Co-funded by the European Union

OSCRAT

Open-Source Cyber Resilience Act Tools

D3.7

OSCRAT - Testing Report M18

Submission date: 24.06.2026

Author: Oves Enterprise

Project acronym	OSCRAT
Project title	Open-Source Cyber Resilience Act Tools
Name	Testing report M18
Number	01190180
Work package	WP3 – Software design and development
Due Date	31/05/2025
Submission Date	24/06/2026
Lead Partner	OVES Enterprise
Author name(s)	OVES Enterprise
Version	1.0
Status	Final version
Type:	☒ R – Document, Report ☐ DEC – Websites, patent filings, videos, etc. ☐ DEM – Demonstrator, pilot, prototype
Dissemination level:	☒ PU - Public ☐ SEN - Sensitive

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.

Document History			
Version	**Date**	**Modified by**	**Comments**
0.1	01/06/26	Liliana Hornea	First Draft
0.2	4/06/2026	Nadja Dokter	Internal Review
0.3	23/06/2026	Predrag Tasevski,	Internal Review
1.0	23/06/2026	Liliana Hornea	Final

Abstract

This reporting period covers the final set of tasks for the OSCRAT platform, bringing it to feature-complete stage. The work added four new pillars: Configuration Management, Risk Assessment, a Technical Documentation Checklist, and Security Awareness and Training and expanded audit logging across the platform. With these in place, OSCRAT covers the full set of Cyber Resilience Act activities the project set out to support: assessing compliance, treating risk, training users, documenting products, managing configuration, and keeping a complete record of user actions. The remaining work in this period reorganized the data model around the organization concept, replaced the email subsystem, and resolved a range of defects.

Keywords

test scenario, functionality, methodologies

DISCLAIMER

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.

Table of contents

1. Introduction 7
Objectives 9
2. Testing Methodologies Used 12
Manual Functional Testing 12
Exploratory Testing 12
Black Box Testing 12
Regression Testing 12
3. Configuration Management 13
3.1 Functionality Overview 13
3.1.1 Configuration Management Tab 13
3.1.2 Configuration Scan Report 13
3.1.3 Create Task from Failed Rule 14
3.1.4 Re-upload and Task Lifecycle 15
3.2 Test Scenarios 15
1. Configuration Management Tab — Navigation & Layout 15
2. Import File Drawer 16
3. Jobs Table — Row Data & Actions 17
4. Configuration Scan Report Page 18
5. Create Task from Failed Rule 20
6. Re-upload & Task Lifecycle 21
4. Risk Assessment Task 23
4.1 Functionality Overview 23
4.1.1 Risk Assessment Task 23
4.2 Test Scenarios 25
1. Risk Checkbox & Task Type Field 26
2. Section 1: Risk Details — Field Presence & Validation 26
3. Exposure Auto-Calculation — Full Risk Matrix 28
4. Section 2 Blocked Until Section 1 Complete 29
5. Section 2: Risk Treatment — Field Presence & Validation 30
6. Task Status Transitions & Completion 31
7. Task Visibility in Task List 32
5. Security Awareness and Training Evidence 33
5.1 Functionality Overview 33
5.1.1 Security Awareness and Training Evidence 33
5.2 Test Scenarios 34

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. Automatic Task Creation on First Login 34
2. Task Field Values and Content 35
3. User Interaction with the Task 35
4. Task Visibility and Access 36
5. Regression — Login & Create Account 37
6. Technical Documentation Checklist 38
6.1 Functionality Overview 38
6.1.1 Technical Documentation Checklist 38
6.2 Test Scenarios 39
1. Technical Documentation Checklist 39
7. Conclusion 44
7.1 Configuration Management 44
7.2 Risk Assessment Task 44
7.3 Security Awareness and Training Evidence 45
7.4 Technical Documentation Checklist 45
7.5 Test Scenario Execution Summary 46
Configuration Management 46
Risk Assessment Task 46
Security Awareness and Training Evidence 47
Technical Documentation Checklist 47
Overall Grand Total 47
8. Test Scenarios Summary Chart 49
9. Conclusion 49

Figures

Figure 1: Config Management tab
Figure 2: Configuration Scan Report
Figure 3: Create Task from failed rule
Figure 4: Risk Assessment Task enable check box
Figure 5: Section 1: Risk Details
Figure 6: Section 2: Risk Treatment
Figure 7: Security Awareness task
Figure 8: Technical Documentation Checklist in Areas of Requirements
Figure 9: Technical Documentation Checklist items
Figure 10: Test Scenarios Executed vs Passed per Feature

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
QA Test Report

OSCRAT Platform — Combined Features

Configuration Management · Risk Assessment Task · Security Awareness & Training · Technical Documentation Checklist

OpenSCAP Scan Orchestration, Evidence Processing & Governance

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. Introduction

Configuration Management

Configuration Management lets teams track the security configuration of their products using scan evidence. The platform is not a scanner itself; it processes the results of OpenSCAP scans run outside the platform. Users upload scan artifacts in the supported formats, and the platform turns them into a read-only compliance report showing rule results, severities, an overall score, and per-rule detail. For every failed or unresolved result, a remediation task is created automatically, linked to the product and carrying the relevant control reference and severity. After remediation the user re-scans and uploads fresh results, the report updates, and the related tasks can be closed once compliance is demonstrated. Past results are kept so teams can see how configuration changes over time.

Risk Assessment

Teams can now perform structured risk assessments for their assets, processes, and information systems. A new Risk task type opens an assessment form divided into two stages. In the first stage the user records the asset, the threat, the affected security categories, and the likelihood and impact of the risk; the platform then calculates the resulting exposure from a defined risk matrix. The second stage, which cannot be started until the first is complete, captures the treatment decision: accept, reduce, avoid, or transfer along with mitigation measures, residual exposure, and the responsible party. Exposure scoring lets teams prioritize remediation, with high risks flagged for urgent action and lower risks scheduled or monitored. Each assessment is linked to a product and moves through a status lifecycle from to-do to done.

Technical Documentation Checklist

The compliance assessment gained a Technical Documentation Checklist covering the documentation elements required by the Cyber Resilience Act. Unlike the rest of the questionnaire, which is built around questions, this section is a checklist: each entry pairs a documentation requirement with its regulatory reference and a compliant or non-compliant status, shown as a checkmark. It applies to the manufacturer, importer, and distributor roles, where it counts toward the overall compliance status; for authorized representatives it is optional and excluded from the result, so the user can choose whether to complete it. The checklist is included in the assessment form, the assessment overview, and the exported report, with translation support for the new section.

Security Awareness and Training

The platform now manages recurring security awareness training for every user. When a person signs in for the first time, an awareness training task is created for them automatically, with a due date and links to the training material. Users record their progress by updating the task status as they work through it. When a training

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 is completed, a new one is created for the next period, so training stays current without manual administration. A background job handles this generation and renewal, so it runs reliably regardless of how a user was added.

Audit Logging Expansion

Building on the internal audit system delivered in the previous period, audit logging was broadened and refined to cover the full range of user actions needed for regulatory traceability. Coverage now spans three levels: product-level activity such as files, software bill of materials operations, vulnerabilities, incidents, repositories, and configuration scans; task-level activity such as creation, status changes, and detail changes; and organization-level activity such as membership management, logins, and product changes. Report and file downloads are now recorded as well. Each entry captures who performed the action, when it happened, and what changed. User identities are resolved so entries stay accurate even after accounts change, and the audit log can be filtered by user, date range, and action type.

Platform Improvements, Fixes, and Feedback

Alongside the new features, the data model and references were reorganized around the organization concept, bringing routing and terminology into line across the application. The email subsystem was reworked into a dedicated mail service, simplifying member invitation and management and reducing configuration overhead, and the magic-link login was retired in favor of the standard sign-in flow. Scan artifacts are now compressed before storage to speed up database operations on large files.

A substantial amount of feedback and bug-fixing work was carried out after the beta release, acting on review feedback from across the team and from product demos. This included fixes to the compliance assessment, the assessment report export, and the documentation and Declaration of Conformity flows, along with corrections to the distinction between advisories and vulnerabilities, ensuring artifacts appear consistently under product files, and resolving a stale authentication redirect. Feedback gathered ahead of the demos was also addressed, tidying the dashboard and navigation.

Technical Approach

All four new pillars are built on a single task model. Rather than building separate tracking for risk, training, configuration, and documentation, each one creates and manages tasks of a declared type, so they share the same lifecycle, audit trail, and interface. Heavier or recurring work like configuration scan processing, training generation, and artifact handling will run as background jobs to keep the application responsive. Audit logging is written within the same database transactions as the operations it records, so the trail always matches actual state. Scan artifacts are compressed before storage to speed up database operations on large files.

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.

This QA Test Report documents the verification and validation of the following functionalities implemented in the OSCRAT platform:

- Configuration Management — A scan orchestration, evidence processing, and governance module that allows users to import OpenSCAP configuration scan results (ARF, XCCDF, OVAL, XML), review structured compliance reports, and create remediation tasks directly from failed rules.
- Risk Assessment Task — A structured workflow that enables OSCRAT users to identify, evaluate, and treat risks associated with a product. It is activated by checking a Risk Assessment checkbox on the task form, which reveals two additional sections: Risk Details (Section 1) and Risk Treatment (Section 2). Section 2 cannot be completed until all mandatory Section 1 fields are filled. Risk Exposure is automatically calculated from the selected Likelihood and Impact values using a predefined matrix.
- Security Awareness and Training Evidence — A mechanism that automatically generates an 'Awareness training' task for every new OSCRAT user upon their first login, ensuring all registered users are directed to and can confirm completion of mandatory awareness training materials hosted externally.
- Technical Documentation Checklist — A checklist-based assessment tool that enables users to verify whether all mandatory technical documentation requirements defined in CRA Annex VII and Annex II are fulfilled for a given product version.

Objectives

Configuration Management:

- Validate the end-to-end import flow for all supported file formats (ARF, XCCDF, OVAL)
- Confirm that scan jobs are created, processed asynchronously, and transition to Completed status
- Verify the Jobs table displays all required columns and that row interaction (click, download, delete) works correctly
- Ensure the Configuration Scan Report page renders Overview, Benchmark, and Rules sections with accurate data
- Validate Create Task dialog pre-fill logic, field constraints, and task creation outcome
- Confirm that only one task can be linked per rule per scan job
- Verify that re-uploading an updated scan creates a new independent job and updates compliance data
- Ensure pagination, Refresh, and breadcrumb navigation function correctly

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.

Risk Assessment Task:

- Validate that the Risk Assessment checkbox correctly shows and hides the extra risk fields
- Confirm that the Task Type dropdown contains all required options and operates independently of the Risk checkbox
- Verify all Section 1 fields (Asset, Threat, Category, Likelihood, Impact, Exposure, Owner) render correctly with the correct input types
- Validate the full Exposure auto-calculation matrix covering all 9 Likelihood × Impact combinations
- Confirm that Section 2 is inaccessible until all mandatory Section 1 fields are populated, and re-locks if a Section 1 field is cleared
- Verify all Section 2 fields (Treatment, Measures, Residual Exposure, Responsible) including mandatory vs optional rules
- Ensure all four Treatment options (ACCEPT, REDUCE, AVOID, TRANSFER) can be selected and saved
- Validate the full task status progression: To Do → Planned → In Progress → Done
- Confirm that completed task data persists correctly on re-open and that risk tasks appear and can be filtered in the organisation task list

Security Awareness and Training Evidence:

- Validate that an 'Awareness training' task is automatically created immediately after a new user's first login
- Ensure the auto-generated task carries the correct predefined field values: Name, Assignee, Status, Due Date, and Description
- Confirm that the Description contains working external links to the training materials
- Verify that the task is visible in the organisation task list and accessible to appropriate members
- Validate that users can manually update the task status to reflect training progress and confirm completion
- Ensure that no duplicate tasks are generated on subsequent logins by the same user
- Confirm that multiple new users each receive their own individually assigned task
- Verify that existing authentication flows (Login and Create Account) are unaffected by this feature

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.

Technical Documentation Checklist:

- Validate that all 41 checklist items are correctly displayed across the 9 required sections
- Ensure checkbox interaction (check/uncheck) works correctly with immediate visual feedback
- Confirm the progress counter updates in real time upon each toggle
- Verify that saving persists state to the server and triggers the correct 'Evaluated' status
- Validate role-based behavior: mandatory for Manufacturer, Importer, Distributor; optional for Authorized Representative
- Confirm that checklist state is independent per product version
- Verify all CRA Annex reference links open correctly in a new tab

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.

2. Testing Methodologies Used

To ensure thorough and reliable coverage, the following testing methodologies were applied across all four features:

Manual Functional Testing

- Step-by-step validation of UI workflows, business rules, field rendering, and save/navigation behaviour
- Performed in modern desktop browsers to simulate real end-user interaction
- Focused on validating business rules such as one-task-per-rule enforcement, Section 1 → Section 2 dependency gate, no-duplicate enforcement, and 41-item threshold for Evaluated status

Exploratory Testing

- Performed around areas involving asynchronous processing, pagination edge cases, dynamic field locking, multi-user task generation, and partial save scenarios
- Allowed identification of unexpected behaviors in drawer interactions, exposure recalculation, repeated logins, and unsaved state navigation

Black Box Testing

- Tests written from the end-user perspective, without knowledge of internal implementation details
- Inputs and outputs validated against documented expected behaviour — all nine Likelihood × Impact matrix combinations, file uploads, button clicks, dialog interactions, and status changes were covered

Regression Testing

- Ensured each new feature integrates cleanly with existing platform functionality: Tasks tab, version detail navigation, task list filtering, and authentication flows
- Confirmed that no existing compliance assessment flows, task management, or sign-in/create-account flows were broken by any of the new features

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.

3. Configuration Management

3.1 Functionality Overview

3.1.1 Configuration Management Tab

The Configuration Management tab, accessible from the Version Detail page, acts as a scan orchestration hub. It does not perform scans itself — scans are executed externally using OpenSCAP, and results are uploaded to OSCRAT for processing, reporting, and compliance tracking.

Key behaviour includes:

- A Jobs table listing all scan imports for the version, sorted newest-first, showing Status, Format, Started, Triggered By, Duration, Total Rules, Pass, and Fail counts.
- A Refresh button to poll for updated job statuses without navigating away.
- An Import button that opens a drawer for uploading .xml scan files (ARF 1.1, XCCDF 1.2, OVAL 5.x).
- Download and Delete actions available per job row. Delete requires confirmation.
- Clicking a Completed job row navigates to the Configuration Scan Report detail page.
- Pagination controls for navigating across multiple scan jobs.

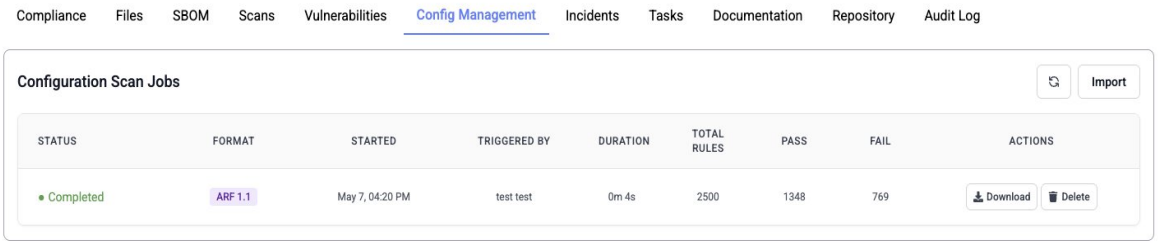

Figure 1: Config Management tab

3.1.2 Configuration Scan Report

Opened by clicking a Completed job row. Displays structured scan output in three sections:

- Overview — Total Rules, Pass, Fail, Error, Not Applicable, Scan Date, Format, Triggered By.
- Benchmark — Benchmark ID and version, applied Profile, Target Hostname.
- Rules — A full table of all evaluated rules with Rule ID, Title, Severity, Result, and a context-sensitive Action button.

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.

Action button logic:

- Failed rule, no linked task → 'Create Task' button.
- Failed rule with linked task → 'View Task' button.
- Pass / Error / Not Applicable → no action button.

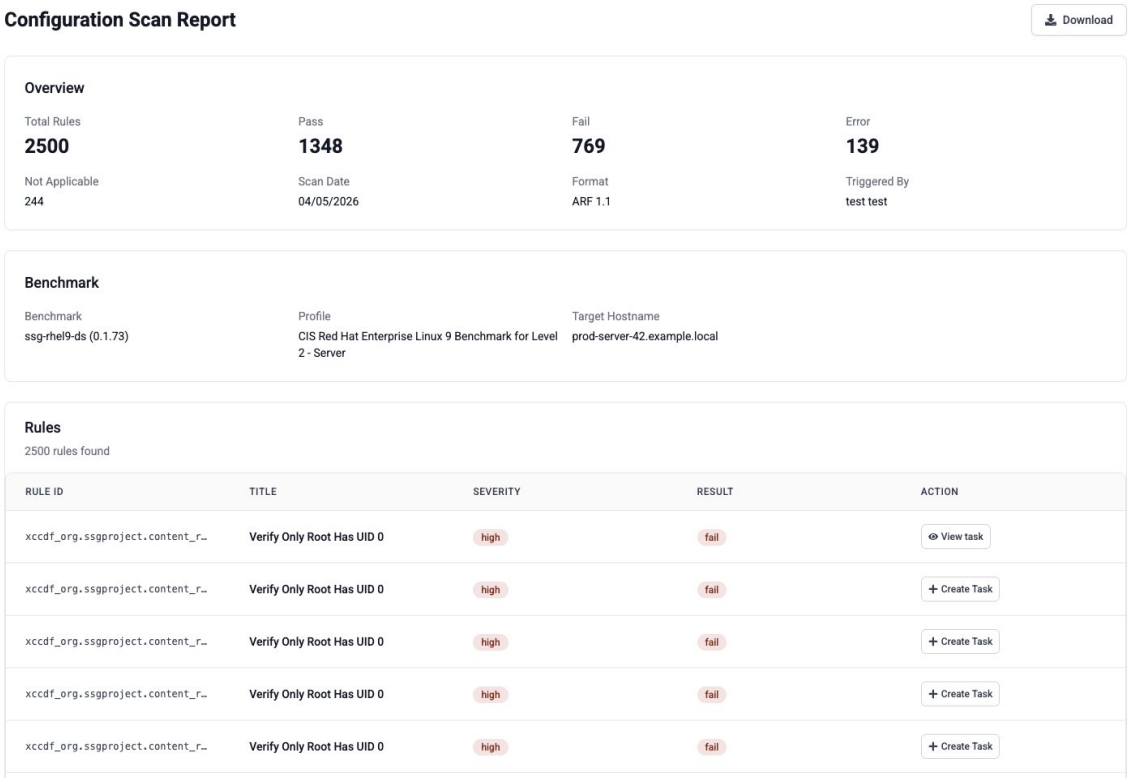

Figure 2: Configuration Scan Report

3.1.3 Create Task from Failed Rule

Clicking 'Create Task' on a failed rule opens a pre-filled dialog:

- Title pre-filled as 'Remediate Config [Rule Title]' — editable.
- Status defaults to 'To Do'.
- Product and Version are pre-set and locked to the current context.
- Due Date defaults to today's date.
- Description pre-filled with Rule ID and Severity — editable.
- On creation, the task appears in the version's Tasks tab with type Configuration Management. The rule row button changes from 'Create Task' to 'View Task'.

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.

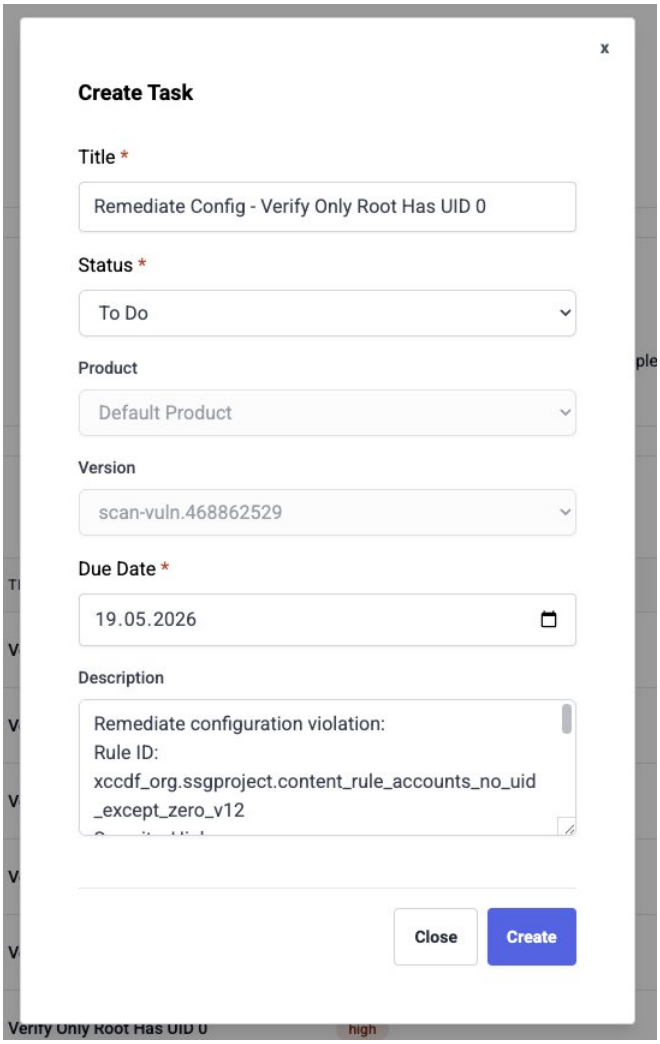

Figure 3: Create Task from failed rule

3.1.4 Re-upload and Task Lifecycle

After external remediation, users import a new scan file. OSCRAT creates a new scan job independently of previous imports, allowing historical tracking and compliance drift analysis. Configuration Management tasks can be marked Done once compliance is demonstrated in an updated scan.

3.2 Test Scenarios

1. Configuration Management Tab — Navigation & Layout

Nr	Scenario	Steps	Expected Result	Status
ID 1	Navigate to Configuration Management tab	Open any product version detail page and click the 'Config Management' tab	The tab loads showing the heading 'Configuration Scan Jobs', a Refresh button, an Import button, and a	**Pass**

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.

Nr	Scenario	Steps	Expected Result	Status
			(possibly empty) jobs table	
ID 2	Jobs table column headers present	Navigate to the Config Management tab with at least one existing job	Table columns displayed: Status, Format, Started, Triggered By, Duration, Total Rules, Pass, Fail, Actions	**Pass**
ID 3	Empty state — no jobs	Navigate to the Config Management tab on a version with no prior imports	The jobs table is empty; Import button and Refresh button are still visible and clickable	**Pass**
ID 4	Refresh button reloads the jobs list	Click the Refresh button	The jobs list is reloaded without full page navigation; job statuses reflect the latest server state	**Pass**
ID 5	Jobs sorted newest-first	Import two scan files sequentially	The most recently imported job appears at the top of the table	**Pass**

2. Import File Drawer

Nr	Scenario	Steps	Expected Result	Status
ID 6	Open Import File drawer	Click the Import button	The Import File drawer opens with heading 'Import File', a file upload area, a Cancel button, and a disabled Import button	**Pass**
ID 7	Import button disabled before file selection	Open the Import File drawer without selecting a file	The Import button inside the drawer is disabled and cannot be clicked	**Pass**
ID 8	Cancel drawer without importing	Open the Import File drawer and click Cancel	The drawer closes; no new job is added to the jobs table	**Pass**
ID 9	Upload a valid ARF 1.1 XML file	Open the drawer, select a valid ARF 1.1 .xml file, click Import	The drawer closes; a new job row appears in the table; clicking Refresh eventually	**Pass**

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.

Nr	Scenario	Steps	Expected Result	Status
			shows status 'Completed'	
ID 10	Upload a valid XCCDF 1.2 XML file	Open the drawer, select a valid XCCDF 1.2 .xml file, click Import	The drawer closes; a new job row appears; after Refresh the job reaches 'Completed' and Format shows 'XCCDF 1.2'	**Pass**
ID 11	Upload a valid OVAL 5.x XML file	Open the drawer, select a valid OVAL 5.x .xml file, click Import	The drawer closes; a new job row appears and processes successfully	**Pass**
ID 12	Drag-and-drop file upload	Drag a valid .xml file onto the upload area in the drawer	The file is accepted; the filename is shown; the Import button becomes enabled	**Pass**
ID 13	Import button enabled after file selection	Select a valid .xml file via the file chooser	The Import button in the drawer becomes enabled	**Pass**
ID 14	Job row appears immediately after import	Click Import in the drawer	A new row is visible in the jobs table immediately (possibly with a non-Completed status) without requiring a manual Refresh	**Pass**
ID 15	Job transitions to Completed after Refresh	After importing, click Refresh periodically	The job's status dot changes to '● Completed' once processing finishes	**Pass**

3. Jobs Table — Row Data & Actions

Nr	Scenario	Steps	Expected Result	Status
ID 16	Completed job displays correct columns	Open the tab after a job reaches Completed status	Row shows: ● Completed status, correct Format (ARF 1.1 or XCCDF 1.2), Started timestamp, Triggered By (current user), Duration, Total	**Pass**

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.

Nr	Scenario	Steps	Expected Result	Status
			Rules, Pass count, Fail count	
ID 17	Click a completed job row navigates to report	Click anywhere on a Completed job row	Browser navigates to the Configuration Scan Report detail page for that job	**Pass**
ID 18	Download original scan file from table	Click the Download button on a job row	The original .xml scan file is downloaded without modification	**Pass**
ID 19	Delete job shows confirmation prompt	Click the Delete button on a job row	A native confirmation prompt appears asking the user to confirm deletion	**Pass**
ID 20	Confirm delete removes job permanently	Click Delete on a job row and confirm the prompt	The job row is removed from the table; the scan report is no longer accessible	**Pass**
ID 21	Cancel delete keeps job	Click Delete on a job row, then cancel/dismiss the prompt	The job row remains in the table; no data is lost	**Pass**
ID 22	Pagination — next page button	Import enough jobs to exceed one page	The Next Page button becomes enabled; clicking it shows the next page of jobs	**Pass**
ID 23	Pagination — previous page button disabled on first page	Navigate to the Config Management tab with jobs present	The Previous Page button is disabled on the first page	**Pass**
ID 24	Pagination counter shows correct page numbers	Navigate between pages	Page counter shows 'X / Y' reflecting the current and total page numbers correctly	**Pass**

4. Configuration Scan Report Page

Nr	Scenario	Steps	Expected Result	Status
ID 25	Scan report page loads correctly	Click a Completed job row	The Configuration Scan Report page loads with heading 'Configuration	**Pass**

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.

Nr	Scenario	Steps	Expected Result	Status
			Scan Report', breadcrumb, Download button, Overview section, Benchmark section, and Rules section	
ID 26	Breadcrumb version link returns to Config tab	Click the version link in the breadcrumb	User is navigated back to the Config Management tab of the version	**Pass**
ID 27	Download button on report page	Click the Download button on the scan report page	The original uploaded .xml file is downloaded unchanged	**Pass**
ID 28	Overview section displays all summary fields	Open any completed scan report	Overview section shows: Total Rules, Pass, Fail, Error, Not Applicable, Scan Date, Format, Triggered By	**Pass**
ID 29	Benchmark section displays metadata	Open a completed scan report	Benchmark section shows: Benchmark ID and version, Profile name, Target Hostname	**Pass**
ID 30	Rules section shows rule count	Open a completed scan report	Rules section heading shows 'X rules found' matching the Total Rules value in the Overview	**Pass**
ID 31	Rules table columns present	Open a completed scan report	Rules table displays columns: Rule ID, Title, Severity, Result, Action	**Pass**
ID 32	Failed rule shows 'Create Task' button	Open a scan report with at least one failed rule	The Action cell for each failed rule (with no linked task) shows a 'Create Task' button	**Pass**
ID 33	Passing rule shows no action button	Open a scan report with passing rules	The Action cell for passing rules is empty — no button is shown	**Pass**
ID 34	Error / Not Applicable rules show no action	Open a scan report containing Error or Not Applicable results	The Action cell for Error and Not Applicable rules is empty	**Pass**

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.

Nr	Scenario	Steps	Expected Result	Status
	button			
ID 35	Severity values displayed correctly	Inspect individual rule rows	Severity column shows one of: high, medium, or low for each rule	**Pass**
ID 36	Result values displayed correctly	Inspect individual rule rows	Result column shows one of: pass, fail, error, or not applicable for each rule	**Pass**

5. Create Task from Failed Rule

Nr	Scenario	Steps	Expected Result	Status
ID 37	Open Create Task dialog from failed rule	Click 'Create Task' on a failed rule in the Rules section	The Create Task dialog opens with heading 'Create Task'	**Pass**
ID 38	Title field pre-filled	Open the Create Task dialog for a failed rule	The Title field is pre-filled with 'Remediate Config [Rule Title]' and is editable	**Pass**
ID 39	Status defaults to 'To Do'	Open the Create Task dialog	The Status field defaults to 'To Do'	**Pass**
ID 40	Product and Version fields pre-set and disabled	Open the Create Task dialog	Product is pre-set to the current product and Version to the current version; both fields are disabled and cannot be changed	**Pass**
ID 41	Due Date defaults to today	Open the Create Task dialog	The Due Date field is pre-filled with today's date	**Pass**
ID 42	Description pre-filled with rule details	Open the Create Task dialog	Description field is pre-filled with the rule ID and severity level; field is editable	**Pass**
ID 43	Close dialog without creating task	Open the Create Task dialog and click Close	The dialog closes; no task is created; the 'Create Task' button remains on the rule row	**Pass**
ID 44	Create task successfully	Open the Create Task dialog, review pre-filled	The task is created; the dialog closes; the 'Create Task' button on	**Pass**

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.

Nr	Scenario	Steps	Expected Result	Status
		fields, and click Create	the rule row is replaced with 'View Task'	
ID 45	Created task appears in Tasks tab	After creating a task from a failed rule, navigate to the version's Tasks tab	The new task is listed in the Tasks tab with type Configuration Management and status To Do	**Pass**
ID 46	'View Task' button navigates to task detail	After task creation, click 'View Task' on the rule row	The browser navigates to the task detail page for the linked task	**Pass**
ID 47	Only one task linkable per rule per scan job	Create a task for a failed rule; attempt to create another task for the same rule	The 'Create Task' button is replaced by 'View Task' after the first task is created; a second task cannot be created for the same rule in the same scan job	**Pass**
ID 48	Edit task title before creating	Open Create Task dialog, clear the title field, enter a custom title, click Create	The task is created with the custom title; 'View Task' link navigates to a task with that title	**Pass**
ID 49	Edit description before creating	Open Create Task dialog, append additional text to the	The task description includes the original pre-filled text plus the appended content	**Pass**

6. Re-upload & Task Lifecycle

Nr	Scenario	Steps	Expected Result	Status
ID 50	Re-upload updated scan after remediation	After fixing a failing rule externally, import a new scan file	OSCRAT processes the new file and generates a new Configuration Scan Report; the updated rule result (e.g., pass) is reflected in the new report	**Pass**
ID 51	Previous scan job preserved after re-upload	Import a second scan file	The original scan job remains in the jobs table; new job is added as a separate row (newest-first)	**Pass**

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.

Nr	Scenario	Steps	Expected Result	Status
ID 52	Mark task as Done after compliance demonstrated	Open a Configuration Management task and change status to Done	Task status is updated to Done; the task in the Tasks tab reflects the change	**Pass**

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. Risk Assessment Task

4.1 Functionality Overview

4.1.1 Risk Assessment Task

The Risk Assessment Task extends OSCRAT's standard task model with a structured risk management workflow. It is not a separate task type — it is enabled by checking a Risk Assessment checkbox on the task form, which reveals additional fields while leaving all standard task fields (Name, Assignee, Status, Due Date, Description, Product) intact.

Key behaviour includes:

- The Risk Assessment checkbox is unchecked by default; checking it reveals Section 1 (Risk Details) and Section 2 (Risk Treatment). Unchecking hides these sections 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.

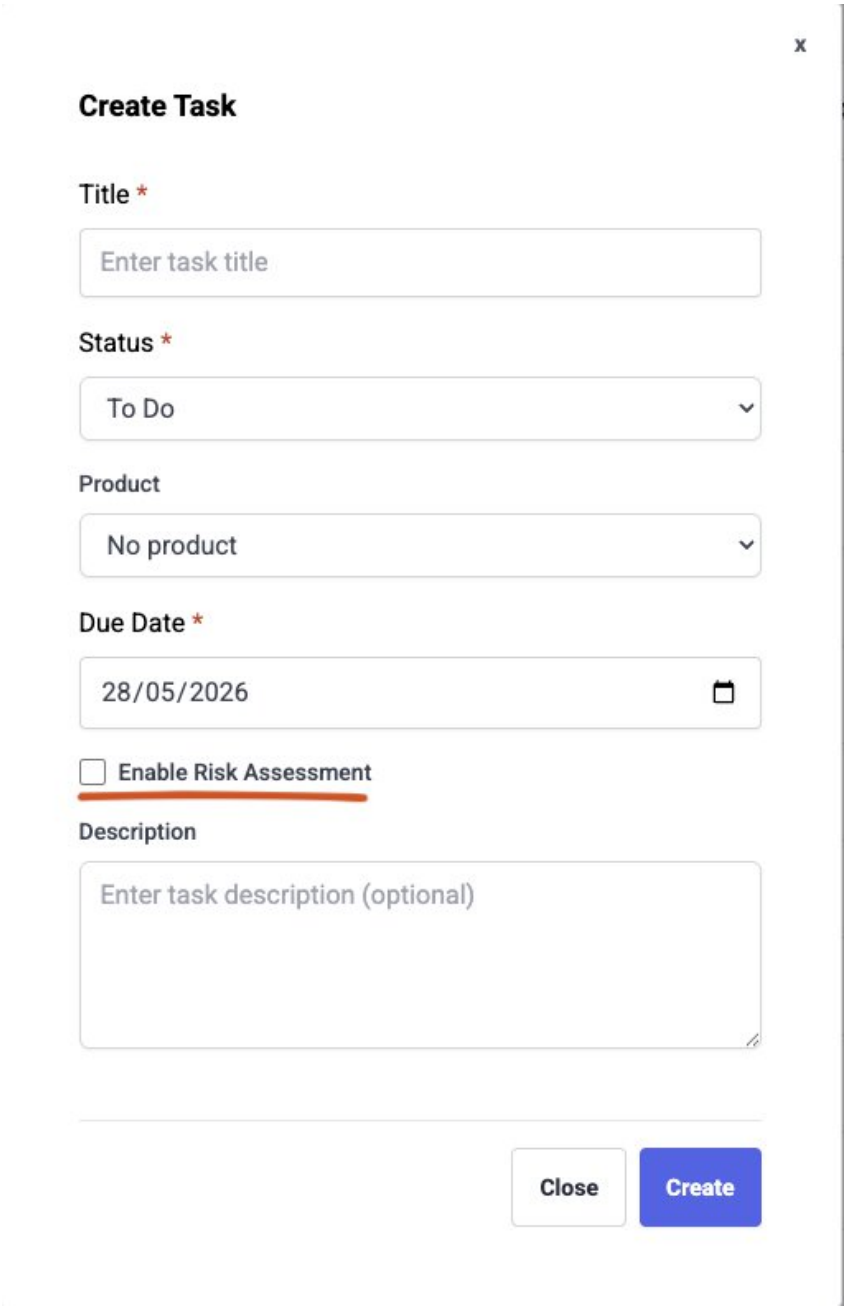

Figure 4: Risk Assessment Task enable check box

- The Task Type dropdown is a separate field with nine options: Vulnerability, Incident, SBOM, Documentation, Risk, Training, Configuration Management, Requirements, Other. It is independent of the Risk Assessment checkbox.
- Section 1 captures the risk context: Asset (linked to the task's Product), Threat (long text), Category (multi-select: CONFIDENTIALITY, INTEGRITY, AVAILABILITY), Likelihood (Low/Medium/High), Impact (Low/Medium/High), Exposure (auto-calculated, read-only), and Owner (organisation user).

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.

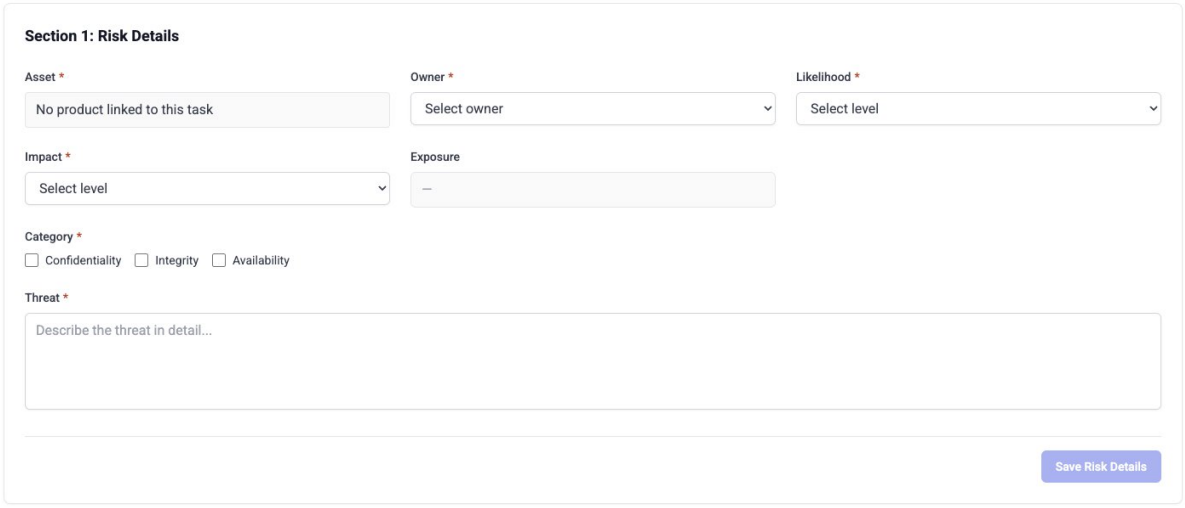

Figure 5: Section 1: Risk Details

- Section 2 captures the treatment decision: Treatment (ACCEPT/REDUCE/AVOID/TRANSFER), Measures (optional long text), Residual Exposure (Low/Medium/High), and Responsible (organisation user).
- Section 2 is gated: it cannot be interacted with until all mandatory Section 1 fields have been filled. If a Section 1 field is cleared after Section 2 is unlocked, Section 2 locks again.

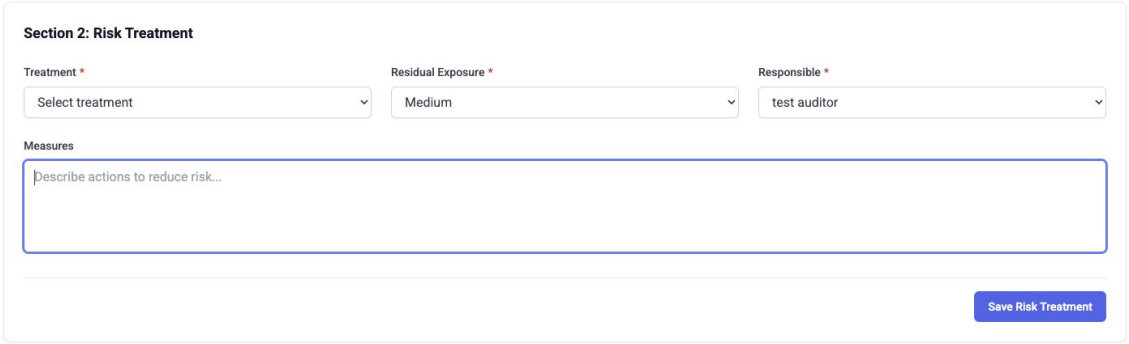

Figure 6: Section 2: Risk Treatment

- Risk Exposure is automatically calculated using the matrix: High × High = High, High × Medium = High, High × Low = Medium, Medium × High = High, Medium × Medium = Medium, Medium × Low = Low, Low × High = Medium, Low × Medium = Low, Low × Low = Low. The field updates immediately on any Likelihood or Impact change.
- Task status follows the progression: To Do → Planned → In Progress → Done. Marking Done confirms completion of the risk assessment.
- All risk data is linked to the associated Product and persists across sessions.

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.

4.2 Test Scenarios

1. Risk Checkbox & Task Type Field

Nr	Scenario	Steps	Expected Result	Status
ID 53	Risk checkbox visible on task creation form	Open the task creation form for any product version	A 'Risk Assessment' checkbox is visible on the form; it is unchecked by default	**Pass**
ID 54	Enabling Risk checkbox reveals Section 1 and Section 2 fields	Check the Risk Assessment checkbox on the task creation form	Section 1 (Risk Details) and Section 2 (Risk Treatment) fields appear below the task description; they are hidden when the checkbox is unchecked	**Pass**
ID 55	Unchecking Risk checkbox hides the extra fields	Check the Risk Assessment checkbox, then uncheck it	Section 1 and Section 2 fields are hidden again; previously entered values are discarded	**Pass**
ID 56	Task Type dropdown contains all required options	Open the task creation form and inspect the Task Type dropdown	Dropdown contains: Vulnerability, Incident, SBOM, Documentation, Risk, Training, Configuration Management, Requirements, Other	**Pass**
ID 57	Task Type can be set independently of the Risk checkbox	Select 'Risk' from the Task Type dropdown without checking the Risk Assessment checkbox	The Task Type field accepts the 'Risk' value; the extra risk fields are only shown when the Risk Assessment checkbox is checked, not solely based on Task Type	**Pass**

2. Section 1: Risk Details — Field Presence & Validation

Nr	Scenario	Steps	Expected Result	Status
ID 58	All Section 1 fields are present	Check the Risk Assessment checkbox and inspect Section 1	Section 1 displays: Asset, Threat, Category, Likelihood, Impact, Exposure, Owner — all labelled	**Pass**

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.

Nr	Scenario	Steps	Expected Result	Status
			correctly	
ID 59	Asset field is linked to the task's Product	Check the Risk Assessment checkbox and inspect the Asset field	Asset is predefined and linked to the product associated with the task; it cannot be a free-text entry inconsistent with that product	**Pass**
ID 60	Threat field accepts long text input	Enter a detailed multi-sentence description into the Threat field	The field accepts long text without truncation; content is saved correctly	**Pass**
ID 61	Category allows multiple selections	Click the Category field and select CONFIDENTIALITY, INTEGRITY, and AVAILABILITY simultaneously	All three values can be selected at the same time; each selected value is displayed in the field	**Pass**
ID 62	Category allows a single selection	Select only INTEGRITY from the Category field	Only INTEGRITY is selected; the field reflects a single value	**Pass**
ID 63	Likelihood dropdown contains correct options	Open the Likelihood dropdown in Section 1	Dropdown shows exactly three options: Low, Medium, High	**Pass**
ID 64	Impact dropdown contains correct options	Open the Impact dropdown in Section 1	Dropdown shows exactly three options: Low, Medium, High	**Pass**
ID 65	Exposure field is read-only and auto-calculated	Select values for Likelihood and Impact; attempt to edit the Exposure field directly	The Exposure field is read-only; its value is automatically calculated based on the selected Likelihood and Impact	**Pass**
ID 66	Owner field lists organisation users	Open the Owner dropdown in Section 1	The dropdown shows users from the organisation; a user can be selected as the	**Pass**

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.

Nr	Scenario	Steps	Expected Result	Status
			risk owner	
ID 67	All Section 1 mandatory fields are required	Check the Risk Assessment checkbox, leave all Section 1 fields empty, and attempt to save or proceed to Section 2	Validation errors appear for each empty mandatory field: Asset, Threat, Category, Likelihood, Impact, Owner	**Pass**

3. Exposure Auto-Calculation — Full Risk Matrix

Nr	Scenario	Steps	Expected Result	Status
ID 68	Exposure: Low × Low = Low	Set Likelihood = Low and Impact = Low	Exposure auto-populates as 'Low'	**Pass**
ID 69	Exposure: Low × Medium = Low	Set Likelihood = Low and Impact = Medium	Exposure auto-populates as 'Low'	**Pass**
ID 70	Exposure: Low × High = Medium	Set Likelihood = Low and Impact = High	Exposure auto-populates as 'Medium'	**Pass**
ID 71	Exposure: Medium × Low = Low	Set Likelihood = Medium and Impact = Low	Exposure auto-populates as 'Low'	**Pass**
ID 72	Exposure: Medium × Medium = Medium	Set Likelihood = Medium and Impact = Medium	Exposure auto-populates as 'Medium'	**Pass**
ID 73	Exposure: Medium × High = High	Set Likelihood = Medium and Impact = High	Exposure auto-populates as 'High'	**Pass**
ID 74	Exposure: High × Low = Medium	Set Likelihood = High and Impact = Low	Exposure auto-populates as 'Medium'	**Pass**
ID 75	Exposure: High × Medium = High	Set Likelihood = High and Impact = Medium	Exposure auto-populates as 'High'	**Pass**
ID 76	Exposure: High × High = High	Set Likelihood = High and Impact = High	Exposure auto-populates as 'High'	**Pass**

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.

Nr	Scenario	Steps	Expected Result	Status
ID 77	Exposure updates immediately when Likelihood changes	Set Likelihood = Low and Impact = High (Exposure = Medium); change Likelihood to High	Exposure immediately updates to 'High' without requiring a page action	**Pass**
ID 78	Exposure updates immediately when Impact changes	Set Likelihood = Medium and Impact = Low (Exposure = Low); change Impact to High	Exposure immediately updates to 'High' without requiring a page action	**Pass**

4. Section 2 Blocked Until Section 1 Complete

Nr	Scenario	Steps	Expected Result	Status
ID 79	Section 2 is inaccessible when Section 1 is empty	Check the Risk Assessment checkbox; leave all Section 1 fields empty; attempt to interact with any Section 2 field	Section 2 fields are disabled or blocked; a message or visual indicator communicates that Section 1 must be completed first	**Pass**
ID 80	Section 2 is inaccessible when Section 1 is partially filled	Fill in some but not all mandatory Section 1 fields; attempt to interact with Section 2	Section 2 remains inaccessible until all mandatory Section 1 fields have values	**Pass**
ID 81	Section 2 becomes accessible once all Section 1 fields are filled	Complete all mandatory Section 1 fields (Asset, Threat, Category, Likelihood, Impact, Owner)	Section 2 fields become enabled and interactive	**Pass**
ID 82	Clearing a Section 1 field after Section 2 is unlocked blocks Section 2 again	Complete Section 1 to unlock Section 2, then clear a mandatory Section 1 field	Section 2 becomes inaccessible again until the cleared field is re-populated	**Pass**

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. Section 2: Risk Treatment — Field Presence & Validation

Nr	Scenario	Steps	Expected Result	Status
ID 83	All Section 2 fields are present	Complete Section 1 and inspect Section 2	Section 2 displays: Treatment, Measures, Residual Exposure, Responsible — all labelled correctly	**Pass**
ID 84	Treatment dropdown contains correct options	Open the Treatment dropdown in Section 2	Dropdown shows exactly four options: ACCEPT, REDUCE, AVOID, TRANSFER	**Pass**
ID 85	Measures field accepts long text	Enter a detailed multi-sentence description into the Measures field	The field accepts long text without truncation; content is saved correctly	**Pass**
ID 86	Measures field is optional	Complete all mandatory Section 2 fields but leave Measures empty; save the task	The task saves successfully without a value in the Measures field; no validation error is shown for this field	**Pass**
ID 87	Residual Exposure dropdown contains correct options	Open the Residual Exposure dropdown in Section 2	Dropdown shows exactly three options: Low, Medium, High	**Pass**
ID 88	Responsible field lists organisation users	Open the Responsible dropdown in Section 2	The dropdown shows users from the organisation; a user can be selected as the responsible party	**Pass**
ID 89	All Section 2 mandatory fields are required	Complete Section 1, then leave Treatment, Residual Exposure, and Responsible empty; attempt to save	Validation errors appear for each empty mandatory Section 2 field: Treatment, Residual Exposure, Responsible	**Pass**

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.

Nr	Scenario	Steps	Expected Result	Status
ID 90	Treatment: ACCEPT can be selected	Select ACCEPT from the Treatment dropdown	ACCEPT is saved as the treatment value; the task saves without error	**Pass**
ID 91	Treatment: REDUCE can be selected	Select REDUCE from the Treatment dropdown	REDUCE is saved as the treatment value; the task saves without error	**Pass**
ID 92	Treatment: AVOID can be selected	Select AVOID from the Treatment dropdown	AVOID is saved as the treatment value; the task saves without error	**Pass**
ID 93	Treatment: TRANSFER can be selected	Select TRANSFER from the Treatment dropdown	TRANSFER is saved as the treatment value; the task saves without error	**Pass**

6. Task Status Transitions & Completion

Nr	Scenario	Steps	Expected Result	Status
ID 94	Default task status is 'To Do'	Create a new risk assessment task and inspect the Status field	Status is set to 'To Do' by default	**Pass**
ID 95	Status can be updated to 'Planned'	Open a risk task and change Status to 'Planned'	Status is updated to 'Planned' and persisted	**Pass**
ID 96	Status can be updated to 'In Progress'	Open a risk task and change Status to 'In Progress'	Status is updated to 'In Progress' and persisted	**Pass**
ID 97	Status can be updated to 'Done'	Complete all risk fields and change Status to 'Done'	Status is updated to 'Done' and persisted; this confirms risk assessment completion	**Pass**
ID 98	Full status progression: To Do → Planned → In Progress → Done	Step through each status in order for a single risk task	Each transition is accepted; the status at each step is saved correctly	**Pass**
ID 99	Task linked to correct	Create a risk assessment task	The task's Product field is pre-linked to the	**Pass**

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.

Nr	Scenario	Steps	Expected Result	Status
	Product	from a specific product version	originating product and cannot be set to a different product	
ID 100	Completed task data persists on re-open	Fill in all Section 1 and Section 2 fields, save, close, and reopen the task	All entered values (threat text, category selections, likelihood, impact, exposure, treatment, residual exposure, etc.) are retained exactly as entered	**Pass**

7. Task Visibility in Task List

Nr	Scenario	Steps	Expected Result	Status
ID 101	Risk task appears in organisation task list	Create and save a risk assessment task; navigate to the organisation task list	The task is listed with correct Name, Assignee, Status, and Due Date	**Pass**
ID 102	Risk task can be filtered by status in task list	Apply a status filter (e.g., 'To Do') in the organisation task list	Risk assessment tasks with that status appear in the filtered results	**Pass**
ID 103	Risk task detail page accessible from task list	Click a risk assessment task row in the task list	The task detail page opens and displays all standard and risk-specific fields	**Pass**
ID 104	Multiple risk tasks can exist for the same product	Create two separate risk assessment tasks for the same product version	Both tasks appear in the task list independently; their risk data does not interfere	**Pass**

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. Security Awareness and Training Evidence

5.1 Functionality Overview

5.1.1 Security Awareness and Training Evidence

This feature ensures that every registered OSCRAT user is directed to complete mandatory security awareness training. OSCRAT does not host the training content itself — training materials are externally hosted and linked from within the auto-generated task.

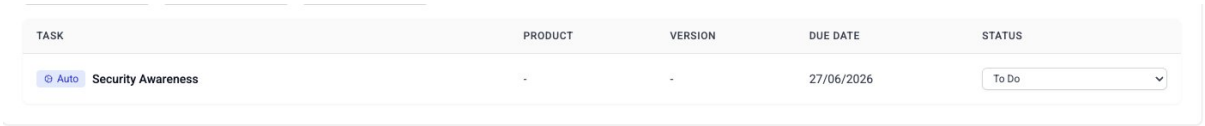

Figure 7: Security Awareness task

Key behaviour includes:

- On the user's first login to their OSCRAT account, the system automatically creates an 'Awareness training' task without any manual action required.
- The task is immediately visible in the organisation's task list.
- The auto-generated task is pre-filled with all required field values (see Task Field Values below).
- The Description field contains external links to the relevant training materials, which the user must access and complete outside the OSCRAT platform.
- The user confirms training completion by manually updating the task status to 'Done'.
- No duplicate tasks are created if the user logs in again after the initial task has been generated.
- Each new user independently triggers their own task creation on first login; multiple users each receive a separate task assigned to them.

Task field values (auto-generated):

- Task Name — predefined value, e.g. 'Awareness training'.
- Assignee — the user who logged in for the first time.
- Status — initially set to 'To Do'; can be manually updated by the user as training progresses.
- Due Date — automatically set to a defined period from creation (e.g. up to one month from the creation date).
- Description — contains links to the external training materials and guidance on how to complete them.

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.

5.2 Test Scenarios

1. Automatic Task Creation on First Login

Nr	Scenario	Steps	Expected Result	Status
ID 105	Awareness task auto-created on first login	Register a new OSCRAT user account and log in for the first time	An 'Awareness training' task is automatically generated and is visible in the organisation's task list	**Pass**
ID 106	Task not duplicated on subsequent logins	Log out and log in again with the same account that already had a task created	No additional 'Awareness training' task is created; only the original task remains	**Pass**
ID 107	Task Name is predefined correctly	Inspect the auto-generated task after first login	Task Name is set to 'Awareness training' (or the predefined platform value)	**Pass**
ID 108	Assignee field populated with the new user	Inspect the auto-generated task after first login	The Assignee field is set to the user who just logged in for the first time	**Pass**
ID 109	Initial status is 'To Do'	Inspect the auto-generated task after first login	The Status field is set to 'To Do'	**Pass**
ID 110	Due date set automatically within defined period	Inspect the Due Date of the auto-generated task	Due Date is set to approximately one month (or the configured period) from the task creation date	**Pass**
ID 111	Description contains training material links	Open the auto-generated task and read the Description field	Description includes at least one external link pointing to the awareness training materials	**Pass**
ID 112	Task visible in organisation task list	Navigate to the organisation's task list after first login	The 'Awareness training' task is listed and visible to organisation members with appropriate access	**Pass**
ID 113	Task creation is immediate	Log in as a new user and immediately	The task is already present without needing to refresh or	**Pass**

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.

Nr	Scenario	Steps	Expected Result	Status
	— no delay required	navigate to the task list	wait	

2. Task Field Values and Content

Nr	Scenario	Steps	Expected Result	Status
ID 114	Task type is correct	Open the auto-generated task and check the Task Type field	Task Type is set to the appropriate category for awareness training tasks	**Pass**
ID 115	External training links are reachable	Open the task Description and click each external link	Each link opens an external page in a new browser tab without errors	**Pass**
ID 116	Description is not empty	Inspect the Description field of the auto-generated task	Description field contains meaningful content (links and/or guidance text); it is not blank	**Pass**
ID 117	Due date is not set in the past	Inspect the Due Date of the newly created task	The Due Date is today or a future date; it is never set in the past	**Pass**
ID 118	Due date respects configured period boundary	Compare the Due Date with the task creation timestamp	Due Date does not exceed the maximum configured period (e.g., no more than 31 days from creation)	**Pass**

3. User Interaction with the Task

Nr	Scenario	Steps	Expected Result	Status
ID 119	User can manually change status to 'In Progress'	Open the 'Awareness training' task and change Status to 'In Progress'	Status is updated to 'In Progress' and the change is persisted	**Pass**
ID 120	User can manually change status to 'Done'	Open the 'Awareness training' task and change Status to 'Done'	Status is updated to 'Done' and the change is persisted	**Pass**
ID 121	User can change status back	Set task status to 'In Progress', then revert it to 'To Do'	Status returns to 'To Do' and is saved correctly	**Pass**

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.

Nr	Scenario	Steps	Expected Result	Status
	to 'To Do'			
ID 122	Status change is reflected in the organisation task list	Change task status to 'Done', then navigate to the organisation task list	The task in the list reflects the updated status without requiring a full page reload	**Pass**
ID 123	User can edit the task title	Open the task and modify the Task Name field, then save	The new title is persisted and reflected in the task list and task detail view	**Pass**
ID 124	User can edit the Description field	Open the task and append text to the Description, then save	The updated description is persisted and visible on reopening the task	**Pass**
ID 125	User can modify the Due Date	Open the task and change the Due Date to a different future date, then save	The new Due Date is saved and displayed correctly in the task detail view	**Pass**
ID 126	Training confirmed by marking task as Done	User completes the external training and marks the task status as 'Done'	Task status shows 'Done'; this serves as the in-platform confirmation of training completion	**Pass**

4. Task Visibility and Access

Nr	Scenario	Steps	Expected Result	Status
ID 127	Task appears in the organisation task list	Navigate to the organisation's task list	The 'Awareness training' task is visible in the list with correct Name, Assignee, Status, and Due Date columns	**Pass**
ID 128	Task can be filtered by assignee	Apply an assignee filter for the new user in the organisation task list	Only tasks assigned to that user are shown; the 'Awareness training' task is included	**Pass**
ID 129	Task can be filtered by status	Apply a 'To Do' status filter in the organisation task list	The 'Awareness training' task appears under the 'To Do' filter results	**Pass**

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.

Nr	Scenario	Steps	Expected Result	Status
ID 130	Task detail page accessible from task list	Click the 'Awareness training' task row in the organisation task list	The task detail page opens showing all fields: Name, Assignee, Status, Due Date, and Description	**Pass**
ID 131	Multiple new users each receive their own task	Register two new user accounts and log each in for the first time	Each user receives a separate 'Awareness training' task assigned specifically to them	**Pass**
ID 132	Task assignee cannot be changed to another user	Open the auto-generated task and attempt to change the Assignee field	If the assignee is locked: the field is disabled. If editable: the change can be saved; no system error occurs	**Pass**

5. Regression — Login & Create Account

Nr	Scenario	Steps	Expected Result	Status
ID 133	Login with valid credentials still works	Enter a registered email and correct password, click 'Sign In'	User is successfully logged in and redirected to the dashboard; awareness task triggers correctly on first login	**Pass**
ID 134	Create account flow still works	Complete the registration form with valid data and click 'Register'	Account is created successfully; on first login the awareness task is auto-generated	**Pass**

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.

6. Technical Documentation Checklist

6.1 Functionality Overview

6.1.1 Technical Documentation Checklist

This checklist is a version-level tool that helps users verify all required technical documentation items for a product version under the EU Cyber Resilience Act (CRA). It is integrated into the CRA Compliance Assessment as an additional Area of Requirements.

Key behaviour includes:

- The checklist contains 41 items grouped into 9 sections, each referencing the relevant CRA Annex or Article.
- Users check items as fulfilled (Evaluated and Fully compliant); unchecked items are marked as Not Evaluated.
- No free-text answers are required — interaction is binary (checked / unchecked).
- A progress counter (X of 41 items checked) updates immediately upon each toggle.
- A 'Save Checklist' button persists state to the server. Navigating away via the Back button without saving discards unsaved changes.
- When all 41 items are checked and saved, the area is automatically marked as 'Evaluated' in the Requirements Status Table.
- The checklist is mandatory for Manufacturer, Importer, and Distributor roles and optional for Authorized Representatives (whose result does not affect the overall compliance status).
- The checklist is independent per product version.

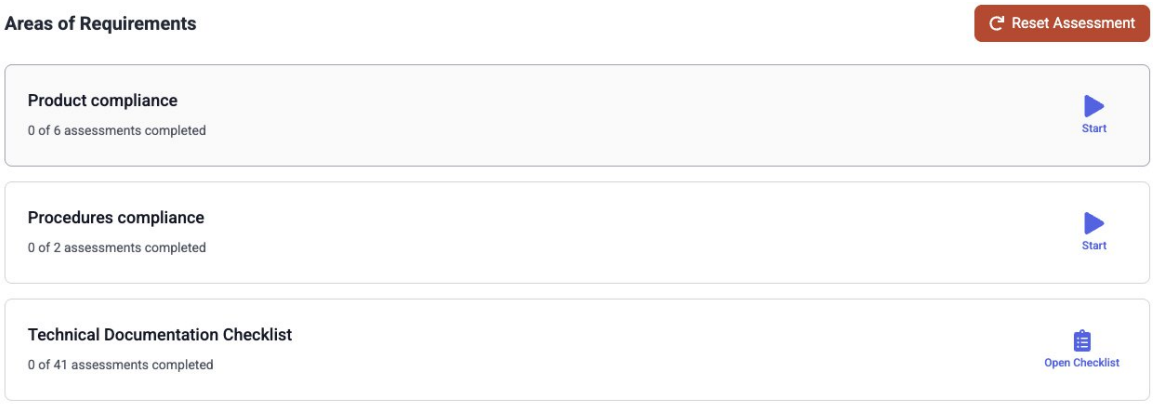

Figure 8: Technical Documentation Checklist in Areas of Requirements

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.

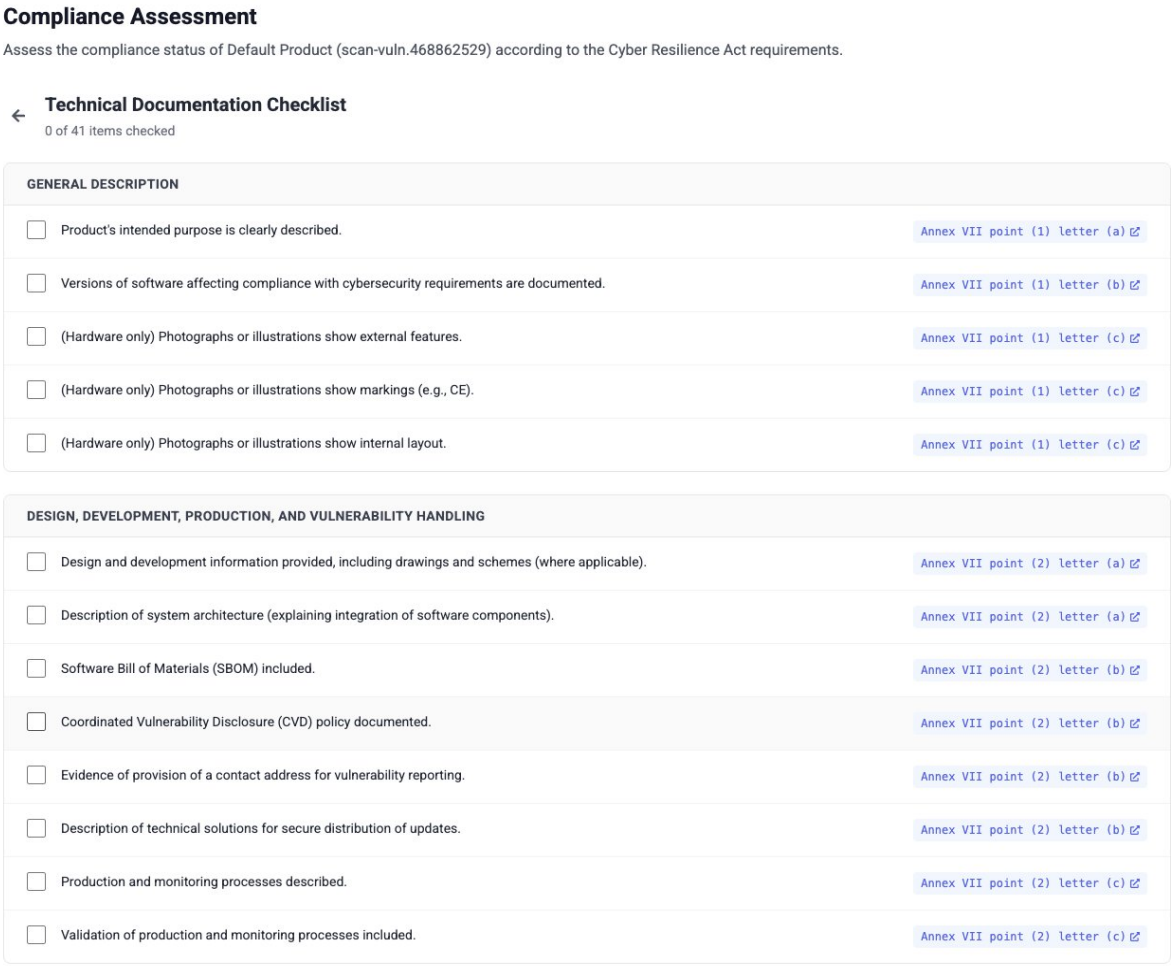

Figure 9: Technical Documentation Checklist items

6.2 Test Scenarios

1. Technical Documentation Checklist

Nr	Scenario	Steps	Expected Result	Status
ID 135	Navigate to the checklist	Open the compliance assessment for a product version → Click 'Start Assessment' → Click 'Open Checklist' on the Technical Documentation Checklist card	The checklist page loads, showing the heading 'Technical Documentation Checklist' and a progress counter 'X of 41 items checked'	**Pass**
ID 136	Back button returns to Areas of Requiremen	On the checklist page, click the Back icon button at the top left	User is returned to the Areas of Requirements view; no unsaved changes are persisted	**Pass**

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.

Nr	Scenario	Steps	Expected Result	Status
	ts			
ID 137	Progress counter starts at correct value	Open the checklist when no items have been checked	Counter shows '0 of 41 items checked'	**Pass**
ID 138	Progress counter increments on check	Check any unchecked item	Counter updates immediately to reflect the new checked count (e.g., '1 of 41 items checked')	**Pass**
ID 139	Progress counter decrements on uncheck	Check an item, then uncheck it	Counter decrements immediately back to the previous value	**Pass**
ID 140	Progress counter reaches maximum	Check all 41 items	Counter shows '41 of 41 items checked'	**Pass**
ID 141	Check a single checklist item	Click the checkbox of an unchecked item	A green check icon appears next to the item and the item text is displayed with a strikethrough	**Pass**
ID 142	Uncheck a checked item	Click the checkbox of an already-checked item	The green check icon disappears and the strikethrough is removed from the item text	**Pass**
ID 143	All 41 items are present and grouped	Open the checklist and review all sections	Exactly 41 items are displayed across 9 sections matching the CRA requirements	**Pass**
ID 144	Annex link opens in a new tab	Click the Annex/Article hyperlink on any item	The official EUR-Lex CRA regulation page opens in a new browser tab	**Pass**
ID 145	Save partial progress	Check a subset of items and click 'Save Checklist'	Checked states are persisted; reloading the page shows the same items checked	**Pass**
ID 146	Save all 41 items checked	Check all 41 items and click 'Save Checklist'	All states are persisted and the Technical Documentation	**Pass**

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.

Nr	Scenario	Steps	Expected Result	Status
			Checklist area is marked 'Evaluated' in the Requirements Status Table	
ID 147	Navigating away without saving discards changes	Check some items, then click the Back button without saving	Unsaved changes are discarded; the checklist retains the last saved state on next open	**Pass**
ID 148	Area NOT marked Evaluated when fewer than 41 items saved	Check 40 items and save	Area status remains unchanged (not 'Evaluated') in the Requirements Status Table	**Pass**
ID 149	Checklist area card shows progress count	Navigate to the Areas of Requirements view	The Technical Documentation Checklist card displays 'X of 41 assessments completed'	**Pass**
ID 150	Checklist is mandatory for Manufacturer role	Access the compliance assessment as a Manufacturer	The Technical Documentation Checklist area is displayed and its status is included in overall compliance	**Pass**
ID 151	Checklist is mandatory for Importer role	Access the compliance assessment as an Importer	The Technical Documentation Checklist area is displayed and its status is included in overall compliance	**Pass**
ID 152	Checklist is mandatory for Distributor role	Access the compliance assessment as a Distributor	The Technical Documentation Checklist area is displayed and its status is included in overall compliance	**Pass**
ID 153	Checklist is optional for Authorized Representative role	Access the compliance assessment as an Authorized Representative	The user can choose whether or not to complete the checklist; checklist result does NOT affect overall compliance status	**Pass**

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.

Nr	Scenario	Steps	Expected Result	Status
ID 154	Authorized Representative can still complete checklist voluntarily	As Authorized Representative, open and complete the checklist, then save	Checklist is saved but does not change the overall compliance assessment result	**Pass**
ID 155	Section 1 — General Description has 5 items	Open the checklist and count Section 1 items	5 items are displayed, all referencing Annex VII point (1)	**Pass**
ID 156	Section 2 — Design, Development, Production has 8 items	Open the checklist and count Section 2 items	8 items are displayed, all referencing Annex VII point (2)	**Pass**
ID 157	Section 9 — User Information has 14 items	Open the checklist and count Section 9 items	14 items are displayed, all referencing Annex II	**Pass**
ID 158	Checklist state is independent per product version	Complete the checklist for Version A, then open the checklist for Version B of the same product	Version B's checklist is independent; it does not inherit the checked state from Version A	**Pass**
ID 159	Hardware-only items visible for all product types	Open the checklist for a software-only product and review Section 1 items 3–5	Hardware-only items are displayed; user documentation notes they may be skipped for software-only products	**Pass**
ID 160	Section 4 Article 13(8) item has no Annex link	Open the checklist and inspect the Article 13(8) item in Section 4	No Annex link hyperlink is shown for that item (standalone article reference)	**Pass**
ID 161	Reload page retains last saved state	Check several items, save, then refresh the browser	Items that were saved remain checked; unsaved items since last save are not checked	**Pass**

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. Conclusion

The QA validation process for the latest release of the OSCRAT Platform confirms that all four tested features are functionally stable, logically consistent, and meet the defined business requirements.

7.1 Configuration Management

- Configuration Management Tab — Navigation, tab loading, Refresh polling, Import button, and empty-state rendering all behave correctly. Jobs are sorted newest-first and pagination controls function as expected.
- Import File Drawer — All three supported formats (ARF 1.1, XCCDF 1.2, OVAL 5.x) are accepted. Drag-and-drop and file-chooser upload paths work correctly. The Import button is properly disabled until a file is selected. Cancel discards without side effects.
- Jobs Table — All columns render accurate data. Download returns the original unmodified file. Delete requires and respects confirmation. Clicking a row correctly navigates to the scan report.
- Configuration Scan Report — Overview, Benchmark, and Rules sections render complete data from the uploaded scan file. Rule count, severity, and result values are displayed accurately. Action button logic (Create Task / View Task / none) is correctly applied by result type.
- Create Task from Failed Rule — Dialog pre-fill logic (title, status, product, version, due date, description) is correct. One-task-per-rule enforcement is working. Created tasks appear in the Tasks tab and are navigable via 'View Task'.
- Re-upload & Task Lifecycle — Re-uploading a new scan creates a separate, independent job without affecting existing jobs. Task status can be updated to Done to reflect completed remediation.

7.2 Risk Assessment Task

- Risk Checkbox & Task Type Field — The Risk Assessment checkbox correctly controls field visibility; unchecking removes the sections. The Task Type dropdown contains all nine required values and operates independently of the checkbox.
- Section 1: Risk Details — All seven fields render with the correct input types. Asset is properly linked to the task's Product. Category supports multi-select. Likelihood and Impact expose the correct three-value dropdowns. The Exposure field is read-only. All mandatory fields produce validation errors when left empty.
- Exposure Auto-Calculation — All nine combinations of the Likelihood × Impact matrix have been explicitly tested and produce the correct Exposure

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.

value. The field recalculates immediately on any change without requiring a save action.

- Section 2 Dependency Gate — Section 2 is correctly blocked when Section 1 is empty or partially filled, and unlocks only when all mandatory Section 1 fields are populated. Re-clearing a Section 1 field correctly re-locks Section 2.
- Section 2: Risk Treatment — All four Treatment options (ACCEPT, REDUCE, AVOID, TRANSFER) can be selected and saved. The Measures field is correctly optional. Residual Exposure and Responsible are mandatory and enforce validation.
- Task Status Transitions — The full progression To Do → Planned → In Progress → Done works correctly. Each transition is persisted. Marking Done confirms risk assessment completion.
- Task Visibility — Risk tasks appear in the organisation task list with correct field values. Filtering by status works as expected. Multiple risk tasks for the same product version are independent.

7.3 Security Awareness and Training Evidence

- Automatic Task Creation on First Login — The 'Awareness training' task is created immediately and correctly on the first login of every new user. No duplicate tasks are generated on subsequent logins.
- Task Field Values and Content — All auto-populated fields (Name, Assignee, Status, Due Date, Description) carry the correct predefined values. External training links in the Description are present and reachable. Due Date boundaries are respected.
- User Interaction with the Task — Status transitions (To Do → In Progress → Done) work correctly and are persisted. Users can edit the title, description, and due date. Marking the task as 'Done' serves as the in-platform confirmation of training completion.
- Task Visibility and Access — The task appears in the organisation task list and can be filtered by assignee and status. Multiple new users each receive their own individually assigned task.
- Regression — Login & Create Account — All critical authentication scenarios remain unaffected. The awareness task triggers correctly on first login without disrupting the account creation or sign-in flows.

7.4 Technical Documentation Checklist

- Technical Documentation Checklist — Thoroughly validated for checkbox interaction, progress tracking, save/discard behavior, role-based optionality (including Authorized Representative handling), cross-version independence, section integrity (all 41 items across 9 sections), and CRA Annex link navigation.

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.

7.5 Test Scenario Execution Summary

Configuration Management

Category	Executed	Passed	Failed	Notes
Config Management Tab — Navigation & Layout	5	5	0	All scenarios passed
Import File Drawer	10	10	0	All scenarios passed
Jobs Table — Row Data & Actions	9	9	0	Delete tested with confirmation
Configuration Scan Report Page	12	12	0	All scenarios passed
Create Task from Failed Rule	13	13	0	One task per rule enforced
Re-upload & Task Lifecycle	3	3	0	Re-upload creates separate job
Total	**52**	**52**	**0**	**No blocking defects detected**

Risk Assessment Task

Category	Executed	Passed	Failed	Notes
Risk Checkbox & Task Type Field	5	5	0	Checkbox-driven field visibility confirmed
Section 1: Risk Details — Fields & Validation	10	10	0	All mandatory fields and input types verified
Exposure Auto-Calculation (Full Matrix)	11	11	0	All 9 matrix combinations covered
Section 2 Blocked Until Section 1 Complete	4	4	0	Dependency logic fully validated
Section 2: Risk Treatment —	11	11	0	All treatment options and optionality

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.

Category	Executed	Passed	Failed	Notes
Fields & Validation				checked
Task Status Transitions & Completion	7	7	0	Full To Do → Done progression tested
Task Visibility in Task List	4	4	0	List, filter, and multi-task independence
Total	**52**	**52**	**0**	**No blocking defects detected**

Security Awareness and Training Evidence

Category	Executed	Passed	Failed	Notes
Automatic Task Creation on First Login	9	9	0	Task created immediately; no duplicates
Task Field Values and Content	5	5	0	All field defaults validated
User Interaction with the Task	8	8	0	Status updates and edits covered
Task Visibility and Access	6	6	0	Multi-user and filtering verified
Regression — Login & Create Account	2	2	0	Existing flows unaffected
Total	**30**	**30**	**0**	**No blocking defects detected**

Technical Documentation Checklist

Category	Executed	Passed	Failed	Notes
Technical Documentation Checklist	27	27	0	All scenarios passed
Total	**27**	**27**	**0**	**No blocking defects detected**

Overall Grand Total

Feature	Executed	Passed	Failed	Notes
Configuration Management	52	52	0	All scenarios passed

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.

Feature	Executed	Passed	Failed	Notes
Risk Assessment Task	52	52	0	All scenarios passed
Security Awareness & Training	30	30	0	All scenarios passed
Technical Documentation Checklist	27	27	0	All scenarios passed
Grand Total	**161**	**161**	**0**	**No blocking defects detected**

Overall Assessment: The system is ready for release from a QA standpoint. All verified features are working as expected. Please keep in mind that most of the data is mocked and does not represent the final version.

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. Test Scenarios Summary Chart

The chart below presents the total number of test scenarios executed and passed per feature across the four tested functionalities.

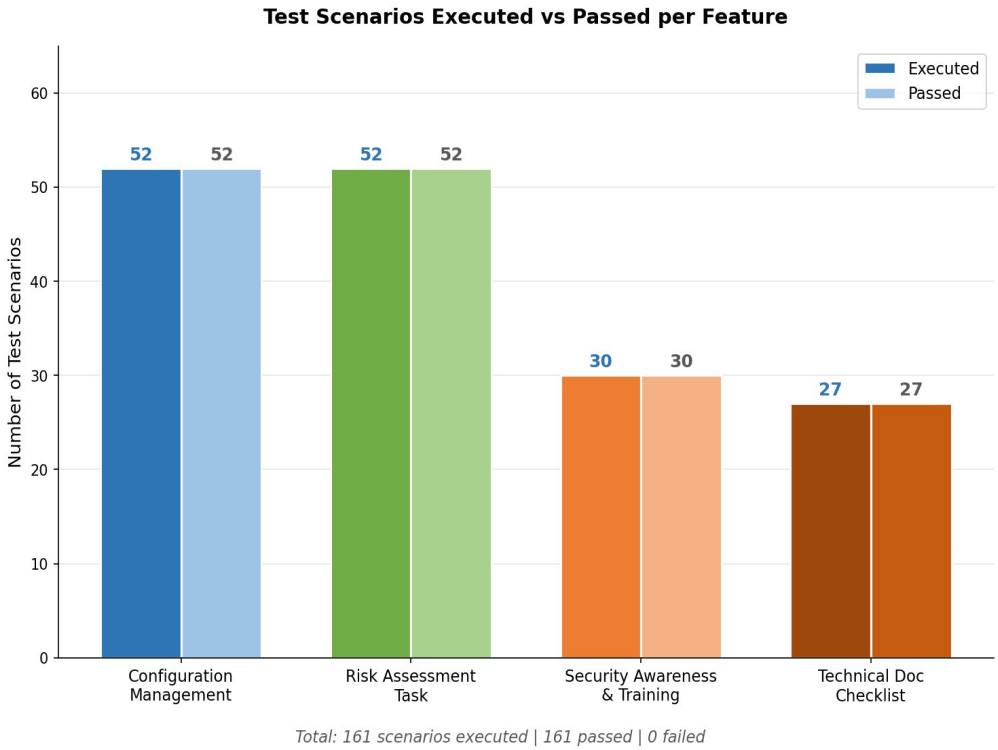

Figure 10: Test Scenarios Executed vs Passed per Feature

9. Conclusion

With this period's work, OSCRAT is feature complete. Teams can assess and treat risk, run a continuous security awareness program, check their technical documentation against regulatory requirements, manage security configuration with evidence-based scanning and remediation, and rely on a full audit trail of user actions. These pillars build on the documentation, conformity, and encryption work delivered earlier, and together they cover the full set of Cyber Resilience Act activities the project set out to support. We will focus on QA, feedback and the rest of the technical polish required for final release.

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 M18

www.oscrat.eu

https://www.linkedin.com/comp