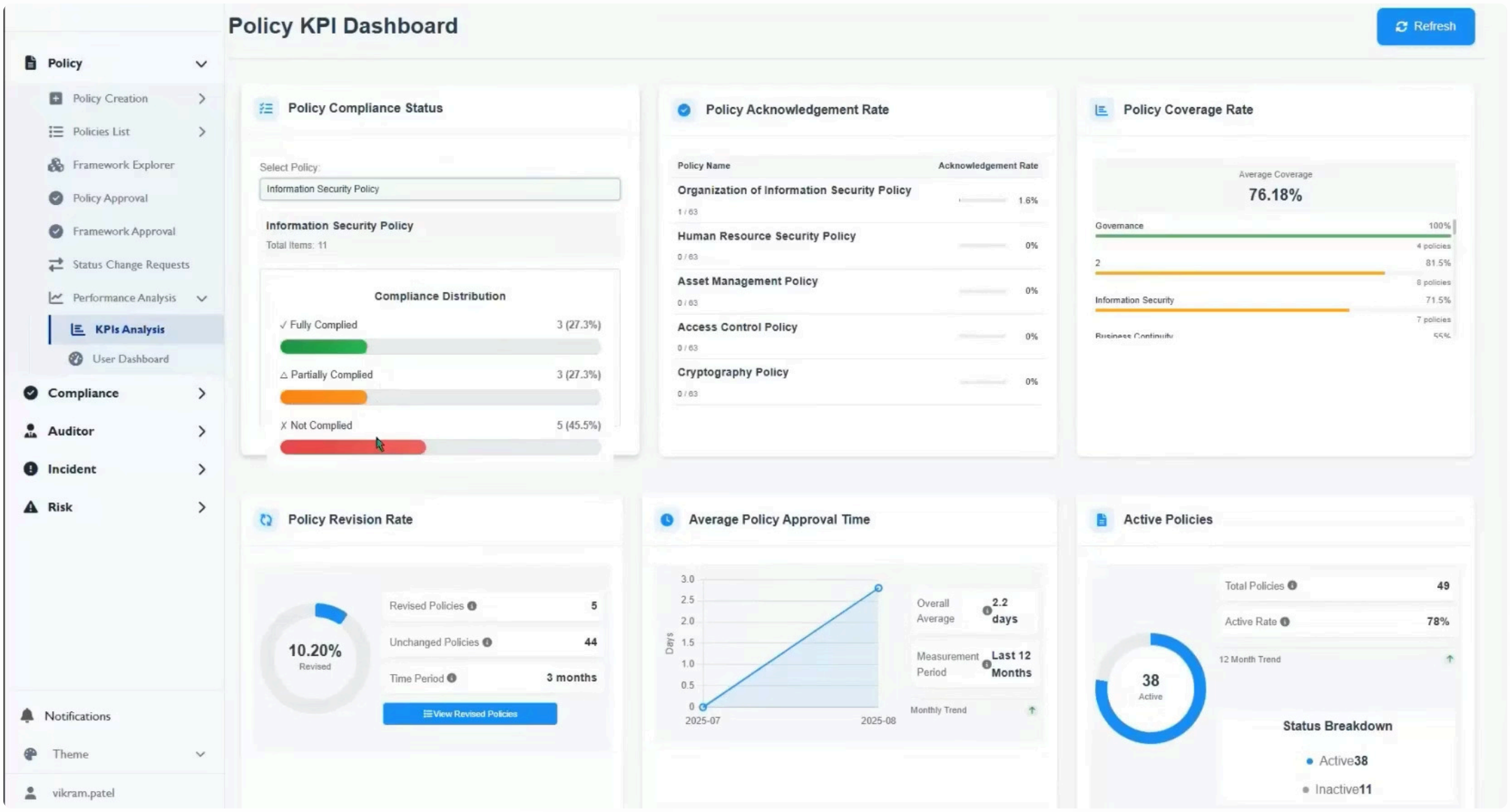


Uploading Frameworks

The Upload Framework feature uses AI to automatically extract policies, sub-policies, controls, and compliance requirements from uploaded documents:

1. Navigate to Policy & Framework Management > Framework Explorer
2. Click "Upload Document" and select the PDF or policy file
3. The system's AI will automatically:
    - Parse the framework document
    - Extract Policies, Sub-Policies, and Controls
    - Map them to Compliance requirements
4. Review the extracted content in the Framework Content Reviewer pop-up
5. Select all content or choose individual items
6. Edit, add, or delete extracted elements as required
7. Click "Save Selection" and then "View Extracted Policies"
8. After confirming the content, click "Save All Details"

KPI Analysis Dashboard



The KPI Analysis Dashboard provides comprehensive metrics to track policy performance:

Policy Compliance Status

View compliance distribution across Fully Complied, Partially Complied, and Not Complied categories

Acknowledgement Rate

Track the percentage of users who have acknowledged each policy

Coverage Rate

Monitor policy coverage across domains with overall average percentage

Revision Rate

See the percentage of policies revised within a selected time period

Approval Time

Track the average days taken for policy approval with monthly trends

Active Policies

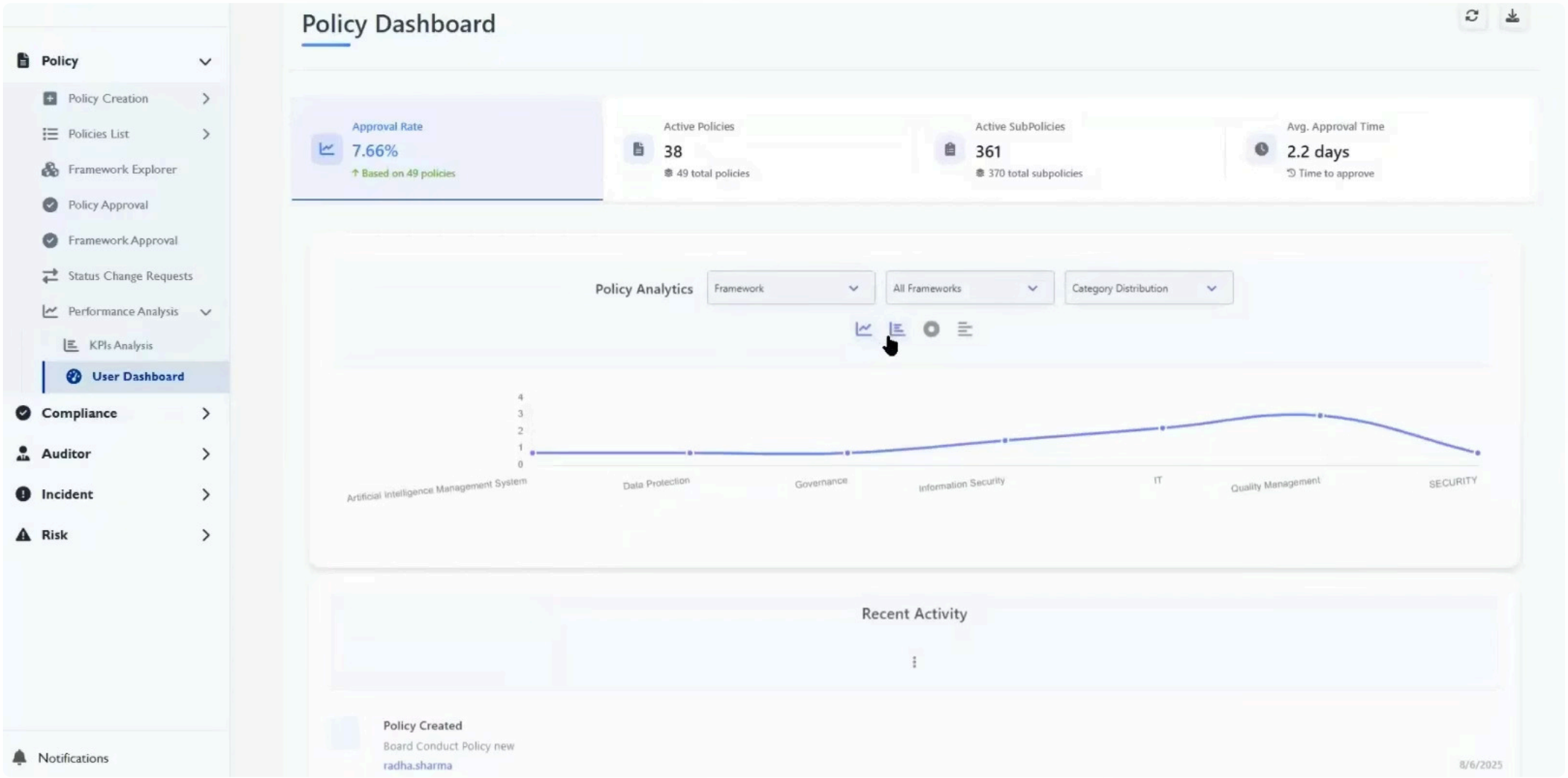
View the total number of policies and their active/inactive status

Use the Refresh button (top right) to update dashboard data in real-time.

User Dashboard

The User Dashboard provides a consolidated view of key policy and framework activities, enabling efficient tracking of progress and engagement:

- **Approval Rate** - Select Frameworks, Policies, or Sub-Policies from the dropdown to view approval statistics with additional filtering options
- **Active Policies & Sub-Policies** - Track the number of currently active items to monitor adoption and usage
- **Average Approval Time** - Monitor the average time taken for approvals to support process optimization
- **Recent Activities** - Quickly view newly created policies and frameworks to stay updated on system changes



Compliance Management System

The **Compliance Module** enables organizations to define, document, and monitor compliance requirements by linking them to frameworks, policies, and sub-policies. It streamlines compliance creation, approval, tailoring, and version control, ensuring that regulatory obligations are accurately captured and maintained. With features such as control management, audit tracking, and compliance dashboards, the module provides visibility into compliance maturity, non-compliance patterns, and mitigation effectiveness. Integrated KPIs and analytics allow organizations to measure approval rates, identify high-risk areas, and track reputational and operational impacts, fostering proactive compliance management across the enterprise

Role-Specific Permissions

Role	View	Create	Edit	Approve	Delete
Compliance Officer	✅	✅	✅	✅	❌
GRC Manager	✅	✅	✅	✅	❌

Create Compliance

The Compliance Creation module allows users to define and document compliance requirements by linking them with frameworks, policies, and sub-policies, and capturing associated risks, classifications, and approvals.

Navigation & Framework Selection

Click on the Compliance module → Compliance Creation → Create Compliance. Then select the relevant Framework, Policy, and Sub-policy.

Enter Compliance Details

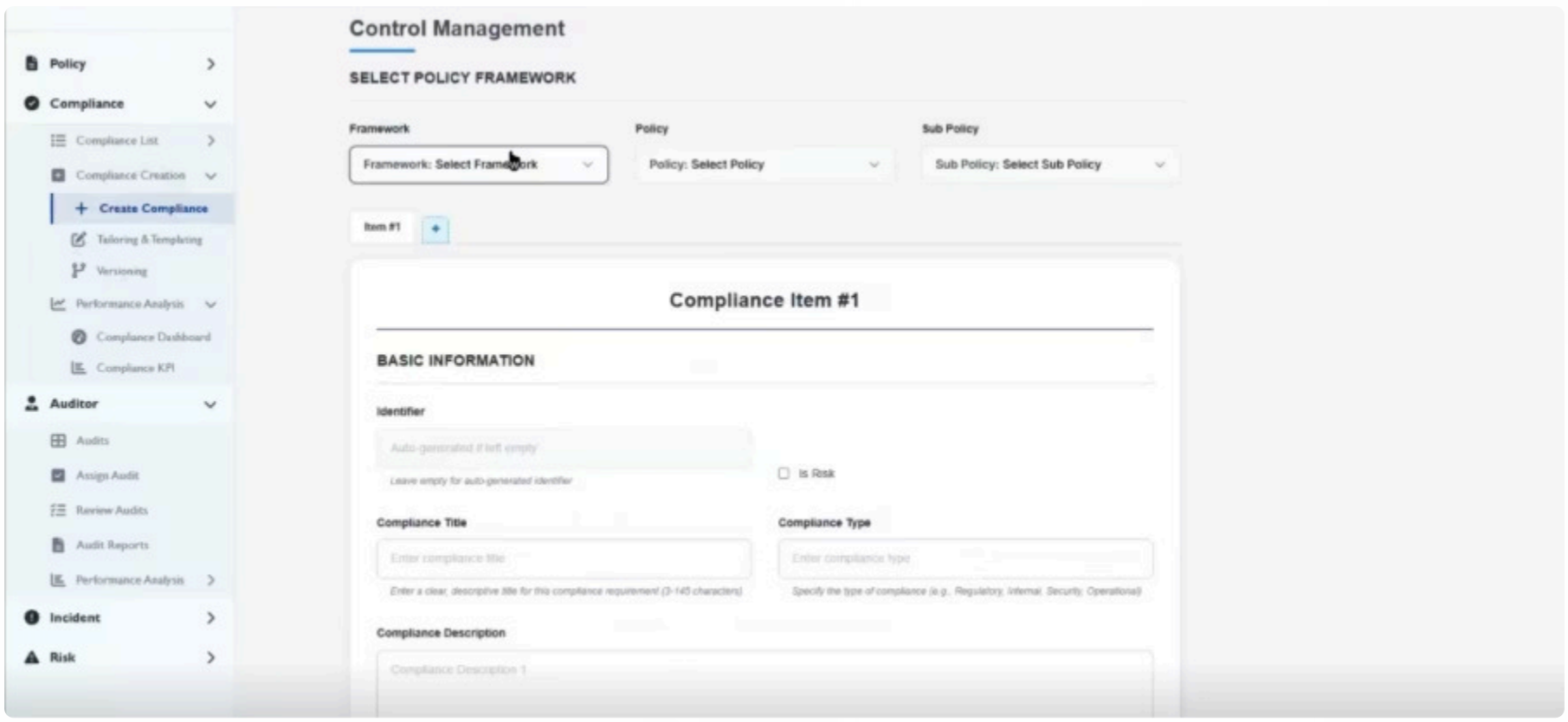
Add Identifier, Risk Flag, Compliance Title, Type, Description, Scope, Objective, and Business Units Covered.

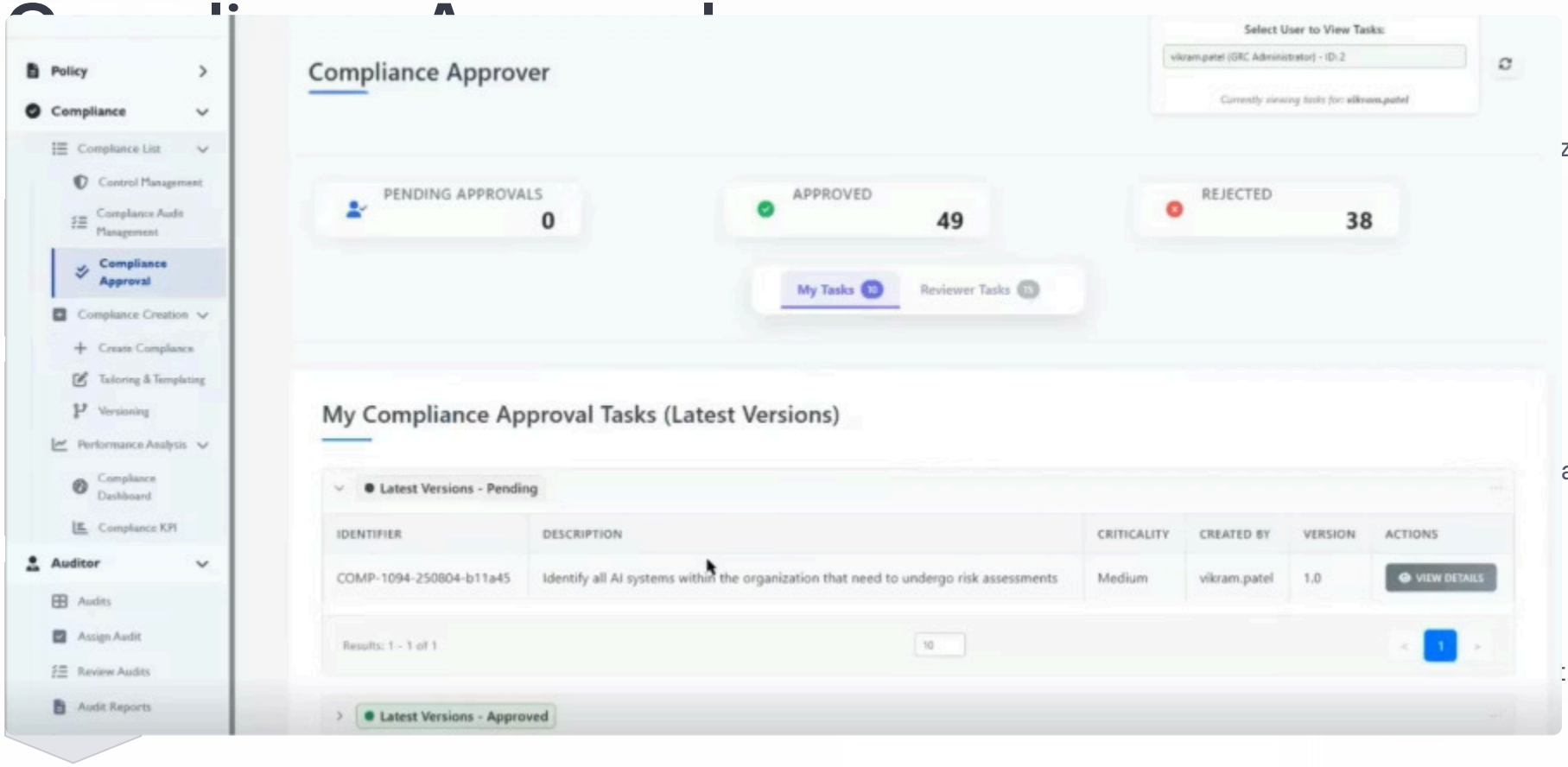
Risk & Classification

Document Possible Impact, Mitigation Steps, Risk Scenarios, Type, Category, Business Impact, Criticality, Mandatory status, Manual/Automatic, Applicability, and Severity/Probability Ratings.

Approval & Submission

Assign a Reviewer for approval. To add multiple compliances, click the plus icon. Once complete, click Submit Compliance to send for approval.





zed.

ance record and review

: incorporate changes

Compliance Tailoring and Templating

Users can manage existing compliances by either editing them to create a new version or copying them to reuse under a different framework, policy, or sub-policy.

Navigation

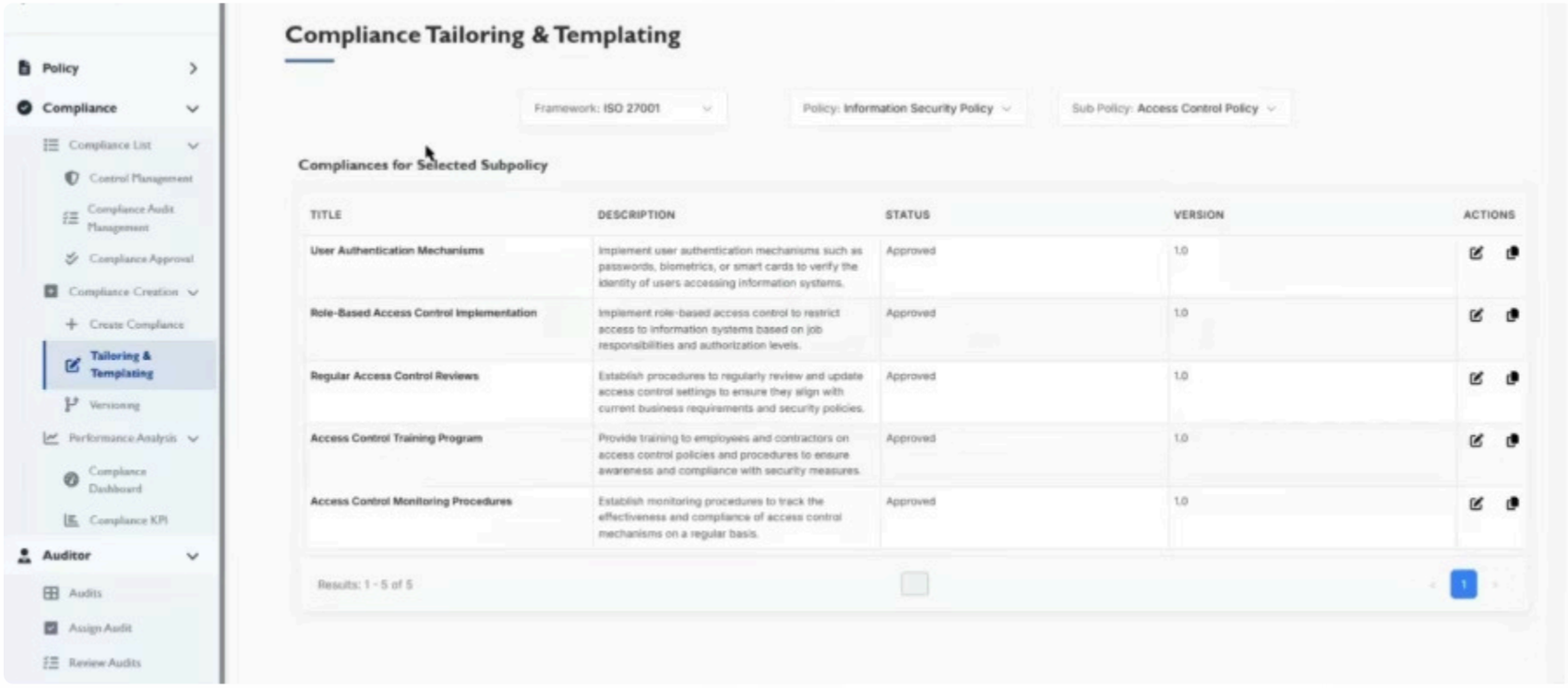
1. Go to this section from Compliance Creation section on left nav
2. Select the Framework, Policy, and Sub-policy
3. The compliances under the selected sub-policy will be displayed

Edit Compliance

1. Click Edit to open compliance details
2. Make necessary changes and click Submit
3. The compliance goes through the approval process, creating a new version

Copy Compliance

1. Click Copy to duplicate the compliance
2. Assign it to a different framework, policy, or sub-policy as required
3. Users can edit the details and click on save to run it through approval process



Compliance Versioning

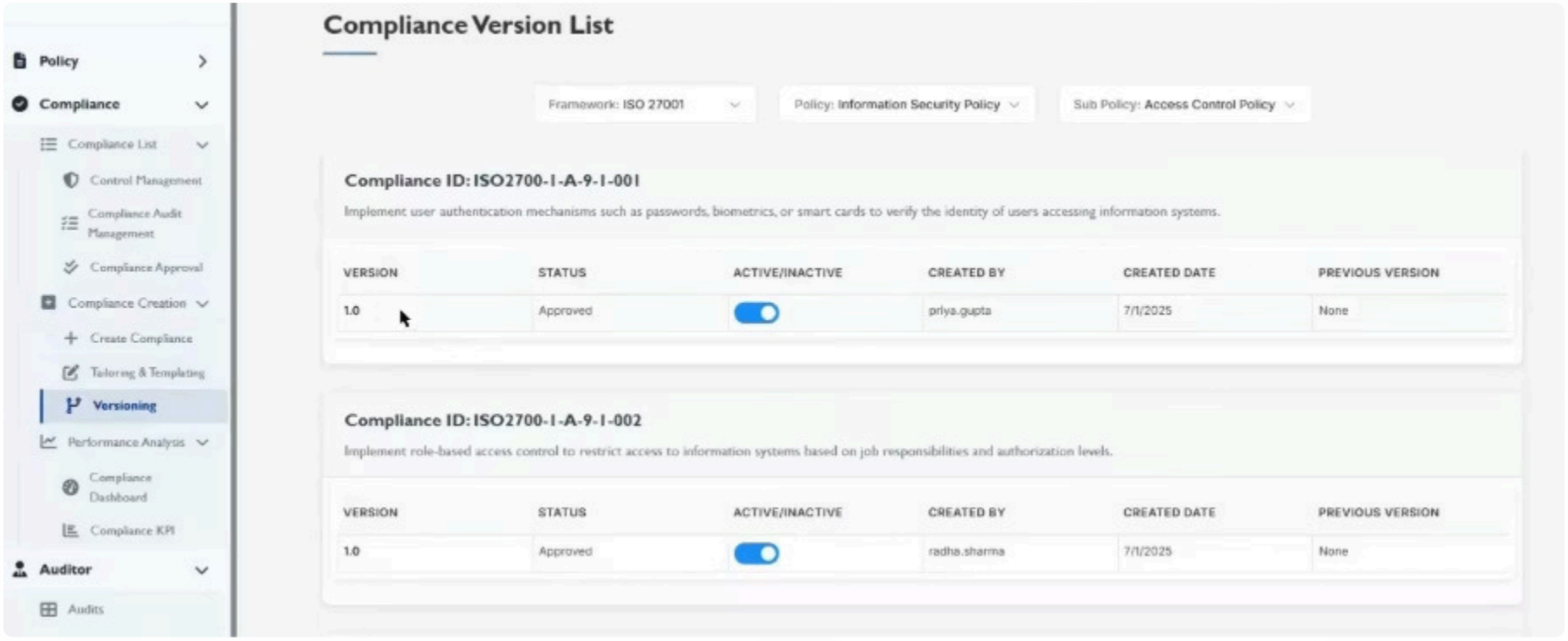
Users can manage multiple versions of a compliance and control which version remains active.

Navigation

Select the Framework, Policy, and Sub-policy to view the list of associated compliances. Each compliance will display its available versions.

Version Control

By default, the latest version of a compliance is set as Active. Users can switch between versions by using the Activate/Deactivate toggle to enable an older version or disable the current one.



Control Management

This page provides a comprehensive list of compliances associated with the selected Framework → Policy → Sub-policy. Users can easily navigate from frameworks down to specific compliances.

Framework Selection

On landing, users see a list of all available Frameworks. Select the desired framework to proceed.

Policy Selection

On the next page, select the relevant Policy.

Sub-policy Selection

On the following page, choose the Sub-policy to view.

Compliance List

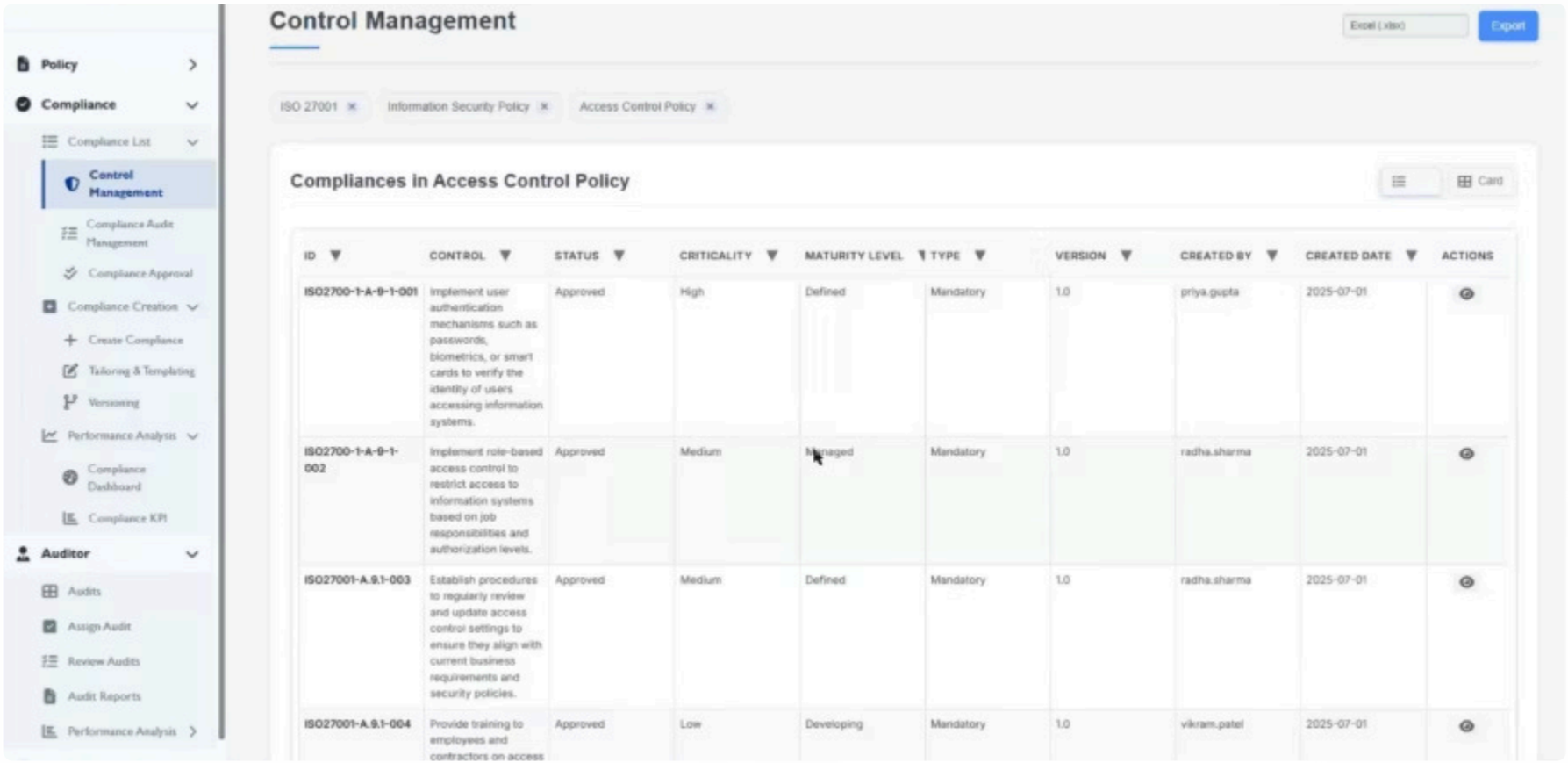
The system displays all Compliances associated with the selected sub-policy.

Compliance List Details

Each compliance entry is displayed with the following details: Compliance ID, Status, Criticality, Maturity Level, Type, Version, Created By, Created Date. To view more detailed information about a compliance, users can click the Eye icon at the end of the respective row.

Users can view all compliances under a particular framework or policy by clicking the corresponding button in the Action column.

The page also provides an Export option (top right). Clicking on it allows users to export compliance data and choose the desired file format before downloading.



Compliance Audit Management

In this section, users can not only view all compliances but also monitor their audit status, categorized as:

Fully Compliant

Compliances that meet all requirements

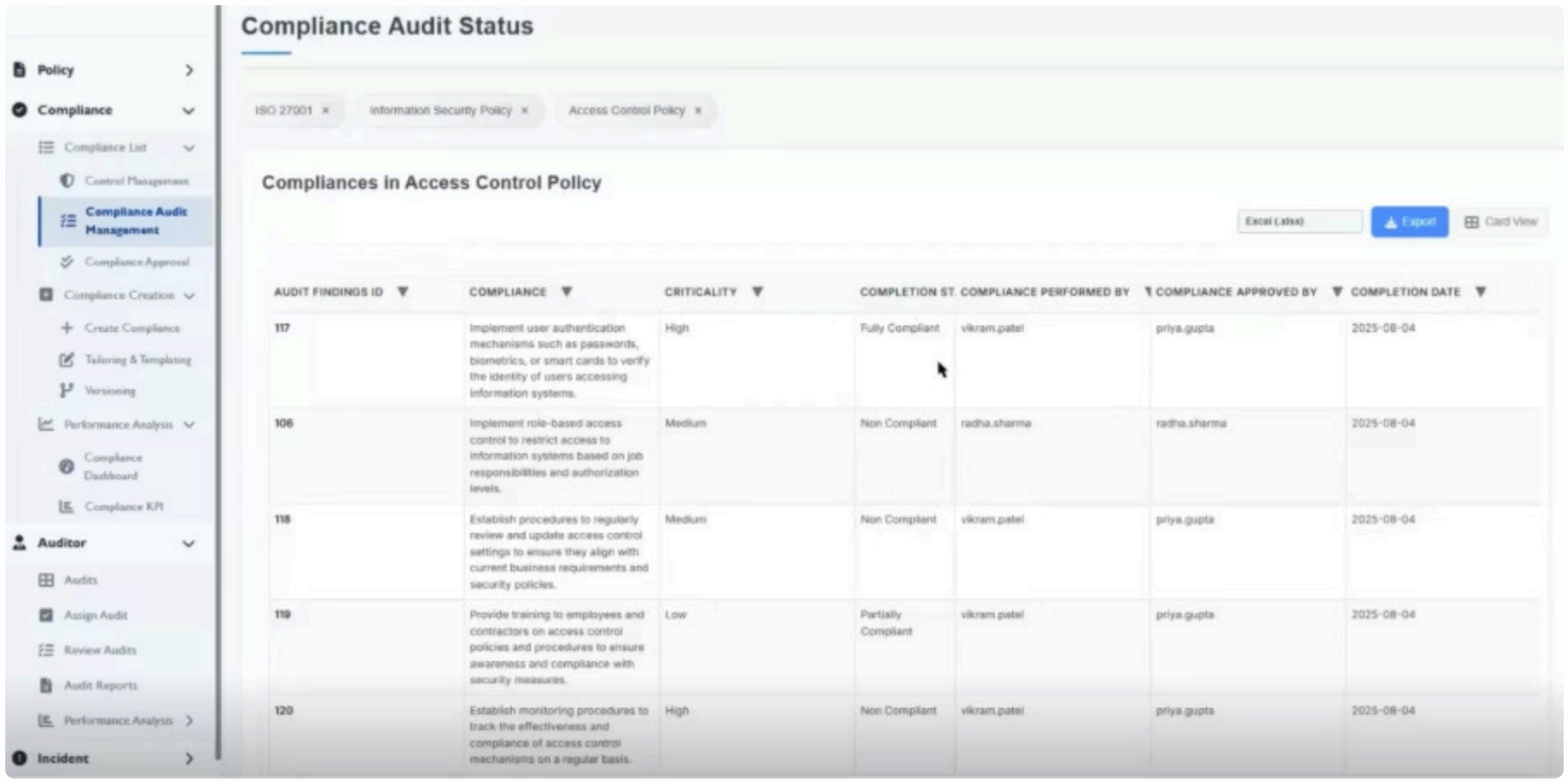
Partially Compliant

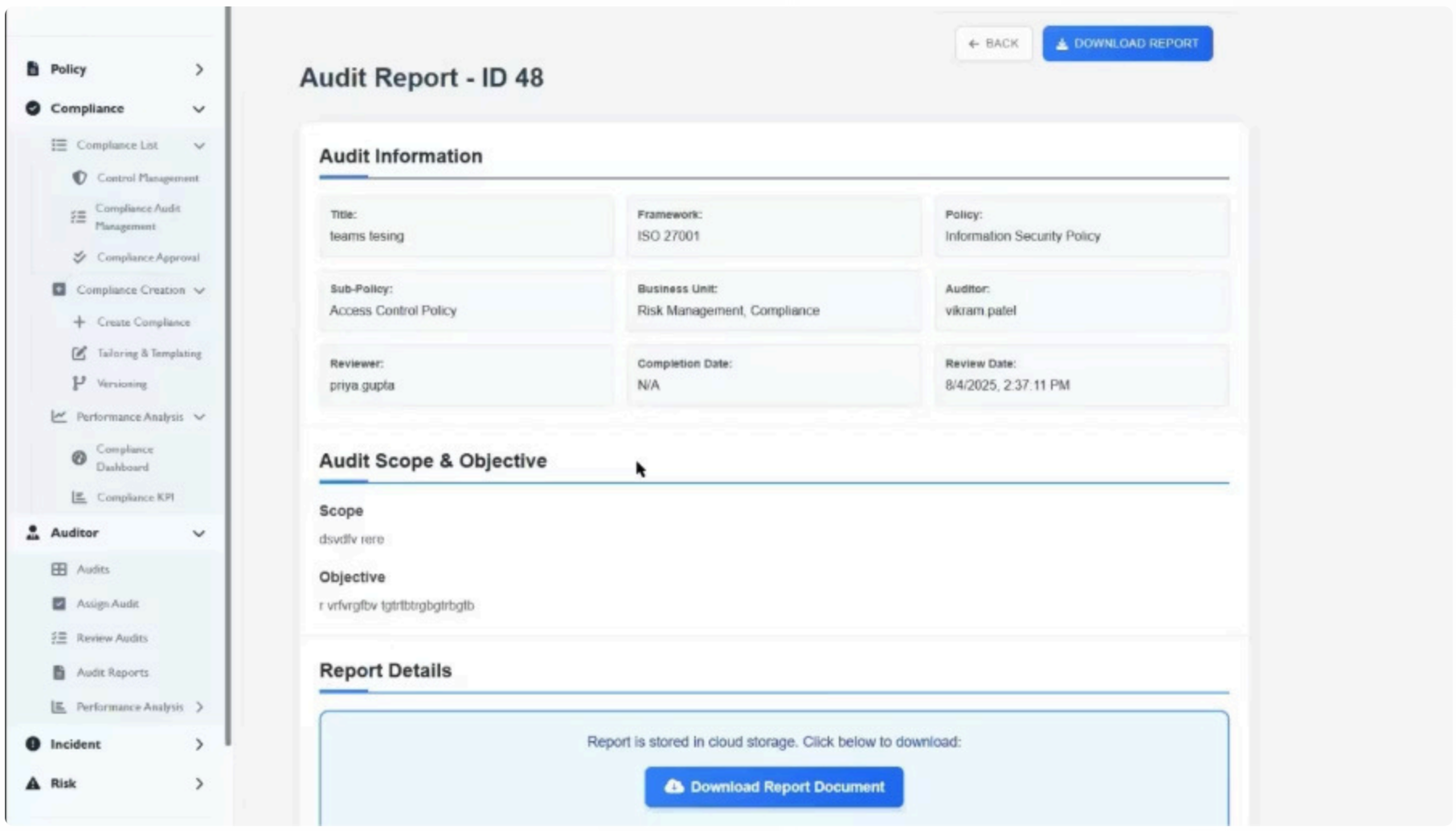
Compliances that meet some but not all requirements

Non-Compliant

Compliances that fail to meet requirements

The audit status can be viewed at the framework, policy, and sub-policy levels, giving users a clear overview of compliance performance across different layers. Users can download the report for a specific compliance by clicking on the corresponding Audit ID in the list. This action opens the detailed Report Page, where all compliance-related audit information is displayed. At the bottom of this page, users can click on the Download Report button to export the report for reference or record-keeping.





Compliance Dashboard

This section provides an interactive dashboard to analyze and track compliance performance.

Key Metrics

At the top of the page, users can view key metrics including:

- Approval Rate
- Active Compliances
- Total Findings
- Compliances Under Review

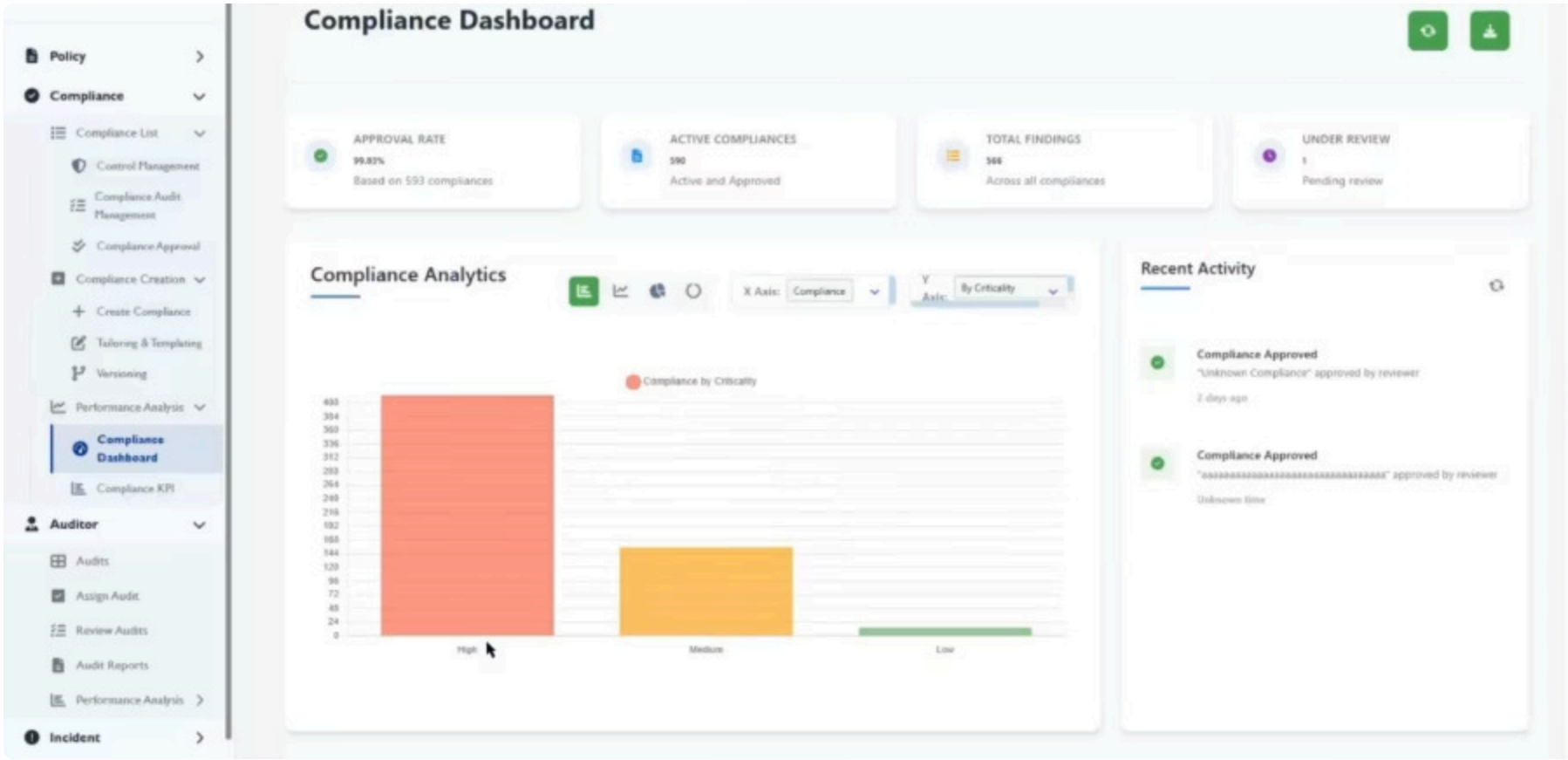
Interactive Graph

An interactive graph allows users to customize the view by selecting parameters for the X and Y axes:

- X-axis options include Compliances
- Y-axis can show Criticality, Status (Approval Status), or Mandatory Status

For example, selecting Compliances on the X-axis and Criticality on the Y-axis displays compliances grouped by their criticality levels.

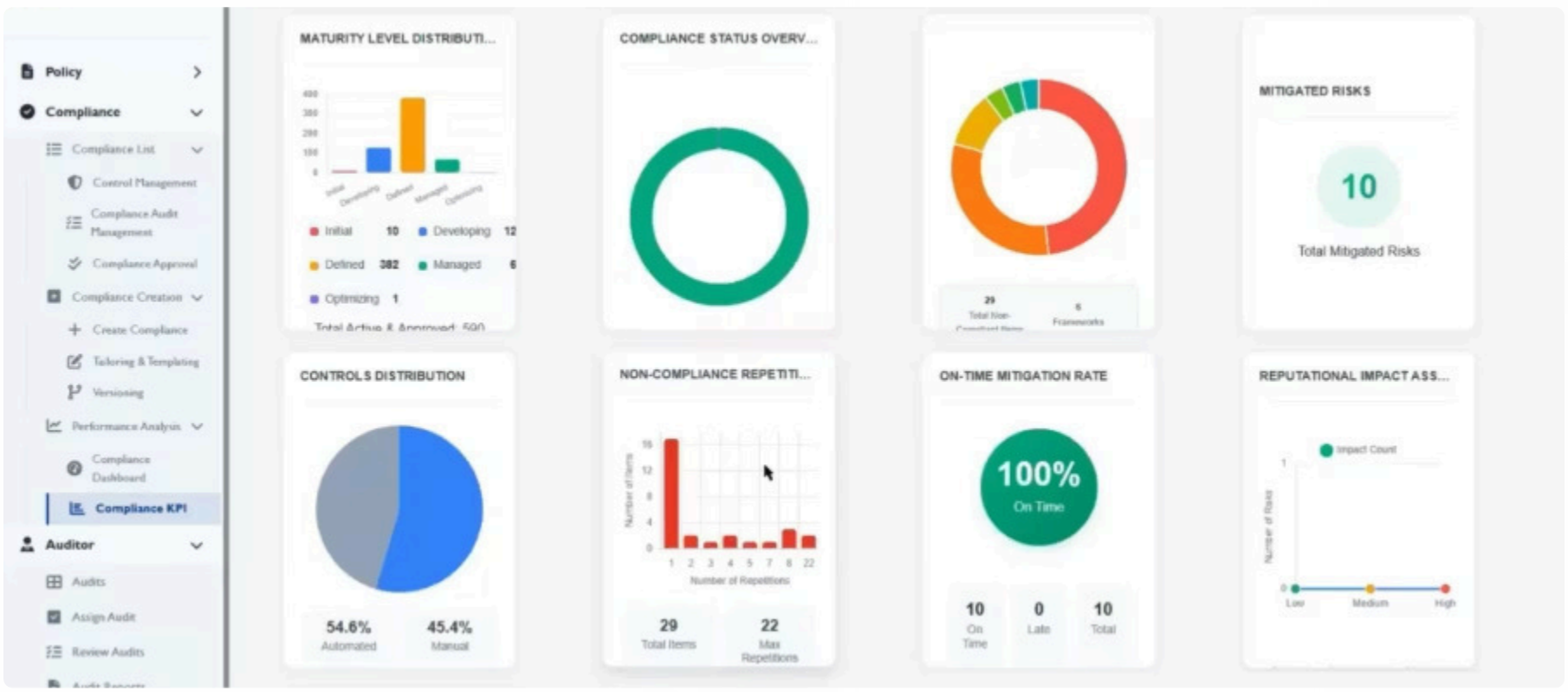
On the right side of the dashboard, users can see a feed of Recent Activities for quick updates on compliance changes.



Compliance KPI

The Compliance KPI page provides a consolidated view of compliance performance metrics, helping users track maturity, distribution, non-compliance patterns, risk mitigation, and reputational impact.

1	**Maturity & Status** • Maturity Level Distribution across stages: Initial, Developing, Defined, Managed, Optimizing • Compliance Status Overview showing approval status • Controls Distribution showing Automated vs. Manual proportions
2	**Non-Compliance Analysis** • Non-Compliance Summary across frameworks • Non-Compliance Repetition Analysis showing total items and max repetitions • Non-compliant incidents in the last x days (selectable from dropdown)
3	**Risk & Impact** • Mitigated Risks total count • On-Time Mitigation Rate showing on-time, late, and total items • Reputational Impact Assessment categorized by Low, Medium, High impact • Remediation cost analysis showing average and total cost



Auditor Module: Comprehensive Audit Management

The Auditor Module enables internal and external auditors to plan, execute, and track audits across organizational frameworks and policies. It provides structured workflows for scheduling audits, uploading evidence, recording findings, and linking results to incidents or risks. With AI-assisted documentation and compliance mapping, the module streamlines audit activities while ensuring accuracy, transparency, and accountability.

This section provides access to Audit, Assign Audit, Review Audit, Audit Reports, and Performance Analysis.

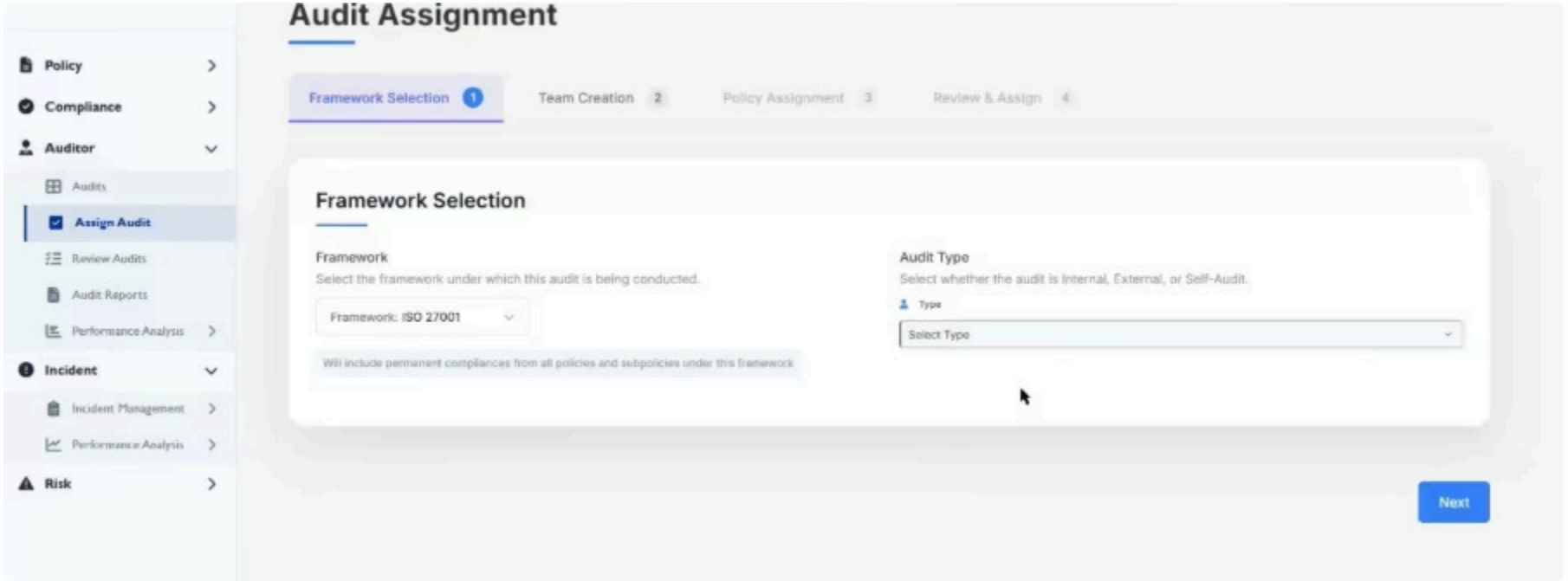
Role-Specific Permissions

Role	View	Create	Edit	Approve	Delete
Auditor	✅	✅	✅	✅	❌
GRC Manager	✅	✅	✅	✅	❌

Assign Audits: Step 1 - Framework Selection

The audit assignment process begins with selecting the appropriate framework and audit type. This initial step establishes the foundation for the entire audit process.

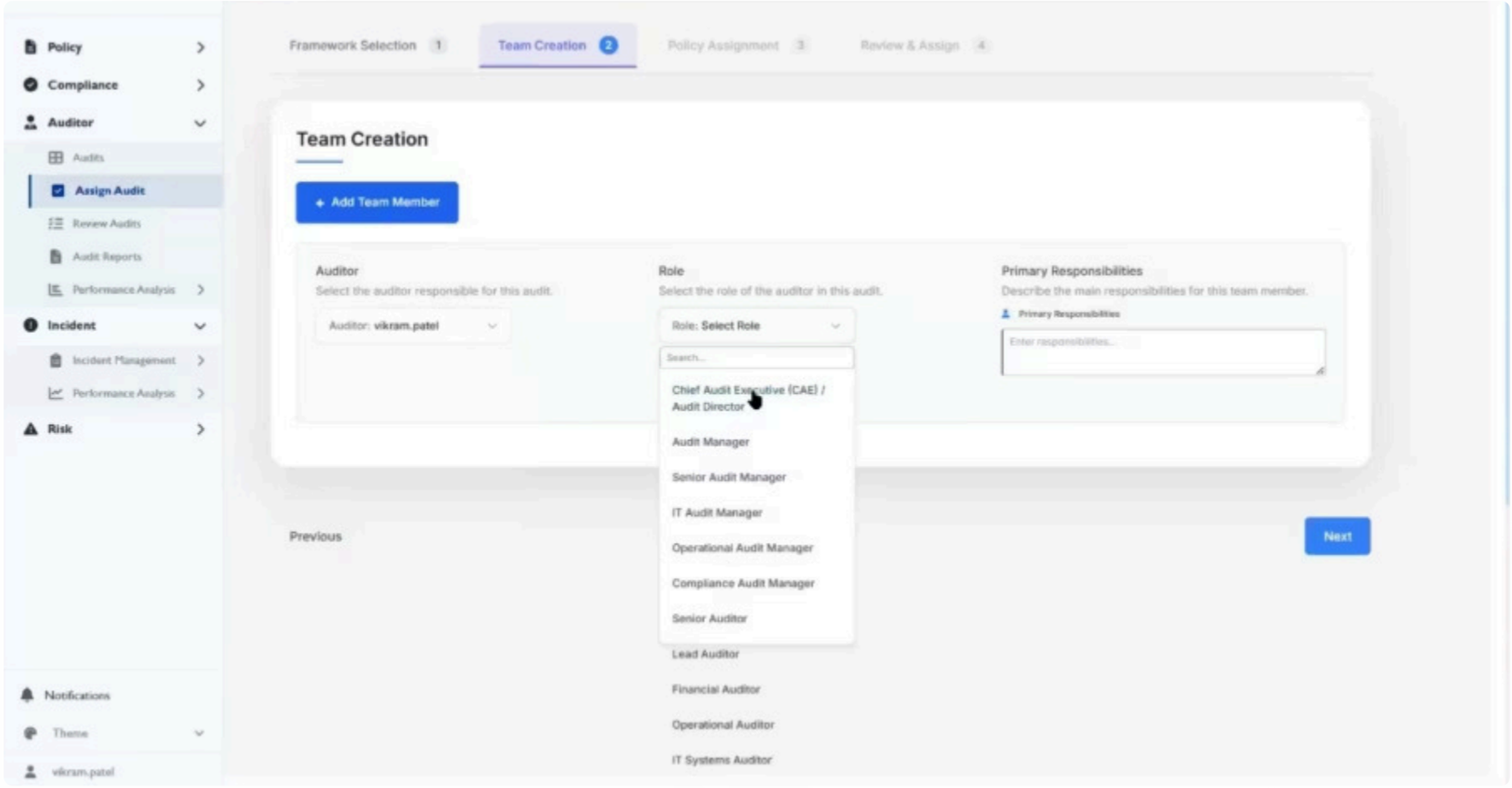
On the first page, the user selects the framework and the type of audit (Internal, External, or Self Audit).



Assign Audits: Step 2 - Team Creation

Building the right audit team is crucial for effective auditing. The system allows for detailed role assignment and responsibility allocation.

On the next page, the user creates the audit team by selecting the reviewer (from a dropdown list with roles such as Audit Director, Chief Audit Executive, Senior Auditor, IT Audit Manager, etc.) and assigning primary responsibilities.



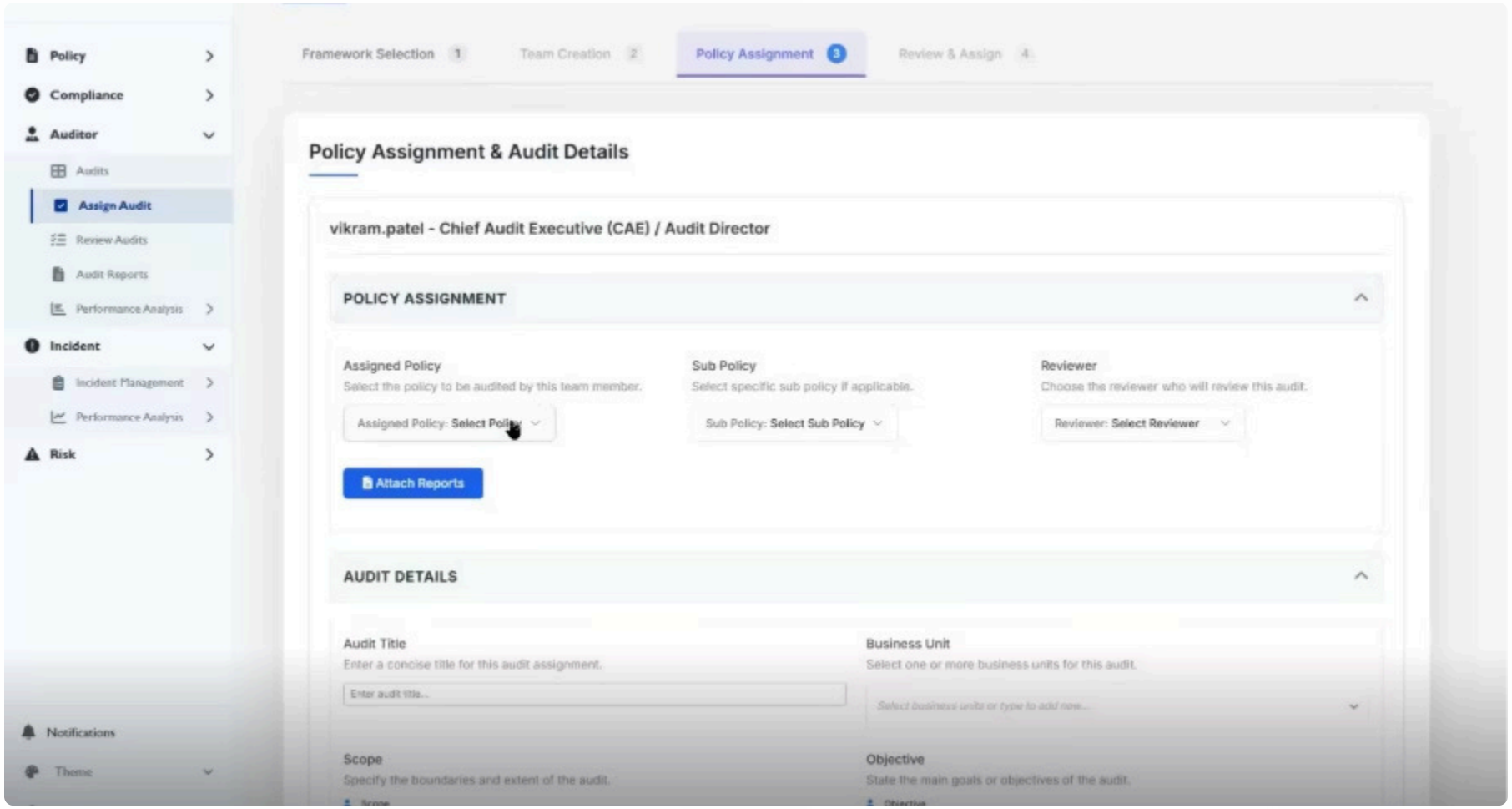
Assign Audits: Steps 3 & 4 - Policy Assignment and Audit Details

After entering the initial details, the user clicks Next to navigate to the Policy Assignment and Audit Details pages.

In the Policy Assignment section, the user selects the assigned policy (the policy to be audited), sub-policy, and reviewer. Users can also attach previous reports using the Attach Reports button.

In the Audit Details section, the user fills in information such as Audit Title, Business Unit, Scope (boundaries and extent of the audit), Objectives (main goals and purpose of the audit), Frequency (how often the audit should occur), and Due Date.

Finally, on the last page, the user reviews all the entered details and assigns the audit.

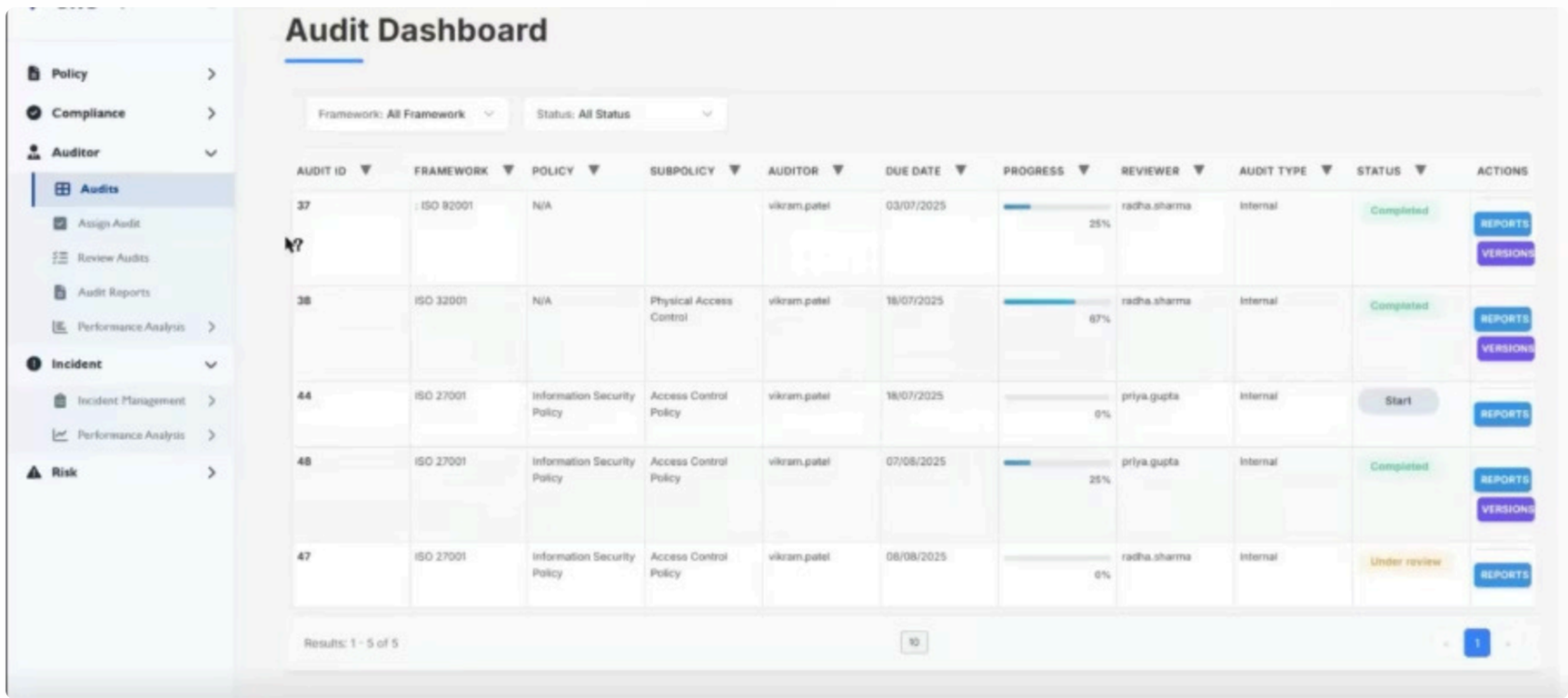


Audits: Dashboard Overview

The Audits section provides a comprehensive view of all audits in the system, allowing for efficient tracking and management.

This section displays all created audits along with their details such as framework, policy, sub-policy, auditor name, due date, progress (in percentage), reviewer, audit type (internal, external, or self-audit), and status. Users can also download the reports of a particular audit and view its versions.

To begin an audit, the user clicks on the Start button in the Status column. Once initiated, the status changes to Work in Progress and the user is redirected to the Audit Details page.



Audits: Audit Details Page

The Audit Details page provides a focused view of the specific audit being conducted, showing all relevant contextual information.

This page displays the audit title, scope, objectives, business units, and associated framework, policy, and sub-policy.

Below this section, users can view the compliance items along with their details.

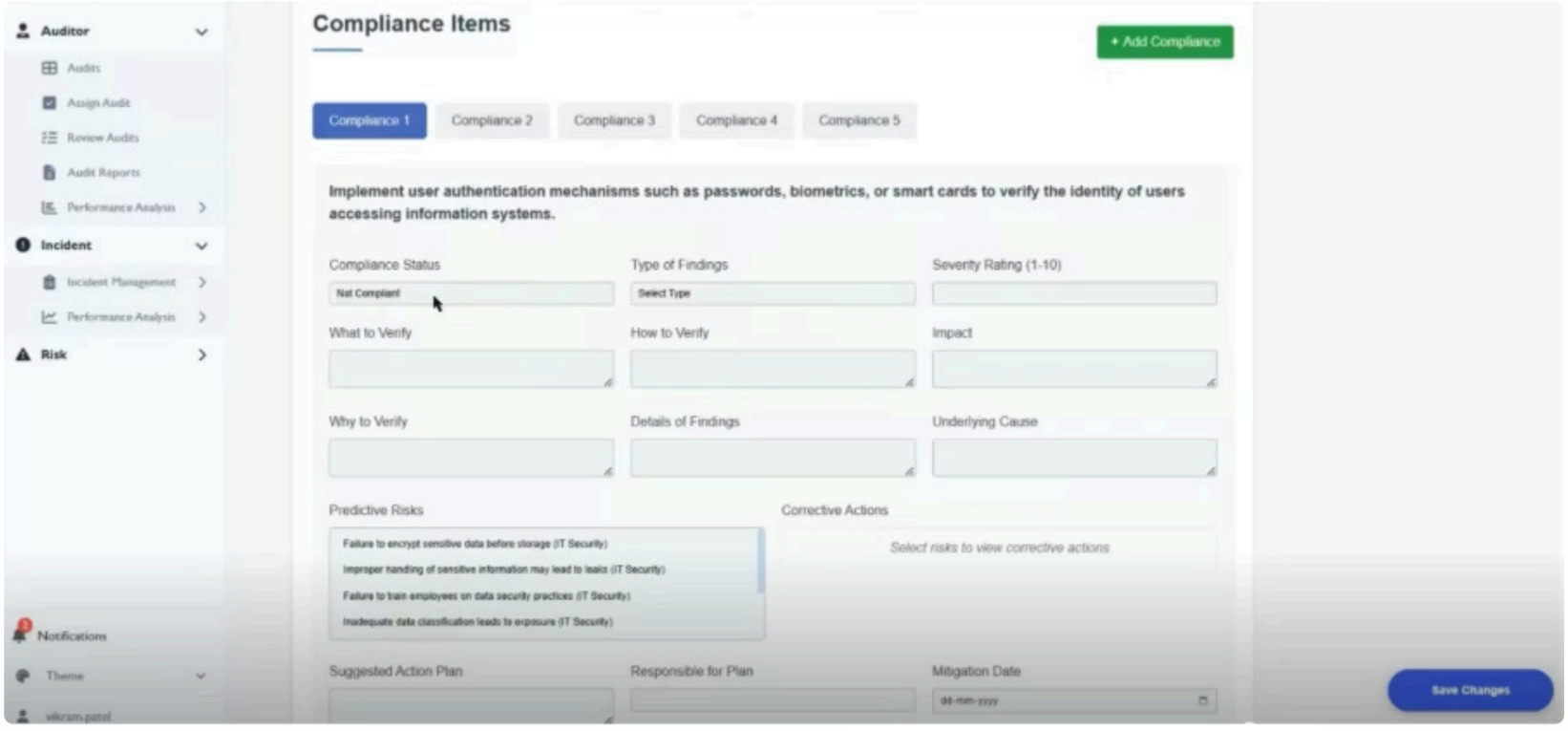
Audits: Compliance Assessment

The compliance assessment section is where the actual audit work happens, with detailed documentation of findings and recommendations.

In this section, users fill in details such as compliance status (fully, partially, or non-compliant), type of findings (minor, major), severity rating (1–10), what to verify, how to verify, impact, why to verify, details of findings, underlying cause, predictive risks, corrective actions, suggested action plan, responsible owner, mitigation date, re-audit requirement, comments, review status, review comments, overall audit comments, and overall review comments.

When a predictive risk is selected, a corrective action is automatically assigned.

Below this, users can also add compliance evidence and audit evidence. Once all details are filled, clicking on the Save Changes button sends the record to the reviewer, and the audit status changes to 'Under Review' on the audit dashboard.



Review Audits: Overview

The Review Audits section enables reviewers to efficiently manage and evaluate completed audits.

This module provides an overview of assigned audits, their progress, review status, and downloadable reports.

The table displays the following fields:

ID: Unique identifier assigned to each audit.

Framework: The compliance framework under which the audit is being conducted (e.g., ISO 27001, ISO 92001, AI Risk Assessment Standard).

Policy: The policy under review (e.g., Information Security Policy).

Subpolicy: Specific subpolicy being audited (e.g., Access Control Policy).

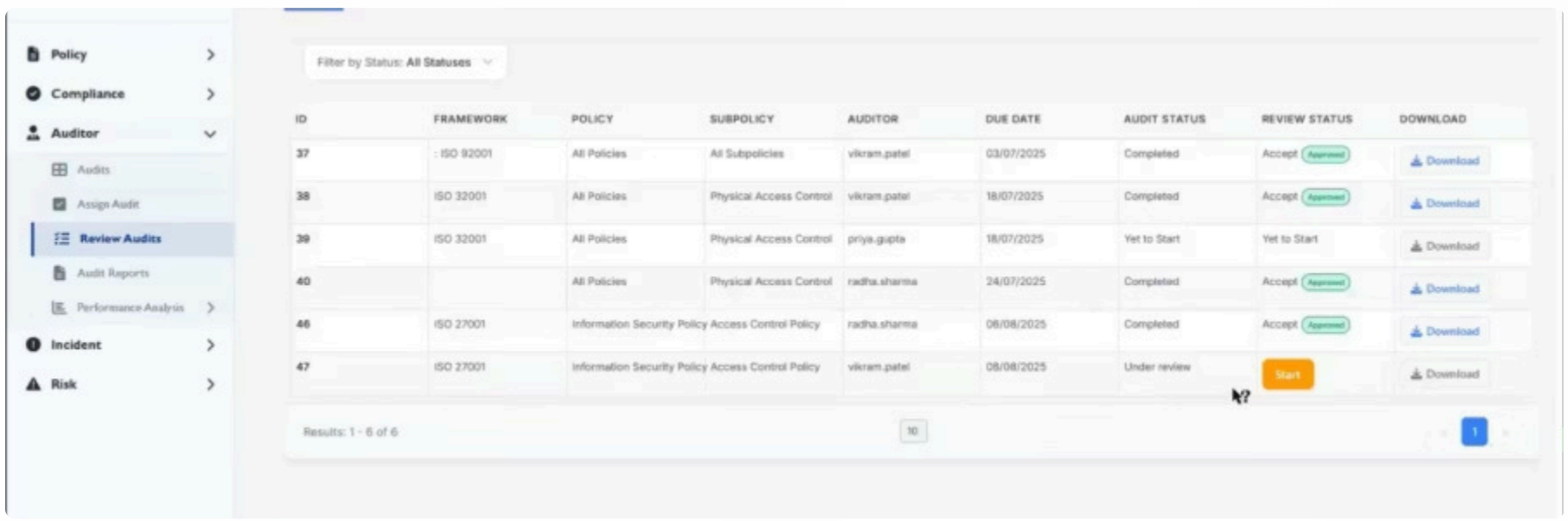
Auditor: Name of the auditor responsible for conducting the audit.

Due Date: Deadline for completing the audit.

Audit Status: Indicates progress — Yet to Start, Work in Progress, Completed.

Review Status: Status of the audit review.

Download: Allows you to download the completed or ongoing audit report in PDF/Excel format.



Review Audits: Review Process

The review process is a critical quality control step that ensures audit findings are accurate and recommendations are appropriate.

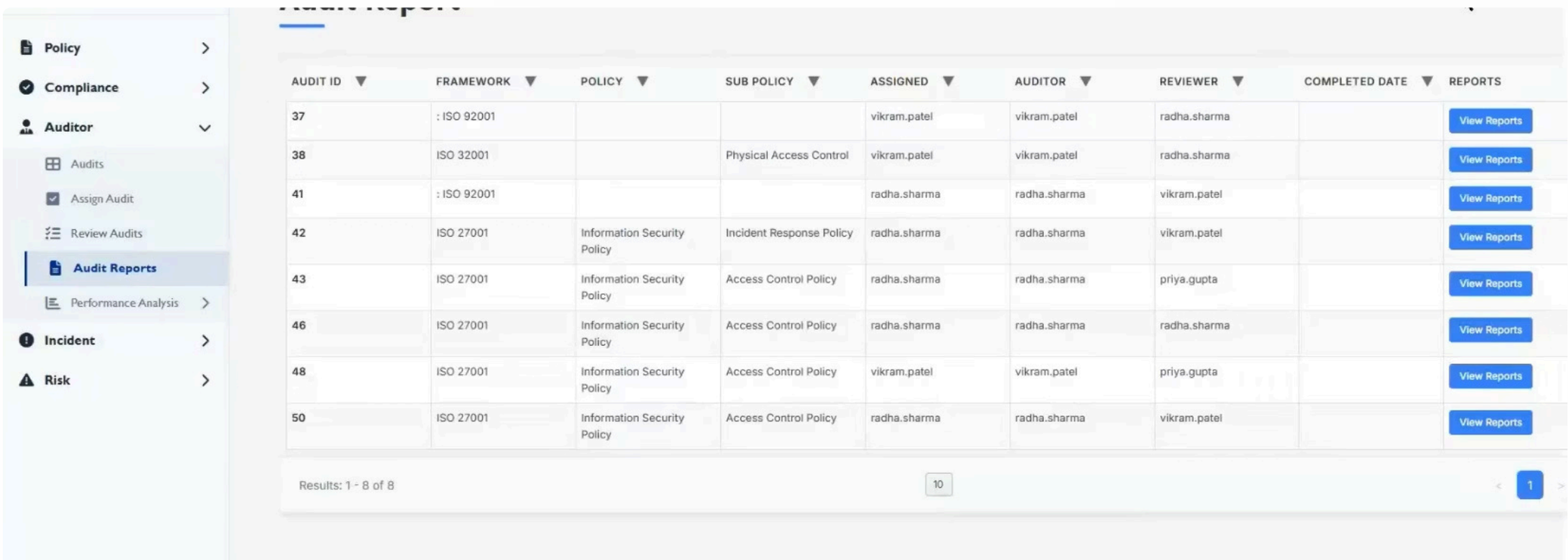
In the Review Status column, the audit reviewer gets an option to start the audits for the ones that are not started yet.

In the audit review page, the reviewer can add the status of the review and then add comments and click save review to complete the review process.

Audit Report: Consolidated View

The Audit Report section provides a comprehensive overview of all audit activities, enabling efficient tracking and reporting.

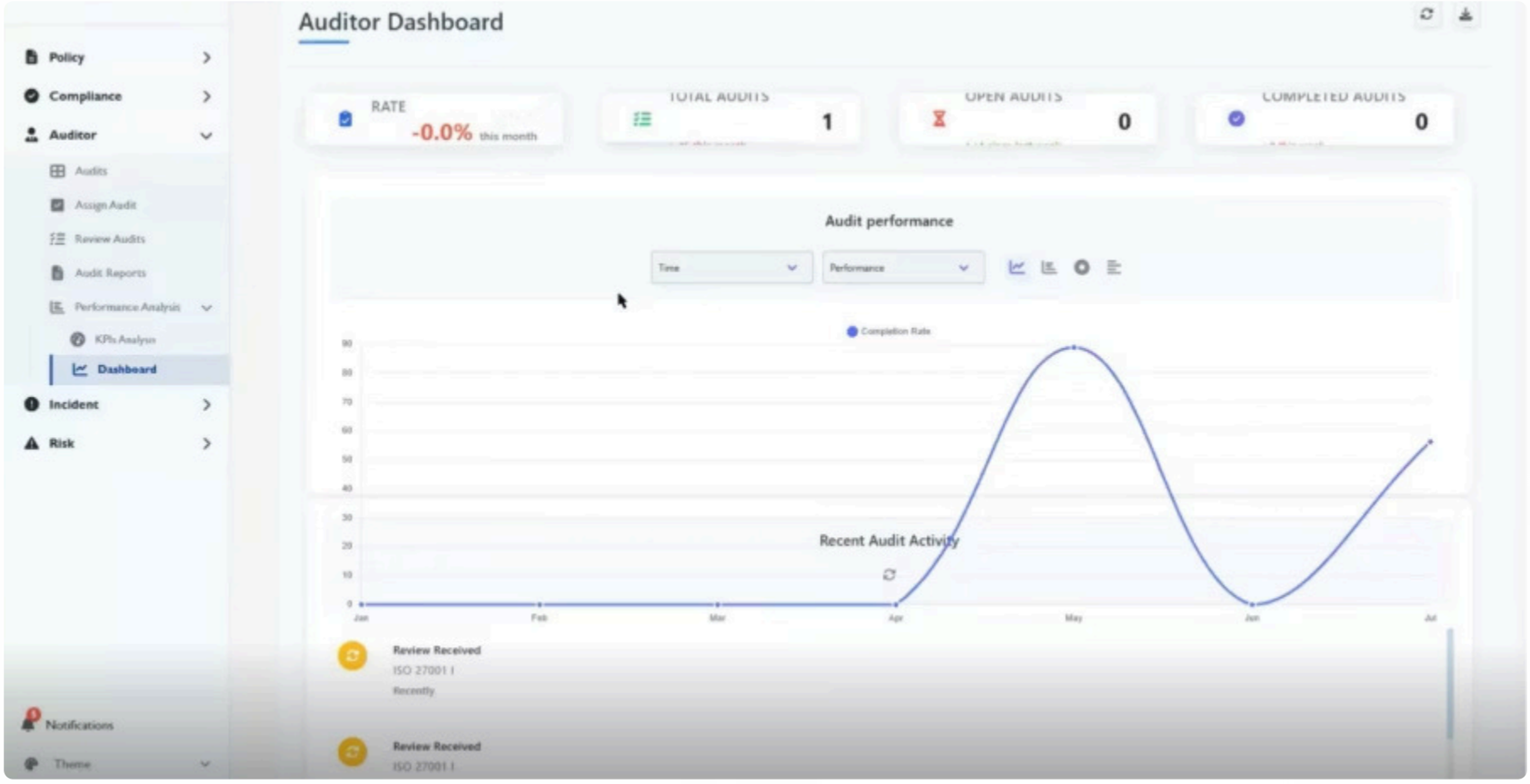
The Audit Report page provides a consolidated view of all completed and ongoing audits within the system, helping auditors, reviewers, and managers quickly track audit status, responsibilities, and access detailed reports. Each entry displays key details such as the Audit ID, framework, policy, sub-policy, assigned user, auditor, reviewer, completed date, and available reports. Users can also sort and filter audits, as well as view detailed audit versions through the report actions.



Performance Analysis: Dashboard

The Performance Analysis Dashboard provides at-a-glance insights into audit performance metrics, enabling data-driven decision making.

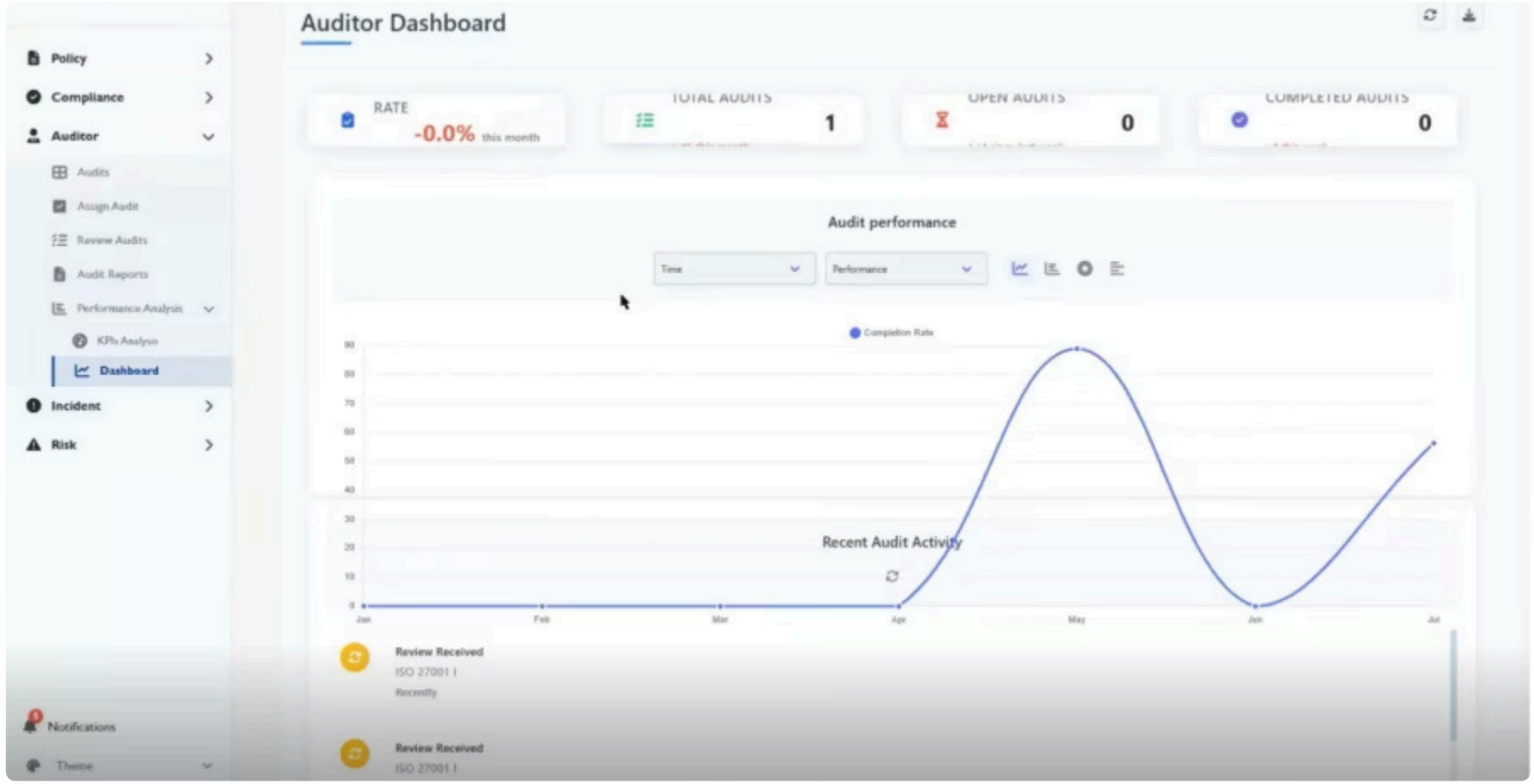
The Auditor Dashboard provides a quick snapshot of audit performance, helping users monitor overall progress, completion trends, and recent activity. The top section highlights key metrics including rate changes, total audits, open audits, and completed audits. A performance graph shows completion rates over time, allowing users to track patterns and trends. Filters for time and performance enable customized views of audit activity, while the recent audit activity section lists updates such as reviews received for specific frameworks.



Performance Analysis: KPI Analysis

The KPI Analysis section provides detailed metrics for evaluating audit effectiveness and efficiency.

The KPI Analysis section presents key metrics for evaluating audit performance. It displays noncompliance issues identified during audits to highlight areas needing attention, shows the audit completion rate by month to track progress, and measures audit cycle time with options to filter by month, quarter, or year. It also provides the audit findings rate, giving a clear view of audit depth and areas requiring further review.



Incident Management Module

The Incident module enables comprehensive management of compliance, security, and operational incidents through structured workflows with clear ownership. Users can log, track, and resolve incidents with detailed information including category, severity, impact, and evidence, while maintaining links to related policies or risks.

The module is divided into two main sections:

- Incident Management - includes incident list, creation, audit findings, and user tasks
- KPI Analysis - provides performance metrics and dashboard insights

Role-Specific Permissions

Role	View	Create	Edit	Approve	Delete
Business User	✅	✅	❌	❌	❌
Risk Owner	✅	✅	✅	✅	❌
GRC Manager	✅	✅	✅	✅	❌

Incident List

The Incident List provides a comprehensive tabular view of all recorded incidents with essential details including ID, Title, Origin, Priority, Date, and Actions. Incidents are sourced from both audit findings and manual entries.

Search & Filter

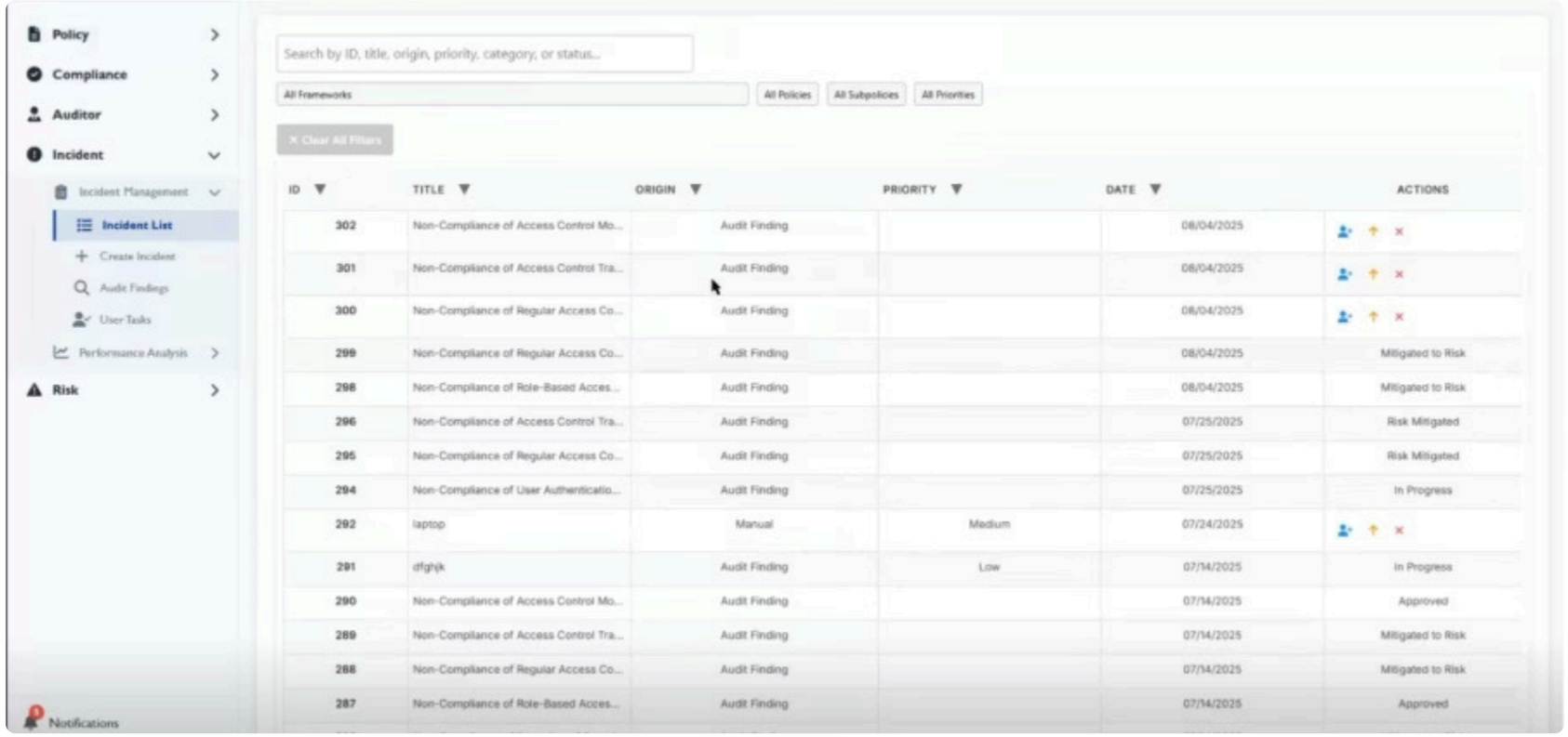
Locate incidents by ID, title, origin, priority, category, or status. Apply filters by framework, policy, subpolicy, or priority.

Status Tracking

Status indicators (Mitigated to Risk, Approved, In Progress) show current resolution stage.

Detailed View

Click on Incident Title to access all information associated with that record.



Audit Findings

This section displays incidents originating from audits, showing ID, title, priority, status, origin, date, time, and description. At the top, users can view counts of open, assigned, closed, rejected, mitigated, and total incidents.

Detailed Information

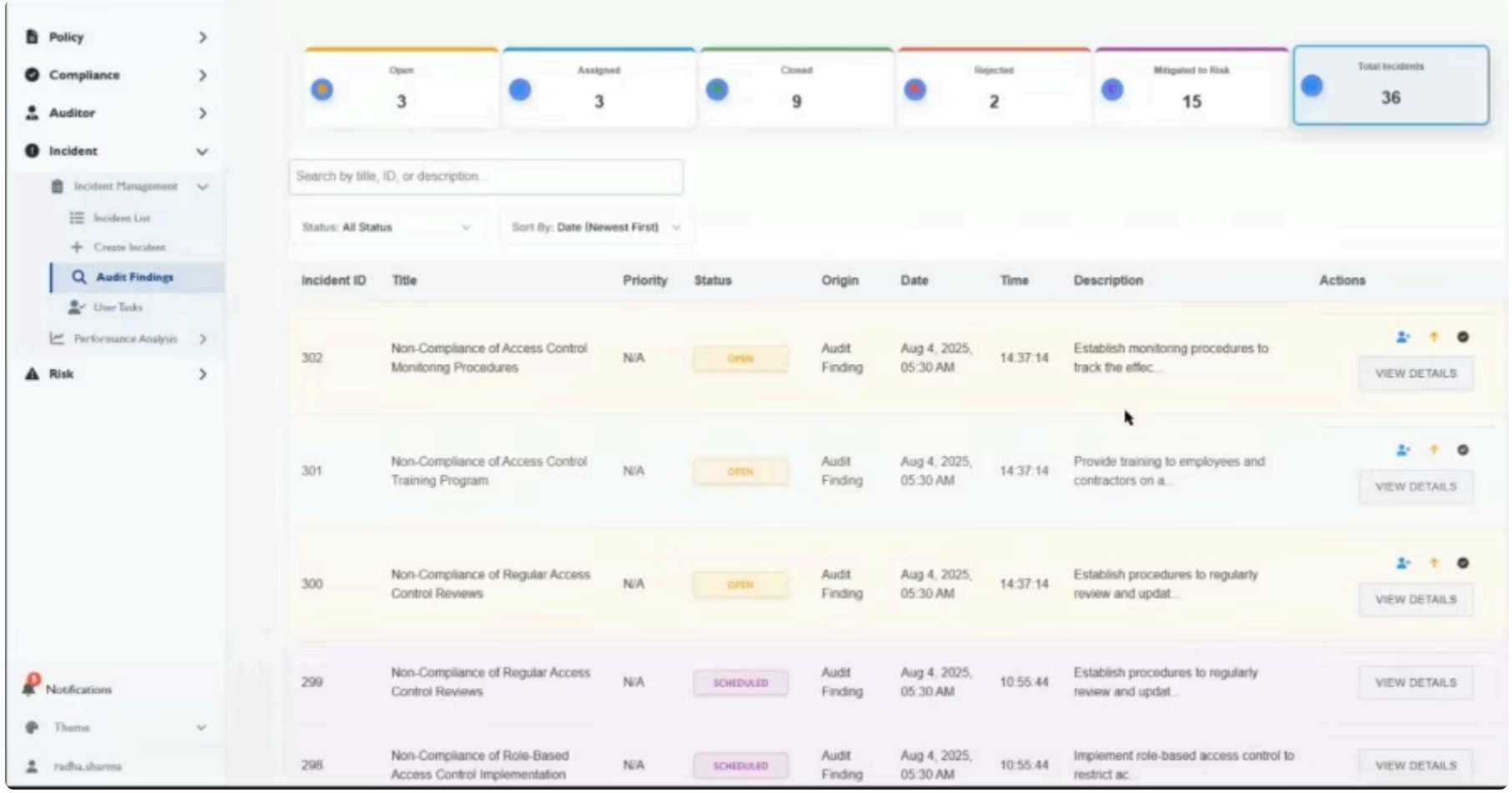
Click "View Details" to access comprehensive information including:

- Description and business impact
- Possible damage assessment
- System assets and location
- Mitigation plan and comments

Available Actions

The Actions column enables users to:

- Escalate the incident to risk
- Close the incident
- Start an incident workflow with assigners, reviewers, and mitigation steps
- Export the incident list in multiple formats



User Tasks

The User Tasks section manages incidents requiring review and approval. Incidents awaiting action appear under Reviewer Tasks, providing a clear workflow for assessment and resolution.

Review Process

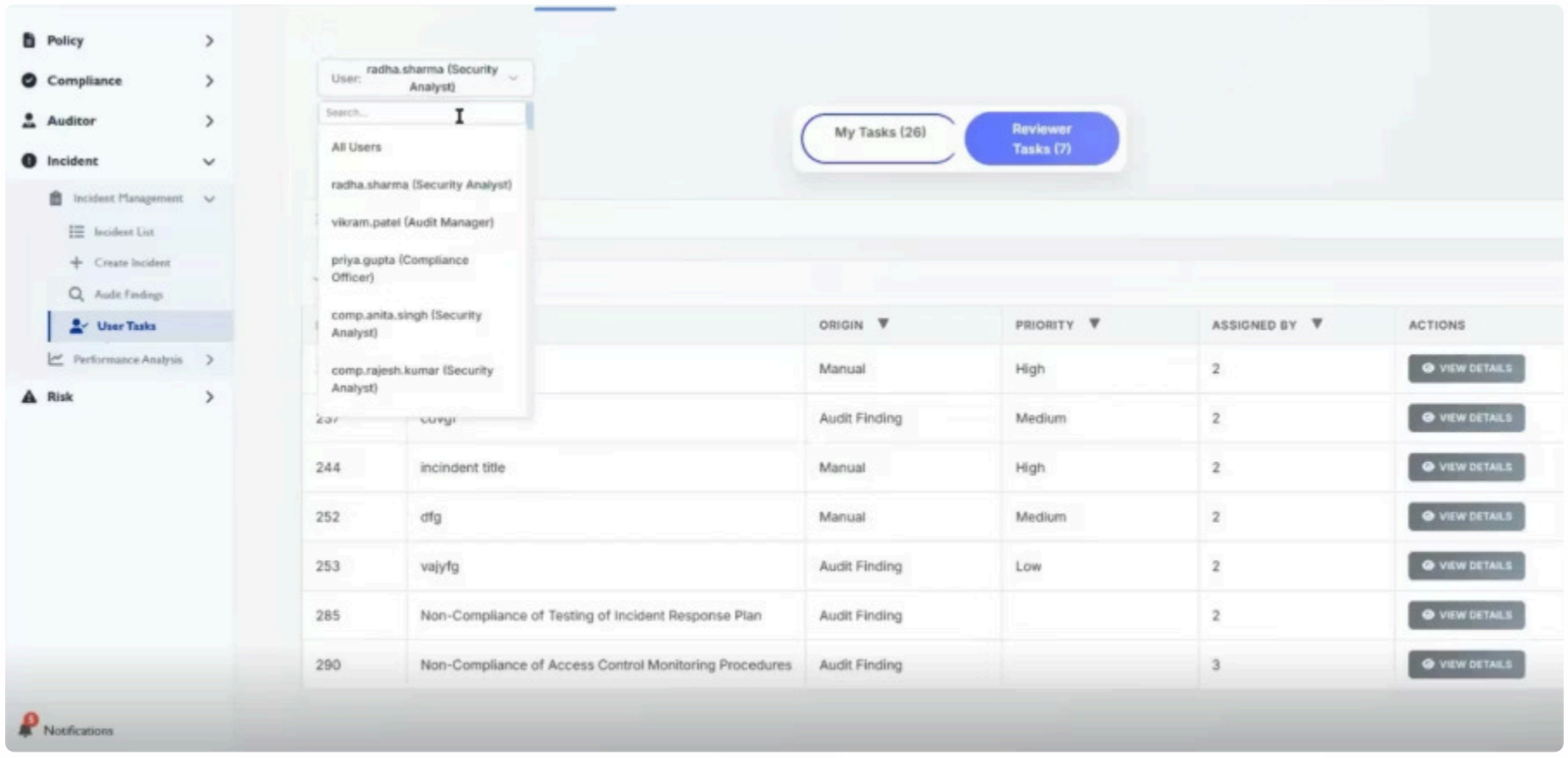
Click "View Details" in the last column to open the assessment page where reviewers can evaluate the incident.

Decision Point

Reviewers can choose to Approve or Reject the incident based on the provided information and mitigation plan.

Post-Approval

Once approved, the incident moves to the Approved section where users can view all information, including the approved mitigation steps.



Create Incident

The Create Incident feature enables users to log new incidents from audits, compliance checks, or live organizational events. Each incident can be categorized, risk-scored, and linked to corrective actions or mitigation plans.

Basic Information

Title, Description, Origin, Date, Time, Risk Priority, Category, Criticality, Cost, and Financial Impact

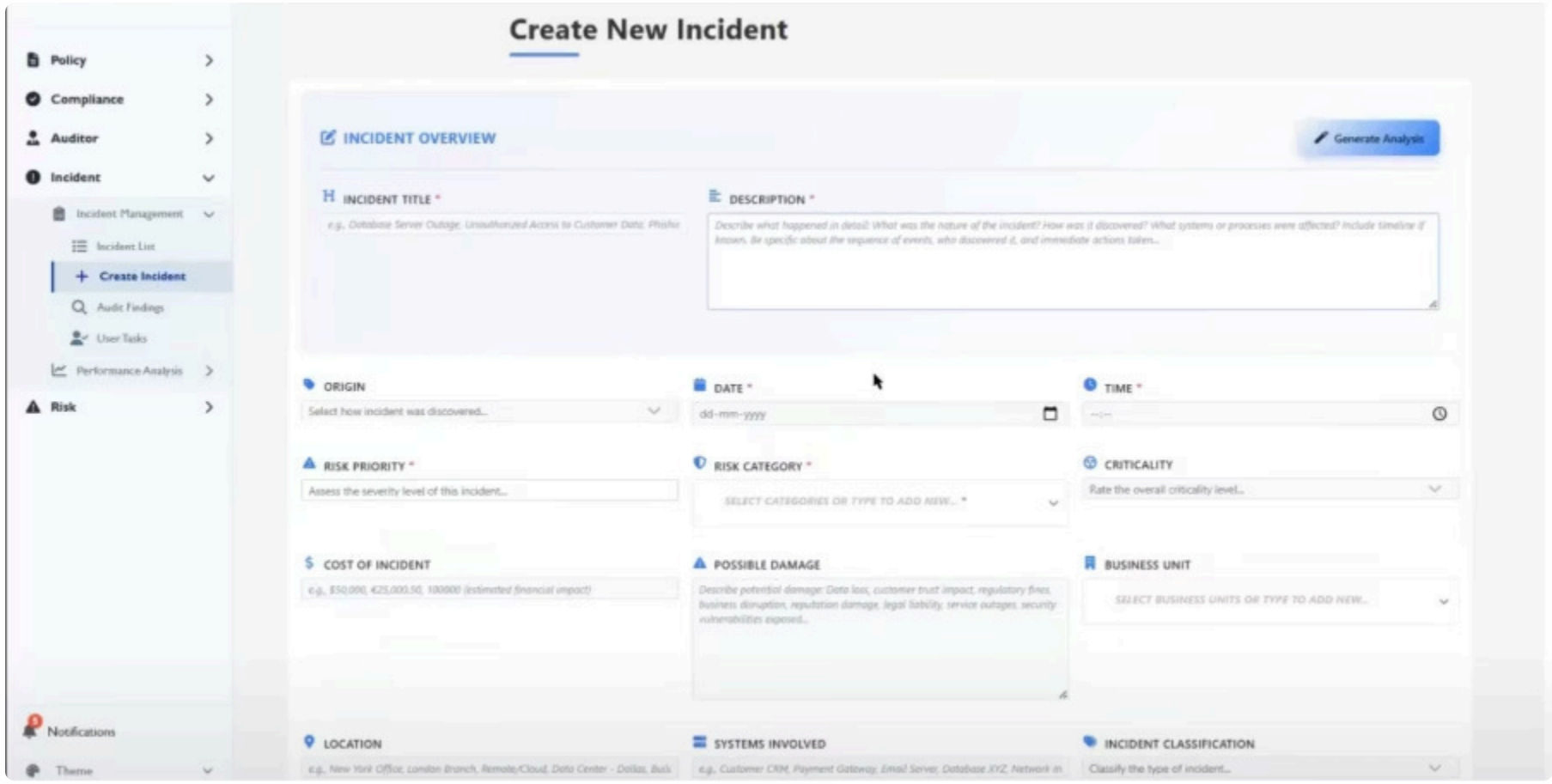
Impact Details

Potential Damage, Business Unit, Department, Location, Systems Involved, Classification, and Impact Assessment

Resolution Planning

Mitigation Steps, Comments, Internal/External Contacts, Regulatory Bodies, Violated Policies, Control Failures, and Lessons Learned

Time-saving feature: Users can click "Generate Analysis" after filling basic details to automatically populate fields including possible damage, cost, and mitigation steps.



Performance Analysis - KPI Analysis

The KPI Analysis dashboard provides a consolidated view of incident performance metrics, helping users monitor response effectiveness and identify areas for improvement.

Time Metrics

- Mean Time to Detect (MTTD)
- Mean Time to Respond (MTTR)
- Mean Time to Contain (MTTC)
- Mean Time to Resolve (MTTRv)
- First Response Time

Volume & Distribution

- Incidents by Severity (High, Medium, Low)
- Incident Origin Distribution
- Root Cause Categories
- Volume of Incident Types
- Incident Escalation Rate
- Repeat Incident Rate

Each KPI is visualized through graphs, charts, or percentages to help track performance trends. Users can drill down into each metric for more detailed insights.

Performance Analysis – Dashboard

The Incident Dashboard provides a real-time overview of all incidents, their status, and recent activity to help users quickly assess the organization's incident landscape.

Total

Incidents

Complete count of all incidents in the system

Open

Incidents

Awaiting resolution or action

Rejected

Incidents

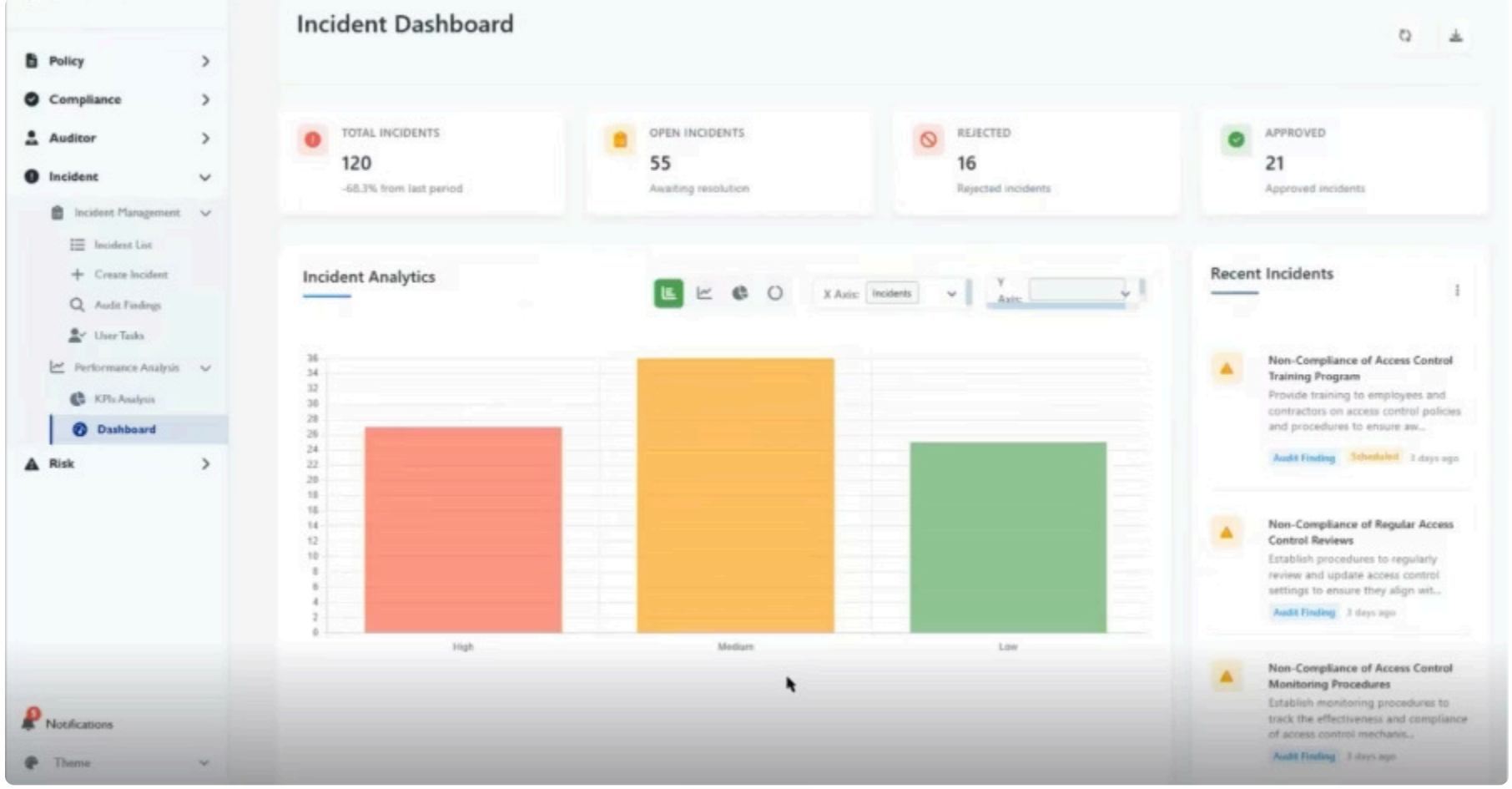
Not approved during review

Approved

Incidents

Validated and in resolution process

The dashboard includes visual charts showing incident distribution by severity level (High, Medium, Low), which can be toggled to show distribution by status. A side panel lists recently logged incidents with details such as title, category, status, and reporting date.



Risk Module

The Risk Module enables users to identify, assess, and manage risks across the organization in a structured and consistent manner. Users can log new risks with detailed attributes such as risk category, source, severity, likelihood, potential impact, and mitigation measures.

Risks can be linked to relevant policies, controls, incidents, and compliance frameworks, ensuring traceability and alignment with governance requirements. The module provides tools for qualitative and quantitative risk assessment, supports automated scoring, and highlights high-priority risks requiring immediate attention.

Interactive dashboards and reports display risk trends, open vs. mitigated risks, and residual exposure, helping management make informed decisions and track the effectiveness of mitigation strategies over time.

Role-Specific Permissions

Role	View	Create	Edit	Approve	Delete
Risk Owner	✅	✅	✅	✅	❌
Risk Contributor	✅	✅	✅	❌	❌
GRC Manager	✅	✅	✅	✅	❌

Risk Register List

The Risk Register List provides a centralized view of all risks logged within the system. Each risk entry includes key details such as:

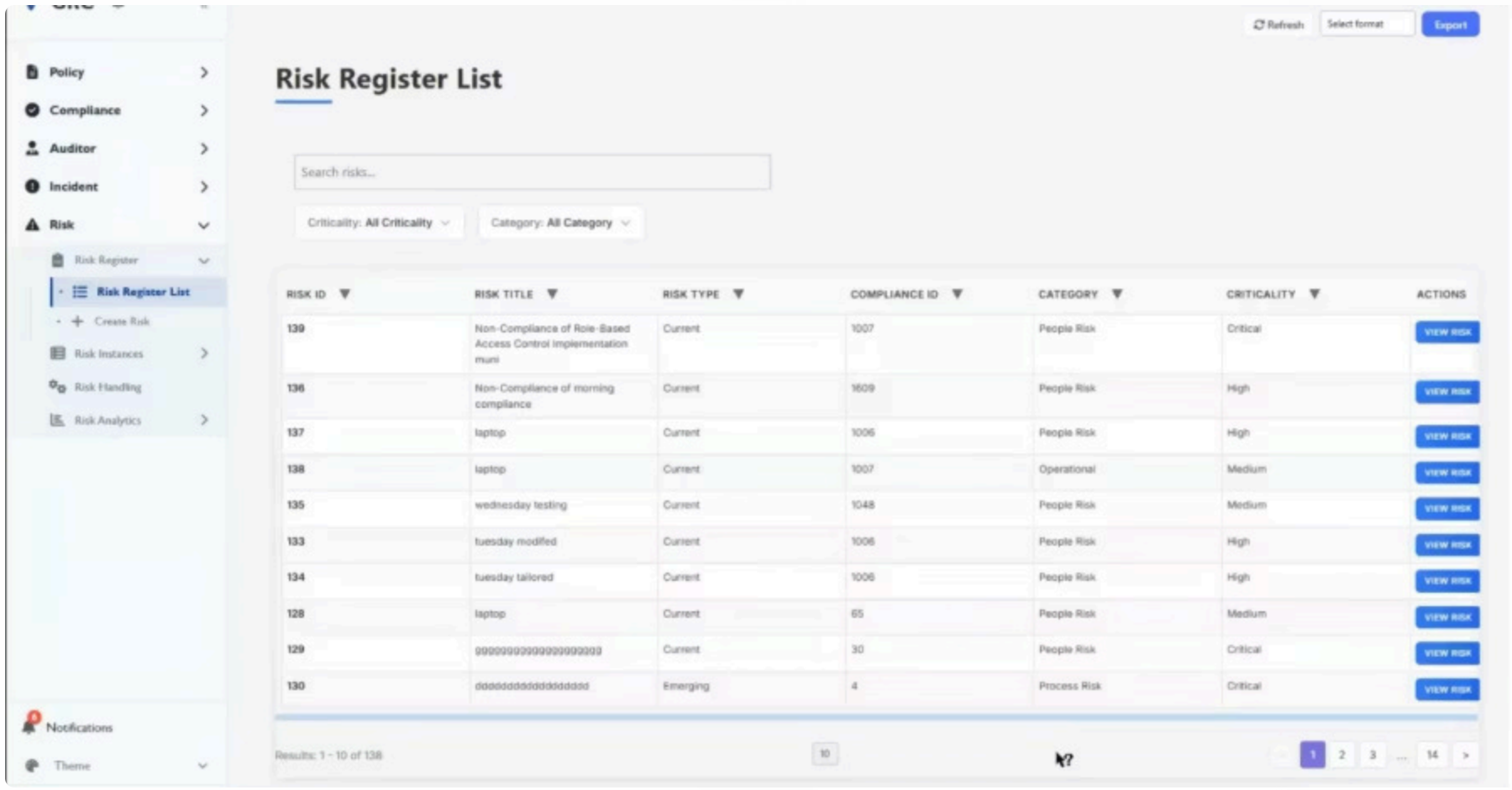
Key Information

- Risk ID – A unique identifier automatically assigned to each risk
- Risk Title – A short description of the risk
- Risk Type – Whether the risk is Current or Emerging
- Compliance ID – The compliance requirement associated with the risk

Classification

- Category – Classification of the risk (e.g., People Risk, Operational, Process Risk)
- Criticality – The severity rating of the risk (e.g., Medium, High, Critical)
- Actions – A quick link to View Risk, which opens the detailed risk record

Users can search, filter, and sort risks by criticality, category, or other parameters to locate relevant records quickly. The list can be refreshed for updated information and exported in different formats using the Export button on the top right.



Risk Details Page

Clicking View Risk from the Risk Register List opens the Risk Details page, which displays comprehensive information about the selected risk.

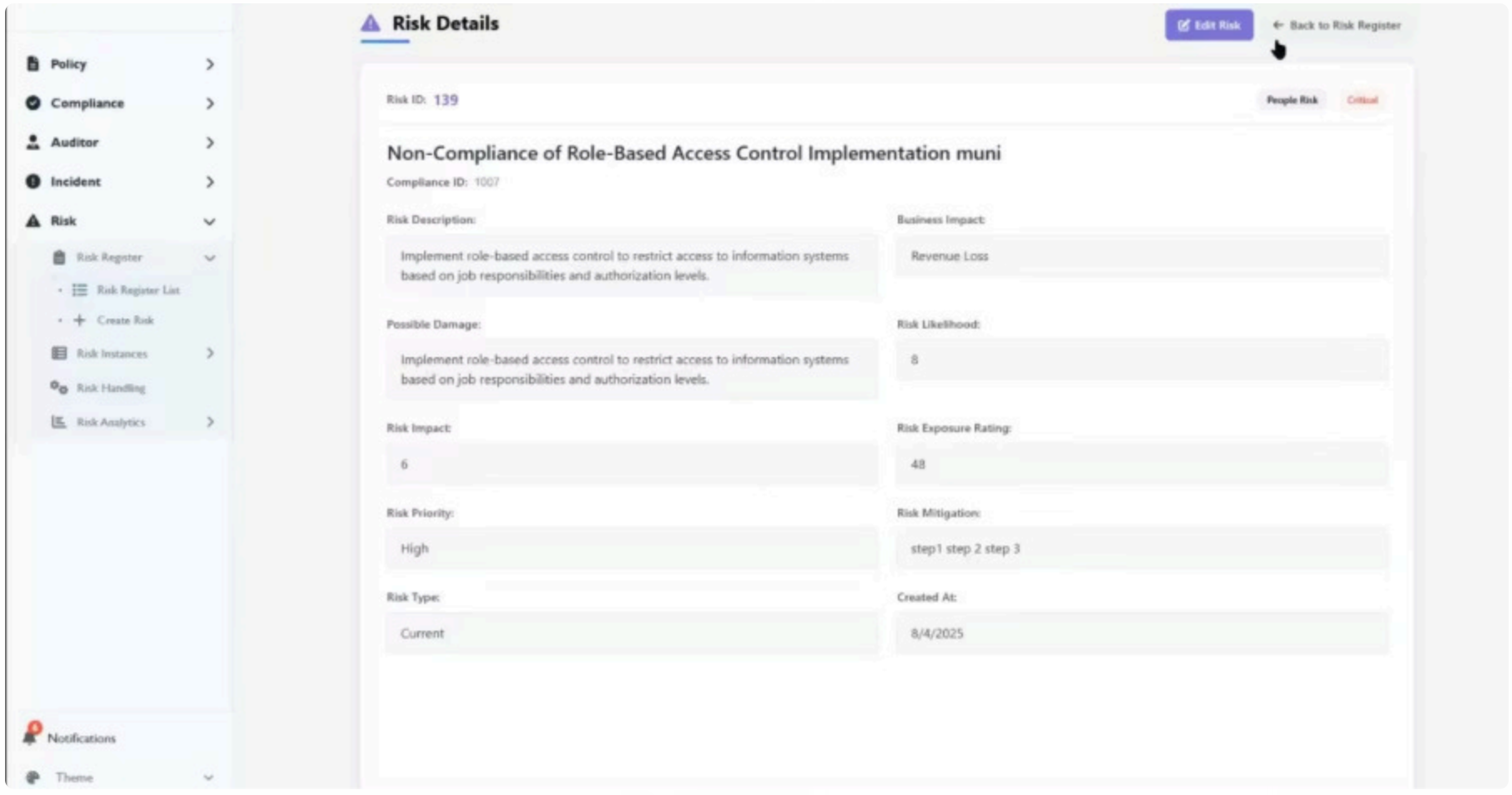
Risk Identification

- Risk ID & Title – Unique identifier and descriptive name
- Compliance ID – Linked compliance requirement
- Risk Description – Detailed explanation of the risk scenario
- Possible Damage – Potential adverse outcomes
- Business Impact – Business consequence (e.g., Revenue Loss)

Risk Assessment

- Risk Impact & Likelihood – Numeric scoring of severity and probability
- Risk Exposure Rating – Calculated overall risk score
- Risk Priority – Assigned criticality level (e.g., High, Critical)
- Risk Type – Classification as Current or Emerging
- Risk Mitigation – Defined steps to address the risk
- Created At – Timestamp of risk record creation

Users can Edit Risk from this page to update information or return to the Risk Register List using the navigation link at the top.



Risk Scoring

Escalated incidents from the incident module will appear here. The Risk Scoring section provides a consolidated view of all risk instances and their associated scoring details.

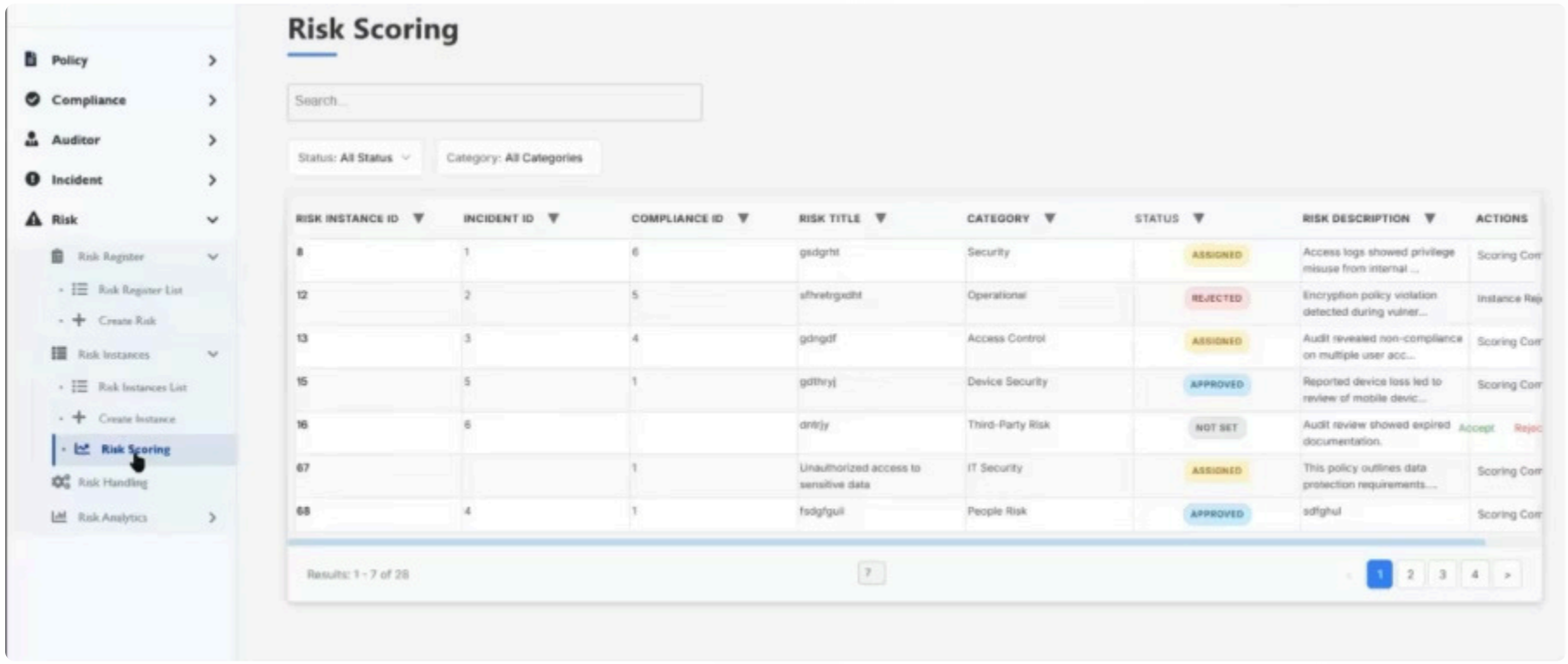
Key Identifiers

- Risk Instance ID – Unique identifier for each risk instance
- Incident ID – Reference to the linked incident
- Compliance ID – Connected compliance requirement
- Risk Title – Short description of the risk

Classification & Status

- Category – Risk classification (e.g., Security, Operational, Access Control)
- Status – Current state (e.g., Assigned, Approved, Rejected, Not Set)
- Risk Description – Brief summary of risk context and details
- Actions – Options to complete scoring or accept/reject the risk instance

Users can search, filter, and sort risk instances by category or status for better tracking. The scoring process allows organizations to evaluate risks systematically, ensuring each risk instance is assessed and documented for further handling.



Risk Scoring Details

Clicking on accept risk takes us to the risk scoring details page, which contains comprehensive fields for risk assessment.

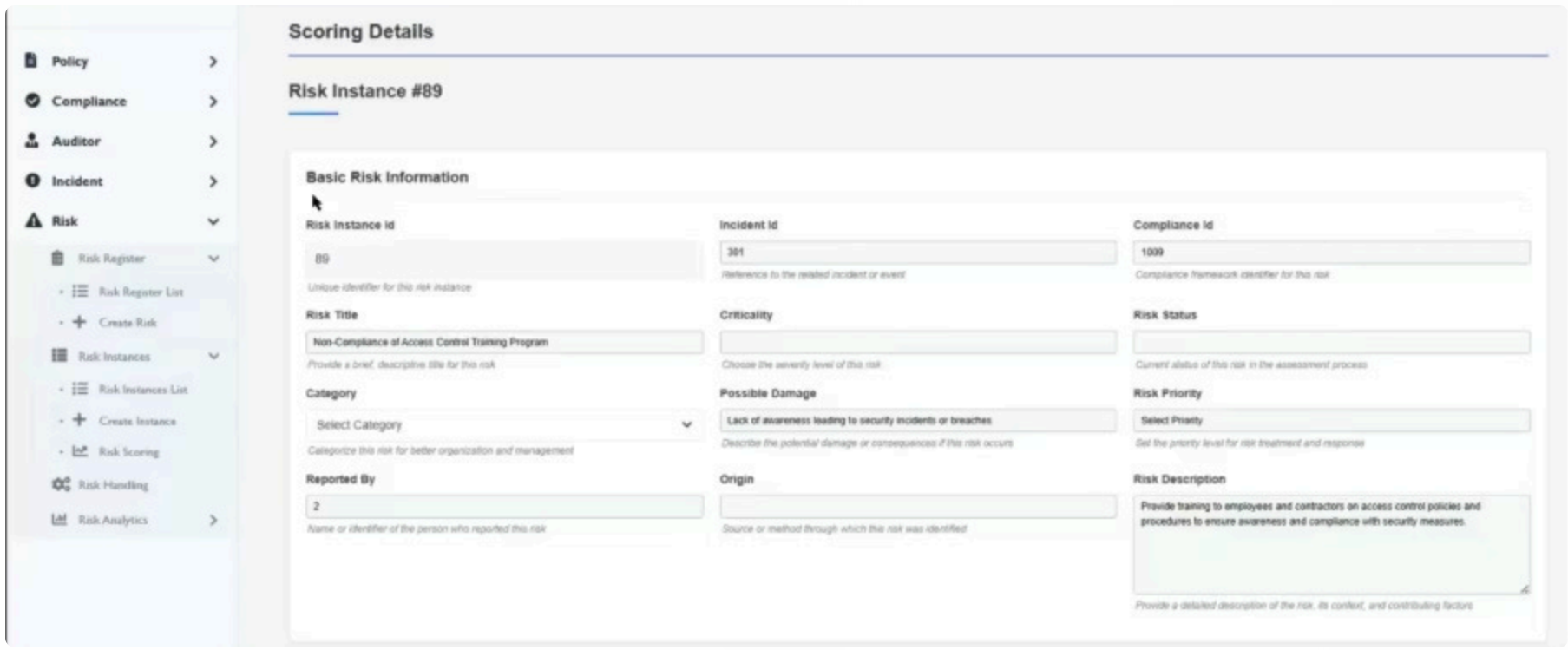
Risk Identification

- Risk Instance ID – Auto-generated unique identifier
- Incident ID – Links to associated incident
- Compliance ID – Mapped compliance requirement
- Risk Title – Brief descriptive name
- Category – Classification dropdown (e.g., IT Security, People Risk)
- Reported By – User or team identifier
- Criticality – Severity level (Low, Medium, High, Critical)

Risk Details

- Possible Damage – Potential consequences
- Origin – Identification method or source
- Risk Status – Current workflow stage
- Risk Priority – Importance level (Low, Medium, High)
- Risk Description – Detailed explanation and context

The Mapped Risks feature allows users to select risks from the Risk Register that match the compliance ID. Clicking the checkbox and "fill risk details" button automatically populates information including Risk ID, Likelihood, Impact, Exposure Rating, Type, Appetite, Business Impact, and Response details. Users can then add Mitigation Steps and save changes, which updates the status to "risk scoring completed."



Create Risk

The Create Risk page allows users to log new risks by entering detailed information for proper tracking and management.

Risk Classification

- Compliance ID – Related compliance requirement
- Criticality – Severity level
- Category – Risk classification
- Risk Priority – Urgency level
- Risk Type – Current or potential

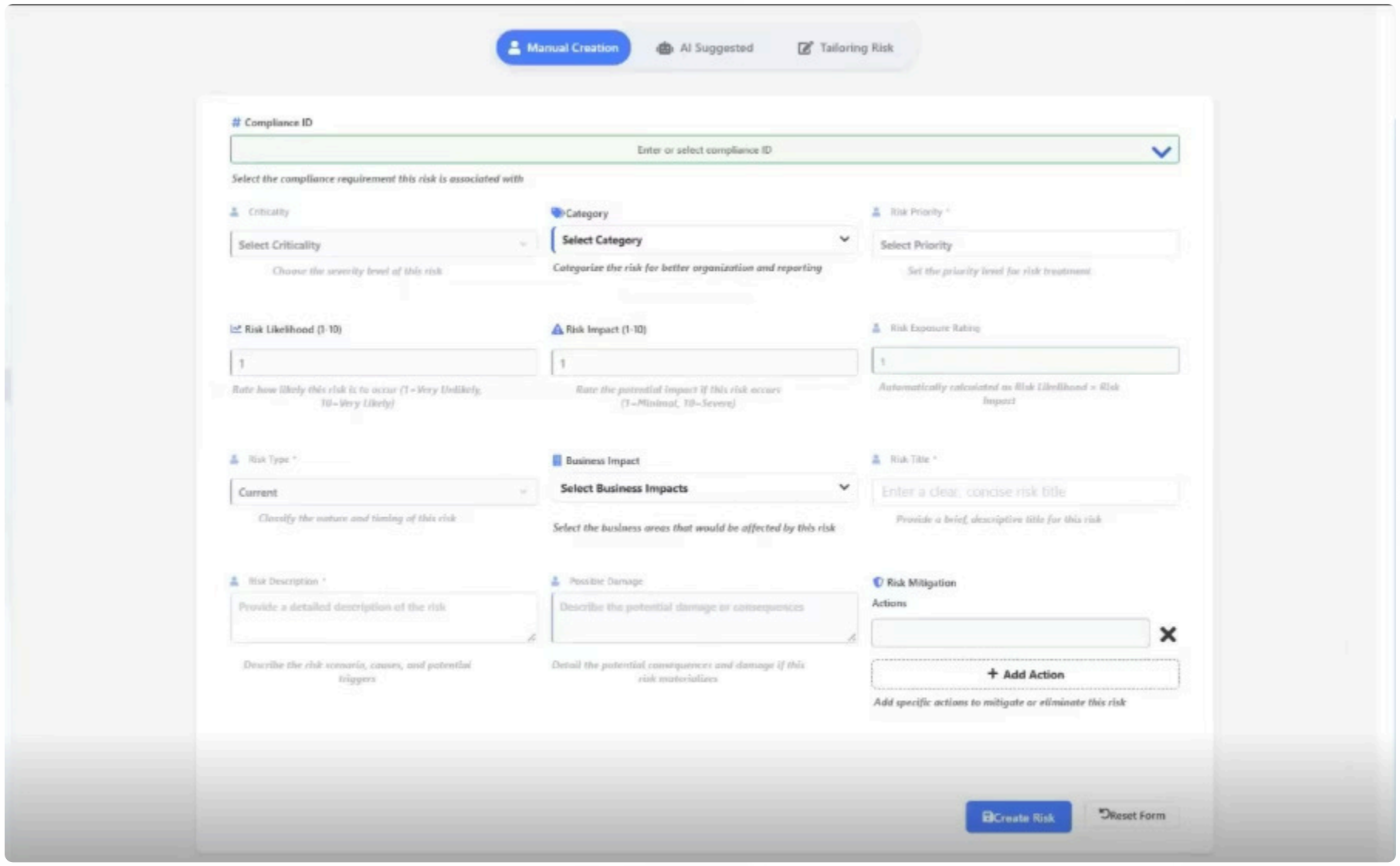
Risk Assessment

- Risk Likelihood (1–10) – Probability rating
- Risk Impact (1–10) – Severity rating
- Risk Exposure Rating – Auto-calculated (likelihood × impact)
- Business Impact – Affected business area(s)

Risk Description

- Risk Title – Short, clear title
- Risk Description – Detailed explanation
- Possible Damage – Potential consequences
- Risk Mitigation (Actions) – Steps to reduce or remove risk

In manual creation, users must complete all these fields to properly document and categorize the risk, enabling effective management and mitigation planning.

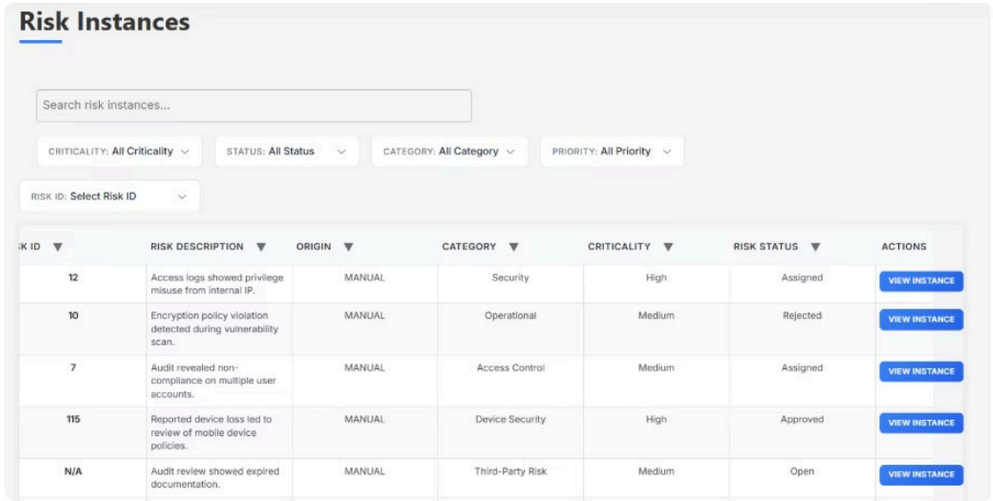


Risk Instances Management

Risk Instances List

The Risk Instances page provides a detailed list of all identified risk instances in the system. Each entry captures key details such as the Risk ID, Description, Origin, Category, Criticality, and Risk Status.

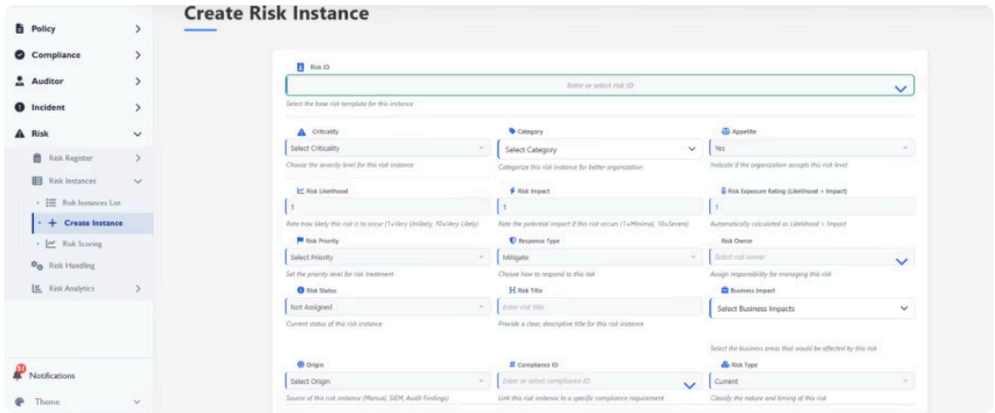
- Navigate to Risk → Risk Instances from the left menu
- Search, filter, or browse risks by descriptions, categories, and criticality levels
- Click View Instance to see full details, scoring, and history



Create Risk Instance

The Create Risk Instance page allows users to log a new risk instance with key details:

- Base Risk ID, Criticality, Category, and appetite assessment
- Likelihood, Impact, and auto-calculated Risk Exposure Rating
- Risk Priority, Response Type, Owner, Business Impact, and Type
- Risk Title, Description, Possible Damage, and Response Description
- Origin, Compliance ID, and planned Mitigation steps



Risk Handling

The Risk Handling page enables users to track and manage risks through two main tabs:

1

Risk Resolution Tab

Users can view risks by their status, criticality, assigned owner, and reviewer, along with review counts. Clicking on View Details opens a detailed page where users can:

- Assign risks to appropriate personnel
- Define specific mitigation steps
- Update handling actions and progress
- Track resolution status and effectiveness

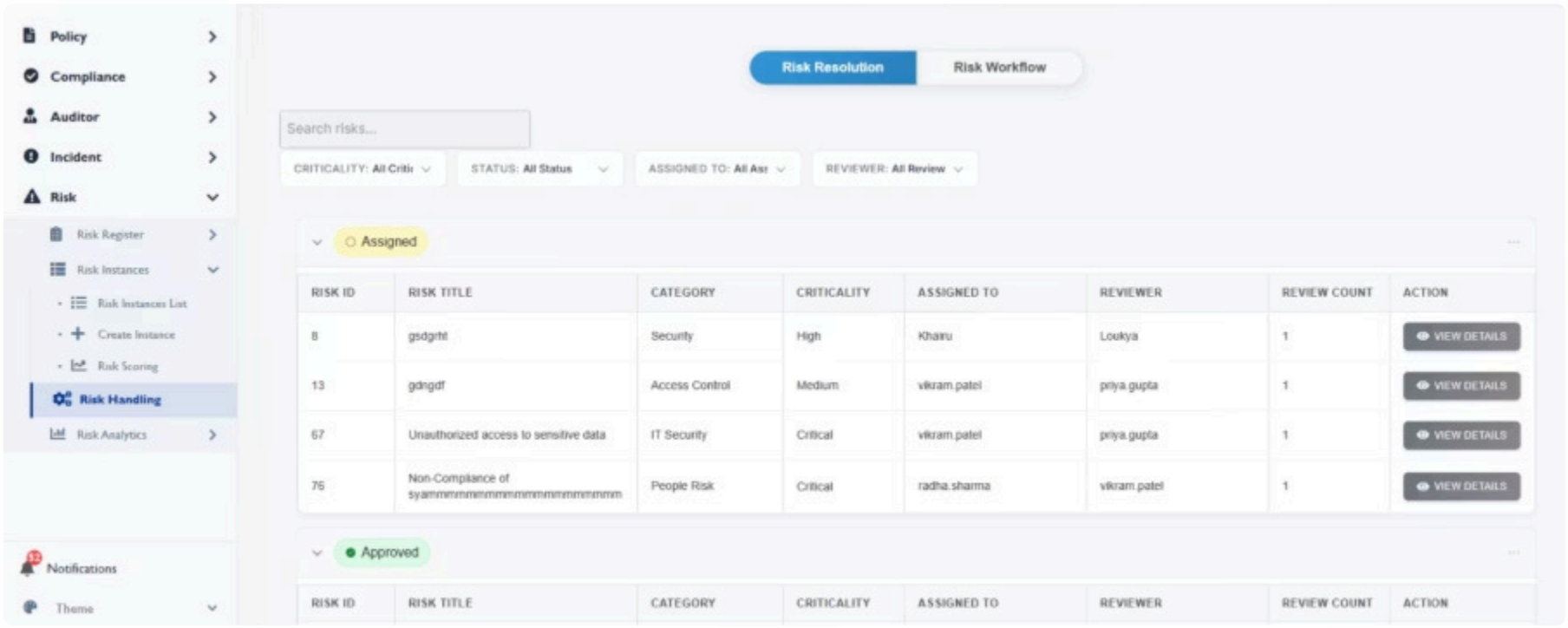
2

Risk Workflow Tab

Displays all risks and tasks assigned to a particular user, including:

- Risks requiring the user's attention
- Tasks assigned for mitigation or review
- Responsibilities for risk assessment
- Deadlines and priority indicators

This structured approach ensures that risks are properly assigned, tracked, and resolved through a defined workflow, with clear accountability at each stage of the risk management process.



Risk Analytics Dashboard

The Risk Dashboard provides a consolidated view of the organization's risk landscape through key metrics and visual analytics.

Key Metrics

Real-time counters for total risks, accepted, rejected, mitigated, and in-progress risks

Risk Distribution

Chart showing risk breakdown by category to identify the highest occurring risk types

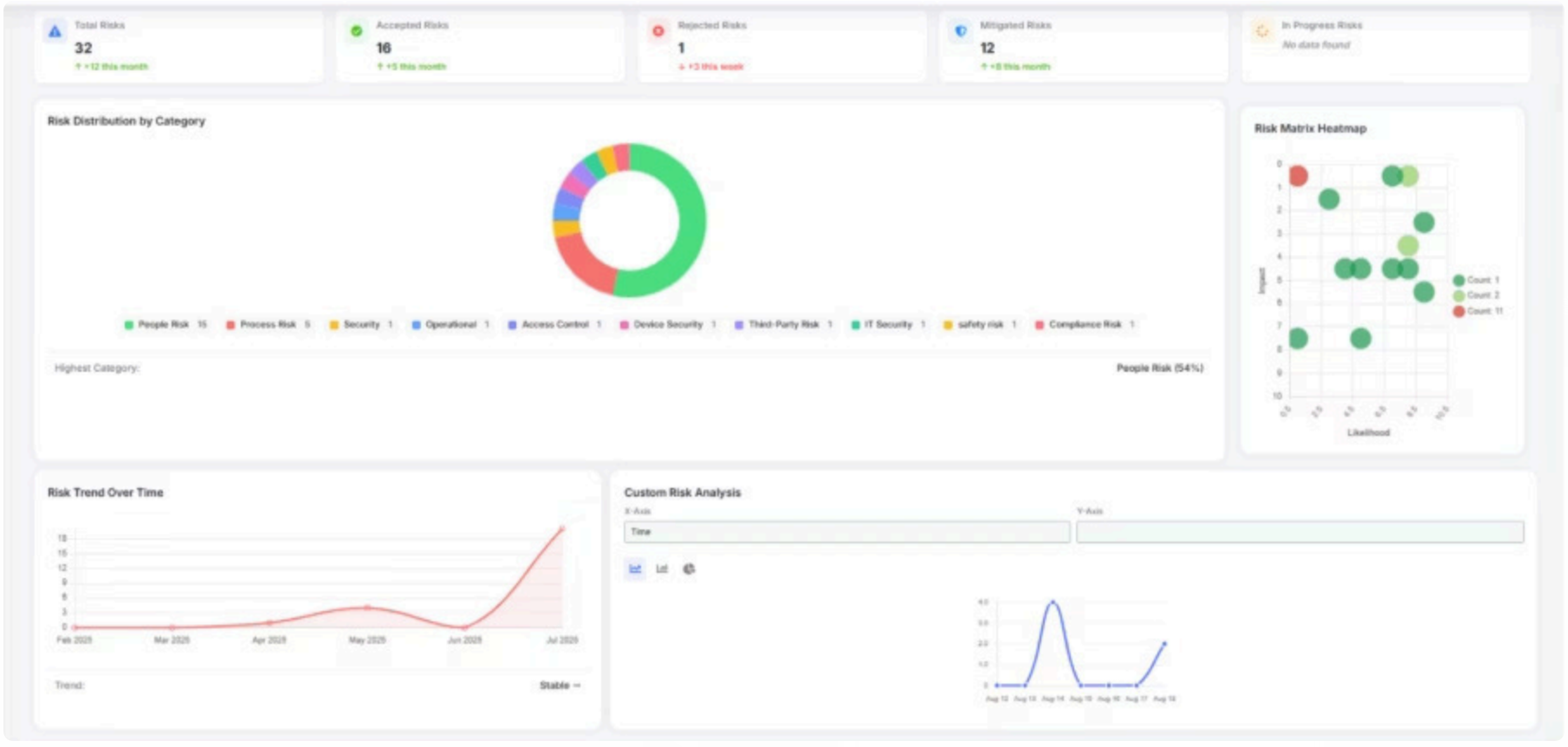
Risk Matrix Heatmap

Visual representation of likelihood vs. impact for quick assessment of risk severity

Risk Trend Analysis

Graph tracking risk patterns over time and Custom Risk Analysis tool for deeper insights

These visualizations help management monitor changes and patterns effectively, enabling data-driven decision making and proactive risk management across the organization.



KPI Dashboard

The Risk KPI Dashboard provides a performance-focused view of key risk management indicators:

100%

Active Risks

Total number of currently active risks, with emphasis on high criticality items

75%

Recurrence Rate

Tracking one-time vs. recurring risks to identify systemic issues

90%

Review Completion

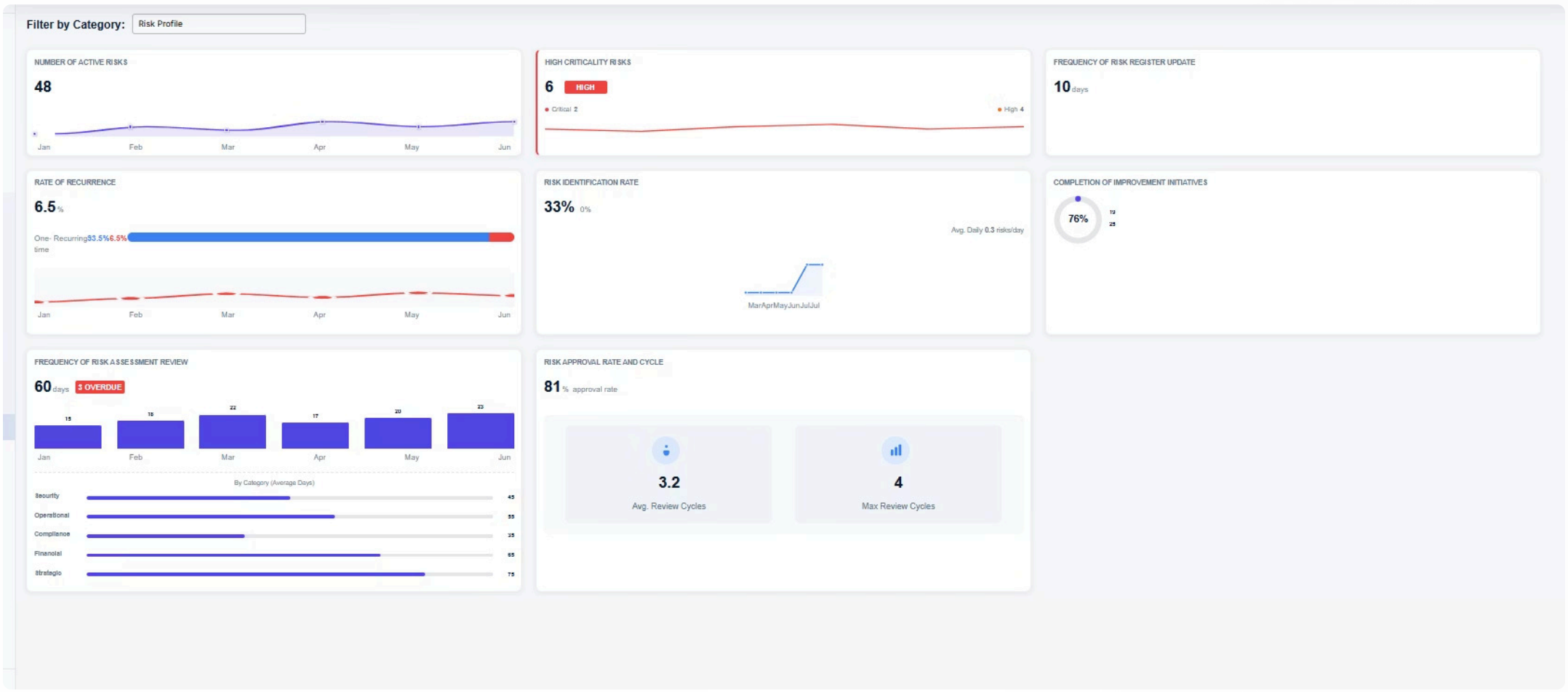
Monitoring frequency of risk register updates and assessment reviews

85%

Initiative Completion

Rate of completion for risk improvement initiatives

Additional metrics include risk identification rate, approval rate and cycle metrics, with overdue reviews flagged for action. These KPIs help track progress, identify gaps, and ensure risks are being managed effectively over time, offering insight into the overall efficiency of the risk management program.



Summary

The platform user manual is designed to help you quickly get started and make the most of the system. From logging in and setting up your profile to accessing dashboards tailored to your role, the guide ensures you can navigate with ease. Core functions like managing policies, monitoring compliance, and tailoring frameworks are explained in simple steps, making it easy to stay aligned with organizational standards.

You will also find details on conducting audits, reviewing findings, and leveraging dashboards for clear performance insights. The manual covers incident management workflows for logging, tracking, and resolving issues effectively, while also providing structured approaches for identifying, scoring, and mitigating risks. Throughout, the emphasis is on security, transparency, and streamlined workflows.

For assistance or feedback, you can reach us anytime at **info@vardaanglobal.com** or call us at **+91 40-35171118, +91 40-35171119**. We are located at **Aurum, 1st Floor, Plot No 57, Jayabheri Enclave, Gachibowli Hyderabad-500032, INDIA**.

Thank You!

The platform user manual is designed to help you quickly get started and make the most of the system. From logging in and setting up your profile to accessing dashboards tailored to your role, the guide ensures you can navigate with ease. Core functions like managing policies, monitoring compliance, and tailoring frameworks are explained in simple steps, making it easy to stay aligned with organizational standards.

You will also find details on conducting audits, reviewing findings, and leveraging dashboards for clear performance insights. The manual covers incident management workflows for logging, tracking, and resolving issues effectively, while also providing structured approaches for identifying, scoring, and mitigating risks. Throughout, the emphasis is on security, transparency, and streamlined workflows.

We appreciate your time and interest in our Risk Management Platform. Our goal is to empower your organization with robust tools for proactive risk identification, assessment, and mitigation.

Contact Us

For any questions, feedback, or further information, please reach out to us:

Email: info@vardaanglobal.com

Phone: +91 40-35171118, +91 40-35171119

Visit Us

You can find us at:

Aurum, 1st Floor, Plot No 57, Jayabheri Enclave,

Gachibowli Hyderabad-500032, INDIA