SOFTWARE REQUIREMENTS SPECIFICATION

for

ISO Audit Software

Version 1.0

Prepared by :
1. Abhignya Kotha (PES1UG21CS018)
2. Adithya B (PES1UG21CS036)
3. Aditi Prabhu A (PES1UG21CS039)
4. Ambati Revanth Sreeram (PES1UG21CS070)

Submitted to : Anand M S
Lecturer

September 15, 2023

Contents

1 Introduction

1.1 Purpose

The purpose of this document is to define the requirements for the development of Audit Management Software. This software is designed to streamline and manage audit processes by providing a comprehensive set of tools for audit planning, execution, reporting, and compliance tracking.

1.2 Intended Audience and Reading Suggestions

Project managers: project managers should make use of this document to gain a better understanding of the objectives and high-level requirements.

Developers and designers: Developers and designers should make use of this document to understand the system architecture and user requirements (functional, non-functional, etc.). The system should be designed efficiently and such that all requirements are met.

QA and Testers: Testers should pay close attention to the functional requirements specified in this document and design test cases to make sure the requirements are implemented in flawless manner.

End users: Users can read the sections which contain the features of the system, user classes (use-case diagrams), and functionalities relevant to them to and help them to use the system effectively.

1.3 Project Scope

This document provides guidance on auditing management systems, including the principles of auditing, managing an audit program and conducting management system audits, as well as guidance on the evaluation of competence of individuals involved in the audit process. These activities include the individual(s) managing the audit program, auditors and audit teams.
It is applicable to all organizations that need to plan and conduct internal or external audits of management systems or manage an audit program.
The application of this document to other types of audits is possible, provided that special consideration is given to the specific competence needed.

1.4 References

1. https://synersia.org/wp-content/uploads/2021/02/ISO-19011-2018-Pedoman-Audit-Sistem-Manajemen-EN.pdf
2.https://www.iso.org/standard/70017.html
3.https://www.iso.org/home.html

2 Overall Description

2.1 Product Perspective

The ISO audit management system is a comprehensive software solution designed to facilitate and streamline the entire audit process of any type. It is intended to support compliance with ISO standards. It enables efficient planning, execution, reporting, and follow-up activities related to an audit.

2.2 User Classes and Characteristics

1. Administrator: Responsible for system configuration and maintenance. Manages user accounts and privileges.
2. Audit Manager: Supervises the planning and execution of audits, assigns auditors to audits, monitors audit progress, analyses and approves audit reports.
3. Auditors: In-charge of conducting and audit according to the defined standards. Generates the checklist using the system. Reports non-conformance, observations.
4. QA Team: Keeps track of audit processes and ensures their quality. Checks the audit reports for compliance with the defined standards. May provide guidance to auditors.
5. Document Managers: Maintains the document repository. Manages audit related documents and ensures their version control and compliance.
6. Stakeholders: Includes department heads, executives, regulatory bodies. They can access reports and findings related to an audit which are relevant to their areas of interest.

2.3 Product Functions

1. User Authentication and access control: Allow user to register/login with appropriate roles (auditor, audit managers, administrators,etc.) and provide role based access.
2. Audit Planning: Helps define the scope and objectives of an audit, manage the team and schedule an audit.

3. Audit Execution: Helps in check-list creation, collection of evidence (documents, photos,etc.). Can be used for on-site and remote auditing.

4. Audit Reporting: Enables generation of standardised reports that comply with ISO standard, distribution of audit reports to relevant stakeholders. Custom templates also available for specific needs.

5. Audit Follow-Up: Track non-conformance and findings. Create corrective action plans with progress tracking. Monitor the progress of corrective actions and verify their helpfulness.

6. Document Management: Provide a centralised repository to store audit related documents and other reference material. Maintain version control for documents to assure the accuracy. Users can search and retrieve the documents.

7. Security and Compliance: Ensures the security of audit related data through security measures and access control. Make sure all audit related activities comply to ISO standards.

8. User Training and Support: Provide training materials to help users become proficient in the system.

2.4 Operating Environment

OE-1: The ISO audit management system will operate on windows (10 and above), Mac OS(version 10.15 (Catalina) and above) and Linux(Ubuntu, Red hat, Enterprise Linux)
OE-2: The system will run on Intel processors(10th generation and above), AMD processors, apple processors (M1 and above).
OE-3: The system will permit user access from the organization's intranet or through the institution's firewall if the user is authorised for outside access.

2.5 Design and implementation constraints

CO-1: All HTML code shall conform to the HTML 4.0 standard.
CO-2: All C++ code shall contain features from version 14 and above.
CO-3: The system shall use the current enterprise edition of MySQL.

2.6 User Documentation

UD-1: An instruction page should be made available to new users explaining the registering process and various functionalities of the system.

UD-2: An tutorial and playground page should be made available to the users who have registered where online video tutorials are available to them. The users can use the playground to practice planning an audit, conducting and audit, use the document repository. These actions should not be stored in the database and should be deleted when the user logs out.

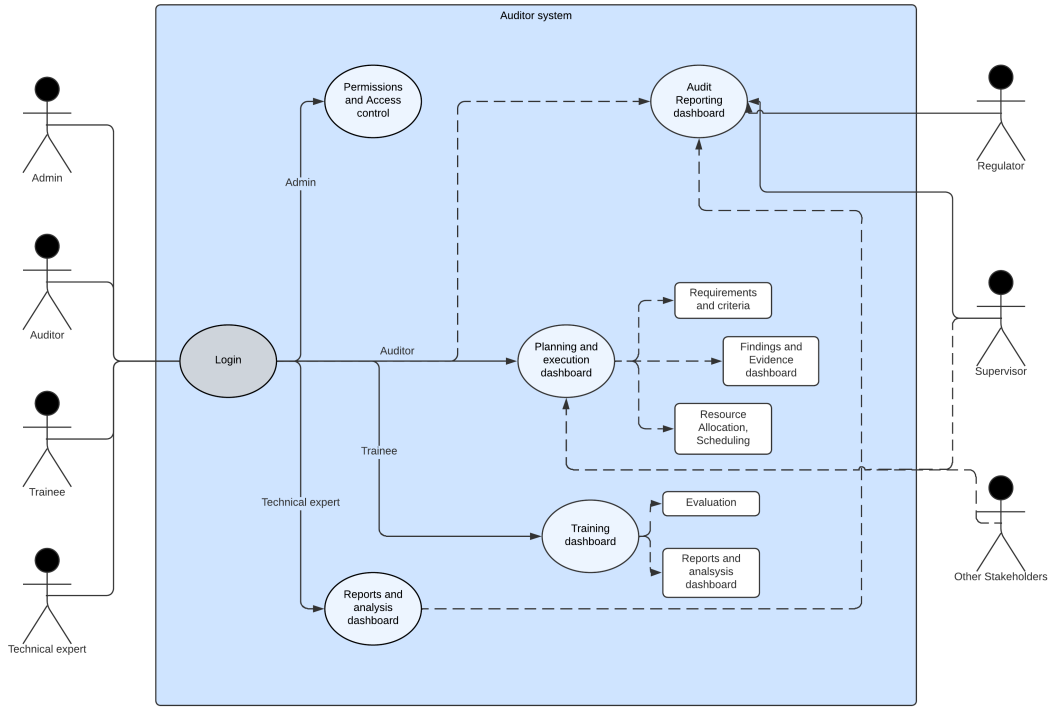

Figure 2.1: Auditor System

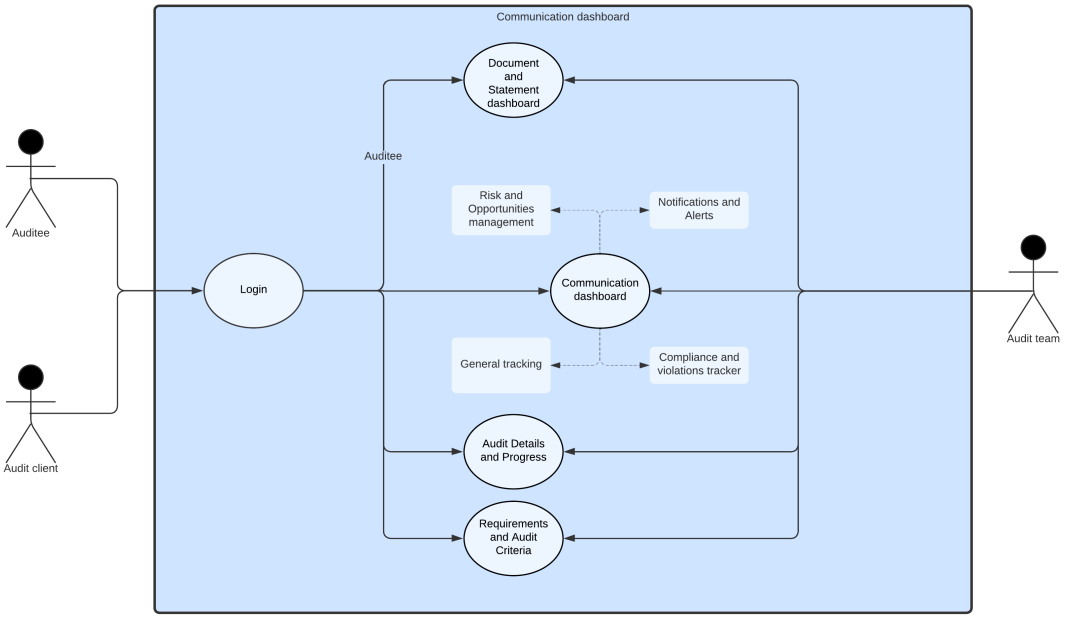

Figure 2.2: Communication Dashboard

3 External Interface Requirements

3.1 User Interfaces

1. Login Page: contains the username and password fields. Buttons: Login, Remember me and a forgot password option.

2. Dashboard: contains widgets displaying upcoming audits, task lists, and notifications. This serves as the main interface after login.

3. Audit Planning interface: This interface allows audit managers and planners to create and manage audit plans, schedules, and objectives. Contains forms with fields for objectives, scope, team management. A calendar for scheduling audits. This page should be integrated with document management for attaching documents.

4. Audit Execution interface: Auditors will use this interface to conduct audits. Contains checklist of tasks and forms to record evidence, communication tools in case of remote audit, form to report non-conformance.

5. Audit Reporting and Analysis: This interface is for generating, reviewing, and analyzing audit reports. It should contain report templates that comply to ISO standards and exporting options (PDF, Excel)

6. Document Management Interface: This interface provides access to the document repository, where audit related documents and material are stored. Features of this interface include searching and filter options for document retrieval, version control history, access controls to manage document permissions.

7. User Profile and Settings: This interface allows user to manage and edit their profile. Features include profile editing, password reset/change.

3.2 Hardware Interfaces

1. Printers to generate physical audit reports. Printer types include Ink-jet, laser. The printers can be connected through USB or Wi-fi.

2. Cameras and document scanners to generate digital copies of physical documents. Camera types can be web cams, digital cameras.

3.3 Software Interfaces

1. The audit management system uses MySQL Enterprise version for data storage and retrieval. Tables and schema shall be optimised for performance and scalability.

2. The audit management system will be compatible with google chrome(latest version), Brave(latest version), Safari(latest version). It shall include support for all JavaScript and HTML5.

3. The audit management system shall provide API endpoints for integrating with document management systems via RESTful services. This integration will allow users to attach relevant documents to audit records.

4. The audit management system shall use SMTP protocol for sending email notifications

5. User authentication shall be performed against the organization's LDAP/AD server and Single sign-on shall be enabled for seamless user access.

6. External audit services will be provided through secure APIs. Audit schedules and findings shall be transmitted and received using XML data format.

3.4 Communication Interfaces

1. The audit management system shall send an email to the auditors and the auditee(specified personnel) when the schedule for an audit is fixed by the audit manager.

2. The audit management system shall provide real-time chat and messaging features to the users for them to communicate and collaborate during the audit.

3. The audit management system uses MySQL Enterprise version. It interacts with the database for data retrieval and manipulation.

4. The system will support VPN connections for remote access. The protocols used shall be OpenVPN or IPsec.

4 System Features

The audit management software has features that are main and also some are sub. But all the feature is necessary for this software.

4.1 User Management and Access control

Description: Users can register and authenticate themselves and get a role. Different roles get functionalities and access/permissions relevant to them. This ensures security and data privacy while making the software simplified and more organised. The auditors should have access to audit related data only when assigned to specific audit teams.

4.1.1 User Registration

Functionality:

- This allows users to register themselves with the software and get roles assigned to them.
- Users can register by providing necessary details, and the system verifies the authenticity and validity of the details provided before creating an account.

Priority : High

4.1.2 User Authentication

Functionality:

- Users access their accounts by providing necessary login details.
- The system securely hashes and verifies passwords.
- After successful authentication, users are redirected to their dashboard or the relevant part of the system based on their role.

Priority : High

4.1.3 Role-Based Access Control (RBAC)

Functionality:

Admins have access to user management features to create, edit, or deactivate user accounts. When creating roles, Admins can specify the permissions and access levels

associated with each role. Users are assigned roles (Admin, Auditor, Auditee, Audit Client, Trainee, Technical expert, Observer, Supervisor, Regulator) by Admins. Access to specific features, data such as tasks and checklists is controlled based on the user's assigned role. Changes to the roles and permissions are logged in the system's audit trail.

4.2 Audit Planning

Description: Authorised users can create new audit instances. When an instance is created, details pertaining to audit type, scope, objectives/criteria and team personnel are specified. The auditors can schedule the upcoming audits along with details such as timelines and locations. Resource allocation and personnel specific permissions are also managed in this section.

Priority : High

The system should support the assignment of specific auditors to scheduled audits while providing a pre-defined audit checklist based on the ISO standards and specified criteria and allow the users to create a custom checklist.

Priority : Medium

4.2.1 Audit Creation

Functionality:

Authorised users such as the admin or specific auditors can create audit instances. Details such as Audit Scope, Plan, Criteria, Clients, Auditees, Audit team and specific roles of members are mentioned. Audit programme objectives are needed to be mentioned clearly for effective implementation of the audit.

4.2.2 Audit Scheduling

Functionality:

Scheduling of Audit involves creation of timeline(s) for individual audits as well as multiple audits. Details such as Location, Date, Time are mentioned. The schedule can also contain details about team member allocation and stakeholder meetings scheduled.

4.2.3 Audit Checklist

Functionality:

Checklist(s) are created here for audits tasks based on the criteria and plans mentioned during audit creation. Checklists can be personalised to each specific team member and also to specific sections of audits or audits part of combined audits.

4.2.4 Resource Allocation

Functionality:

Allocate necessary resources for the audit, including equipment, personnel, costs and materials. Resources can be allocated and managed for individual team members and requests for resources can also be made through this section/module. Track resource utilisation and budget allocations related to the audit project.

4.3 Audit Execution

Description: This section/module allows the Audit team to conduct their audits, access documentation pertaining to company records, statements and also the requirements for the audit. The audit team can also record their findings and capture evidence while maintaining and tracking progress real-time. Stakeholders can use this section to track progress and ensure satisfaction of requirements. It also lets the tracking and management of trainee auditors and competence of auditors.

Priority : High

4.3.1 Audit Data Collection

Functionality:

- The Audit team can access and verify documents, statements etc. pertaining to the auditee using this module.
- The Auditee can upload and view documents, statements using this module while maintaining version control.
- Any data collected by the auditing team separately can also be documented and verified.
- Other stakeholders can view the data based on permissions given by admins.

4.3.2 Audit Evidence and Findings Management

Functionality:

The system/module provides a centralised repository for storing audit evidence, findings, documents, and supporting materials.

- Reporting includes categorising findings, assessing severity, and recommending corrective actions.
- Various stakeholders can review the data and can use it for gaining insights.
- Evidence is logged with proper timestamps and can be labelled based on findings to back them up.

4.3.3 Progress

Functionality:

- Allows auditors and team members to update the progress of audits, tasks, and checklist items in real-time.
- Use status labels to categorise the overall status of the audits.
- Automatically notify stakeholders, such as audit team leaders and team members, when significant milestones or completions occur.

4.3.4 Communication
Functionality:

- Create dedicated communication channels or threads for each audit project, allowing audit teams and other stakeholders to focus on discussions related to specific audits and other issues.
- Enable users to share audit-related documents, meeting reports, checklists, and evidence within the software.

4.3.5 Auditor Training and Competence
Functionality:

- Allows administrators to create and manage trainee profiles within the software. The audit team leaders can evaluate and track auditor competencies.
- Integrate with external certification bodies to facilitate the validation of auditor certifications and qualifications.
- Members of the audit team such as auditors, technical experts, observers etc. can upload reports pertaining to their tasks.

4.4 Audit Reporting

Description: This section/module lets the Audit team submit all findings and evidence alongside the final reports with recommendations and certificates. It also allows for data visualisation with charts, graphs etc.. The Documents are submitted for approval by Approvers in this section. Reporting on training status and remarks for trainee auditors and other members of the team can be done if required. Incident reporting and management and report distribution can also be done in this module.
Priority : High

4.4.1 Automated Report Generation
Functionality:

- Users can request automated reports, including audit findings, compliance status, and audit summaries.
- Reports are generated in a format compliant with ISO standards.
- Generated reports are stored and can be accessed by authorised users.

4.4.2 Report Distribution
Functionality:

- Reports can be distributed to relevant stakeholders, such as audit team members, management, and external certification bodies.
- Distribution options include email notifications, PDF exports, and secure sharing links.

4.4.3 Data visualisation

Functionality:

Data can be visualised in the form of bar graphs, pie charts and trend charts and various other visualisation types.

- This can be used by stakeholders to select and filter the data they want to visualise based on criteria such as audit type, date range, and audit status and help understand the data better.
- Reports being generated can be made more informative and easy to understand by using the visualisations generated in this module.

4.5 Compliance and Risk, Opportunities Dashboard

Description: This module lets all stakeholders manage documentation and various other details pertaining to the audit. The Audit team can report issues and violations. This module can be used to track compliance and also to identify risks and opportunities while providing risk mitigation strategies and general remediation action management. The module should maintain a version control for all the documents to ensure that the latest versions are accessible to the authorised users. The module can also send alerts and notifications for various events.

Priority : Medium

4.5.1 Compliance Management

Functionality:

- This module tracks compliance related events such as adherence to policies or regulatory requirements.
- The compliance criteria and rules can be configured in this section.
- Reports related to compliance are managed here alongside remediation actions.

4.5.2 Risks and Opportunities Management

Functionality:

- Risk and Opportunities identified during the audit are managed in this module.
- Risk remediation methods and opportunity assessment can also be accomplished in this module.

4.5.3 Notifications and Updates

Functionality:

- Display important announcements, updates, and news related to the ISO Audit Management Software or audit projects.

- Automated alerts or notifications can be generated for activities related to the audit such as compliance-related events or tracking of issues reported among other things, This ensures stakeholders do not miss important information.

4.5.4 General Tracking Functionality:

- Issue tracking and document version control is handled in this module.
- Other general tracking is combined into one tracking module integrated in this section.

5 Other Nonfunctional Requirements

5.1 Performance

The software should be able to handle large amounts of data quickly and efficiently. This is important to ensure that audits can be conducted in a timely manner.

5.2 Security

The software should be secure and protect the confidentiality, integrity, and availability of data. This includes protecting data from unauthorized access, modification, or destruction.

5.3 Safety Requirements

The software must be designed to prevent accidental data loss and must prevent data corruption.

5.4 Software Quality Attributes

- Portability: To ensure that the software can be used by organizations of all sizes it must be portable and be able to be used on various platforms, such as Windows, macOS and Linux.
- Maintainability: The software must be maintainable and should be easy to update and fix bugs to ensure that the software remains up-to-date and secure. The software should be well-documented and should have a clear change management process in place.
- Usability: It should have a user-friendly interface. This is to ensure that users can easily navigate the software and complete tasks.

5.5 Compliance

The software must comply with all applicable laws and regulations. This is important to ensure that the software is used in a lawful and ethical manner.

6 Other Requirements

No other requirements are to be mentioned at this stage.

Appendix A: Glossary

1. Audit ID:
    - Data type: alphanumeric
    - Description: unique identifier for audit records.
2. Audit Title:
    - Data type: Text
    - Description: Title or name of the audit.
3. Audit Description:
    - Data type: Text
    - Description: the objectives of the audit and it's purpose.
4. Audit Dates:
    - Data type: Date
    - Description: When the audit starts or ends.
5. Audit Location:
    - Data type: text
    - Description: specifies the physical or virtual location of the audit.
6. Finding ID:
    - Data type: alphanumeric
    - Description: unique identifier for audit findings.
7. Finding Description:
    - Data type: text
    - Description: description of the audit finding.
8. User ID:
    - Data type: alphanumeric
    - Description: unique identifier for each user.
9. User name:
    - Data type: text

- Description: The full name of the user.

10. User role:
    - Data type: enumeration(administrator, auditor, manager)
    - Description: specifies the role or access level of the user.
11. User email:
    - Data type: email address
    - Description: the email id of the user.
12. Action ID:
    - Data type: alphanumeric
    - Description: unique identifier for each corrective action.
13. Action Description:
    - Data type: text
    - Description: Details about the corrective actions needed to be taken.
14. Action Due Date:
    - Data type: date
    - Description: date by which the corrective action should be completed.
15. Report ID:
    - Data type: alphanumeric
    - Description: unique identifier for each audit report.
16. Report Title:
    - Data type: text
    - Description: title or name of the audit report.
17. Report Date:
    - Data type: date
    - Description: the date on which the audit report was generated.
18. Report Content:
    - Data type: text
    - Description: contains the details of the report.