Galaxy ISO Audit Management System

Product Explainer

Enterprise Audit Workflow Digitization Platform

Version 1.0

Date: January 03, 2026

Table of Contents

1. Executive Summary

The Galaxy ISO Audit Management System is an enterprise-grade platform designed to digitize and streamline the entire organizational audit lifecycle. It replaces traditional paper-based audit processes with a modern, secure, and role-based digital solution that ensures compliance with international standards including ISO 19011, ISO 27001, ISO 9001, and other frameworks.

This system enables organizations to manage audits from initial planning through execution, reporting, follow-up, and final closure. It provides real-time visibility into audit status, findings, corrective actions, and compliance metrics through intuitive dashboards and analytics.

2. What is Galaxy Audit System

Galaxy Audit System is a comprehensive audit management platform that helps organizations:

Plan and schedule audits	Create annual audit programmes with risk-based prioritization
Execute audits efficiently	Collect evidence, document findings, and track progress
Generate reports	AI-powered report generation with ISO-compliant formatting
Manage corrective actions	Track CAPA items from identification to closure
Ensure compliance	Built-in support for multiple ISO frameworks
Analyze trends	Dashboard analytics for continuous improvement

3. Key Benefits

3.1 For Organizations

- Reduced audit cycle time through automation and streamlined workflows
- Improved compliance with ISO standards and regulatory requirements
- Centralized repository for all audit documentation and evidence
- Real-time visibility into audit status and organizational risk posture
- Cost savings through elimination of paper-based processes
- Better decision-making with analytics and trend analysis

3.2 For Audit Teams

- Structured workflow guidance following ISO 19011 methodology

- Easy evidence collection and management
- Collaborative tools for team-based audits
- AI-assisted report generation saves time
- Mobile-friendly interface for field audits
- Clear task assignments and progress tracking

3.3 For Management

- Executive dashboard with key performance indicators
- Risk heatmaps for quick risk assessment
- Compliance score tracking across frameworks
- Audit programme oversight and resource planning
- Trend analysis for continuous improvement initiatives

4. Core Features

Multi-Role Access Control	Six distinct user roles with granular permissions ensure proper segregation of duties
Complete Audit Lifecycle	End-to-end support from planning through closure following ISO 19011
Digital Working Papers	Electronic evidence management with version control and timestamping
Automated Workflows	Multi-level approval processes for reports and documents
Real-Time Collaboration	Query threads between auditors and auditees
AI-Powered Reports	Automatic report generation using audit findings
Risk Assessment	5x5 risk matrix with likelihood and impact scoring
CAPA Management	Corrective and preventive action tracking with root cause analysis
Document Control	Centralized document library with approval workflows
Analytics Dashboard	Executive insights with charts, graphs, and KPIs
Gap Analysis	Compare current state against ISO requirements
Asset Management	Track organizational assets linked to audits and risks

5. User Roles and Access

The system implements role-based access control (RBAC) with six predefined roles. Each role has specific permissions aligned with ISO requirements for segregation of duties.

Role	Description	Key Permissions
System Admin	Full system access	All features, user management, configuration
Audit Manager	Plans and oversees audits	Create audits, assign teams, approve reports, analytics
Auditor	Conducts audits	Execute audits, collect evidence, document findings
Department Head	Reviews findings	View department audits, approve workflows, CAPA
Department Officer	Responds to audits	View assigned audits, upload evidence, respond to queries
Viewer	Read-only access	View audits and reports only

6. The Audit Lifecycle

The system follows the ISO 19011 audit methodology with seven distinct phases:

Phase	ISO Reference	Activities
1. Planned	Clause 6.2	Audit is scheduled in the annual programme
2. Initiated	Clause 6.2	Define objectives, scope, criteria, assign team
3. Preparation	Clause 6.3	Create checklists, request documents, plan interviews
4. Executing	Clause 6.4	Collect evidence, conduct interviews, document findings
5. Reporting	Clause 6.5	Generate report, submit for approval
6. Follow-up	Clause 6.6	Track corrective actions, verify implementation
7. Closed	-	All actions complete, audit archived

Audit Workflow Summary

Planning: Create audit in the system with title, scope, and risk rating. Initiation: Define detailed objectives, criteria, and methodology. Team Assignment: Assign lead auditor and team members with specific roles. Preparation: Create checklists, send document requests, conduct risk assessment. Execution: Collect evidence, document observations, record findings. Reporting: Generate AI-assisted report, route through approval workflow. Follow-up: Create CAPA items, assign responsible persons, track completion. Closure: Verify all actions complete, finalize and archive the audit.

7. Module Descriptions

Dashboard

Provides a real-time overview of your audit programme including audit status distribution, open findings by severity, risk heatmap, compliance scores, CAPA status, and overdue follow-ups.

Audits

Central hub for managing individual audits through their complete lifecycle. Includes sub-sections for initiation, team assignment, preparation, work program, evidence, findings, queries, reports, and follow-up.

Workflows

Manages approval processes for audit reports and documents. Supports actions including approve, reject, return, sign, review, and acknowledge.

Planning

Annual audit programme management with risk-based scheduling, resource allocation, and audit prioritization.

Reports

Generate and manage audit reports with AI-powered content generation, version control, and export capabilities.

Follow-ups

Track corrective actions across all audits with status filtering, due date management, and completion verification.

Risk Assessment

Identify and assess risks using a 5x5 matrix. Calculate risk scores, define mitigation plans, and link controls to risks.

CAPA Management

Manage Corrective and Preventive Actions with root cause analysis, progress tracking, and effectiveness review.

Documents

Central document library with version control, approval workflows, expiry tracking, and confidentiality levels.

Assets

Manage organizational assets including hardware, software, data, people, facilities, and services.

Vendors

Third-party vendor management with risk ratings, compliance tracking, and contract management.

Analytics

Advanced reporting and trend analysis including audit completion trends, finding trends, and compliance scores.

Access Control

Fine-grained permission management with team assignment, user management, audit visibility, and role matrix.

8. ISO Compliance

The Galaxy Audit System is designed to support compliance with multiple international standards:

Standard	Coverage
ISO 19011:2018	Complete audit methodology from planning to follow-up
ISO 27001	Information security controls, risk assessment, CAPA
ISO 9001	Quality management, document control, corrective actions
ISO 31000	Risk management framework and assessment
ISO 22301	Business continuity management
COBIT 5	IT governance framework support
NIST	Cybersecurity framework alignment

Built-in Compliance Features

- EARS-compliant requirements documentation
- ISO-structured audit checklists with clause references
- Evidence upload with automatic timestamping
- Complete audit trail logging
- Segregation of duties through role-based access
- Document control with version history
- Gap analysis against ISO requirements
- CAPA tracking with root cause analysis

9. Technical Architecture

9.1 Technology Stack

Component	Technology
Backend Framework	FastAPI (Python)
Frontend Framework	Next.js 14 with React
Database	PostgreSQL (Supabase)
Authentication	JWT Token-based
ORM	SQLAlchemy
Styling	TailwindCSS
State Management	Zustand
API Client	Axios with React Query

9.2 Architecture Highlights

- Stateless architecture with no file storage in database

- RESTful API design with comprehensive documentation

- Responsive web interface accessible from any device

- Scalable cloud-native deployment options

- Database migrations managed through Alembic

- Type-safe development with TypeScript and Pydantic

10. Security Features

JWT Authentication	Secure token-based authentication with configurable expiration
Role-Based Access	Granular permissions based on user roles
Audit Trail	Complete logging of all user actions with timestamps
Input Validation	Server-side validation using Pydantic schemas

SQL Injection Prevention	ORM-based queries prevent injection attacks
XSS Protection	Built-in cross-site scripting prevention
CORS Configuration	Controlled cross-origin resource sharing
HTTPS Support	SSL/TLS encryption for data in transit

11. Getting Started

11.1 System Requirements

- Modern web browser (Chrome, Firefox, Safari, Edge)

- Internet connection

- Valid user account with assigned role

11.2 First Steps

1. Navigate to the system URL provided by your administrator

2. Enter your email address on the login page

3. Complete authentication (password or two-factor if enabled)

4. You will be directed to the Dashboard

5. Explore the sidebar menu to access different modules

6. Your available features depend on your assigned role

11.3 Quick Tips

- Check the Dashboard daily for overdue items and pending tasks

- Use the Workflows section to see tasks requiring your action

- Upload evidence for every finding to maintain audit quality

- Create CAPA items promptly for non-conformities

- Use the Analytics section to track improvement trends

- Contact your System Administrator for access issues

Support

For technical support, training requests, or feature inquiries, please contact your System Administrator or the IT Help Desk.