OSCRAT

Open-Source Cyber Resilience Act Tools

D3.6.

OSCRAT – Testing Report M15

Submission date: 02/03/2026

Author: Liliana Hornea – Oves Enterprise

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Project acronym	**OSCRAT**
Project title	Open-Source Cyber Resilience Act Tools
Deliverable Name	D3.6. – Testing Report M15
Number	101190180
Work package	Work Package 3 – Software design and development
Due Date	28/02/2026
Submission Date	02/03/2026
Lead Partner	OVES Enterprise
Author name(s)	Liliana Hornea
Version	1.0
Status	Draft
Type:	Document, report
Dissemination level:	Public

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Document History			
Version	**Date**	**Modified by**	**Comments**
0	23/02/2026	Liliana Hornea	First draft
0.1	24/02/2026	Nadja Dokter	Review and formatting
0.1	28/02/2026	Predrag Tasevski,Dariusz Rogowski	Internal Review
1.0	28/02/2026	Liliana Hornea	Final

Abstract

During this reporting period, the OSCRAT platform underwent significant functional and architectural enhancements, evolving into a more comprehensive product security operations platform. Major developments included the introduction of a Documentation Management pillar, a fully internalized audit logging system, enhanced compliance workflows with automated remediation tracking and Declaration of Conformity generation, and strengthened encryption for sensitive data. In parallel, a framework upgrade to Next.js 16 and frontend refactoring improved performance, maintainability, and scalability, positioning the platform for continued growth.

Keywords

Product Management, Compliance Assessment, Functional Testing, Vulnerability Management, Incident Tracking, Dashboard, SBOM, Data Integrity, Regression Testing

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

DISCLAIMER

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Contents

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

1. Executive Summary

1.1 Summary

This reporting period saw the OSCRAT platform evolve significantly across several fronts. The most substantial new capability is a full Documentation Management pillar, giving teams a structured way to create, edit, and share product documentation directly within the platform. In parallel, the platform's audit and compliance infrastructure was fundamentally rearchitected, moving from an external dependency to a purpose-built internal system, and a Declaration of Conformity workflow was introduced. Underneath these user-facing features, the team invested in security hardening, a major framework upgrade to Next.js 16, and broad component refactoring to improve maintainability.

1.2 Documentation Management System

The largest body of work in this period was the introduction of a dedicated Documentation pillar, establishing documentation as a first-class concept alongside existing pillars like compliance, vulnerabilities, and tasks. Teams can now create, read, update, and delete documentation entries associated with their products. Each document supports both public and private visibility, and public documents can be shared via a generated URL, useful for distributing compliance narratives or product manuals to external stakeholders without granting platform access.

The platform's markdown editing experience was overhauled with MDXEditor, a fully featured rich-text component supporting toolbars, undo functionality, and in-container scrolling. The editor is loaded dynamically to avoid impacting initial page load performance. Pre-built documentation templates give authors a starting point rather than a blank page. Documentation entries can be linked to tasks, creating traceability between planned work and supporting written artifacts.

1.3 Audit Logging & Compliance Tracking

The external Retraced audit logging service was replaced with a fully internal system. Every significant platform operation now generates an audit log entry capturing the acting user, their IP address, user agent, the operation performed, and a structured description of the change. Audit log creation is wrapped within the same database transactions as the operations they record, ensuring the log always reflects actual state changes. The audit log UI supports filtering by date range, user, and operation type, along with text search across log descriptions.

1.4 Compliance & Assessment Enhancements

When a compliance assessment identifies gaps or non-conformities, the platform can now automatically generate tasks to track remediation, bridging the gap between findings and actionable work items. A new Declaration of Conformity (DoC) workflow allows teams to generate a formal declaration document with PDF export, suitable for regulatory submission or customer distribution.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

An import mechanism was introduced for both team-level and version-level compliance assessments, removing the need for manual re-entry when data originates externally. All compliance-related forms received comprehensive input validation, and organization management forms were enhanced with translation support. The product survey question management was improved with the ability to delete and replace questions.

1.5 Security & Encryption Infrastructure

A general-purpose two-way encryption facility was introduced for sensitive data at rest, going beyond one-way hashing to support use cases where the platform must both store and later retrieve sensitive values such as API tokens or integration credentials. Personal Access Tokens are now stored in encrypted form rather than as plaintext, significantly reducing exposure risk in the event of a database compromise. The env.ts configuration layer was reworked to ensure that encryption keys and other sensitive environment values are handled consistently and validated at startup.

1.6 Platform Modernization & Reliability

The frontend framework was upgraded from Next.js 14 to Next.js 16, bringing performance improvements, updated React support, and access to the latest framework capabilities. A NextAuth compatibility workaround was implemented to maintain authentication functionality during the transition. A dedicated refactoring pass extracted shared hooks and reorganized component structures across the frontend, reducing duplication and improving consistency.

A new generic “team data” API and schema provides a flexible mechanism for storing structured data associated with a team without requiring schema migrations for each new data category. The platform now sends open incident and vulnerability counts directly from the database and supports creating vulnerabilities from CVE and package data. Several bugs in the task management system were identified and resolved.

1.7 Technical Approach

The work in this period reflects several deliberate architectural choices. Replacing Retraced with an internal audit system eliminated a runtime dependency and gave the team full control over the audit data schema. The consistent use of database transactions wrapping both business logic and audit logging ensures the audit trail is always consistent with actual state. The MDXEditor integration uses dynamic imports to keep the bundle size in check, and the Declaration of Conformity feature establishes a server-side PDF generation pattern reusable for other exportable documents.

1.8 Conclusion

Over the past three months, the OSCRAT platform has expanded from a compliance assessment and vulnerability management tool into a more complete product

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

security operations platform. Teams can now assess compliance, track remediation tasks, generate formal declarations, document their processes, and maintain a full audit trail, all within a single platform. The underlying infrastructure improvements in encryption, framework modernization, and component refactoring position the codebase well for continued feature development in the coming months.

2. Introduction

This QA Test Report documents the verification and validation of core compliance and governance features implemented in the OSCRAT platform:

- **Declaration of Conformity** (Conformity Assessment Report + Declaration Wizard + PDF lifecycle)
- **Tasks Management** (task lifecycle, assignment, filtering, details, documentation linkage)
- **Audit Logs** (product-level and organization-level immutable traceability for CRA readiness)
- **Documentation Module** (CRA Annex VII technical documentation creation, publishing, visibility, and task backlinking)

These modules collectively strengthen CRA compliance readiness by enforcing controlled workflows, ensuring traceability and accountability, and supporting structured technical documentation and operational governance.

3. Objectives

- Validate regulatory gating logic (Assessment → Declaration → Ready for Market)
- Verify correct behavior of questionnaire, uploads, wizard navigation, and PDF lifecycle actions
- Validate tasks lifecycle, filtering, and detail editing (including assignee selection)
- Confirm audit logging coverage, immutability, record correctness (When/Who/What), and filtering
- Validate documentation creation flows (org/product), templates, editing, publishing/visibility, URL generation
- Verify documentation ↔ tasks linking and backlink rules (bidirectional, private-only backlinks in public view)
- Ensure data consistency and persistence across modules

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

4. Testing Methodologies Used

4.1 Manual Functional Testing

Step-by-step validation of UI workflows, business rules, and state transitions in modern desktop browsers.

4.2 Exploratory Testing

Focused on edge cases: conditional rendering, wizard navigation, linking/backlinking behavior, and state recovery.

4.3 Black Box Testing

Validated system behaviour strictly via inputs/outputs without internal implementation knowledge.

4.4 Regression Testing

Ensured new functionality did not negatively impact: version detail views, product indicators, tasks, documentation linkage, audit logs, and existing upload/download flows.

5. Declaration of Conformity

5.1 Introduction

This QA Test Report documents the verification and validation of the Declaration of Conformity functionality within the OSCRAT platform, available under a Version Detailed Page of a product.

The Declaration of Conformity feature is composed of two tightly coupled functional parts:

1. **Conformity Assessment Report**

   1.1 Mandatory prerequisite

   1.2 Can be completed via:

   - Self-Assessment Questionnaire, or
   - Upload of a third-party assessment report

2. **Create Declaration of Conformity**

- A controlled, step-based wizard
- Allows generation, signing, and finalization of the declaration

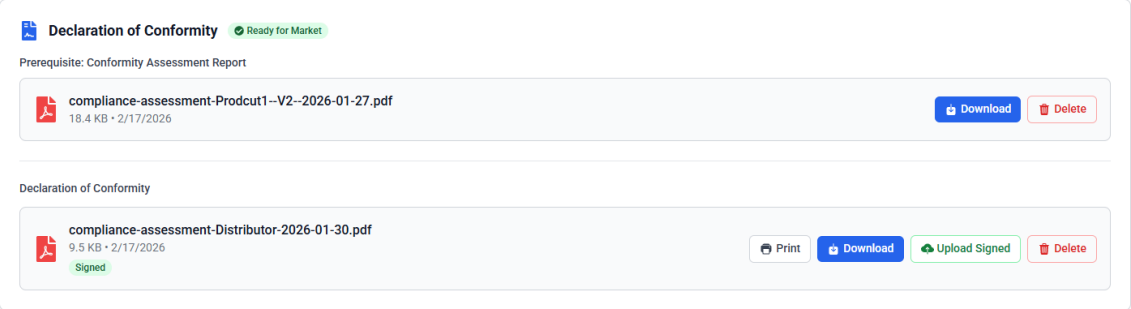
Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

- Leads to a “Ready for Market” status

  Both parts together form a single business flow, enforcing regulatory compliance before a product version can be considered market-ready.

  Figure 1: Declaration of conformity section



5.2 Functional Overview

Entry Context

- Feature is accessed under **Declaration of Conformity** within a **Version Detailed Page**
- Initially, no declaration can be created without a valid assessment report

Conformity Assessment Report

A. Entry State

When accessing the section:

- Informational message is displayed:
  "A Conformity Assessment Report is required before creating a Declaration of Conformity.
  You can either upload a third-party assessment report (PDF/XLS) or complete the self-assessment questionnaire."
- The following UI elements are visible:
  - **Complete Self-Assessment Questionnaire** (hyperlink)
  - **Upload** button
- **Create Declaration of Conformity button is not visible**

B. Self-Assessment Questionnaire Flow

1. User clicks **Complete Self-Assessment Questionnaire**
2. Language selection screen opens
   - English is selected by default

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

- Only English is available for the current release

3. Questionnaire contains two sections:
   - Product Compliance
   - Procedures Compliance
4. All questions must be answered
5. Both sections must reach **Fully Compliant** status
6. Upon successful completion:
   - A Conformity Assessment Report is generated
   - The report appears in the UI
   - **Download** and **Delete** buttons are available
   - **Create Declaration of Conformity** button becomes visible

C. Third-Party Assessment Upload Flow

- User uploads a valid PDF or XLS file
- On successful upload:
  - The file is displayed in the UI
  - **Download** and **Delete** buttons are available
  - **Create Declaration of Conformity** button becomes visible

D. Report Actions

For both generated and uploaded reports:

- **Download**: Downloads the report file
- **Delete**:
  - Removes the report
  - Hides the Create Declaration button
  - Resets the section to its initial state

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

5.3 Create Declaration of Conformity

1. Entry Conditions

- A valid Conformity Assessment Report exists
- **Create Declaration of Conformity** button is visible and enabled
  Clicking the button opens a **four-step wizard**.

2. Step 1 – Review Conformity Assessment Guide

- Informational text is displayed:
  "Before proceeding, please review the Conformity Assessment Guide to understand how to select the appropriate conformity assessment type."
- **Open Conformity Assessment Guide** button is displayed
- Clicking the button opens the guide in a **new browser tab**
- User proceeds via **Next**

3. Step 2 – Select Conformity Assessment Type

- Three single-select radio options:
  - Self-Assessment
  - External Assessment Module B+C
  - External Assessment Module H
- Only one option can be selected
- Navigation:
  - **Next** → Step 3
  - **Back** → Step 1

4. Step 3 – Select Declaration Type

- Two single-select radio options:
  - Simple Declaration of Conformity
  - Full Declaration of Conformity
- Selected option determines the template shown in Step 4
- Navigation via **Next** and **Back**

5. Step 4 – Declaration Template

1. **Common Behavior**
   - Prefilled & non-editable:
     - Organisation Name
     - Product Name

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

- Product Version
- **Generate PDF** button is available

2. **Simple Declaration Template**
   - User generates a PDF only
   - PDF must be:
     - Downloaded
     - Signed externally
     - Re-uploaded using **Upload signed**

3. **Full Declaration Template**
   - Additional prefilled & non-editable fields:
     - Full Postal Address
     - Signed for and on behalf of
   - All other declaration fields are editable
   - User completes the form and clicks **Generate PDF**

6. **Post-Generation Behavior**

After generating the PDF:

- The generated file replaces the Create Declaration button
- Available actions:
  - **Print** (browser print)
  - **Download**
  - **Upload signed**
  - **Delete**

After Uploading Signed Declaration

- A green **Signed** indicator appears under the file
- A green **Ready for Market** indicator appears next to the section title

Delete Behavior

- Removes the declaration
- Resets the entire process
- Create Declaration button becomes visible again

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

5.4 Conformity Assessment Report – Test Cases

Test Case ID	Test Case Description	Input	Expected Result
TC-1	Test that informational message is displayed on entry	Navigate to Declaration of Conformity section	Informational message displayed correctly
TC-2	Test that Self-Assessment hyperlink is visible	Load section	Hyperlink visible and clickable
TC-3	Test that Upload button is visible	Load section	Upload button visible
TC-4	Test Create Declaration button is not visible initially	Load section	Button not displayed
TC-5	Test language selection opens	Click questionnaire link	Language selection screen opens
TC-6	Test English default selection	Open language screen	English preselected
TC-7	Test only English available	Open dropdown	Only English selectable
TC-8	Test Product Compliance section displayed	Open questionnaire	Section visible
TC-9	Test Procedures Compliance section displayed	Open questionnaire	Section visible
TC-10	Test unanswered questions block completion	Leave question blank	Completion blocked
TC-11	Test partial compliance blocks report	One section not Fully Compliant	Report not generated
TC-12	Test both sections must be Fully Compliant	One compliant, one not	Report not generated
TC-13	Test report generation success	All Fully Compliant	Report generated
TC-14	Test generated report appears in UI	Complete questionnaire	Report displayed

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

TC-15	Test Download button visible	Report generated	Download button visible
TC-16	Test Delete button visible	Report generated	Delete button visible
TC-17	Test report download works	Click Download	File downloaded
TC-18	Test deleting report removes it	Click Delete	Report removed
TC-19	Test deleting report resets gating	Delete report	Create button hidden
TC-20	Test uploading valid PDF	Upload PDF	Upload successful
TC-21	Test uploading valid XLS	Upload XLS	Upload successful
TC-22	Test invalid file rejected	Upload JPG	Error displayed
TC-23	Test uploaded report shows actions	Upload valid file	Download/Delete visible
TC-24	Test downloading uploaded report	Click Download	File downloaded
TC-25	Test deleting uploaded report	Click Delete	File removed
TC-26	Test Create button appears after questionnaire	Fully Compliant	Button visible
TC-27	Test Create button appears after upload	Upload valid file	Button visible

5.5 Create Declaration Wizard – Test Cases

Test Case ID	Test Case Description	Input	Expected Result
TC-28	Test wizard opens	Click Create Declaration	Wizard opens Step 1
TC-29	Test Step 1 text correct	Open Step 1	Text matches requirement

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

TC-30	Test guide button visible	Step 1	Button visible
TC-31	Test guide opens new tab	Click guide	New tab opens
TC-32	Test Next Step 1→2	Click Next	Step 2 displayed
TC-33	Test Back Step 2→1	Click Back	Step 1 displayed
TC-34	Test Step 2 options visible	Open Step 2	3 options visible
TC-35	Test Step 2 single-select	Select options	Only one selected
TC-36	Test Next Step 2→3	Click Next	Step 3 displayed
TC-37	Test Back Step 3→2	Click Back	Step 2 displayed
TC-38	Test Step 3 options visible	Open Step 3	2 options visible
TC-39	Test Step 3 single-select	Select options	Only one selected
TC-40	Test Next Step 3→4	Click Next	Step 4 displayed
TC-41	Test Simple template shown	Select Simple	Simple template visible
TC-42	Test Full template shown	Select Full	Full template visible
TC-43	Test prefilled fields non-editable	Step 4	Fields read-only

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

TC-44	Test Full extra fields read-only	Full template	Fields read-only
TC-45	Test editable fields accept input	Full template	Input saved
TC-46	Test Generate PDF available	Step 4	Button visible
TC-47	Test Generate PDF works (Simple)	Click Generate	PDF generated
TC-48	Test Generate PDF works (Full)	Fill + Generate	PDF contains data
TC-49	Test generated file replaces button	Generate	File displayed
TC-50	Test file action buttons visible	After generate	Print/Download/Upload/Delete visible
TC-51	Test Print works	Click Print	Print dialog opens
TC-52	Test Download works	Click Download	File downloaded
TC-53	Test Upload signed works	Upload signed PDF	Upload success
TC-54	Test Signed indicator visible	After upload	Green Signed indicator

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

TC-55	Test Ready for Market visible	After upload	Green indicator displayed
TC-56	Test Delete resets process	Click Delete	Wizard reset
TC-57	Test Back/Next preserves selection	Navigate	Selections remain
TC-58	Test steps cannot be skipped	Attempt skip	Sequential enforcement

6. Tasks

6.1 Introduction

This QA Test Report documents the verification and validation of the **Tasks** functionality within the OSCRAT platform.

The Tasks feature allows users to:

- View all tasks created for the current Organization
- Filter tasks by Status, Product, and Version
- Create new tasks via the **Add Task** pop-up
- Update task status directly from the table
- Access detailed task information via the **Task Details Page**
- Edit task attributes (Name, Due Date, Status, Description, Assignee)
- View linked documentation under the **Documentation** tab

The feature ensures centralized task tracking across Products and Versions within an Organization.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Figure 2: Tasks page

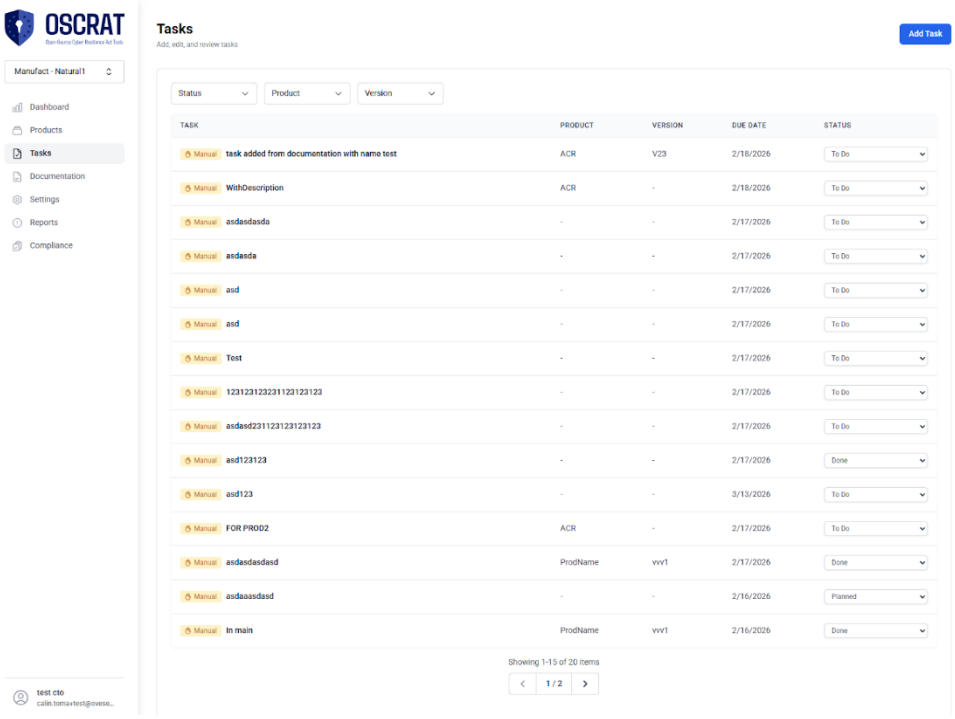
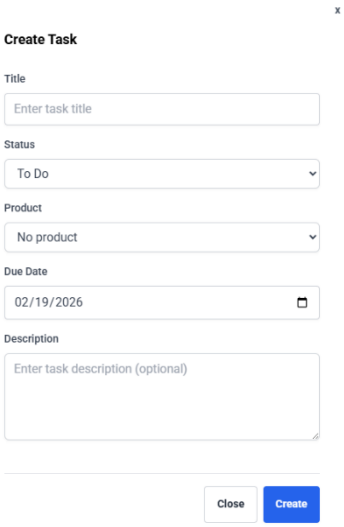


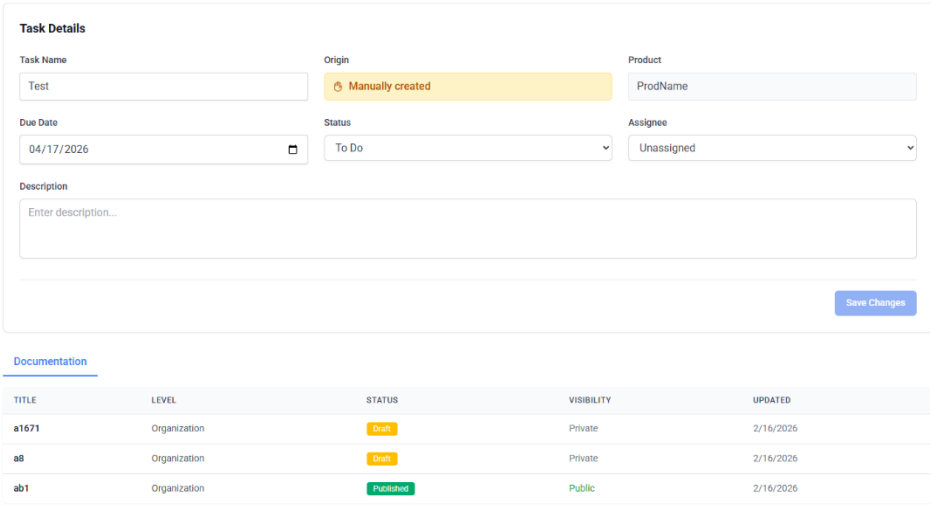
Figure 3: Add Tasks pop-up



Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Figure 4: Task detailed page



6.2 Functional Overview

Entry Context

- The user accesses Tasks by clicking **Tasks** under **Products** in the left sidebar.

Tasks Page Contains:

- Filters dropdown list:
  - Status
  - Product
  - Version
- **Add Task** button
- Tasks table with headers:
  - Task (Name)
  - Product
  - Version
  - Due Date
  - Status (editable dropdown)

Clicking a task redirects to the **Task Details Page**.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Tasks Page – Functional Behavior

Filters

- Status filter filters tasks by selected status
- Product filter filters tasks by selected product
- Version filter filters tasks by selected version
- Filters work independently and in combination

Tasks Table

Displays all tasks created under the current Organization.

Each row includes:

- Task Name (clickable link)
- Product
- Version
- Due Date
- Status (dropdown editable)

Status dropdown values:

- To-do
- Planned
- Done
- In progress

Users can change status directly from the table.

Add Task Pop-up

Fields:

Field	Type	Rules
Title	Text (mandatory)	Only letters, numbers, basic punctuation allowed
Status	Dropdown	Default: To-do
Product	Dropdown	Optional
Version	Dropdown	Visible only if Product selected
Due Date	Date picker	Cannot select past date; default = current date
Description	Text	Optional

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Task Details Page

Editable fields:

- Name
- Due Date
- Status
- Description
- Assignee (all users in Organization)

Contains:

Documentation tab (shows linked documentation if exists)

6.3 Test Cases

Navigation & Page Load

Test Case ID	Description	Input	Expected Result
TC-1	Verify navigation to Tasks page	Click Tasks in sidebar	Tasks page opens
TC-2	Verify all organization tasks are displayed	Load page	Table shows all tasks for current Organization
TC-3	Verify table headers are correct	Load page	Headers displayed correctly

Filters

Test Case ID	Description	Input	Expected Result
TC-4	Verify Status filter works	Select Status filter value	Table updates accordingly
TC-5	Verify Product filter works	Select Product	Only tasks for selected Product shown
TC-6	Verify Version filter works	Select Version	Only tasks for selected Version shown
TC-7	Verify combined filters work	Select Status + Product	Table reflects combined filter

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

TC-8	Verify clearing filters resets results	Clear filters	All tasks displayed

Table Status Editing

Test Case ID	Description	Input	Expected Result
TC-9	Verify status dropdown contains correct values	Click Status dropdown	To-do, Planned, Done, In progress visible
TC-10	Verify changing status updates task	Change status	Status updated successfully
TC-11	Verify status change persists after refresh	Change status → refresh	Updated status remains

Add Task Pop-up

Test Case ID	Description	Input	Expected Result
TC-12	Verify Add Task button opens pop-up	Click Add Task	Pop-up appears
TC-13	Verify Title is mandatory	Leave Title empty	Create button disabled or validation shown
TC-14	Verify Title accepts valid characters	Enter valid text	Input accepted
TC-15	Verify Title rejects invalid characters	Enter disallowed characters	Input rejected or validation shown
TC-16	Verify default Status is To-do	Open pop-up	Status defaults to To-do
TC-17	Verify Product dropdown lists Organization products	Open Product dropdown	Correct product list shown
TC-18	Verify Version appears only after Product selection	Select Product	Version dropdown becomes visible
TC-19	Verify Version list contains versions of selected Product	Select Product → open Version	Only related versions displayed

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

TC-20	Verify Version default is “No version selected”	Select Product	Version default state correct
TC-21	Verify Due Date defaults to current date	Open pop-up	Current date preselected
TC-22	Verify past date cannot be selected	Try selecting past date	Selection blocked
TC-23	Verify Description is optional	Leave empty	Task can be created
TC-24	Verify successful task creation	Fill mandatory fields → Create	Task added to table
TC-25	Verify created task appears with correct values	Create task	Data displayed correctly in table

Task Details Page

Test Case ID	Description	Input	Expected Result
TC-26	Verify clicking task redirects to details page	Click task name	Task Details page opens
TC-27	Verify Name field editable	Edit Name	Changes saved
TC-28	Verify Due Date editable with no past selection	Edit date	Future/current date accepted
TC-29	Verify Status editable	Change Status	Status updated
TC-30	Verify Description editable	Edit Description	Changes saved
TC-31	Verify Assignee dropdown contains Organization users	Open Assignee dropdown	All users listed
TC-32	Verify assigning a user works	Select Assignee	Assignment saved
TC-33	Verify Documentation tab is visible	Open Task Details	Documentation tab present
TC-34	Verify Documentation tab displays linked documents	Open Documentation tab	Linked docs displayed if available
TC-35	Verify changes persist after refresh	Edit fields → refresh	Changes retained

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

7. Audit Logs

7.1 Introduction

This QA Test Report documents the verification and validation of the **Audit Logs** functionality within the OSCRAT platform.

The Audit Logs feature ensures **traceability, accountability, and audit-readiness**, particularly for **CRA compliance purposes**.

The OSCRAT platform inherits audit logging capabilities from the Unicis platform and extends them to cover all relevant user actions across:

- Product Version level modules
- Organization-level management and workflows

Each audit log entry must include:

- **When** – Timestamp of the action
- **Who** – User identity
- **What** – Description of the action and affected data

Action details must include:

- **Creation** → new value
- **Modification** → previous value(s) + new value(s)
- **Deletion** → old value

Logs must be:

- Immutable
- Non-editable
- Filterable
- Retained according to compliance/legal rules

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Figure 5: Audit logs Organisation level

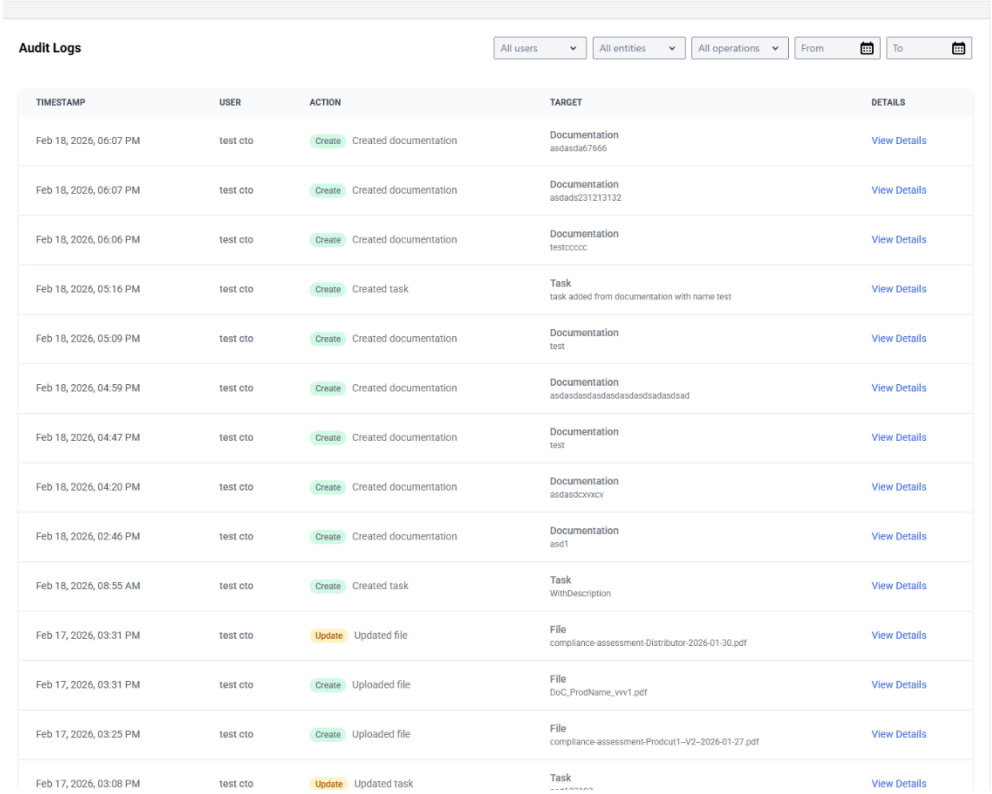
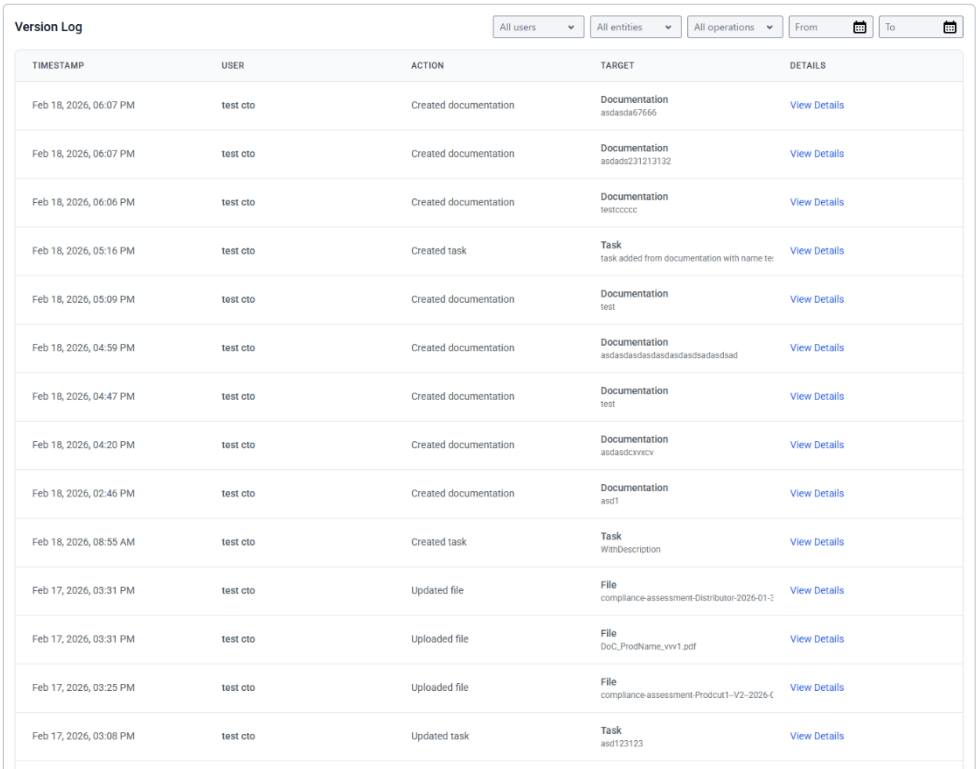


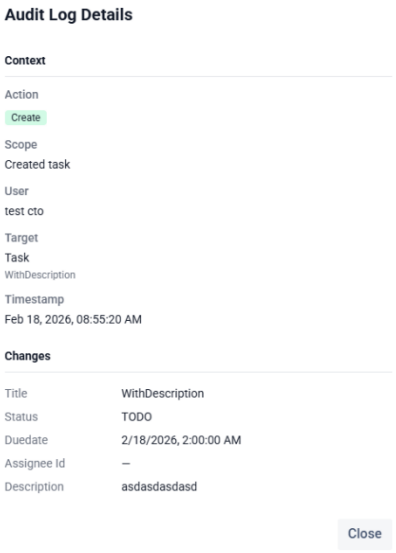
Figure 6: Version logs



Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Figure 7: Logs details page



7.2 Functional Overview

Product Level Audit Logs

Scope

Applies to all modules within **Product Version View**, including:

- Files
- SBOM
- Scans
- Vulnerabilities
- Incidents
- Repository

UI Placement

- New tab in Product Version View
- Name: **Audit Logs**
- Positioned at the far right
- Replaces current Version Log tab

Logged Actions – Product Level

Files

- Add file
- Delete file

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

SBOM

- Import SBOM
- Generate SBOM
- Delete SBOM
- Scan SBOM

Vulnerabilities

- Add vulnerability
- Edit vulnerability
- Delete vulnerability

Incidents

- Add incident
- Edit incident
- Delete incident

Repository

- Add repository
- Edit repository
- Delete repository

7.3 Organization Level Audit Logs

UI Placement

Left Menu → Settings → **Audit Logs**

Logged Actions – Organization Level

Team & Members

- Create team
- Edit team settings
- Add member
- Manage member
- Member login
- Member logout

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Integrations

- Create webhook
- Create API key

Conformity

- Start conformity assessment
- Complete conformity assessment

7.4 Products

- Add product
- Edit product
- Add product version
- Edit product version

7.5 Tasks

- Task creation
- Task status change
- Task detail changes:
  - Name
  - Due date
  - Status
  - Assignee
  - Description
  - Task Type

7.6 Audit Log Record Structure

Each record must contain:

- Timestamp
- User
- Action description
- Affected object identifier
- Old value (if applicable)

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

- New value (if applicable)

Logs must be:

- Read-only
- Non-deletable
- Non-editable

7.7 Test Cases

UI Placement & Accessibility

Test Case ID	Description	Input	Expected Result
TC-1	Verify Product Level Audit Logs tab exists	Open Product Version View	Audit Logs tab visible (far right)
TC-2	Verify Organization Level Audit Logs page exists	Go to Settings → Audit Logs	Page loads successfully
TC-3	Verify logs are read-only	Attempt to edit log entry	Editing not possible
TC-4	Verify logs cannot be deleted	Attempt to delete entry	No delete option available

Log Structure Validation

Test Case ID	Description	Input	Expected Result
TC-5	Verify Creation log format	Add product	Log contains timestamp, user, new value
TC-6	Verify Modification log format	Edit product name	Log shows previous and new values
TC-7	Verify Deletion log format	Delete file	Log shows deleted value
TC-8	Verify Timestamp accuracy	Perform action	Timestamp reflects action time

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

TC-9	Verify User identity logging	Perform action as different user	Correct user displayed in log

Product Level Logging

Test Case ID	Description	Input	Expected Result
TC-10	Verify file upload logged	Add file	Log entry created
TC-11	Verify file deletion logged	Delete file	Log entry created
TC-12	Verify SBOM import logged	Import SBOM	Log entry created
TC-13	Verify SBOM generation logged	Generate SBOM	Log entry created
TC-14	Verify SBOM deletion logged	Delete SBOM	Log entry created
TC-15	Verify SBOM scan logged	Scan SBOM	Log entry created
TC-16	Verify vulnerability add logged	Add vulnerability	Log entry created
TC-17	Verify vulnerability edit logged	Edit vulnerability	Log shows old + new values
TC-18	Verify vulnerability delete logged	Delete vulnerability	Log entry created
TC-19	Verify incident add logged	Add incident	Log entry created
TC-20	Verify incident edit logged	Edit incident	Log shows value changes
TC-21	Verify incident delete logged	Delete incident	Log entry created
TC-22	Verify repository add logged	Add repository	Log entry created
TC-23	Verify repository edit logged	Edit repository	Log shows changes
TC-24	Verify repository delete logged	Delete repository	Log entry created

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Organization Level Logging

Test Case ID	Description	Input	Expected Result
TC-25	Verify team creation logged	Create team	Log entry created
TC-26	Verify team edit logged	Edit team	Log shows old + new values
TC-27	Verify member addition logged	Add member	Log entry created
TC-28	Verify member management logged	Modify member	Log entry created
TC-29	Verify member login logged	Login	Log entry created
TC-30	Verify member logout logged	Logout	Log entry created
TC-33	Verify conformity start logged	Start conformity assessment	Log entry created
TC-34	Verify conformity completion logged	Complete conformity assessment	Log entry created
TC-35	Verify product creation logged	Add product	Log entry created
TC-36	Verify product edit logged	Edit product	Log shows value changes
TC-37	Verify product version add logged	Add version	Log entry created
TC-38	Verify product version edit logged	Edit version	Log entry created
TC-39	Verify task creation logged	Add task	Log entry created
TC-40	Verify task status change logged	Change task status	Log shows old + new status
TC-41	Verify task detail changes logged	Edit name/due date/assignee	Log shows previous + new values
TC-42	Verify task type change logged	Change task type	Log entry created

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Filtering Functionality

Test Case ID	Description	Input	Expected Result
TC-43	Verify filter by user works	Select user filter	Only that user's logs displayed
TC-44	Verify filter by date range works	Select date range	Only logs within range displayed
TC-45	Verify filter by action type works	Select action type	Only selected action type shown
TC-46	Verify combined filters work	Apply user + date + action	Correct subset displayed
TC-47	Verify clearing filters resets results	Clear filters	All logs displayed

Expected Outcome

The Audit Logs feature ensures:

- Full traceability of user actions
- Regulatory and CRA compliance readiness
- Transparent accountability
- Immutable audit history
- Consistent logging across modules

7.8 Status

- Audit logging coverage validated
- Immutability and integrity verified
- Filtering functionality confirmed
- Compliance traceability ensured
- Feature ready for release and regulatory audit use

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

8. Conclusion

The QA testing activities performed for the OSCRAT Platform – Compliance & Governance Modules confirm that all implemented functionalities meet the defined business requirements, regulatory constraints, and user workflow expectations as documented in the test specification

Across the following modules:

- Declaration of Conformity (Assessment + Wizard + PDF lifecycle)
- Tasks Management
- Audit Logs (Product & Organization level)
- Documentation Module (CRA Annex VII compliance support)

All defined test cases were executed successfully.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

8.1 Test Execution Summary

8.2 Quality Assessment

The platform demonstrates:

- Correct regulatory gating logic enforcement
- Stable multi-step wizard behavior
- Accurate task lifecycle management
- Immutable and structured audit logging
- Controlled documentation publishing and backlink traceability
- Consistent persistence and filtering behavior across modules

No critical, major defects were identified during final validation. All compliance-related traceability requirements for CRA readiness have been verified.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

8.3 Release Readiness

The tested modules are:

- Functionally complete
- Stable under normal and edge-case scenarios
- Compliant with defined regulatory workflow constraints
- Ready for production release and regulatory audit usage

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

OSCRAT

Open-Source Cyber Resilience Act Tools

OSCRAT – Testing report M 15

www.oscrat.eu https://www.linkedin.com/

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.