OSCRAT

Open-Source Cyber Resilience Act Tools

OSCRAT USER MANUAL

Version: 08.09.2026

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.

Table of contents

PURPOSE AND SCOPE OF THE MANUAL 3
1. GETTING STARTED 6
1.1 LOGIN PAGE 6
1.2 FORGOT PASSWORD PAGE 9
1.3 ACCOUNT CREATION PAGE 11
1.4 CRA APPLICABILITY CHECK PAGE 13
2. ACCOUNT MANAGEMENT 16
2.1 ACCOUNT SETTINGS PAGE 16
3. NAVIGATION 22
3.1 SIDEBAR NAVIGATION 22
4. ORGANIZATIONS 25
4.1 ORGANIZATIONS PAGE 25
4.2 ORGANIZATION DASHBOARD PAGE 28
4.3 ORGANIZATION SETTINGS PAGE 32
5. PRODUCTS 39
5.1 PRODUCTS PAGE 39
5.2 PRODUCT DETAIL PAGE 45
5.3 ADD NEW PRODUCT VERSION PAGE 48
6. VERSION DETAIL PAGE & TABS 50
6.1 VERSION DETAIL PAGE — OVERVIEW & HEADER 50
6.2 DECLARATION OF CONFORMITY SECTION 54
6.3 FILES TAB 58
6.4 SBOM TAB 59
6.5 SCANS TAB 61
6.6 VULNERABILITIES TAB 63
6.7 INCIDENTS TAB 66
6.8 TASKS TAB (VERSION) 67
6.9 CONFIGURATION MANAGEMENT TAB 69
6.10 AUDIT LOG TAB 72
6.11 DOCUMENTATION TAB (VERSION) — FILTERS 75
7. COMPLIANCE ASSESSMENT 77
7.1 COMPLIANCE ASSESSMENT PAGE 77

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.

7.2 CRA TECHNICAL DOCUMENTATION CHECKLIST 81
8. TASKS 86
8.1 ORGANIZATION TASKS PAGE 86
8.2 TASK DETAIL PAGE 90
8.3 RISK ASSESSMENT TASK 94
8.4 SECURITY AWARENESS TRAINING TASK 100
8.5 AUTO-GENERATED COMPLIANCE OBLIGATION TASKS 101
8.6 CONFIGURATION MANAGEMENT SCAN-TRIGGERED TASKS 103
9. DOCUMENTATION 104
9.1 DOCUMENTATION PAGE 104

Figures

Figure 1: Login screen 7
Figure 2: Forgot Password screen 10
Figure 3: Account Creation screen 12
Figure 4: CRA Applicability Check screen (Question 1) 14
Figure 5: Account Settings screen 18
Figure 6: Sidebar — organization dropdown menu open 23
Figure 7: Sidebar Navigation 24
Figure 8: Organizations page 26
Figure 9: Create Organization modal 27
Figure 10: Organization Dashboard page 31
Figure 11: Organization Settings — Settings tab 34
Figure 12: Invite New Member dialog 35
Figure 13: Pending Invitations table 36
Figure 14: Organization Settings — Members tab 37
Figure 15: Organization Settings — Audit Logs tab 38
Figure 16: Organization Settings — Audit Logs tab 41
Figure 17: Products page — Filters panel 42
Figure 18: Add Product wizard — Step 1 43
Figure 19: Add Product wizard — Step 2 44
Figure 20: Product Detail page 47
Figure 21: Add New Product Version page 49
Figure 22: Version Detail page — header & stats bar 51

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 23: Version Detail — Repository tab 53
Figure 24: Declaration of Conformity section 55
Figure 25: Version Detail — Files tab 59
Figure 26: Version Detail — SBOM tab 60
Figure 27: Version Detail — Scans tab 62
Figure 28: Version Detail — Vulnerabilities tab 64
Figure 29:Vulnerability Details page 65
Figure 30: Version Detail — Incidents tab 67
Figure 31: Version Detail — Tasks tab 68
Figure 32: Version Detail — Configuration Management tab 70
Figure 33: Configuration Scan Report page 72
Figure 34: Version Detail — Audit Log tab 74
Figure 35: Version Detail — Documentation tab 75
Figure 36: Compliance Assessment — Areas of Requirements view 78
Figure 37 : Compliance Assessment — requirement question 79
Figure 38: CRA Technical Documentation Checklist 82
Figure 39: Organization Tasks page 88
Figure 40: Create Task dialog 89
Figure 41: Task Detail page 93
Figure 42: Risk Assessment — Risk Details & Risk Treatment 98
Figure 43: Security Awareness Training task 101
Figure 44: Auto-generated compliance obligation task 102
Figure 45: Documentation page 105
Figure 46: Create Documentation dialog 106
Figure 47: Documentation detail/editor page 108

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.

PURPOSE AND SCOPE OF THE MANUAL

This User Manual provides practical guidance on how to access, navigate, and use the OSCRAT platform. OSCRAT is an open-source solution designed to support small and medium-sized enterprises in managing activities related to compliance with the Cyber Resilience Act.

The platform brings together the main organisational, technical, and documentation processes required throughout the compliance lifecycle. These include assessing whether the Cyber Resilience Act applies to a product, managing organisations and user roles, registering products and product versions, carrying out organisation- and version-level compliance assessments, generating and managing Software Bills of Materials, performing vulnerability and configuration scans, recording incidents, conducting cybersecurity risk assessments, managing compliance tasks, preparing technical documentation, and producing the EU Declaration of Conformity. The platform also maintains audit logs to ensure the traceability of actions performed by users.

This manual is intended for SMEs, manufacturers, importers, distributors, authorised representatives, compliance officers, cybersecurity professionals, product managers, and other users involved in managing products with digital elements. It explains the main functions of the platform through page descriptions, step-by-step instructions, screenshots, and practical notes.
The manual follows the structure of the platform, beginning with account creation, login, and the Cyber Resilience Act Applicability Check, before covering organisation management, product and version management, compliance assessments, security activities, tasks, documentation, and reporting. Users may read the manual in sequence or consult individual sections when guidance on a specific feature is required.

OSCRAT is designed to support and structure compliance-related activities. However, the platform and this manual do not replace legal, regulatory, or technical advice. Organisations remain responsible for assessing the specific obligations applicable to their products and for ensuring that the information and evidence entered into the platform are complete, accurate, and up to date.

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. GETTING STARTED

1.1 LOGIN PAGE

URL: /auth/login

OVERVIEW

The Login page is the entry point to the OSCRAT platform. It allows registered users to authenticate and access their account, or navigate to account creation and password recovery flows.

The page is clean and minimal, centered on the screen, with the OSCRAT branding (shield logo + "Open-Source Cyber Resilience Act Tools" tagline) displayed prominently at the top.

PAGE ELEMENTS

1. OSCRAT LOGO & BRANDING

- Displayed at the top center of the page.
- Shows the shield icon alongside the "OSCRAT" name and the subtitle "Open-Source Cyber Resilience Act Tools".

2. WELCOME HEADING

- Title: "Welcome"
- Subtitle: "Log in to your account"
- Provides context to the user about the purpose of this page.

3. EMAIL FIELD — Mandatory

- Label: "Email"
- Input type: text (email address)
- Purpose: Enter the email address associated with your account.
- Example: user@example.com

4. PASSWORD FIELD — Mandatory

- Label: "Password"
- Input type: password (characters are hidden by default)
- A toggle button (eye icon) on the right side of the field allows you to show or hide the password text.
- Purpose: Enter your account password.

5. "FORGOT YOUR PASSWORD?" LINK

- Located to the right of the "Password" label.
- Clicking this link navigates to the password recovery page (/auth/forgot-password), where you can request a reset email.

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. SIGN IN BUTTON

- A prominent dark-blue button labeled "Sign in".
- Clicking this submits the form with the entered email and password to authenticate the user.
- On success: redirects to the main application (/organization).
- On failure: an error message is displayed on the page.
- Note: By clicking "Sign in", you agree to the platform's Terms and Conditions, Privacy Statement, and Security Policy (links provided below the button).

7. APPLICABILITY CHECK BUTTON

- A secondary button labeled "Applicability Check".
- Allows users to access the CRA Applicability Check tool without requiring a full login.
- Use this to check whether the Cyber Resilience Act applies to your product/organization before creating an account.

8. LEGAL LINKS

- Displayed below the action buttons.
- Text: "By clicking Sign in, you agree to our..."
- Three clickable links:
  a. Terms and Conditions -> https://www.unicis.tech/terms
  b. Privacy Statement -> https://www.unicis.tech/privacy
  c. Security Policy -> https://www.unicis.tech/security

9. CREATE A FREE ACCOUNT LINK

- Located below the login form.
- Text: "Don't have an account? Create a free account"
- Clicking navigates to the account registration page (/auth/join).

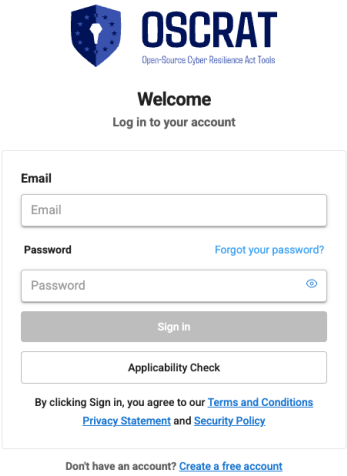

Figure 1: Login screen

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.

HOW TO LOG IN — STEP BY STEP

Step 1: Open your browser and navigate to the OSCRAT login page: /auth/login
Step 2: In the "Email" field, type your registered email address.
Step 3: In the "Password" field, type your account password.
(Optionally, click the eye icon to reveal the password and verify it is correct before submitting.)
Step 4: Click the "Sign in" button.
Step 5: If your credentials are correct, you will be redirected to the OSCRAT organizations page (/organization). If not, an error message will appear — check your email and password and try again.

FORGOT YOUR PASSWORD?

If you cannot remember your password:

1. Click the "Forgot your password?" link next to the Password label.
2. You will be redirected to the password recovery page.
3. Enter your registered email address and follow the instructions sent to your inbox.

DON'T HAVE AN ACCOUNT?

If you are a new user and need to register:

1. Click "Create a free account" at the bottom of the page.
2. You will be redirected to the registration page (/auth/join).
3. Fill in your details to create a new OSCRAT account.

APPLICABILITY CHECK (NO LOGIN REQUIRED)

The "Applicability Check" button provides access to a CRA (Cyber Resilience Act) applicability assessment tool without requiring an account. Use this feature to quickly determine whether the CRA obligations apply to your product or service.

NOTES

- The login page automatically redirects authenticated users. If you are already logged in and visit /auth/login, you will be taken directly to /organization.
- Credentials are transmitted securely over HTTPS.
- For account or access issues, contact your organization administrator or refer to the support resources at https://www.unicis.tech.

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.

1.2 FORGOT PASSWORD PAGE

URL: /auth/forgot-password

OVERVIEW

The Forgot Password page allows you to request a password reset link if you cannot remember your account password. Enter your registered email address and OSCRAT will send you a link to reset your password.

This page is accessible from the Login page via the "Forgot your password?" link next to the Password field.

PAGE ELEMENTS

1. OSCRAT LOGO & BRANDING
- Displayed at the top center of the page.

2. PAGE HEADING
- Title: "Reset Password"
- Confirms the purpose of this page.

3. EMAIL FIELD — Mandatory
- Label: "Email"
- Input type: text (email address)
- Purpose: Enter the email address associated with your OSCRAT account.
- Required field.

4. EMAIL PASSWORD RESET LINK BUTTON
- Labeled "Email Password Reset Link".
- Clicking this submits the form and sends a password reset email to the address entered.
- On success: a confirmation message is shown and an email is sent with a reset link.
- If the email is not found: the form may show an error or still show a confirmation to prevent account enumeration.

5. SIGN IN LINK
- Text: "Already have an account? Sign in"
- Located below the form.
- Clicking "Sign in" navigates back to the Login page (/auth/login).

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.

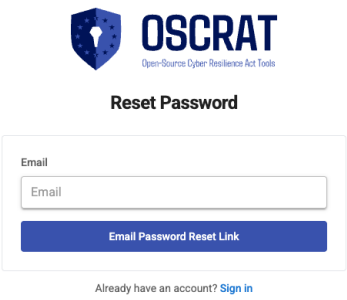

Figure 2: Forgot Password screen

HOW TO RESET YOUR PASSWORD — STEP BY STEP

Step 1: On the Login page (/auth/login), click the "Forgot your password?" link next to the Password label. (Or navigate directly to /auth/forgot-password)
Step 2: In the "Email" field, type the email address registered to your OSCRAT account.
Step 3: Click "Email Password Reset Link".
Step 4: Check your email inbox (and spam/junk folder) for a message from OSCRAT contains a password reset link.
Step 5: Click the link in the email. You will be taken to a page where you can set a new password.
Step 6: Enter and confirm your new password, then save. You can then log in with your new credentials.

NOTES

- The reset link sent to your email is time-limited. If it expires, repeat the process to request a new link.
- If you do not receive the email, check your spam or junk folder. Also verify that you entered the correct email address.
- If you no longer have access to the email address associated with your account, contact your organization administrator or support at https://www.unicis.tech.

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.

1.3 ACCOUNT CREATION PAGE

URL: /auth/join

OVERVIEW

The Account Creation page allows new users to register for a free OSCRAT account. It collects basic personal information and credentials to create a new user profile on the platform.

The page is accessible from the Login page via the "Create a free account" link.

PAGE ELEMENTS

1. **FIRST NAME FIELD — Mandatory**
   - Label: "First Name" | Required field.

2. **LAST NAME FIELD — Mandatory**
   - Label: "Last Name" | Required field.

3. **EMAIL FIELD — Mandatory**
   - Label: "Email" — the email used as your login identifier.
   - Example: user@example.com | Required field.

4. **PASSWORD FIELD — Mandatory**
   - Label: "Password" | Required field.

5. **CONFIRM PASSWORD FIELD — Mandatory**
   - Label: "Confirm Password"
   - Both password fields must match. | Required field.

6. **CANCEL BUTTON**
   - Discards the form and returns you to the previous page (Login page).

7. **CREATE ACCOUNT BUTTON**
   - Submits the registration form.
   - On success: your account is created and you are redirected into OSCRAT.
   - On failure: an error message is displayed (e.g., email already in use, password too weak).

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.

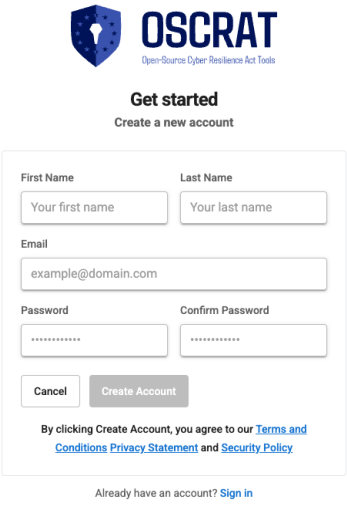

Figure 3: Account Creation screen

HOW TO CREATE A FREE ACCOUNT — STEP BY STEP

Step 1: Navigate to /auth/join (or click "Create a free account" on the Login page).
Step 2: Enter your First Name.
Step 3: Enter your Last Name.
Step 4: Enter a valid email address (this will be your login email).
Step 5: Choose a secure password.
Step 6: Re-enter the password in "Confirm Password".
Step 7: Click "Create Account".
Step 8: If all fields are valid, your account will be created and you will receive a confirmation email. Check your email inbox (and spam/junk folder) for a message from OSCRAT contains an activation link.

NOTES

- All fields are required. The form cannot be submitted unless all fields are filled in correctly.
- Use a unique, strong password to keep your account secure.
- If you already have an account, return to the Login page at /auth/login instead of creating a duplicate account.

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.

1.4 CRA APPLICABILITY CHECK PAGE

URL: /form

OVERVIEW

The CRA Applicability Check page is a guided questionnaire that helps you determine whether the EU Cyber Resilience Act (CRA) applies to your product or service.

This tool is accessible WITHOUT logging in — no account is required. It can also be used from within OSCRAT after logging in, in which case the result page offers additional actions such as directly adding the assessed product.

The check consists of 13 questions answered one at a time. A progress indicator shows how many questions you have completed and the percentage of the form done.

PAGE ELEMENTS

1. PAGE HEADING
- Title: "Cyber Resilience Act Applicability Check"

2. CLOSE BUTTON
- Exits the questionnaire and returns you to the previous page.

3. PROGRESS INDICATOR
- Displays current progress, e.g. "3/13 Questions" and "23%".
- Updates after each question is answered and "Next" is clicked.

4. QUESTION TEXT
- Each question is displayed one at a time in the main area of the page. It shows a descriptive paragraph above the Yes/No answer options, explaining the regulatory context, followed by a "References:" line linking to specific sections (e.g. "Section 1.1 of the CRA Form", "Section 1.2 of the CRA Form").

5. ANSWER OPTIONS (Radio Group) — Mandatory
- Most questions present a set of radio buttons with selectable answer options. Select exactly one answer before proceeding.
- Question 13 uses a category dropdown instead (see item 6 below).

6. CATEGORY DROPDOWN (Question 13 only) — Mandatory
- The final question asks you to select a product category from a dropdown list.
-

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. **BACK BUTTON**
   - Returns you to the previous question. Not available on the first question.

8. **NEXT BUTTON**
   - Advances to the next question. Only available after an answer has been selected. Not shown on the last question (replaced by "Finish").

9. **FINISH BUTTON**
   - Appears on the last question (Question 13) in place of the "Next" button. Submits all answers and displays the result.

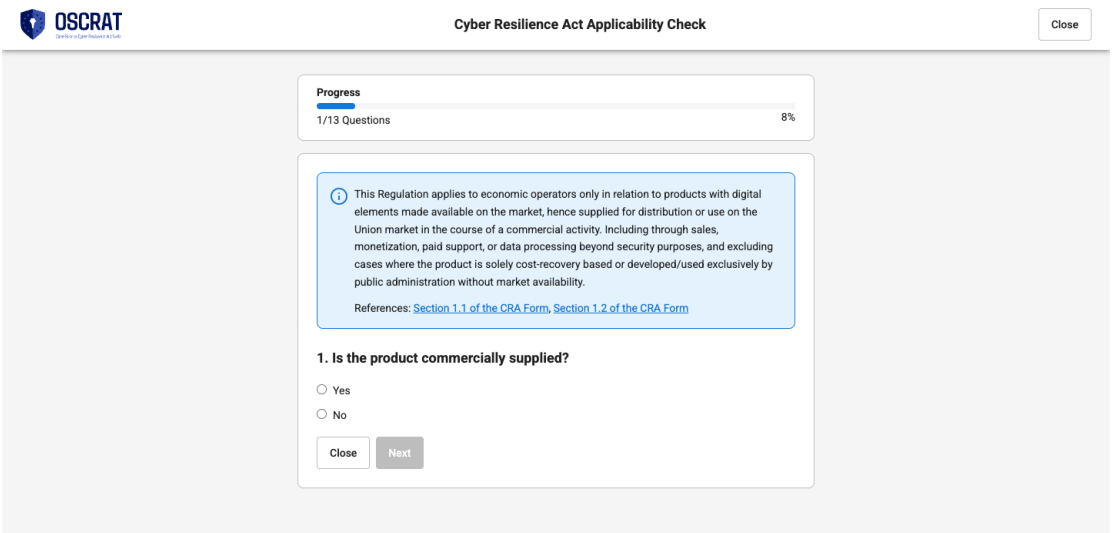

Figure 4: CRA Applicability Check screen (Question 1)

RESULT PAGE (UNAUTHENTICATED USER)

If you completed the check without logging in and the result indicates the CRA may apply, the result page shows:

1. HEADING: "Continue eligibility check"
2. REGISTER BUTTON — navigates to /auth/join.
3. LOG IN BUTTON — navigates to /auth/login.

RESULT PAGE (AUTHENTICATED USER)

If you are logged in and the result indicates your product requires assessment, the result page shows:

1. HEADING: "Product Requires Assessment"

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. ADD PRODUCT BUTTON — takes you directly to the product creation flow, pre-filled with data from the applicability check results (cache).
3. TRY AGAIN BUTTON — resets the form so you can start the check over.

HOW TO COMPLETE THE APPLICABILITY CHECK — STEP BY STEP

Step 1: Navigate to /form (or click "Applicability Check" on the Login page — no account required).
Step 2: Read the first question carefully.
Step 3: Select the radio button that best matches your situation, then click "Next".
Step 4: Repeat for each subsequent question. Use "Back" if you need to revise a previous answer.
Step 5: On Question 13, select your product category from the dropdown then click "Finish".
Step 6: Review the result:

- If not logged in: register or log in to proceed.
- If logged in: click "Add Product" to register the assessed
- product, or "Try Again" to restart.

NOTES

- No account is required to run the applicability check.
- Your answers are cached temporarily. If you are logged in, you can later add a product using those cached results ("From cache" option in the Add Product flow).
- The check covers 13 questions spanning product type, software classification, intended use, and CRA scope exclusions.

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. ACCOUNT MANAGEMENT

2.1 ACCOUNT SETTINGS PAGE

URL: /settings/account

OVERVIEW

The Account Settings page allows you to manage your personal OSCRATaccount. From here you can update your display name, email address, and profile avatar, and sign out of the platform.

Access this page by clicking your name/avatar link in the bottom of the sidebar on any page after login.

PAGE ELEMENTS

1. GO TO DASHBOARD LINK

- Located at the top of the page, above the Name section.
- Clicking it navigates to the dashboard of your most recently active organization.

2. NAME SECTION

- Heading: "Name"
- Description: "This is how your name will appear in the interface.
- Set the first and the last name."

a. FIRST NAME INPUT — Mandatory
- Label: "First Name" | Placeholder: "Your first name"

b. LAST NAME INPUT — Mandatory
- Label: "Last Name" | Placeholder: "Your last name"

c. SAVE CHANGES BUTTON (Name section)
- Disabled until you modify the first or last name fields.
- Click to save your updated name.

3. EMAIL ADDRESS SECTION

- Heading: "Email Address"
- Description: "The email address you use to sign in to your account."

a. EMAIL INPUT (read-only)
- Label: "Your email" — displays your current login email address.
- This field is read-only and cannot be edited from this page.

4. AVATAR SECTION

- Heading: "Avatar"

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.

- Description: "Click on the avatar to upload a custom one from your
- files."
- Accepted file types: .png, .jpg | Maximum file size: 2 MB

a. AVATAR IMAGE
- Displays your current profile picture.
- A default avatar (initials-based) is shown if no custom image has been uploaded.
- Click the avatar image to open a file picker and upload a new profile picture.

b. AVATAR NAME BUTTON
- Displays your name below the avatar image.
- Can also be clicked to trigger the file upload.

c. SAVE CHANGES BUTTON (Avatar section)
- Click to save the newly uploaded avatar image.

d. DELETE BUTTON (Avatar section)
- Appears (red, trash-can icon) next to "Save Changes" only after a new image file has been selected but not yet saved.

5. ACCOUNT ACTIONS SECTION

- Heading: "Account Actions"

a. SIGN OUT BUTTON
- Clicking this ends your current session and redirects you to the Login page (/auth/login).

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.

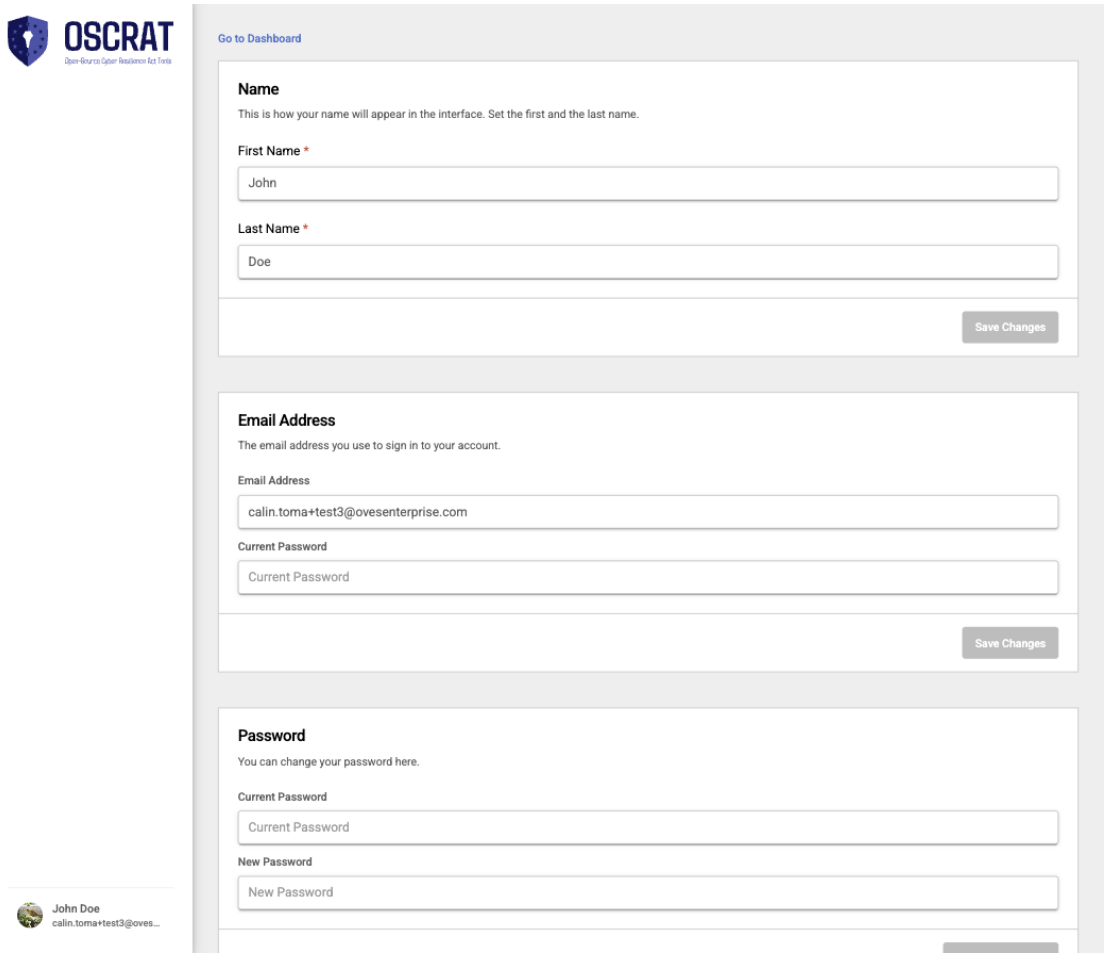

Figure 5: Account Settings screen

HOW TO UPDATE YOUR NAME

Step 1: Navigate to /settings/account.
Step 2: In the "Name" section, update the "First Name" and/or "Last Name".
Step 3: Click "Save Changes" in the Name section.

EMAIL ADDRESS

The email address shown is the one used to log in to OSCRAT. It is displayed for reference only and cannot be changed from this page. Contact your organization administrator or support if you need to update your login email.

HOW TO UPLOAD A PROFILE AVATAR

Step 1: Navigate to /settings/account.

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.

Step 2: In the "Avatar" section, click on the avatar image or your name button.
Step 3: A file picker opens. Select a .png or .jpg image file (max 2 MB).
Step 4: Click "Save Changes" in the Avatar section.

HOW TO SIGN OUT

Step 1: Navigate to /settings/account (or click your name/email link in the sidebar).
Step 2: Scroll to the "Account Actions" section.
Step 3: Click "Sign Out". You are immediately logged out and redirected to the Login page.

NOTES

- Changes to your name are reflected across the entire OSCRAT application immediately after saving.
- The "Save Changes" button is only enabled when you have actually modified a field's value.
- Your email address is used as your login identifier. It is displayed in Account Settings for reference but cannot be edited from this page.

CHANGE EMAIL & CHANGE PASSWORD

URL: /settings/account

OVERVIEW

The Account Settings page lets you change the email address and password used to sign in to OSCRAT. Both actions live in their own section on the page, below the "Name" section, and both require you to confirm your current password before the change is accepted.

- Changing your email address does not take effect immediately: OSCRAT sends a confirmation link to the NEW address, and the change only completes once that link is clicked. Your login email stays the same until then.
- Changing your password takes effect immediately once submitted successfully.

PAGE ELEMENTS

1. EMAIL ADDRESS SECTION

- Heading: "Email Address"
- Description: "The email address you use to sign in to your account."

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.

a. EMAIL ADDRESS INPUT
- Label: "Email Address"
- Placeholder: "Your email"
- Pre-filled with your current login email address.
- Editable. Enter the new email address you want to sign in with.
- Shows an inline "Invalid email format" message if the value is not a valid email address.

b. CURRENT PASSWORD INPUT (Email section)
- Label: "Current Password"
- Placeholder: "Current Password"
- Masked (password) field.
- Required to confirm your identity before the email change is accepted.
- Shows an inline "Current password is required" message if left empty when you submit.

c. SAVE CHANGES BUTTON (Email section)
- Labeled "Save Changes".
- Disabled until the email field has been changed AND the current password field has a value.
- Click to request the email change.
- Shows a "Your current password is incorrect" error if the password is wrong.
- On success, shows a confirmation banner: "We sent a confirmation link to <new email>. Click it to finish changing your email address." Your email is NOT changed yet at this point.

2. PASSWORD SECTION
- Heading: "Password"
- Description: "You can change your password here."

a. CURRENT PASSWORD INPUT (Password section)
  - Label: "Current Password"
  - Masked (password) field.
  - Required. Must match your existing password.

b. NEW PASSWORD INPUT
  - Label: "New Password"
  - Masked (password) field.
  - There is no "confirm new password" field.
  - Must meet the password strength rules to enable
  - the button (see NOTES below).

c. CHANGE PASSWORD BUTTON
  - Labeled "Change Password".
  - Disabled until the Current Password field has a value AND the New Password field meets the strength 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.

- Click to submit the password change.
- Shows a "Your current password is incorrect" error if the current password is wrong.
- On success, shows a "Changes saved successfully." confirmation and both fields are cleared. Your password is changed immediately — you continue using your current session, but you must use the new password on your next sign-in.

HOW TO CHANGE YOUR EMAIL ADDRESS

Step 1: Navigate to /settings/account (click your name/email link in the sidebar).

Step 2: In the "Email Address" section, replace the "Email Address" field with your new email.

Step 3: Enter your current account password in the "Current Password" field of that same section.

Step 4: Click "Save Changes".

Step 5: A banner confirms a confirmation link was sent to the new email address. Open that email and click the link to finish the change. Until you do, you keep signing in with your old email.

HOW TO CHANGE YOUR PASSWORD

Step 1: Navigate to /settings/account.

Step 2: In the "Password" section, enter your existing password in the "Current Password" field.

Step 3: Enter your new password in the "New Password" field. It must meet the strength requirements (see NOTES below) for the button to enable.

Step 4: Click "Change Password". A "Changes saved successfully." message confirmsthe update, and the fields are cleared. Use the new password the next time you sign in.

NOTES

- Both the email and password changes require you to re-enter your CURRENT password as a security check, even though you are already signed in.
- If you enter the wrong current password for either action, the page shows: "Your current password is incorrect."

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 email change is only a request until the emailed confirmation link is clicked — the address shown in the sidebar and the "Email Address" field will not update until then.
- A password change is immediate and does not require any email confirmation.

3. NAVIGATION

3.1 SIDEBAR NAVIGATION

LOCATION: Persistent sidebar, visible on all pages after logging in.

OVERVIEW

The sidebar is the primary navigation component of the OSCRAT application. It is visible on every page after you log in and provides quick access to all main sections of the platform for the currently selected organization.

The sidebar also contains an organization switcher at the top, allowing you to move between different organizations without returning to the Organizations page (/organization).

SIDEBAR ELEMENTS

1. ORGANIZATION DROPDOWN TOGGLE

- Located at the very top of the sidebar, above the navigation links.
- Displays the name of the currently active organization.
- Click it to open the organization dropdown menu.
- DROPDOWN MENU ITEMS (shown after clicking the toggle):
  a. All Organizations link — navigates to /organization (full list).
  b. New Organization link — shortcut to create a new organization.
  c. Existing organization entries — each organization you belong to appears as a clickable link.

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.

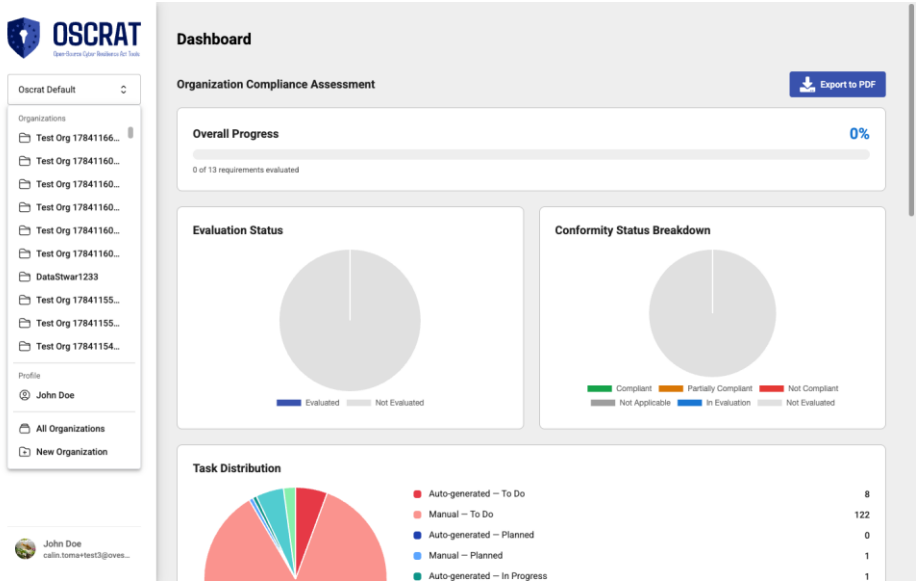

Figure 6: Sidebar — organization dropdown menu open

2. DASHBOARD LINK

- Navigates to the current organization's Dashboard page (/organization/{slug}/dashboard).

3. PRODUCTS LINK

- Navigates to the Products list page (/organization/{slug}/products).

4. TASKS LINK

- Navigates to the Organization Tasks page (/organization/{slug}/tasks).

5. DOCUMENTATION LINK

- Navigates to the organization's Documentation section (/organization/{slug}/documentation).

6. SETTINGS LINK

- Navigates to the organization's Settings page (/organization/{slug}/settings).

7. COMPLIANCE LINK

- Navigates to the Organization Compliance Assessment page (/organization/{slug}/compliance).

8. USER ACCOUNT LINK

- Located at the bottom of the sidebar.
- Displays your account name and email.
- Click it to access account settings (/settings/account).

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.

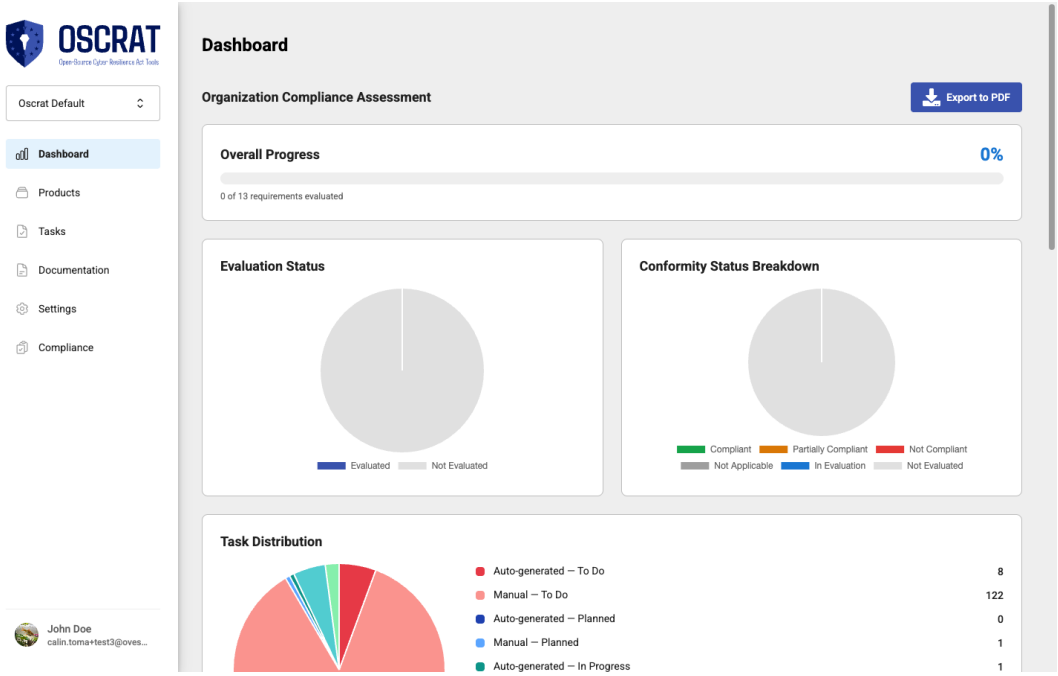

Figure 7: Sidebar Navigation

HOW TO SWITCH ORGANIZATIONS

Step 1: Click the Organization Dropdown Toggle at the top of the sidebar (shows the current org name).
Step 2: A dropdown menu appears with "All Organizations", "New Organization", and your existing organizations by name.
Step 3: Click the organization you want to switch to. The sidebar and all page content updates to reflect the selected organization's context.

NOTES

- The sidebar always reflects the context of the currently active organization.
- Links in the sidebar route to that organization's pages.
- To access a different organization's data, use the organization dropdown to switch context first.

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. ORGANIZATIONS

4.1 ORGANIZATIONS PAGE

URL: /organization

OVERVIEW

The Organizations page is the main landing page after logging in. It lists all organizations you belong to and allows you to create new organizations.

An organization in OSCRAT represents a company, team, or entity whose CRA compliance is being managed. Each organization has its own products, tasks, and compliance assessment.

PAGE ELEMENTS

1. PAGE HEADING

- Title: "All Organizations"
- Subtitle: "Your organizations are listed here."

2. CREATE ORGANIZATION BUTTON

- Clicking this opens the Create Organization modal.

3. ORGANIZATIONS TABLE — columns:

a. NAME — the display name (clicking it navigates to the organization's dashboard)
b. MEMBERS — number of users in the organization
c. CREATED AT — the date the organization was created
d. ACTIONS — row-level action buttons. For organizations where you are a member but not the owner, this shows a "Leave Organization" button. Owner-level actions (e.g., delete) may differ.

4. PAGINATION

- Previous page / Next page buttons with item count (e.g., "1-15 of 28 items").

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.

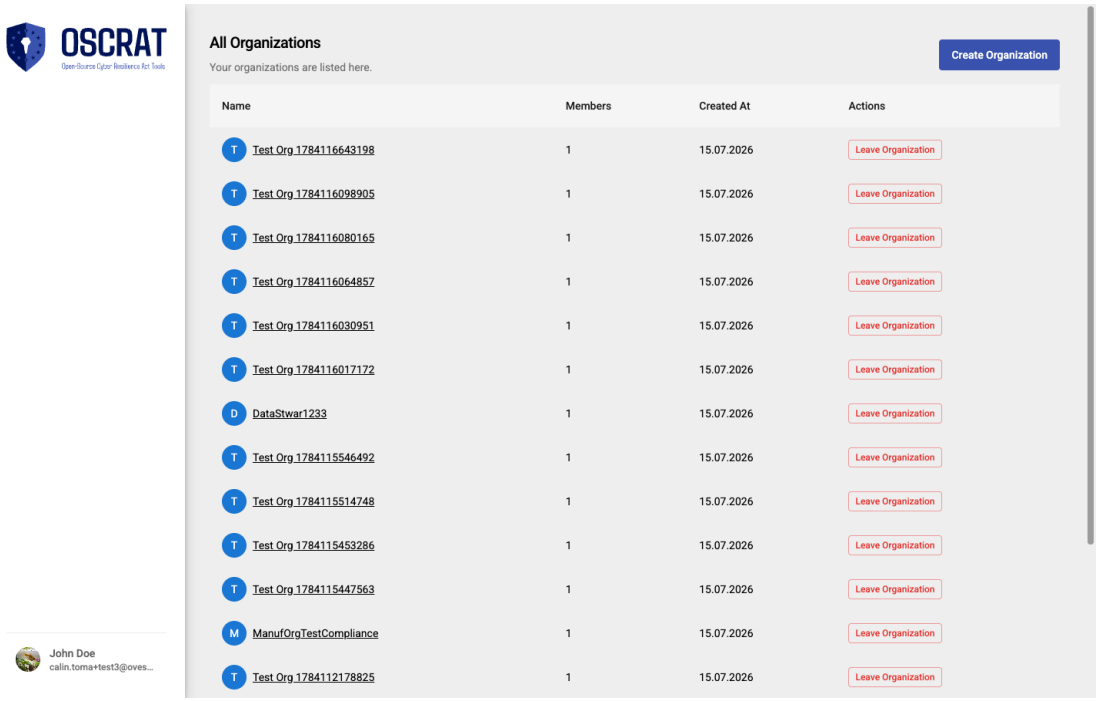

Figure 8: Organizations page

LEAVE ORGANIZATION

Clicking "Leave Organization" in a row opens a confirmation dialog:

- Heading: "Leave Organization [Organization Name]"
- Warning: "Are you sure you want to leave the organization? You'll lose access to all resources and data associated with the organization."
- LEAVE ORGANIZATION button — confirms the action.
- CANCEL button — closes without leaving.

CREATE ORGANIZATION MODAL

Clicking "Create Organization" opens a modal titled "Organization Information" with the following fields:

1. CLOSE BUTTON — closes the modal without saving.

2. PERSON TYPE (Radio Buttons) — Mandatory
   - "Natural Person" — for individual users or sole proprietors.
   - "Legal Person" — for registered companies or legal entities.
   - Selecting "Legal Person" reveals additional fields (Tax ID and Organization Size).

3. ORGANIZATION ROLE DROPDOWN — CRA context role (e.g., manufacturer, importer, distributor). Required. — Mandatory

4. ORGANIZATION NAME INPUT — Placeholder: "Enter organization 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.

Required. — Mandatory and unique

5. POSTAL ADDRESS INPUT — Official postal address. Required. — Mandatory
6. CONTACT EMAIL INPUT — Primary contact email. Required. — Mandatory
7. PHONE PREFIX DROPDOWN — Country code for the phone number. — Optional
8. CONTACT PHONE INPUT — Placeholder: "123-4567-8901". — Optional
9. ADDITIONAL INFORMATION INPUT — Optional free-text notes. — Optional
10. TAX ID INPUT (Legal Person only) — Label: "Tax ID (Optional)". — Optional
11. ORGANIZATION SIZE DROPDOWN (Legal Person only) — micro, small, medium, large enterprise. — Optional
12. CANCEL BUTTON — closes without creating.
13. CREATE ORGANIZATION BUTTON (modal) — submits and creates the organization. The modal closes and the new organization appears in the table on success.

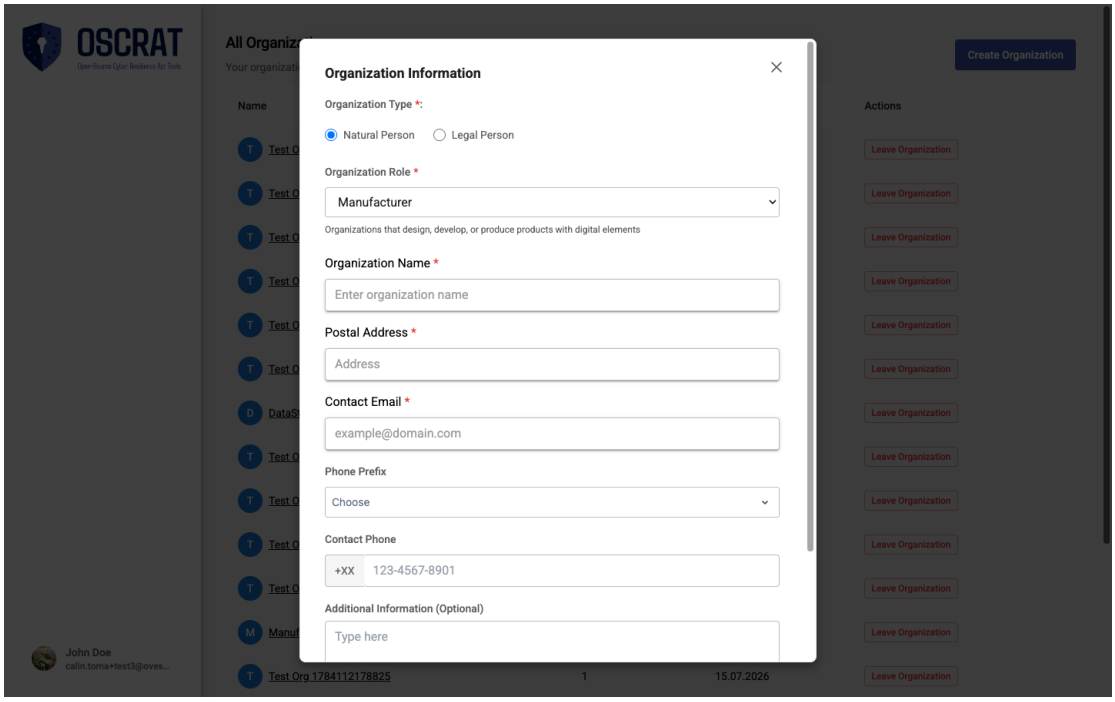

Figure 9: Create Organization modal

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.

HOW TO CREATE AN ORGANIZATION — STEP BY STEP

Step 1: Navigate to /organization.
Step 2: Click "Create Organization".
Step 3: Select "Natural Person" or "Legal Person".
Step 4: Choose the Organization Role.
Step 5: Enter the Organization Name.
Step 6: Enter the Postal Address.
Step 7: Enter the Contact Email.
Step 8: (Optional) Select phone country prefix and enter phone number.
Step 9: (Optional) Enter Additional Information.
Step 10: If "Legal Person": optionally enter Tax ID, select Organization Size.
Step 11: Click "Create Organization".
Step 12: The modal closes and the new organization appears in the table.

NOTES

- Organization names should be unique and clearly identify the entity.
- After creating an organization, you can invite other users from the organization's Settings page.
- The "Leave Organization" action is irreversible — you will lose access to all resources in that organization.

4.2 ORGANIZATION DASHBOARD PAGE

URL: /organization/{organization-slug}/dashboard

OVERVIEW

The Organization Dashboard page provides a high-level overview of your organization's CRA compliance posture. It aggregates data across all products and versions managed within the organization into summary charts, statistics, and a recent activity feed.

This page is the first screen you see after navigating into a specific organization.

PAGE ELEMENTS

1. PAGE HEADING

- Title: "Dashboard"
- Confirms you are viewing the organization's top-level dashboard.

a. COMPLETED APPLICABILITY CHECK CARD

- Appears above the Organization Compliance Assessment card only when cached results exist from a completed CRA Applicability Check (§1.4) that have not yet been converted into a product.
- CARD HEADING — "Completed Applicability Check"

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.

- DESCRIPTION TEXT — reads: "Use the results of the completed applicability check to add an [CATEGORY] Product", where [CATEGORY] is the CRA product category determined by the check (e.g., "IMPORTANT CLASS I"), shown as an emphasized inline badge.
- ADD PRODUCT BUTTON — opens the Add Product wizard (§5.1) pre-selected to the "From cache (applicability check results)" option.
- Once the product is created from the cached results, this card no longer appears on later dashboard visits.

2. ORGANIZATION COMPLIANCE ASSESSMENT CARD

- Heading: "Organization Compliance Assessment"
- Summarizes the organization-level compliance assessment status (separate from product-level assessments).
- Contains a "Start Assessment" or "Continue Assessment" button that takes you to the organization's Compliance page (/organization/{slug}/compliance).

3. OVERALL PROGRESS SECTION

- Heading: "Overall Progress"
- Displays a percentage figure representing the share of CRA requirements that have been evaluated across your products.
- A description line shows the absolute count, e.g.: "12 of 50 requirements evaluated".

4. EVALUATION STATUS CHART

- Heading: "Evaluation Status"
- A pie chart showing the distribution of requirements by their evaluation state (evaluated vs. not yet evaluated).

5. CONFORMITY STATUS BREAKDOWN CHART

- Heading: "Conformity Status Breakdown"
- A pie chart showing the distribution of evaluated requirements across conformity statuses:
  - Compliant
  - Partially Compliant
  - Not Compliant
  - Not Applicable
  - In Evaluation
  - Not Evaluated

6. TASK DISTRIBUTION CHART

- Heading: "Task Distribution"
- A pie chart showing the breakdown of tasks by origin and status.
- Legend categories (origin × status):
  - Auto-generated — To Do
  - Manual — To Do
  - Auto-generated — Planned

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.

    - Manual — Planned
    - Auto-generated — In Progress
    - Manual — In Progress
    - Auto-generated — Done
    - Manual — Done
- Each legend item shows the count of tasks in that category.
- "Auto-generated" tasks are created automatically by the system (e.g., from compliance assessments or scans). "Manual" tasks are created directly by users.
- This chart also appears inside the Compliance tab on each Version Detail page, scoped to that version's tasks.

7. REQUIREMENTS STATUS TABLE

- Heading: "Requirements Status Table"
- A table listing individual CRA requirements with the following columns:
    a. Requirement ID — e.g., "TD-1", "IO1"
    b. Security Requirement — the requirement text
    c. Area — the compliance area the requirement belongs to
    d. Evaluation Status — whether the requirement has been evaluated
    e. Conformity Status — the compliance verdict for that requirement

8. RECENT ACTIVITIES TABLE

- Heading: "Recent Activities"
- A table logging recent actions taken within the organization, with the following columns:
    a. Date — when the action occurred (DD.MM.YYYY)
    b. Product — the product affected
    c. Version — the product version affected
    d. User — who performed the action
    e. Action — a description of what was done
- This feed helps track progress and audit who made what changes and when.

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.

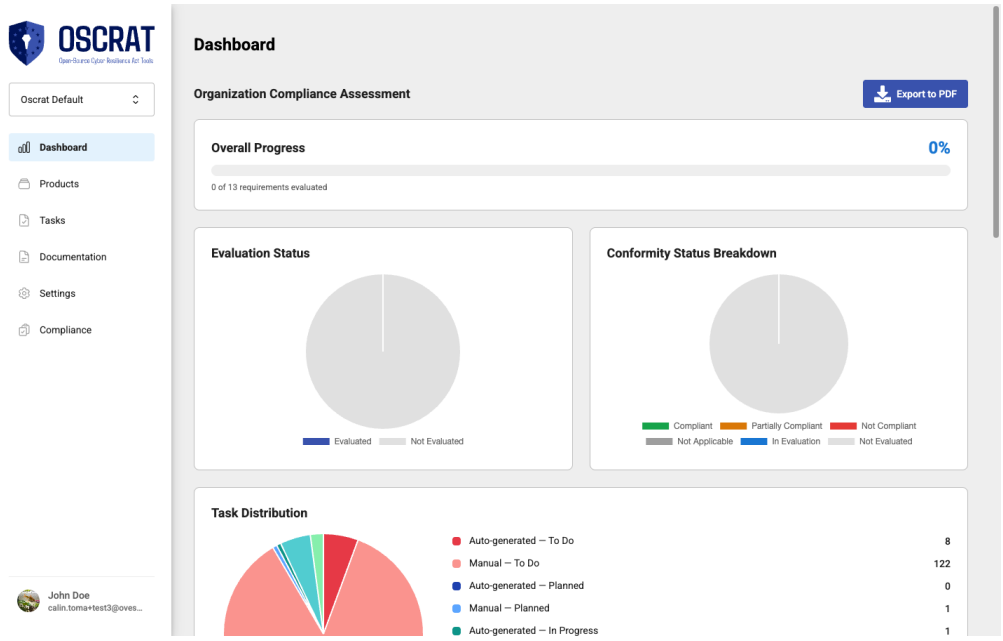

Figure 10: Organization Dashboard page

HOW TO USE THE DASHBOARD

Viewing Overall Compliance Progress:

1. Navigate to /organization/{your-org-slug}/dashboard.
2. Check the "Overall Progress" percentage for an immediate sense of how much CRA assessment work has been completed.
3. Read the description line to see exact counts.

Understanding the Charts:

1. The "Evaluation Status" pie chart shows what fraction of requirements have been assessed.
2. The "Conformity Status Breakdown" chart shows the compliance results for assessed requirements across six categories.
3. The "Task Distribution" chart shows how tasks are distributed across auto-generated vs. manual origin and their current statuses.

Starting or Continuing the Org-Level Assessment:

1. Locate the "Organization Compliance Assessment" card near the top.
2. Click "Start Assessment" or "Continue Assessment" to open the compliance assessment for the organization.

Reviewing Recent Activity:

1. Scroll down to the "Recent Activities" table.
2. Use Date, Product, Version, User, and Action columns to understand what was recently changed.

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.

NOTES

- The dashboard reflects real-time data from all products and versions in the organization.
- The Requirements Status Table aggregates data across all product versions — for version-level detail, navigate to the specific version's Compliance tab.
- The "Conformity Status" column in the Requirements Status Table and the Conformity Status Breakdown chart both use "Compliant" as the displayed label.

4.3 ORGANIZATION SETTINGS PAGE

URL: /organization/{organization-slug}/settings

Related tabs

Members: /organization/{organization-slug}/members
Audit Logs: /organization/{organization-slug}/audit-logs

OVERVIEW

The Organization Settings page lets administrators manage an organization's name, slug, compliance assessment translations, and perform destructive actions such as removing the organization entirely. It is divided into three tabs: Settings, Members, and Audit Logs.

TAB NAVIGATION

1. Settings — org name, slug, translations, remove org
2. Members — manage members and invitations
3. Audit Logs — view a full log of all org actions

SETTINGS TAB (/organization/{slug}/settings)

1. ORGANIZATION SETTINGS SECTION

- Heading: "Organization Settings"

a. ORGANIZATION NAME INPUT — Mandatory
   - Edit and click "Save Changes" to rename the organization.

b. ORGANIZATION SLUG INPUT — Mandatory
   - The URL-safe identifier used in all organization URLs.
   - Changing the slug will change all URLs for this organization — update any saved bookmarks.

c. SAVE CHANGES BUTTON — click to save the updated name and/or slug.

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. COMPLIANCE ASSESSMENT TRANSLATIONS SECTION

- Heading: "Compliance Assessment Translations"
- Manage translations for compliance assessment questionnaires.
- Workflow: Download the default English template, translate it, and upload for your desired language.
- UPLOAD NEW TRANSLATION:
  a. ASSESSMENT TYPE DROPDOWN — options include: — Mandatory Manufacturer (Team), Distributor (Team), Importer (Team), SME Manufacturer (Team), Manufacturer (Version), Distributor (Version), Importer (Version), SME Manufacturer (Version). Authorized Representative (Team), Authorized Representative (Version). This indicates the "Authorized Representative" CRA role (alongside Manufacturer, Distributor, Importer, SME Manufacturer) is now supported for compliance assessments, at both team and version scope.

  b. LANGUAGE DROPDOWN — all 24 official EU languages supported. — Mandatory Languages currently not uploaded appear as "(Not available)" in the selector.

  c. DOWNLOAD ENGLISH TEMPLATE BUTTON — downloads a JSON file with the English assessment questions (keys + values). Translate the values (keep keys unchanged), then upload the translated file.

  d. UPLOAD TRANSLATION BUTTON — opens a file picker to upload the translated JSON file.
  EXISTING TRANSLATIONS TABLE — columns: Assessment Type, Language, Last Edited, Actions (download or delete).

3. REMOVE ORGANIZATION SECTION

- Warning: "Deleting the organization will delete all resources and data associated with the organization forever. This action cannot be undone."

  1. REMOVE ORGANIZATION BUTTON — opens a confirmation dialog. CONFIRMATION DIALOG:
     - DELETE BUTTON: confirms permanent deletion.
     - CANCEL BUTTON: closes without deleting.

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.

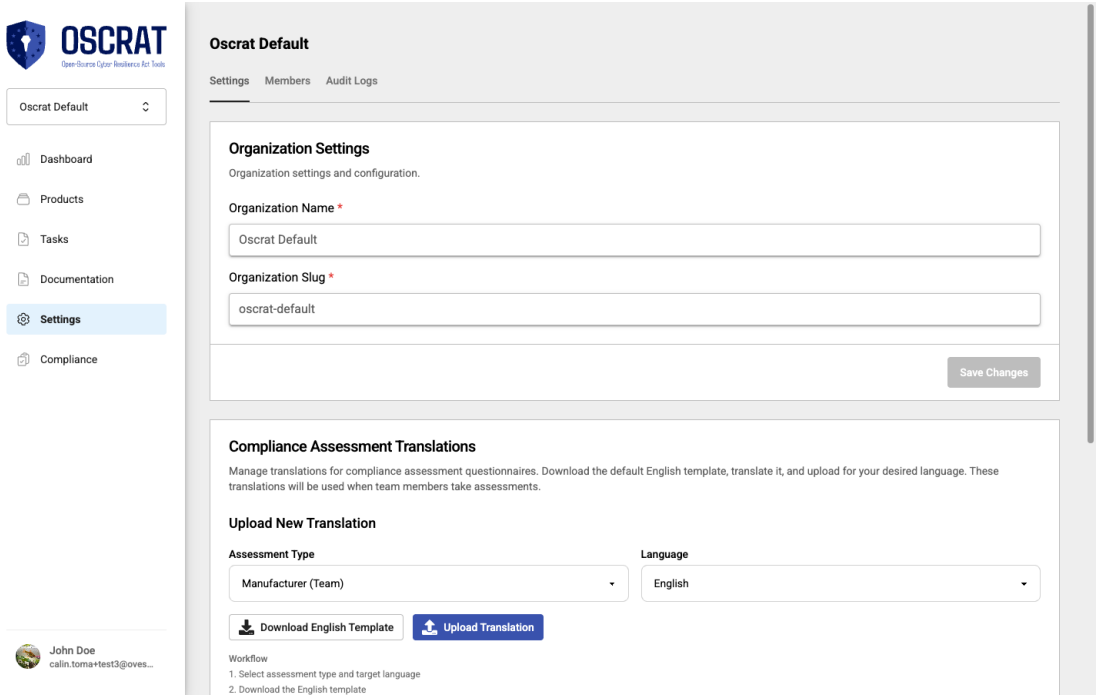

Figure 11: Organization Settings — Settings tab

<u>MEMBERS TAB</u> (/organization/{slug}/members)

1. **MEMBERS TABLE — columns: NAME, EMAIL, ROLE, ACTION (remove button).**

2. **ADD MEMBER BUTTON — opens the "Invite New Member" dialog.** INVITE NEW MEMBER DIALOG:
    - EMAIL INPUT — placeholder: "email@unicis.tech" — Mandatory
    - ROLE DROPDOWN — select the role to assign. — Mandator defaulting to "Member": Member, Admin, Owner, Auditor.
    - SEND INVITE BUTTON — sends the invitation email.

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.

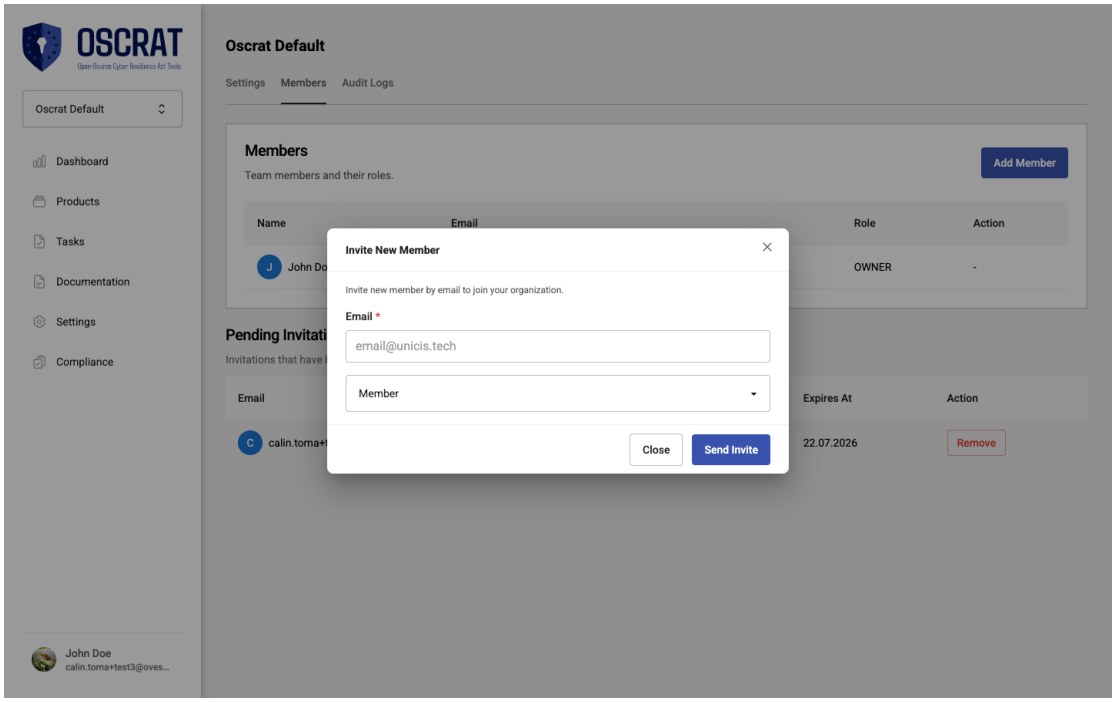

Figure 12: Invite New Member dialog

2.1 PENDING INVITATIONS TABLE

- Located directly below the Members table
  a. SECTION HEADING — "Pending Invitations"
  b. DESCRIPTION — "Invitations that have been sent to users but have not yet been accepted."
  c. TABLE — columns:
     - EMAIL — invited address, with a colored initial-letter avatar.
     - ROLE — the role to be assigned once accepted (e.g., "MEMBER").
     - EXPIRES AT — the date the invitation link stops working (DD.MM.YYYY).
     - ACTION — a "Remove" button that revokes the invitation. There is no "Resend" action.

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.

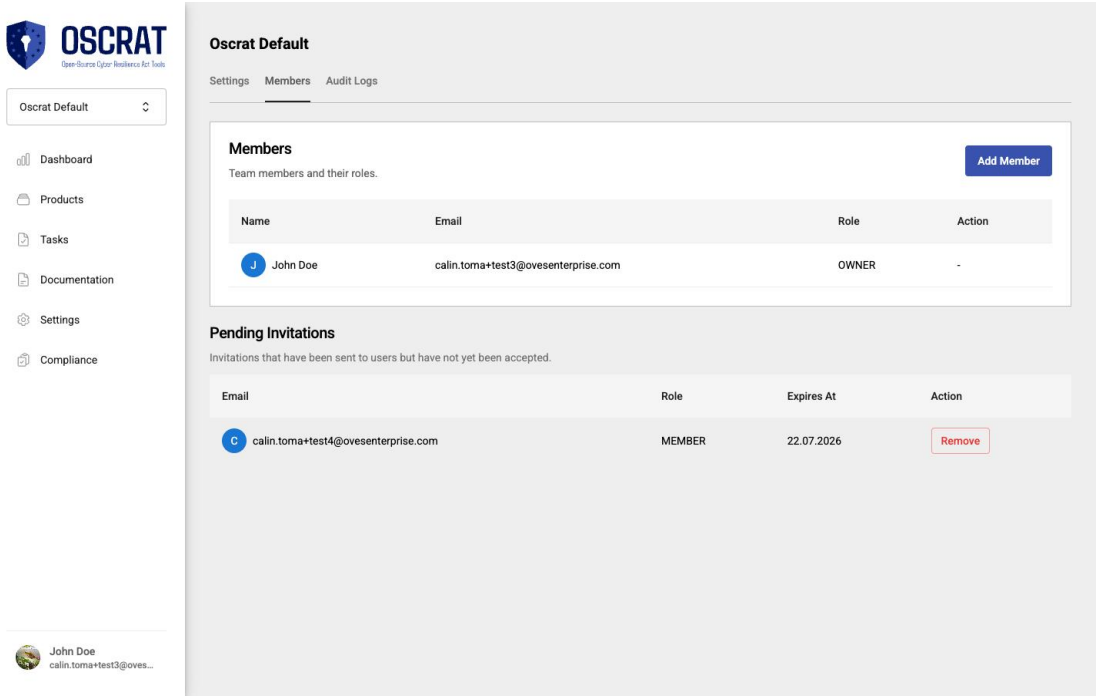

Figure 13: Pending Invitations table

2.2 THE INVITATION LINK & ACCEPTANCE FLOW

URL pattern: /invitations/{invitation-id} — this is the exact link sent in the invitation email; it cannot be regenerated from the UI.

Opening it with NO active OSCRAT session shows a dedicated, minimal landing page (not the standard app chrome):

1. OSCRAT LOGO, centered.
2. HEADING — "{Organization Name} is inviting you to join their organization." (page <title>: "You've been invited to join {Organization Name}").
3. SUBHEADING — "To continue, you must either create a new account or login to an existing account."
4. CREATE A NEW ACCOUNT BUTTON.
5. LOGIN USING AN EXISTING ACCOUNT BUTTON.

"CREATE A NEW ACCOUNT" → navigates to /auth/join?token={invitation-id}, a token-aware variant of the Account Creation page (§1.3):

- Heading "Get started" / "Create a new account".
- First Name / Last Name — empty, as standard.
- Email — pre-filled with the invited address and DISABLED (read-only); the standard join page's Email field is normally editable.
- Password / Confirm Password — empty, as standard.
- Cancel / Create Account (disabled until required fields filled).

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.

- "Already have an account? Sign in" link also carries the token forward to /auth/login?token={invitation-id}. account-level behavior, not specific to one invitation or org. /auth/login?token={invitation-id}, a token-aware variant of the Login page (§1.1) — visually and structurally identical (Email, Password, Forgot your password?, Sign in, Applicability Check, legal text, "Don't have an account? Create a free account" — that link also carries the token forward). The invitation token travels silently in the URL.

3. CONFIRM DELETE MEMBER DIALOG

- Warning: "Deleting a member will delete all activities related to that member. This action cannot be undone."
- DELETE BUTTON / CANCEL BUTTON.

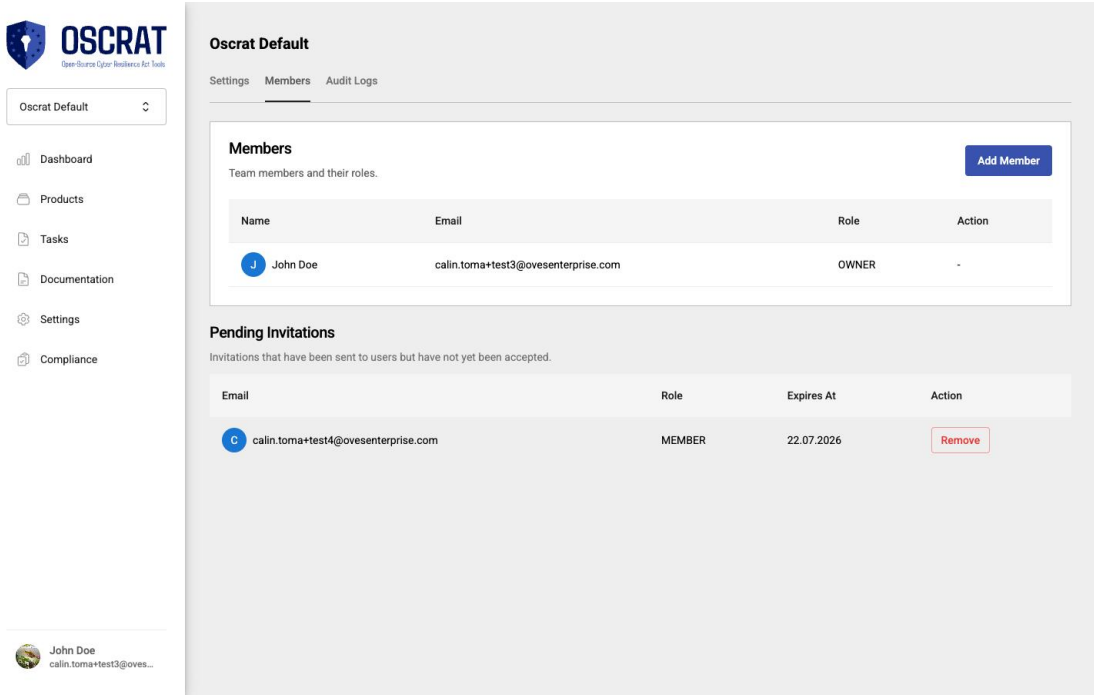

Figure 14: Organization Settings — Members tab

AUDIT LOGS TAB (/organization/{slug}/audit-logs)

1. HEADING: "Audit Logs"

2. FILTERS:

a. All users dropdown — filter by actor — Optional
b. All entities dropdown — filter by entity type (Product, Assessment, Task, Vulnerability, etc.) — Optional
c. All operations dropdown — filter by action type (Create, Delete, Update, etc.) — Optional
d. From date picker — start date for range filter — 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.

e. To date picker — end date for range filter — Optional

3. **AUDIT LOG TABLE — columns: Timestamp, User, Action, Target, Details ("View Details" opens a modal with the full change record).**

4. **PAGINATION — Previous / Next buttons; item count displayed.**

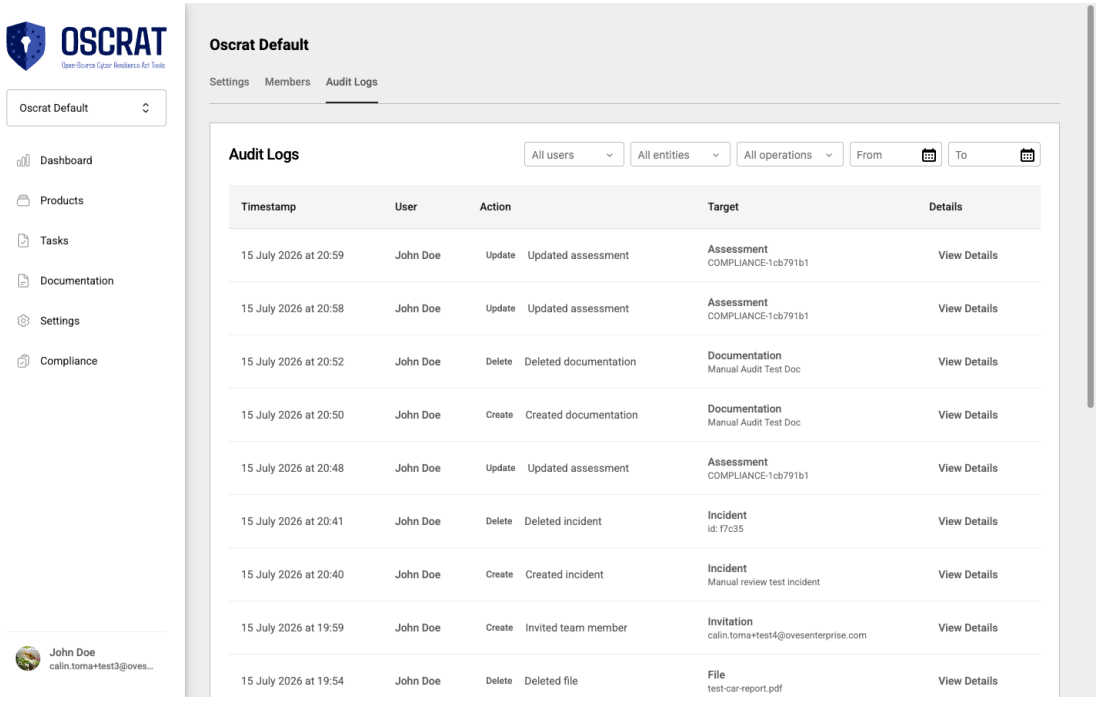

Figure 15: Organization Settings — Audit Logs tab

HOW TO RENAME THE ORGANIZATION

Step 1: Navigate to /organization/{slug}/settings.
Step 2: Update "Organization Name" and/or "Organization Slug".
Step 3: Click "Save Changes".

HOW TO ADD A COMPLIANCE TRANSLATION

Step 1: Go to /organization/{slug}/settings.
Step 2: In "Compliance Assessment Translations", select Assessment Type and Language.
Step 3: Click "Download English Template" and translate the JSON values (do not change the keys).
Step 4: Click "Upload Translation" and select your translated JSON file.

HOW TO INVITE A NEW MEMBER

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.

Step 1: Go to /organization/{slug}/members.
Step 2: Click "Add Member".
Step 3: Enter the invitee's email address.
Step 4: Select their role.
Step 5: Click "Send Invite". The invitee receives an email invitation. The invite now appears in the "Pending Invitations" table (item 2A above) with its expiry date.

HOW TO ACCEPT AN INVITATION

Step 1: The invitee opens the emailed link (/invitations/{invitation-id}) in a browser with no other OSCRAT session active, and sees the "You've been invited..." landing page.
Step 2

a. If they have no account, they click "Create a new account", fill in their name and a password (email is locked to the invited address), and click "Create Account". They must then confirm their email address via a link sent to their inbox before they can log in.
b. If they already have an OSCRAT account under that email, they click "Login using an existing account" and sign in normally.

Step 3: Once accepted, the invitee should be removed from "Pending Invitations" and appear as a row in the Members table with the assigned role.

NOTES

- Changing the organization slug updates all URLs. Any existing bookmarks or shared links will break.
- Removing an organization is permanent and cannot be undone. All products, versions, compliance data, tasks, and documentation are deleted forever.
- Only organization owners can remove the organization or change the slug.
- Audit log entries cannot be deleted. They provide a permanent, tamper-evident record of all actions.

5. PRODUCTS

5.1 PRODUCTS PAGE

URL: /organization/{organization-slug}/products

OVERVIEW

The Products page lists all products registered under your organization. Each product represents a hardware or software item subject to CRA assessment. From this page you can search, filter, and browse products, as well as add new ones.

PAGE ELEMENTS

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. **PAGE HEADING**
- Title: "Products List"
- Description: "Add a new product, verify if it falls within the scope of the Cyber Resilience Act, or manage existing ones."

2. **SEARCH INPUT — Optional**
- Placeholder: "Search by title"
- Type a product name or keyword to filter the list in real time.

3. **FILTER BUTTON**
- An icon-only button next to the search box that opens the Filters panel. Click to reveal category, role, status, and external-reporting filters.

4. **ADD PRODUCT BUTTON**
- Labeled "Add Product".
- Opens the multi-step Add Product wizard.

5. **PRODUCT CARDS**
- Each registered product appears as a card. Each card shows:
  a. PRODUCT NAME (heading) — displayed prominently at the top of the card.
  b. PRODUCT ACRONYM — a short identifier displayed next to the product name (e.g., "TST").
  c. STATUS BADGE — shows the current product status (e.g., "Active") with an icon.
  d. DETAILED DATA FIELDS — always visible on the card (not collapsed or hidden by default):
     - Category — the CRA product category (e.g., "Critical", "Important Class I")
     - Product Type — the type of product (e.g., "Application Software")
     - Open Incidents — count of open security incidents (e.g., "17 Open" or "None")
     - Open Vulnerabilities — count of open vulnerabilities (e.g., "40 Open" or "None")
     - External Reporting — whether external reporting is required (e.g., "N/A")
     - Status — the CRA evaluation status (e.g., "Not evaluated")
     A "Show More" button is also present on every card, but it does NOT expand or collapse anything — all detail fields above are already visible by default. Clicking "Show More" instead navigates directly to the Product Detail page for that product; it is a second, redundant way to trigger the same navigation as item e below ("Click anywhere on the card body").
  e. CLICK TO NAVIGATE — clicking anywhere on the card body (or the "Show More" button) navigates to the Product Detail page for that 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.

6. NO PRODUCTS MESSAGE

- Text: "No products found"
- Shown when the list is empty (either no products exist yet or no products match the active filters).

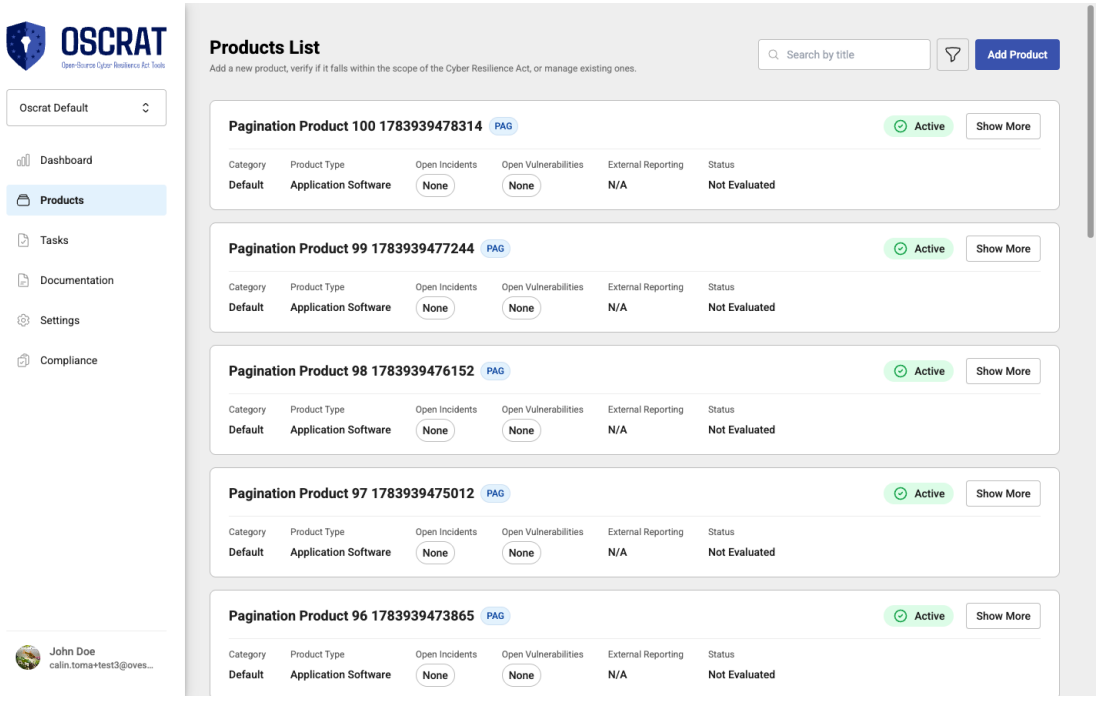

Figure 16: Organization Settings — Audit Logs tab

FILTERS PANEL

Click the filter icon button to open the Filters panel on the right side of the page. It contains:

1. FILTERS HEADING — Title: "Filters"
2. CLOSE FILTERS BUTTON — Labeled "Close filters". Closes the panel without resetting filters.
3. CATEGORY DROPDOWN — Filter products by CRA product category. — Optional
4. ROLE DROPDOWN — Filter products by your organization's role (e.g., manufacturer, importer, distributor). — Optional
5. STATUS DROPDOWN — Filter products by their current status (e.g., active, archived). — Optional
6. EXTERNAL REPORTING DROPDOWN — Filter by whether external reporting is required for the product. — 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.

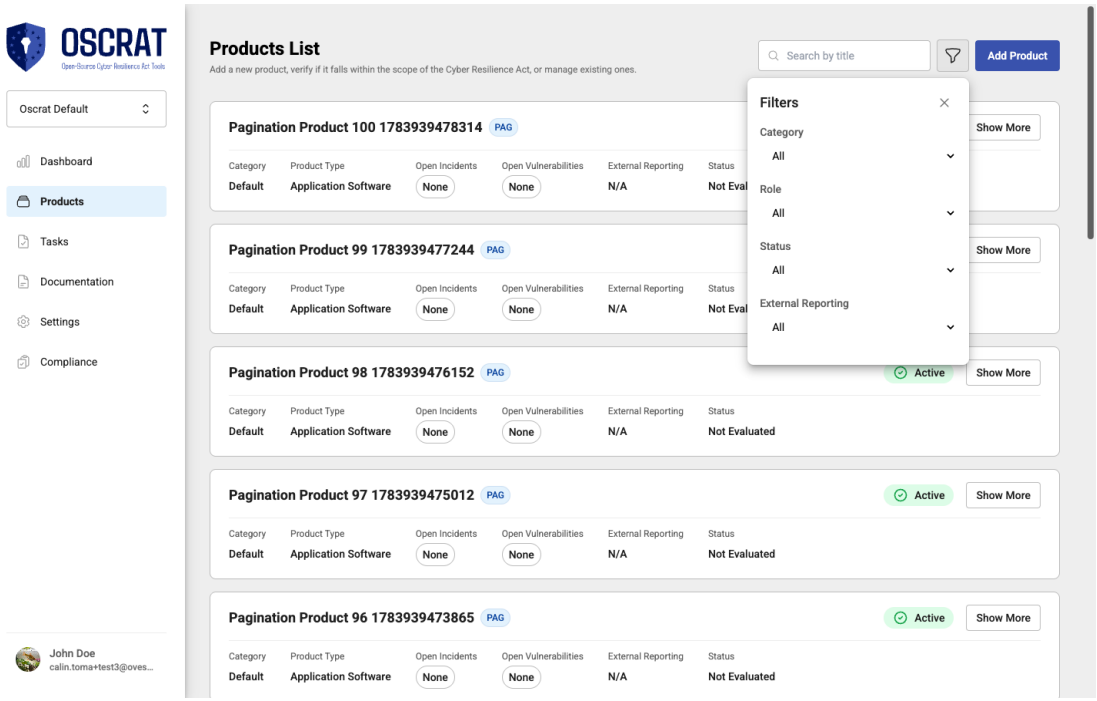

Figure 17: Products page — Filters panel

ADD PRODUCT WIZARD — STEP 1

Clicking "Add Product" starts a two-step wizard.
Step 1 asks: "How would you like to add the new product?"

1. **FROM SCRATCH (Radio button) — Mandatory**
   - Start a brand-new product entry with no pre-filled data.

2. **FROM CACHE (Radio button) — Mandatory**
   - Label: "From cache (applicability check results)"
   - Pre-fills the product form with data saved from a previous CRA
   - Applicability Check (/form).

3. **FROM EXISTING PRODUCT (Radio button) — Mandatory**
   - Copy configuration from an existing product in your organization.

4. **CLOSE BUTTON — Closes the wizard without creating a product.**

5. **NEXT BUTTON — Advances to Step 2. Enabled after an option is selected.**

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.

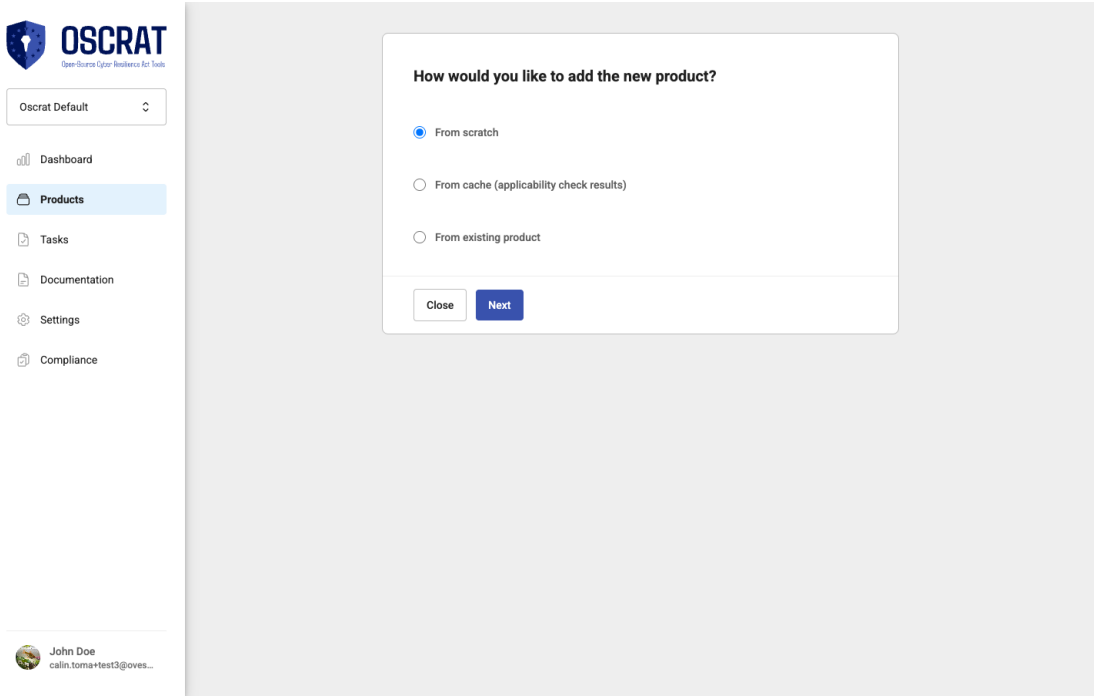

Figure 18: Add Product wizard — Step 1

ADD PRODUCT WIZARD — STEP 2

Heading: "Provide some initial information about your product"

1. RETAKE SURVEY BUTTON (cache mode only) — Returns to /form.
2. PRODUCT ACRONYM INPUT — Label: "Product Acronym *" | Required. — Mandatory
3. PRODUCT NAME INPUT — Label: "Product Name *" | Required. — Mandatory
4. PRODUCT VERSION INPUT — Label: "Product Version *" | Required. — Mandatory
5. PRODUCT DESCRIPTION INPUT — Optional. — Optional
6. BACK BUTTON — Returns to Step 1.
7. CREATE BUTTON — Submits and creates the product. Navigates to the new product's detail page on success.

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.

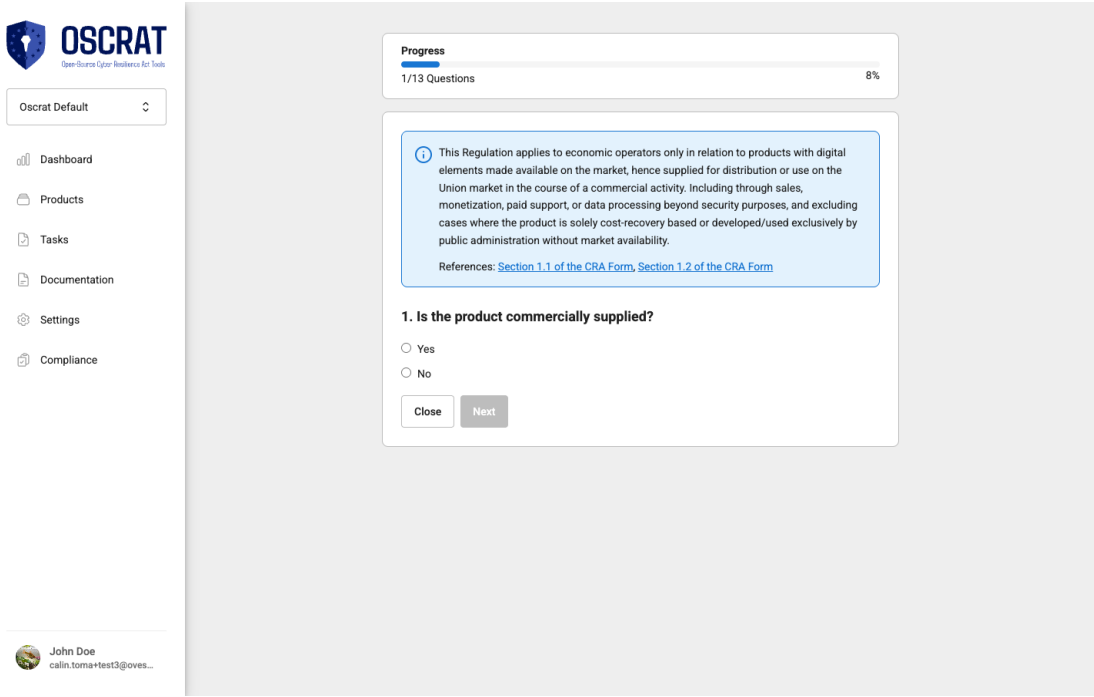

Figure 19: Add Product wizard — Step 2

HOW TO ADD A PRODUCT — STEP BY STEP

Step 1: Navigate to /organization/{org-slug}/products.
Step 2: Click "Add Product".
Step 3: Select how you want to add the product (from scratch, from cache, or from existing products).
Step 4: Click "Next".
Step 5: Fill in the Product Acronym, Product Name, and Product Version (all required).
Step 6: Optionally add a description.
Step 7: Click "Create". You are redirected to the new product's Detail page.

NOTES

- Product acronyms should be short and unique within the organization (e.g., "CRM", "PORTAL-V2").
- The initial version entered here creates the first version record.
- Additional versions can be added later from the Product Detail page.
- Use filters to quickly locate products in large lists.

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 PRODUCT DETAIL PAGE

URL: /organization/{organization-slug}/products/{product-id}

OVERVIEW

The Product Detail page shows all information for a specific product.
From here you can manage the product's metadata, view and edit its CRA applicability survey results, and manage its versions.

PAGE ELEMENTS

1. **BREADCRUMB NAVIGATION**
   - Shows: Organization > Products > Product Name.

2. **EDIT BUTTON — opens an edit form to update product metadata.**

3. **DELETE BUTTON**
   - Permanently deletes the product and all its versions.
   - A confirmation prompt appears. This action cannot be undone.

   3.1 PRODUCT STATS GRID & DESCRIPTION
   - Directly below the header (Edit/Delete buttons) and a separator, the page shows a six-field stats grid, then a second separator, then a Description section. Neither is a modal or dialog — both are always visible on the page.
   - PRODUCT STATS GRID — six labeled fields:
     a. CATEGORY — the CRA product category (e.g., "Default").
     b. PRODUCT TYPE — e.g., "Application Software".
     c. OPEN INCIDENTS — status badge with the product's total open incident count (aggregated across all versions), e.g., "101 Open".
     d. OPEN VULNERABILITIES — status badge with the product's total open vulnerability count (aggregated across all versions), e.g., "5 Open".
     e. EXTERNAL REPORTING — whether external reporting is required (e.g., "N/A").
     f. ASSESSMENT TYPE — the compliance assessment type assigned to the product (e.g., "N/A" if none assigned).

   - DESCRIPTION SECTION
     - Heading: "Description"
     - Paragraph: the product's free-text description, as entered
     - when the product was created or last edited.

4. **APPLICABILITY SURVEY SECTION**
   - Heading: "Applicability Survey"

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.

a. VIEW BUTTON — opens a read-only summary of the applicability survey.
b. EDIT / RETAKE BUTTON — modify or fully retake the CRA applicability check for this product.

5. **VERSIONS TABS**
   a. ACTIVE/SUPPORTED TAB — lists currently active or supported versions (default tab).
   b. NOT SUPPORTED TAB — lists withdrawn or end-of-life versions.

6. **ADD VERSION BUTTON — navigates to the Add New Product Version page.**

7. **VERSION LIST — each version is a row/card. Clicking it opens the Version Detail page. Each version row also displays inline summary stats, without requiring a click into the Version Detail page:**
   - VERSION LABEL — e.g., "Version - repo1783945026720" or the semantic version identifier.
   - STATUS FIELD — e.g., "Active".
   - INCIDENTS FIELD — status badge, e.g., "None" or "N Open".
   - VULNERABILITIES FIELD — status badge, e.g., "None" or "N Open".
   - TASKS FIELD — status badge, e.g., "None" or "N Open".
   - SHOW MORE BUTTON — labeled "Show More", present on every

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.

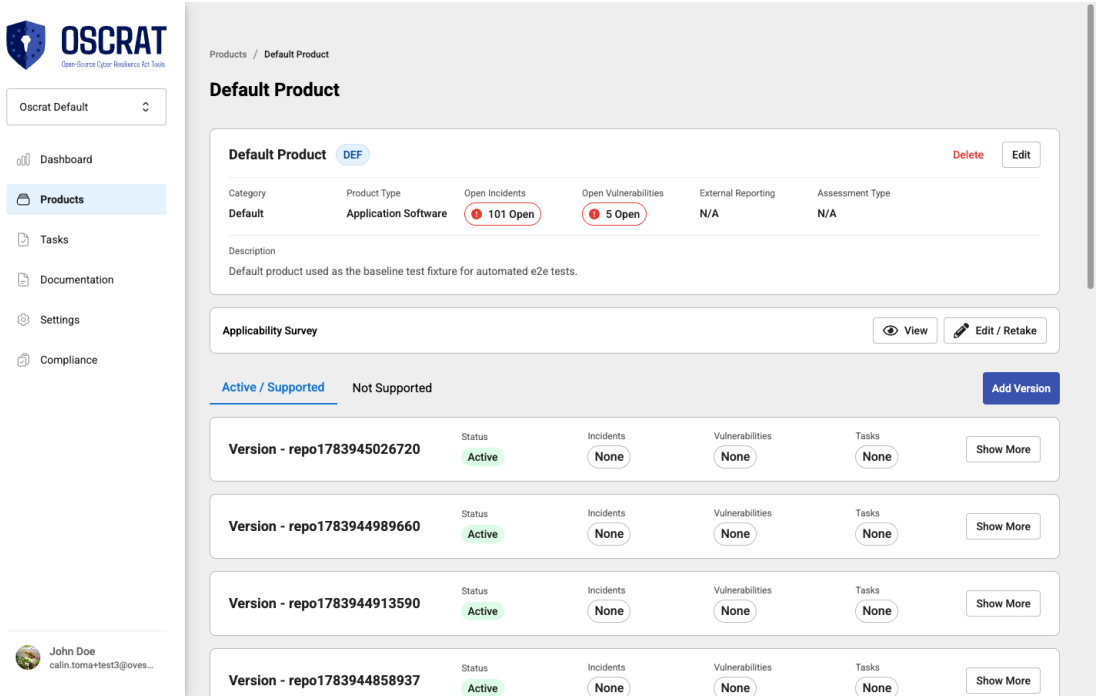

Figure 20: Product Detail page

HOW TO MANAGE A PRODUCT

Editing Product Details:
1. Click "Edit". 2. Update the desired fields. 3. Save.

Viewing Applicability Survey Results:
Click "View" in the "Applicability Survey" section.

Retaking the Applicability Survey:
Click "Edit / Retake" to restart or modify the CRA questionnaire.

Adding a New Version:
1. Click "Add Version". 2. Fill in version details. 3. Click "Create Version" to save.

Deleting a Product:
1. Click "Delete". 2. Confirm the deletion. The product and all its versions are permanently removed.

NOTES

- Deleting a product is irreversible. All associated versions, compliance data, tasks, and files are permanently deleted.
- The "Not Supported" tab shows versions marked as withdrawn. You can withdraw a version from the Version Detail page using the "Withdraw" 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.

5.3 ADD NEW PRODUCT VERSION PAGE

URL: /organization/{org-slug}/products/{product-id}/versions/new

OVERVIEW

The Add New Product Version page allows you to register a new version for an existing product. Each version receives its own compliance assessment, file attachments, SBOM, vulnerability scans, and tasks.

PAGE ELEMENTS

1. PAGE HEADING — Title: "Add New Product Version"

2. PRODUCT ACRONYM INPUT (read-only) — pre-filled with the parent product's acronym.

3. PRODUCT NAME INPUT (read-only) — pre-filled with the parent product's name.

4. NEW PRODUCT VERSION INPUT — Mandatory
   - Placeholder: "e.g., 1.2.4"
   - Enter the version identifier. Required.

5. VERSION SHORT DESCRIPTION INPUT — Optional Placeholder: "Type here" | Optional.

6. STATUS DROPDOWN — set the initial support status (Draft, Active, Not Supported, Archived, Withdrawn). Required. — Mandatory

7. BACK BUTTON — returns to the Product Detail page without creating the version.

8. CREATE VERSION BUTTON — submits and creates the new version. Navigates to the newly created version's Detail page on success.

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.

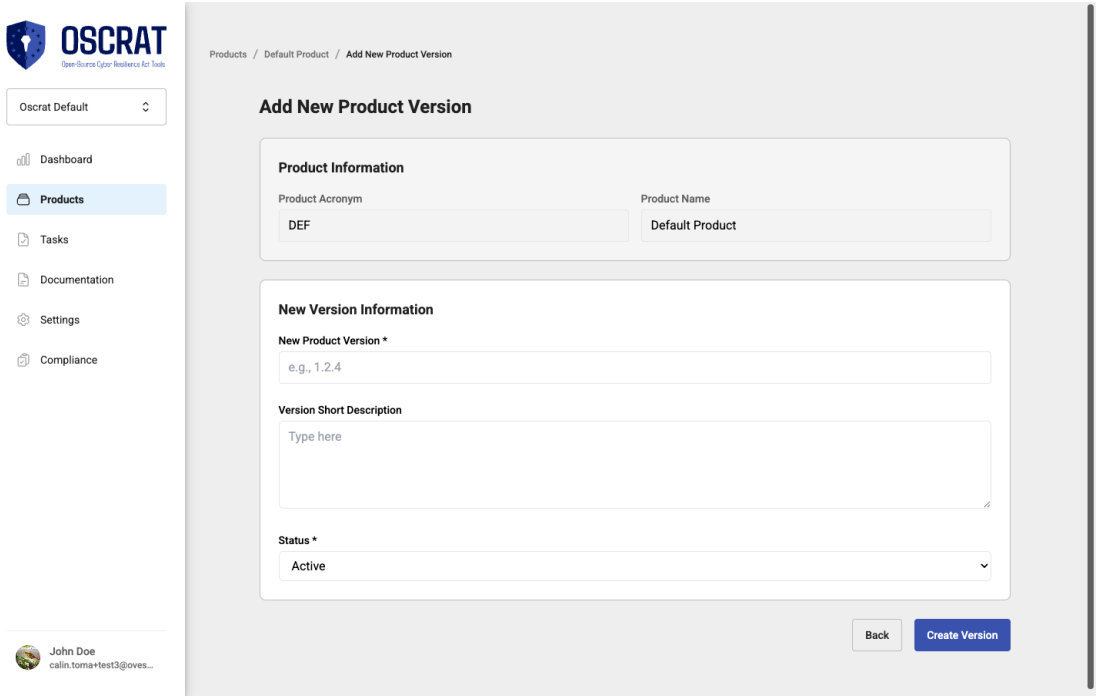

Figure 21: Add New Product Version page

HOW TO ADD A NEW VERSION — STEP BY STEP

Step 1: Navigate to the Product Detail page for the relevant product.
Step 2: Click "Add Version". The Add New Product Version page loads.
Step 3: Verify the Product Acronym and Product Name match the correct product.
Step 4: In "New Version", type the version identifier (e.g., "2.1.0").
Step 5: (Optional) Enter a Version Description.
Step 6: Select the appropriate Status.
Step 7: Click "Create Version". You are redirected to the new version's Detail page.

NOTES

- Version identifiers should be unique within a product.
- Semantic versioning (MAJOR.MINOR.PATCH, e.g. 2.1.0) is recommended.
- After creating a version, you can start its compliance assessment from
- the Compliance tab on the Version Detail 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.

6. VERSION DETAIL PAGE & TABS

6.1 VERSION DETAIL PAGE — OVERVIEW & HEADER

URL: /organization/{org-slug}/products/{product-id}/versions/{version-id}

OVERVIEW

The Version Detail page is the central hub for managing all compliance, security, and documentation data for a specific product version. It is organized into tabs, each covering a different aspect of the version's CRA compliance lifecycle.

HEADER ELEMENTS

1. BREADCRUMB NAVIGATION

- Shows the full path: Products > Product Name > Version.
- Click any segment to navigate back to that level.

2. VERSION TITLE

- Displays the version identifier prominently (e.g., "1.0.0").

3. ACTION BUTTONS (top right)

- DELETE BUTTON — permanently deletes this version and all its associated data. A confirmation prompt appears before deletion. This action cannot be undone.
- WITHDRAW BUTTON — marks the version as no longer supported / end-of-life. After withdrawal, the version moves to the "Not Supported" tab on the Product Detail page.
- EDIT BUTTON — opens an edit form to update the version's metadata (e.g., description, status, release date).

4. VERSION STATS BAR

- A row of six key metrics displayed below the version title:

a) STATUS

- Label: "Status:"
- Shows the current support status as a badge, e.g., "Supported".
- Possible values include: Draft, Active, Not Supported, Archived, Withdrawn

b) RELEASE DATE

- Label: "Release Date:"
- The version's official release date (DD.MM.YYYY), e.g., "29.04.2026".
- Shows "Not set" if no release date has been recorded.

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.

c) INCIDENTS

- Label: "Incidents:"
- Shows the count of open security incidents, e.g., "17 Open".

d) VULNERABILITIES

- Label: "Vulnerabilities:"
- Shows the count of open vulnerabilities, e.g., "40 Open".

e) TASKS

- Label: "Tasks:"
- Shows the count of open tasks, e.g., "25 Open".

f) SUPPORT PERIOD

- Label: "Support Period:"
- Shows the configured support end date or "Not set" if not yet
- configured.

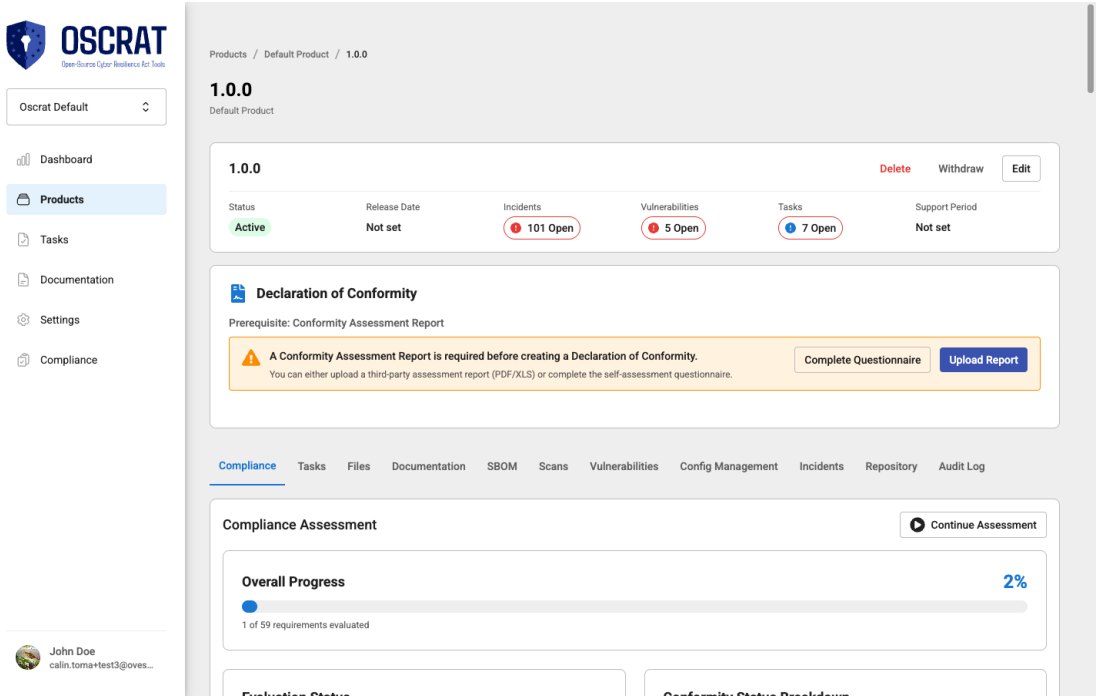

Figure 22: Version Detail page — header & stats bar

TABS OVERVIEW

The page is divided into 11 tabs. Click a tab heading to switch to that panel.

1. Compliance — CRA compliance assessment (see Part 7)
2. Tasks — version-specific tasks (section 6.9)
3. Files — file attachments (section 6.4)
4. Documentation — documentation files/links

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. SBOM — SBOM generation jobs (section 6.5)
6. Scans — vulnerability scan jobs (section 6.6)
7. Vulnerabilities — known vulnerabilities (section 6.7)
8. Config Management — OpenSCAP configuration scan jobs (section 6.10)
9. Incidents — security incidents (section 6.8)
10. Repository — linked source code repositories
11. Audit Log — chronological record of all changes (section 6.11)

REPOSITORY TAB — ADD REPOSITORY DIALOG

Clicking "Add New" in the Repository tab opens a dialog:

1. HEADING: "Add New Repository"
2. PROVIDER SELECT — e.g., GitHub, GitLab, Bitbucket. — Optional
3. REPOSITORY URL INPUT — full URL of the repository. — Mandatory
4. USER / ORG INPUT — Placeholder: "octocat" — Optional
5. REPOSITORY NAME INPUT — Placeholder: "my-repository" — Optional
6. AUTH TYPE SELECT — authentication method (public, token, etc.) — Mandatory
7. ADD BUTTON — saves and closes the dialog.
8. CANCEL BUTTON — closes without saving.

REPOSITORY TAB — LINKED REPOSITORY VIEW

The "Add New Repository" dialog above only appears when no repository is yet linked to the version. Once a repository IS linked, the Repository tab instead shows a read view with the repository's details and sync target configuration:

1. **TAB HEADING — "Repository"**
2. **ACTION BUTTONS**
   a) EDIT BUTTON — edit the linked repository's connection details.
   b) DELETE BUTTON — unlink/remove the repository from this version (after which the tab reverts to the empty "Add New" state above).
3. **REPOSITORY INFORMATION SECTION**
- Heading: "Repository Information"
   a) REPOSITORY NAME — e.g., "testingVulneran".
   b) PROVIDER — e.g., "GitHub".
   c) USER/ORGANIZATION — the GitHub user or org that owns the repo.
   d) REPOSITORY URL — a clickable link to the repository.
   e) AUTHENTICATION TYPE — e.g., "Public".
4. **TARGET CONFIGURATION SECTION**
- Heading: "Target Configuration"
- Description: "Specify a branch, tag, or commit to sync (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.

a) TARGET BRANCH — shows the configured branch or "Not specified".
b) TARGET TAG — shows the configured tag or "Not specified".
c) TARGET COMMIT — shows the configured commit or "Not specified".

- SBOM generation (§6.5) reads from this linked repository and, when
- configured, from the specified Target Branch/Tag/Commit.
- Only one repository can be linked per version at a time.

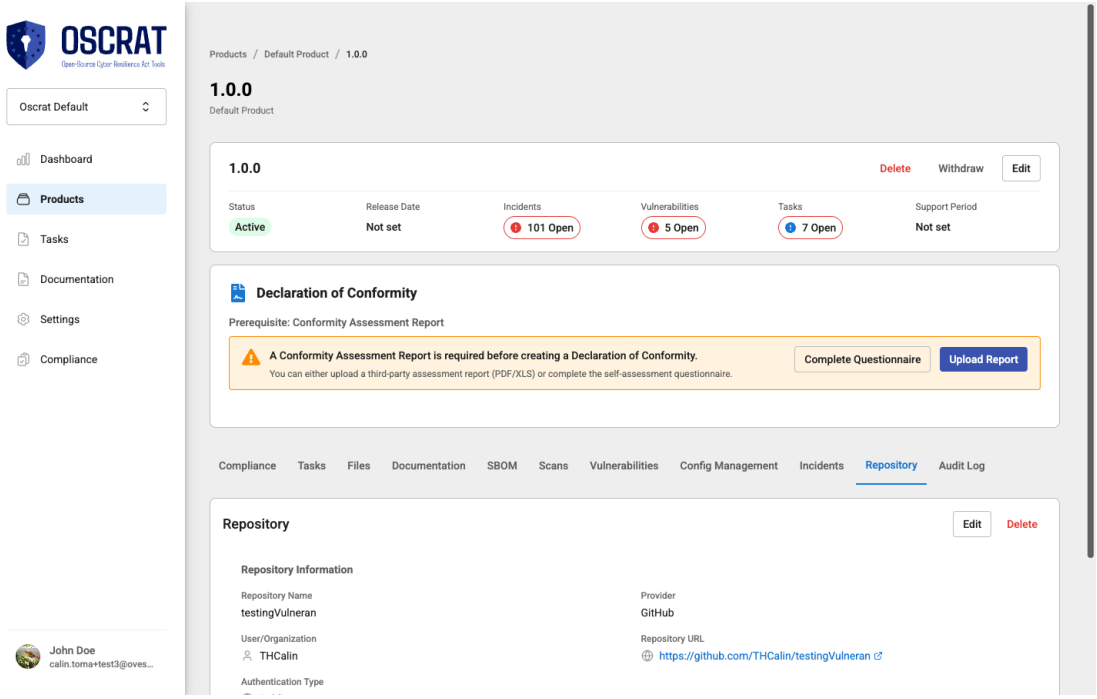

Figure 23: Version Detail — Repository tab

HOW TO USE THE VERSION DETAIL PAGE

Starting the Compliance Assessment:

1. Click the "Compliance" tab.
2. Click "Start Assessment".

Adding a Repository:

1. Click the "Repository" tab.
2. Click "Add New".
3. Fill in the provider, URL, user/org, and repo name.
4. Click "Add".

Withdrawing a Version (End-of-Life):

1. Click "Withdraw" in the header.
2. Confirm the action. The version moves to "Not Supported" on the Product Detail 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.

Reviewing the Audit Log:

1. 1. Click the "Audit Log" tab.
2. 2. Browse the chronological list of changes.

NOTES

- Deleting a version is irreversible. All compliance data, files, SBOM records, tasks, and audit logs for the version are permanently removed.
- The Compliance tab contains the CRA Technical Documentation Checklist, which tracks 41 items across 9 CRA documentation sections.
- Use the Audit Log tab to maintain traceability for regulatory purposes.

6.2 DECLARATION OF CONFORMITY SECTION

LOCATION: Version Detail page — above the tab panel

OVERVIEW

The Declaration of Conformity (DoC) section appears on every Version Detail page, above the tab panel. It manages the two key documents required for CRA market placement:

1. Conformity Assessment Report (CAR) — the prerequisite evidence document.
2. Declaration of Conformity (DoC) — the formal EU declaration signed by the manufacturer.

SECTION ELEMENTS

1. **SECTION HEADING — "Declaration of Conformity" with an icon.**
2. **PREREQUISITE: CONFORMITY ASSESSMENT REPORT**

   When no CAR has been uploaded, the section shows:

   a. A warning paragraph: "A Conformity Assessment Report is required before creating a Declaration of Conformity."
   b. A second line: "You can either upload a third-party assessment report (PDF/XLS) or complete the self-assessment questionnaire."
   c. COMPLETE QUESTIONNAIRE BUTTON — opens the self-assessment flow for this version.
   d. UPLOAD REPORT BUTTON — opens a file picker to upload a Conformity Assessment Report. Accepted formats: PDF or Excel (XLS, XLSX).

   When a CAR has been uploaded:

   a. FILE ICON + FILE NAME — e.g., "CAR_Prod1__v1__2026-02-27.pdf"

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.

b. FILE SIZE & DATE DOWNLOAD BUTTON — downloads the CAR file.
c. DELETE BUTTON — permanently removes the CAR file.
d. Clicking Delete opens a confirmation dialog ("Delete Conformity Assessment Report" — "Are you sure you want to delete the Conformity Assessment Report? This action cannot be undone.") with Cancel/Delete buttons; confirming reverts the whole section to the empty, no-CAR state.

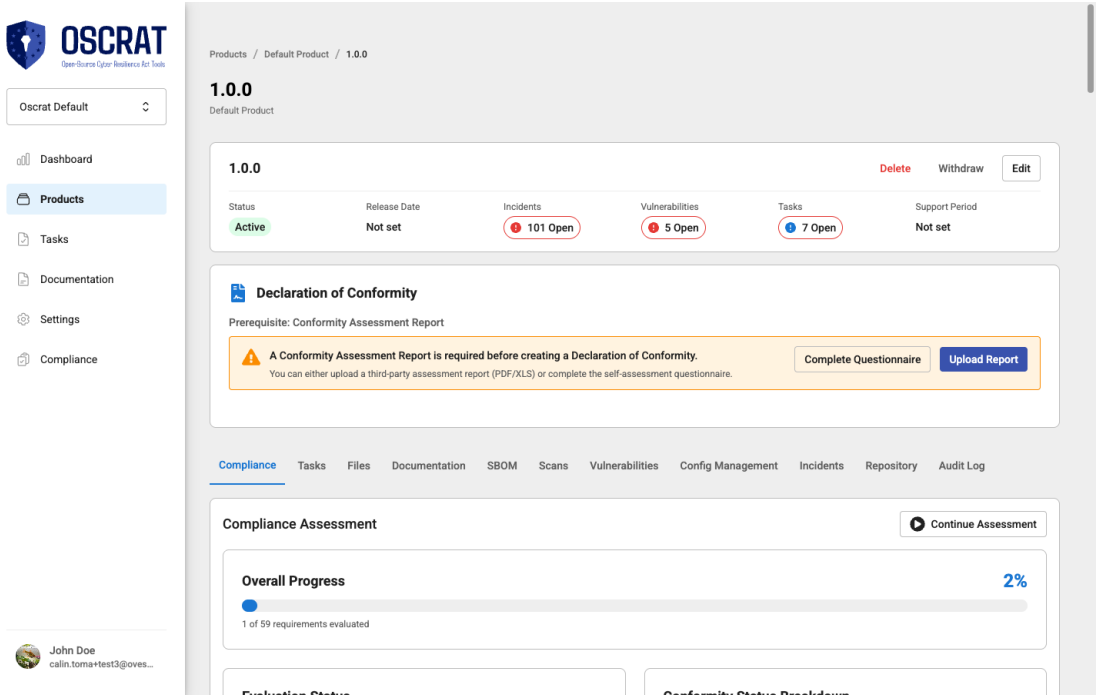

Figure 24: Declaration of Conformity section

2.1 CREATE DECLARATION OF CONFORMITY" BUTTON

Once a CAR exists, a "Declaration of Conformity" sub-heading and a dashed"+ Create Declaration of Conformity" button/drop-zone appear below it. This button is the only way to start creating a DoC, and it is not present until a CAR (or completed self-assessment) exists. It is not mentioned anywhere in the original documentation of this section.

3. DECLARATION OF CONFORMITY

When a DoC is present:

a. FILE ICON + FILE NAME — e.g., "DoC_Prod1_v1.pdf"
b. FILE SIZE, DATE, AND SIGNED BADGE
c. PRINT BUTTON — opens the DoC in a print-friendly view.
d. DOWNLOAD BUTTON — downloads the DoC file.
e. UPLOAD SIGNED BUTTON — upload the signed version of the DoC. Once uploaded, a "Signed" badge is shown.

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.

f. DELETE BUTTON — permanently removes the DoC file.
Clicking Delete opens a confirmation dialog ("Delete Declaration of Conformity" — "Are you sure you want to delete the Declaration of Conformity? This action cannot be undone.") with Cancel/Delete buttons; confirming removes the DoC and reverts the section to the "+ Create Declaration of Conformity" state (item 2A), and also reverts the "Ready for Market" badge and the version's Status field (see below) — both are computed live from DoC state, not stored independently.

3.1 CREATE DECLARATION OF CONFORMITY WIZARD (4 steps)

Clicking "+ Create Declaration of Conformity" (item 2A) opens a 4-step modal wizard.

STEP 1 of 4 — "Review the Conformity Assessment Guide"

- Heading "Create Declaration of Conformity", subtitle "Step 1 of 4", close (X) button.
- Body heading "Review the Conformity Assessment Guide" with description: "Before proceeding, please review the Conformity Assessment Guide to understand how to select the appropriate conformity assessment type."
- "Open Conformity Assessment Guide" LINK — opens an external Guide in a new tab.
- BACK BUTTON (disabled on step 1) and NEXT BUTTON.

STEP 2 of 4 — "Select Conformity Assessment Type"

- RADIO GROUP, "Self-Assessment" pre-selected:
  - Self-Assessment
  - External Assessment - Module B + C
  - External Assessment - Module H
- BACK / NEXT buttons.

STEP 3 of 4 — "Select Declaration Type"

- RADIO GROUP, "Simple Declaration of Conformity" pre-selected:
  - Simple Declaration of Conformity — "A brief declaration suitable for most products."
  - Full Declaration of Conformity — "A comprehensive declaration with detailed product information."
- BACK / NEXT buttons.

STEP 4 of 4 — "Complete the Declaration Template"

- A preview box titled "Simplified EU Declaration of Conformity" with auto-filled, legally-templated text: "Hereby, {Organization Name} declares that the product with digital elements type

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 Name} {Version} is in compliance with Regulation (EU) 2024/2847." "The full text of the EU declaration of conformity is available at the following internet address:" followed by a link to https://europa.eu/youreurope/business/product-requirements/compliance/signing-declaration-conformity/index_en.htm

- BACK BUTTON and "GENERATE PDF" BUTTON (primary) — generates the DoC, closes the wizard, and adds the file under item 3 above.

VERSION STATUS / MARKET READINESS

- Ready for Market — the DoC is complete and the version has met the CRA conformity requirements for market placement.
- The "✓ Ready for Market" badge (green) appears next to the "Declaration of Conformity" H2 heading ONLY once the DoC is uploaded via "Upload Signed"
- Uploading the signed DoC ALSO changes the Version's STATUS field in the Version Stats Bar (§6.1, item 4a) — e.g., from "Active" to "Supported"
- Deleting the signed DoC reverts both the "Ready for Market" badge and the version's Status field back to their prior values

HOW TO UPLOAD THE CONFORMITY ASSESSMENT REPORT

Step 1: On the Version Detail page, locate the "Declaration of Conformity" section above the tabs.
Step 2: In the "Prerequisite: Conformity Assessment Report" area, click the "Upload Report" button.
Step 3: Select a PDF, XLS, or XLSX file from your device.
Step 4: The CAR appears with its file name, size, and date.

HOW TO USE THE SELF-ASSESSMENT QUESTIONNAIRE

Step 1: In the CAR section, click "Complete Questionnaire".
Step 2: Complete the assessment within the opened flow.
Step 3: Upon completion, the assessment result serves as the CAR evidence.

HOW TO CREATE A DECLARATION OF CONFORMITY (FULL WIZARD)

Step 1: With a CAR already uploaded (or self-assessment completed), click "+ Create Declaration of Conformity".

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.

Step 2: Step 1 of 4 — optionally open the Conformity Assessment Guide, then click "Next".
Step 3: Step 2 of 4 — select a Conformity Assessment Type (Self-Assessment, External Assessment - Module B + C, or External Assessment - Module H), then click "Next".
Step 4: Step 3 of 4 — select a Declaration Type (Simple or Full Declaration of Conformity), then click "Next".
Step 5: Step 4 of 4 — review the auto-filled declaration text (citing Regulation (EU) 2024/2847), then click "Generate PDF".
Step 6: The unsigned DoC appears with Print/Download/UploadSigned/Delete actions.

HOW TO UPLOAD A SIGNED DECLARATION OF CONFORMITY

Step 1: Locate the "Declaration of Conformity" sub-section.
Step 2: After the unsigned DoC has been generated and signed, click "Upload Signed".
Step 3: Select the signed DoC file from your device.
Step 4: The signed file replaces the previous version and a "Signed" badge is displayed. This also makes the "✓ Ready for Market" badge appear on the section heading and changes the version's Status field (Version Stats Bar) to "Supported"

NOTES

- The CAR must be completed and uploaded (or a self-assessment questionnaire completed) before the DoC is considered finalized under the CRA.
- Accepted CAR formats: PDF, XLS (Excel 97-2003), XLSX (Excel 2007+).
- The DoC must be signed by the authorized representative of the manufacturer.

6.3 FILES TAB

URL /organization/{org-slug}/products/{product-id}/versions/{version-id}?tab=files

OVERVIEW

The Files tab lets you upload and manage arbitrary files attached to a specific product version. Typical files include test reports, technical specifications, or any other CRA-relevant documents.

TAB ELEMENTS

1. **TAB HEADING — "Files"**
2. **ADD FILE BUTTON — opens a file picker to upload a new file.**
3. **FILES TABLE — columns:**
   a. NAME — the file 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.

b. DESCRIPTION — "No description" if none was provided at upload.
c. DATE ADDED — upload date (DD.MM.YYYY).
d. ADDED BY — the user who uploaded the file.
e. ACTIONS — Download and Delete buttons.

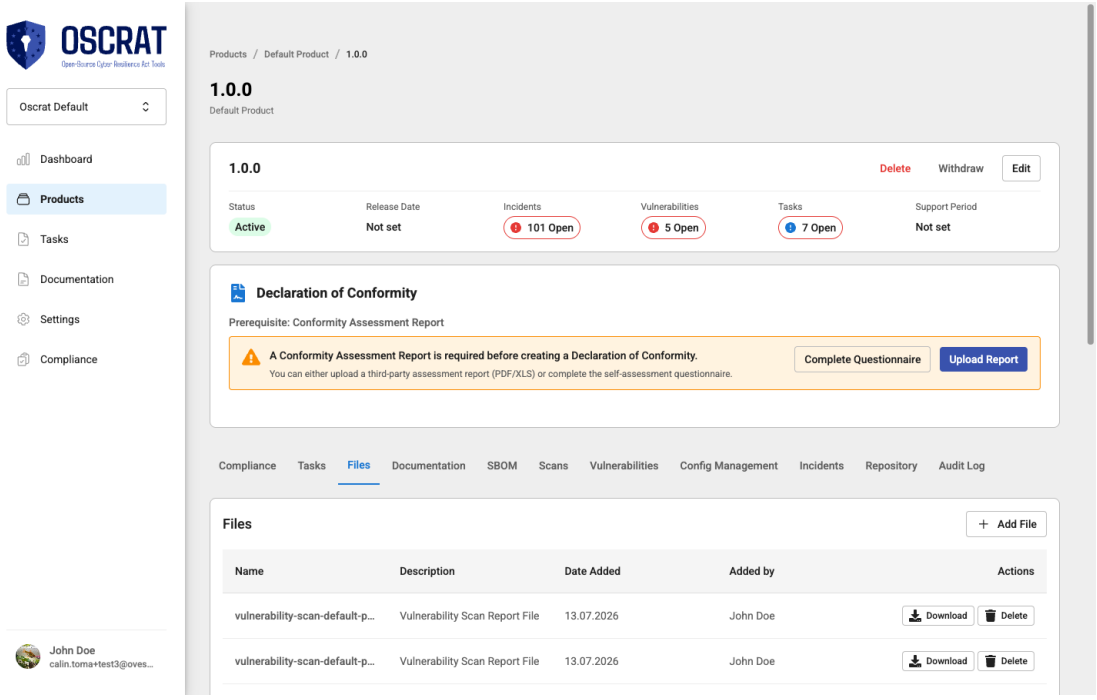

Figure 25: Version Detail — Files tab

HOW TO UPLOAD A FILE

Step 1: Navigate to the Version Detail page and click the "Files" tab.
Step 2: Click "Add File".
Step 3: Select the file you want to upload.
Step 4: The file is uploaded and appears in the table.

NOTES

- Deleted files cannot be recovered.
- For the official Declaration of Conformity (DoC) and Conformity Assessment Report (CAR), use the dedicated "Declaration of Conformity" section above the tab panel.
- All file uploads are logged in the Audit Log tab.

6.4 SBOM TAB

URL: /organization/{org-slug}/products/{product-id}/versions/{version-id}?tab=sbom

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.

OVERVIEW

The SBOM (Software Bill of Materials) tab manages SBOM generation jobs for a specific product version. An SBOM is a formal, machine-readable inventory of all software components and dependencies — a key requirement under the CRA.

TAB ELEMENTS

1. TAB HEADING — "SBOM Generation Jobs"
2. REFRESH BUTTON — reloads the job list.
3. IMPORT BUTTON — upload an existing SBOM file (CycloneDX XML or SPDX).
4. GENERATE BUTTON — triggers a new SBOM generation job from the linked repository.
5. SBOM JOBS TABLE — columns:
   a. STATUS — Completed / Running / Failed
   b. SOURCE — "Repository" or "Import"
   c. STARTED — date and time
   d. TRIGGERED BY — the user who initiated the job
   e. DURATION — how long the job took
   f. PACKAGES — number of software packages detected
   g. SCAN — short ID of associated vulnerability scan (if any)
   h. ACTIONS — Download, Scan, Delete buttons

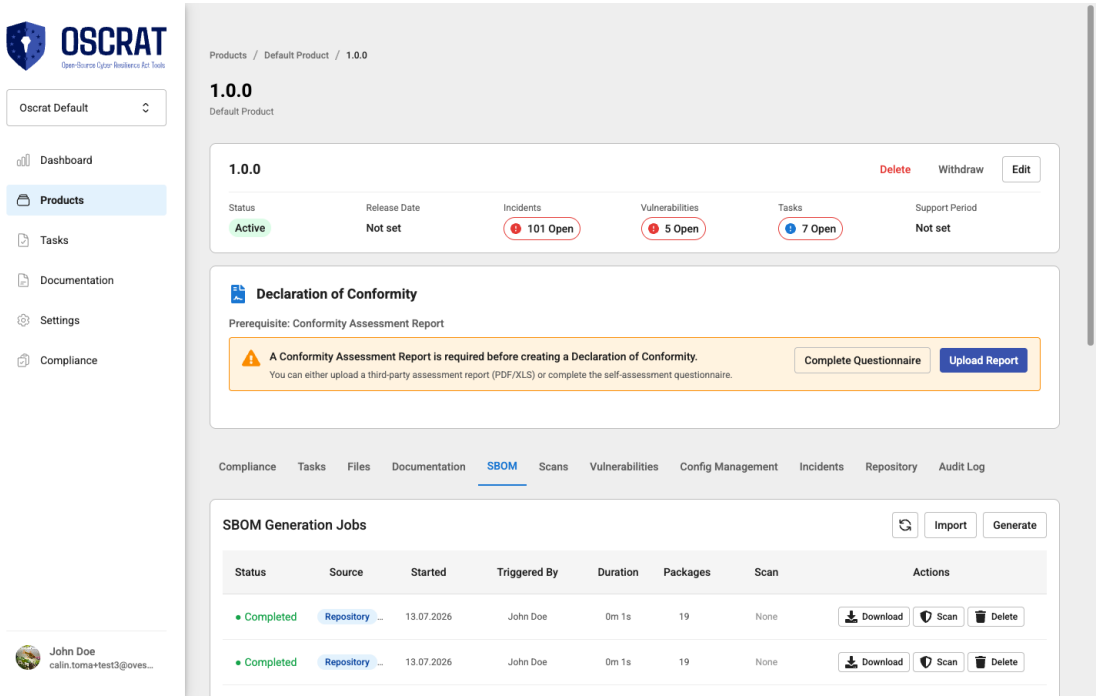

Figure 26: Version Detail — SBOM tab

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.

HOW TO GENERATE AN SBOM

Step 1: Ensure a repository is linked (configure it in the Repository tab).
Step 2: Navigate to the SBOM tab.
Step 3: Click "Generate". A new job entry appears with "Running" status.
Step 4: Click "Refresh" until status changes to "Completed".
Step 5: Click "Download" to save the SBOM file.

HOW TO IMPORT AN EXISTING SBOM

Step 1: Navigate to the SBOM tab.
Step 2: Click "Import".
Step 3: Select your existing SBOM file (CycloneDX XML or supported format).
Step 4: The imported SBOM appears in the jobs table with source "Import".

HOW TO TRIGGER A VULNERABILITY SCAN FROM AN SBOM

Step 1: Locate a completed SBOM job in the table.
Step 2: Click "Scan" in the Actions column.
Step 3: Navigate to the Scans tab to monitor progress.

NOTES

- SBOM generation requires a repository to be linked via the Repository tab.
- The generated SBOM is in CycloneDX format.
- Under the CRA, manufacturers must make the SBOM available to market surveillance authorities upon reasoned request.

6.5 SCANS TAB

URL: /organization/{org-slug}/products/{product-id}/versions/{version-id}?tab=scans

OVERVIEW

The Scans tab shows all vulnerability scan jobs run against a specific product version. Scans analyse the version's SBOM to detect known security vulnerabilities (CVEs) in the software components used.

TAB ELEMENTS

1. TAB HEADING — "Vulnerability Scan Jobs"
2. REFRESH BUTTON — reloads the table.
3. SCAN JOBS TABLE — columns:
   a. STATUS — Completed / Running / Failed
   b. SOURCE — the short ID of the SBOM used as input
   c. STARTED — date and 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.

d. TRIGGERED BY — the user who triggered the scan
e. DURATION — e.g., "0m 15s"
f. TOTAL — total vulnerabilities found
g. CRITICAL — count of Critical severity CVEs
h. HIGH — count of High severity CVEs
i. MEDIUM — count of Medium severity CVEs
j. LOW — count of Low severity CVEs
k. ACTIONS — Download and Delete buttons

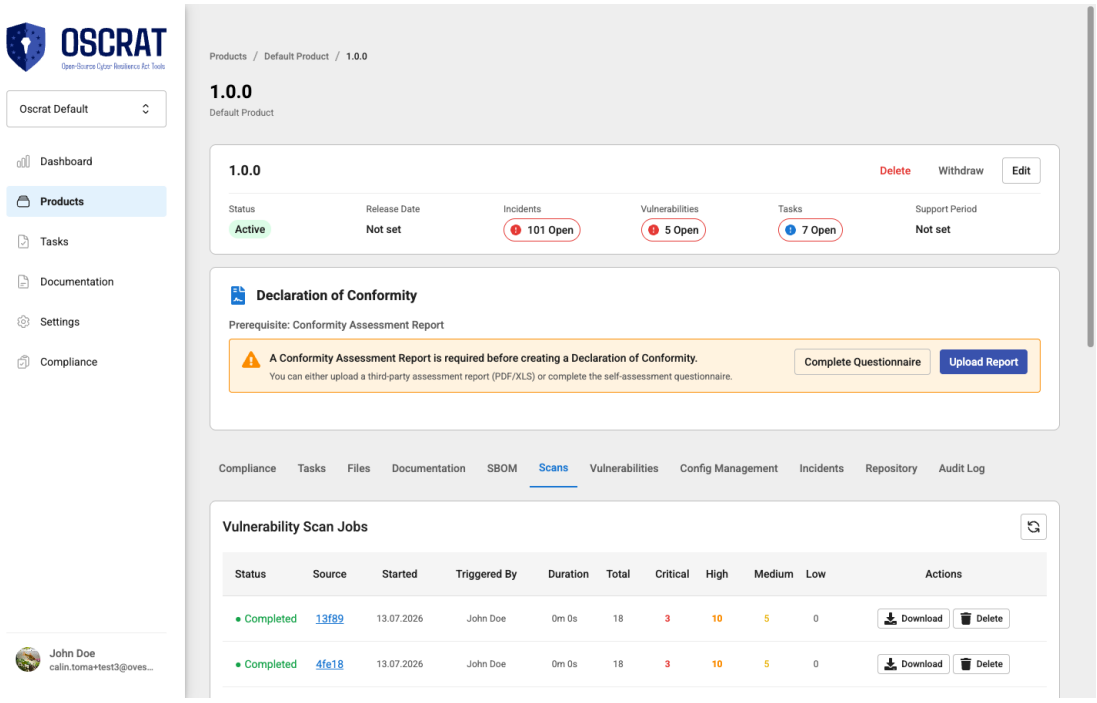

Figure 27: Version Detail — Scans tab

HOW TO TRIGGER A SCAN

Step 1: Go to the SBOM tab and locate a completed SBOM generation job.
Step 2: Click "Scan" in the SBOM job's Actions column.
Step 3: Click "Refresh" on the Scans tab until status shows "Completed".
Step 4: Review the vulnerability counts.
Step 5: Click "Download" to get the full scan report.
Step 6: Navigate to the Vulnerabilities tab to view individual findings.

NOTES

- Scans are based on the SBOM content. Ensure the SBOM is up-to-date before triggering a scan.
- Scan results are imported into the Vulnerabilities tab automatically after a scan completes.
- Regular scanning is recommended to stay on top of newly disclosed CVEs.

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.

6.6 VULNERABILITIES TAB

URL: /organization/{org-slug}/products/{product-id}/versions/{version-id}?tab=vulnerabilities

OVERVIEW

The Vulnerabilities tab lists all known security vulnerabilities associated with a specific product version. Vulnerabilities can be imported automatically from a completed scan or added manually.

TAB ELEMENTS

1. **TAB HEADING — "Vulnerabilities"**
2. **ADD VULNERABILITY BUTTON — opens a dialog to manually add a vulnerability.**
3. **VULNERABILITIES TABLE — columns:**
   a. CVE ID — the CVE identifier (e.g., "CVE-2023-12345")
   b. SEVERITY — Critical / High / Medium / Low
   c. COMPONENT — the affected software component
   d. STATUS — current remediation status in the CVD (Coordinated Vulnerability Disclosure) pipeline. Values, in pipeline order:
      1. Pending
      2. Preparation
      3. Receipt
      4. Verification
      5. Remediation Development
      6. Release
      7. Post Release
   e. ACTIONS — View, Delete buttons

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.

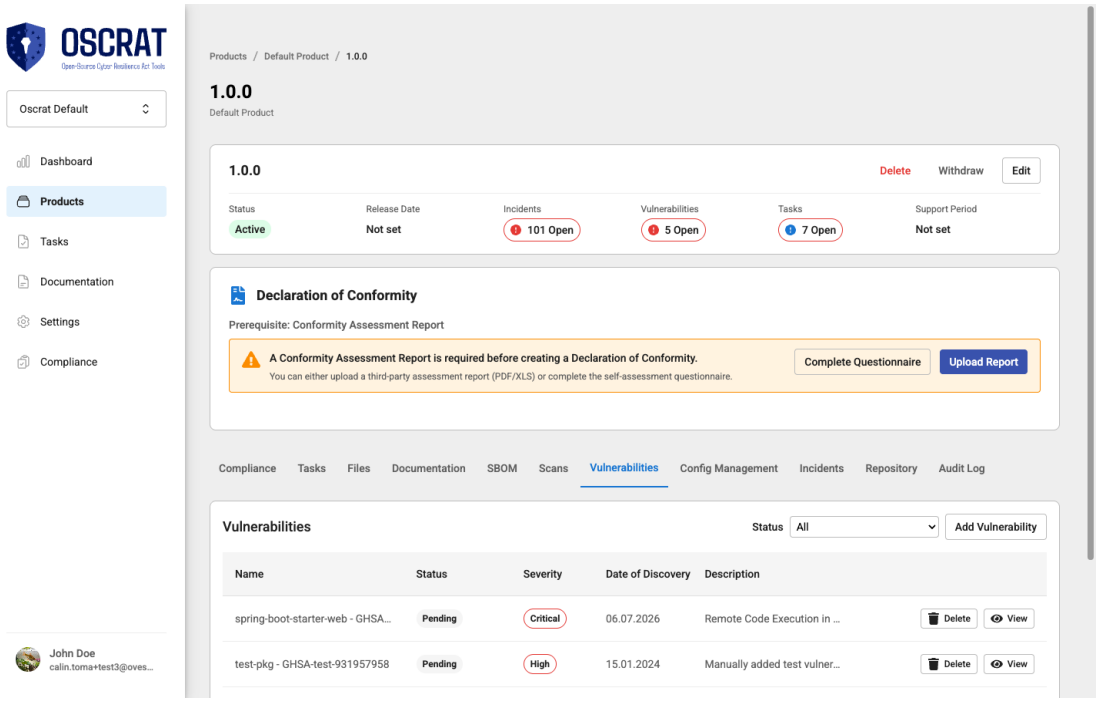

Figure 28: Version Detail — Vulnerabilities tab

HOW TO VIEW VULNERABILITIES

Step 1: Navigate to the Version Detail page.
Step 2: Click the "Vulnerabilities" tab.
Step 3: Review the list of CVEs. Use the filters or search to narrow results.

NOTES

- Vulnerability data is typically populated automatically after a successful vulnerability scan.
- Manual vulnerability entries can be added if you discover vulnerabilities through other means.

VULNERABILITY DETAILS PAGE

URL: /organization/{org-slug}/products/{product-id}/versions/{version-id}/vulnerabilities/{vulnerability-id}

Clicking a row in the Vulnerabilities table navigates to a dedicated Vulnerability Details page:

1. **BREADCRUMB NAVIGATION — Products / Product Name / Version / Vulnerability Details.**
2. **PAGE HEADING — "Vulnerability Details: {name}" (truncated with an ellipsis if long).**

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. **CONTEXT INFORMATION SECTION**

- Heading: "Context Information"; EDIT BUTTON and CLOSE BUTTON.
    a) VULNERABILITY NAME
    b) STATUS — current CVD pipeline stage.
    c) SEVERITY
    d) AFFECTED VENDOR — shows "-" if not set.
    e) AFFECTED PRODUCT
    f) AFFECTED VERSION

4. **EXTENDED DATA SECTION**

- Heading: "Extended Data"
    a) CVE — the CVE identifier, e.g., "CVE-2022-22965".
    b) ADVISORY ID — e.g., a GHSA identifier.
    c) DESCRIPTION — full vulnerability description.
    d) CREATED BY — user name and email.
    e) CREATED AT — date.
    f) UPDATED BY — user name and email.
    g) UPDATED AT — date.

5. **ATTACHMENTS SECTION**

- Heading: "Attachments"
    a) ADD ATTACHMENT — opens a file picker. Restrictions shown: "Max file size: 10MB • Allowed types: PDF, DOC, DOCX, TXT, CSV, JSON, XML, YML, YAML, ZIP, TAR, GZ, TGZ, PNG, JPG, JPEG, GIF".
    b) Shows "No attachments" when none have been uploaded.

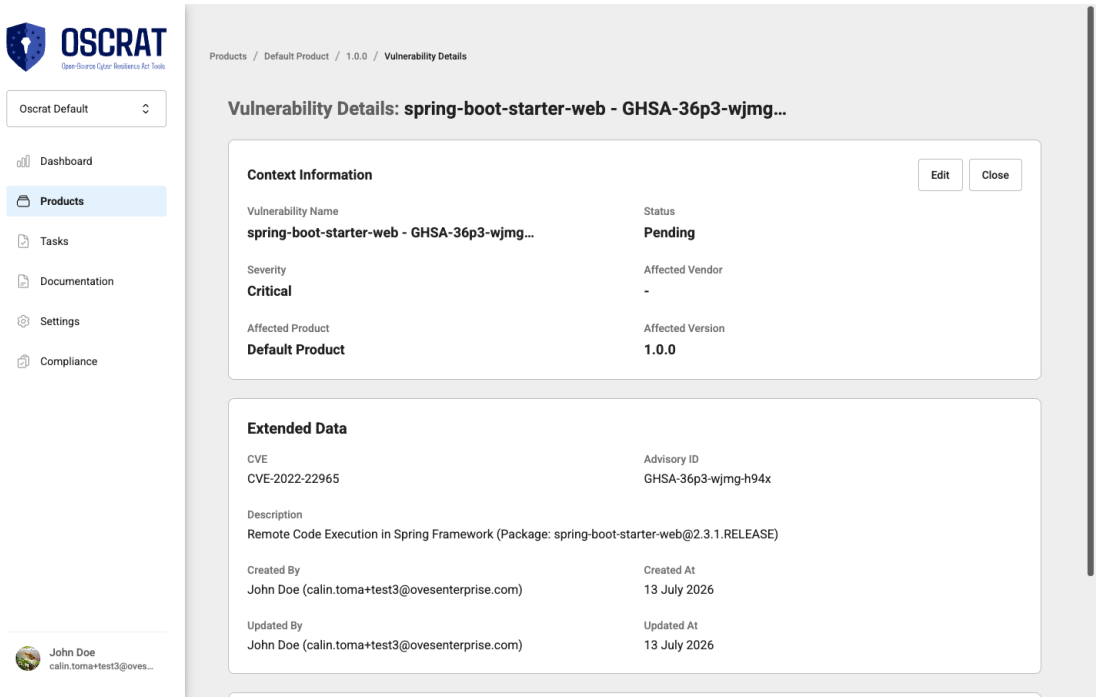

Figure 29:Vulnerability Details page

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.

HOW TO VIEW VULNERABILITY DETAILS

Step 1: Navigate to the Version Detail page and click the "Vulnerabilities" tab.
Step 2: Click any row in the vulnerabilities table.
Step 3: Review Context Information and Extended Data. Click "Edit" to modify the vulnerability's editable fields.
Step 4: Use the Attachments section to upload supporting evidence (e.g., scan output, remediation notes) for this vulnerability.

NOTES

- The Advisory ID and CVE fields are typically populated automatically when the vulnerability originates from an automated scan (§6.6); manually added vulnerabilities may leave these blank.

6.7 INCIDENTS TAB

URL: /organization/{org-slug}/products/{product-id}/versions/{version-id}?tab=incidents

OVERVIEW

The Incidents tab records and tracks security incidents associated with a specific product version. Incident reporting is an obligation under the CRA.

TAB ELEMENTS

1. **TAB HEADING — "Incidents"**
2. **ADD INCIDENT BUTTON — opens a dialog to record a new incident.**
3. **INCIDENTS TABLE — columns :**
   - NAME (the incident title)
   - STATUS
     1. Pending
     2. Start
     3. Declared
     4. Stable
     5. Active
     6. Resolved
     7. Completed
   - CLASSIFICATION
   - SEVERITY
   - DATE DETECTED (DD.MM.YYYY)
   - ACTIONS.

This pipeline mirrors the structure of the vulnerability CVD pipeline (§6.7) but uses different stage names — the two should not be assumed interchangeable.

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.

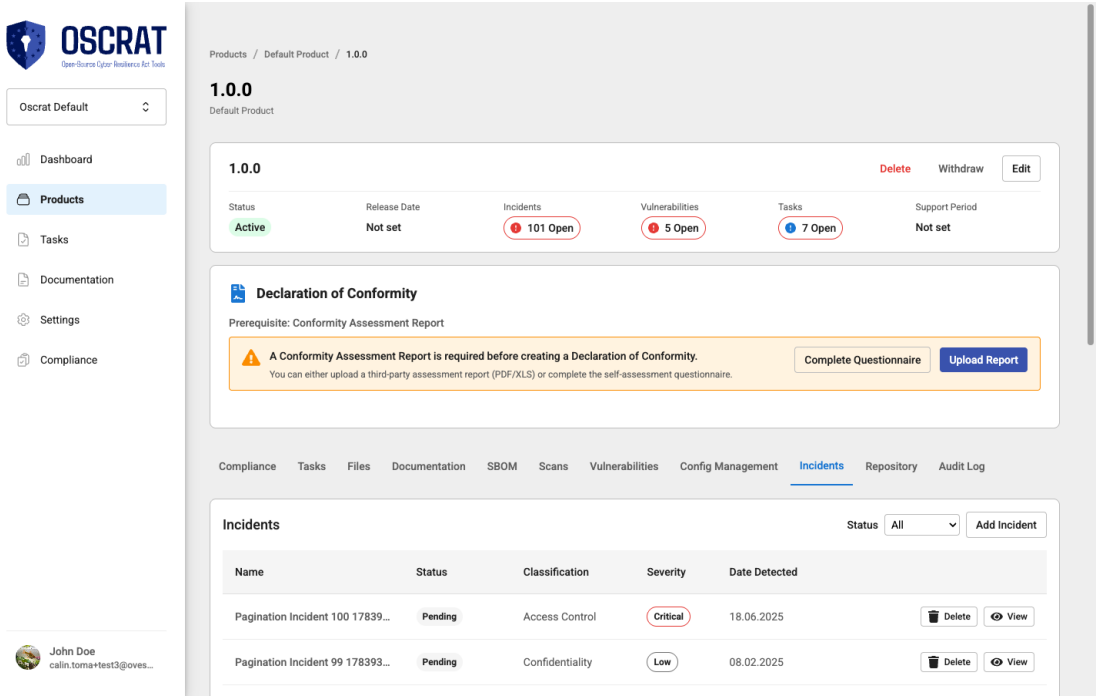

Figure 30: Version Detail — Incidents tab

HOW TO RECORD AN INCIDENT

Step 1: Navigate to the Version Detail page.
Step 2: Click the "Incidents" tab.
Step 3: Click "Add Incident".
Step 4: Fill in the incident details and submit.

NOTES

- Incident count is shown in the Version Stats Bar at the top of the Version Detail page.
- Use incidents to maintain the CRA-required record of security incidents affecting your products.

6.8 TASKS TAB (VERSION)

URL: /organization/{org-slug}/products/{product-id}/versions/{version-id}?tab=task

OVERVIEW

The Tasks tab on the Version Detail page provides a focused view of all tasks linked to a specific product version. It is a filtered subset of the Organization Tasks 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.

TAB ELEMENTS

1. TAB HEADING — "Tasks"
2. STATUS FILTER — dropdown, filter tasks by status (All / To Do / Planned / In Progress / Done). — Optional. Default: All.
3. TYPE FILTER — dropdown, filter tasks by Task Type (All / Vulnerability / Incident / SBOM / Documentation / Risk / Training / Configuration Mgmt / Requirements / Other). — Optional. Default: All.
4. ADD TASK BUTTON — opens the Create Task dialog, pre-scoped to this version. Product and Version are pre-filled and disabled in this dialog (see the Create Task Dialog description in Section 8.1, which now also lists the Type field added to this dialog).
5. TASKS TABLE — columns, in this order:
   a. TASK — task title (with task type/origin badge, e.g. "Manual" or "Auto"). Clicking navigates to the Task Detail page.
   b. TYPE — the task's Type value (e.g. "Configuration Mgmt", "Risk", "Vulnerability").
   c. DUE DATE — target completion date (DD.MM.YYYY).
   d. ASSIGNEE — column, showing "Unassigned" when no assignee is set.
   e. STATUS — current status dropdown; can be changed inline.
6. PAGINATION — Previous / Next buttons with item count.

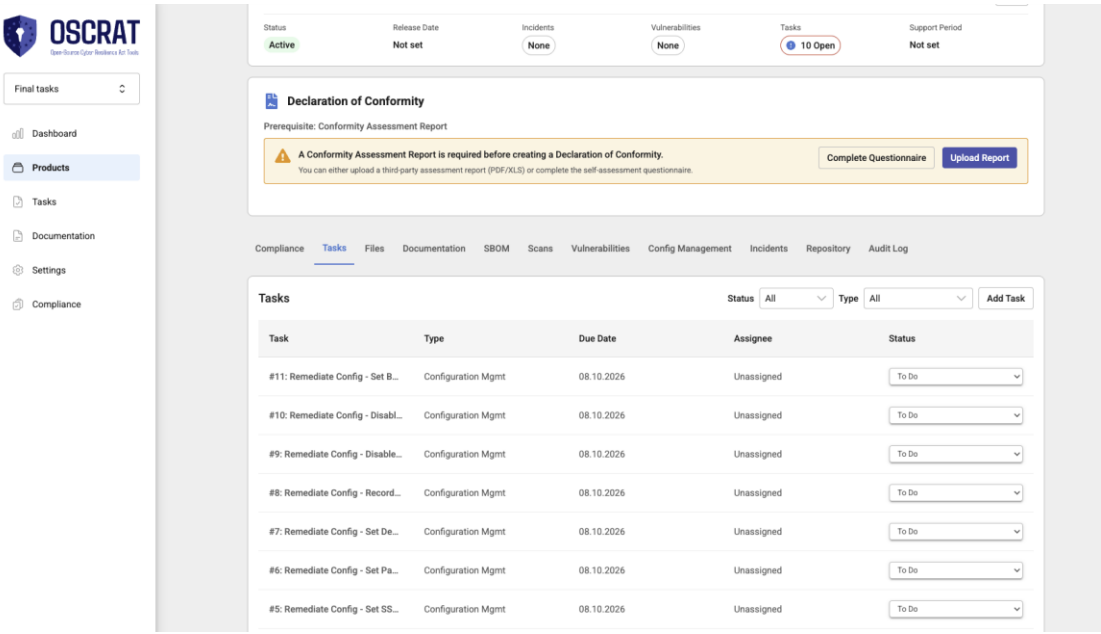

Figure 31: Version Detail — Tasks tab

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.

HOW TO ADD A VERSION TASK

Step 1: Click the "Tasks" tab on the Version Detail page.
Step 2: Click "Add Task".
Step 3: Fill in the task title and any optional fields (Type, Status, Due Date, Description). Product and Version are already set to this version and cannot be changed from this dialog.
Step 4: Click "Create".

NOTES

- Tasks created from the version Tasks tab are also visible on the Organization Tasks page.
- See Section 8.1 for full task table details and Section 8.3 for the Risk Assessment feature (now driven by setting the task's Type to "Risk", not by a checkbox — see Section 8.3).
- Open task count is shown in the Version Stats Bar.

6.9 CONFIGURATION MANAGEMENT TAB

URL: /organization/{org-slug}/products/{product-id}/versions/{version-id}?tab=configuration

OVERVIEW

The Configuration Management tab manages OpenSCAP-based configuration scan jobs for a specific product version. Configuration scans verify that a product version's system configuration meets defined security baselines or compliance profiles.

TAB ELEMENTS

1. **TAB HEADING — "Config Management"**
2. **REFRESH BUTTON — reloads the jobs table.**
3. **IMPORT BUTTON — opens the "Import File" side drawer to upload an OpenSCAP results file.**
4. **IMPORT FILE DRAWER:**
   - Description: "Upload an OpenSCAP results file (.xml). Supported:
   - ARF 1.1, XCCDF 1.2, OVAL 5.x."
   - UPLOAD AREA — click to open a file picker (single .xml file).
   - IMPORT BUTTON (in drawer) — enabled after a file is selected;
   - submits the upload and closes the drawer.
5. **SCAN JOBS TABLE — columns:**
   a. STATUS — processing / Completed / Failed
   b. FORMAT — e.g., "XCCDF 1.2" or "ARF 1.1"
   c. STARTED — date and time of the import
   d. TRIGGERED BY — the user who initiated the import

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.

e. DURATION — time taken to process the file
f. TOTAL RULES — total number of rules evaluated
g. PASS — count of rules that passed
h. FAIL — count of rules that failed
i. ACTIONS — Download and Delete buttons per row Clicking a completed row navigates to the Configuration Scan Report page for that job.

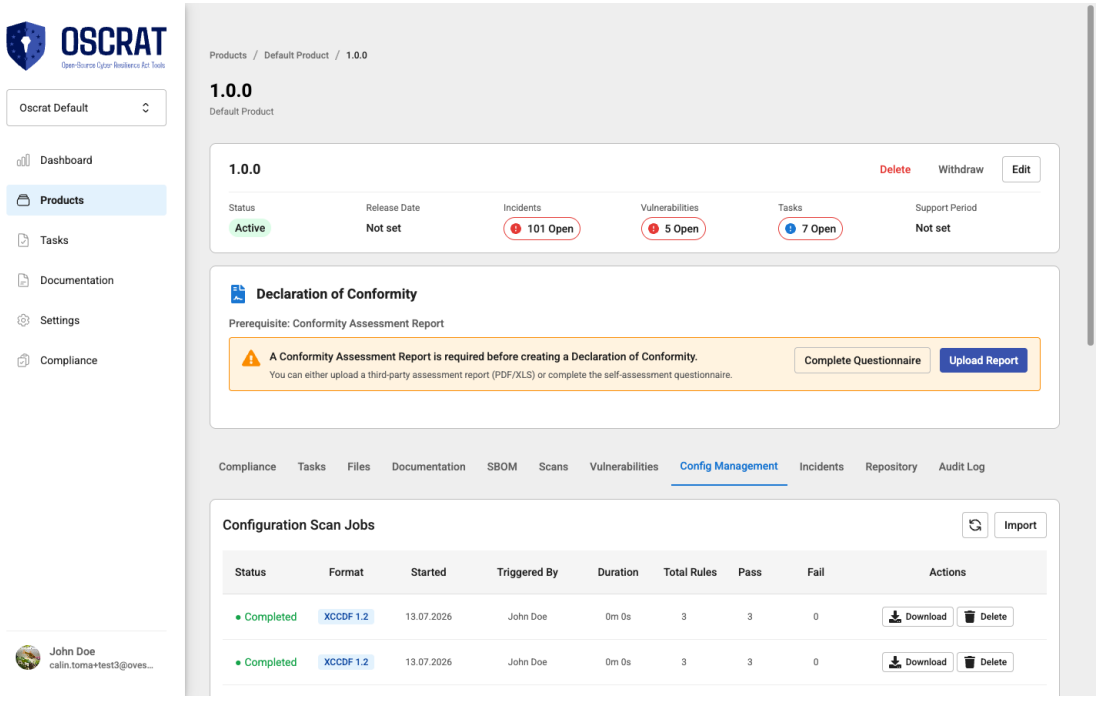

Figure 32: Version Detail — Configuration Management tab

HOW TO IMPORT A CONFIGURATION SCAN REPORT

Step 1: Navigate to the Version Detail page and click the "Config Management" tab.
Step 2: Click "Import". The "Import File" drawer opens on the right.
Step 3: Click the upload area and select an OpenSCAP results file (.xml — ARF 1.1, XCCDF 1.2, or OVAL 5.x format).
Step 4: Click "Import" in the drawer. The drawer closes and a new job row appears with a processing status.
Step 5: Click "Refresh" to check for the latest status. Once processing is complete the row shows "Completed".
Step 6: Click the job row to open the Configuration Scan Report, or click "Download" in the Actions column to download the original 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.

NOTES

- Configuration scan results are logged in the Audit Log tab.
- Configuration Management is the 8th tab on the Version Detail page, located between the Vulnerabilities and Incidents tabs.

CONFIGURATION MANAGEMENT SCAN REPORT PAGE

URL: /organization/{org-slug}/products/{product-id}/versions/{version-id}/configuration/{scan-id}

Clicking a completed row in the Scan Jobs table navigates to a full Configuration Scan Report page:

1. **BREADCRUMB NAVIGATION — Products / Product Name / Version / Configuration Scan Report.**
2. **PAGE HEADING — "Configuration Scan Report", with a close/back button.**
3. **OVERVIEW SECTION**
   - Heading: "Overview"
     a. TOTAL RULES — total number of rules evaluated.
     b. PASS — count of passing rules.
     c. FAIL — count of failing rules.
     d. ERROR — count of rules that errored during evaluation.
     e. NOT APPLICABLE — count of rules not applicable to the target.
     f. SCAN DATE — date the scan was performed (DD.MM.YYYY).
     g. FORMAT — the OpenSCAP format, e.g., "XCCDF 1.2" or "ARF 1.1".
     h. TRIGGERED BY — the user who imported/triggered the scan.
4. **BENCHMARK SECTION**
   - Heading: "Benchmark"
     a. BENCHMARK — the benchmark identifier and version, e.g., "ssg-rhel9-ds (0.1.73)".
     b. PROFILE — the compliance profile applied, e.g., "CIS Red Hat Enterprise Linux 9 Benchmark for Level 2 - Server".
     c. TARGET HOSTNAME — the hostname of the scanned system.
5. **RULES SECTION**
   - Heading: "Rules", with a count subtitle (e.g., "3 rules found").
   - RULES TABLE — columns: RULE ID (the OpenSCAP rule identifier, e.g. "xccdf_org.ssgproject.content_rule_no_empty_passwords"), TITLE (human-readable rule description), SEVERITY (e.g., "high", "medium"), RESULT (e.g., "pass", "fail"), and ACTION.

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.

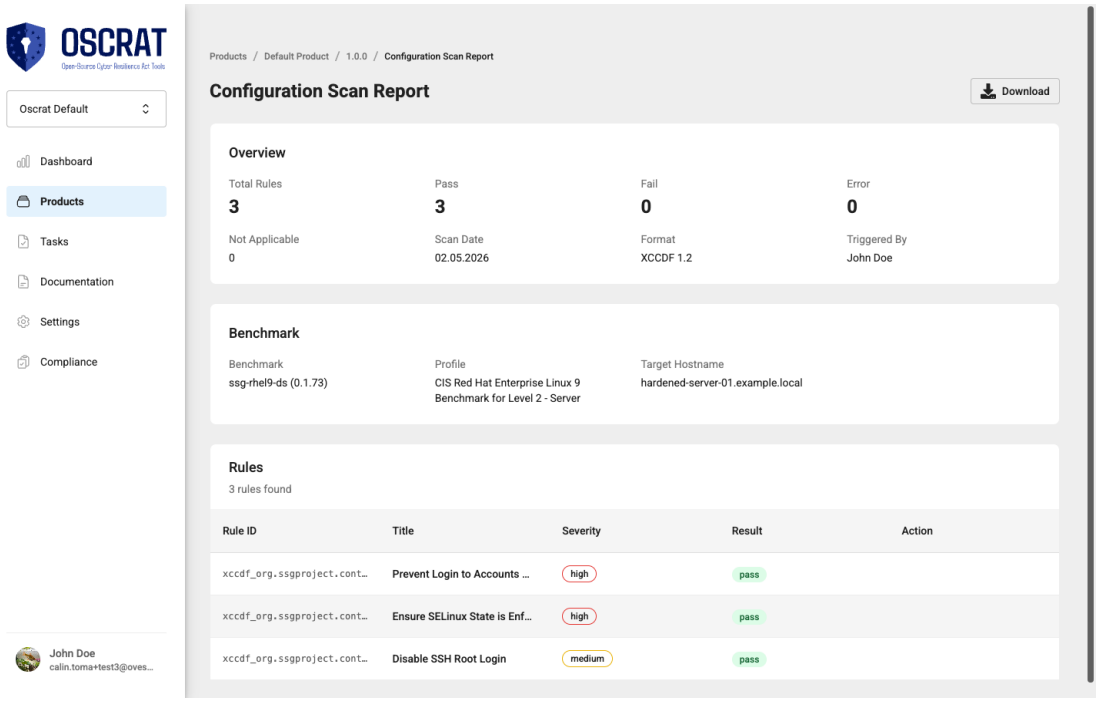

Figure 33: Configuration Scan Report page

HOW TO VIEW A CONFIGURATION SCAN REPORT

Step 1: Navigate to the Version Detail page and click the "Config Management" tab.
Step 2: Click any row with status "Completed".
Step 3: Review the Overview, Benchmark, and Rules sections to see the full results of that configuration scan.

NOTES

- This page is read-only; use the Config Management tab's Download action to export the original uploaded file.
- Rule-level Result values map directly to the Pass/Fail counts shown both here and in the Config Management tab's jobs table.

6.10 AUDIT LOG TAB

URL: /organization/{org-slug}/products/{product-id}/versions {version-id}?tab=audit-log

OVERVIEW

The Audit Log tab provides a chronological audit trail of all actions taken on a specific product version. It records who did what and when, covering compliance assessments, file uploads, vulnerability discoveries, incident reports, SBOM generation, task creation, configuration scans, and more.

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.

TAB ELEMENTS

1. **TAB HEADING — "Audit Log"**
2. **FILTERS:**
   a. ALL USERS DROPDOWN — filter by actor — Optional
   b. ALL ENTITIES DROPDOWN — filter by entity type: — Optional Assessment, Vulnerability, Vulnerability Scan Report, Incident, Attachment, SBOM Report, Repository, Product Version, Task, Documentation, File, Configuration Scan.
   c. ALL OPERATIONS DROPDOWN — Create / Delete / Update / — Optional Processed / Downloaded
   d. FROM DATE PICKER — show only entries from this date onward. — Optional
   e. TO DATE PICKER — show only entries up to this date. — Optional

3. **AUDIT LOG TABLE — columns:**
   a. TIMESTAMP — date and time of the action (format: "7 May 2026, 15:40")
   b. USER — display name of the user
   c. ACTION — human-readable description (e.g., "Created configuration scan")
   d. TARGET — entity type and identifier (e.g., "Configuration Scan id: 91a2a")
   e. DETAILS — "View Details" opens a modal with the full change record

4. **PAGINATION — Previous / Next buttons; item count shown.**

EXAMPLE LOG ENTRY TYPES

- "Created assessment"
- "Deleted assessment"
- "Uploaded attachment"
- "Created incident"
- "Created vulnerability"
- "Started vulnerability scan"
- "Generated SBOM report"
- "Added repository"
- "Created task"
- "Created documentation"
- "Uploaded file"
- "Created configuration scan"
- "Processed configuration scan"
- "Downloaded attachment"

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.

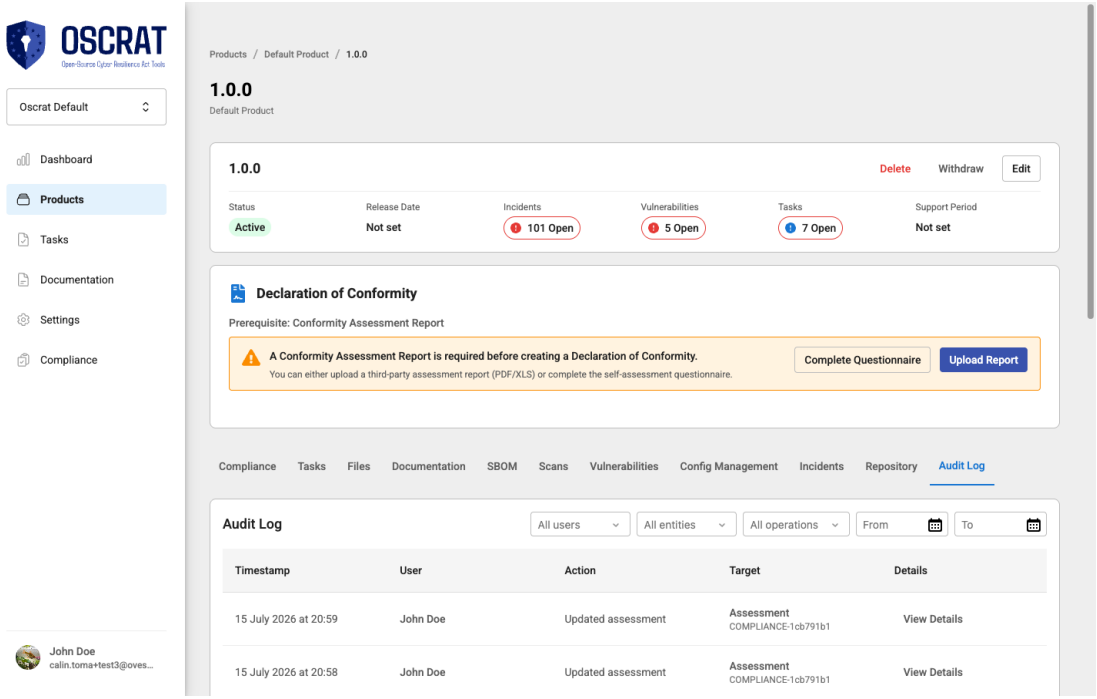

Figure 34: Version Detail — Audit Log tab

HOW TO USE THE AUDIT LOG

Viewing all activity: Click the "Audit Log" tab and browse in reverse-chronological order.

Filtering by user / entity / operation / date: Use the respective dropdown or date picker filters.

Viewing full change details: Locate the entry and click "View Details". The modal shows the complete record of the change.

NOTES

- Audit Log entries are immutable — they cannot be edited or deleted.
- This ensures a tamper-evident record for regulatory purposes.
- For the organization-wide audit log (covering all products and versions), use the Audit Logs tab under the organization Settings 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.

6.11 DOCUMENTATION TAB (VERSION) — FILTERS

URL: /organization/{org-slug}/products/{product-id}/versions/{version-id}?tab=documentation

OVERVIEW

The Documentation tab on the Version Detail page (listed only by name in 6.1, tab 4 of the TABS OVERVIEW) is the same underlying Documentation feature as §9.1, pre-filtered to documents scoped to the current product version, with its own filter set.

TAB ELEMENTS

1. **TAB HEADING — "Documentation"**
2. **FILTERS**
   a. STATUS DROPDOWN — All / Draft / Published / Archived. — Optional
   b. VISIBILITY DROPDOWN — All / Private / Public. — Optional
   c. UPDATED DROPDOWN (sort order) — Newest first / Oldest first. — Optional
3. **ADD DOCUMENTATION BUTTON — opens the Create Documentation dialog, pre-scoped to this version (see §9.1).**
4. **DOCUMENTATION TABLE — columns: Title, Status, Visibility, Updated. Clicking a row opens that document's detail/editor page (§9.1).**
5. **PAGINATION — Previous / Next buttons with item count.**

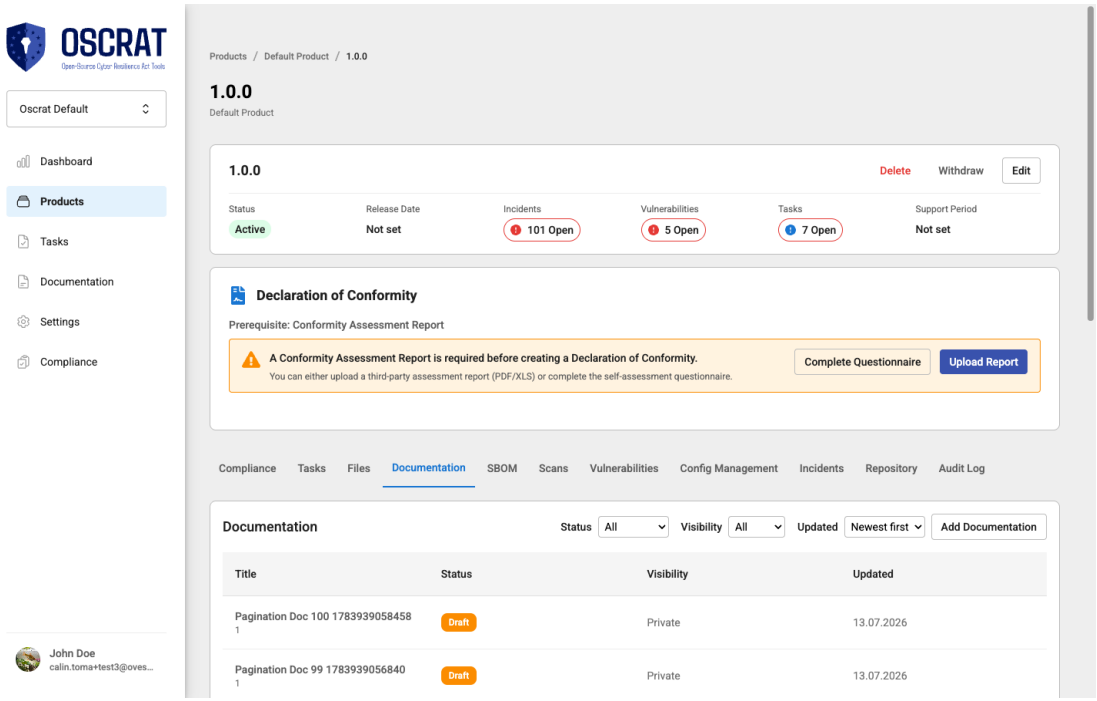

Figure 35: Version Detail — Documentation tab

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.

HOW TO FILTER VERSION-LEVEL DOCUMENTATION

Step 1: Navigate to the Version Detail page and click the "Documentation" tab.
Step 2: Use the Status and/or Visibility dropdowns to narrow the list.
Step 3: Use the Updated dropdown to sort by newest or oldest first.

NOTES

- The org-level Documentation page (§9.1) does not offer the "Updated" sort dropdown — this is specific to the version-level 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.

7. COMPLIANCE ASSESSMENT

7.1 COMPLIANCE ASSESSMENT PAGE

ORGANIZATION-LEVEL URL:
/organization/{organization-slug}/compliance

VERSION-LEVEL URL:
/organization/{org-slug}/products/{product-id}/versions/{version-id}/compliance

OVERVIEW

The Compliance Assessment page guides you through the process of evaluating your organization's (or a product version's) adherence to CRA requirements.

There are two types of compliance assessment in OSCRAT:

1. ORGANIZATION-LEVEL ASSESSMENT — covers organizational processes and policies. Accessed from the Organization Dashboard or the sidebar.
2. VERSION-LEVEL ASSESSMENT — covers product-specific technical requirements for a given product version. Accessed from the Compliance tab on the Version Detail page. Includes the CRA Technical Documentation Checklist.

ORGANIZATION COMPLIANCE PAGE ELEMENTS

1. PAGE HEADING — "Organization Compliance Assessment"
2. DESCRIPTION — e.g., "Assess the compliance status of [Org Name] according to the Cyber Resilience Act requirements."
3. ASSESSMENT LANGUAGE — heading: "Assessment Language". A language selector that controls the language of requirement questions and hints. Options include all 24 EU official languages (those without an uploaded translation appears as "Language (Not available)").
   - The selector is disabled once an assessment has been started. A note reads: "The language is locked because the assessment has already started." — Optional
4. START ASSESSMENT / CONTINUE ASSESSMENT BUTTON — proceeds to the Areas of Requirements view.

AREAS OF REQUIREMENTS VIEW

After clicking Start or Continue Assessment:

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. HEADING: "Areas of Requirements" — lists all CRA compliance areas as cards.
2. AREA CARDS — each shows:
   - The area name.
   - A counter: "X of Y assessments completed".
   - Remaining assessments count and a progress percentage.
   - A Start / Continue button for that area. Once all requirements in an area is complete, the button may show "Edit".
   - Partially- and fully-completed area cards render with visually distinct styling, not just a different progress percentage:
     - 0% (not started): white/neutral card background; button labeled "Start" (play-style icon).
     - Partially complete (>0%, <100%): pale blue card background; button labeled "Continue" (document/checklist icon).
     - Fully complete (100%): pale green card background, a green checkmark icon in the top-right corner; button changes to "Edit".

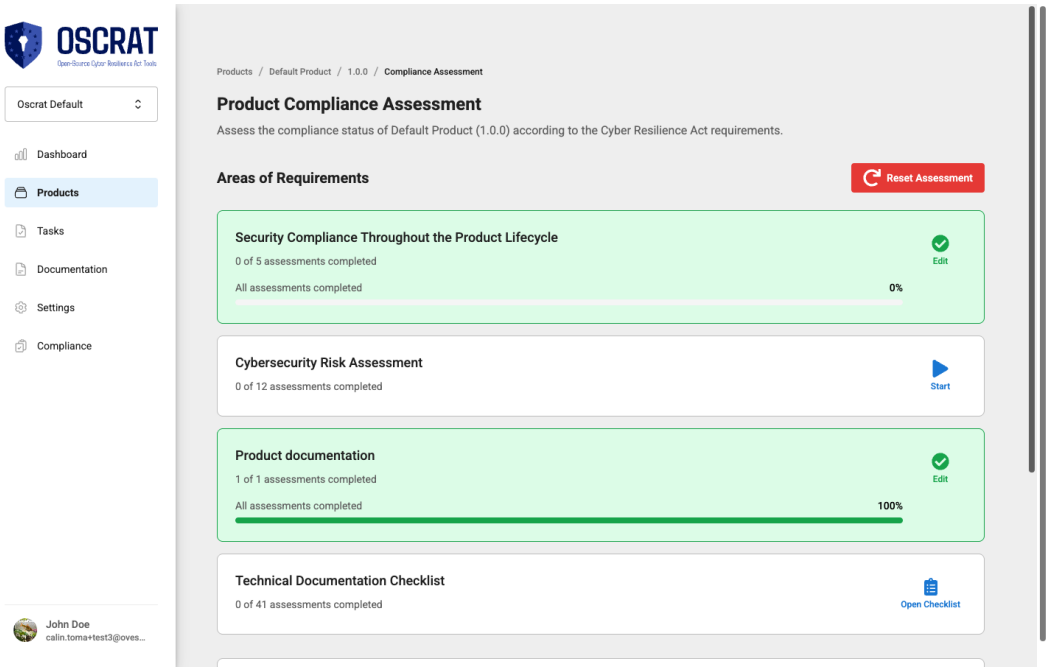

Figure 36: Compliance Assessment — Areas of Requirements view

3. RESET ASSESSMENT BUTTON
   - Opens a confirmation modal to reset all assessment progress.
   - USE WITH CAUTION — resetting deletes all answers and compliance statuses for this assessment.
4. ASSESSMENT FILES SECTION
   - Heading: "Assessment 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.

- Description: "Supporting evidence and documents uploaded for this assessment."
- ADD FILE BUTTON — opens a file picker to upload a supporting evidence document for this assessment.
- Lists all files uploaded; shows "No files added" when empty.

INSIDE A REQUIREMENT ASSESSMENT

1. HINT TEXT — a contextual paragraph displayed above each question, describing the relevant CRA regulation. Includes "References:" links to official CRA form sections.
2. QUESTION DISPLAY — the current CRA requirement question.
3. ANSWER OPTIONS — Yes/No radio buttons, or a free-text area. — Mandatory
4. PREVIOUS BUTTON — returns to the previous question.
5. NEXT BUTTON — advances to the next question (enabled after an answer is provided).
6. BACK BUTTON — returns to the Areas of Requirements view.
7. COMPLETE REQUIREMENT BUTTON — shown on the last question. Click instead of "Next" to finish the requirement and proceed to status selection.

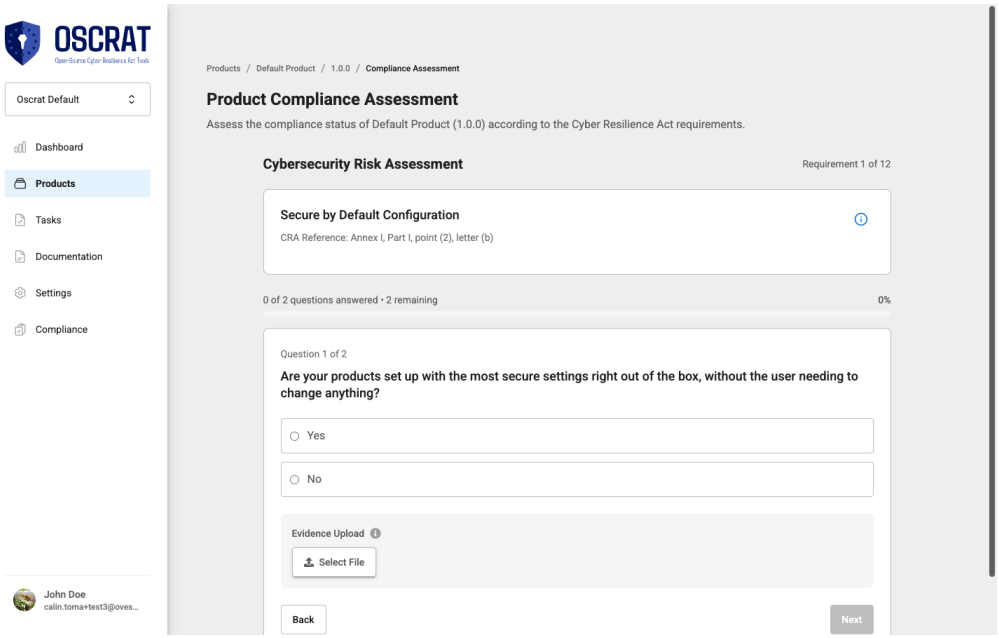

Figure 37 : Compliance Assessment — requirement question

REQUIREMENT COMPLETION — STATUS SELECTION

After clicking "Complete Requirement": Heading: "Requirement Assessment Complete" / "Select Compliance Status"

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.

Four status buttons:

a. Fully Compliant — all controls are in place. — Mandatory
b. Partially Compliant — some controls are in place, gaps remain. — Mandatory
c. Not Compliant — controls are missing or inadequate. — Mandatory
d. Not Applicable — requirement does not apply. — Mandatory

Click the appropriate status to save it and move to the next requirement.

CRA TECHNICAL DOCUMENTATION CHECKLIST (VERSION-LEVEL)

The version-level compliance assessment includes a dedicated CRA Technical Documentation Checklist with 41 checkbox items across 9 sections:

1. General Description (5 items)
2. Design, Development, Production, and Vulnerability Handling
3. (8 items)
4. Cybersecurity Risk Assessment (2 items)
5. Support Period (2 items)
6. Standards, Common Specifications, or Certification Schemes
7. (5 items)
8. Test Reports (2 items)
9. EU Declaration of Conformity (1 item)
10. Software Bill of Materials (SBOM) (2 items)
11. User Information (Annex II) (14 items)

HOW TO USE THE CHECKLIST:

1. Navigate to the version's Compliance tab.
2. Click "Start Assessment" to enter the areas view.
3. Click "Start assessment for Technical Documentation Checklist".
4. Check each item that applies by clicking its checkbox.
5. A green check icon appears next to checked items.
6. The progress counter shows "X of 41 items checked".
7. Click "Save Checklist" to persist your selections.
8. Click "Back" to return to the areas view.

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.

RESET ASSESSMENT MODAL

1. CANCEL BUTTON — closes modal without resetting.
2. RESET ASSESSMENT BUTTON — confirms the reset. A success toast notification is displayed.

COMPLIANCE STATUSES REFERENCE

- Fully Compliant — Requirement is fully met.
- Partially Compliant — Requirement is partially met.
- Not Compliant — Requirement is not met.
- Not Applicable — Requirement does not apply.

NOTES

- Progress is saved after each requirement is completed. You can leave and return to continue an assessment.
- The "All Areas Completed!" screen appears when every area is finished.
- Assessment data feeds into the Organization Dashboard charts and the Requirements Status Table.
- Resetting an assessment is irreversible.

7.2 CRA TECHNICAL DOCUMENTATION CHECKLIST

URL: /organization/{org-slug}/products/{product-id}/versions/ {version-id}/compliance

OVERVIEW

The CRA Technical Documentation Checklist is a version-level tool that helps you verify all required technical documentation items for a product version under the EU Cyber Resilience Act (CRA). It contains 41 checkbox items across 9 sections, each referencing the specific Annex of the CRA.

HOW TO REACH THE CHECKLIST

1. Open the Compliance Assessment for a product version.
2. Click "Start Assessment" to enter the Areas of Requirements view.
3. Locate the "Technical Documentation Checklist" area card (shows "X of 41 assessments completed").
4. Click "Open Checklist".

CHECKLIST PAGE ELEMENTS

1. **BACK BUTTON —** returns to Areas of Requirements view (without saving unsaved changes).
2. **HEADING:** "Technical Documentation Checklist"

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. **PROGRESS COUNTER** — "X of 41 items checked". Updates on each toggle.
4. **CHECKLIST SECTIONS AND ITEMS** — each item has:
   a. A CHECKBOX
   b. ITEM TEXT — description of the documentation requirement.
   c. ANNEX LINK — hyperlink to the specific Annex/Article in the CRA on EUR-Lex (opens in new tab). When checked: green check icon appears and text has strikethrough.
5. **SAVE CHECKLIST BUTTON** — at the bottom; persists all checked/unchecked states. Must be clicked to save — navigating away with Back without saving discards unsaved changes.

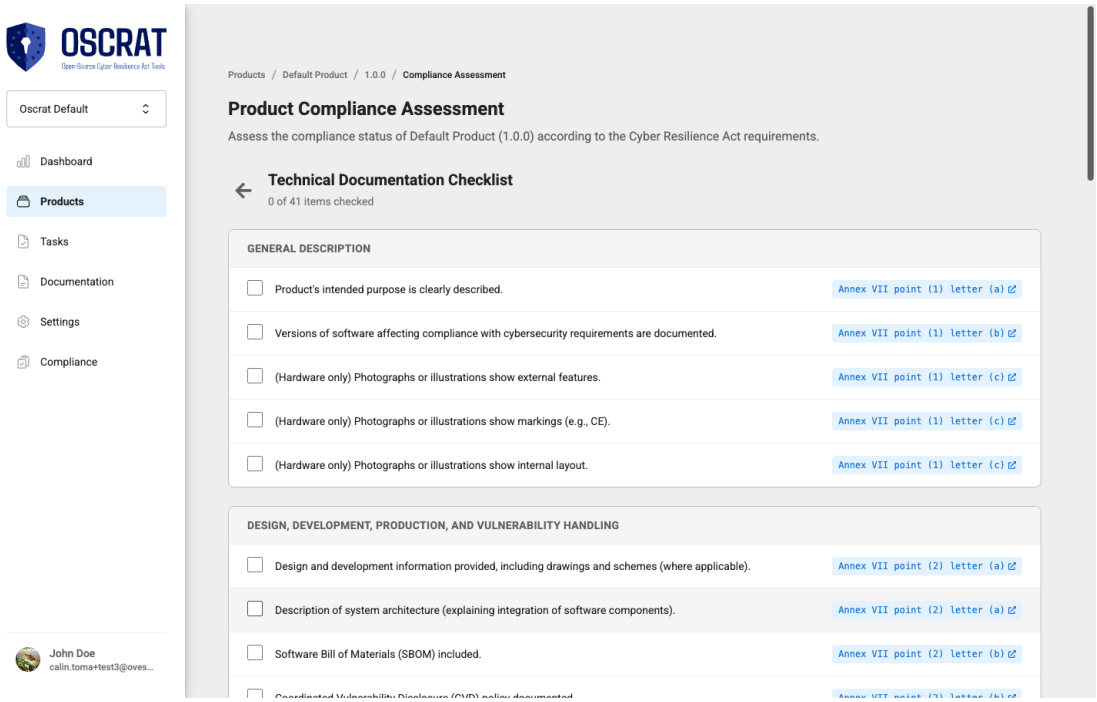

Figure 38: CRA Technical Documentation Checklist

CHECKLIST SECTIONS AND ITEMS (ALL 41)

SECTION 1 — GENERAL DESCRIPTION (5 items, Annex VII point (1))

[ ] Product's intended purpose is clearly described. — Optional [Annex VII point (1)(a)]

[ ] Versions of software affecting compliance with cybersecurity requirements are documented. — Optional [Annex VII point (1)(b)]

[ ] (Hardware only) Photographs or illustrations show external features. [Annex VII point (1)(c)] — Optional

[ ] (Hardware only) Photographs or illustrations show markings (e.g., CE). [Annex VII point (1)(c)] — Optional

[ ] (Hardware only) Photographs or illustrations show internal layout. [Annex VII point (1)(c)] — 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.

SECTION 2 — DESIGN, DEVELOPMENT, PRODUCTION, AND VULNERABILITY HANDLING (8 items, Annex VII point (2))

[ ] Design and development information provided, including drawings and schemes (where applicable). [Annex VII point (2)(a)] — Optional
[ ] Description of system architecture (explaining integration of software components). [Annex VII point (2)(a)] — Optional
[ ] Software Bill of Materials (SBOM) included. — Optional [Annex VII point (2)(b)]
[ ] Coordinated Vulnerability Disclosure (CVD) policy documented. — Optional [Annex VII point (2)(b)]
[ ] Evidence of provision of a contact address for vulnerability reporting. [Annex VII point (2)(b)] — Optional
[ ] Description of technical solutions for secure distribution of updates. [Annex VII point (2)(b)] — Optional
[ ] Production and monitoring processes described. — Optional [Annex VII point (2)(c)]
[ ] Validation of production and monitoring processes included. — Optional [Annex VII point (2)(c)]

SECTION 3 — CYBERSECURITY RISK ASSESSMENT (2 items)

[ ] Assessment of cybersecurity risks documented. — Optional [Annex VII point (3)]
[ ] Shows how essential requirements in Annex I (Part I) are applicable. [Annex VII point (3)] — Optional

SECTION 4 — SUPPORT PERIOD (2 items)

[ ] Includes justification for support period determined under Article 13(8). [Annex VII point (4)] — Optional
[ ] Information supporting how the support period was determined is documented. [Article 13(8)] — Optional

SECTION 5 — STANDARDS, COMMON SPECIFICATIONS, OR CERTIFICATION SCHEMES (5 items, Annex VII point (5))

[ ] List of harmonised standards applied (full or partial). — Optional
[ ] List of common specifications (Article 27) applied, if any. — Optional
[ ] List of European cybersecurity certification schemes applied (EUCC, EUCS, etc.), if relevant. — Optional
[ ] Description of alternative solutions used to meet Annex I requirements (if no harmonised standards applied). — Optional
[ ] Specification of parts applied when standards/specifications/ certifications are partly applied. — Optional

SECTION 6 — TEST REPORTS (2 items, Annex VII point (6))

[ ] Reports of tests carried out to verify conformity with cybersecurity requirements (Annex I Parts I & II). — Optional
[ ] Reports of tests verifying vulnerability handling processes. — 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.

SECTION 7 — EU DECLARATION OF CONFORMITY (1 item)

[ ] Copy of the EU Declaration of Conformity is included and current. [Annex VII point (7)] — Optional

SECTION 8 — SOFTWARE BILL OF MATERIALS (SBOM) (2 items, Annex VII point (8))

[ ] SBOM is prepared and available for submission to market surveillance authorities upon reasoned request. — Optional

[ ] SBOM is sufficient for verifying compliance with Annex I requirements. — Optional

SECTION 9 — USER INFORMATION (ANNEX II) (14 items)

[ ] Manufacturer's name, registered trade name/trademarks, postal address, email/digital contact, and website (if available). [Annex II point (1)] — Optional

[ ] Single point of contact for reporting vulnerabilities and access to coordinate vulnerability disclosure policy. [Annex II point (2)] — Optional

[ ] Product name, type, and any additional information for unique identification. [Annex II point (3)] — Optional

[ ] Intended purpose of the product, including provided security environment, essential functionalities, and security properties. [Annex II point (4)] — Optional

[ ] Disclosure of known or foreseeable circumstances that may lead to significant cybersecurity risks during use or foreseeable misuse. [Annex II point (5)] — Optional

[ ] Internet address at which the EU Declaration of Conformity can be accessed (if applicable). [Annex II point (6)] — Optional

[ ] Type of technical security support offered and end-date of support period for vulnerability handling and security updates. [Annex II point (7)] — Optional

[ ] Detailed instructions (or internet address) on necessary measures during initial commissioning and throughout lifetime for secure use. [Annex II point (8)(a)] — Optional

[ ] Explanation of how changes to the product may affect the security of data. [Annex II point (8)(b)] — Optional

[ ] Instructions on how security-relevant updates can be installed. [Annex II point (8)(c)] — Optional

[ ] Guidance on secure decommissioning, including how user data can be securely removed. [Annex II point (8)(d)] — Optional

[ ] Information on how the default setting for automatic installation of security updates can be turned off. [Annex II point (8)(e)] — Optional

[ ] Integration guidance: information necessary for integrators to comply with essential cybersecurity requirements (Annex I). [Annex II point (8)(f)] — 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.

[ ] Information on where the SBOM file can be accessed (if SBOM has been made available to users). [Annex II point (9)] — Optional

HOW TO USE THE CHECKLIST — STEP BY STEP

Step 1: Navigate to the Compliance Assessment for the target product version and click "Start Assessment".
Step 2: Click "Open Checklist" on the "Technical Documentation Checklist" card.
Step 3: Review each item in every section and check the items that are satisfied by clicking the checkbox. A green check icon and strikethrough text confirms the item is checked.
Step 4: Uncheck any item by clicking its checkbox again if needed.
Step 5: Click "Save Checklist" at the bottom of the page. A "Checklist saved successfully" toast appears and you are returned to the Areas of Requirements view automatically — Step 6 below is not a separate manual action in practice.
Step 6: (If you navigated elsewhere without saving) Click "Back" to return to the Areas of Requirements view.

IMPACT ON REQUIREMENTS STATUS TABLE

When all 41 items are checked and saved, the "Technical Documentation Checklist" area is automatically marked as "Evaluated" in the Requirements Status Table. Partial progress is saved but does not change the status.

NOTES

- Annex links open the official EUR-Lex publication in a new browser tab.
- Hardware-only items (Section 1, items 3–5) can be skipped for software-only products.
- Progress is not auto-saved. Always click "Save Checklist" before navigating away.

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. TASKS

8.1 ORGANIZATION TASKS PAGE

URL: /organization/{organization-slug}/tasks

OVERVIEW

The Organization Tasks page provides a centralized view of all tasks across every product and version within your organization. Tasks are work items tracking compliance actions, remediation steps, or other activities needed to meet CRA requirements.

From this page you can view, filter, create, and navigate to individual tasks.

PAGE ELEMENTS

1. **PAGE HEADING — "Tasks"**
   - Subtitle: "Add, edit, and review tasks"

2. **ADD TASK BUTTON — opens the Create Task dialog to add a new task.**

3. **FILTER BUTTONS**
   - Four filter buttons allow you to narrow down the task list, in this order:

     a. STATUS FILTER — Labeled "Status". Filter tasks by current status: — Optional To Do, Planned, In Progress, Done
     b. TYPE FILTER — Labeled "Type". Filter tasks by Task Type (Vulnerability, Incident, SBOM, Documentation, Risk, Training, Configuration Mgmt, Requirements, Other). — Optional
     c. PRODUCT FILTER — Labeled "Product". Filter tasks to show only — Optional those belonging to a specific product.
     d. VERSION FILTER — Labeled "Version". Filter tasks to show only — Optional those belonging to a specific product version.

4. **TASKS TABLE**
   - The main content is a table with the following columns, in this order:
     a. TASK
        - Displays a task type badge followed by the task title, in the format "#{id}: {title}" (e.g. "#19: Manual Other task").
        - TASK TYPE BADGE: An icon badge immediately before the task title indicating how the task was created (its origin — this is a separate concept from the Type field/column described below, which records what kind of compliance activity the task represents):
          - *"Manual" badge (orange, with icon; aria-label "Manually*

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.

- *created") — the task was created directly by a user.*
- *"Auto-generated" badge (aria-label "Automatically generated"; displayed text "Auto") — the task was created automatically*
- *by the system (e.g., from a compliance assessment or scan).*

- Clicking a task row navigates to the Task Detail page.

b. TYPE — the task's Type value: one of Vulnerability, Incident, SBOM, Documentation, Risk, Training, Configuration Mgmt, Requirements, or Other. See "TASK 'TYPE' FIELD REFERENCE" below.
c. PRODUCT — the product the task is associated with. Shows "-" when no product is linked.
d. VERSION — the product version the task is linked to. Shows "-" when no version is linked.
e. DUE DATE — target completion date (DD.MM.YYYY).
f. STATUS — a dropdown showing the current task status. You can change the status directly in the table by clicking the dropdown.

5. **PAGINATION**
   - PREVIOUS PAGE button: navigates to the prior page.
   - NEXT PAGE button: navigates to the next page.
   - Item count shown (e.g., "1–15 of 124 items").

TASK ORIGIN REFERENCE

- Manual — the task was created by a user via "Add Task". These are the most common tasks and represent deliberate compliance or remediation actions chosen by your team.
- Auto-generated — the task was created automatically by the system, for example as part of a compliance assessment workflow or triggered by a scan result.

The Task Distribution chart on the Organization Dashboard breaks down task counts by origin (Manual vs. Auto-generated) and status, providing an at-a-glance view of your team's task workload.

TASK "TYPE" FIELD REFERENCE

Every task also has a Type field, independent of its origin (Manual/Auto-generated) above. Type is selected when the task is created (or edited later) and is shown as its own column in both the Organization Tasks table and the Version Tasks tab table. The available values are:

- Vulnerability
- Incident
- SBOM
- Documentation

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 — setting a task's Type to "Risk" and saving is what activates the Risk Assessment workflow described in Section 8.3 (this replaces the former "Enable Risk Assessment" checkbox).
- Training
- Configuration Mgmt — used automatically for tasks generated from a failed Configuration Management scan rule (see Section 8.5).
- Requirements
- Other — the default value for a new task if no Type is chosen.

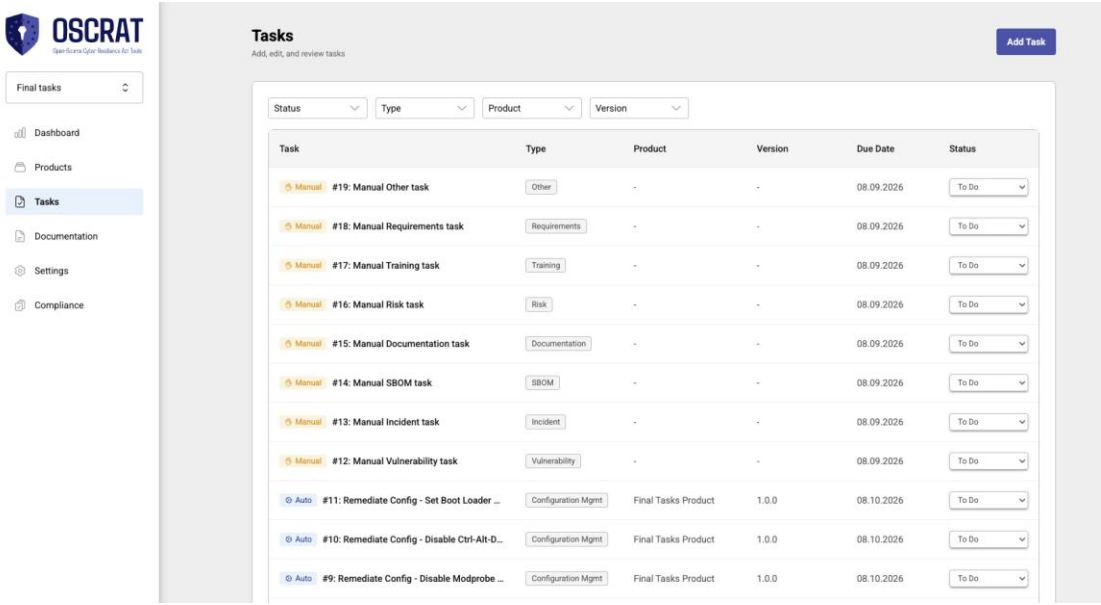

Figure 39: Organization Tasks page

CREATE TASK DIALOG

Clicking "Add Task" opens a modal dialog titled "Create Task":

1. DIALOG HEADING: "Create Task"
2. CLOSE / CANCEL BUTTON — closes the dialog without creating.
3. TITLE INPUT — Placeholder: "Enter task title" | Required. — Mandatory
4. TYPE SELECT — dropdown listing the nine Type values above (Vulnerability, Incident, SBOM, Documentation, Risk, Training, Configuration Mgmt, Requirements, Other). — Optional. Default: Other.
5. STATUS SELECT — To Do / Planned / In Progress / Done. — Optional Default: To Do.
6. PRODUCT SELECT — select the product this task is associated with. Default: "No product". –Optional
7. DUE DATE INPUT — Required. Defaults to today's date; can be changed before submitting.
8. DESCRIPTION INPUT — Optional free-text notes. — 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.

9. CREATE BUTTON — creates the task and closes the dialog. The new task appears in the table.

There is no longer an "Enable Risk Assessment" checkbox in this dialog. To create a task that will use the Risk Assessment workflow, select Type = "Risk" here (or set it later on the Task Detail page and save) — see Section 8.3.

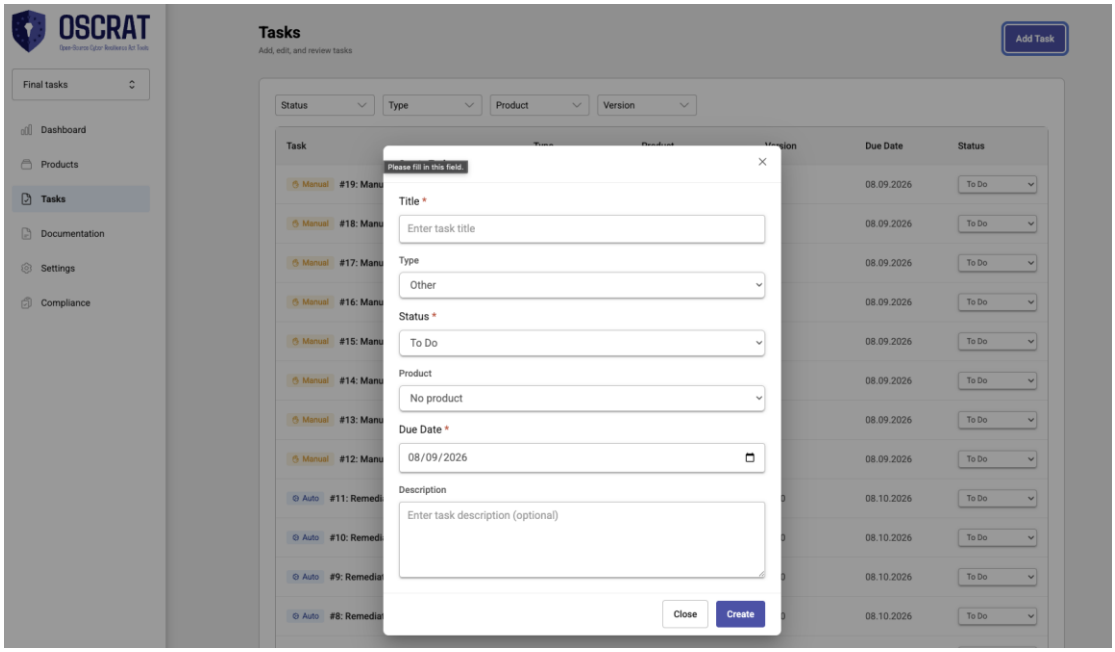

Figure 40: Create Task dialog

HOW TO CREATE A TASK — STEP BY STEP

Step 1: Navigate to /organization/{org-slug}/tasks.
Step 2: Click "Add Task". The Create Task dialog opens.
Step 3: Enter a task title.
Step 4: (Optional) Select a Type other than the default "Other".
Step 5: (Optional) Select a status other than "To Do".
Step 6: Select the product this task belongs to.
Step 7: Enter or update the due date (defaults to today's date).
Step 8: (Optional) Add a description.
Step 9: Click "Create". The task appears in the table.

HOW TO VIEW TASK DETAILS

1. Locate the task in the table (use filters or pagination if needed).
2. Click anywhere on the task's row.
3. You are navigated to the Task Detail page (/organization/{slug}/tasks/{task-id}).

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.

HOW TO CHANGE A TASK STATUS INLINE

1. Locate the task in the table.
2. Click the status dropdown in the task's row.
3. Select the new status. The change is saved immediately.

TASK STATUS REFERENCE

- To Do — Work has not yet started.
- Planned — Work is scheduled but not started.
- In Progress — Work is actively underway.
- Done — Work has been completed.

NOTES

- Tasks can also be created and viewed from within a specific version's Tasks tab on the Version Detail page.
- Due dates are displayed in DD.MM.YYYY format.
- Use the Status, Type, Product, and Version filters to focus on tasks relevant to a specific release.
- All tasks (both Manual and Auto-generated) appear in this list. Use filters to narrow the view.

8.2 TASK DETAIL PAGE

URL: /organization/{organization-slug}/tasks/{task-id}

OVERVIEW

The Task Detail page displays the full information for a single task and allows you to edit its properties. Navigate here by clicking a task row from either the Organization Tasks page or the Version Tasks tab.

PAGE ELEMENTS

1. **BREADCRUMB NAVIGATION**
   - Shows: Tasks / #{id}: {task title}.
   - Click "Tasks" to return to the Organization Tasks page.
2. **PAGE HEADING — "Task Details" followed by the task's numeric ID (e.g. "Task Details #16").**
3. **TASK FIELDS (left panel), in this order:**
   a. TASK NAME INPUT — shows the current task title.
   Required. — Mandatory
      - For manually created tasks, click to edit. For auto-generated tasks, this field is read-only and cannot be renamed.
   b. ORIGIN FIELD (read-only)
      - Label: "Origin"

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.

- Shows how the task was created:
  - "Manually created" (with icon) — task was created by a user.
  - "Auto-generated" (with icon) — task was created by the system.
- This field cannot be edited.

c. ORGANIZATION FIELD (read-only)
   - Label: "Organization"
   - Shows the organization the task belongs to.

d. DUE DATE INPUT — target completion date (YYYY-MM-DD). Click to edit. Optional. — Optional
e. TYPE SELECT — dropdown to set the task's Type. Same nine values as the Create Task dialog (Vulnerability, Incident, SBOM, Documentation, Risk, Training, Configuration Mgmt, Requirements, Other). Setting this to "Risk" and clicking "Save Changes" activates the Risk Assessment workflow — see Section 8.3. — Optional

f. STATUS SELECT — dropdown showing the current status. Click to change. — Optional Available statuses and internal values:
   - To Do (internal: TODO)
   - Planned (internal: PLANNED)
   - In Progress (internal: IN_PROGRESS)
   - Done (internal: DONE)

g. ASSIGNEE SELECT — dropdown to assign the task to an organization member. Optional. — Optional

h. DESCRIPTION INPUT — free-text notes. Click to edit. Optional. — Optional

There is no longer an "Enable Risk Assessment" checkbox on this page.

4. SAVE CHANGES BUTTON

- Saves any edits made to the task fields above (name, due date, type, status, assignee, description).
- Disabled until a field has been modified.

5. INFORMATION TABS (bottom panel)

- TAB: Documentation — lists documentation entries linked to this task. Includes a "Link Documentation" button
  a. SELECT DOCUMENTATION DROPDOWN — Mandatory. Placeholder "Select documentation...". Lists every documentation entry in the organization by title — both version-scoped and

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-scoped entries appear together in one flat list, not filtered to this task's linked product/version.

b. LINK BUTTON — disabled until a documentation entry is selected; once enabled and clicked, links the selected entry to this task and closes the picker.

c. CANCEL BUTTON — closes the picker without linking anything. This mirrors the "Link a Task" flow on the Documentation editor page (§9.1 / §6.1) — the two linking flows are the inverse of each other (Task → Documentation here; Documentation → Task in §9.1).

- Linking and unlinking documentation from this tab is individually recorded in the Audit Log ("Linked documentation" / "Unlinked documentation").

- TAB: Comments — add and view comments on this task. Elements:
  a. NEW COMMENT LABEL — "New Comment"
  b. NEW COMMENT TEXTAREA — placeholder "New Comment". — Mandatory
  c. ADD COMMENT BUTTON — disabled until the textarea has content; submits the comment and clears the textarea.
  d. COMMENT LIST — shows "No comments yet." when empty. Each posted comment displays as a card with Author Name (e.g., "John Doe"), Timestamp (e.g., "15 July 2026 at 17:27"), and the comment text. Comment text is rendered as plain text (HTML/script content is escaped, not executed).
- Unlike the Documentation and Attachments tabs, posting a comment is NOT currently recorded in the Audit Log — there is no "Comment" audit-log entity.
- TAB: Attachments — upload and manage file attachments for this task. Elements:
  a. UPLOAD AREA — a dashed drop zone with an upload icon and the text "Click to upload or drag and drop"; supports both click and drag-and-drop. No file-type or file-size restriction text is shown here (contrast with the Vulnerability Details page's Attachments section, §6.7, which does show "Max file size" and "Allowed types" text). A "File uploaded successfully" toast appears after a successful upload.
  b. ATTACHMENTS LIST — shows "No attachments" when empty. Each uploaded file displays as a row with File Name; File Size, MIME Type, and Uploader on one line (e.g., "0.0 KB · application/octet-stream · John Doe"); a Download button; and a Delete button that removes the attachment immediately (with a "Attachment deleted successfully" toast and no confirmation dialog).
- Upload, download, and delete are all individually recorded in the Audit Log ("Uploaded attachment", "Downloaded attachment", "Deleted attachment").

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.

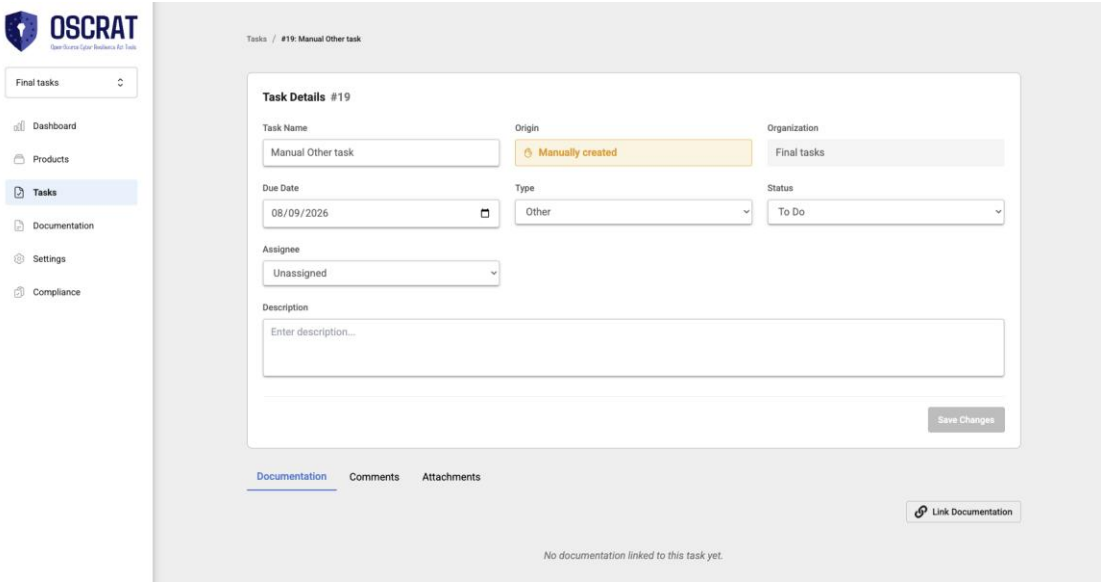

Figure 41: Task Detail page

HOW TO EDIT A TASK

Changing the Task Name:

1. Click on the Task Name field (manually created tasks only — this field is read-only for auto-generated tasks).
2. Type the new name.
3. Click "Save Changes".

Setting the Type:

1. Click the "Type" dropdown.
2. Select the new Type.
3. Click "Save Changes". If Type is set to "Risk", the Risk Details and Risk Treatment sections appear below once the save completes — see Section 8.3.

Updating the Status:

1. Click the "Status" dropdown.
2. Select the new status.
3. Click "Save Changes".

Setting or Updating the Due Date:

1. Click "Due Date".
2. Enter or select the new date (YYYY-MM-DD format).
3. Click "Save Changes".

Assigning the Task:

1. Click the "Assignee" dropdown.
2. Select an organization member.
3. Click "Save Changes".

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.

NOTES

- Tasks can also be updated inline from the task table on the Organization Tasks page or Version Tasks tab.
- The "Origin" field is system-controlled and cannot be edited.
- To enable the Risk Assessment feature, set the Type field to "Risk" and click "Save Changes" — see Section 8.3.

8.3 RISK ASSESSMENT TASK

URL: /organization/{org-slug}/tasks/{task-id} (Risk Assessment fields appear on the Task Detail page)

OVERVIEW

OSCRAT supports structured risk assessments for assets, processes, or information systems. A Risk Assessment is activated by setting a task's Type field to "Risk" on the Task Detail page and clicking "Save Changes" — this can be done at creation time (by selecting Type = "Risk" in the Create Task dialog) or at any later point on an existing task. Once the task's Type is saved as "Risk", two additional sections appear beneath the standard task fields:

Section 1 — Risk Details

Captures the asset, threat description, affected categories, likelihood, impact, and the calculated exposure score.

Section 2 — Risk Treatment

Records the chosen treatment option, mitigation measures, residual exposure, and the person responsible for implementing measures.

Section 2 cannot be filled until all mandatory fields in Section 1 have been completed and saved.

All risk data is linked to the task's Product, giving a single location to track decisions and mitigation measures throughout the product lifecycle.

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.

MANDATORY FIELDS SUMMARY

SECTION 1 — RISK DETAILS

Field	***Required?***
Asset	Not directly editable — read-only, auto-populated from the task's linked Product (see field description below).
Owner	Yes — must select an organisation member
Likelihood	Yes — Low / Medium / High
Impact	Yes — Low / Medium / High
Exposure	Auto-calculated (read-only, not entered)
Category	Yes — at least one checkbox required
Threat	Yes — free-text description required

All fields must be complete (Asset populated via a linked Product, and the remaining fields filled in) before Section 2 unlocks. Partial saves do not unlock Section 2.

SECTION 2 — RISK TREATMENT

Field	***Required?***
Treatment	Yes — Accept / Reduce / Avoid / Transfer
Residual Exposure	Yes — Low / Medium / High
Responsible	Yes — must select an organisation member
Measures	Conditional — required when Treatment is Reduce; optional otherwise

HOW TO CREATE A RISK ASSESSMENT TASK

Step 1: Navigate to the Organization Tasks page (/organization/{org-slug}/tasks) or the Version Tasks tab of a specific product version.
Step 2: Click "Add Task".
Step 3: Enter the task title (required) and optionally set the Type to "Risk", a status, due date, and description. Select the Product (and Version if applicable) — this is what the Asset field in Risk Details will later be populated from.
Step 4: Click "Create". The dialog closes and the new task appears in the tasks table.
Step 5: Click the task row to open the Task Detail page.
Step 6: If Type was not already set to "Risk" in Step 3, select "Risk" in the Type dropdown on the detail page and click "Save Changes". Section 1 — Risk Details appears below the task fields.

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.

SECTION 1 — RISK DETAILS

Fields displayed once the task's Type is saved as "Risk". All fields are mandatory (Asset is read-only — see below).

1. **ASSET — Mandatory, read-only**
   - A disabled, read-only text field automatically populated with the name of the product linked to this task (the Product field set on the main task fields, or in the Create Task dialog).
   - Shows "No product linked to this task" if no product is linked to the task.
   - Cannot be edited directly in Risk Details — to change it, update the task's Product field and save, which updates Asset automatically.

2. **OWNER — Mandatory**
   - A dropdown listing members of the organisation.
   - Select the user responsible for managing this risk.

3. **LIKELIHOOD — Mandatory**
   - Dropdown: Low / Medium / High
   - How probable is it that the threat materialises?

4. **IMPACT — Mandatory**
   - Dropdown: Low / Medium / High
   - What is the magnitude of harm if the risk occurs?

5. **EXPOSURE (auto-calculated, read-only)**
   - Automatically derived from Likelihood × Impact using the Risk Level Matrix (see below).
   - Displays "—" until both Likelihood and Impact are selected.
   - Updates immediately when Likelihood or Impact changes. No manual entry is required.

6. **CATEGORY — Mandatory (at least one must be checked)**
   - Multiple checkboxes (select one or more):
     - Confidentiality — risk of data exposure — Mandatory (at least one in this group required)
     - Integrity — risk of data modification — Mandatory (at least one in this group required)
     - Availability — risk of service disruption — Mandatory (at least one in this group required)
   - At least one category must be selected.

7. **THREAT — Mandatory**
   - A long-text textarea. Placeholder: "Describe the threat in detail..."
   - Describe the threat: what could happen, how it could be exploited, and the potential source.

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.

- Example: "Unauthorised access to customer data via an unprotected API endpoint."

After all Section 1 fields are saved, Section 2 becomes available.

RISK LEVEL MATRIX

Use the following table to understand how Exposure is derived. OSCRAT calculates it automatically; this table is provided as a reference.

Likelihood \ Impact	**Low**	**Medium**	**High**
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium

Exposure thresholds:

High (H) — Urgent action required
Medium (M) — Planned action recommended
Low (L) — Monitoring only

SECTION 2 — RISK TREATMENT

Visible only after all mandatory Section 1 fields are complete and saved. Fields remain disabled (greyed out) until Section 1 is saved. The section shows the message "Complete all Risk Details fields to unlock Risk Treatment" while locked.

1. **TREATMENT — Mandatory**
   - Dropdown:
     - Accept — Management accepts the risk as-is.
     - Reduce — Mitigation measures will be or have been implemented.
     - Avoid — Stop the activity that causes the risk.
     - Transfer — Shift the risk to another entity (e.g., via insurance or contract).

2. **RESIDUAL EXPOSURE — Mandatory**
   - Dropdown: Low / Medium / High
   - The expected exposure level after the chosen treatment is applied.
   - Should be lower than the initial Exposure when Treatment is Reduce or Avoid.

3. **RESPONSIBLE — Mandatory**
   - Dropdown listing organisation members.
   - Select the user accountable for implementing the treatment measures.
   - Can be the same as or different from the Owner in Section 1.

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. **MEASURES (optional / conditional) — Mandatory (only when Treatment is Reduce)**
   - A long-text textarea. Placeholder: "Describe actions to reduce risk..."
   - Describe the specific actions taken or planned to reduce or eliminate the risk.
   - Required when Treatment is "Reduce"; recommended for "Avoid" and "Transfer" to document rationale.
   - Example: "Implement rate limiting and OAuth 2.0 on the affected API endpoint."

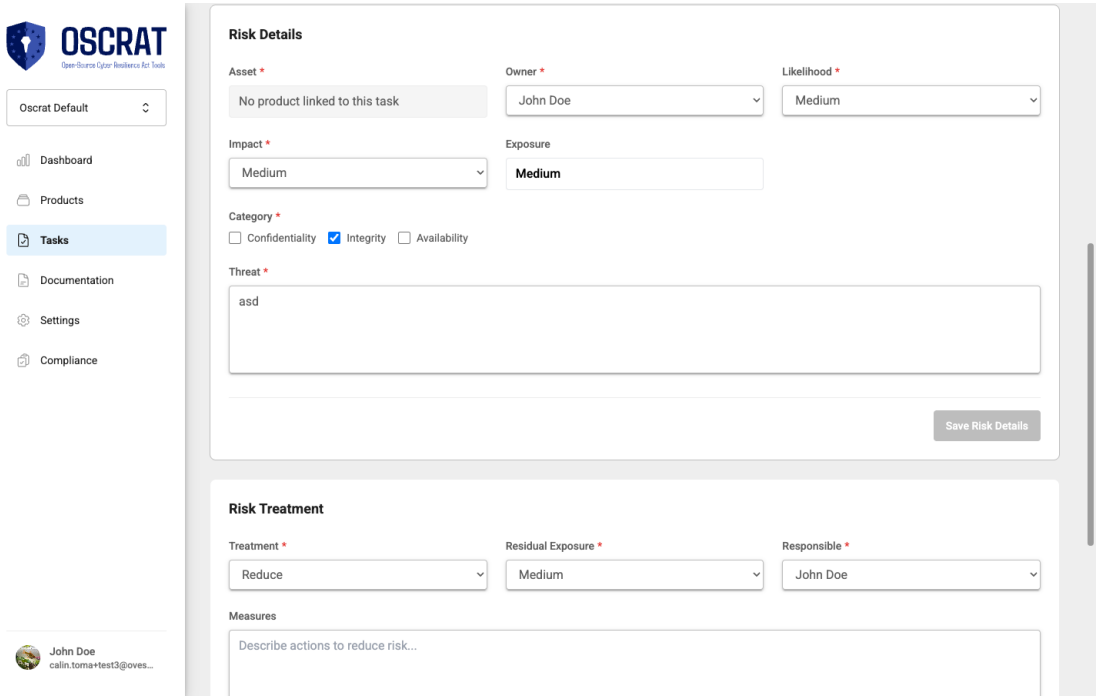

Figure 42: Risk Assessment — Risk Details & Risk Treatment

HOW TO COMPLETE A FULL RISK ASSESSMENT

Step 1: Open the task, set Type to "Risk", and click "Save Changes". Section 1 — Risk Details appears.

Step 2: Confirm the Asset field shows the correct product — it is read-only and auto-populated from the task's linked Product. (Link a product to the task first, via the Product field on the main task fields, if Asset shows "No product linked to this task".)

Step 3: Select the Owner responsible for managing the risk.

Step 4: Select Likelihood (Low / Medium / High).

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.

Step 5: Select Impact (Low / Medium / High). OSCRAT immediately calculates and shows the Exposure score.

Step 6: Check one or more Category options (Confidentiality / Integrity / Availability).

Step 7: Enter a detailed Threat description in the textarea.

Step 8: Click "Save Risk Details". Section 2 — Risk Treatment becomes visible and editable.

Step 9: Select a Treatment option (Accept / Reduce / Avoid / Transfer).

Step 10: Select Residual Exposure — the expected exposure level after treatment is applied.

Step 11: Select the Responsible person who will implement the treatment measures.

Step 12: (If Reduce) Enter Measures describing the mitigation actions.

Step 13: Click "Save Risk Treatment". The risk assessment is now complete. Update the task Status to reflect progress: To Do → Planned → In Progress → Done

TASK STATUS REFERENCE

Status Label	***Internal Value***
To Do	TODO
Planned	PLANNED
In Progress	IN_PROGRESS
Done	DONE

Update the task Status manually as work progresses. Status can be changed from the Task Detail page or inline from the task table.

NOTES

- Risk Assessment is activated by setting the task's Type field to "Risk" on the Task Detail page and clicking "Save Changes" — there is no separate "Enable Risk Assessment" checkbox.
- Asset is read-only and requires a product to be linked to the task via the task's Product field — it cannot be set directly in Risk Details. If Asset shows "No product linked to this task", set the task's Product field (Step 3 of creating the task, or edit it later on the Task Detail page) and save; Asset updates automatically.

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.

- Exposure is read-only and recalculated automatically whenever Likelihood or Impact changes.
- Section 2 fields remain disabled until every mandatory field in Section 1 has been completed and saved.
- All risk assessment data is stored alongside the task and is visible to all organisation members with access to the task.
- Risk tasks follow the same status workflow as all other OSCRAT tasks.
- Risk tasks created from the Tasks page are visible on both the Organisation Tasks page and the Version Tasks tab (if linked to a version).

8.4 SECURITY AWARENESS TRAINING TASK

URL: /organization/{organization-slug}/tasks/{task-id} (Auto-generated; no creation URL — the task appears automatically)

OVERVIEW

When a user joins or creates a new organization in OSCRAT, the system automatically generates a Security Awareness Training task and assigns it to that user. This task serves as a prompt to complete onboarding security awareness training within the organization.

The task is created without any manual action. It appears in the Organization Tasks page as soon as the new organization is set up, with a due date approximately one month from the creation date.

TASK PROPERTIES

Field	***Value***
Origin	Auto-generated (cannot be changed)
Type	Training (pre-set; can be changed manually like any other task)
Assignee	The user who joined or created the organization
Status	To Do (default; update as work progresses)
Due Date	Approximately one month from organization creation (pre-filled; can be updated on the Task Detail page)

HOW TO FIND AND COMPLETE THE TASK

Step 1: After joining or creating an organization, navigate to the Organization Tasks page (/organization/{slug}/tasks).
Step 2: The Security Awareness Training task appears in the task list, assigned to you, with status "To Do" and Type "Training".
Step 3: Click the task row to open the Task Detail 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.

Step 4: Review the task description and complete the required training steps within your organization.
Step 5: Update the Status as you progress: To Do → Planned → In Progress → Done.
Step 6: Click "Save Changes" to persist any status or field updates.

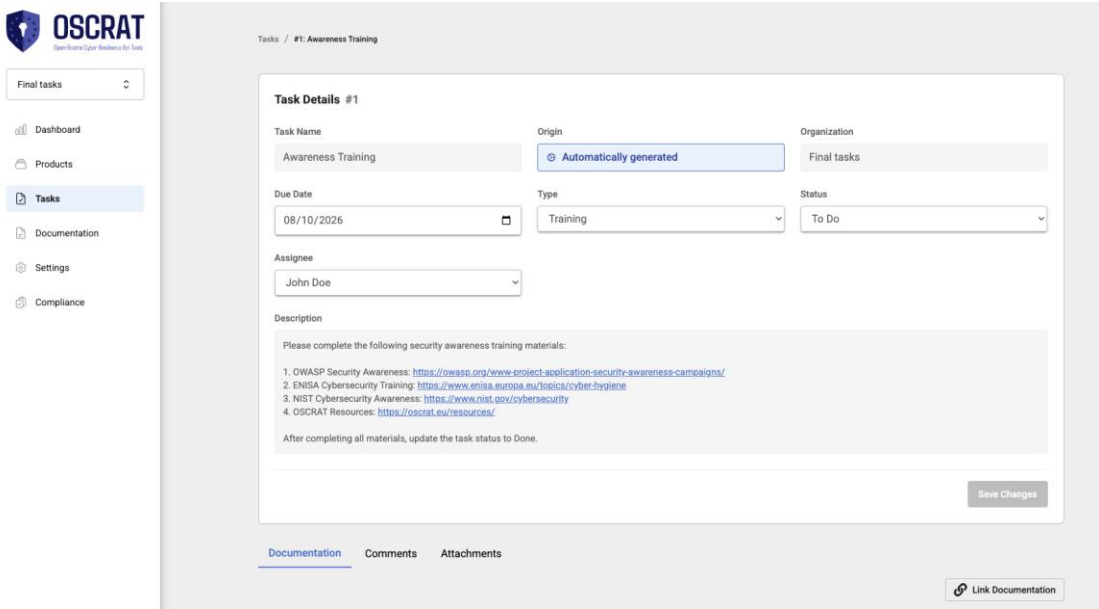

Figure 43: Security Awareness Training task

NOTES

- This task is created automatically — one task per user per new organization. It cannot be suppressed.
- The due date is pre-set but can be updated from the Task Detail page.
- The task appears on the Organization Tasks page and behaves identically to any other task: it can be assigned, have comments added, and its status updated inline or from the detail page.

8.5 AUTO-GENERATED COMPLIANCE OBLIGATION TASKS

URL: /organization/{organization-slug}/tasks (list)/organization/{organization-slug}/tasks/{task-id} (detail)

OVERVIEW

8.4 documents exactly one auto-generated task type: Security Awareness Training, created once per user per new organization. In the live application, OSCRAT also auto-generates a family of CRA compliance-obligation tasks — at both the organization level and the per-product-version level — which represent the core CRA obligations being tracked. This is distinct from, and in addition to, the Security Awareness Training task. A further, separately-triggered category of

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.

auto-generated tasks comes from Configuration Management scans — see below.

VERSION-LEVEL AUTO-GENERATED TASKS

HOW THESE TASKS APPEAR — STEP BY STEP

Step 1: Create a new product version (or, for [IO1]/[IO2], simply have an active organization).
Step 2: Navigate to the Organization Tasks page (/organization/{slug}/tasks).
Step 3: The auto-generated compliance obligation tasks appear in the list with the "Auto" badge, already populated with a due date, status "To Do", and a pre-filled description.
Step 4: Treat and update these tasks like any other task (§8.1/§8.2) — assign an owner, change status, add comments/attachments, or set Type to "Risk" to enable Risk Assessment (§8.3) as needed.

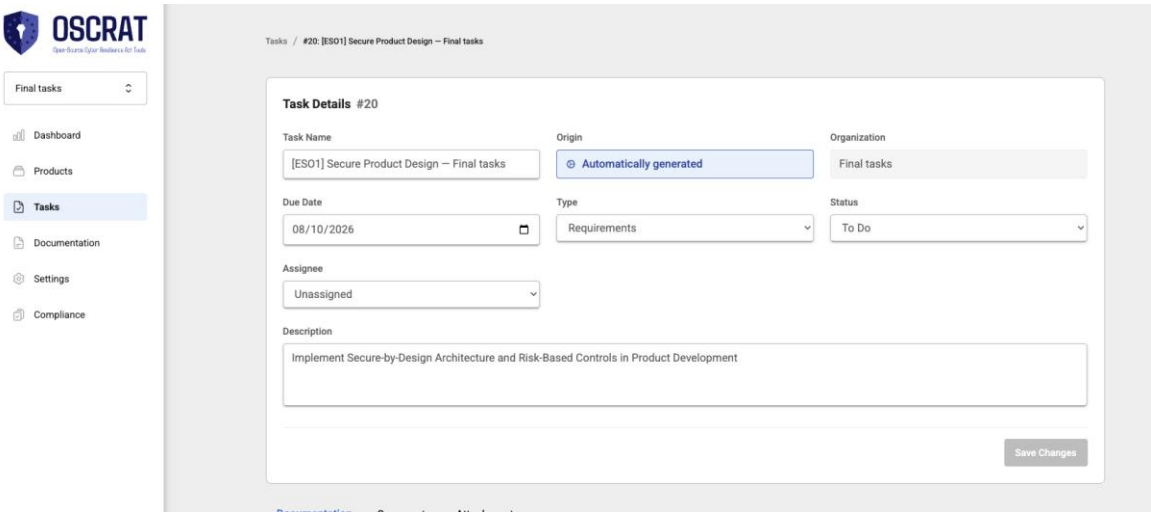

Figure 44: Auto-generated compliance obligation task

NOTES

- These tasks appear to represent the core CRA obligations tracked per product version (technical documentation, CE marking, EU Declaration of Conformity, accompanying information, support period) and per organization (compliance assurance procedures, informing procedures).

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.

8.6 CONFIGURATION MANAGEMENT SCAN-TRIGGERED TASKS

OVERVIEW

When an OpenSCAP configuration scan is processed on the Configuration Management tab of a Version Detail page, OSCRAT automatically creates one task for every rule that fails the scan. There is no manual "Create Task" step for this — task creation is fully automatic, triggered directly by the scan result.

TASK PROPERTIES

Field	*Value*
Origin	Auto-generated
Type	Configuration Mgmt
Title	"Remediate Config - {rule title}", e.g. "Remediate Config - Set Boot Loader Password in grub2"
Product / Version	The product and version the scan was run against
Status	To Do (default; update as work progresses)

HOW TO VIEW A SCAN-TRIGGERED TASK

Step 1: Open the version's Configuration Management tab and view a processed scan's Configuration Scan Report.
Step 2: In the Rules table, locate a failed rule. A "View Task" button appears in that rule's row.
Step 3: Click "View Task" to navigate directly to the auto-created task's Task Detail page.
Step 4: The task is also visible in the Organization Tasks page and in the version's Tasks tab, like any other task, with Type "Configuration Mgmt".

NOTES

- "View Task" appears for any rule that currently has, or has ever had, an associated task — including a rule that later starts passing on a re-scan. Rules that have never failed show no button at all.
- These tasks can be assigned, commented on, have attachments added, and have their Type changed to "Risk" to additionally track them as a risk, exactly like any other 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.

9. DOCUMENTATION

9.1 DOCUMENTATION PAGE

LIST URL: */organization/{organization-slug}/documentation*
DETAIL URL: */organization/{organization-slug}/documentation/{doc-id}*

OVERVIEW

The Documentation section allows you to create, manage, and publish technical documentation for your organization and its product versions. Documentation can cover CRA conformity guides, process descriptions, policies, or any written content relevant to CRA compliance.

Documentation entries can be:

- Scoped to the organization or to a specific product version.
- Set to Draft or Published status.
- Made public (accessible via a public URL without login) or kept private.
- Linked to tasks for traceability.

DOCUMENTATION LIST PAGE

1. **PAGE HEADING — "Documentation"**
2. **ADD DOCUMENTATION BUTTON — opens the Create Documentation dialog (Step 1).**
3. **FILTER BUTTONS:**
    a. STATUS FILTER — Draft or Published. — Optional
    b. LEVEL FILTER — Organization-level or Version-level. — Optional
4. **DOCUMENTATION TABLE — columns:**
    a. TITLE — document title (version-level docs show product/version name as a subtitle)
    b. LEVEL — "Organization" or "Version"
    c. STATUS — "Published" or "Draft" badge
    d. VISIBILITY — "Public" or "Private"
    e. UPDATED — last updated date (DD.MM.YYYY) Clicking any row navigates to that document's detail/editor 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.

5. **PAGINATION — Previous / Next buttons with item count.**

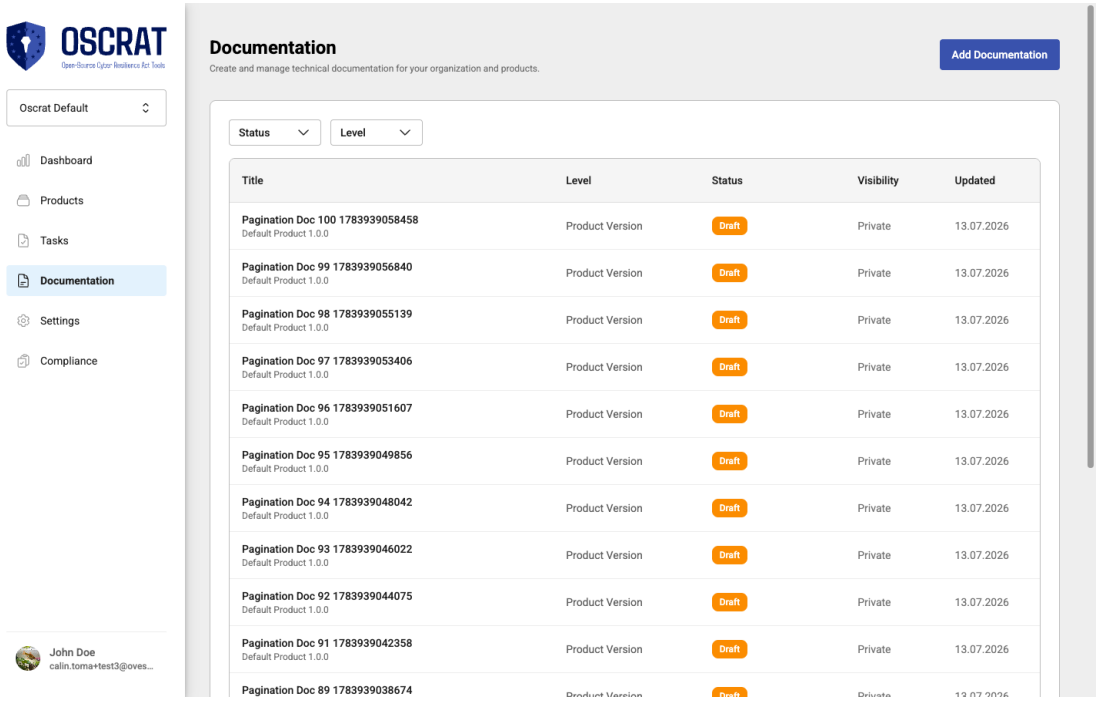

Figure 45: Documentation page

CREATE DOCUMENTATION DIALOG (Step 1)

a. LEVEL DROPDOWN — Organization or Version. — Mandatory
b. TEMPLATE DROPDOWN — pre-built template or blank document. — Mandatory
c. CANCEL BUTTON — closes without creating.
d. NEXT BUTTON — advances to Step 2 (title, content, visibility).

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.

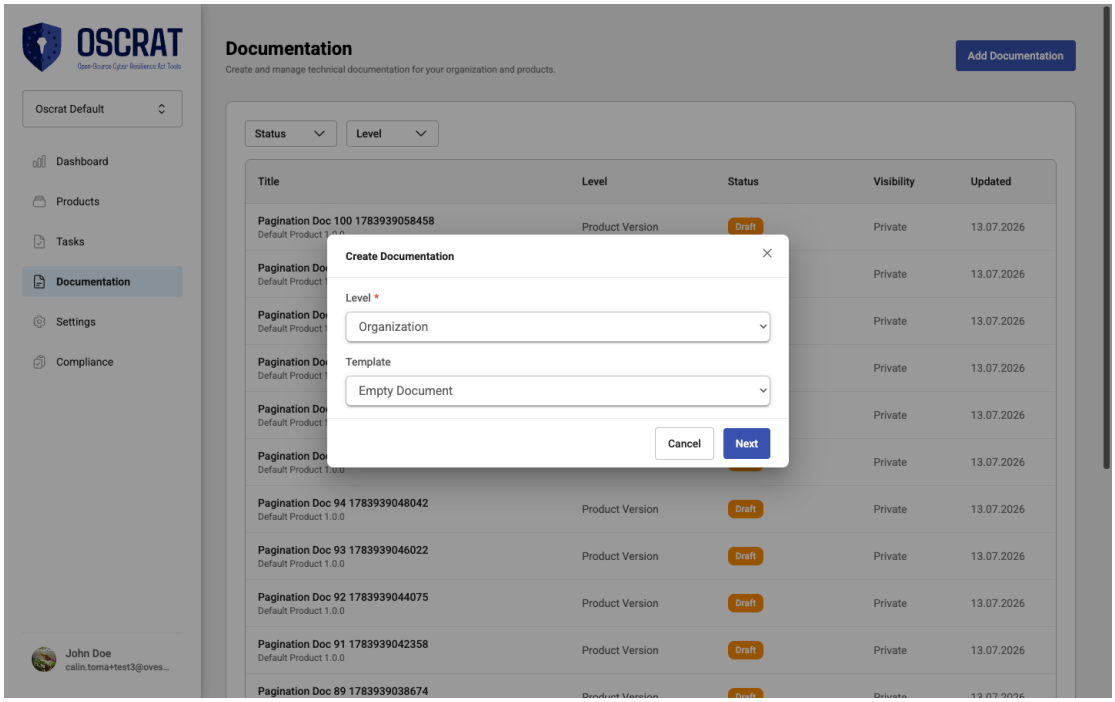

Figure 46: Create Documentation dialog

DOCUMENTATION DETAIL / EDITOR PAGE

1. **BREADCRUMB NAVIGATION — Documentation / Document Title.**
2. **DOCUMENT HEADER**
   a. DOCUMENT TITLE (heading)
   b. DOCUMENTATION VERSION — current revision number.
   c. VERSION: labels next to the title.
   d. This counter increments by 1 every time "Save Changes" is clicked — not only on content edits. Toggling Status to Published and checking the "publicly accessible" Visibility box, then clicking Save, was enough to advance the counter from "Documentation Version: 1" to "Documentation Version: 2". This also updates the "Version {N}" label shown on the public view page (see item 5 below).
3. **ACTION BUTTONS**
   a. ARCHIVE BUTTON — archives the document (preserves content but moves it out of the active list).
   b. DELETE BUTTON — permanently deletes the document. Warning: "This action cannot be undone. All content and linked tasks will be unlinked."
4. **METADATA FIELDS**
   a. TITLE INPUT — read-only in view mode. — Mandatory
   b. STATUS DROPDOWN — Draft or Published. — Mandatory
   c. VISIBILITY CHECKBOX — "Make this documentation publicly accessible". When checked, accessible via a public URL without login. — 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.

5. **PUBLIC URL SECTION (shown when Visibility is set to Public)**
- Displays the full public URL.
- COPY URL BUTTON — copies the URL to clipboard.

6. **CONTENT EDITOR — rich markdown editor. Supports headings, bold, italic, bullet lists, numbered lists, and other markdown formatting. — Optional**
   a. UNDO / REDO — standard undo/redo controls.
   b. BLOCK TYPE DROPDOWN — select the current block's type (e.g., paragraph, heading level).
   c. BOLD / ITALIC / UNDERLINE — text formatting toggles.
   d. LIST TOGGLE GROUP — Bulleted list / Numbered list / Check list.
   e. CREATE LINK BUTTON — inserts a hyperlink at the cursor.
   f. Three further icon-only toolbar buttons sit between "Create Link" and the view-mode toggle.
   g. VIEW MODE TOGGLE GROUP — "Rich text" (WYSIWYG editing) / "Diff mode" (view changes against a prior revision) / "Source mode" (edit the raw markdown directly).

7. **LINKED TASKS SECTION**
- Heading: "Linked Tasks"
- Lists tasks linked to this document.
- Note: "Linked tasks are not shown on the public view."
- A "Create Task" dialog can be opened to link a new task.
   a. "LINK A TASK" DROPDOWN — placeholder "Select a task to link..."; lists every task in the organization by ID and title that is NOT already linked to this document (already-linked tasks are excluded).
   b. LINK BUTTON — links the selected task. On success, a "Task linked successfully" toast appears, the task is added to the list below, and it is removed from the dropdown's option list.
   c. NEW TASK BUTTON (labeled "+ New Task") — this is the button behind "A 'Create Task' dialog can be opened to link a new task" above. Opens the CREATE TASK DIALOG detailed below.
   d. LINKED TASK ROW — each linked task is a clickable link to its Task Detail page, formatted "#{id}: {title} ({status})", followed by an unlink action shown as a red "×" icon (accessible name "Unlink this task"). Clicking it removes the task from this document's linked list immediately (no confirmation dialog), and the task reappears as an option in the "Link a Task" dropdown.

CREATE TASK DIALOG (from Linked Tasks):

- Same fields as the standard Create Task dialog.
- CLOSE BUTTON — cancels.
- CREATE BUTTON — creates and links the 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.

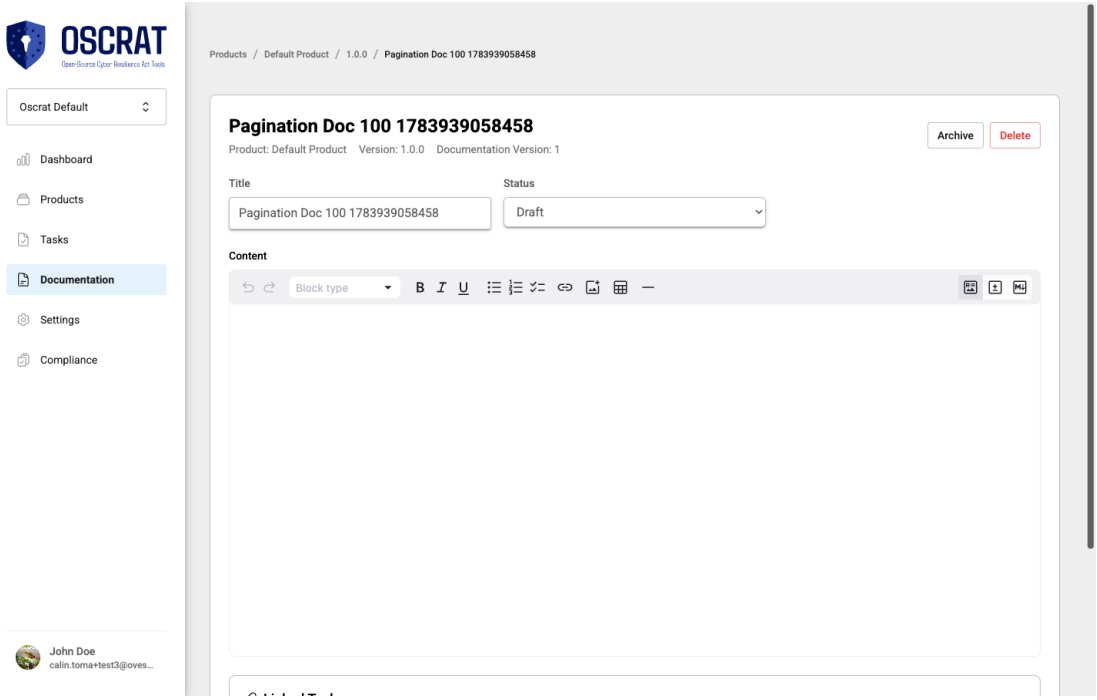

Figure 47: Documentation detail/editor page

HOW TO CREATE A DOCUMENTATION ENTRY

Step 1: Navigate to /organization/{slug}/documentation.
Step 2: Click "Add Documentation".
Step 3: Select the Level (Organization or Version) and optionally a Template.
Step 4: Click "Next" and fill in the title and initial content.
Step 5: Set the Status (Draft or Published) and Visibility.
Step 6: Save the document.

HOW TO PUBLISH A DOCUMENT AND SHARE THE PUBLIC URL

Step 1: Open the document from the list.
Step 2: Set Status to "Published".
Step 3: Check "Make this documentation publicly accessible".
Step 4: Copy the URL shown in the "Public URL" field.
Step 5: Share the URL with external stakeholders. They can view the document without logging in.

HOW TO LINK A TASK TO A DOCUMENT

Step 1: Open the document detail page.
Step 2: Scroll to the "Linked Tasks" section.
Step 3: Click the button to create a new 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.

Step 4: Fill in the task details and click "Create". The task appears in the Linked Tasks list and is also visible on the Org Tasks Page.

NOTES

- Archived documents are not permanently deleted but are hidden from the default list view.
- Public documents are visible to anyone with the URL, without login.
- Linked tasks are intentionally excluded from the public view to avoid exposing internal work items.
- Documentation at the "Version" level is also accessible from the Documentation tab on the relevant Version Detail 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.

OSCRAT

Open-Source Cyber Resilience Act Tools

OSCRAT – User manual

www.oscrat.e

https://www.linkedin.co

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.