Galaxy ISO Audit Management System

USER MANUAL

Comprehensive Guide to Enterprise Audit Management

ISO 19011 Compliant Audit Workflow System

Document Version	1.0
Release Date	January 03, 2026
Classification	Internal Use
Department	Internal Audit

Table of Contents

1. Introduction 4

2. Getting Started 5

3. User Roles and Permissions 7

4. Dashboard Overview 9

5. Audit Management 11

6. Workflow Management 16

7. Risk Assessment 18

8. CAPA Management 20

9. Document Control 22

10. Gap Analysis 24

11. Reports and Analytics 26

12. Access Control 28

13. Asset and Vendor Management 30

14. Best Practices 32

15. Troubleshooting 33

16. Glossary 34

1. Introduction

1.1 About This Manual

This user manual provides comprehensive guidance for using the Galaxy ISO Audit Management System. The system is designed to digitize and streamline the entire organizational audit lifecycle, from planning through execution to follow-up and closure, in compliance with ISO 19011 guidelines.

1.2 System Overview

The Galaxy ISO Audit Management System is an enterprise-grade platform that replaces manual, paper-based audit processes with a modern, secure, role-based digital solution. The system supports multiple ISO frameworks including ISO 27001, ISO 9001, ISO 22301, and ISO 45001.

Key Features:

- Complete audit lifecycle management following ISO 19011 guidelines
- Multi-role access control with six distinct user roles
- Digital working papers and evidence management
- Automated workflow approval processes
- AI-powered report generation
- Real-time collaboration through query threads
- Comprehensive analytics and dashboards
- Risk assessment with ISO 31000 compliance
- CAPA management per ISO 9001 requirements
- Document control system with version management

1.3 ISO Compliance

The system is built to comply with international standards for audit management and quality systems:

Standard	Description	System Coverage
ISO 19011:2018	Guidelines for auditing management systems	Full audit lifecycle
ISO 27001	Information security management	Controls A.5-A.18
ISO 9001	Quality management systems	Clause 10.2 CAPA
ISO 31000	Risk management	Risk assessment module
ISO 22301	Business continuity	Checklist templates

2. Getting Started

2.1 System Requirements

The Galaxy ISO Audit Management System is a web-based application accessible through modern web browsers. No software installation is required on user workstations.

Supported Browsers:

- Google Chrome (recommended)
- Mozilla Firefox
- Microsoft Edge
- Safari

2.2 Accessing the System

To access the system, open your web browser and navigate to the system URL provided by your administrator. You will be presented with the login page.

2.3 Logging In

Follow these steps to log in:

1. Enter your registered email address in the Email field
2. Click the Sign In button
3. If Two-Factor Authentication is enabled, enter the 6-digit code from your authenticator app
4. Upon successful authentication, you will be redirected to the Dashboard

Note: The system uses JWT token-based authentication. Your session will remain active until you log out or the token expires.

2.4 Two-Factor Authentication

For enhanced security, the system supports Two-Factor Authentication (2FA). When enabled, you will need to provide a verification code from your authenticator app in addition to your email.

Setting up 2FA:

1. Access your profile settings
2. Enable Two-Factor Authentication
3. Scan the QR code with your authenticator app (Google Authenticator, Microsoft Authenticator, etc.)
4. Enter the verification code to confirm setup
5. Save your backup codes in a secure location

2.5 Navigation Overview

The system interface consists of a sidebar navigation menu on the left and the main content area. The sidebar provides access to all system modules based on your assigned role.

Module	Description

Dashboard	Overview of audit program metrics and KPIs
Audits	Create and manage individual audits
Workflows	Manage approval processes
Planning	Annual audit planning
Reports	Generate and view audit reports
Follow-ups	Track corrective actions
Risk Assessment	Identify and assess risks
CAPA Management	Corrective and preventive actions
Documents	Document control system
Assets	Asset inventory management
Vendors	Third-party vendor management
Analytics	Advanced reporting and trends
Users	User management
Departments	Organizational structure
Access Control	Role-based permissions

3. User Roles and Permissions

The system implements role-based access control (RBAC) to ensure proper segregation of duties as required by ISO standards. Each user is assigned a primary role that determines their access level.

3.1 Role Definitions

Role	Description	Access Level
System Admin	Full system access including user management, configuration, and all modules	Full Access
Audit Manager	Plans and oversees audits, assigns teams, reviews findings, approves reports	Planning, Audits, Findings, Analytics, Assets, Vendors
Auditor	Conducts audits, collects evidence, documents findings, creates reports	Audits, Evidence, Findings
Department Head	Reviews audit findings for their department, approves corrective actions	View audits, Approve workflows
Department Officer	Responds to audit queries, provides evidence, implements actions	View assigned audits, Upload evidence
Viewer	Read-only access to audit information and reports	View only

3.2 Module Access by Role

Module	Admin	Manager	Auditor	Dept Head	Officer	Viewer
Dashboard	Yes	Yes	Yes	Yes	Yes	Yes
Audits	Yes	Yes	Yes	Yes	Yes	Yes
Workflows	Yes	Yes	Yes	Yes	Yes	Yes
Planning	Yes	Yes	No	No	No	No
Reports	Yes	Yes	Yes	Yes	Yes	Yes
Follow-ups	Yes	Yes	Yes	Yes	Yes	Yes
Risk Assessment	Yes	Yes	Yes	Yes	Yes	Yes
CAPA	Yes	Yes	Yes	Yes	Yes	Yes
Documents	Yes	Yes	Yes	Yes	Yes	Yes
Assets	Yes	Yes	No	No	No	No
Vendors	Yes	Yes	No	No	No	No
Analytics	Yes	Yes	No	No	No	No
Users	Yes	No	No	No	No	No
Departments	Yes	No	No	No	No	No

Access Control	Yes	Yes	No	No	No	No

3.3 Audit Visibility Rules

Audit visibility is controlled based on user role and department assignment:

System Administrators can view all audits in the system
Audit Managers can view audits in their department plus audits assigned to them
Auditors can only view audits they are assigned to as team members
Department Heads and Officers can view audits related to their department
Viewers have read-only access to audits they are permitted to see

4. Dashboard Overview

The Dashboard provides a comprehensive overview of your audit program at a glance. It displays key metrics, compliance scores, risk information, and pending actions.

4.1 Metrics Overview

The top section displays key performance indicators for your audit program:

- Total Audits: Count of all audits in the system with status breakdown
- Open Findings: Number of unresolved findings categorized by severity
- Compliance Score: Overall compliance percentage across frameworks
- Pending Actions: Count of overdue follow-ups and CAPA items

4.2 Risk Heatmap

The Risk Heatmap visualizes risks across a 5x5 matrix based on likelihood and impact scores. Colors indicate risk severity:

- Green (1-4): Low risk - acceptable with monitoring
- Yellow (5-9): Medium risk - requires attention
- Orange (10-15): High risk - requires mitigation
- Red (16-25): Critical risk - immediate action required

4.3 Compliance Gauges

Circular gauges display compliance scores for each ISO framework being tracked. The gauges show the percentage of requirements that have been assessed as compliant.

4.4 CAPA Tracker

The CAPA Tracker section shows the status of Corrective and Preventive Actions:

- Open: Newly created CAPA items awaiting action
- In Progress: CAPA items currently being implemented
- Pending Verification: Completed actions awaiting effectiveness review
- Closed: Verified and completed CAPA items

4.5 Quick Actions

The Quick Actions section provides shortcuts to common tasks:

- New Audit - Create a new audit
- Risk Assessment - Start a new risk assessment
- Generate Report - Create an AI-powered audit report
- CAPA Management - Access corrective action tracking

5. Audit Management

The Audits module is the core of the system, managing the complete audit lifecycle in accordance with ISO 19011:2018 guidelines.

5.1 Audit Lifecycle

Each audit progresses through defined phases as specified in ISO 19011:

Phase	ISO Clause	Description
Planned	6.2	Audit is scheduled but not yet started
Initiated	6.2	Objectives, scope, criteria defined; team assigned
Preparation	6.3	Checklists created, documents requested, interviews planned
Executing	6.4	Evidence collection, interviews, observations documented
Reporting	6.5	Audit report generated with findings and recommendations
Follow-up	6.6	Corrective actions tracked and verified
Closed	-	Audit complete, all actions verified

5.2 Creating an Audit

To create a new audit:

1. Navigate to Audits from the sidebar
2. Click the Create Audit button
3. Enter the audit title and select the audit year
4. Define the audit scope and select the target department
5. Assign a risk rating (Low, Medium, High, Critical)
6. Click Create to save the audit

5.3 Audit Initiation (ISO 19011 Clause 6.2)

During initiation, you define the audit parameters:

Objectives: What the audit aims to achieve
Scope: Boundaries and extent of the audit
Criteria: Standards and requirements to audit against
Methodology: Approach and techniques to be used
Feasibility: Confirmation that the audit can be conducted

5.4 Team Assignment

Assign qualified personnel to the audit team:

Lead Auditor: Heads the audit team, responsible for overall audit conduct
Senior Auditor: Experienced auditor who can mentor others
Auditor: Conducts audit procedures and collects evidence
Technical Specialist: Provides expertise in specific technical areas
Observer: Watches the audit process for training or oversight
Trainee Auditor: Learning auditor under supervision

5.5 Audit Preparation (ISO 19011 Clause 6.3)

Preparation activities include:

Creating audit checklists based on ISO requirements
Sending document requests to auditees
Conducting preliminary risk assessment
Planning interview schedules
Reviewing previous audit findings

5.6 Audit Execution (ISO 19011 Clause 6.4)

During execution, auditors collect evidence and document findings:

Evidence Collection:

Upload supporting documents (images, PDFs, spreadsheets)
Record interview notes and observations
Link evidence to specific controls or requirements
Automatic timestamping for audit trail

Documenting Findings:

Major Non-conformity: Significant failure to meet requirements
Minor Non-conformity: Isolated lapse that does not affect system effectiveness
Observation: Area for potential improvement
Opportunity for Improvement: Suggestion for enhancement

5.7 Query Management

The Queries feature enables communication between auditors and auditees:

Create queries requesting clarification or additional information
Auditees receive notifications and can respond directly
Full conversation history maintained for audit trail
Queries can be linked to specific findings or evidence

5.8 Work Program

The Work Program defines the audit procedures to be performed:

- Define specific audit procedures and tests
- Assign procedures to team members
- Track completion status of each procedure
- Link procedures to evidence collected

5.9 Audit Reporting (ISO 19011 Clause 6.5)

Generate comprehensive audit reports:

- AI-powered report generation from audit findings
- ISO-structured report sections (Executive Summary, Scope, Findings, Recommendations)
- Version control for report revisions
- Multi-level approval workflow
- Export to PDF and Word formats

5.10 Follow-up (ISO 19011 Clause 6.6)

Track corrective actions after the audit:

- Create follow-up items for each finding
- Assign responsible persons and due dates
- Track implementation progress
- Upload evidence of completion
- Verify effectiveness of corrective actions

5.11 Closing an Audit

To close an audit, ensure all follow-up items are complete and verified. Click the Close Audit button to finalize. Once closed, the audit status is locked and the audit is archived for future reference.

6. Workflow Management

The Workflow module manages approval processes for audit reports and documents, ensuring proper authorization as required by ISO standards.

6.1 Understanding Workflows

Workflows define the sequence of approvals required before a document or report can be finalized. Each workflow consists of multiple steps, with each step assigned to a specific user or department.

6.2 Creating a Workflow

To create a new workflow:

1. Navigate to Workflows from the sidebar
2. Click Create Workflow
3. Select the audit or document to associate with the workflow
4. Add approval steps in sequence
5. Assign each step to a user or department
6. Save the workflow

6.3 Workflow Actions

Users can perform the following actions on workflow steps:

Action	Description
Approve	Accept the item and move to the next step
Reject	Send back with comments for revision
Return	Request changes without full rejection
Sign	Add digital signature to the document
Review	Mark as reviewed without formal approval
Acknowledge	Confirm receipt of the document

6.4 Workflow Status

Workflows progress through the following statuses:

Pending: Workflow created but not yet started
In Progress: Currently being processed through approval steps
Approved: All steps completed successfully
Rejected: Workflow rejected at one of the steps

6.5 My Tasks

The Workflows badge in the sidebar shows the count of pending tasks assigned to you. Click on Workflows to view and action your pending approvals.

7. Risk Assessment

The Risk Assessment module enables identification, assessment, and management of risks in compliance with ISO 31000 and ISO 27005 standards.

7.1 Risk Assessment Process

The risk assessment process follows these steps:

1. Identify the risk and provide a description
2. Assess likelihood (1-5 scale)
3. Assess impact (1-5 scale)
4. System calculates risk rating (Likelihood x Impact)
5. Define mitigation plans and controls
6. Link risks to assets, findings, or CAPA items

7.2 Risk Scoring

Risks are scored using a 5x5 matrix:

Score Range	Category	Action Required
1-4	Low	Monitor and review periodically
5-9	Medium	Implement controls within defined timeframe
10-15	High	Prioritize mitigation actions
16-25	Critical	Immediate action required

7.3 Risk Matrix View

The Risk Matrix tab provides a visual representation of all risks plotted on a 5x5 grid. Click on any cell to view risks at that likelihood/impact intersection.

7.4 Control Suggestions

The system provides AI-suggested controls based on ISO 27001 Annex A. When viewing a risk, you can see recommended controls and add them to your mitigation plan.

7.5 Risk Linking

Risks can be linked to other entities in the system:

Assets - Link risks to specific organizational assets
Audits - Associate risks with audit findings
CAPA - Create corrective actions for risk mitigation
Controls - Map risks to implemented controls

8. CAPA Management

The CAPA (Corrective and Preventive Action) module manages actions to address non-conformities and prevent recurrence, as required by ISO 9001 Clause 10.2.

8.1 CAPA Types

Corrective: Actions to fix existing problems and prevent recurrence
Preventive: Actions to prevent potential problems from occurring
Both: Combined corrective and preventive approach

8.2 CAPA Workflow

CAPA items progress through the following statuses:

Open: CAPA created and awaiting action
In Progress: Actions being implemented
Pending Verification: Awaiting effectiveness check
Closed: Verified and complete

8.3 Creating a CAPA

To create a new CAPA:

1. Navigate to CAPA Management from the sidebar
2. Click Create New CAPA
3. Enter the CAPA title and description
4. Select the CAPA type (Corrective, Preventive, or Both)
5. Link to related findings, risks, or gaps
6. Assign a responsible person and due date
7. Save the CAPA

8.4 Root Cause Analysis

The system supports root cause analysis using the Five Whys technique. Click Root Cause Analysis on a CAPA to document the analysis process.

8.5 Effectiveness Review

After implementing corrective actions, conduct an effectiveness review to verify that the actions have resolved the issue and prevented recurrence.

Document the review date and reviewer
Assess whether the root cause was addressed
Verify that the problem has not recurred
Record any additional observations
Close the CAPA if effective

8.6 CAPA Tracker

The CAPA Tracker provides an overview of all CAPA items with filtering options:

Filter by status, type, or assignee
View progress percentage for each CAPA
Track overdue items
Export CAPA data for reporting

9. Document Control

The Document Control module provides ISO 9001 and ISO 27001 compliant document management with version control, approval workflows, and expiry tracking.

9.1 Document Lifecycle

Documents progress through the following stages:

Draft: Document created but not yet submitted for review
Under Review: Document submitted for approval
Approved: Document approved and ready for use
Active: Document currently in use
Expired: Document past its expiry date
Archived: Document no longer active but retained for records

9.2 Uploading Documents

To upload a new document:

1. Navigate to Documents from the sidebar
2. Click Upload Document
3. Select the file to upload
4. Enter document metadata (title, number, type)
5. Select the department and confidentiality level
6. Set the expiry date if applicable
7. Assign a responsible person
8. Click Upload

9.3 Document Types

The system supports various document types:

Policies and Procedures
HR Manual
Business Continuity Policy
Access Control Policy
Cryptography Policy
Backup Policy
Acceptable Use Policy
Standard Operating Procedures (SOPs)
Training Records
Contracts and Agreements

9.4 Confidentiality Levels

Public: Available to all users
Internal: Available to internal staff only
Confidential: Restricted to specific departments

Restricted: Highly sensitive, limited access

9.5 Version Control

The system maintains version history for all documents. When uploading a new version, the previous version is retained for audit trail purposes.

9.6 Document Approval

Documents requiring approval go through a workflow process. Approvers can review the document, add comments, and approve or reject.

9.7 Expiry Tracking

The system tracks document expiry dates and provides alerts for documents expiring soon. The Expiring tab shows all documents requiring attention.

10. Gap Analysis

The Gap Analysis module enables comparison of your organization against ISO framework requirements to identify compliance gaps and track remediation.

10.1 Compliance Dashboard

The Compliance Dashboard provides an overview of your compliance status:

- Overall compliance percentage across frameworks
- Gaps by severity (Critical, High, Medium, Low)
- Remediation progress tracking
- Trend analysis over time

10.2 Framework Analysis

Compare your organization against multiple ISO frameworks:

- ISO 27001 - Information Security Management
- ISO 9001 - Quality Management
- ISO 22301 - Business Continuity
- ISO 45001 - Occupational Health and Safety

10.3 Conducting Gap Analysis

To conduct a gap analysis:

1. Select the ISO framework to assess against
2. Review each clause or control requirement
3. Assess current compliance status
4. Document gaps and evidence
5. Assign severity to each gap
6. Create remediation plans

10.4 Compliance Tracker

The Compliance Tracker monitors individual gaps across frameworks and departments. Filter by status, severity, or framework to focus on priority items.

10.5 Gap Remediation

Manage gap closure through CAPA integration:

- Create CAPA items directly from gaps
- Track remediation progress
- Upload evidence of closure
- Verify effectiveness of remediation

11. Reports and Analytics

11.1 Report Generation

The Reports module enables generation of ISO 19011 compliant audit reports:

- AI-powered report generation from audit findings
- ISO-structured report sections
- Version control for report revisions
- Multi-level approval workflow
- Export to PDF and Word formats

11.2 Generating a Report

To generate a new report:

1. Navigate to Reports from the sidebar
2. Click Generate New Report
3. Select the audit to generate a report for
4. The system will compile findings and generate the report
5. Review and edit the generated content
6. Submit for approval through workflow

11.3 Report Structure

Generated reports follow the ISO 19011 structure:

- Executive Summary
- Audit Objectives and Scope
- Audit Criteria
- Audit Methodology
- Findings (Conformities and Non-conformities)
- Evidence Summary
- Recommendations
- CAPA Plan
- Conclusion

11.4 Analytics Dashboard

The Analytics module provides advanced reporting and trend analysis:

- Audit completion trends over time
- Finding trends by severity
- Compliance score trends
- Risk distribution analysis
- CAPA effectiveness metrics
- Department performance comparison

Note: Analytics is available to System Administrators and Audit Managers only.

12. Access Control

The Access Control module provides fine-grained permission management with enhanced Role-Based Access Control (RBAC) in compliance with ISO 27001.

12.1 Team Assignment

Assign auditors to audit teams with proper roles per ISO 19011 requirements:

1. Enter or select an Audit ID
2. Select a Lead Auditor from available users
3. Add team members and assign their role in the audit
4. Click Assign Team

12.2 User Management

Manage users and assign additional roles from the role matrix:

Search and filter users by name, role, or department
View user details and current role assignments
Assign additional roles with reasons
Set temporary assignments with expiry dates

12.3 Audit Visibility

Control which audits users can see based on their role and department:

Full Access: System Administrators - All audits
Department + Assigned: Audit Managers - Department audits plus assigned
Assigned Only: Auditors - Only audits assigned to them
Department Audits: Department Staff - Audits related to their department

12.4 Role Matrix

Define custom roles with specific permissions:

System: High-level system administration
Audit: Audit-related activities
Business: Business operations
Compliance: Compliance activities

12.5 Available Permissions

Category	Permissions
Audit Management	Create, View All, View Assigned, Edit, Delete, Approve Reports
System Management	Manage Users, Manage Departments, View Analytics, Export Data

Risk and CAPA	Create Risks, Assess Risks, Approve Treatments, Create/Assign/Close CAPA
Document Control	Upload Documents, Approve Documents, Archive Documents
Asset and Vendor	Manage Assets, Assign Assets, Manage Vendors, Evaluate Vendors

13. Asset and Vendor Management

13.1 Asset Management

The Assets module manages organizational assets for audit scope definition in compliance with ISO 27001 Annex A.8.

Asset Categories:

- Hardware - Physical computing equipment
- Software - Applications and systems
- Data - Information assets
- People - Human resources
- Facilities - Physical locations
- Services - External services

Asset Information:

- Asset value and procurement date
- Responsible person and assignment history
- Criticality assessment
- Link to risks and controls
- Disposal date and value (if applicable)

13.2 Vendor Management

The Vendors module manages third-party vendors and suppliers in compliance with ISO 27001 Annex A.15.

Vendor Information:

- Vendor registry with contact details
- Risk rating (Low, Medium, High, Critical)
- Compliance tracking and evidence
- Contract and SLA management
- Performance monitoring
- Evaluation questionnaires

Note: Asset and Vendor Management is available to System Administrators and Audit Managers only.

14. Best Practices

14.1 Audit Best Practices

Always upload evidence - Every finding should have supporting documentation
Use the workflow system - Get proper approvals for all reports
Document everything - The system maintains a full audit trail
Follow ISO 19011 phases - Progress through each phase systematically
Verify team competency - Ensure audit team members are qualified

14.2 Access Control Best Practices

Follow least privilege - Give users only the permissions they need
Use temporary assignments - For short-term access needs, set expiry dates
Document override reasons - Always explain why emergency access was granted
Review roles regularly - Audit role assignments quarterly
Segregate duties - Do not let one person control entire processes

14.3 CAPA Best Practices

Track CAPA items diligently - Do not let corrective actions slip
Perform root cause analysis - Address the underlying cause, not just symptoms
Verify effectiveness - Confirm that actions have resolved the issue
Link to findings - Maintain traceability between findings and actions
Set realistic due dates - Allow adequate time for implementation

14.4 Document Control Best Practices

Maintain version control - Track all document revisions
Set appropriate expiry dates - Review documents before they expire
Use proper confidentiality levels - Protect sensitive information
Follow approval workflows - Ensure documents are properly authorized
Archive obsolete documents - Retain for audit trail but mark as inactive

15. Troubleshooting

15.1 Common Issues

Issue: Cannot log in

Solution: Verify your email address is correct. If 2FA is enabled, ensure you are entering the correct code from your authenticator app.

Issue: Cannot see audits

Solution: Check your role and department assignment. You may only have access to audits assigned to you or your department.

Issue: Workflow not progressing

Solution: Ensure all required approvers have actioned their steps. Check for rejected or returned items.

Issue: Cannot upload documents

Solution: Verify the file size is within limits and the file type is supported.

Issue: Report generation fails

Solution: Ensure the audit has findings documented. The AI report generator requires audit data to create the report.

15.2 Getting Help

Contact your System Administrator for:

- Password resets and account issues
- Role changes and permission requests
- Access issues and visibility problems
- Training requests and user guides
- System configuration questions

16. Glossary

Audit: Systematic, independent, and documented process for obtaining audit evidence and evaluating it objectively

Audit Criteria: Set of policies, procedures, or requirements used as a reference against which audit evidence is compared

Audit Evidence: Records, statements of fact, or other information relevant to the audit criteria and verifiable

Audit Finding: Results of the evaluation of the collected audit evidence against audit criteria

CAPA: Corrective and Preventive Action - actions to eliminate the cause of a detected nonconformity or potential nonconformity

Compliance: Fulfillment of a requirement

Gap Analysis: Comparison of actual performance or compliance against potential or desired performance

ISO 19011: International standard providing guidelines for auditing management systems

ISO 27001: International standard for information security management systems

ISO 9001: International standard for quality management systems

Non-conformity: Non-fulfillment of a requirement

RBAC: Role-Based Access Control - method of regulating access based on roles of individual users

Risk: Effect of uncertainty on objectives

Risk Assessment: Overall process of risk identification, risk analysis, and risk evaluation

Workflow: Sequence of steps through which a piece of work passes from initiation to completion