Cedrus Product Requirements - MVP & Phase 1

Document Version: 1.0
Last Updated: 2024
Product Owner: Cedrus Product Owner Agent
Status: Draft

Executive Summary

This document defines the **Minimum Viable Product (MVP)** scope and **Phase 1 Epics** for the Cedrus platform's External Audit module. The MVP focuses on delivering core audit lifecycle management capabilities that align with ISO/IEC 17021 requirements and mirror workflows found in commercial certification body portals (DNV, TÜV, LRQA, Bureau Veritas).

Target Users

- **Certification Body Administrators (CB Admins)**: Manage client portfolios, create audits, make certification decisions
- **Lead Auditors**: Manage assigned audits, document findings, coordinate teams
- **Auditors**: Document findings, collaborate on audits
- **Client Organization Admins**: Respond to findings, track audit status
- **Client Users**: View audits, respond to nonconformities

MVP Scope Definition

MVP Goal

Enable a Certification Body to conduct a complete external audit lifecycle from creation through certification decision, with client collaboration on nonconformity responses.

MVP In-Scope

Core Entities (Foundation)

- ✅ Organizations (client companies)
- ✅ Sites (physical locations)
- ✅ Standards (ISO 9001, ISO 14001, etc.)
- ✅ Certifications (active certifications per organization/standard)

Audit Management

- ✅ Audit creation (CB Admin only)
- ✅ Audit types: Stage 1, Stage 2, Surveillance, Recertification, Transfer, Special
- ✅ Audit status workflow: Draft → Client Review → Submitted to CB → Decided
- ✅ Audit team assignment (lead auditor, auditors, technical experts, trainees, observers)

- ✅ Multi-site and multi-certification audit support

Findings Management

- ✅ Nonconformities (Major/Minor) with client response workflow
- ✅ Observations (informational)
- ✅ Opportunities for Improvement (OFI)
- ✅ Finding-to-standard clause mapping
- ✅ Client response to nonconformities (root cause, correction, corrective action)

Audit Documentation

- ✅ Audit metadata sections:
  - Organization changes tracking
  - Audit plan review and deviations
  - Audit summary and evaluation
- ✅ Evidence file attachments (audit-level and finding-level)

Certification Decision

- ✅ Audit recommendations (CB Admin editable)
- ✅ Certification decision workflow (approve, suspend, revoke, require special audit)

Access Control

- ✅ Role-based permissions (CB Admin, Lead Auditor, Auditor, Client Admin, Client User)
- ✅ Organization-scoped access for client users
- ✅ Audit-scoped access for auditors

MVP Out-of-Scope

- Internal audits (separate module for Phase 2)
- Risk management module
- Compliance tracking beyond certifications
- Document management system (basic file upload only)
- Email notifications (manual communication)
- Reporting and analytics dashboards
- API for external integrations
- Mobile applications
- Multi-language support
- Accreditation body oversight features
- Audit scheduling and calendar management
- Invoice/billing management
- Client self-registration
- Advanced search and filtering
- Audit templates and checklists

Phase 1: External Audit Module - Epics

Epic 1: Foundation & Core Entities Management

Epic ID: EPIC-001
Priority: Critical (P0)
Status: ✅ Implemented (Partially)

Description

Establish the foundational data model and CRUD operations for organizations, sites, standards, and certifications. These entities form the basis for all audit activities.

User Stories

US-001: Manage Organizations

As a CB Admin
I want to create, view, edit, and list client organizations
So that I can maintain my client portfolio and link audits to organizations

Acceptance Criteria:

- **Given** I am logged in as a CB Admin
- **When** I navigate to `/core/organizations/`
- **Then** I see a list of all organizations
- **And** I can create a new organization with:
  - Name (required)
  - Registered ID (optional)
  - Registered address (required)
  - Customer ID (required, unique)
  - Total employee count (required, > 0)
  - Contact information (telephone, fax, email, website)
  - Signatory name and title
  - MS Representative name and title
- **And** I can edit existing organizations
- **And** I can view organization details

Edge Cases:

- Customer ID must be unique across all organizations
- Employee count must be positive integer
- Email addresses must be valid format
- Website URLs must be valid format

Dependencies: None (Foundation)

US-002: Manage Sites

As a CB Admin
I want to create and manage sites for organizations
So that I can track multiple locations per organization and assign sites to audits

Acceptance Criteria:

- **Given** I am logged in as a CB Admin
- **When** I navigate to `/core/sites/`
- **Then** I see a list of all sites
- **And** I can create a new site with:
  - Organization (required, dropdown of existing organizations)
  - Site name (required)
  - Site address (required)
  - Site employee count (optional, > 0 if provided)
  - Site scope override (optional)
  - Active status (default: true)
- **And** I can edit existing sites
- **And** I can filter sites by organization
- **And** I can deactivate sites (set active = false)

Edge Cases:

- Site must belong to an organization
- Employee count must be positive if provided
- Deactivated sites should still be visible in historical audits

Dependencies: US-001 (Organizations must exist)

US-003: Manage Standards Library

As a CB Admin
I want to maintain a library of management system standards
So that I can create certifications based on these standards

Acceptance Criteria:

- **Given** I am logged in as a CB Admin
- **When** I navigate to `/core/standards/`
- **Then** I see a list of all standards
- **And** I can create a new standard with:
  - Code (required, unique, e.g., "ISO 9001:2015")
  - Title (required, e.g., "Quality management systems — Requirements")
  - NACE code (optional)
  - EA code (optional)
- **And** I can edit existing standards
- **And** Standards are sorted alphabetically by code

Edge Cases:

- Standard code must be unique
- Standard code should follow ISO naming conventions (e.g., "ISO 9001:2015")

Dependencies: None (Reference data)

US-004: Manage Certifications

As a CB Admin
I want to create and manage certifications for organizations
So that I can track which organizations hold which certifications and link them to audits

Acceptance Criteria:

- **Given** I am logged in as a CB Admin
- **When** I navigate to `/core/certifications/`
- **Then** I see a list of all certifications
- **And** I can create a new certification with:
  - Organization (required, dropdown)
  - Standard (required, dropdown)
  - Certification scope (required)
  - Certificate ID (optional)
  - Certificate status (draft, active, suspended, withdrawn, expired)
  - Issue date (optional)
  - Expiry date (optional)
- **And** I can edit existing certifications
- **And** I can filter certifications by organization
- **And** I can update certification status
- **And** The system enforces unique organization+standard combination

Edge Cases:

- Organization+Standard combination must be unique
- If expiry date is provided, it should be after issue date
- Status transitions should be logical (e.g., cannot go from "withdrawn" to "active" without proper workflow)
- Expired certifications should be automatically marked as expired if expiry_date < today

Dependencies: US-001 (Organizations), US-003 (Standards)

Blockers:

- Date validation (issue_date < expiry_date) - NOT IMPLEMENTED
- Automatic expiry status update - NOT IMPLEMENTED

Epic 2: Audit Creation & Lifecycle Management

Epic ID: EPIC-002
Priority: Critical (P0)
Status: 🟡 Partially Implemented

Description

Enable CB Admins to create audits and manage them through the complete lifecycle from draft to certification decision. Support multiple audit types and status transitions.

User Stories

US-005: Create Audit

As a CB Admin
I want to create a new audit
So that I can initiate the audit process for a client organization

Acceptance Criteria:

- **Given** I am logged in as a CB Admin
- **When** I navigate to `/audits/create/`
- **Then** I see an audit creation form
- **And** I can create an audit with:
  - Organization (required, dropdown)
  - Certifications (required, multi-select, filtered to selected organization)
  - Sites (required, multi-select, filtered to selected organization)
  - Audit type (required: Stage 1, Stage 2, Surveillance, Recertification, Transfer, Special)
  - Total audit date from (required, date picker)
  - Total audit date to (required, date picker)
  - Audit duration hours (required, >= 0)
  - Lead auditor (required, dropdown filtered to lead_auditor group)
  - Status (default: "draft")
- **And** Upon submission, the audit is created and I am redirected to the audit detail page
- **And** The audit is assigned to the selected lead auditor

Edge Cases:

- End date must be >= start date
- Certifications must belong to the selected organization
- Sites must belong to the selected organization
- Lead auditor must be in the "lead_auditor" group
- Duration hours must be >= 0
- At least one certification must be selected
- At least one site must be selected

Dependencies: US-001 (Organizations), US-002 (Sites), US-004 (Certifications), User roles (lead_auditor group)

Blockers:

- Date validation (end_date >= start_date) - NOT IMPLEMENTED
- Certification organization validation - NOT IMPLEMENTED
- Site organization validation - NOT IMPLEMENTED
- Lead auditor role validation - NOT IMPLEMENTED

US-006: View Audit List (Role-Based Filtering)

As a user (CB Admin, Lead Auditor, Auditor, Client Admin, Client User)
I want to view a list of audits relevant to my role
So that I can see audits I need to work on

Acceptance Criteria:

- **Given** I am logged in
- **When** I navigate to `/audits/`
- **Then** I see audits filtered by my role:
  - **CB Admin**: All audits
  - **Lead Auditor**: Audits where I am the lead auditor or team member
  - **Auditor**: Audits where I am a team member
  - **Client Admin/User**: Audits for my organization
- **And** Each audit shows:
  - Organization name
  - Audit type
  - Status
  - Date range
  - Lead auditor name
- **And** I can click on an audit to view details

Edge Cases:

- Users with multiple roles see union of all relevant audits
- Client users see only audits for their organization (from profile.organization)
- Auditors see audits where they are assigned as team members

Dependencies: US-005 (Audits must exist), User roles, Profile.organization

---

US-007: View Audit Details

As a user
I want to view complete audit details
So that I can see all information about an audit

Acceptance Criteria:

- **Given** I have permission to view an audit

- **When** I navigate to `/audits/<id>/`
- **Then** I see:
  - Audit header (organization, type, status, dates, duration, lead auditor)
  - Certifications covered
  - Sites covered
  - Team members
  - Audit metadata sections (if created):
    - Organization changes
    - Audit plan review
    - Audit summary
  - Findings (Nonconformities, Observations, OFIs)
  - Evidence files
  - Recommendations (if status >= "submitted_to_cb")
- **And** I see action buttons based on my role and permissions:
  - Edit (CB Admin or Lead Auditor if status = "draft")
  - Add Finding (CB Admin or team member if status = "draft")
  - Submit to Client (Lead Auditor if status = "draft")
  - Respond to NCs (Client Admin/User if status = "client_review")
  - Make Decision (CB Admin if status = "submitted_to_cb")
  - Print (all authorized users)

Edge Cases:

- Users without permission see 403 Forbidden
- Edit button only visible if user has edit permission and status allows editing
- Recommendations only visible to CB Admins until status = "submitted_to_cb"

Dependencies: US-005, US-006, US-008 (Edit), US-010 (Findings), US-012 (Recommendations)

US-008: Edit Audit (Lead Auditor)

As a Lead Auditor
I want to edit audit details for audits I am assigned to
So that I can update audit information during the draft phase

Acceptance Criteria:

- **Given** I am a Lead Auditor assigned to an audit
- **And** The audit status is "draft"
- **When** I navigate to `/audits/<id>/edit/`
- **Then** I can edit:
  - Certifications (multi-select)
  - Sites (multi-select)
  - Audit type
  - Date range
  - Duration hours
  - Lead auditor (dropdown)

- **And** I cannot edit:
  - Organization (locked)
  - Created by (locked)
  - Status (changed via workflow actions)
- **And** Upon saving, changes are persisted
- **And** I am redirected to the audit detail page

Edge Cases:

- If audit status is not "draft", editing is blocked (403 or redirect)
- If I am not the lead auditor, editing is blocked (403)
- CB Admin can always edit regardless of status (separate permission)

Dependencies: US-005, US-007

Blockers:

- Status-based edit restrictions - NOT IMPLEMENTED
- Lead auditor permission check - PARTIALLY IMPLEMENTED

US-009: Audit Status Workflow Transitions

As a Lead Auditor or CB Admin
I want to transition audits through status workflow
So that I can move audits through the approval process

Acceptance Criteria:

- **Given** I am a Lead Auditor with an audit in "draft" status
- **When** I complete the audit documentation
- **And** I click "Submit to Client"
- **Then** The audit status changes to "client_review"
- **And** Client users can now view and respond to nonconformities
- **Given** I am a CB Admin with an audit in "submitted_to_cb" status
- **When** I review the audit and recommendations
- **And** I make a certification decision
- **Then** The audit status changes to "decided"
- **And** The audit is locked from further editing (except by CB Admin override)

Status Transition Rules:

- `draft` → `client_review`: Lead Auditor only, requires minimum documentation

- `client_review` → `submitted_to_cb`: Automatic after client responds to all major NCs (or manual trigger by CB Admin)
- `submitted_to_cb` → `decided`: CB Admin only, requires recommendations to be completed
- `decided`: Final state, no further transitions

Edge Cases:

- Cannot skip status transitions (e.g., draft → decided)
- Cannot go backwards (e.g., client_review → draft) without CB Admin override
- Status transitions should be logged/audited
- Major nonconformities must have client responses before moving to "submitted_to_cb"

Dependencies: US-005, US-008, US-010 (Findings), US-012 (Recommendations)

Blockers:

- Status transition validation - NOT IMPLEMENTED
- Workflow enforcement - NOT IMPLEMENTED
- Transition logging - NOT IMPLEMENTED

Epic 3: Audit Team Management

Epic ID: EPIC-003
Priority: High (P1)
Status: 🟡 Partially Implemented

Description

Enable assignment and management of audit team members, including internal auditors (users) and external experts (name/title only).

User Stories

US-010: Assign Team Members to Audit

As a Lead Auditor or CB Admin
I want to assign team members to an audit
So that I can build the audit team and track who is involved

Acceptance Criteria:

- **Given** I am a Lead Auditor or CB Admin
- **And** I am viewing/editing an audit
- **When** I add a team member
- **Then** I can specify:
  - User (optional, dropdown of users if internal auditor)
  - Name (required if user is null, otherwise auto-filled)
  - Title (optional)

    - Role (required: Lead Auditor, Auditor, Technical Expert, Trainee, Observer)
    - Date from (required, within audit date range)
    - Date to (required, within audit date range, >= date from)
- **And** The team member is added to the audit
- **And** If user is specified, they can now see the audit in their list
- **And** If user is null, it's an external expert (name/title only)

Edge Cases:

- Team member dates must be within audit date range
- Date to >= date from
- If user is provided, name should auto-fill from user profile
- If user is null, name is required
- Lead auditor role should match the audit's lead_auditor field (or allow multiple lead auditors for large audits)
- External experts (user=null) cannot log in but are tracked for documentation

Dependencies: US-005 (Audits), User management

Blockers:

- Date range validation (team member dates within audit dates) - NOT IMPLEMENTED
- Auto-fill name from user - NOT IMPLEMENTED

US-011: View Audit Team

As a user
I want to view the audit team for an audit
So that I can see who is involved in the audit

Acceptance Criteria:

- **Given** I have permission to view an audit
- **When** I view the audit details
- **Then** I see a "Team Members" section listing:
    - Name
    - Title
    - Role
    - Date range
    - Internal/External indicator
- **And** Team members are sorted by role, then name

Edge Cases:

- External experts show "External" indicator
- Internal auditors show their user account link (if permission allows)

Dependencies: US-010, US-007

Epic 4: Findings Management

Epic ID: EPIC-004
Priority: Critical (P0)
Status: 🔴 Not Implemented (BLOCKING)

Description

Enable auditors to document findings (nonconformities, observations, opportunities for improvement) and enable clients to respond to nonconformities with corrective actions.

User Stories

US-012: Create Nonconformity

As an Auditor or Lead Auditor
I want to document a nonconformity finding
So that I can record issues found during the audit

Acceptance Criteria:

- **Given** I am an Auditor or Lead Auditor assigned to an audit
- **And** The audit status is "draft" or "client_review"
- **When** I add a nonconformity
- **Then** I can specify:
  - Standard (required, dropdown of standards covered by audit)
  - Clause (required, e.g., "4.1", "7.5.1")
  - Category (required: Major or Minor)
  - Objective evidence (required, text)
  - Statement of NC (required, text)
  - Auditor explanation (required, text)
  - Due date (optional, for corrective action)
- **And** The nonconformity is created with status "open"
- **And** It appears in the audit's findings list
- **And** If audit status is "client_review", client users can see and respond to it

Edge Cases:

- Standard must be one of the certifications' standards for this audit
- Clause should follow standard clause numbering (e.g., "4.1", "7.5.1", "8.2.1")
- Major NCs typically have shorter due dates than minor NCs
- Due date should be in the future
- Cannot create NCs if audit status is "decided"

Dependencies: US-005 (Audits), US-003 (Standards), US-010 (Team assignment)

Blockers:

- Finding creation UI - NOT IMPLEMENTED

- Finding models exist but views/forms missing

US-013: Create Observation

As an Auditor or Lead Auditor
I want to document an observation finding
So that I can record informational findings that don't require corrective action

Acceptance Criteria:

- **Given** I am an Auditor or Lead Auditor assigned to an audit
- **And** The audit status is "draft" or "client_review"
- **When** I add an observation
- **Then** I can specify:
  - Standard (required, dropdown)
  - Clause (required)
  - Statement (required, text)
  - Explanation (optional, text)
- **And** The observation is created
- **And** It appears in the audit's findings list
- **And** No client response is required (observations are informational only)

Edge Cases:

- Standard must be one of the audit's certifications' standards
- Observations are read-only for clients (no response workflow)

Dependencies: US-005, US-003, US-010

Blockers:

- Finding creation UI - NOT IMPLEMENTED

US-014: Create Opportunity for Improvement

As an Auditor or Lead Auditor
I want to document an opportunity for improvement
So that I can suggest enhancements to the client's management system

Acceptance Criteria:

- **Given** I am an Auditor or Lead Auditor assigned to an audit
- **And** The audit status is "draft" or "client_review"
- **When** I add an OFI
- **Then** I can specify:
  - Standard (required, dropdown)
  - Clause (required)
  - Description (required, text)

- **And** The OFI is created
- **And** It appears in the audit's findings list
- **And** No client response is required (OFIs are optional suggestions)

Edge Cases:

- Standard must be one of the audit's certifications' standards
- OFIs are read-only for clients (no response workflow)

Dependencies: US-005, US-003, US-010

Blockers:

- Finding creation UI - NOT IMPLEMENTED

US-015: Respond to Nonconformity (Client)

As a Client Admin or Client User
I want to respond to nonconformities with root cause analysis and corrective actions
So that I can address audit findings and move the audit forward

Acceptance Criteria:

- **Given** I am a Client Admin or Client User
- **And** I am viewing an audit for my organization
- **And** The audit status is "client_review"
- **And** There are nonconformities with status "open" or "client_responded"
- **When** I respond to a nonconformity
- **Then** I can edit:
  - Root cause analysis (required, text)
  - Correction (required, text - immediate action taken)
  - Corrective action (required, text - plan to prevent recurrence)
  - Due date (optional, can update)
- **And** Upon saving, the NC status changes to "client_responded"
- **And** The auditor can review my response

Edge Cases:

- Cannot respond if audit status is not "client_review"
- Cannot respond if NC status is "closed"
- All three fields (root cause, correction, corrective action) must be provided
- Response should be substantial (minimum character count? - business rule)
- Can update response if status is "client_responded" (before auditor verification)

Dependencies: US-012 (Nonconformities), US-006 (Audit list), US-007 (Audit details)

Blockers:

- Client response UI - NOT IMPLEMENTED

- Status update on response - NOT IMPLEMENTED

US-016: Verify Nonconformity Response (Auditor)

As a Lead Auditor or Auditor
I want to verify client responses to nonconformities
So that I can accept or request changes to corrective actions

Acceptance Criteria:

- **Given** I am a Lead Auditor or Auditor assigned to the audit
- **And** There are nonconformities with status "client_responded"
- **When** I review a client response
- **Then** I can:
  - Accept the response (status → "accepted")
  - Request changes (status → "client_responded", notify client)
  - Close the NC (status → "closed", only if accepted)
- **And** When I accept/close, I can add verification notes
- **And** My verification is recorded (verified_by, verified_at)

Edge Cases:

- Cannot close NC without accepting first
- Cannot accept if response is incomplete (business rule)
- Verification should be logged for audit trail
- Major NCs typically require more thorough verification than minor NCs

Dependencies: US-015 (Client response), US-012

Blockers:

- Verification UI - NOT IMPLEMENTED
- Status workflow - NOT IMPLEMENTED

US-017: View Findings List

As a user
I want to view all findings for an audit
So that I can see a comprehensive list of all issues and observations

Acceptance Criteria:

- **Given** I have permission to view an audit
- **When** I view the audit details
- **Then** I see findings organized by type:
  - Nonconformities (grouped by Major/Minor, sorted by clause)
  - Observations (sorted by clause)
  - Opportunities for Improvement (sorted by clause)

- **And** Each finding shows:
  - Clause reference
  - Standard
  - Summary/statement
  - Status (for NCs: open, client_responded, accepted, closed)
  - Created by and date
- **And** I can click on a finding to view details
- **And** For NCs, I can see response status and due dates

Edge Cases:

- Findings should be sorted logically (by clause, then by creation date)
- Major NCs should be visually distinct from minor NCs
- Closed NCs might be shown in a collapsed section

Dependencies: US-012, US-013, US-014, US-007

Blockers:

- Findings display in audit detail view - NOT IMPLEMENTED

Epic 5: Audit Documentation & Metadata

Epic ID: EPIC-005
Priority: High (P1)
Status: 🟡 Partially Implemented (Models exist, UI missing)

Description

Enable completion of audit documentation sections required for ISO/IEC 17021 compliance: organization changes, audit plan review, and audit summary.

User Stories

US-018: Track Organization Changes

As a Lead Auditor
I want to document changes to the organization during the audit
So that I can track modifications that affect the certification

Acceptance Criteria:

- **Given** I am a Lead Auditor assigned to an audit
- **And** I am editing the audit
- **When** I complete the "Organization Changes" section
- **Then** I can indicate changes in:
  - Name
  - Scope

    - Sites
    - Management System Representative
    - Signatory
    - Employee count
    - Contact information
    - Other (with description field)
- **And** Each change is a boolean checkbox
- **And** If "Other" is checked, description is required
- **And** Changes are saved and displayed in audit details

Edge Cases:

- Changes section is optional (can be left blank if no changes)
- "Other" description is required if "other_has_change" is true
- Changes should be compared to organization data at audit creation time (future enhancement)

Dependencies: US-005, US-008

Blockers:

- Organization Changes UI - NOT IMPLEMENTED (model exists)

US-019: Review Audit Plan and Deviations

As a Lead Auditor
I want to document audit plan review and any deviations
So that I can record if the audit was conducted as planned

Acceptance Criteria:

- **Given** I am a Lead Auditor assigned to an audit
- **And** I am editing the audit
- **When** I complete the "Audit Plan Review" section
- **Then** I can specify:
    - Were there deviations from the audit plan? (Yes/No)
    - If yes, details of deviations (required if yes)
    - Were there issues affecting the audit? (Yes/No)
    - If yes, details of issues (required if yes)
    - Proposed next audit date from (optional)
    - Proposed next audit date to (optional)
- **And** Details fields are required if corresponding yes/no is true
- **And** Next audit dates are optional but if provided, end >= start

Edge Cases:

- Deviations section is optional
- If "deviations_yes_no" is true, "deviations_details" is required
- If "issues_affecting_yes_no" is true, "issues_affecting_details" is required

- Next audit dates should be in the future

Dependencies: US-005, US-008

Blockers:

- Audit Plan Review UI - NOT IMPLEMENTED (model exists)

US-020: Complete Audit Summary

As a Lead Auditor
I want to complete the audit summary evaluation
So that I can document the overall assessment of the management system

Acceptance Criteria:

- **Given** I am a Lead Auditor assigned to an audit
- **And** I am editing the audit
- **When** I complete the "Audit Summary" section
- **Then** I can answer evaluation questions (Yes/No with comments):
  - Were audit objectives met?
  - Was the scope appropriate?
  - Does the management system meet requirements?
  - Was management review effective?
  - Was internal audit effective?
  - Is the management system effective?
  - Was there correct use of certification logos?
  - Should this be promoted to certification committee?
- **And** Each question has an optional comments field
- **And** There is a general commentary field (A.4)
- **And** All fields are optional but recommended for completeness

Edge Cases:

- Summary section is optional but should be completed before submission
- Comments can be lengthy (text fields)
- General commentary is free-form text

Dependencies: US-005, US-008

Blockers:

- Audit Summary UI - NOT IMPLEMENTED (model exists)

Epic 6: Evidence File Management

Epic ID: EPIC-006
Priority: Medium (P2)

Status: 🟡 Partially Implemented

Description

Enable upload and management of evidence files attached to audits and findings.

User Stories

US-021: Upload Evidence Files

As a user (Auditor, Client Admin, Client User)
I want to upload evidence files to audits or findings
So that I can attach supporting documentation

Acceptance Criteria:

- **Given** I have permission to upload files (based on my role and audit status)
- **When** I am viewing an audit or nonconformity
- **Then** I can upload a file with:
  - File (required, various formats: PDF, DOC, DOCX, XLS, XLSX, images)
  - Optional link to a specific nonconformity (if uploading at audit level)
- **And** The file is stored securely
- **And** The file metadata is recorded (uploaded_by, uploaded_at)
- **And** The file appears in the evidence list
- **And** File size is limited (e.g., 10MB max)

Edge Cases:

- File size validation (reject if > 10MB)
- File type validation (allow common document and image formats)
- Virus scanning (future enhancement)
- Storage quota per organization (future enhancement)
- Files linked to NCs should be clearly associated

Dependencies: US-005, US-012 (for NC-linked files)

Blockers:

- File upload UI - NOT IMPLEMENTED
- File storage configuration - NOT IMPLEMENTED

US-022: View and Download Evidence Files

As a user
I want to view and download evidence files
So that I can access supporting documentation

Acceptance Criteria:

- **Given** I have permission to view an audit
- **When** I view the audit details
- **Then** I see a list of evidence files showing:
  - File name
  - Uploaded by
  - Upload date
  - Linked finding (if applicable)
- **And** I can click to download/view the file
- **And** Files are organized by:
  - Audit-level files
  - Finding-specific files (grouped by finding)

Edge Cases:

- Download permission should match audit view permission
- Large files should stream/download efficiently
- File preview for images/PDFs (future enhancement)

Dependencies: US-021

Blockers:

- File download/view UI - NOT IMPLEMENTED

Epic 7: Certification Decision & Recommendations

Epic ID: EPIC-007
Priority: Critical (P0)
Status: 🟡 Partially Implemented (Model exists, UI/Workflow missing)

Description

Enable CB Admins to review audit recommendations and make certification decisions (approve, suspend, revoke, require special audit).

User Stories

US-023: Create/Edit Audit Recommendations

As a Lead Auditor
I want to create audit recommendations
So that I can provide guidance to the CB Admin for the certification decision

Acceptance Criteria:

- **Given** I am a Lead Auditor assigned to an audit
- **And** The audit is ready for CB review
- **When** I complete the recommendations section

- **Then** I can specify:
  - Special audit required? (Yes/No)
  - If yes, special audit details (required if yes)
  - Suspension recommended? (Yes/No)
  - If yes, certificates to suspend (text list)
  - Revocation recommended? (Yes/No)
  - If yes, certificates to revoke (text list)
  - Stage 2 required? (Yes/No, for Stage 1 audits)
  - Decision notes (optional, free-form text)
- **And** Recommendations are saved
- **And** CB Admin can view and edit recommendations

Edge Cases:

- Recommendations are optional but should be completed before submission
- If special audit/suspension/revocation is recommended, details are required
- Recommendations can be edited by CB Admin before decision

Dependencies: US-005, US-009 (Status workflow)

Blockers:

- Recommendations UI - NOT IMPLEMENTED (model exists)

US-024: Make Certification Decision

As a CB Admin
I want to make the final certification decision based on audit recommendations
So that I can approve, suspend, or revoke certifications

Acceptance Criteria:

- **Given** I am a CB Admin
- **And** I am viewing an audit with status "submitted_to_cb"
- **And** Recommendations have been completed
- **When** I make a certification decision
- **Then** I can:
  - Review all audit information
  - Review recommendations
  - Edit recommendations if needed
  - Make decision:
    - Approve certification (issue/renew certificate)
    - Suspend certification(s)
    - Revoke certification(s)
    - Require special audit
    - Require Stage 2 (if Stage 1)
- **And** Upon decision, the audit status changes to "decided"

- **And** Certification statuses are updated accordingly:
  - If approved: certification status → "active", issue_date set, expiry_date set
  - If suspended: certification status → "suspended"
  - If revoked: certification status → "withdrawn"
- **And** The audit is locked from further editing (except CB Admin override)

Edge Cases:

- Cannot make decision if audit status is not "submitted_to_cb"
- Cannot make decision if recommendations are incomplete
- Decision should be logged/audited
- Multiple certifications can be affected by one decision
- Decision notes should be comprehensive for audit trail

Dependencies: US-023 (Recommendations), US-009 (Status workflow), US-004 (Certifications)

Blockers:

- Decision UI - NOT IMPLEMENTED
- Certification status update automation - NOT IMPLEMENTED
- Decision logging - NOT IMPLEMENTED

Epic 8: Print & Reporting

Epic ID: EPIC-008
Priority: Medium (P2)
Status: ✅ Partially Implemented

Description

Enable generation of print-friendly audit reports for official documentation and client delivery.

User Stories

US-025: Print Audit Report

As a user
I want to generate a print-friendly audit report
So that I can create official documentation

Acceptance Criteria:

- **Given** I have permission to view an audit
- **When** I navigate to `/audits/<id>/print/`
- **Then** I see a print-optimized layout with:
  - Audit header (organization, type, dates, team)
  - Certifications and sites covered
  - Organization changes (if any)

    - Audit plan review (if completed)
    - Audit summary (if completed)
    - All findings (organized by type)
    - Recommendations (if status >= "submitted_to_cb")
    - Evidence file list
- **And** The layout is optimized for A4 printing
- **And** Page breaks are logical
- **And** Headers/footers include audit ID and date

Edge Cases:

- Long findings should not break awkwardly across pages
- Tables should fit on pages
- Print CSS should hide navigation/buttons
- Should work in all major browsers

Dependencies: US-007 (Audit details), US-017 (Findings), US-023 (Recommendations)

Status: ✅ Basic print view exists, may need enhancement

Dependencies & Blockers Summary

Critical Blockers (Must Fix for MVP)

1. **Findings Management (EPIC-004) - NOT IMPLEMENTED**
    - No UI for creating findings (NCs, Observations, OFIs)
    - No UI for client responses
    - No UI for auditor verification
    - **Impact:** Cannot complete audit workflow
2. **Status Workflow Validation (US-009) - NOT IMPLEMENTED**
    - No validation of status transitions
    - No enforcement of workflow rules
    - **Impact:** Audits can skip required steps
3. **Data Validation (Multiple US) - NOT IMPLEMENTED**
    - Date validation (end >= start)
    - Organization-scoped validation (certifications, sites)
    - Lead auditor role validation
    - **Impact:** Data integrity issues
4. **Audit Documentation UI (EPIC-005) - NOT IMPLEMENTED**
    - Models exist but no UI for:
        - Organization changes
        - Audit plan review

        - Audit summary
    - **Impact:** Cannot complete audit documentation

5. **Recommendations & Decision (EPIC-007) - NOT IMPLEMENTED**
    - No UI for recommendations
    - No decision workflow
    - No certification status updates
    - **Impact:** Cannot complete certification decision

High Priority (Should Fix for MVP)

6. **Evidence File Management (EPIC-006) - NOT IMPLEMENTED**
    - No file upload UI
    - No file storage configuration
    - **Impact:** Cannot attach evidence

7. **Team Member Date Validation (US-010) - NOT IMPLEMENTED**
    - Team member dates not validated against audit dates
    - **Impact:** Data integrity

Medium Priority (Nice to Have for MVP)

8. **Print Report Enhancements (US-025) - PARTIALLY IMPLEMENTED**
    - Basic print view exists but may need styling improvements

---

Edge Cases & Business Rules

Audit Creation

- Organization must exist and be active
- Certifications must belong to selected organization
- Sites must belong to selected organization
- Lead auditor must be in "lead_auditor" group
- At least one certification and one site required
- End date >= start date
- Duration hours >= 0

Status Workflow

- Cannot skip status transitions
- Cannot go backwards without CB Admin override
- Major NCs must have client responses before "submitted_to_cb"
- Recommendations must be completed before "decided"
- "Decided" status locks audit (except CB Admin override)

Findings

- Standard must be one of audit's certifications' standards
- Clause should follow standard numbering (e.g., "4.1", "7.5.1")
- Major NCs typically have shorter due dates
- Cannot create findings if audit is "decided"
- Client can only respond if audit status is "client_review"

Certifications

- Organization+Standard combination must be unique
- Expiry date > issue date (if both provided)
- Status transitions should be logical
- Expired certifications should auto-update status

Permissions

- CB Admin: Full access to all audits
- Lead Auditor: Edit own audits, view assigned audits
- Auditor: View assigned audits, add findings
- Client Admin/User: View own organization's audits, respond to NCs

---

Acceptance Criteria Template

All user stories follow this structure:

```
**Given** [initial context/state]
**When** [action taken]
**Then** [expected outcome]
**And** [additional outcomes/validations]
```

ISO/IEC 17021 Alignment

Key Requirements Addressed

1. **Audit Planning** (Clause 9.2)
    - Audit creation with type, dates, scope
    - Team assignment
    - Site and certification coverage
2. **Audit Conduct** (Clause 9.3)
    - Findings documentation (NCs, Observations, OFIs)
    - Evidence collection
    - Audit plan review and deviations
3. **Audit Reporting** (Clause 9.4)

- Audit summary and evaluation
- Findings reporting
- Recommendations

4. **Certification Decision** (Clause 9.5)
    - Recommendation review
    - Decision making (approve, suspend, revoke)
    - Certification status management
5. **Nonconformity Management** (Clause 9.6)
    - Client response workflow
    - Verification of corrective actions
    - Closure of nonconformities

Next Steps

1. **Prioritize Blockers**: Address EPIC-004 (Findings) first as it's blocking the core workflow
2. **Implement Status Workflow**: Add validation and enforcement for status transitions
3. **Complete Documentation UI**: Build forms for audit metadata sections
4. **Build Decision Workflow**: Implement recommendations and certification decision
5. **Add Data Validation**: Implement all validation rules identified
6. **Testing**: Comprehensive testing of all user stories and edge cases

---

Document End