Chapitre 2 : Planification du projet

February 26, 2025

1 Introduction

In a context where information security has become a strategic issue for companies, compliance with international standards such as ISO/IEC 27001:2022 is essential. However, security audit management still largely relies on traditional tools like Excel, leading to risks of errors, lack of traceability, and inefficient handling of non-conformities.

To address these challenges, our project aims to develop a centralized web platform for planning, executing, and monitoring security audits within Coficab. This solution will provide better organization of audit processes and enhanced traceability of results.

2 Problem Statement

Information security audits play a crucial role in assessing and continuously improving data protection measures. However, the use of manual tools such as Excel complicates the centralization of information, collaboration between auditors, and the generation of detailed reports.

Thus, our project seeks to address the following questions:

- How can the management of security audits be automated and centralized?

- How can non-conformities detected during audits be effectively tracked?

- How can compliance with ISO/IEC 27001:2022 requirements be ensured while optimizing the audit process?

3 Project Objectives

3.1 General Objective

Develop a web-based security audit management platform to centralize and optimize audit processes in compliance with ISO/IEC 27001:2022 requirements.

3.2 Specific Objectives

- Automate audit planning and tracking by providing an intuitive interface for auditors.

- Facilitate non-conformity management through detailed tracking and appropriate corrective actions.

- Generate comprehensive audit reports to support better decision-making.

- Ensure traceability of actions taken throughout the audit lifecycle.

- Integrate AI features to analyze documents and detect recurring non-conformities.

- Enhance access security through Active Directory authentication and an action log.

4 Requirements Specifications

4.1 Functional Requirements

The functional requirements correspond to the expected functionalities of the system:

- **Audit Management**: Creation, updating, deletion, and consultation of audits.
- **Non-Conformity Management**: Recording, categorization, and tracking of non-conformities.
- **Audit Planning via Interactive Calendar**: Scheduling and managing audits with reminders.
- **Automated Report Generation and Data Export**: Reports in PDF/Excel format.
- **Secure Authentication via Active Directory**: Ensuring secure access control.
- **Action Logging**: Keeping records of all performed actions for traceability.
- **Notifications and Automatic Reminders**: Alerts for audit deadlines.
- **AI Document Analysis**: Detecting recurring non-conformities automatically.

4.2 Non-Functional Requirements

Non-functional requirements relate to the system's quality and constraints:

- **Security**: Data protection with access permissions and encryption.
- **Performance**: Optimized response time for smooth navigation.
- **Scalability**: Ability to expand to handle a growing volume of audits.
- **Reliability**: Continuous service availability with fault tolerance.
- **Usability**: Intuitive interface facilitating user experience.
- **Compatibility**: Multi-platform access (PC, tablet, mobile).

5 Business Rules

5.1 User

The primary user is the auditor.

5.2 Audit Details

- Start date and due date.
- Status (in progress, completed, canceled).
- Type (internal, external).
- Associated comments.
- Ability to attach documents to audits.

5.3 Audit Outcomes

- Opportunity for improvement (OFI).
- Strength.
- Minor non-conformities.
- Major non-conformities.
- Sensitive points.

5.4 Opportunity for Improvement (OFI)

- ID.
- Audit ID/name.
- Description of the non-conformity.
- Impacted asset.
- Corrective action plan.

5.5 Non-Conformities

- ID.
- Audit ID/name.
- Description of the non-conformity.
- Root cause.
- Impacted assets.
- Corrective and preventive action plan.

5.6 Corrective and Preventive Action Plan

- Due date.
- Responsible person.
- Status.
- Effectiveness (if status is "done").

6 User Stories (Ordered and Numbered)

6.1 Audit Management

1. **Create an Audit**
   As an auditor, I want to create an audit with the required details to track and manage the audit process.

2. **Update an Audit**
   As an auditor, I want to modify the details of an existing audit to correct or add information.

3. **Delete an Audit**
   As an auditor, I want to delete an obsolete audit to maintain a clear and relevant record.

4. **Attach Documents to an Audit**
   As an auditor, I want to attach documents to audits to centralize relevant information.

5. **View Audit Details**
   As an auditor, I want to view audit details, including non-conformities, comments, and corrective actions, for comprehensive management.

6. **Filter Audits by Criteria**
   As an auditor, I want to filter audits by status, type, or due date for better management.

7. **Audit Planning via Calendar**
   As an auditor, I want to view all scheduled audits on a calendar to effectively manage my schedule.

8. *Duplicate an Audit*
   As an auditor, I want to duplicate an existing audit to save time when creating similar audits.

9. Archive an Audit
As an auditor, I want to archive completed audits to keep a record without cluttering the interface.

6.2 Non-Conformity Management

1. **Document Non-Conformities**
As an auditor, I want to record non-conformities with descriptions, affected assets, and corrective action plans.

2. **Categorize Non-Conformities**
As an auditor, I want to categorize non-conformities as major or minor for risk assessment.

3. **Track Opportunities for Improvement (OFI)**
As an auditor, I want to track Opportunities for Improvement (OFI) and related corrective action plans.

4. **Create Sub-Actions for Non-Conformities**
As an auditor, I want to create sub-actions for each non-conformity to manage corrective actions in more detail.

5. **Validate Corrective Actions**
As an auditor, I want to validate corrective actions once completed and record their effectiveness.

6. **View Non-Conformity History**
As an auditor, I want to view the history of non-conformities and their associated corrective actions.

6.3 AI-Assisted Features

1. **AI-Assisted Document Analysis**
As an auditor, I want AI to extract key information from uploaded documents to streamline audit processing.

2. *AI Detection of Recurring Non-Conformities*
As an auditor, I want AI to detect recurring patterns in non-conformities for continuous process improvement.

3. **Detect High-Risk Audits**
As an auditor, I want the system to flag high-risk audits (with multiple major non-conformities) for immediate attention.

6.4 Notifications & Tracking

1. **Receive Notifications of Due Dates**
As an auditor, I want automated notifications for upcoming audit due dates.

2. **Reminders for Corrective Actions**
As an auditor, I want reminders for corrective action deadlines to ensure timely resolution.

3. **Audit Trail & Action Logging**
As an auditor, I want an audit trail that logs all actions for compliance and traceability.

6.5 Access & Security

1. **Active Directory Authentication**
As an auditor, I want to log in via Active Directory for secure authentication.

2. **User Profile Modification**
As an auditor, I want to modify my personal information (name, profile picture).

3. **Customizable Interface**
As a user, I want to customize my interface (dark/light theme, *layout of elements*).

6.6   Audit Reporting & Exporting

1. **Generate Detailed Audit Reports**
   As an auditor, I want to generate detailed audit reports for documentation and regulatory compliance.

2. **Export Audit Data**
   As an auditor, I want to export audit data in multiple formats (PDF, Excel) for reporting and analysis.

3. **Generate Monthly Summary of Audits**
   As an auditor, I want to receive a monthly summary of completed audits to have an overview of my activities.

4. **Automatic Report Generation**
   As an auditor, I want the application to automatically generate audit reports, saving time and ensuring consistency in the results.

5. **Customizable Reports**
   As an auditor, I want to customize reports by selecting the data to include (non-conformities, corrective actions, etc.).

6.7   Collaboration & Communication

Add Comments to Audits
As an auditor, I want to add comments to audits to facilitate collaboration with my team.
Mention Colleagues in Comments
As an auditor, I want to mention colleagues in comments to notify them of required actions.
Share Documents with Stakeholders
As an auditor, I want to share documents related to an audit with other stakeholders to facilitate collaboration.
Integrated Chat
As an auditor, I want to chat in real-time with colleagues about a specific audit.

6.8   Analytics & Dashboards

1. **Audit Dashboard**
   As an auditor, I want a dashboard that displays key statistics (number of ongoing audits, major non-conformities, etc.).

2. **Trend Analysis Charts**
   As an auditor, I want to view charts showing trends in non-conformities (by month, type, etc.).

3. **High-Risk Audit Alerts**
   As an auditor, I want the system to alert me about audits with a high risk of non-conformities.

6.9   User Experience & Customization

1. **Integrated User Guide**
   As a user, I want access to an integrated user guide to learn how to use the platform.

2. **Submit Feedback**
   As a user, I want to submit feedback or suggestions to improve the platform.