Enterprise Audit Management System

Detailed Scope Document

Document Version: 1.0
Date: December 26, 2025
Client: Sustenergy Foundation
Project: Enterprise Upgrade for Electrical Safety Audit System

---

1. Introduction

1.1 About This Document

This document describes the complete features and functionalities required to upgrade the current Electrical Safety Audit Application from a simple form-based tool into a fully-featured **Enterprise Audit Management System**.

The new system will enable multiple users to work together efficiently, track audits from start to finish, maintain complete records, and ensure quality through proper review processes.

1.2 Business Objectives

The upgraded system aims to achieve the following goals:

1. **Streamlined Operations:** Replace manual tracking with an automated digital workflow
2. **Quality Assurance:** Ensure every audit goes through proper review before delivery
3. **Accountability:** Track who did what and when throughout the audit process
4. **Client Satisfaction:** Provide clients with professional, timely, and accurate reports
5. **Business Intelligence:** Generate insights from audit data to improve operations
6. **Scalability:** Handle growing numbers of audits, users, and clients

---

2. User Roles and Access Levels

The system will have four types of users, arranged in a hierarchy. Each user type has specific responsibilities and access to different parts of the system.

2.1 Super Administrator (Highest Level)

Who is this? The Super Administrator is the master user who has complete control over the entire system. Typically, this would be the business owner or IT manager of Sustenergy Foundation.

What can they do?

- **Create and Manage All Users:** Add new users to the system, edit their information, or remove them when they leave the organization
- **Assign Roles:** Decide what role each user should have (Admin, Supervisor, or Auditor)
- **Set Permissions:** Create custom roles with specific permissions based on business needs
- **Configure the System:** Set up company-wide settings like working hours, notification preferences, and escalation rules
- **View Everything:** Access all audits, reports, and data across the entire organization
- **Manage Audit Templates:** Create or modify different types of audit forms for various industries
- **Access All Reports and Analytics:** See company-wide statistics, performance reports, and business insights
- **Handle Billing and Subscriptions:** Manage the company's subscription plan (if applicable)

What they see when they log in: A master dashboard showing overall system health, total number of audits, pending approvals, user activity, and any system alerts that need attention.

2.2 Administrator / Manager (Second Level)

Who is this? Administrators are senior staff members who manage specific departments or regions. They handle day-to-day operations but cannot change system-wide settings.

What can they do?

- **Create and Manage Team Members:** Add new Supervisors and Auditors to their department
- **Create New Audits:** When a client requests an audit, Administrators can create the audit entry in the system
- **Assign Audits to Teams:** Allocate audits to appropriate Supervisors or directly to Auditors
- **Monitor Progress:** Track all audits within their department
- **Approve Reports:** Give final approval on audit reports before they are sent to clients
- **View Department Analytics:** See performance statistics for their team
- **Handle Client Communication:** Respond to client queries and share reports with clients

What they cannot do:

- Change system-wide settings
- View audits from other departments (unless given permission)
- Create or modify audit templates
- Delete users from other departments

What they see when they log in: A department dashboard showing their team's audits, pending reviews, upcoming deadlines, and team performance metrics.

2.3 Supervisor (Third Level)

Who is this? Supervisors are experienced auditors who lead small teams. They ensure quality by reviewing audits before they are approved.

What can they do?

- **Assign Audits to Auditors:** Distribute audit work among their team members
- **Review Submitted Audits:** Check the quality of audits completed by their team
- **Approve or Return Audits:** If an audit meets quality standards, approve it for report generation. If not, return it with comments for correction
- **Generate Reports:** Create the final audit reports (Word and PDF documents)
- **Monitor Team Progress:** See which audits are in progress, pending, or overdue
- **Provide Guidance:** Add comments and feedback to help auditors improve
- **Conduct Audits Themselves:** Supervisors can also perform audits when needed

What they cannot do:

- Create new users
- Approve their own audits (must be reviewed by Admin or another Supervisor)
- Access audits outside their team
- Change system settings

What they see when they log in: A team dashboard showing audits assigned to their team, items pending their review, and team performance at a glance.

2.4 Auditor / Field Engineer (Fourth Level)

Who is this? Auditors are the field staff who visit sites, conduct inspections, and record their findings in the system.

What can they do?

- **View Assigned Audits:** See the list of audits assigned to them
- **Accept or Decline Audits:** Confirm they will perform an assigned audit (or decline with a reason if unavailable)
- **Conduct Audits:** Fill in the audit form with their observations, measurements, and photos
- **Save Draft Work:** Save their progress and continue later
- **Submit for Review:** Send the completed audit to their Supervisor for review
- **Make Corrections:** If an audit is returned with comments, make the required corrections and resubmit
- **Raise Support Tickets:** Report issues or ask questions using the ticketing system

What they cannot do:

- Assign audits to others
- Approve or generate reports
- View other auditors' work
- Access administrative functions

What they see when they log in: A personal dashboard showing their assigned audits, upcoming deadlines, audits returned for correction, and their personal performance statistics.

2.5 Custom Roles (Optional Feature)

In addition to the four standard roles, Super Administrators can create custom roles with specific combinations of permissions.

Example Custom Roles:

Custom Role	Description	Permissions
Regional Coordinator	Oversees audits across multiple branches in a region	View all regional audits, assign work, but cannot approve reports
Quality Auditor	Reviews audits for quality but doesn't manage teams	Can only review and comment, no assignment powers
Client Viewer	External client login to view their reports	Read-only access to their own audit reports
Report Generator	Staff member who only generates and dispatches reports	Can generate reports and mark as delivered, no editing

---

3. The Audit Workflow

The audit workflow describes the journey of an audit from creation to completion. Each stage has clear responsibilities and actions.

3.1 Workflow Overview

```
REQUEST → CREATE → ASSIGN → ACCEPT → CONDUCT → SUBMIT → REVIEW → APPROVE → GENERATE → DELIVER → CLOSE
                                                    ↑                 ↓
                                                    └─── RETURN ◄─────┘
```

3.2 Detailed Stage Descriptions

Stage 1: Audit Creation

What happens: A client requests an electrical safety audit for their facility. An Administrator creates a new audit entry in the system.

Information captured at this stage:

- Client name and contact details
- Branch or facility to be audited
- Type of audit required (Hospital, Hotel, Bank, etc.)
- Requested date of inspection
- Any special instructions or requirements

Who does this: Administrator or Manager

What happens next: The audit moves to the Assignment stage.

Stage 2: Audit Assignment

What happens: The newly created audit is assigned to a Supervisor or directly to an Auditor who will perform the inspection.

Considerations for assignment:

- Auditor's workload and availability
- Auditor's expertise (some may specialize in certain industries)
- Geographic location (assign someone near the site if possible)
- Urgency of the audit

Who does this: Administrator, Manager, or Supervisor

System notifications:

- The assigned person receives an email notification
- A dashboard notification appears when they log in
- If urgent, an SMS can also be sent (optional feature)

What happens next: The assigned person must accept the audit.

Stage 3: Audit Acceptance

What happens: The assigned Auditor reviews the audit details and confirms they can perform it.

Options available:

- **Accept:** Auditor confirms they will perform the audit
- **Decline:** Auditor indicates they cannot perform it (must provide a reason)

If declined: The audit goes back to the assigning person for reassignment.

Who does this: The assigned Auditor

What happens next: Once accepted, the Auditor can begin conducting the audit.

Stage 4: Audit In Progress

What happens: The Auditor visits the site and performs the electrical safety inspection. They record their findings in the system.

What the Auditor captures:

- General observations about the site
- Photographs of electrical installations, issues, or safety concerns
- Electrical measurements (voltage, current, power factor, etc.)
- List of connected electrical loads
- Any safety violations or concerns
- Recommendations and conclusions

Key features during this stage:

- **Auto-Save:** The system automatically saves work periodically to prevent data loss
- **Offline Mode:** If internet is unavailable at the site, data is saved locally and synced later (for mobile app)
- **Photo Upload:** Directly upload photos from the device camera or gallery
- **Draft Status:** Auditors can save their work and continue later

Who does this: The assigned Auditor

What happens next: When complete, the Auditor submits the audit for review.

Stage 5: Audit Submission

What happens: The Auditor finishes their work and submits the audit for review by their Supervisor.

Before submission, the system checks:

- All mandatory fields are filled
- Minimum number of photos have been uploaded
- Conclusions have been provided

What the Auditor sees: A confirmation message asking them to confirm submission. Once submitted, they cannot edit unless it's returned.

Who does this: The Auditor

System notifications:

- The Supervisor receives an email notification that an audit is ready for review
- A dashboard notification appears with the audit details

What happens next: The audit enters the Review stage.

Stage 6: Audit Review

What happens: The Supervisor carefully reviews the submitted audit to ensure quality and completeness.

What the Supervisor checks:

- Are the observations clear and accurate?
- Are the photos relevant and of good quality?
- Are the electrical measurements reasonable?
- Are the conclusions and recommendations appropriate?
- Is the overall audit complete and professional?

Options available to the Supervisor:

- **Approve:** The audit meets quality standards
- **Return for Corrections:** The audit needs changes (Supervisor must provide comments)

Who does this: Supervisor or Administrator

What happens next: Either approval or return.

Stage 7A: Audit Returned (If Corrections Needed)

What happens: If the Supervisor finds issues, they return the audit to the Auditor with comments explaining what needs to be corrected.

The return includes:

- Specific comments on what needs to be fixed
- References to which sections need attention
- Deadline for resubmission (if applicable)

What the Auditor does:

- Reviews the feedback
- Makes the necessary corrections
- Resubmits the audit

Who does this: Auditor (corrections), Supervisor (return action)

System notifications:

- The Auditor receives an email with the return reason
- A dashboard notification highlights the returned audit

What happens next: The audit goes back to the Review stage after resubmission.

Stage 7B: Audit Approved

What happens: The Supervisor confirms that the audit meets all quality standards and approves it for report generation.

Who does this: Supervisor or Administrator

What happens next: The report can now be generated.

Stage 8: Report Generation

What happens: The approved audit data is used to automatically generate professional reports.

Reports generated:

- **Microsoft Word Document (.docx):** Formatted report with company branding, tables, and embedded photos
- **PDF Document (.pdf):** Print-ready version with the same content

Report features:

- Company logo and branding
- All audit data presented in a professional format
- Photos with captions
- Tables for electrical measurements
- Conclusions and recommendations section
- Signature area for the Principal Consultant

Who does this: Supervisor, Administrator, or Manager

What happens next: The report is ready for delivery to the client.

Stage 9: Report Delivery

What happens: The final report is sent to the client through one or more channels.

Delivery options:

- **Email:** Send the report directly to the client's email address
- **Client Portal:** Upload to a secure portal where the client can download it
- **Secure Link:** Generate a time-limited, password-protected link to share the report
- **Manual Delivery:** Mark as "delivered manually" if sent through other means

Who does this: Administrator, Manager, or Supervisor

System notifications:

- The client receives an email with the report or a link to access it
- Internal notification confirms successful delivery

What happens next: The audit is marked as Delivered.

Stage 10: Post-Delivery (Editing if Needed)

What happens: Sometimes, after delivery, corrections or updates may be needed (e.g., client requests a change, or an error is discovered).

How editing works:

- An authorized user (Supervisor or higher) can request to edit a delivered report
- They must provide a reason for the edit
- The original version is preserved, and a new version is created
- The new version is numbered (e.g., v1.1, v1.2)
- A complete history of changes is maintained

Who can do this: Supervisor, Administrator, or Manager

What happens next: The updated report can be re-delivered to the client.

Stage 11: Audit Closure

What happens: Once the client has received the final report and no further changes are needed, the audit is closed.

Closing actions:

- The audit is marked as "Closed"
- All documents are archived
- The audit becomes read-only (no further edits allowed)
- The data is available for historical reference and analytics

Who does this: System (automatic after a set period) or Administrator (manual)

3.3 Workflow Rules and Validations

The system enforces certain rules to maintain data quality and process integrity:

1. **Mandatory Field Validation:** Audits cannot be submitted until all required fields are completed
2. **Minimum Photo Requirement:** Each audit type may require a minimum number of photos (e.g., at least 5 photos for a hospital audit)

3. **Sequential Progression:** Audits must follow the workflow stages in order (cannot skip from "Created" directly to "Approved")
4. **Self-Approval Prevention:** Auditors cannot approve their own audits; another person must review
5. **Change Justification:** Any edits after approval must include a reason
6. **Deadline Tracking:** Overdue audits are flagged automatically

---

4. Industry-Specific Audit Types

Different types of facilities have different electrical safety requirements. The system provides pre-designed audit forms for various industries.

4.1 Available Audit Types

Hospital Electrical Audit

Specialized sections:

- Emergency Power Systems (generators, UPS, changeover mechanisms)
- Critical Area Assessment (ICU, Operation Theatre, Dialysis Unit, Blood Bank)
- Medical Equipment Power (MRI rooms, CT Scan, X-Ray)
- Nurse Call and Communication Systems
- Fire Alarm Integration

Why it's different: Hospitals have life-critical equipment that requires uninterrupted power. The audit focuses heavily on backup power and isolation of sensitive equipment.

Hotel Electrical Audit

Specialized sections:

- Guest Room Electrical Safety
- Kitchen Equipment Power (commercial cooking equipment, cold storage)
- HVAC and Climate Control Systems
- Swimming Pool and Spa Electrical Safety
- Emergency Lighting and Exit Signs
- Banquet Hall and Event Space Wiring

Why it's different: Hotels have diverse electrical needs across public areas, guest rooms, kitchens, and recreational facilities, each with unique safety considerations.

Bank Electrical Audit

Specialized sections:

- Data Center and Server Room Power
- ATM Power Supply and Backup
- Security System Wiring (CCTV, alarms, access control)
- Cash Handling Equipment
- Vault Environmental Controls
- Customer Service Area Safety

Why it's different: Banks require extreme reliability for electronic systems, with emphasis on data center cooling and security system power.

Manufacturing Electrical Audit

Specialized sections:

- Heavy Machinery and Motor Wiring
- Industrial Control Systems (PLCs, SCADA)
- High Voltage Equipment
- Compressed Air and Hydraulic System Motors
- Hazardous Area Installations (if applicable)
- Power Factor Correction Equipment

Why it's different: Factories have heavy electrical loads, often with three-phase motors and specialized industrial equipment requiring specific safety measures.

Retail Electrical Audit

Specialized sections:

- Display and Promotional Lighting
- Point of Sale Systems
- Cold Storage and Refrigeration (for supermarkets)
- Escalator and Elevator Systems (for malls)
- Signage and Facade Lighting
- Stock Room and Storage Areas

Why it's different: Retail spaces have high-density lighting and must balance aesthetics with safety, plus special requirements for refrigerated goods.

Educational Institution Audit

Specialized sections:

- Computer Laboratory Power
- Science Laboratory Equipment
- Auditorium and PA Systems
- Sports Facility Lighting
- Hostel and Residential Buildings
- Canteen and Food Service Areas

Why it's different: Schools and colleges have laboratories with sensitive equipment and must prioritize student safety.

Residential Complex Audit

Specialized sections:

- Common Area Lighting and Power
- Elevator and Lift Systems
- Water Pump Installations
- Generator Backup Systems
- Individual Meter Panels
- Parking and Basement Lighting

Why it's different: Residential buildings need to balance shared infrastructure with individual unit safety.

4.2 Selecting an Audit Type

When creating a new audit, the Administrator selects the appropriate type from a visual menu. The system then loads the specific form with relevant sections for that industry.

Custom Templates: Super Administrators can also create custom audit templates for unique situations or client-specific requirements.

---

5. Notification and Communication System

The system keeps everyone informed through automatic notifications at every stage of the workflow.

5.1 Email Notifications

Emails are sent automatically when important events happen:

Event	Who Gets Notified	Email Content
New Audit Created	Assigned Auditor, Their Supervisor	Audit details, client info, due date
Audit Assigned	Auditor	Assignment details, expected timeline
Audit Accepted	Supervisor, Administrator	Confirmation that auditor will proceed
Audit Submitted	Supervisor	Notification that review is needed
Audit Approved	Auditor, Administrator	Confirmation of approval
Audit Returned	Auditor	What needs to be corrected, comments
Report Delivered	Client, Administrator	Confirmation of delivery, download link
Audit Overdue	Auditor, Supervisor, Administrator	Warning that deadline has passed
Ticket Created	Support Team	Issue details that need attention
Ticket Resolved	Person who raised ticket	Resolution details

Email Preferences: Users can customize which emails they receive. For example, a busy administrator might choose to receive only critical notifications.

5.2 Dashboard Notifications

When users log in to the system, they see real-time notifications in a notification panel:

Types of in-app notifications:

- 🔴 **Urgent:** Overdue audits, system alerts (shown prominently)
- 🟡 **Action Required:** Items waiting for your action (audits to review, approve, etc.)
- 🔵 **Informational:** Updates on audits you're involved with
- ⚪ **Archive:** Read notifications kept for reference

Notification features:

- **Badge Count:** Shows number of unread notifications
- **Direct Links:** Click a notification to go directly to the relevant audit
- **Mark as Read:** Individually or all at once
- **Notification History:** Access past notifications even after reading

---

5.3 Reminder System

The system automatically sends reminders to prevent delays:

- **Approaching Deadline:** Reminder sent 24 hours before an audit is due
- **Overdue Alerts:** Daily reminders for overdue audits (escalating to supervisors)
- **Pending Review:** Reminder if a submitted audit hasn't been reviewed within 24 hours
- **Incomplete Draft:** Reminder if an audit has been in draft status for more than 48 hours

---

5.4 Daily and Weekly Digests

Users can opt to receive summary emails:

- **Daily Digest:** Summary of all activities from the previous day
- **Weekly Summary:** Overview of the week's audits, completions, and pending items

---

6. Smart Search System

The system includes a powerful search feature that makes it easy to find any audit, report, or user quickly.

6.1 How Search Works

Instant Results: As you type in the search box, results appear immediately without pressing Enter. This is similar to how Google or popular apps show suggestions as you type.

Example:

- User types: "Apo..."
- System immediately shows:
  - Apollo Hospital - Jayanagar (Audit)
  - Apollo Hospital - Koramangala (Audit)
  - Apollo Hospitals Group (Client)
  - Apollo Hospital December Report (Document)

6.2 What You Can Search For

Search Category	What It Finds	Example Searches
Audits	Past and current audits	"HDFC Koramangala", "pending audits", "hospital audits"
Reports	Generated documents	"December reports", "Apollo report"
Clients	Client companies and their branches	"ICICI Bank", "Taj Hotels"
Users	Team members	"Priya", "john@sustenergy.com"
Tickets	Support tickets and feedback	"report error", "ticket #1234"

6.3 Search Filters

Users can narrow down results using filters:

- **Date Range:** Find audits from a specific period (e.g., "Last 30 days", "December 2025")
- **Status:** Filter by audit status (e.g., "Pending Review", "Completed")
- **Audit Type:** Filter by industry (e.g., "Hospital", "Bank")
- **Assigned To:** Find audits assigned to a specific person

- **Client:** Find all audits for a specific client

6.4 Recent and Trending Searches

The search box shows:

- **Recent Searches:** Your last few searches for quick access
- **Trending:** Popular searches across the team

6.5 Search Results and Navigation

When you click a search result:

- **For Audits:** Opens the audit details page
- **For Reports:** Opens or downloads the document
- **For Clients:** Shows all audits for that client
- **For Users:** Shows audits assigned to that user

---

7. Audit History and Record Keeping

The system maintains a complete history of all activities, ensuring accountability and enabling review of past actions.

7.1 Audit Trail

Every action taken on an audit is recorded with:

- **What was done:** The specific action (created, assigned, submitted, approved, etc.)
- **Who did it:** The name of the user who performed the action
- **When it happened:** Date and time stamp
- **Additional details:** Any relevant notes or comments

Example Audit History:

Date & Time	Action	Performed By	Details
Dec 26, 2025 3:30 PM	Report Generated	Rahul Sharma	Version 1.1 created
Dec 26, 2025 2:45 PM	Corrections Made	Priya Singh	Updated power parameters
Dec 26, 2025 12:00 PM	Returned for Correction	Rahul Sharma	"Voltage readings inconsistent"
Dec 25, 2025 5:30 PM	Submitted for Review	Priya Singh	12 photos attached
Dec 25, 2025 9:00 AM	Audit Started	Priya Singh	Location verified via GPS
Dec 24, 2025 4:00 PM	Audit Accepted	Priya Singh	-
Dec 24, 2025 2:30 PM	Audit Assigned	Admin User	Assigned to Priya Singh
Dec 24, 2025 2:00 PM	Audit Created	Admin User	Hospital Electrical Audit

---

7.2 Document Version History

Every time a report is regenerated (e.g., after corrections), a new version is created:

- **Original Version:** v1.0 - First generated report

- **Subsequent Versions:** v1.1, v1.2, etc. - Updated reports

For each version, the system stores:

- The complete document file
- Who generated it
- When it was generated
- What changes were made from the previous version

Version Comparison: Users can compare two versions side-by-side to see what changed.

7.3 Archiving and Retention

Active Audits: All in-progress audits are easily accessible from the main dashboard.

Completed Audits: Closed audits move to the archive but remain searchable and accessible.

Retention Policy: Records are kept permanently unless a specific retention period is configured by the Super Administrator.

7.4 System Activity Log (For Administrators)

Super Administrators have access to a comprehensive log of all system activities:

- User logins and logouts
- User account changes (created, modified, deleted)
- Role and permission changes
- Configuration changes
- Report downloads
- Any unusual activity

This log helps maintain security and investigate any issues that may arise.

---

8. Ticketing and Feedback System

The system includes a built-in helpdesk for users to report issues, request help, or provide feedback.

8.1 What Tickets Are For

Ticket Type	Use Case	Priority
Bug Report	Something in the system isn't working correctly	High
Help Request	User needs assistance with a task	Medium
Feature Suggestion	User has an idea for improving the system	Low
Audit Question	Clarification needed about a specific audit	Medium
Document Issue	Problem with a generated report	High
Access Request	User needs access to something they can't see	Medium
General Feedback	Comments about the system overall	Low

8.2 Creating a Ticket

Any user can create a ticket by:

1. Clicking the "Help" or "Support" button in the system
2. Selecting the type of issue
3. Providing a clear subject line
4. Describing the issue in detail
5. Attaching screenshots or files if helpful
6. Submitting the ticket

Linking to Audits: When creating a ticket about a specific audit, users can link the ticket to that audit for context.

8.3 Ticket Lifecycle

1. **Created:** User submits the ticket
2. **Open:** Ticket is waiting to be assigned to a support person
3. **In Progress:** Someone is working on resolving the issue
4. **Awaiting Response:** Support has asked the user for more information
5. **Resolved:** The issue has been fixed or the question answered
6. **Closed:** User confirms the resolution (or closes automatically after a period)

Reopening: If the issue comes back, users can reopen a closed ticket.

8.4 Response Time Expectations

Priority Level	Initial Response	Resolution Target
Urgent	Within 1 hour	Same day
High	Within 4 hours	Within 24 hours
Medium	Within 24 hours	Within 48 hours
Low	Within 48 hours	Within 7 days

8.5 Ticket Dashboard

Users can see all their tickets in one place:

- **My Open Tickets:** Issues I've raised that are still being worked on
- **Resolved Tickets:** Issues that have been fixed
- **All My Tickets:** Complete history of my support requests

Administrators can see tickets from all users for management and oversight.

---

9. Dashboards and Reports

The system provides visual dashboards tailored to each user role, showing relevant information at a glance.

9.1 Auditor Dashboard

What an Auditor sees:

- My Assigned Audits (list with status and due dates)
- Audits Due This Week (calendar view)
- Audits Returned for Correction (highlighted for attention)

- My Performance Summary (audits completed this month, average turnaround time)
- Recent Notifications

9.2 Supervisor Dashboard

What a Supervisor sees:

- Team Overview (auditors and their current workload)
- Pending My Review (audits waiting for approval)
- Team Audits by Status (how many in progress, pending, overdue)
- Overdue Alerts (audits that have missed deadlines)
- Team Performance Metrics (completion rates, quality scores)
- Recent Activities (team actions in the last 24 hours)

9.3 Manager/Administrator Dashboard

What a Manager sees:

- Department Summary (total audits, completion rates, revenue if applicable)
- Audits by Client (which clients have active audits)
- Monthly Trend (audits over time, comparison with previous months)
- Team Workload (who has capacity, who is overloaded)
- Pending Approvals (if applicable)
- Client Satisfaction (feedback scores)
- Escalations (any issues that need attention)

9.4 Super Administrator Dashboard

What a Super Admin sees:

- Organization Overview (all departments, all metrics)
- System Health (any technical issues, storage usage)
- User Statistics (total users, active users, new users)
- All Audits Summary (across the organization)
- Financial Overview (if billing is tracked)
- Security Alerts (failed logins, unusual activity)
- Settings and Configuration Status

9.5 Key Performance Indicators (KPIs)

The system tracks and displays important metrics:

KPI	What It Measures	Target
Completion Rate	Percentage of audits completed on time	95%
Average Turnaround Time	Days from assignment to delivery	Under 3 days
First-Time Approval Rate	Audits approved without returns	85%
Client Satisfaction Score	Average rating from clients	4.5 out of 5
Overdue Percentage	Audits that missed deadlines	Under 5%

User Productivity	Audits completed per auditor per month	15+

---

10. Security and Data Protection

The system implements robust security measures to protect sensitive audit data.

10.1 User Access Security

Login Security:

- Strong password requirements (minimum length, complexity)
- Account lockout after multiple failed attempts
- Optional two-factor authentication (additional code sent to phone)
- Session timeout after inactivity

Password Management:

- Secure password reset via email
- No password sharing (each user has their own account)
- Regular password change reminders (optional)

10.2 Data Access Controls

Principle of Least Access: Users can only see and do what is necessary for their role.

Examples:

- Auditors cannot see audits assigned to other auditors
- Supervisors can only see audits within their team
- Client users (if set up) can only see their own audit reports

Sensitive Data Protection:

- Client contact information is only visible to authorized personnel
- Financial data (if any) has additional access restrictions

10.3 Data Backup and Recovery

Automatic Backups:

- The system automatically backs up all data daily
- Backups are stored securely in a separate location
- In case of any system failure, data can be restored

Document Storage:

- All generated reports are saved securely
- Photos and attachments are stored with high reliability
- No risk of data loss even if a user's device fails

10.4 Audit Trail for Compliance

The complete activity log helps with:

- Demonstrating compliance with regulations

- Investigating any disputes or discrepancies
- Supporting legal requirements for record keeping

---

11. Implementation Approach

The enterprise upgrade will be implemented in phases to ensure smooth adoption.

Phase 1: Foundation (Weeks 1-4)

- Set up user accounts and roles
- Implement login and basic access control
- Create the main dashboard framework
- Migrate existing data

Phase 2: Workflow Engine (Weeks 5-8)

- Implement the complete audit workflow
- Set up status transitions and validations
- Build notification system (email and in-app)
- Test with pilot users

Phase 3: Industry Templates (Weeks 9-10)

- Create templates for all industry types
- Build template selection interface
- Test forms with real audit scenarios

Phase 4: Search and History (Weeks 11-12)

- Implement smart search with autocomplete
- Build audit history and version tracking
- Create activity logging system

Phase 5: Ticketing and Feedback (Weeks 13-14)

- Set up ticketing system
- Implement feedback collection
- Configure response workflows

Phase 6: Dashboards and Polish (Weeks 15-16)

- Build role-based dashboards
- Add analytics and KPI displays
- Conduct user acceptance testing
- Fix any issues and launch

---

12. Training and Support

12.1 User Training

Training Sessions:

- Role-based training (different sessions for Administrators, Supervisors, Auditors)
- Hands-on practice with sample audits
- Quick reference guides for daily tasks

Training Materials:

- Video tutorials for common tasks
- Step-by-step user manuals
- FAQ documents

12.2 Ongoing Support

Help Resources:

- In-app help tooltips and guides
- Searchable knowledge base
- Ticketing system for issues

Support Availability:

- Business hours support for general questions
- Priority support for urgent issues

---

13. Success Criteria

The enterprise upgrade will be considered successful when:

Criterion	Target	How We'll Measure
User Adoption	90% of team actively using the system	Weekly login rates
Audit Completion	95% completed on time	System reports
Client Satisfaction	4.5/5 average rating	Feedback surveys
Turnaround Time	Under 48 hours average	System analytics
Error Rate	Under 2% of audits returned twice	Return statistics
Search Effectiveness	Under 5 seconds to find any audit	User feedback
System Uptime	99.5% availability	System monitoring

---

14. Glossary

Term	Meaning
Audit	A formal inspection and assessment of electrical safety at a facility
RBAC	Role-Based Access Control - limiting access based on user roles
Workflow	The sequence of steps an audit goes through from creation to completion
Template	A pre-designed form with sections specific to an industry type
Ticket	A support request raised by a user
Dashboard	A visual summary screen showing key information at a glance
Turnaround Time (TAT)	The time taken from audit assignment to report delivery
Draft	An incomplete audit that has been saved but not submitted

Archive	Storage of completed audits for historical reference
Version	A specific iteration of a report (v1.0, v1.1, etc.)

---

15. Appendix

A. Related Documents

- [Project_Scope_Document.md] - Current application features
- [Mobile_App_Scope.md] - Mobile application plans
- [Future_Features_Proposal.md] - Original feature ideas

B. Document History

Version	Date	Author	Changes
1.0	December 26, 2025	Sustenergy Team	Initial document

Document Prepared By: Sustenergy Development Team
For: Sustenergy Foundation
Last Updated: December 26, 2025