# Product Requirements Document (PRD) for Internal Audit and Compliance Management Tool (IACMT)

May 22, 2025

Contents

# 1 Overview

## 1.1 Product Name

Internal Audit and Compliance Management Tool (IACMT)

## 1.2 Product Description

The IACMT is a software solution designed to streamline the internal audit process by enabling users to:

- Upload guidelines and circulars in various formats (e.g., PDF, Word).
- Automatically extract applicable security controls using AI-powered natural language processing (NLP).
- Organize controls into a centralized audit tracker.
- Identify gaps and assess risks based on compliance status.
- Integrate with Jira for risk mitigation tracking and notifications based on criticality.
- Generate comprehensive, customizable audit reports.

The tool aims to reduce manual effort, improve compliance accuracy, and provide real-time visibility into audit progress and risk mitigation.

## 1.3 Target Audience

- Primary Users: Internal auditors, compliance officers, and risk managers responsible for conducting audits and managing risks.
- Secondary Users: Management teams requiring audit reports and oversight of compliance and risk mitigation.

## 1.4 Problem Statement

Current internal audit processes are often manual, time-consuming, and prone to errors, particularly when extracting security controls from large volumes of guidelines and circulars. Organizations need a tool to automate control identification, track compliance, manage risks, and integrate with existing workflows like Jira to ensure timely mitigation.

## 1.5 Solution Vision

The IACMT will automate and simplify the internal audit process, ensuring organizations can efficiently:

- Extract and track security controls from uploaded documents.
- Identify and prioritize risks based on criticality.
- Facilitate collaboration through Jira integration.
- Generate actionable audit reports for decision-making.

## 2 Key Features

### 2.1 Document Upload and Management

- Users can upload guidelines and circulars in formats such as PDF and Word.
- Documents are stored and organized by metadata (e.g., date, type, source) for easy retrieval.

### 2.2 AI-Powered Control Extraction

- Utilizes NLP to scan uploaded documents and identify applicable security controls.
- Provides a user interface for reviewing and editing extracted controls to ensure accuracy.
- Allows customizable control mapping to define or map specific terms to standard security controls.

### 2.3 Internal Audit Tracker

- Lists all identified controls in a centralized interface.
- Allows users to mark control status (e.g., compliant, non-compliant, needs review).
- Supports adding comments, evidence, or attachments for each control.
- Enables assignment of responsibilities for mitigation actions.

### 2.4 Gap and Risk Assessment

- Automatically identifies gaps where controls are not met.
- Assesses risks as low, medium, or high based on predefined criteria or user-defined rules.
- Prioritizes risks for mitigation based on criticality.

### 2.5 Jira Integration

- Creates Jira tickets for identified risks, including details and required mitigation actions.
- Sends notifications to relevant users (e.g., risk owners, auditors) based on risk criticality.
- Provides a calendar view displaying due dates for mitigation actions.

### 2.6 Audit Report Generation

- Compiles data into comprehensive reports, including:
  - List of identified risks.
  - Current status of each risk (e.g., open, mitigated).
  - Mitigation actions taken.
  - Responsible parties.
- Supports customizable report templates.
- Allows export in formats like PDF and Excel.

### 2.7 User Management and Permissions

- Implements role-based access control to restrict actions (e.g., uploading documents, approving reports) to authorized users.
- Allows administrators to manage user roles and permissions.

### 2.8 Dashboard and Analytics

- Provides a dashboard with key metrics, such as:
  - Number of audits completed.
  - Number of risks identified and mitigated.
  - Compliance status of controls.
- Offers analytics to identify trends (e.g., recurring risks, compliance improvements).

### 2.9 Customizable Report Templates

- Allows users to create or select predefined report templates tailored to organizational needs.

## 3 Technical Requirements

### 3.1 Frontend

- User-friendly interface built with modern web technologies (e.g., React, Angular).
- Responsive design for desktop and tablet use.

### 3.2 Backend

- Robust backend to handle document uploads, AI processing, database management, and integrations.
- Technologies: Node.js, Python (for AI), or similar.

### 3.3 AI/NLP Component

- Integration with an NLP service (e.g., IBM Watson, Google Cloud NLP) or a custom model for control extraction.
- Trainable AI model to improve accuracy with domain-specific terminology.

### 3.4 Database

- Relational database (e.g., PostgreSQL) to store user data, document metadata, control information, audit status, and risk data.

### 3.5 Integrations

- API integration with Jira for ticket creation, updates, and notifications.
- Optional integration with document management systems for guideline retrieval.

### 3.6 Security

- Encryption for document uploads and storage.
- Secure authentication and authorization (e.g., OAuth, SSO).
- Compliance with data protection regulations (e.g., GDPR, CCPA).

### 3.7 Scalability

- Cloud-based architecture to handle large volumes of documents and users.
- Scalable to accommodate organizational growth.

## 4 User Stories

1. Upload Documents: As an auditor, I want to upload a new guideline so that it can be scanned for security controls.
2. Extract Controls: As an auditor, I want the system to automatically extract security controls from the uploaded document.
3. Track Compliance: As an auditor, I want to see all extracted controls in a list where I can check their compliance status.
4. Risk Notification: As a risk manager, I want to be notified when a new risk is identified, with details on its criticality.
5. Generate Reports: As a manager, I want to generate a report that shows all identified risks and their current status.
6. Track Mitigation: As an auditor, I want to track the progress of mitigation actions in a calendar view.

## 5 Workflow

1. Upload Documents: Auditor uploads guidelines and circulars.
2. Scan and Extract Controls: System processes documents using AI to extract security controls.
3. Review Controls: Auditor reviews and edits extracted controls.
4. Assess Compliance: Auditor marks each control as compliant or non-compliant in the tracker.
5. Identify Gaps and Risks: System identifies gaps and assesses risks based on non-compliant controls.
6. Create Jira Tickets: For each identified risk, a Jira ticket is created with mitigation tasks.
7. Track Mitigations: Users update mitigation status in Jira, reflected in the tool.
8. Generate Reports: Managers generate audit reports based on current data.

## 6 Success Metrics

- User Adoption: Percentage of auditors using the tool for audits.
- Time Savings: Reduction in time spent on manual control extraction and report generation.
- Accuracy: Accuracy rate of AI-extracted controls compared to manual extraction.
- Risk Mitigation: Percentage of risks mitigated within set timelines.
- User Satisfaction: Feedback scores on usability and effectiveness.

## 7 Open Questions

1. AI Accuracy: What is the expected accuracy of control extraction, and how will it be measured?
2. Integration Details: What specific APIs or methods will be used for Jira integration?
3. Document Formats: How will the tool handle non-text document formats (e.g., scanned PDFs)?
4. Scalability: What is the expected volume of documents and users, and how will the system handle it?
5. Security and Compliance: What security measures are needed to protect sensitive audit data?

## 8 Development Considerations

- Team Composition: Frontend developers, backend developers, AI/NLP specialists, database administrators, integration specialists.
- Timeline: To be determined based on project scope and resource availability.
- Training and Support: Provide documentation and training for users to ensure effective adoption.

## 9 Sample Internal Audit Tracker

| Control ID | Description | Status | Risk Level | Responsible Party |
|---|---|---|---|---|
| CTRL-001 | Implement access controls | Compliant | N/A | IT Team |
| CTRL-002 | Regular security training | Non-compliant | High | HR Team |
| CTRL-003 | Data encryption | Needs Review | Medium | Security Team |

Table 1: Sample Internal Audit Tracker

## 10 Sample Audit Report Structure

- Executive Summary: Overview of audit findings, key risks, and mitigation progress.
- Control Compliance: List of controls with status (compliant, non-compliant, needs review).
- Risk Assessment: Identified risks, criticality, and mitigation actions.
- Recommendations: Suggested actions for unresolved risks.
- Responsible Parties: Teams or individuals assigned to mitigation tasks.