

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

- Login Process
- Dashboard Overview
- Navigation System (Left Navigation Bar & Top Bar)
- Notifications Management
- User Settings
- Profile Management (Account, Role, Password, Notifications)
- Role-Based Access Control
- Requesting Role Changes
- Password Management
- Notification Preferences
- User Dashboard

Policy Management

- Policy Module Overview
- All Policies View
- Policy Hierarchy Navigation
- Policy Tree Visualization
- Creating a New Framework
- Creating a New Policy
- Creating Sub-Policies
- Policy Approval Process
- Reviewer Approval Workflow
- Tailoring and Templating
- Versioning Policies and Frameworks
- Uploading Frameworks
- KPI Analysis Dashboard

Compliance Management

- Compliance Creation
- Compliance Approval
- Compliance Tailoring and Templating
- Compliance Versioning
- Control Management
- Compliance List Details
- Compliance Audit Management
- Compliance Dashboard
- Compliance KPI

Audit Management

- Comprehensive Audit Management Overview
- Assigning Audits (Framework Selection, Team Creation, Policy Assignment, Audit Details)
- Audit Dashboard Overview
- Audit Details Page
- Compliance Assessment
- Review Audits (Overview & Process)
- Audit Report: Consolidated View
- Performance Analysis Dashboard
- KPI Analysis for Audits

Incident Management

- Incident Module Overview
- Incident List
- Audit Findings
- User Tasks (Reviewer Workflow)
- Creating an Incident
- Performance Analysis – KPI Analysis
- Incident Dashboard

Risk Management

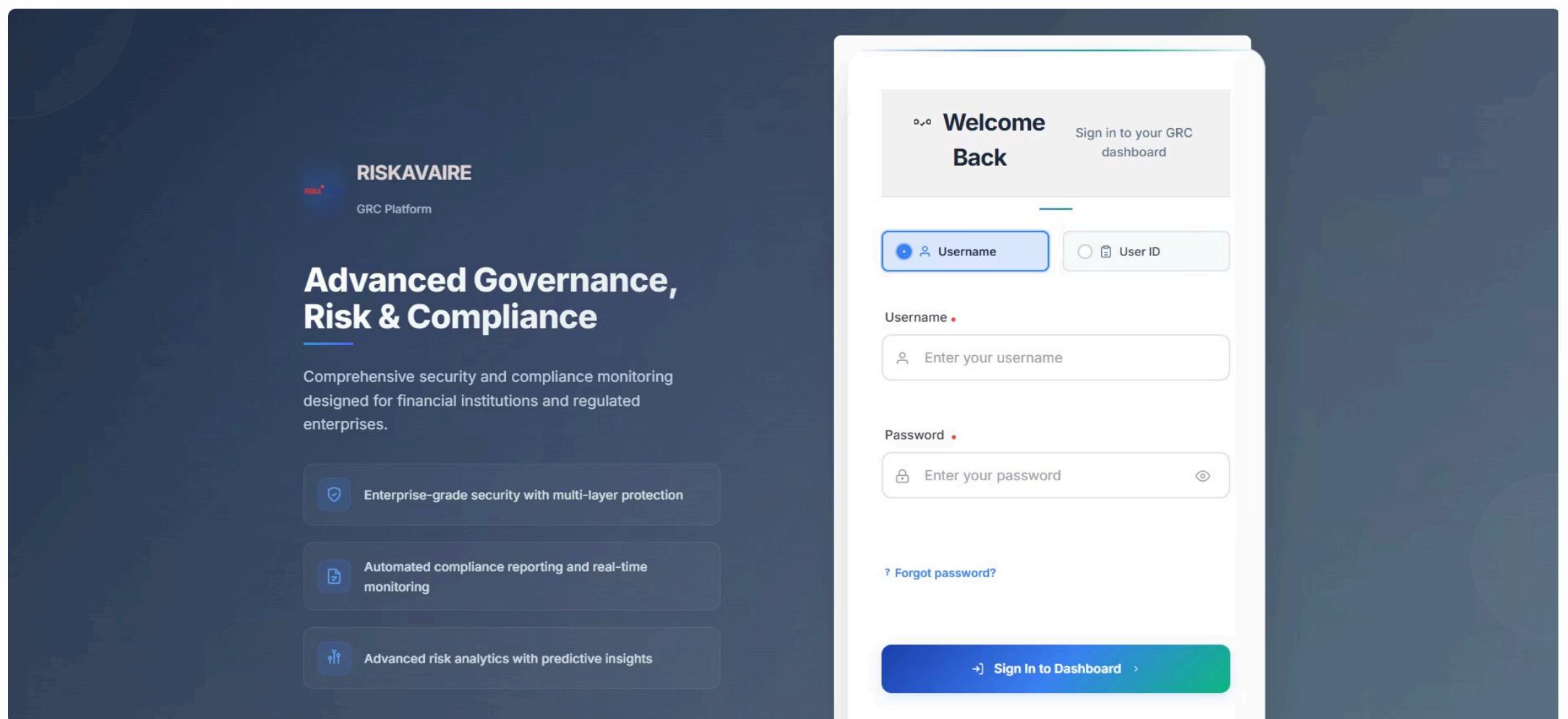
- Risk Module Overview
- Risk Register List
- Risk Details Page
- Risk Scoring
- Risk Scoring Details
- Creating a Risk
- Risk Instances Management
- Risk Handling (Resolution & Workflow Tabs)
- Risk Analytics Dashboard
- Risk KPI Dashboard

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.

The screenshot shows the XYZ Bank GRC dashboard. At the top, there's a navigation bar with icons for GRC, Notifications (23), Dashboard (selected), Policies, Compliance, Risk, Audits, Incidents, a user profile for Radha Sharma, and a Logout button. On the left, a sidebar lists quick access links: Policy, Compliance, Auditor, Incident, and Risk. The main content area features a large banner with the text "Next-Generation GRC Platform for Banking". Below the banner, a paragraph describes the platform's purpose: "Experience the future of Governance, Risk, and Compliance with our unified platform designed for agility, accuracy, and efficiency. Empower your organization to seamlessly manage audits, assess risks, enforce compliance, and monitor policies." Four key performance indicators are displayed in boxes: "99.9% Uptime", "500+ Regulations", "24/7 Monitoring", and "< 1s Response Time". To the right, a chart titled "GRC Dashboard" shows a line graph of a metric over time from January to June, with values ranging from 80 to 100. Below the chart are three summary cards: "1,247 Active Policies +12%", "7.2 Risk Score -5%", and "94% Compliance +3%". At the bottom, there are buttons for "Explore Dashboard" and "View Policies". The footer includes links for Notifications (23), Theme, and a user profile for radha.sharma.

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

Notifications

[Mark All as Read](#)

Notification	Priority	Time	Status
A Reports Attached Reports have been attached to the audit assignment.	medium	2 hours ago	unread <input checked="" type="checkbox"/>
A Audit Notification Status updated to "Work In Progress" successfully	high	2 hours ago	unread <input checked="" type="checkbox"/>
Review Status Updated Review status for audit ID 47 updated to In Review	medium	1 hours ago	unread <input checked="" type="checkbox"/>
A Audit Report Generation Audit report for audit ID 40 is being generated.	medium	1 hours ago	unread <input checked="" type="checkbox"/>
A Audit Report Download Audit report for audit ID 40 download initiated.	medium	1 hours ago	unread <input checked="" type="checkbox"/>
R Risk Register Updated Successfully loaded 138 risks from the Risk Register.	medium	1 hours ago	unread <input checked="" type="checkbox"/>
R Risk Details Viewed Risk "Non-Compliance of Role-Based Access Control Implementation muni" (ID: 139) details have been viewed.	low	1 hours ago	unread <input checked="" type="checkbox"/>

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).

The screenshot shows the 'Personal Information' tab selected within the Profile Management interface. At the top, there is a navigation bar with tabs: 'Account' (highlighted in blue), 'Role', 'Password', and 'Notification'. Below the navigation bar, there are two main sections: 'Personal Information' and 'Business Information'. The 'Personal Information' section is active, displaying fields for First Name, Last Name, Email, and Phone Number, each with a placeholder value. A large blue button at the bottom of this section is labeled 'SAVE PERSONAL INFO'.

Role-Based Access Control

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

Role Assignment

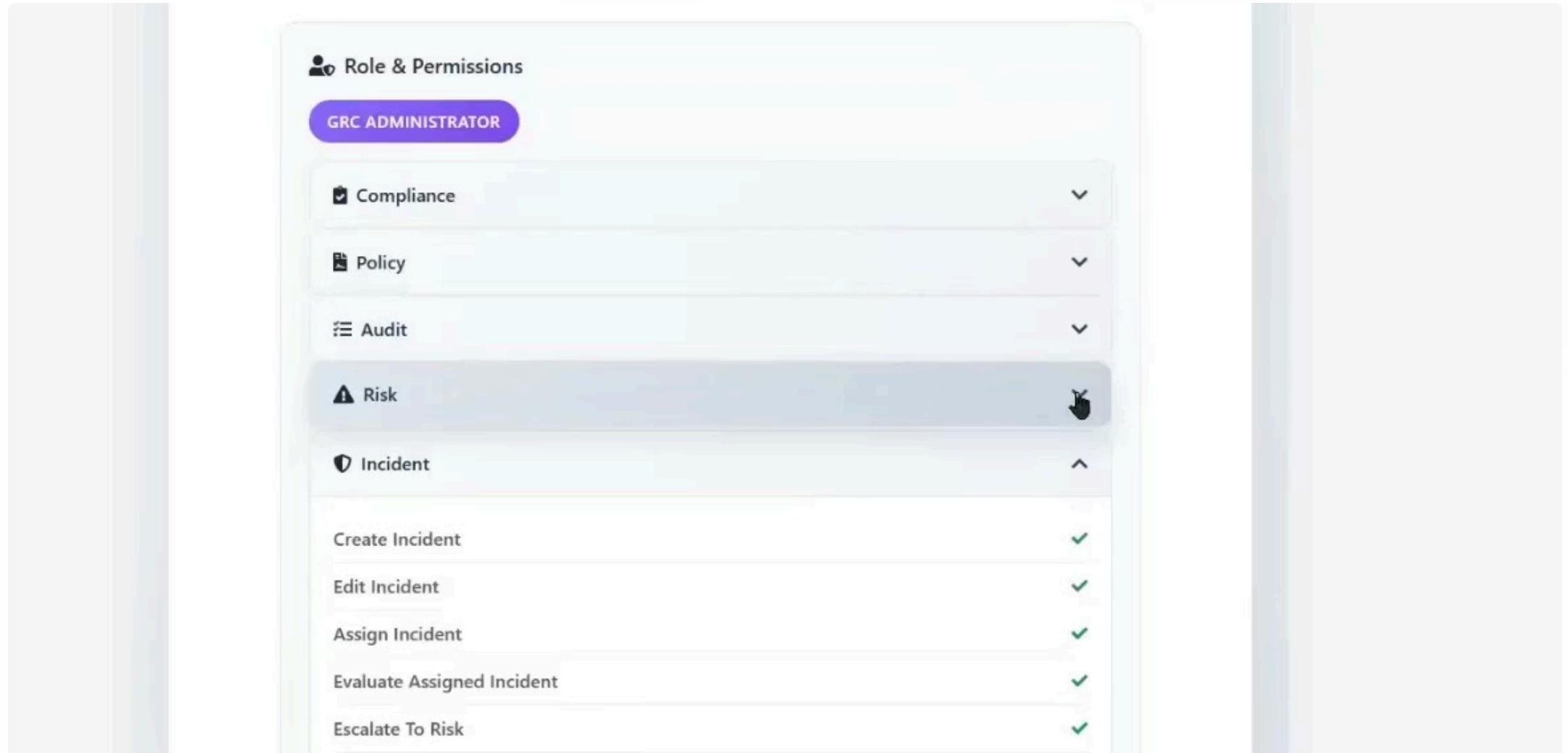
Administrators can assign roles such as ISO Officer, Control Owner, Risk Manager and more

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



The screenshot shows a user interface titled "Role & Permissions". At the top, a purple button labeled "GRC ADMINISTRATOR" is visible. Below it is a tree view of roles:

- Compliance
- Policy
- Audit
- Risk (highlighted with a blue selection bar)
- Incident

Under the "Risk" role, a list of permissions is shown, each with a green checkmark indicating they are assigned:

- Create Incident
- Edit Incident
- Assign Incident
- Evaluate Assigned Incident
- Escalate To Risk

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

The screenshot shows a user interface for changing a password. At the top, there's a header with a key icon and the text 'Change Your Password'. Below the header, a descriptive message reads: 'For your security, please enter your email and a new password. You will need to verify with an OTP sent to your registered email or phone.' There are four input fields: 'Email' (containing 'radha.sharma@company.com'), 'Enter OTP' (with a placeholder 'Enter OTP'), 'New Password' (with a placeholder 'Enter new password'), and 'Confirm Password' (with a placeholder 'Re-enter new password'). A large green button labeled 'Verify' is positioned between the Email and Enter OTP fields. A blue button labeled 'UPDATE PASSWORD' is located at the bottom.

Change Your Password

For your security, please enter your email and a new password. You will need to verify with an OTP sent to your registered email or phone.

Email

radha.sharma@company.com

Verify

Enter OTP

New Password

Confirm Password

Re-enter new password

UPDATE PASSWORD

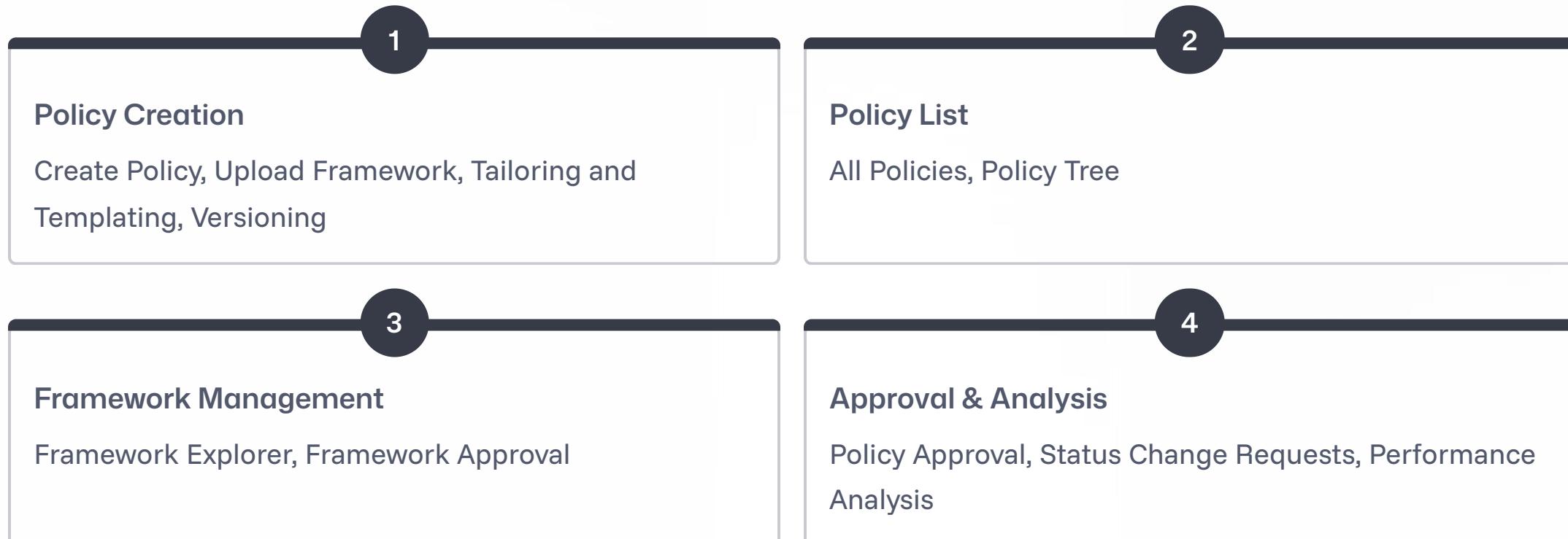
Notification Preferences

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.



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

The screenshot shows the GRC application's 'All Policies' view. On the left is a vertical navigation sidebar with sections like Policy, Compliance, Auditor, Incident, Risk, Notifications, and Theme. The 'Policy' section is expanded, showing options for Policy Creation (Create Policy, Upload Framework, Tailoring & Templating, Versioning), Policies List (All Policies selected), and other analysis tools. The main content area has tabs for Compliance Frameworks, Policies, and Subpolicies, with 'Compliance Frameworks' selected. A dropdown menu says 'Framework: Select...'. Below it is a table titled 'FRAMEWORKS' with columns: NAME, CATEGORY, STATUS, DESCRIPTION, and ACTIONS. The table lists several frameworks:

NAME	CATEGORY	STATUS	DESCRIPTION	ACTIONS
ISO 27001	Information Security	Active	ISO 27001 is the international standard for information security management systems (ISMS), providing a systematic approach to managing sensitive company information, ensuring its confidentiality, integrity, and availability.	
NIST 800-53	Information Security	Active	NIST 800-53 provides a comprehensive framework for securing federal information systems in the United States, covering security controls for all information system components and risk management processes.	
Data Protection Act 2017	Data Protection	Active	This framework provides guidelines for data controllers and processors to comply with personal data protection regulations, ensuring the privacy of individuals and safeguarding their rights in Mauritius as per the Data Protection Act 2017.	
Corporate Governance Framework	IT	Inactive	Defines board responsibilities and ethical oversight	
Corporate Governance Framework New Modified	IT	Inactive	Defines board responsibilities and ethical oversight	
Corporate Governance Framework New Modified version 1	IT	Active	Defines board responsibilities and ethical oversight version 1	
ISO 9001	Quality Management	Active	ISO 9001 sets the criteria for a quality management system (QMS) and is the only standard that can be certified. It is based on a number of quality management principles including a strong customer focus, the motivation and implication of top management, the process approach, and continual improvement	
ISO 32001	SECURITY	Active	TETSING TO POLICY	
ISO 9001 TAILORED Version	Quality Management	Active	ISO 9001 sets the criteria for a quality management system (QMS) and is the only standard that can be certified. It is based on a number of quality management principles including a strong customer focus, the motivation and implication of top management, the process approach, and continual improvement	

Policy Hierarchy Navigation

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

VERSIONS						
Name	Category	Status	Policy Count	Previous Version	Description	Actions
ISO 27001 v1.0	Information Security	Active	17	N/A	ISO 27001 is the international standard for information security management systems (ISMS), providing a systematic approach to managing sensitive company information, ensuring its confidentiality, integrity, and availability.	

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

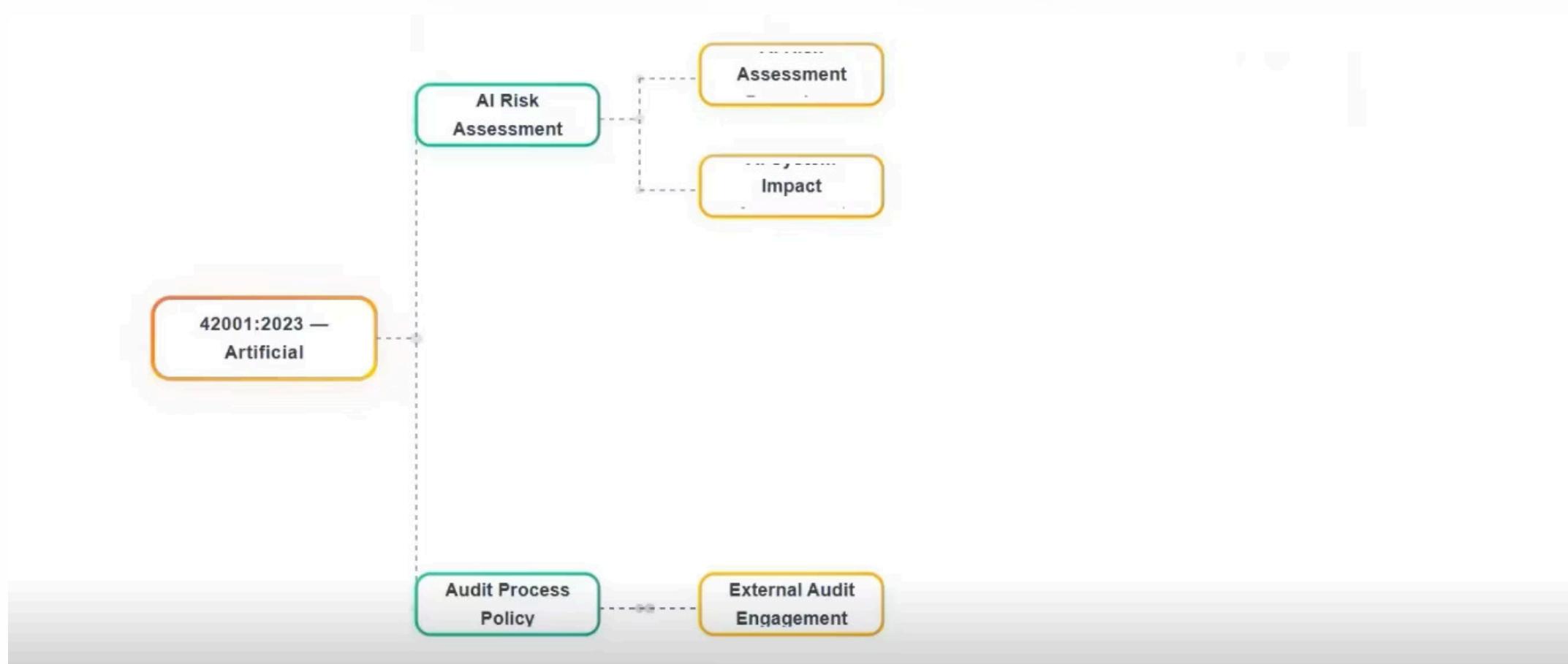
POLICIES					
Name	Category	Status	Versions	Description	Actions
Information Security Policy	Information Security	Approved	1	This policy defines the requirements for establishing, implementing, operating, monitoring, reviewing, and improving the Information Security Management System (ISMS).	
Organization of Information Security Policy	Information Security	Approved	1	Defines the roles, responsibilities, and organizational structure required to manage information security.	
Human Resource Security Policy	Human Resources	Approved	1	Ensures that all employees and contractors understand their roles and responsibilities regarding information security, and are trained accordingly.	
Asset Management Policy	Information Security	Approved	1	Defines the requirements for managing physical and logical assets, including classification and handling of sensitive data and equipment.	
Access Control Policy	Security	Approved	1	Establishes the principles for controlling access to sensitive information and systems.	
Cryptography Policy	Information Security	Approved	1	Defines policies for the use of cryptographic controls to protect information confidentiality and integrity.	
Physical and Environmental Security Policy	Facilities Management	Approved	1	Defines physical security controls to prevent unauthorized access to buildings and IT equipment.	
Operations Security Policy	Operations	Approved	1	Ensures secure operations and protects data during the day-to-day functioning of the organization.	
Communications Security Policy	Information Security	Approved	1	Defines communication security controls to protect data in transit and to prevent unauthorized disclosure.	
System Acquisition, Development, and Maintenance Policy	Development	Approved	1	Outlines the process for acquiring, developing, and maintaining secure information systems throughout their lifecycle.	

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

Create New Policy

Framework *

Framework: Select

Select an existing framework or create a new one to associate with your policy.

Create New Framework

After creating the framework, you can add policies and subpolicies. You can also return to this form later to make corrections.

Framework Name *

Enter Framework name

Enter a descriptive name for your framework

Description *

Enter framework description

0/1000

Describe the purpose, scope, and objectives of this framework

Internal/External *

Select Type

Select whether this framework is for internal or external use

Identifier *

Enter Identifier

Use a unique code like 'FW-001' or 'ISO-27001'

Category *

Enter category

e.g., Security, Compliance, Risk Management, etc.

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

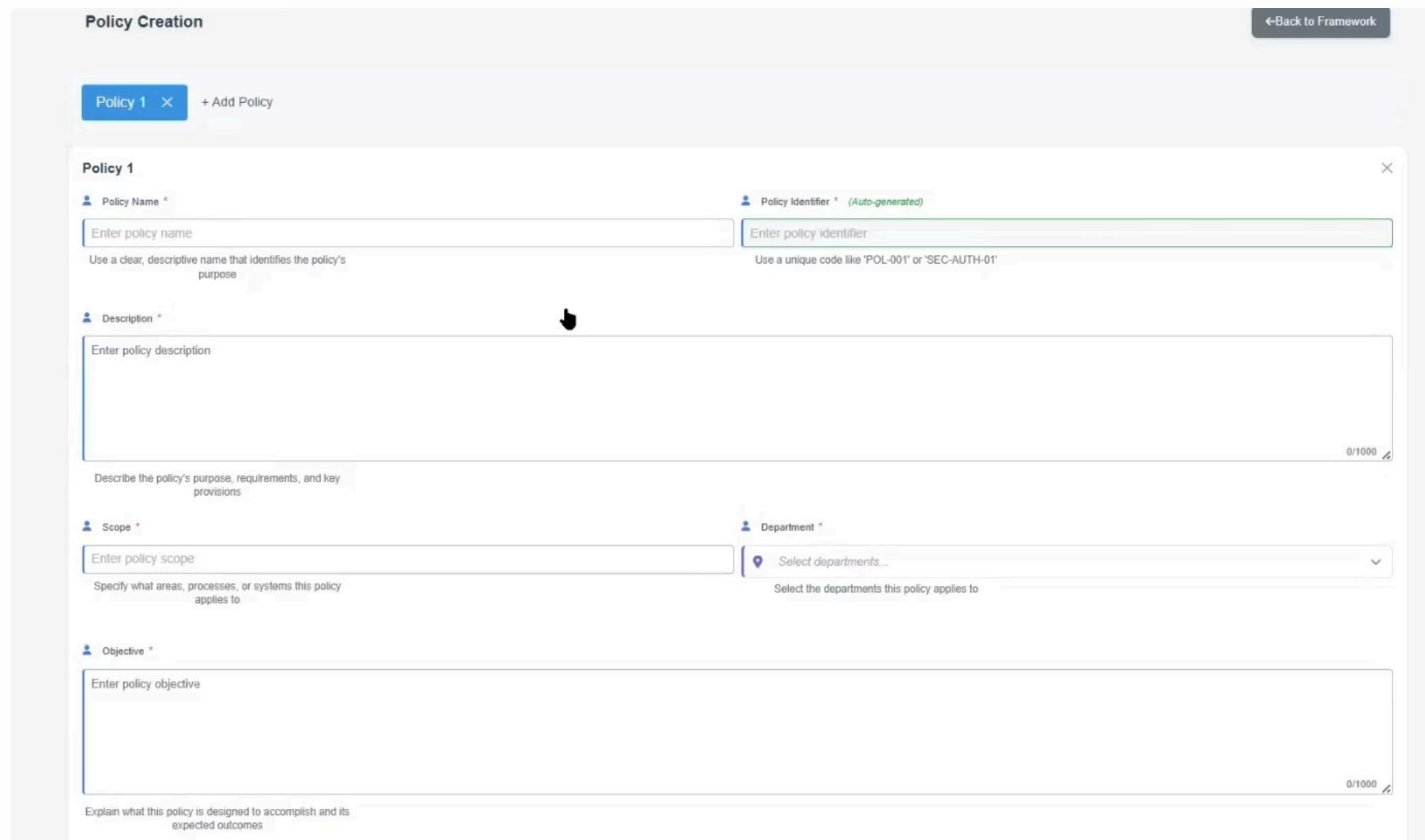
After filling in these details, you can proceed to add Sub-Policies.

Policy Creation ← Back to Framework

Policy 1 X + Add Policy

Policy 1

Policy Name *	Policy Identifier * <small>(Auto-generated)</small>
<input type="text" value="Enter policy name"/> <small>Use a clear, descriptive name that identifies the policy's purpose</small>	<input type="text" value="Enter policy identifier"/> <small>Use a unique code like 'POL-001' or 'SEC-AUTH-01'</small>
Description *	Scope *
<input type="text" value="Enter policy description"/> <small>Describe the policy's purpose, requirements, and key provisions</small>	Department *
Objective *	Objectives
<input type="text" value="Enter policy objective"/> <small>Explain what this policy is designed to accomplish and its expected outcomes</small>	<input type="text" value="Select departments..."/> <small>Select the departments this policy applies to</small>



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.

Subpolicy Creation

Subpolicy 1 X + Add Sub Policy

Sub Policy 1

User Sub Policy Name * Enter sub policy name ?

Use a clear name that describes this sub-policy's specific focus

User Identifier * (Auto-generated) Enter identifier

Use a unique code like 'SUB-001' or append to parent policy ID

User Control * Enter control 0/1000

Specify the control mechanisms, procedures, or safeguards to be implemented

User Description * Enter description

Policy Approval Process

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

1. On the Approvals page, enter:
 - o Created By - Your username
 - o 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

Request Approvals

Created By *
udha.sharma
This policy will be created under your username.

Reviewer *
Select Reviewer
Select the person who will review and approve this framework/policy. This person will receive notification to review the submitted content.

Approval Process

- The selected reviewer will be notified to review your framework and policies
- Once approved, the framework and policies will be activated in the system
- You can track the approval status in the Policies List page
- If changes are needed, the reviewer will provide feedback for updates

Submit for Review

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

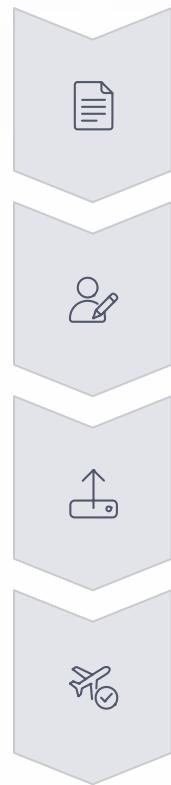
Policy Tailoring

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

The screenshot shows the 'Tailoring & Templating' section of a software application. The left sidebar has a 'Policy' category expanded, with 'Tailoring & Templating' selected. The main area is titled 'Tailoring & Templating' and displays a message: 'Only Internal Frameworks can be tailored'. A navigation bar at the top right has tabs for 'Framework' (which is active) and 'Policy'. Below the tabs, a dropdown menu shows 'Corporate Governance' selected under 'Framework: Framework new (Governance) - Approved'. The form fields include 'FRAMEWORK NAME *' (set to 'Corporate Governance Framework new'), 'DESCRIPTION *' (set to 'Defines board responsibilities and ethical oversight'), and 'IDENTIFIER * (Auto-generated)' (set to 'CORP1'). There is also a 'CATEGORY *' field set to 'Governance'.

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

Policy Versioning

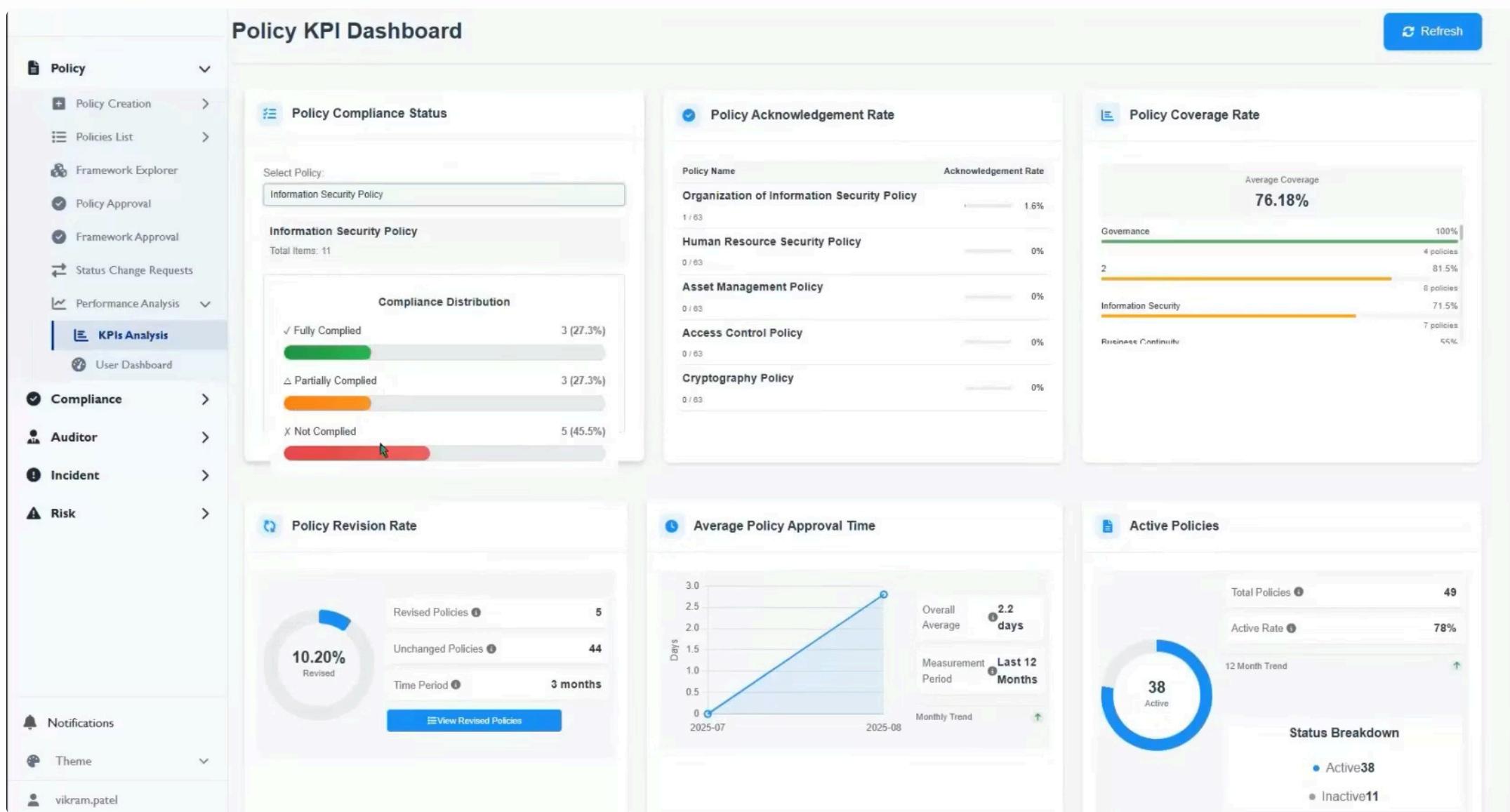
The screenshot shows the 'Policy' section of a software application. On the left is a sidebar with various navigation options under 'Policy' and other categories like 'Compliance', 'Auditor', 'Incident', and 'Risk'. The 'Versioning' option is currently selected. The main area is titled 'Policy Versioning' and shows a 'Framework' tab selected. A dropdown menu indicates the 'Framework: International Organization for Standardization 42001:2023 — Artificial Intelligence Management System' and the 'Policy: AI Risk Assessment'. Below this, a 'Policy 1' card is displayed with fields for 'POLICY NAME *' (AI Risk Assessment), 'POLICY IDENTIFIER * (Auto-generated)' (AITRM-001), 'DESCRIPTION *' (Specifies the process for conducting risk assessments specifically for artificial intelligence (AI) technologies), 'SCOPE *' (Focuses on assessing the risks associated with AI technologies to ensure their safe and secure deployment), 'DEPARTMENT *' (2), and 'OBJECTIVE *' (To identify and evaluate potential risks arising from the use of AI and implement appropriate risk mitigation measures). A note at the bottom says 'Explain what this policy is designed to accomplish'.

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

The screenshot displays the Policy Dashboard interface. On the left, a vertical sidebar menu is visible under the 'Policy' category, listing options like Policy Creation, Policies List, Framework Explorer, Policy Approval, Framework Approval, Status Change Requests, Performance Analysis, KPIs Analysis, and User Dashboard (which is currently selected). Other categories shown include Compliance, Auditor, Incident, and Risk. At the bottom of the sidebar, there is a Notifications section.

The main dashboard area is titled 'Policy Dashboard'. It features several key metrics and visualizations:

- Approval Rate:** 7.66% (Based on 49 policies)
- Active Policies:** 38 (49 total policies)
- Active SubPolicies:** 361 (370 total subpolicies)
- Avg. Approval Time:** 2.2 days (Time to approve)

Below these metrics is a 'Policy Analytics' section with dropdown menus for Framework, All Frameworks, and Category Distribution. A line chart titled 'Artificial Intelligence Management System' tracks a metric across various categories: Artificial Intelligence Management System, Data Protection, Governance, Information Security, IT, Quality Management, and SECURITY. The chart shows a general upward trend followed by a slight decline.

At the bottom of the dashboard, there is a 'Recent Activity' section which is currently empty.

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.

The screenshot shows the 'Control Management' interface with the 'Compliance' module selected in the sidebar. The main area is titled 'SELECT POLICY FRAMEWORK' and contains three dropdown menus: 'Framework' (set to 'Select Framework'), 'Policy' (set to 'Select Policy'), and 'Sub Policy' (set to 'Select Sub Policy'). Below these is a section for 'Compliance Item #1' with fields for 'Identifier' (with a note about auto-generation), 'Is Risk' (checkbox), 'Compliance Title' (text input), 'Compliance Type' (text input), and 'Compliance Description' (text input). The left sidebar also includes sections for 'Auditor', 'Incident', and 'Risk'.

Compliance Approver

Select User to View Tasks:
vikram.patel (GRC Administrator) - ID:2
Currently viewing tasks for vikram.patel

PENDING APPROVALS 0

APPROVED 49

REJECTED 38

My Tasks 1 Reviewer Tasks 1

My Compliance Approval Tasks (Latest Versions)

Latest Versions - Pending

IDENTIFIER	DESCRIPTION	CRITICALITY	CREATED BY	VERSION	ACTIONS
COMP-1094-250804-b11a45	Identify all AI systems within the organization that need to undergo risk assessments	Medium	vikram.patel	1.0	VIEW DETAILS

Results: 1 - 1 of 1

< 1 >

> Latest Versions - Approved

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

The screenshot shows the 'Compliance Tailoring & Templating' page. On the left, there is a navigation sidebar with sections like Policy, Compliance, Tailoring & Templating (which is currently selected), and Auditor. The main content area has a title 'Compliance Tailoring & Templating' and dropdown menus for 'Framework: ISO 27001', 'Policy: Information Security Policy', and 'Sub Policy: Access Control Policy'. Below these is a table titled 'Compliances for Selected Subpolicy' with columns: TITLE, DESCRIPTION, STATUS, VERSION, and ACTIONS. The table contains five rows of compliance details, each with edit and delete icons in the ACTIONS column. At the bottom, it says 'Results: 1 - 5 of 5'.

TITLE	DESCRIPTION	STATUS	VERSION	ACTIONS
User Authentication Mechanisms	Implement user authentication mechanisms such as passwords, biometrics, or smart cards to verify the identity of users accessing information systems.	Approved	1.0	
Role-Based Access Control Implementation	Implement role-based access control to restrict access to information systems based on job responsibilities and authorization levels.	Approved	1.0	
Regular Access Control Reviews	Establish procedures to regularly review and update access control settings to ensure they align with current business requirements and security policies.	Approved	1.0	
Access Control Training Program	Provide training to employees and contractors on access control policies and procedures to ensure awareness and compliance with security measures.	Approved	1.0	
Access Control Monitoring Procedures	Establish monitoring procedures to track the effectiveness and compliance of access control mechanisms on a regular basis.	Approved	1.0	

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.

The screenshot shows a software interface for managing compliance versions. On the left is a vertical navigation sidebar with the following menu items:

- Policy
- Compliance (selected)
- Compliance List
- Control Management
- Compliance Audit Management
- Compliance Approval
- Compliance Creation
- Create Compliance
- Tailoring & Templating
- Versioning (selected)
- Performance Analysis
- Compliance Dashboard
- Compliance KPI
- Auditor
- Audits

The main content area is titled "Compliance Version List". It displays two entries, each with a "Compliance ID":

Compliance ID: ISO2700-I-A-9-I-001
Implement user authentication mechanisms such as passwords, biometrics, or smart cards to verify the identity of users accessing information systems.

VERSION	STATUS	ACTIVE/INACTIVE	CREATED BY	CREATED DATE	PREVIOUS VERSION
1.0	Approved	<input checked="" type="checkbox"/>	priya.gupta	7/1/2025	None

Compliance ID: ISO2700-I-A-9-I-002
Implement role-based access control to restrict access to information systems based on job responsibilities and authorization levels.

VERSION	STATUS	ACTIVE/INACTIVE	CREATED BY	CREATED DATE	PREVIOUS VERSION
1.0	Approved	<input checked="" type="checkbox"/>	radha.sharma	7/1/2025	None

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.

Sub-policy Selection

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

Policy Selection

On the next page, select the relevant Policy.

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.

Control Management

ISO 27001 Information Security Policy Access Control Policy

Compliances in Access Control Policy

ID	CONTROL	STATUS	Criticality	Maturity Level	Type	Version	Created By	Created Date	ACTIONS
ISO27001-A.9.1-001	Implement user authentication mechanisms such as passwords, biometrics, or smart cards to verify the identity of users accessing information systems.	Approved	High	Defined	Mandatory	1.0	priya.gupta	2025-07-01	
ISO27001-A.9.1-002	Implement role-based access control to restrict access to information systems based on job responsibilities and authorization levels.	Approved	Medium	Managed	Mandatory	1.0	radha.sharma	2025-07-01	
ISO27001-A.9.1-003	Establish procedures to regularly review and update access control settings to ensure they align with current business requirements and security policies.	Approved	Medium	Defined	Mandatory	1.0	radha.sharma	2025-07-01	
ISO27001-A.9.1-004	Provide training to employees and contractors on access	Approved	Low	Developing	Mandatory	1.0	vikram.patel	2025-07-01	

Policy

Compliance

- Compliance List
- Control Management**
- Compliance Audit Management
- Compliance Approval
- Compliance Creation
- Create Compliance
- Tailoring & Templating
- Versioning
- Performance Analysis
- Compliance Dashboard
- Compliance KPI

Auditor

- Audits
- Assign Audit
- Review Audits
- Audit Reports
- Performance Analysis

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 Audit Status

ISO 27001 x Information Security Policy x Access Control Policy x

Compliances in Access Control Policy

AUDIT FINDINGS ID	COMPLIANCE	CRITICALITY	COMPLETION ST.	COMPLIANCE PERFORMED BY	COMPLIANCE APPROVED BY	COMPLETION DATE
117	Implement user authentication mechanisms such as passwords, biometrics, or smart cards to verify the identity of users accessing information systems.	High	Fully Compliant	vikram.patel	priya.gupta	2025-08-04
106	Implement role-based access control to restrict access to information systems based on job responsibilities and authorization levels.	Medium	Non Compliant	radha.sharma	radha.sharma	2025-08-04
118	Establish procedures to regularly review and update access control settings to ensure they align with current business requirements and security policies.	Medium	Non Compliant	vikram.patel	priya.gupta	2025-08-04
119	Provide training to employees and contractors on access control policies and procedures to ensure awareness and compliance with security measures.	Low	Partially Compliant	vikram.patel	priya.gupta	2025-08-04
120	Establish monitoring procedures to track the effectiveness and compliance of access control mechanisms on a regular basis.	High	Non Compliant	vikram.patel	priya.gupta	2025-08-04

Audit Report - ID 48

Audit Information

Title: teams testing	Framework: ISO 27001	Policy: Information Security Policy
Sub-Policy: Access Control Policy	Business Unit: Risk Management, Compliance	Auditor: vikram.patel
Reviewer: priya.gupta	Completion Date: N/A	Review Date: 8/4/2025, 2:37:11 PM

Audit Scope & Objective

Scope: dsvdflv rere
Objective: r vrfvrgfbv tgtrlbtrgbglrglbg

Report Details

Report is stored in cloud storage. Click below to download:

[Download Report Document](#)

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.

The screenshot shows the Compliance Dashboard interface. On the left is a vertical sidebar with navigation links for Policy, Compliance (selected), Control Management, Compliance Audit Management, Compliance Approval, Compliance Creation, Tailoring & Templating, Versioning, Performance Analysis (selected), and Incident. The main area has a title 'Compliance Dashboard'. It features four cards: 'APPROVAL RATE' (99.83% based on 593 compliances), 'ACTIVE COMPLIANCE' (590 Active and Approved), 'TOTAL FINDINGS' (566 Across all compliances), and 'UNDER REVIEW' (1 Pending review). Below these is a section titled 'Compliance Analytics' with a bar chart titled 'Compliance by Criticality' showing counts for High (red), Medium (orange), and Low (green) criticality levels. To the right is a 'Recent Activity' feed with two entries: 'Compliance Approved' (Unknown Compliance approved by reviewer, 2 days ago) and another 'Compliance Approved' entry (Unknown Compliance approved by reviewer, Unknown time).

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.

Maturity & Status

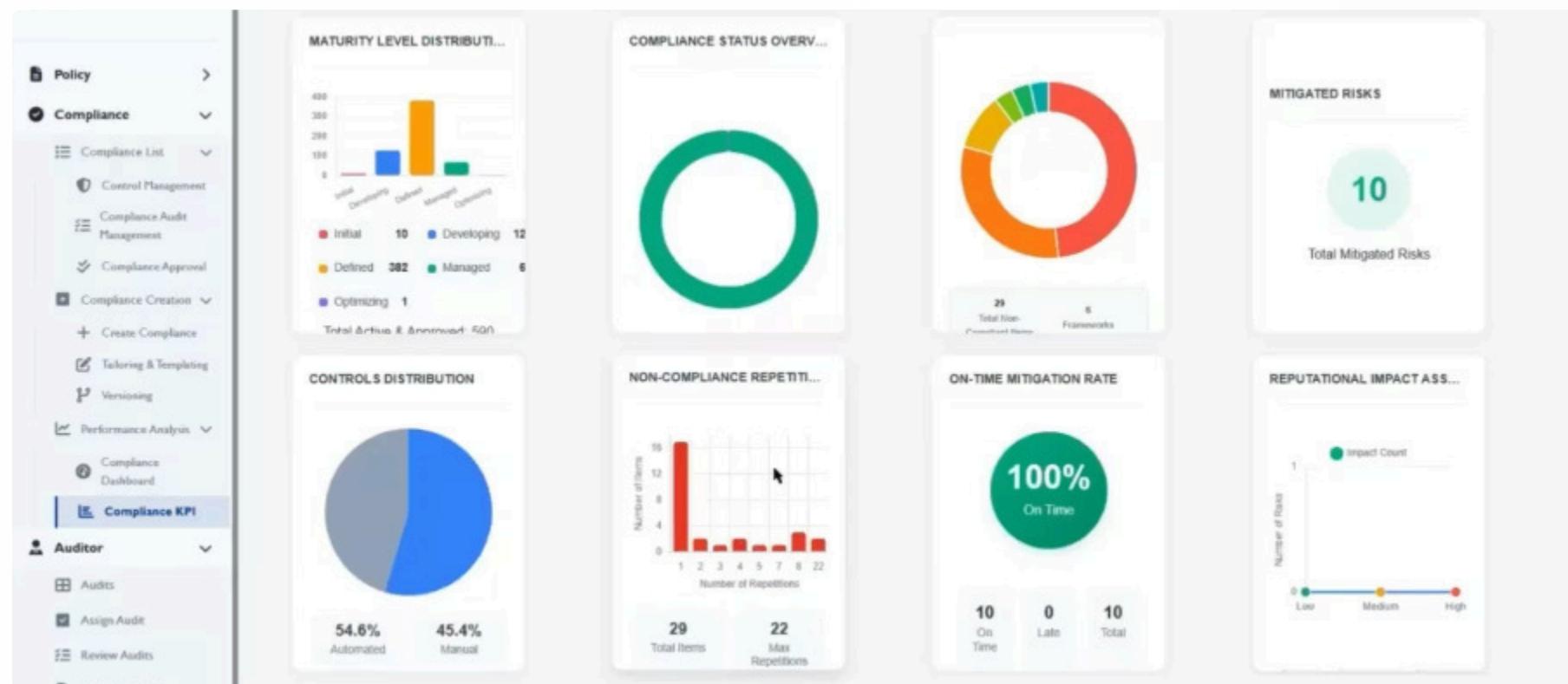
- 1
- Maturity Level Distribution across stages: Initial, Developing, Defined, Managed, Optimizing
 - Compliance Status Overview showing approval status
 - Controls Distribution showing Automated vs. Manual proportions

Non-Compliance Analysis

- 2
- 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)

Risk & Impact

- 3
- 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).

The screenshot shows the 'Audit Assignment' interface. On the left is a sidebar with navigation links: Policy, Compliance, Auditor (selected), Audits (selected), Assign Audit (selected), Review Audits, Audit Reports, Performance Analysis, Incident (selected), Incident Management, Performance Analysis, and Risk. The main area is titled 'Audit Assignment' and shows the 'Framework Selection' step. It has four tabs: Framework Selection (selected), Team Creation (2), Policy Assignment (3), and Review & Assign (4). The 'Framework Selection' tab contains fields for 'Framework' (set to ISO 27001) and 'Audit Type' (a dropdown menu labeled 'Select Type'). A note below says 'Will include permanent compliances from all policies and subpolicies under this framework'. At the bottom right is a 'Next' button.

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.

The screenshot shows the 'Team Creation' step of the audit assignment process. On the left, a sidebar menu includes 'Policy', 'Compliance', 'Auditor' (selected), 'Assign Audit' (highlighted in blue), 'Review Audits', 'Audit Reports', 'Performance Analysis', 'Incident', 'Incident Management', 'Performance Analysis', and 'Risk'. The main area has tabs: 'Framework Selection' (step 1), 'Team Creation' (step 2, currently active), 'Policy Assignment' (step 3), and 'Review & Assign' (step 4). The 'Team Creation' tab has a sub-step indicator '2'. The 'Team Creation' form contains fields: 'Auditor' (dropdown: 'Auditor: vikram.patel'), 'Role' (dropdown: 'Role: Select Role' with options like 'Chief Audit Executive (CAE) / Audit Director', 'Audit Manager', 'Senior Audit Manager', 'IT Audit Manager', 'Operational Audit Manager', 'Compliance Audit Manager', 'Senior Auditor', 'Lead Auditor', 'Financial Auditor', 'Operational Auditor', and 'IT Systems Auditor'), and 'Primary Responsibilities' (text input field: 'Enter responsibilities...'). Navigation buttons 'Previous' and 'Next' are at the bottom.

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.

The screenshot shows the 'Policy Assignment & Audit Details' page. The top navigation bar includes 'Framework Selection 1', 'Team Creation 2', 'Policy Assignment 3' (highlighted in blue), and 'Review & Assign 4'. The left sidebar menu includes: Policy, Compliance, Auditor (with sub-options: Audits, Assign Audit selected, Review Audits, Audit Reports, Performance Analysis), Incident (with sub-options: Incident Management, Performance Analysis), and Risk. The main content area is titled 'Policy Assignment & Audit Details' and displays the following sections:

- POLICY ASSIGNMENT**: Contains three dropdown menus:
 - Assigned Policy: Select Policy
 - Sub Policy: Select Sub Policy
 - Reviewer: Select ReviewerA blue 'Attach Reports' button is located below these fields.
- AUDIT DETAILS**: Contains four input fields:
 - Audit Title: Enter a concise title for this audit assignment. (Input field: Enter audit title...)
 - Business Unit: Select one or more business units for this audit. (Input field: Select business units or type to add now...)
 - Scope: Specify the boundaries and extent of the audit. (Input field: Scope)
 - Objective: State the main goals or objectives of the audit. (Input field: Objective)

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.

Audit Dashboard

AUDIT ID	FRAMEWORK	POLICY	SUBPOLICY	AUDITOR	DUUE DATE	PROGRESS	REVIEWER	AUDIT TYPE	STATUS	ACTIONS
37	ISO 9001	N/A		vikram.patel	03/07/2025	25%	radha.sharma	Internal	Completed	<button>REPORTS</button> <button>VERSIONS</button>
38	ISO 32001	N/A	Physical Access Control	vikram.patel	18/07/2025	67%	radha.sharma	Internal	Completed	<button>REPORTS</button> <button>VERSIONS</button>
44	ISO 27001	Information Security Policy	Access Control Policy	vikram.patel	18/07/2025	0%	priya.gupta	Internal	<button>Start</button>	<button>REPORTS</button>
48	ISO 27001	Information Security Policy	Access Control Policy	vikram.patel	07/08/2025	25%	priya.gupta	Internal	Completed	<button>REPORTS</button> <button>VERSIONS</button>
47	ISO 27001	Information Security Policy	Access Control Policy	vikram.patel	08/08/2025	0%	radha.sharma	Internal	Under review	<button>REPORTS</button>

Results: 1 - 5 of 5

10

1 2

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.

The screenshot shows the 'Compliance Items' section of the audit application. On the left, there's a sidebar with navigation links for Auditor (Audits, Assign Audit, Review Audits, Audit Reports, Performance Analysis), Incident (Incident Management, Performance Analysis), and Risk (Risk Management). The main area has a title 'Compliance Items' with a '+ Add Compliance' button. Below it, tabs for 'Compliance 1' through 'Compliance 5' are visible. A large text area contains the instruction: 'Implement user authentication mechanisms such as passwords, biometrics, or smart cards to verify the identity of users accessing information systems.' Underneath, there are several input fields and dropdown menus:

- Compliance Status: 'Not Compliant' (selected)
- Type of Findings: 'Select Type'
- Severity Rating (1-10): Input field
- What to Verify: Input field
- How to Verify: Input field
- Impact: Input field
- Why to Verify: Input field
- Details of Findings: Input field
- Underlying Cause: Input field
- Predictive Risks: A list including 'Failure to encrypt sensitive data before storage (IT Security)', 'Improper handling of sensitive information may lead to leaks (IT Security)', 'Failure to train employees on data security practices (IT Security)', and 'Inadequate data classification leads to exposure (IT Security)'. A note says 'Select risks to view corrective actions'.
- Corrective Actions: A placeholder text 'Select risks to view corrective actions'.
- Suggested Action Plan: Input field
- Responsible for Plan: Input field
- Mitigation Date: Input field (dd-mm-yyyy)

At the bottom right is a blue 'Save Changes' button.

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.

The screenshot shows a user interface for managing audits. On the left is a sidebar with navigation links: Policy, Compliance, Auditor (with sub-links Audits and Assign Audit), Review Audits (which is selected and highlighted in blue), Audit Reports, Performance Analysis, Incident, and Risk. The main area has a header with a 'Filter by Status: All Statuses' dropdown. Below is a table with the following columns: ID, FRAMEWORK, POLICY, SUBPOLICY, AUDITOR, DUE DATE, AUDIT STATUS, REVIEW STATUS, and DOWNLOAD. The table contains six rows of audit data. Row 37: ID 37, FRAMEWORK ISO 92001, POLICY All Policies, SUBPOLICY All Subpolicies, AUDITOR vikram.patel, DUE DATE 03/07/2025, AUDIT STATUS Completed, REVIEW STATUS Accept Approved, DOWNLOAD button. Row 38: ID 38, FRAMEWORK ISO 32001, POLICY All Policies, SUBPOLICY Physical Access Control, AUDITOR vikram.patel, DUE DATE 18/07/2025, AUDIT STATUS Completed, REVIEW STATUS Accept Approved, DOWNLOAD button. Row 39: ID 39, FRAMEWORK ISO 32001, POLICY All Policies, SUBPOLICY Physical Access Control, AUDITOR priya.gupta, DUE DATE 18/07/2025, AUDIT STATUS Yet to Start, REVIEW STATUS Yet to Start, DOWNLOAD button. Row 40: ID 40, FRAMEWORK ISO 27001, POLICY All Policies, SUBPOLICY Physical Access Control, AUDITOR radha.sharma, DUE DATE 24/07/2025, AUDIT STATUS Completed, REVIEW STATUS Accept Approved, DOWNLOAD button. Row 46: ID 46, FRAMEWORK ISO 27001, POLICY Information Security Policy, SUBPOLICY Access Control Policy, AUDITOR radha.sharma, DUE DATE 06/08/2025, AUDIT STATUS Completed, REVIEW STATUS Accept Approved, DOWNLOAD button. Row 47: ID 47, FRAMEWORK ISO 27001, POLICY Information Security Policy, SUBPOLICY Access Control Policy, AUDITOR vikram.patel, DUE DATE 06/08/2025, AUDIT STATUS Under review, REVIEW STATUS Start, DOWNLOAD button. At the bottom of the table, it says 'Results: 1 - 6 of 6'. There are also navigation buttons for page 10 and a search bar.

ID	FRAMEWORK	POLICY	SUBPOLICY	AUDITOR	DUE DATE	AUDIT STATUS	REVIEW STATUS	DOWNLOAD
37	: ISO 92001	All Policies	All Subpolicies	vikram.patel	03/07/2025	Completed	Accept Approved	
38	ISO 32001	All Policies	Physical Access Control	vikram.patel	18/07/2025	Completed	Accept Approved	
39	ISO 32001	All Policies	Physical Access Control	priya.gupta	18/07/2025	Yet to Start	Yet to Start	
40		All Policies	Physical Access Control	radha.sharma	24/07/2025	Completed	Accept Approved	
46	ISO 27001	Information Security Policy	Access Control Policy	radha.sharma	06/08/2025	Completed	Accept Approved	
47	ISO 27001	Information Security Policy	Access Control Policy	vikram.patel	06/08/2025	Under review		

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.

Policy	>							
Compliance	>							
Auditor	▼							
Audits								
Assign Audit								
Review Audits								
Audit Reports								
Performance Analysis	>							
Incident	>							
Risk	>							
AUDIT ID	▼							
FRAMEWORK	▼							
POLICY	▼							
SUB POLICY	▼							
ASSIGNED	▼							
AUDITOR	▼							
REVIEWER	▼							
COMPLETED DATE	▼							
REPORTS								
37	: ISO 92001			vikram.patel	vikram.patel	radha.sharma		<button>View Reports</button>
38	ISO 32001		Physical Access Control	vikram.patel	vikram.patel	radha.sharma		<button>View Reports</button>
41	: ISO 92001			radha.sharma	radha.sharma	vikram.patel		<button>View Reports</button>
42	ISO 27001	Information Security Policy	Incident Response Policy	radha.sharma	radha.sharma	vikram.patel		<button>View Reports</button>
43	ISO 27001	Information Security Policy	Access Control Policy	radha.sharma	radha.sharma	priya.gupta		<button>View Reports</button>
46	ISO 27001	Information Security Policy	Access Control Policy	radha.sharma	radha.sharma	radha.sharma		<button>View Reports</button>
48	ISO 27001	Information Security Policy	Access Control Policy	vikram.patel	vikram.patel	priya.gupta		<button>View Reports</button>
50	ISO 27001	Information Security Policy	Access Control Policy	radha.sharma	radha.sharma	vikram.patel		<button>View Reports</button>

Results: 1 - 8 of 8

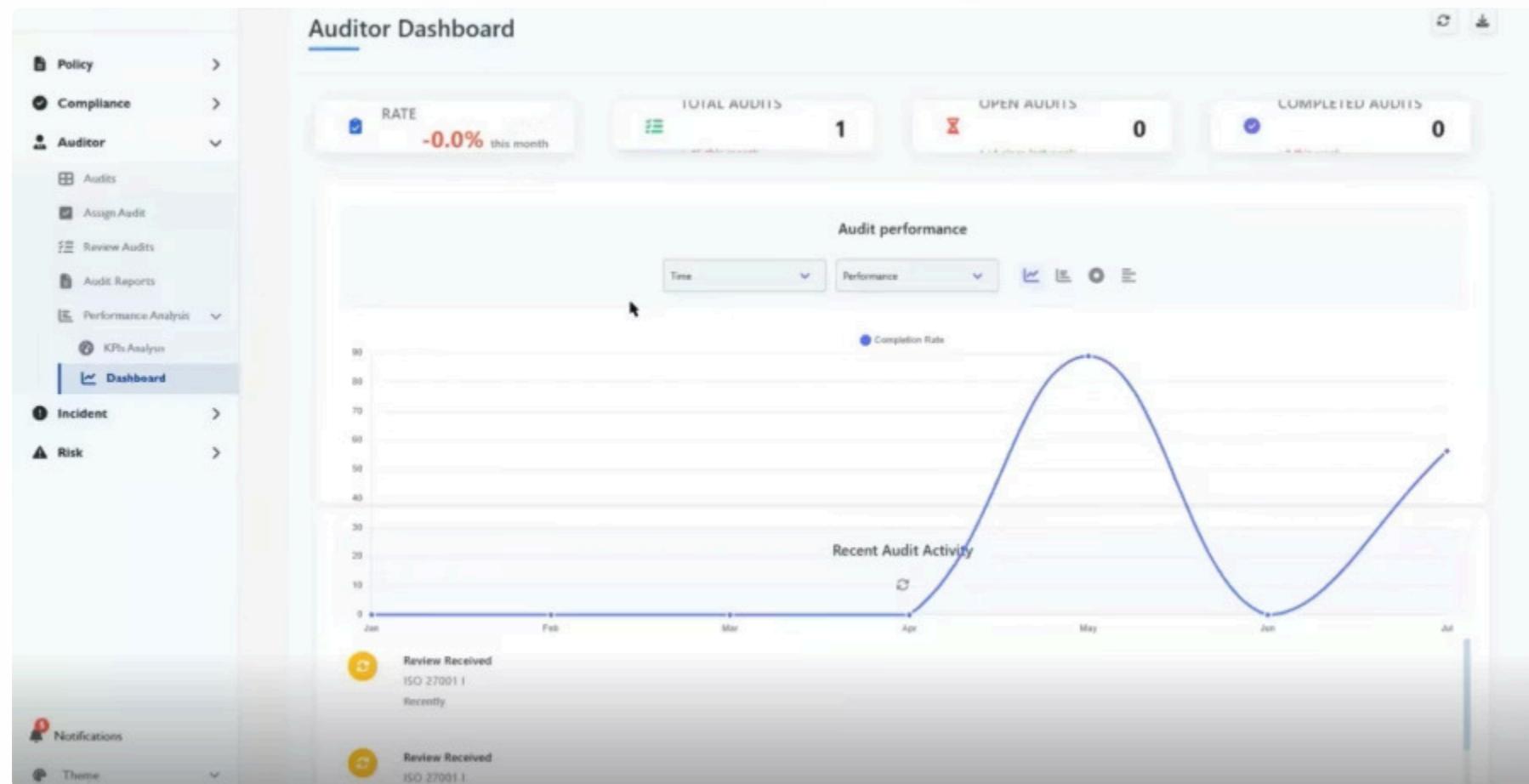
10

< 1 >

Performance Analysis: Dashboard

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

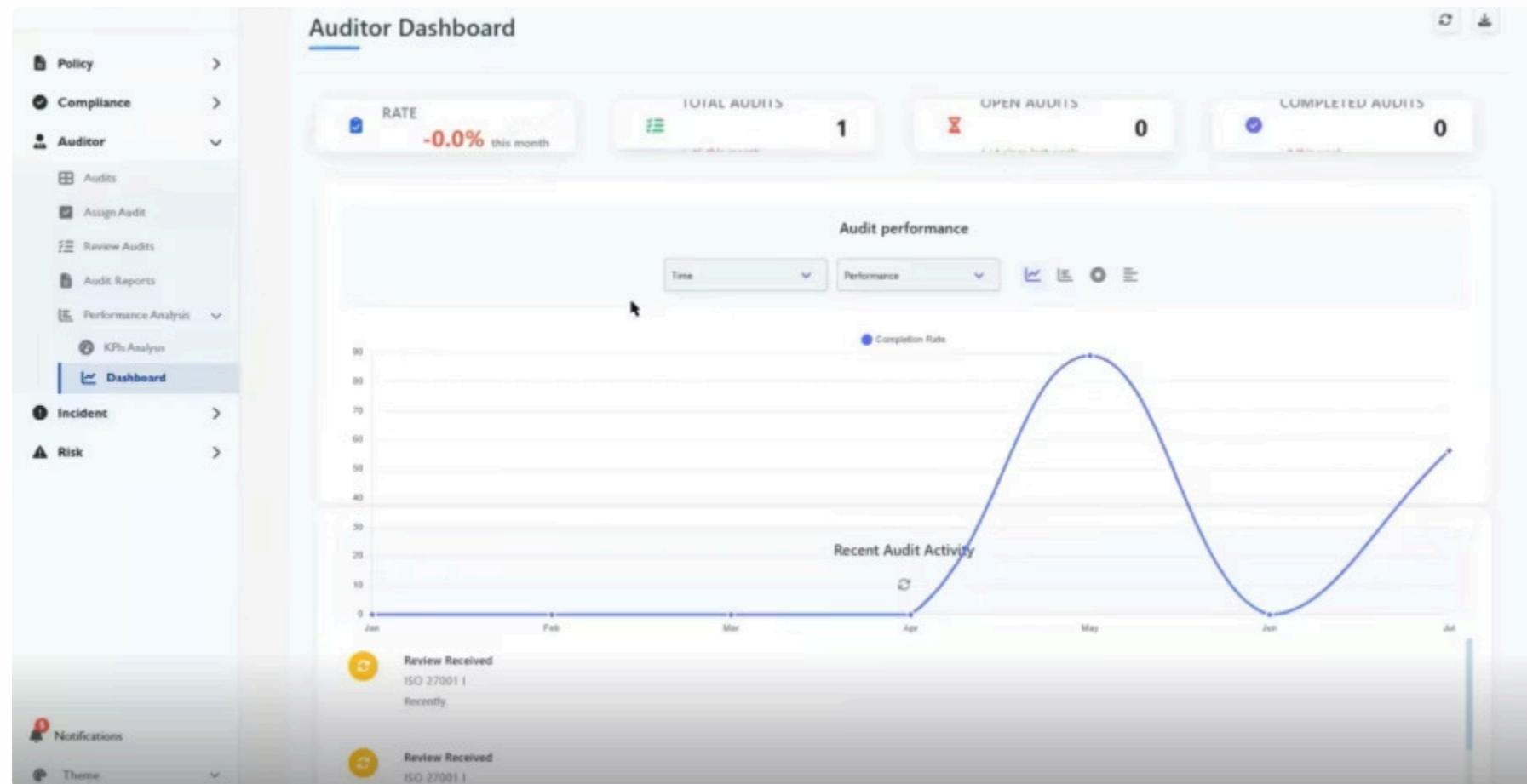
The Auditor Dashboard provides a quick snapshot of audit performance, helping users monitor overall progress, completion trends, and recent activity. The top section highlights key metrics including rate changes, total audits, open audits, and completed audits. A performance graph shows completion rates 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.

The screenshot shows the 'Incident List' page within a larger application interface. On the left, there's a sidebar with navigation links for Policy, Compliance, Auditor, Incident (selected), Incident Management (selected), Risk, and Notifications. The main area has a search bar at the top with placeholder text 'Search by ID, title, origin, priority, category, or status...'. Below it are three filter buttons: 'All Frameworks', 'All Policies', and 'All Subpolicies'. A 'Clear All Filters' button is also present. The central part of the screen is a table with the following columns: ID, TITLE, ORIGIN, PRIORITY, DATE, and ACTIONS. The table contains 15 rows of incident data. The first few rows are Audit Findings, while the last few are Manual entries. The 'Actions' column contains icons for viewing, updating, and deleting each incident.

ID	TITLE	ORIGIN	PRIORITY	DATE	ACTIONS
302	Non-Compliance of Access Control Mo...	Audit Finding		08/04/2025	
301	Non-Compliance of Access Control Tra...	Audit Finding		08/04/2025	
300	Non-Compliance of Regular Access Co...	Audit Finding		08/04/2025	
299	Non-Compliance of Regular Access Co...	Audit Finding		08/04/2025	Mitigated to Risk
298	Non-Compliance of Role-Based Acces...	Audit Finding		08/04/2025	Mitigated to Risk
296	Non-Compliance of Access Control Tra...	Audit Finding		07/25/2025	Risk Mitigated
295	Non-Compliance of Regular Access Co...	Audit Finding		07/25/2025	Risk Mitigated
294	Non-Compliance of User Authenticatio...	Audit Finding		07/25/2025	In Progress
292	laptop	Manual	Medium	07/24/2025	
291	dfghjk	Audit Finding	Low	07/14/2025	In Progress
290	Non-Compliance of Access Control Mo...	Audit Finding		07/14/2025	Approved
289	Non-Compliance of Access Control Tra...	Audit Finding		07/14/2025	Mitigated to Risk
288	Non-Compliance of Regular Access Co...	Audit Finding		07/14/2025	Mitigated to Risk
287	Non-Compliance of Role-Based Acces...	Audit Finding		07/14/2025	Approved

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

The screenshot shows the Audit Findings module within a larger application. On the left is a vertical navigation sidebar with links for Policy, Compliance, Auditor, Incident (selected), Incident Management (with sub-links for Incident List and Create Incident), Audit Findings (selected), User Tasks, Performance Analysis, Risk, Notifications, Theme, and a user profile for radhu.sharma.

The main area is divided into two sections: a summary dashboard at the top and a detailed incident list below.

Summary Dashboard: This section features a horizontal bar with six colored boxes representing different incident statuses: Open (3), Assigned (3), Closed (9), Rejected (2), Mitigated to Risk (15), and Total Incidents (36). Below this is a search bar and two dropdown menus for Status (All Status) and Sort By (Date (Newest First)).

Incident List: This section displays a table of audit findings. The columns are: Incident ID, Title, Priority, Status, Origin, Date, Time, Description, and Actions. The table contains five rows of data, each with a "VIEW DETAILS" button in the Actions column.

Incident ID	Title	Priority	Status	Origin	Date	Time	Description	Actions
302	Non-Compliance of Access Control Monitoring Procedures	N/A	OPEN	Audit Finding	Aug 4, 2025, 05:30 AM	14:37:14	Establish monitoring procedures to track the effec...	VIEW DETAILS
301	Non-Compliance of Access Control Training Program	N/A	OPEN	Audit Finding	Aug 4, 2025, 05:30 AM	14:37:14	Provide training to employees and contractors on a...	VIEW DETAILS
300	Non-Compliance of Regular Access Control Reviews	N/A	OPEN	Audit Finding	Aug 4, 2025, 05:30 AM	14:37:14	Establish procedures to regularly review and updat...	VIEW DETAILS
299	Non-Compliance of Regular Access Control Reviews	N/A	SCHEDULED	Audit Finding	Aug 4, 2025, 05:30 AM	10:55:44	Establish procedures to regularly review and updat...	VIEW DETAILS
298	Non-Compliance of Role-Based Access Control Implementation	N/A	SCHEDULED	Audit Finding	Aug 4, 2025, 05:30 AM	10:55:44	Implement role-based access control to restrict ac...	VIEW DETAILS

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.

The screenshot shows a software interface for managing user tasks. On the left is a navigation sidebar with links to Policy, Compliance, Auditor, Incident (selected), Incident Management (with sub-links for Incident List, Create Incident, and Audit Findings), User Tasks (selected), Performance Analysis, and Risk. At the bottom is a Notifications section with a red notification icon. The main area has a search bar and a dropdown menu for selecting a user, currently set to 'radha.sharma (Security Analyst)'. Below this are buttons for 'My Tasks (26)' and 'Reviewer Tasks (7)', with 'Reviewer Tasks' being highlighted. A table lists several incidents with columns for ID, Title, Origin, Priority, Assigned By, and Actions. Each row includes a 'VIEW DETAILS' button in the Actions column. The table shows incidents like 'incident title' (Audit Finding, Medium priority, 2 assigned), 'dfg' (Manual, High, 2), 'vajyfg' (Audit Finding, Low, 2), 'Non-Compliance of Testing of Incident Response Plan' (Audit Finding, 2), and 'Non-Compliance of Access Control Monitoring Procedures' (Audit Finding, 3). The entire interface has a light blue background with white and grey UI elements.

ID	Title	Origin	Priority	Assigned By	Actions
244	incident title	Manual	High	2	<button>VIEW DETAILS</button>
252	dfg	Manual	Medium	2	<button>VIEW DETAILS</button>
253	vajyfg	Audit Finding	Low	2	<button>VIEW DETAILS</button>
285	Non-Compliance of Testing of Incident Response Plan	Audit Finding		2	<button>VIEW DETAILS</button>
290	Non-Compliance of Access Control Monitoring Procedures	Audit Finding		3	<button>VIEW DETAILS</button>

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.

Create New Incident

INCIDENT OVERVIEW

INCIDENT TITLE *
e.g., Database Server Outage, Unauthorized Access to Customer Data, Phisher

DESCRIPTION *
Describe what happened in detail: What was the nature of the incident? How was it discovered? What systems or processes were affected? Include timeline if known. Be specific about the sequence of events, who discovered it, and immediate actions taken...

Generate Analysis

ORIGIN
Select how incident was discovered...

DATE *
dd-mm-yyyy

TIME *

RISK PRIORITY *
Assess the severity level of this incident...

RISK CATEGORY *
SELECT CATEGORIES OR TYPE TO ADD NEW...

Criticality
Rate the overall criticality level...

COST OF INCIDENT
e.g., \$50,000, €25,000.00, 100000 (estimated financial impact)

POSSIBLE DAMAGE
Describe potential damage: Data loss, customer trust impact, regulatory fines, business disruption, reputation damage, legal liability, service outages, security vulnerabilities exposed...

BUSINESS UNIT
SELECT BUSINESS UNITS OR TYPE TO ADD NEW...

LOCATION
e.g., New York Office, London Branch, Remote/Cloud, Data Center - Dallas, Building

SYSTEMS INVOLVED
e.g., Customer CRM, Payment Gateway, Email Server, Database XYZ, Network in

INCIDENT CLASSIFICATION
Classify the type of incident...

Notifications

Theme

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 Open Rejected Approved

Incidents

Complete count of all incidents in the system

Incidents

Awaiting resolution or action

Incidents

Not approved during review

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.

The screenshot displays the Incident Dashboard interface. On the left, a sidebar navigation menu includes links for Policy, Compliance, Auditor, Incident (selected), Incident Management (with sub-links for Incident List, Create Incident, Audit Findings, User Tasks), Performance Analysis (with sub-links for KPIs Analysis, Dashboard), and Risk. At the bottom of the sidebar are links for Notifications and Theme.

The main content area is titled "Incident Dashboard". It features four large status boxes: "TOTAL INCIDENTS" (120, -68.3% from last period), "OPEN INCIDENTS" (55, Awaiting resolution), "REJECTED" (16, Rejected incidents), and "APPROVED" (21, Approved incidents). Below these is an "Incident Analytics" section containing a bar chart showing the distribution of incidents by severity level: High (red bar, value 26), Medium (orange bar, value 35), and Low (green bar, value 21). The X-axis is labeled "Incidents" and the Y-axis ranges from 0 to 36. To the right of the chart is a "Recent Incidents" section listing three audit findings:

- Non-Compliance of Access Control Training Program: Provide training to employees and contractors on access control policies and procedures to ensure aw... (Audit Finding, Scheduled, 3 days ago)
- Non-Compliance of Regular Access Control Reviews: Establish procedures to regularly review and update access control settings to ensure they align wit... (Audit Finding, 3 days ago)
- Non-Compliance of Access Control Monitoring Procedures: Establish monitoring procedures to track the effectiveness and compliance of access control mechanis... (Audit Finding, 3 days ago)

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.

The screenshot shows the 'Risk Register List' page. On the left is a sidebar with navigation links: Policy, Compliance, Auditor, Incident, Risk (with 'Risk Register' expanded), Risk Register List (selected), Create Risk, Risk Instances, Risk Handling, Risk Analytics, Notifications, and Theme. The main area has a title 'Risk Register List' and a search bar. Below it are filters for 'Criticality: All Criticality' and 'Category: All Category'. A table lists 138 risks. The columns are: RISK ID, RISK TITLE, RISK TYPE, COMPLIANCE ID, CATEGORY, CRITICALITY, and ACTIONS. Each row contains a 'VIEW RISK' button. At the bottom, there's a footer with 'Results: 1 - 10 of 138', a page number '10', a help icon, and a navigation bar with pages 1, 2, 3, ..., 14, >.

RISK ID	RISK TITLE	RISK TYPE	COMPLIANCE ID	CATEGORY	CRITICALITY	ACTIONS
139	Non-Compliance of Role-Based Access Control Implementation	Current	1007	People Risk	Critical	<button>VIEW RISK</button>
136	Non-Compliance of morning compliance	Current	1609	People Risk	High	<button>VIEW RISK</button>
137	laptop	Current	1006	People Risk	High	<button>VIEW RISK</button>
138	laptop	Current	1007	Operational	Medium	<button>VIEW RISK</button>
135	wednesday testing	Current	1048	People Risk	Medium	<button>VIEW RISK</button>
133	tuesday modified	Current	1006	People Risk	High	<button>VIEW RISK</button>
134	tuesday tailored	Current	1006	People Risk	High	<button>VIEW RISK</button>
128	laptop	Current	65	People Risk	Medium	<button>VIEW RISK</button>
129	00000000000000000000	Current	30	People Risk	Critical	<button>VIEW RISK</button>
130	oooooooooooooooooooo	Emerging	4	Process Risk	Critical	<button>VIEW RISK</button>

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.

The screenshot shows the Risk Details page with the following data:

Risk Details	
Risk ID:	139
Non-Compliance of Role-Based Access Control Implementation	
Compliance ID:	1007
Risk Description:	Implement role-based access control to restrict access to information systems based on job responsibilities and authorization levels.
Business Impact:	Revenue Loss
Possible Damage:	Implement role-based access control to restrict access to information systems based on job responsibilities and authorization levels.
Risk Likelihood:	8
Risk Impact:	6
Risk Exposure Rating:	48
Risk Priority:	High
Risk Mitigation:	step1 step 2 step 3
Risk Type:	Current
Created At:	8/4/2025

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.

The screenshot shows the 'Risk Scoring' page with a sidebar menu on the left. The sidebar includes links for Policy, Compliance, Auditor, Incident, Risk (with sub-links for Risk Register List, Create Risk, Risk Instances List, Create Instance, and Risk Scoring), Risk Handling, and Risk Analytics. A black arrow points to the 'Risk Scoring' link in the Risk section. The main area has a search bar and filters for Status (All Status) and Category (All Categories). Below is a table with the following data:

RISK INSTANCE ID	INCIDENT ID	COMPLIANCE ID	RISK TITLE	CATEGORY	STATUS	RISK DESCRIPTION	ACTIONS
8	1	6	gsdgrht	Security	ASSIGNED	Access logs showed privilege misuse from internal ...	Scoring Com
12	2	5	slhretgxdtf	Operational	REJECTED	Encryption policy violation detected during vulner...	Instance Rep
13	3	4	gdngdf	Access Control	ASSIGNED	Audit revealed non-compliance on multiple user acc...	Scoring Com
15	5	1	gdttryj	Device Security	APPROVED	Reported device loss led to review of mobile devic...	Scoring Com
16	6		dntrjy	Third-Party Risk	NOT SET	Audit review showed expired documentation.	Accept Reject
67		1	Unauthorized access to sensitive data	IT Security	ASSIGNED	This policy outlines data protection requirements...	Scoring Com
68	4	1	fsdgfgui	People Risk	APPROVED	sdighul	Scoring Com

At the bottom, it says 'Results: 1 - 7 of 28' and has navigation buttons for pages 1 through 4.

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."

The screenshot shows the 'Scoring Details' page for Risk Instance #89. The left sidebar navigation includes Policy, Compliance, Auditor, Incident, Risk (selected), Risk Register (with sub-options: Risk Register List, Create Risk), Risk Instances (with sub-options: Risk Instances List, Create Instance, Risk Scoring), Risk Handling, and Risk Analytics.

The main content area is titled 'Scoring Details' and shows 'Risk Instance #89'. It has a header 'Basic Risk Information' with fields for Risk Instance Id (89), Incident Id (301), Compliance Id (1009), Risk Title (Non-Compliance of Access Control Training Program), Criticality, Risk Status, Category (Select Category), Possible Damage (Lack of awareness leading to security incidents or breaches), Risk Priority (Select Priority), Reported By (2), Origin, and Risk Description (Provide training to employees and contractors on access control policies and procedures to ensure awareness and compliance with security measures). A note at the bottom states 'Provide a detailed description of the risk, its context, and contributing factors.'

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.

The screenshot displays the 'Create Risk' form with the following sections:

- Manual Creation** tab is selected.
- Risk Classification** section:
 - # Compliance ID: Enter or select compliance ID.
 - Select the compliance requirement this risk is associated with:
 - Criticality: Select Criticality (dropdown).
 - Category: Select Category (dropdown).
 - Risk Priority: Select Priority (dropdown).
 - Risk Type: Current (dropdown).
 - Risk Description: Provide a detailed description of the risk.
- Risk Assessment** section:
 - Risk Likelihood (1–10): Rate how likely this risk is to occur (1 = Very Unlikely, 10 = Very Likely).
 - Risk Impact (1–10): Rate the potential impact if this risk occurs (1 = Minimal, 10 = Severe).
 - Risk Exposure Rating: Automatically calculated as Risk Likelihood × Risk Impact.
 - Possible Damage: Describe the potential damage or consequences.
 - Risk Mitigation Actions: Add specific actions to mitigate or eliminate this risk.
- Risk Description** section:
 - Risk Title: Enter a clear, concise risk title.
- Buttons**: Create Risk (blue button), Reset Form (grey button).

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

Risk Instances						
<input type="text" value="Search risk instances..."/>						
<input type="button" value="CRITICALITY: All Criticality"/> <input type="button" value="STATUS: All Status"/> <input type="button" value="CATEGORY: All Category"/> <input type="button" value="PRIORITY: All Priority"/>						
<input type="button" value="RISK ID: Select Risk ID"/>						
RISK ID	RISK DESCRIPTION	ORIGIN	CATEGORY	CRITICALITY	RISK STATUS	ACTIONS
12	Access logs showed privilege misuse from internal IP.	MANUAL	Security	High	Assigned	<input type="button" value="VIEW INSTANCE"/>
10	Encryption policy violation detected during vulnerability scan.	MANUAL	Operational	Medium	Rejected	<input type="button" value="VIEW INSTANCE"/>
7	Audit revealed non-compliance on multiple user accounts.	MANUAL	Access Control	Medium	Assigned	<input type="button" value="VIEW INSTANCE"/>
115	Reported device loss led to review of mobile device policies.	MANUAL	Device Security	High	Approved	<input type="button" value="VIEW INSTANCE"/>
N/A	Audit review showed expired documentation.	MANUAL	Third-Party Risk	Medium	Open	<input type="button" value="VIEW INSTANCE"/>

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

Create Risk Instance

Enter or select risk ID

Criticality **Category** **Appetite** Yes

Risk Likelihood **Risk Impact** **Risk Exposure Rating** Automatically calculated in Likelihood x Impact

Risk Priority **Mitigate** **Risk Owner**

Risk Status **Risk Title** **Business Impact**

Origin **Compliance ID** **Risk Type**

Select the business areas that would be affected by this risk

Source of this risk instance (Manual, SEM, Audit Findings)

Link this risk instance to a specific compliance requirement

Classify the nature and lineage of this risk

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.

The screenshot shows the Risk Handling page with a sidebar menu on the left. The sidebar includes links for Policy, Compliance, Auditor, Incident, Risk (with sub-options like Risk Register, Risk Instances, and Risk Handling), Risk Analytics, Notifications, and Theme. The Risk Handling link is currently selected and highlighted in blue. The main content area has two tabs at the top: 'Risk Resolution' (which is active) and 'Risk Workflow'. Below the tabs is a search bar labeled 'Search risks...' and several filter dropdowns for CRITICALITY (All Critical), STATUS (All Status), ASSIGNED TO (All Ass.), and REVIEWER (All Review). The main area displays a table of risks under the 'Assigned' tab. The table columns are: RISK ID, RISK TITLE, CATEGORY, CRITICALITY, ASSIGNED TO, REVIEWER, REVIEW COUNT, and ACTION. There are four rows of data:

RISK ID	RISK TITLE	CATEGORY	CRITICALITY	ASSIGNED TO	REVIEWER	REVIEW COUNT	ACTION
8	gsdgrhl	Security	High	Khairu	Loukya	1	<button>VIEW DETAILS</button>
13	gdngdf	Access Control	Medium	vikram.patel	priya.gupta	1	<button>VIEW DETAILS</button>
67	Unauthorized access to sensitive data	IT Security	Critical	vikram.patel	priya.gupta	1	<button>VIEW DETAILS</button>
76	Non-Compliance of syammmmmmmmmmmmmmmmmm	People Risk	Critical	radha.sharma	vikram.patel	1	<button>VIEW DETAILS</button>

Below the 'Assigned' section is another section titled 'Approved' with a similar table structure, showing one row of data:

RISK ID	RISK TITLE	CATEGORY	CRITICALITY	ASSIGNED TO	REVIEWER	REVIEW COUNT	ACTION
1	Approved Risk	Approved Category	Approved Criticality	Approved Assigned To	Approved Reviewer	Approved Count	<button>VIEW DETAILS</button>

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

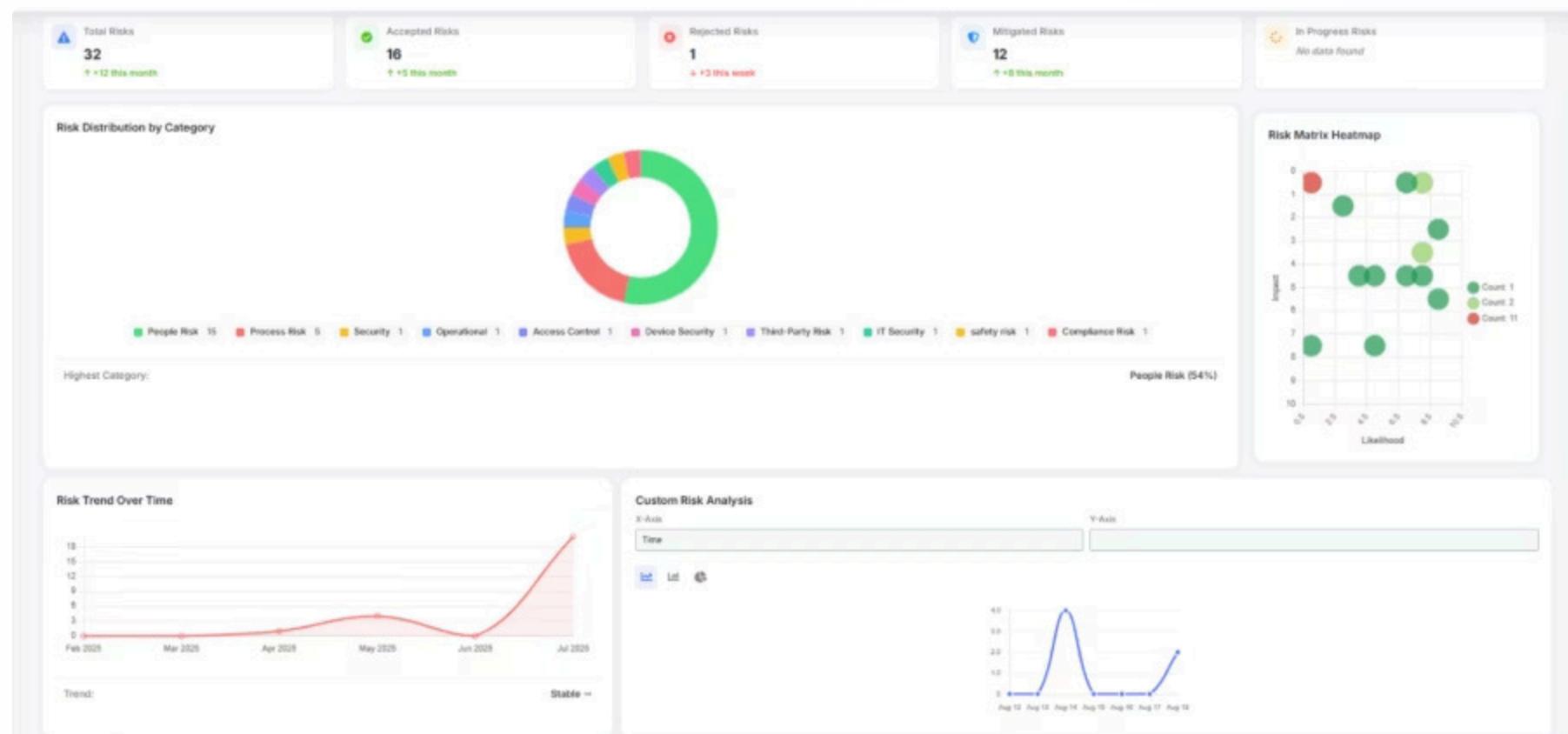
Visual representation of likelihood vs. impact for quick assessment of risk severity



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

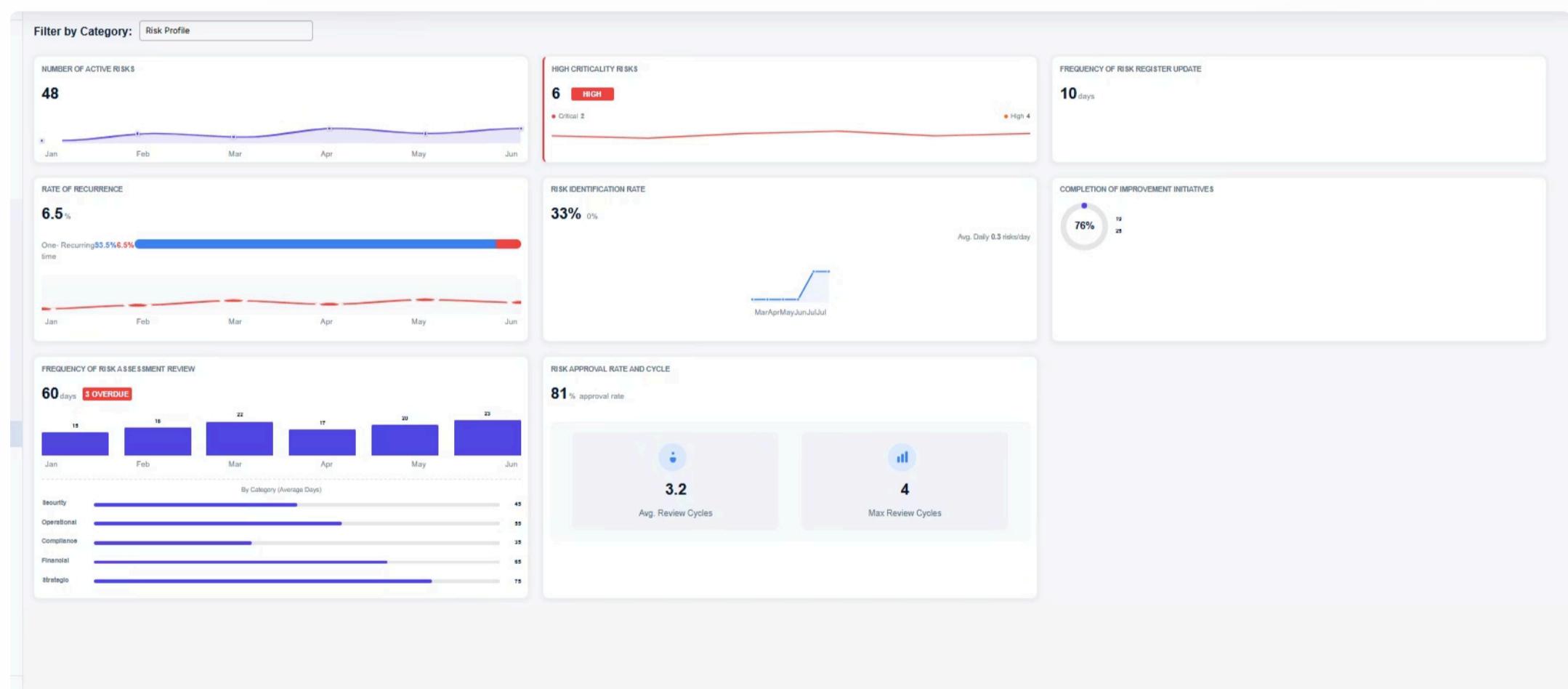
Monitoring frequency of risk register updates and assessment reviews

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