CURIUM
CONTINUUM

CAC
Conformity Assessment & Compliance

User manual for Curium Continuum application — CAC Tool

CAC intro

The Conformity Assessment and Compliance (CAC) Tool supports SMEs in ex-ante compliance activities and helps them meet emerging market expectations. It provides an automated self-assessment process with visual guidance, allowing users to clearly understand the requirements and identify potential gaps.

The tool also includes capabilities for managing technical documentation in line with the Cyber Resilience Act (CRA) and enables the import of Software Bill of Materials (SBOM) to define key components of software products.

All features are tailored to the specific needs of SMEs and are continuously refined based on user feedback.

Planned capabilities of the CAC Tool include:

- Inform users that basic testing is sufficient for products with a 'basic' assurance level, while products with a 'substantial' assurance level require stronger protection and may trigger a recommendation for third-party assessment.
- Guide SMEs through the process of uploading technical documentation and evidence to demonstrate compliance with security requirements.
- Evaluate digital products based on submitted documentation and assign an assurance level.
- Generate a Declaration of Conformity as official proof of the completed evaluation process.

Future roadmap (not included in the current version):

- Advanced visualization of the full CRA compliance journey.
- Enhanced reporting features and technical documentation summaries.
- Post-market monitoring capabilities with automated alerts on new vulnerabilities or regulatory updates under the CRA.

Accessing the CAC Tool

The Conformity Assessment and Compliance (CAC) Tool is accessed exclusively through the **CURIUM portal**. Users cannot access the application directly via a standalone URL; all login and registration activities are performed on the CURIUM platform.

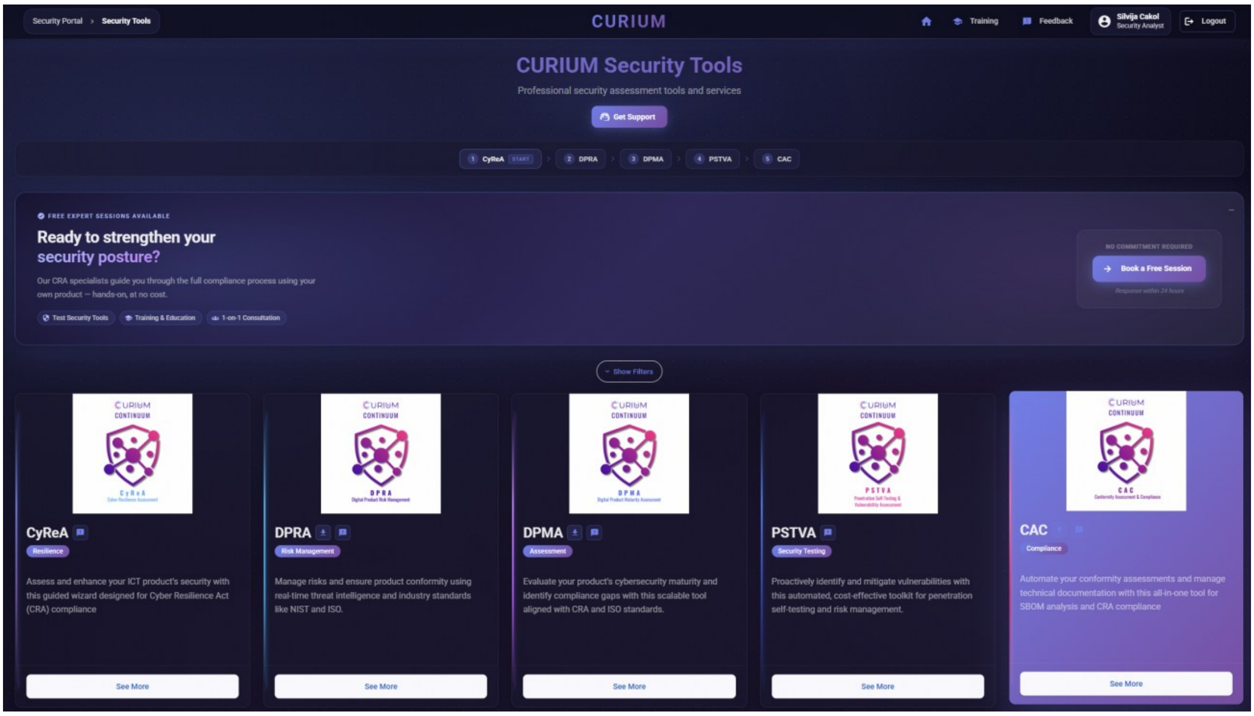
How the user reaches CAC depends on whether they are a **new** or an **existing** user.

New users (after registration)

1. Open a web browser and navigate to the CURIUM portal.
2. Register a new account (see **Registration** below).
3. After successful registration, the user is immediately logged in and the **CAC application opens automatically** (Product list / first product entry). The user does not need to open Security Tools manually at this step.

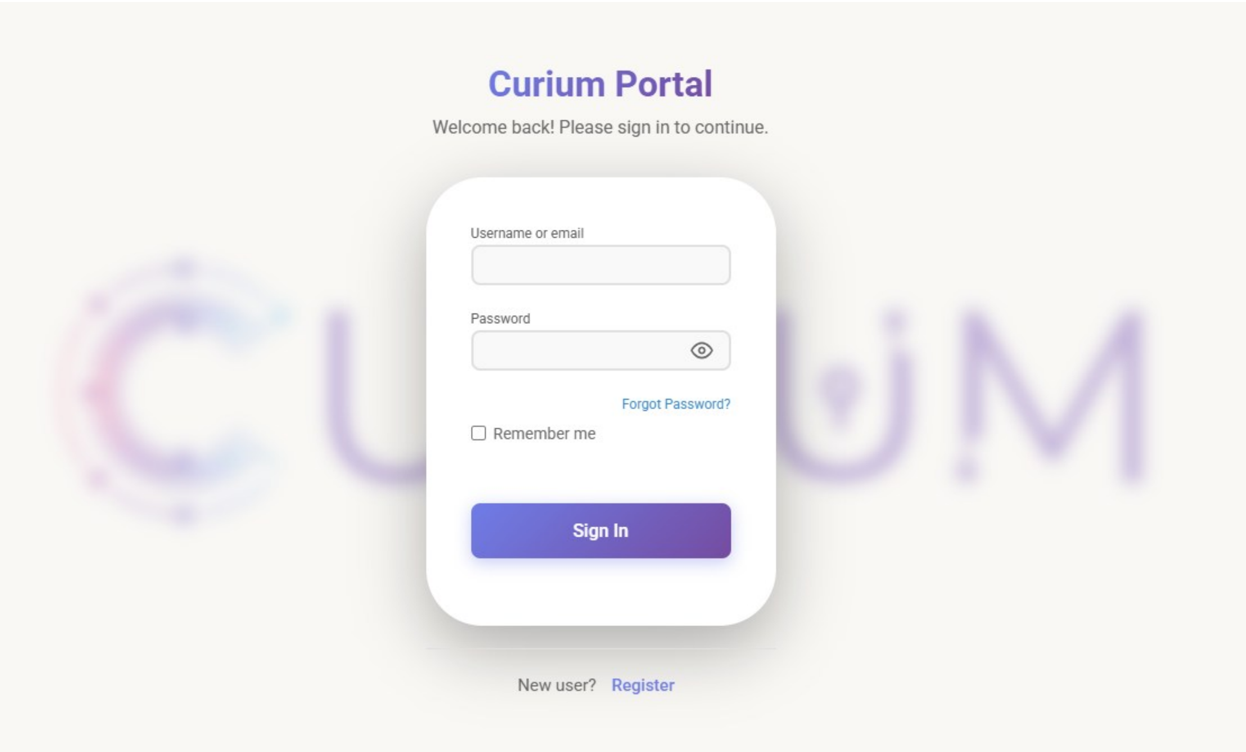
Existing users (already registered)

1. Open a web browser and navigate to the CURIUM portal.
2. Log in with an existing account (see **Login** below).
3. Open the **Security Tools** section and select the **CAC (Conformity Assessment & Compliance)** tool.
4. Click **See More** to launch the CAC application.



Login

If the user already has a CURIUM account, they should enter their credentials on the login page and click the login button to access the portal. After login, the user can navigate to the CAC tool as described above.

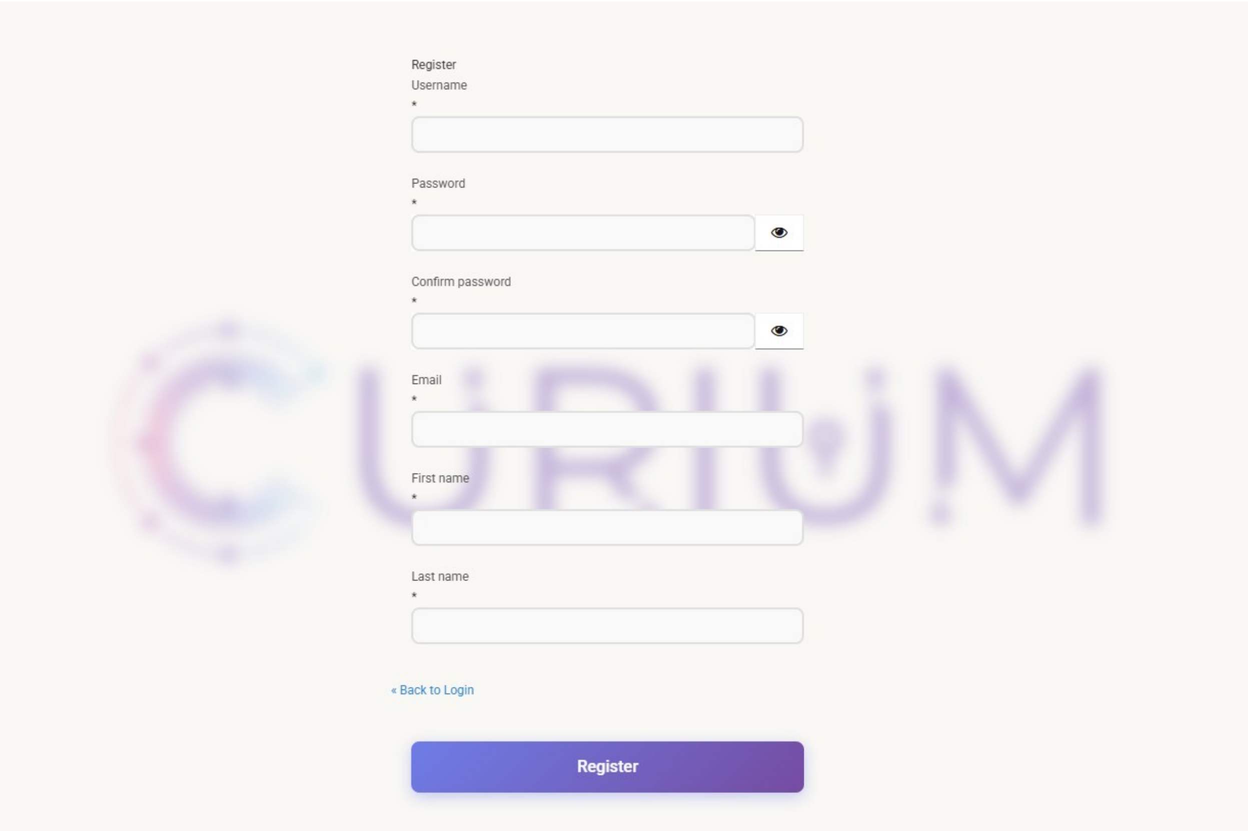


Registration

New users must register on the CURIUM portal before they can access the CAC Tool. On the registration page, the user is required to complete the following mandatory fields:

- **Username**
- **Password**
- **Confirm password**
- **Email**
- **First name**
- **Last name**

Each field marked with an asterisk (*) is mandatory.



To begin registration, the user should click the **Register** option on the login page. After filling in all required fields, the user clicks the **Register** button to submit the form.

If the user already has an account, they can return to the login page by clicking **« Back to Login**.

If the provided information is valid, the account is created and the user is immediately logged in to the CURIUM portal. No confirmation email is sent and no additional email verification step is required. If there are any errors (such as an already registered username or email, or a password that does not meet the requirements), appropriate error messages are displayed and the user must correct the issues before proceeding.

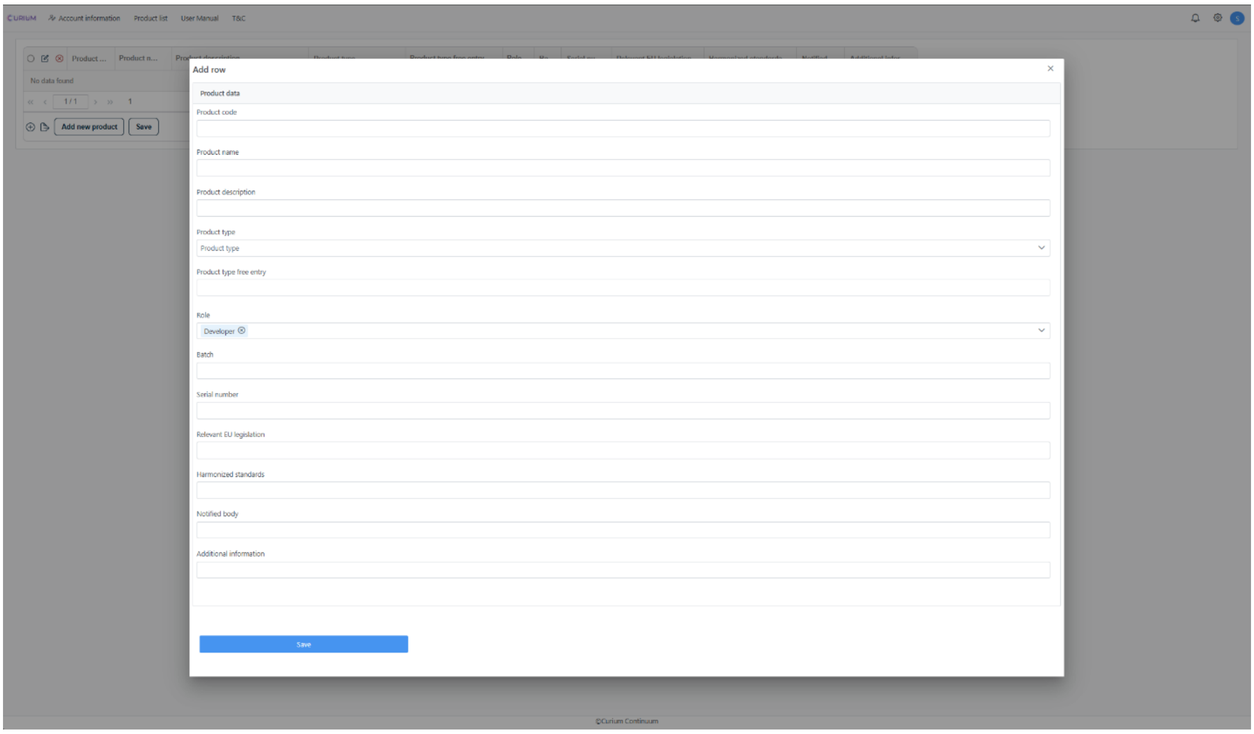
Note: After first login to CAC, the user should complete the **Account information** page inside the application (including company name and other details required for the Declaration of Conformity). Company name is not entered during CURIUM portal registration.

First login and product data entry

After the user reaches the CAC application — either automatically after registration, or by opening CAC from Security Tools after login — the **Product list** screen is displayed.

For a newly registered user, CAC opens automatically and the **Add row** dialog for entering product data is shown so the user can create their first product.

For an existing user opening CAC again, the Product list shows previously entered products (if any). To add a new product, the user clicks **+ Add new product**. Initially, if no products exist, the list displays **No data found**.



The top navigation bar contains the following items:

- Account Information
- Product list
- User Manual
- T&C (Terms and Conditions)

Entering product data

In the Add row dialog, the user enters the basic product information. The following fields are available:

- **Product code**
- **Product name**

- **Product description**
- **Product type**
- **Product type free entry**
- **Role**
- **Batch**
- **Serial number**
- **Relevant EU legislation**
- **Harmonized standards**
- **Notified body**
- **Additional information**

Field labels are displayed above the input fields. The **Role** field is selected from a dropdown list (for example, Developer).

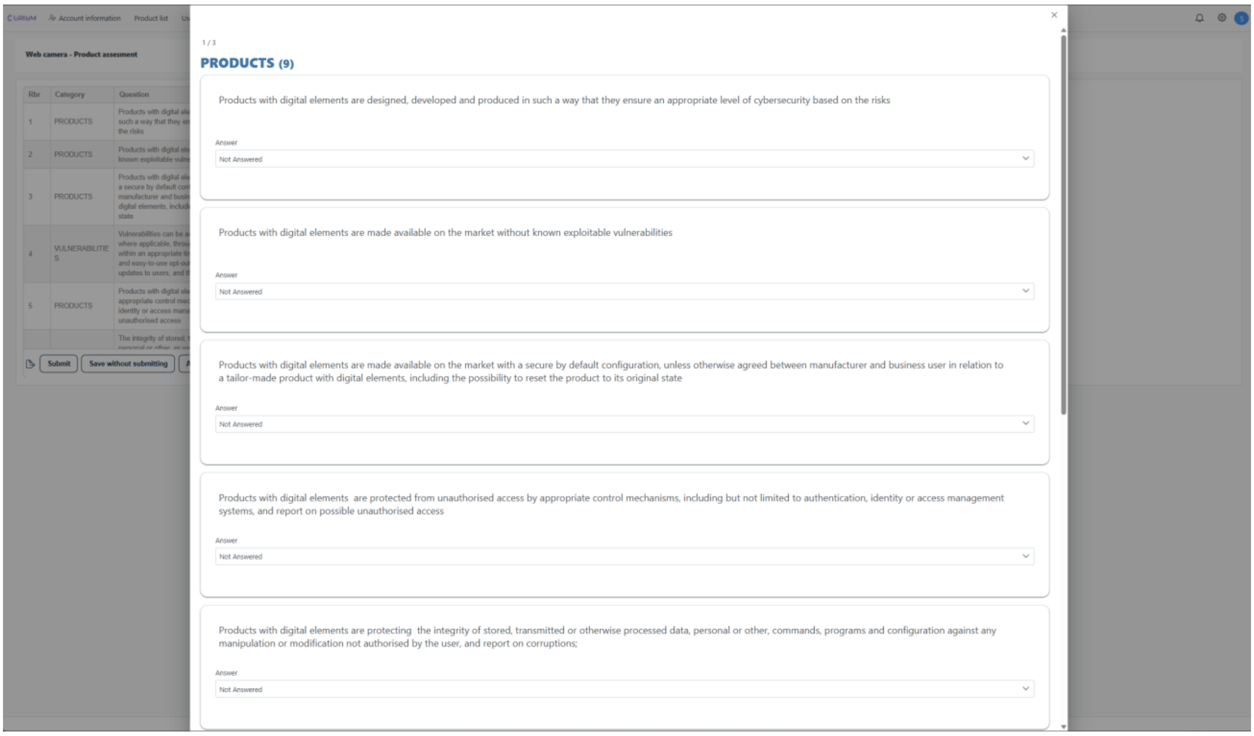
After completing the form, the user clicks the **Save** button in the dialog. The new product appears in the product list.

Note: The **Product code** and **Product name** fields are mandatory.
After saving the product, the assessment workflow continues automatically (see Product assessment).

Product assessment

After the user saves a new product, the Product assessment form opens automatically. The user does not need to open the assessment manually for the first product.

The assessment screen is titled **<PRODUCT_NAME> - Product assessment** (for example, Web camera - Product assessment).



Question categories

Assessment questions are grouped into categories that reflect different aspects of product compliance. The questions relate to the product itself and its handling of **vulnerabilities** and **data**.

Typical categories include:

- **PRODUCTS** — general cybersecurity requirements for the product with digital elements (design, development, secure configuration, access control, data integrity, and related measures)
- **VULNERABILITIES** — identification, documentation, remediation, and disclosure of vulnerabilities, including requirements related to software bill of materials (SBOM) and security updates
- **DATA** — data protection requirements, including data minimization, security-related logging, and user control over stored data and settings

Each category contains one or more pages of questions. The category name and the number of questions on the current page are shown in the modal title (for example, PRODUCTS (9)).

The user should answer all questions in every category before completing the assessment.

Assessment overview

In the background, a table lists all assessment questions with the following columns:

- **Rbr** — row number
- **Category** — question category (for example, PRODUCTS, VULNERABILITIES)
- **Question** — full text of the requirement

At the bottom of the screen, the following actions are available:

- **Submit** — submits the completed assessment
- **Save without submitting** — saves current answers without submitting

Completing the assessment

The assessment questionnaire is displayed in a modal window. Questions are grouped by category and presented across multiple pages.

The page indicator in the top-left corner of the modal shows the current page and total number of pages (for example, 1/3). The category name and number of questions on the current page are shown in the modal title (for example, **PRODUCTS (9)**).

Each question is displayed as a separate item containing:

- the full requirement text
- an **Answer** dropdown with the values **Not Answered, Yes,** and **No**

The user selects an answer for each question on the current page.

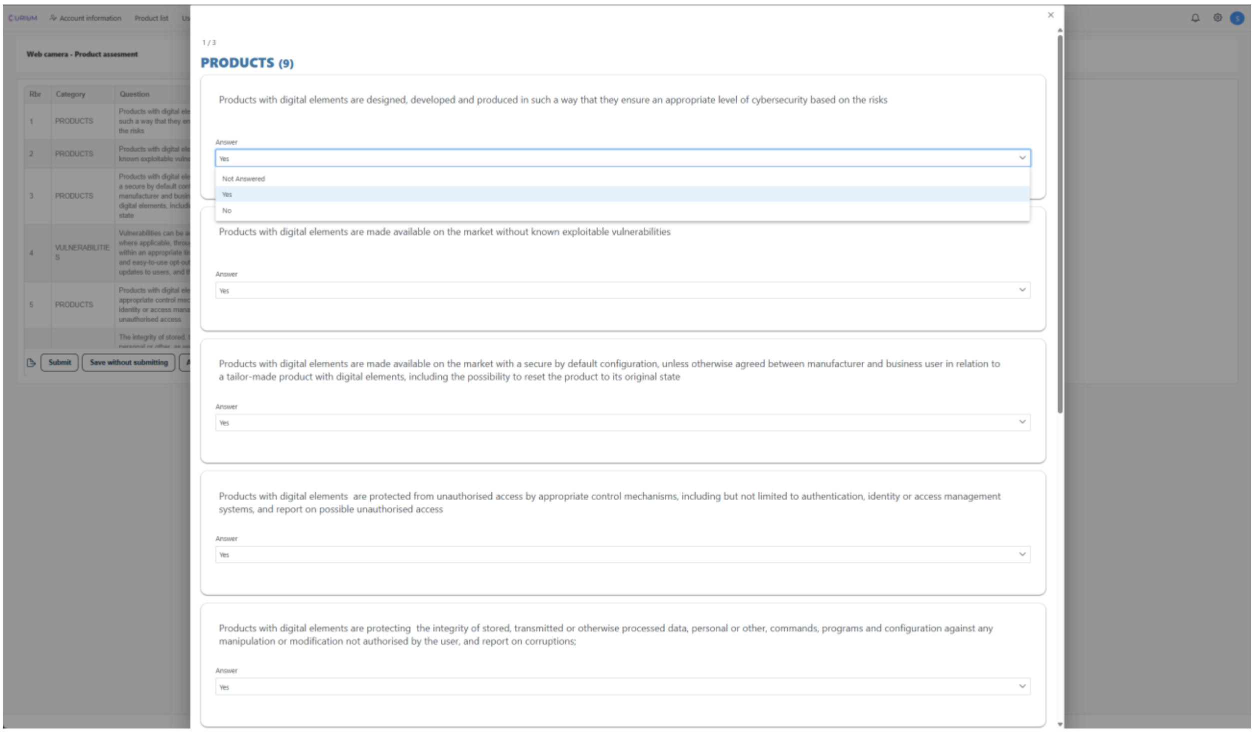
Navigation between pages is performed using:

- **Next** — proceed to the next page of questions
- **Back** — return to the previous page

On the final page, the user clicks **Complete** to finish the assessment.

CURIUM CONTINUUM

CAC
Conformity Assessment & Compliance



Saving and submitting

The user can:

- click **Save without submitting** to save progress and continue later
- click **Submit** to submit the completed assessment

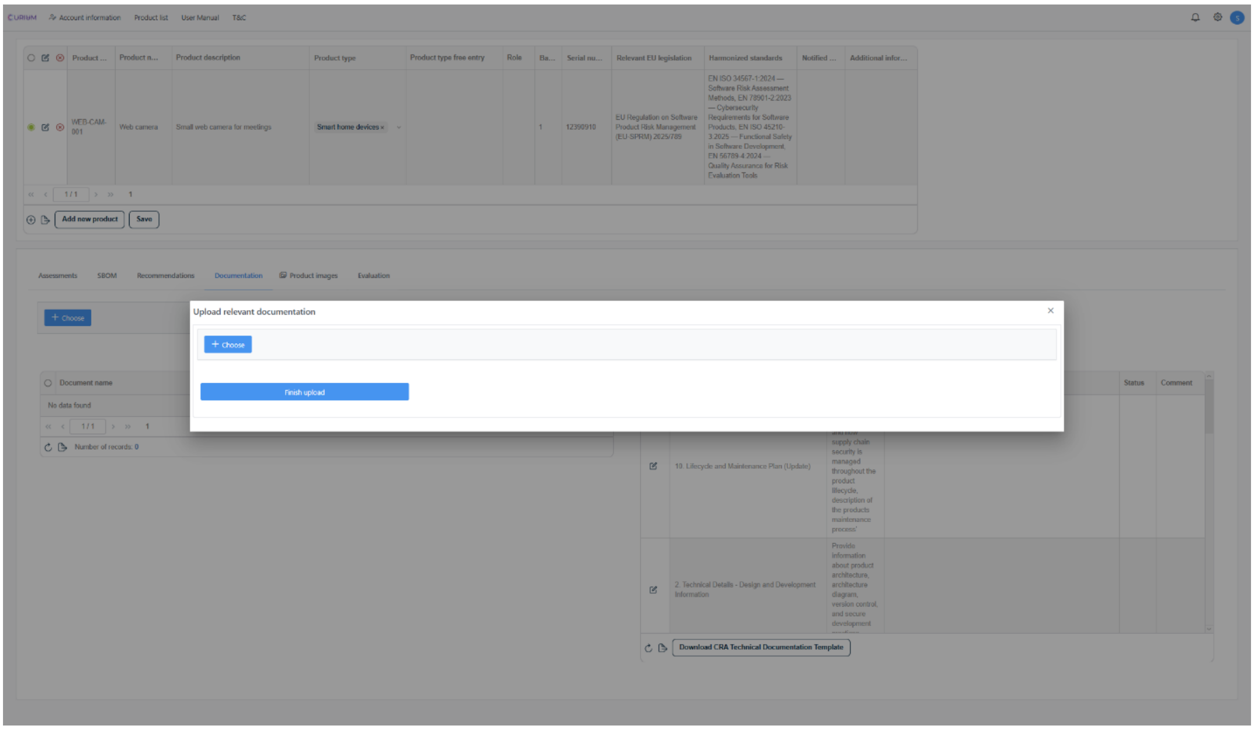
If the assessment modal is closed using the **X** button before completion, unsaved answers may not be stored in the product assessment table.

Once the assessment is completed and submitted, the results are stored and displayed in the **Assessments** tab for the selected product.

After the assessment modal is closed, the user is prompted to upload relevant documentation (see Uploading relevant documentation).

Uploading relevant documentation

After the user completes the product assessment and closes the assessment modal, the **Upload relevant documentation** dialog opens automatically.

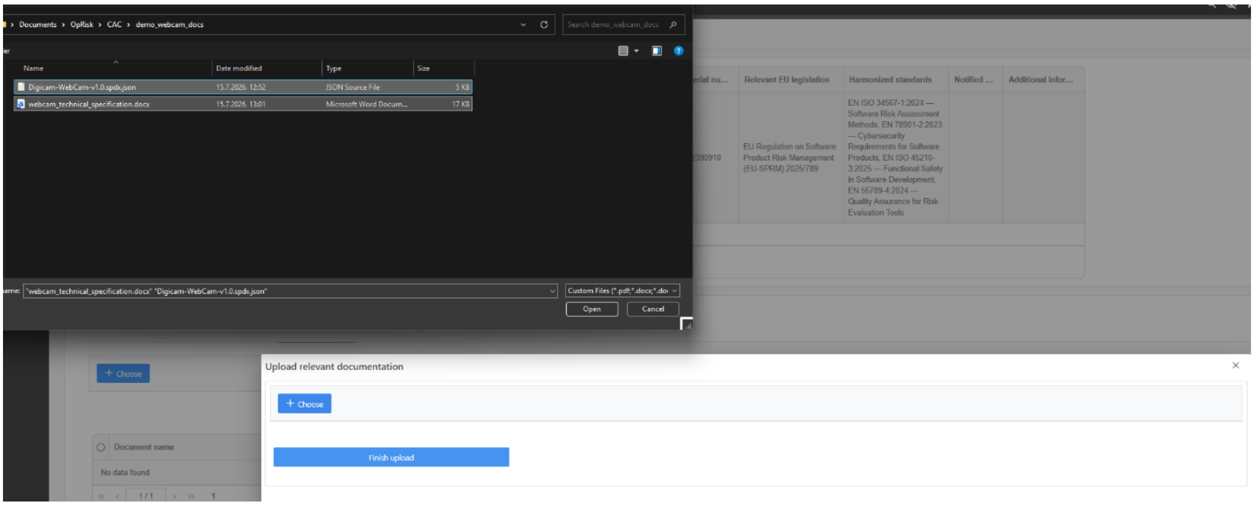


Uploading files

The dialog allows the user to upload one or more documents for the selected product in a single step.

To upload files:

1. Click the **+ Choose** button.
2. Select one or more files from the local file system.
3. Confirm the selection. The selected file names are displayed in the upload dialog.
4. Click Finish upload to complete the upload and proceed to the product overview screen.



Supported file formats

The following file formats are supported in this upload step:

Document type	Supported formats
Technical documentation	**PDF**, **DOCX**, **DOC**
Software Bill of Materials (SBOM)	**JSON – SPDX 2.3 format** (.json file)

SBOM requirements

- The SBOM file must be provided in **JSON – SPDX 2.3 format**.
- The file extension is typically .json (for example, Digicam-WebCam-v1.0.spdx.json).
- After a valid SBOM file is uploaded, the system automatically starts SBOM evaluation. A success notification is displayed when the upload completes successfully (for example, *Digicam-WebCam-v1.0.spdx.json uploaded successfully*).

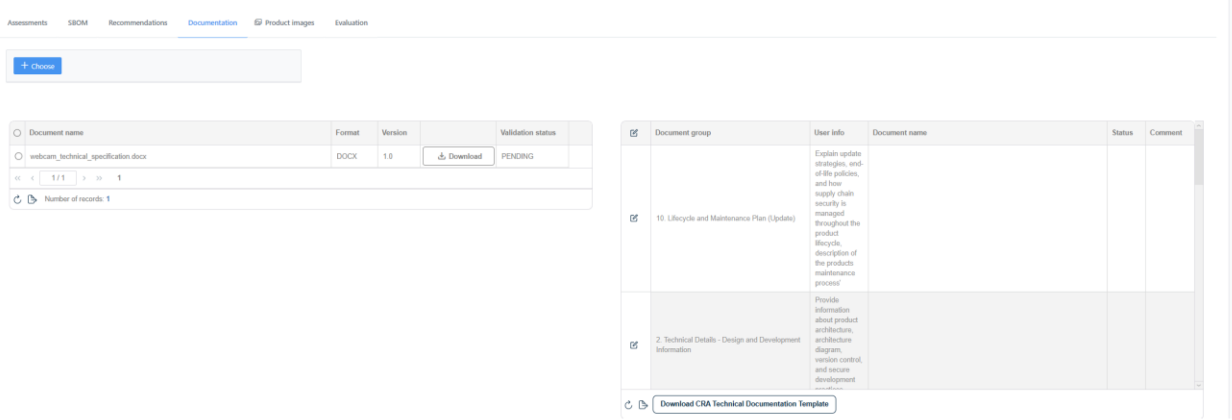
Technical documentation

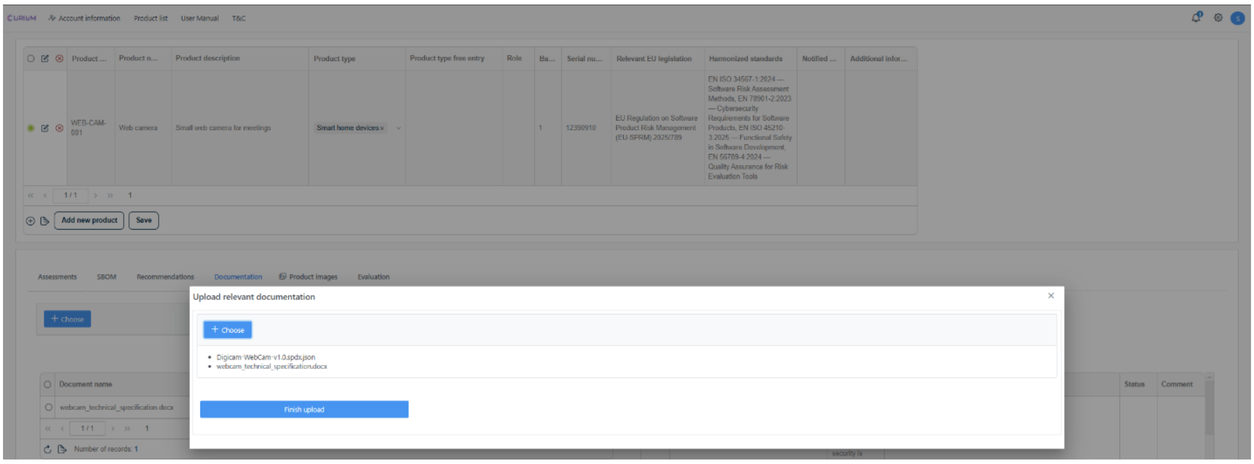
- Technical documentation can be uploaded as a **PDF** or **Word** document (**.docx** or **.doc**).
- In a single upload step, the user may upload both technical documentation and an SBOM file together.

After upload

After clicking **Finish upload**, the upload dialog closes and the product overview screen is displayed.

- Uploaded technical documents are managed under the **Documentation** tab.
- SBOM evaluation results are displayed under the **SBOM** tab.
- If additional documentation is required, the user can upload further files from the **Documentation** tab or use the **Download CRA Technical Documentation Template** button as a starting point.





After SBOM upload

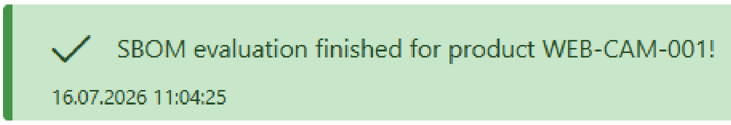
When an SBOM file in **JSON – SPDX 2.3 format** is uploaded, the system automatically starts SBOM evaluation for the selected product.

While evaluation is in progress, the related document may show a validation status such as **PENDING** on the **Documentation** tab.

SBOM evaluation finished notification

When SBOM validation has completed successfully, a green success notification appears on the right side of the screen.

The notification confirms that SBOM evaluation has finished for the selected product (for example: **SBOM evaluation finished for product WEB-CAM-001!**). The notification also shows the date and time of completion (for example, *16.07.2026 11:04:25*).



After this notification appears, the evaluation results are available on the **SBOM** tab. The user can open the **SBOM** tab to review components, identified vulnerabilities, severity levels, and suggested fixes.

Next steps after documentation and SBOM upload

After the initial documentation and SBOM files have been uploaded and SBOM evaluation has finished, the product overview remains available with all product tabs.

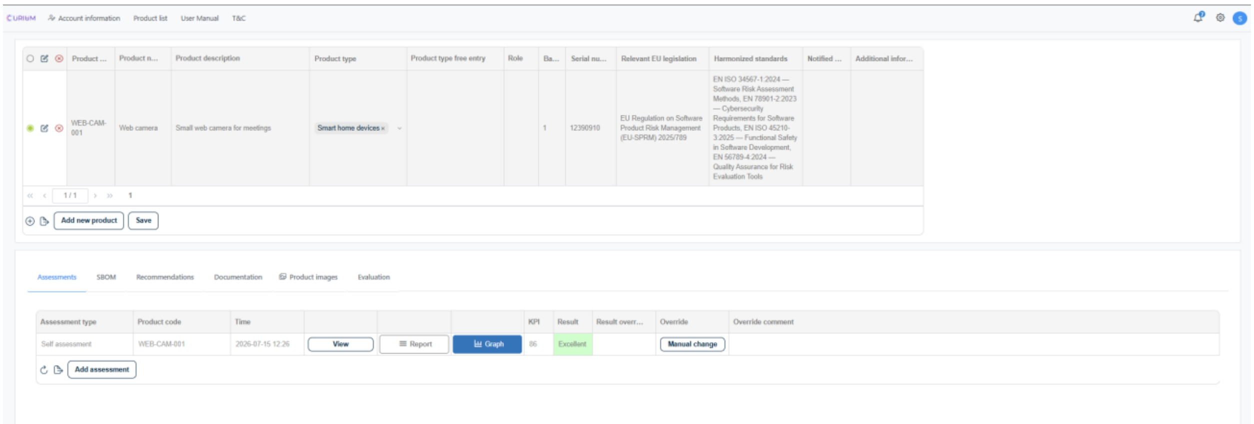
At this stage, the user should:

- Review SBOM results on the SBOM tab.
- Open the Recommendations tab and record an action for every recommendation.
- Complete any missing documentation on the Documentation tab, if required.
- Upload product images on the Product images tab (recommended before evaluation).
- Ensure Account information is completed (company details, logo, and signature).
- Run the product evaluation on the Evaluation tab.
- Generate the EU Declaration of Conformity when the latest evaluation status is Passed.

Product Overview

The **Product overview** screen shows the selected product and its related details.

The top part of the screen contains the **Product list** table. Below the table, a tabbed view presents information for the selected product.



The following tabs are available:

- **Assessments**
- **SBOM**

- **Recommendations**
- **Documentation**
- **Product images**
- **Evaluation**

Each tab is described in a separate section in this document.

By selecting a product row, details of the selected product are shown in the tabs below.

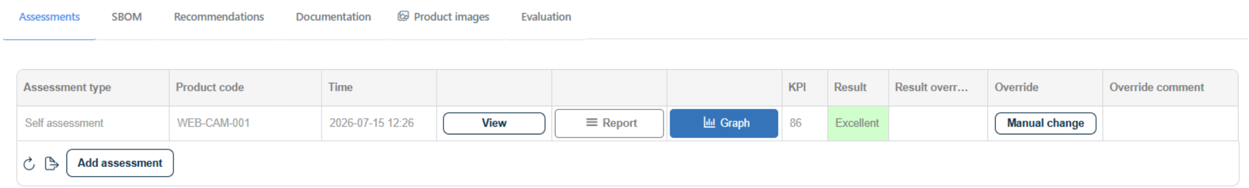
Product information can be edited by clicking the edit button in the product table row, which opens the **Add row** dialog.

The top navigation bar contains **Account Information**, **Product list**, **User Manual**, and **T&C** (Terms and Conditions).

Assessment tab

In the Assessment tab, the user can manage product assessments. Product assessments are questionnaires where each answer is scored, and the sum of per-question scores produces a total result that is graded into categories such as Bad, Good, or Excellent. The result can also be displayed as a chart and can be manually overridden with an optional override comment.

The first assessment is created automatically when a new product is added. If necessary, a product can be re-assessed multiple times by creating and filling out additional assessment records using the Add assessment button.



Each assessment contains the following information:

- Assessment type — always Self assessment.
- Product code — read-only identifier of the assessed product.
- Time — timestamp when the assessment was created or last updated.
- View — opens the assessment form for changes.
- Report — opens a detailed report view (scoring, checks, evidence).
- Graph — opens a KPI/metrics chart for this assessment.

- KPI — numeric score or key performance indicator.
- Result — qualitative outcome derived from KPI (for example Bad, Good, Excellent).
- Result override — shows the current override status/value if any.
- Override — button to change the computed result manually.
- Override comment — free-text reason recorded with an override.

By selecting View, the assessment is displayed so the user can review and change answers.

Rbr	Category	Question	Response
1	PRODUCTS	Products with digital elements are designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks	Yes
2	PRODUCTS	Products with digital elements are made available on the market without known exploitable vulnerabilities	No
3	PRODUCTS	Products with digital elements are made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state	Yes
4	VULNERABILITIES	Vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them	Yes
5	PRODUCTS	Products with digital elements are protected from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access	No
6	DATA	The integrity of stored, transmitted, or otherwise processed data, whether personal or other, as well as commands, programs, and configurations, has been protected against any manipulation or modification not authorized by the user, with reporting mechanisms in place for any detected corruptions.	Yes
7	PRODUCTS	Products with digital elements are protecting the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;	Yes
8	DATA	Only data, whether personal or other, that are adequate, relevant, and limited to what is necessary in relation to the intended purpose of the product with digital elements, have been processed, in accordance with the principle of data minimization	Yes

Return to product page

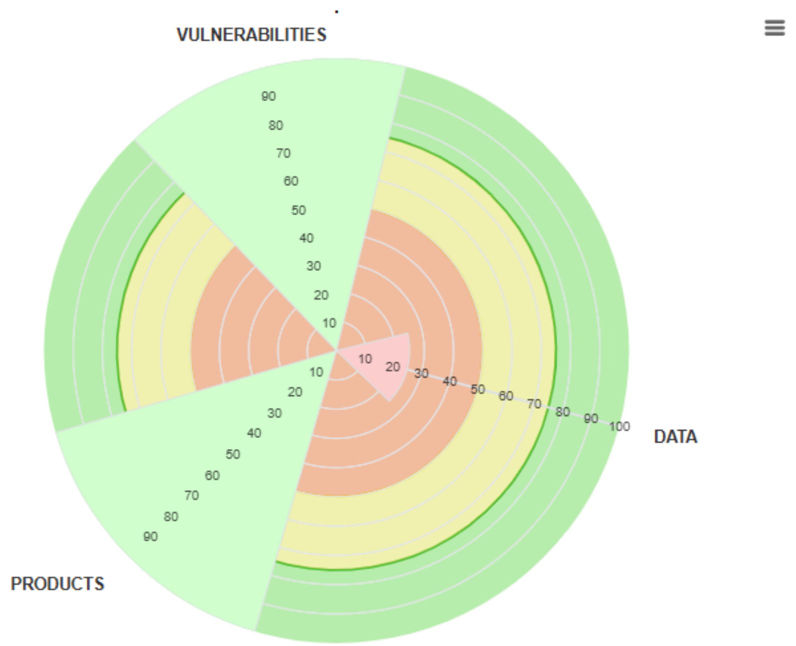
By clicking on Report, a summary representation of the assessment is shown:

Category	Points	Percentage	Percentage_status
DATA	1	25	Bad
PRODUCTS	9	100	Excellent
VULNERABILITIES	9	100	Excellent
	19	86	Excellent

1 / 1 1

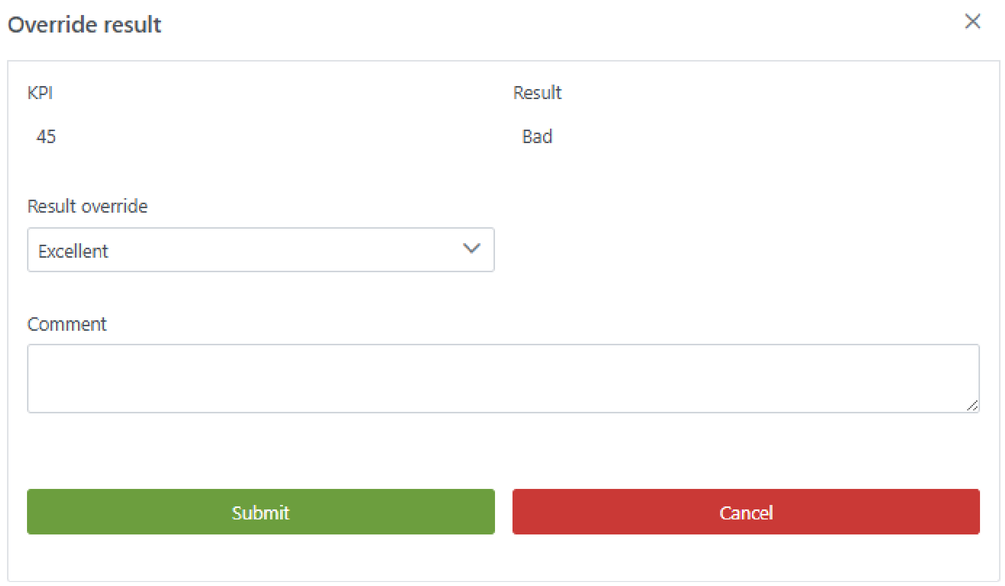
Number of records: 4

By clicking on Graph, a summary representation of the assessment is shown as a graph:



If the evaluation of the assessment shows bad results — for instance, when the assessment criteria do not fully apply to certain products or when specific conditions lead to inaccurate scoring — the user has the option to override the result using the **Manual Change** function.

When applying a manual override, the user is required to provide a clear and concise explanation in the comments field, describing why the automatic assessment result is considered invalid or not applicable.



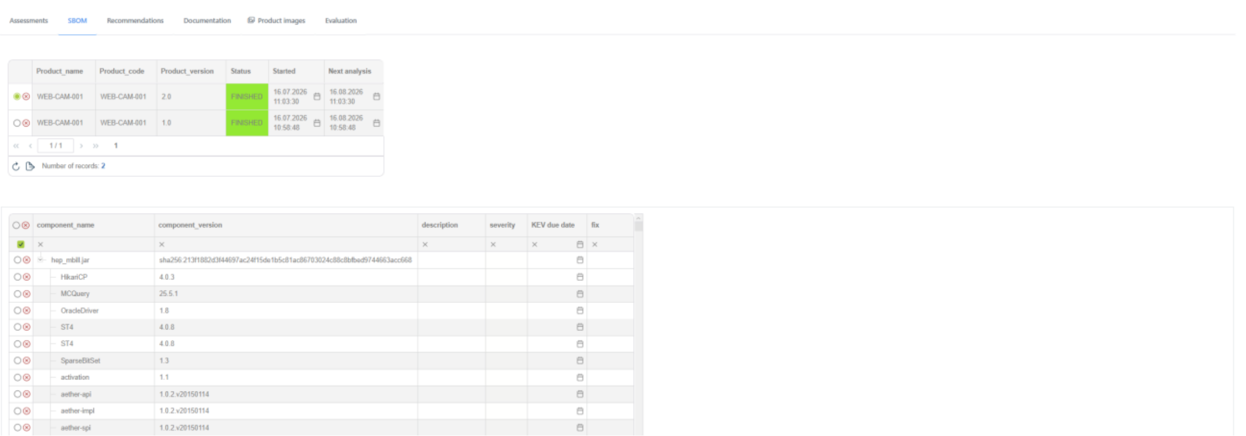
SBOM tab

The **SBOM** tab displays the results of Software Bill of Materials evaluation for the selected product.

After SBOM evaluation has finished, results are shown on this tab (see SBOM evaluation finished notification).

The SBOM tab contains two main areas:

- an upper table with SBOM analysis history
- a lower table with components and identified vulnerabilities



SBOM analysis history (upper table)

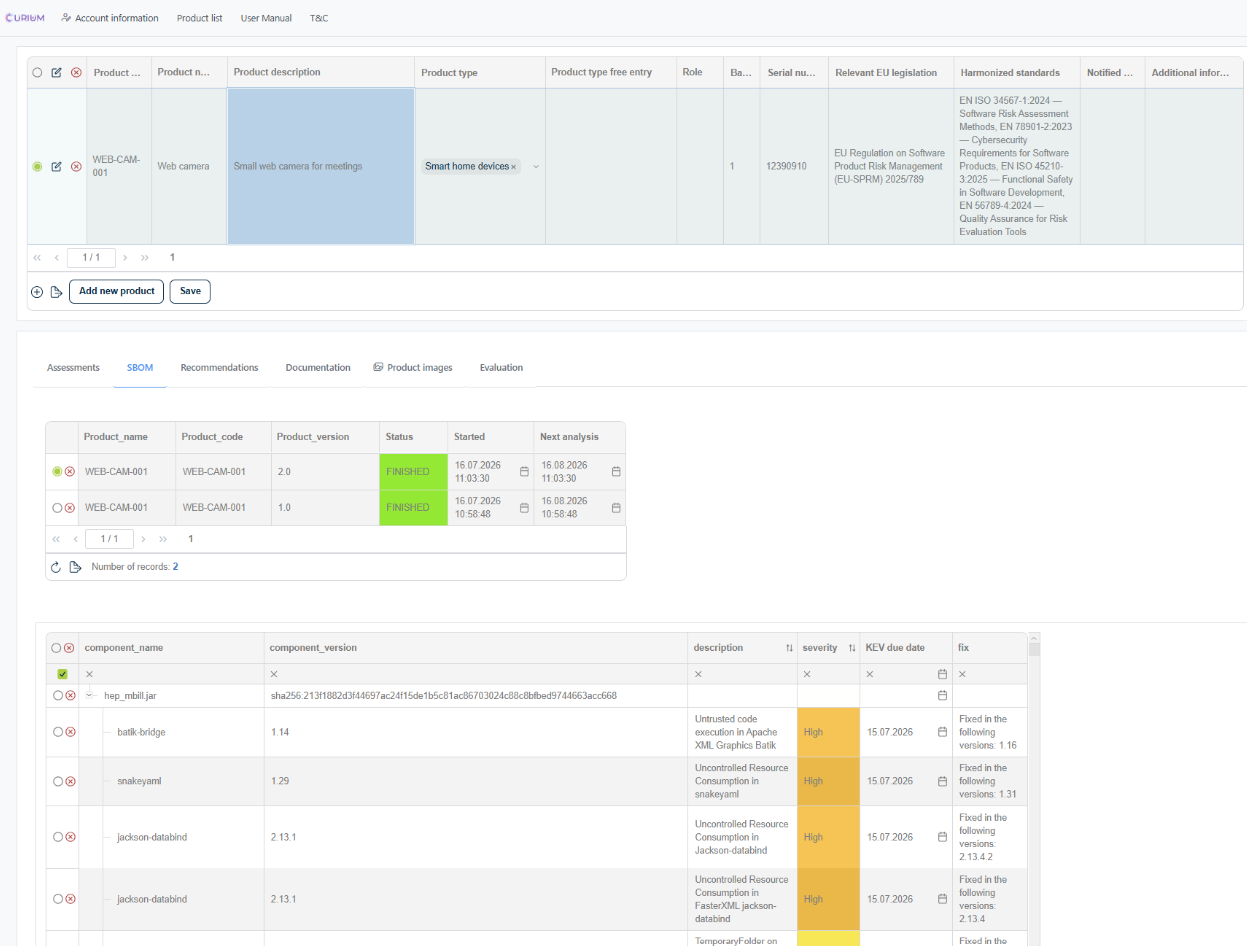
The upper table lists SBOM evaluation records for the selected product.

Column	Description
Product_name	Name of the product
Product_code	Product code
Product_version	SBOM / product version (for example, 1.0, 2.0)
Status	Evaluation status (for example, **FINISHED**)
Started	Date and time when evaluation started
Next analysis	Date and time of the next planned analysis

Each new SBOM upload creates a new analysis record. Multiple versions can be listed (for example, version **1.0** and version **2.0**), each with its own status and timestamps.

When evaluation is complete, the **Status** column shows **FINISHED** (highlighted in green).

Example: For product WEB-CAM-001, two finished analyses are shown with different start times.



Components and vulnerabilities (lower table)

When a row in the upper table is selected, the lower table shows the components extracted from the uploaded SBOM and any identified vulnerabilities.

Column	Description
component_name	Name of the software component
component_version	Version of the component
description	Description of the identified vulnerability or issue
severity	Severity level (for example, **High**, **Medium**, **Low**, **Critical**), colour-coded
KEV due date	Known Exploited Vulnerability due date, if available
fix	Suggested remediation (for example, the version in which the issue is fixed)

Components can be shown in a hierarchical / expandable structure. Expanding a parent component reveals related libraries and vulnerability entries.

Example entries after upload:

- batik-bridge 1.14 — High — Fixed in version 1.16
- snakeyaml 1.29 — High — Fixed in version 1.31
- jackson-databind 2.13.1 — High — Fixed in later versions (for example, 2.13.4 / 2.13.4.2)

The user is responsible for obtaining the SBOM file. The CAC application does not generate the SBOM; it evaluates an uploaded SPDX 2.3 JSON file.

Relationship with Recommendations

Identified SBOM vulnerabilities may also appear on the **Recommendations** tab, where the user must select an action for each recommendation (for example, **Acknowledged**, **Not applicable**) before the product can pass evaluation and generate the EU Declaration of Conformity.

Recommendations tab

On the Recommendations tab the user can review recommendations generated from the uploaded SBOM, the assessment questionnaire, and missing or delayed documentation.

Each record has a Category value that specifies the source of the recommendation, for example SBOM or Document.

Typical columns in the recommendations table include:

- Category
- Name
- Version
- Status — for SBOM items this may show severity levels such as Critical or High
- Recommendations — detailed remediation guidance
- Links
- Action
- Comment
- Username
- Changed date

In order for a product to be eligible for EU declaration creation, the user must make a decision for **every** presented recommendation.

For each row:

1. Review the **Status** and the text in **Recommendations**.
2. Open the **Action** dropdown.
3. Select one of the following values:
   - **Acknowledged**
   - **Not applicable**
4. Optionally enter a note in the **Comment** field.
5. Click **Save** at the bottom of the tab to store the decisions.

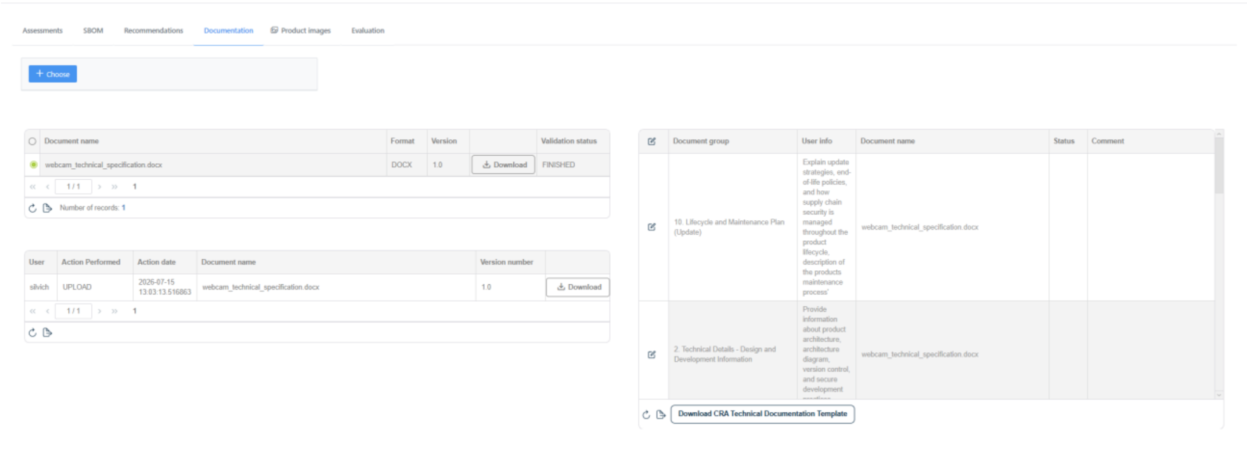
Note: The user must make a decision for all recommendations before the evaluation can pass and the EU Declaration of Conformity can be generated.

Documentation tab

The **Documentation** tab is used to manage all documentation required for the selected product. Documentation is mandatory for every product.

The screen is divided into three main areas:

- **Uploaded documents** (top left)
- **Action history** (bottom left)
- **Documentation requirements checklist** (right)



Uploaded documents

At the top left, the **+ Choose** button allows the user to upload additional documents at any time.

The table lists uploaded documents with the following columns:

- **Document name** — name of the uploaded file
- **Format** — file format (for example, DOCX, PDF, JSON)
- **Version** — document version number
- **Download** — downloads the uploaded file
- **Validation status** — processing status of the document

Typical validation status values include:

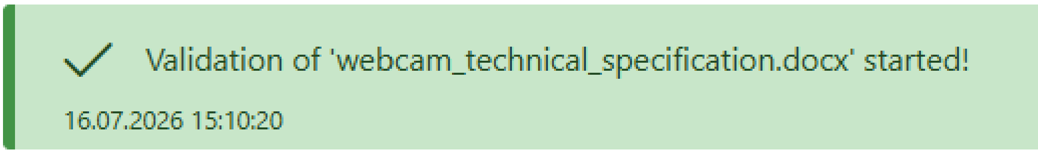
- **PENDING** — uploaded and validation is in progress
- **FINISHED** — validation has completed successfully

Example: webcam_technical_specification.docx appears with format **DOCX**, version **1.0**, and validation status **FINISHED**.

Document validation notification

After a technical document is uploaded (for example, webcam_technical_specification.docx), the system starts validation of the file.

A green notification appears on the right side of the screen confirming that validation has started, for example:



The notification also shows the date and time (for example, *16.07.2026 15:10:20*). While validation is in progress, the document **Validation status** on the Documentation tab may show **PENDING**. When validation completes successfully, the status changes to **FINISHED**.

Action history

The lower-left table shows the history of document actions, for example:

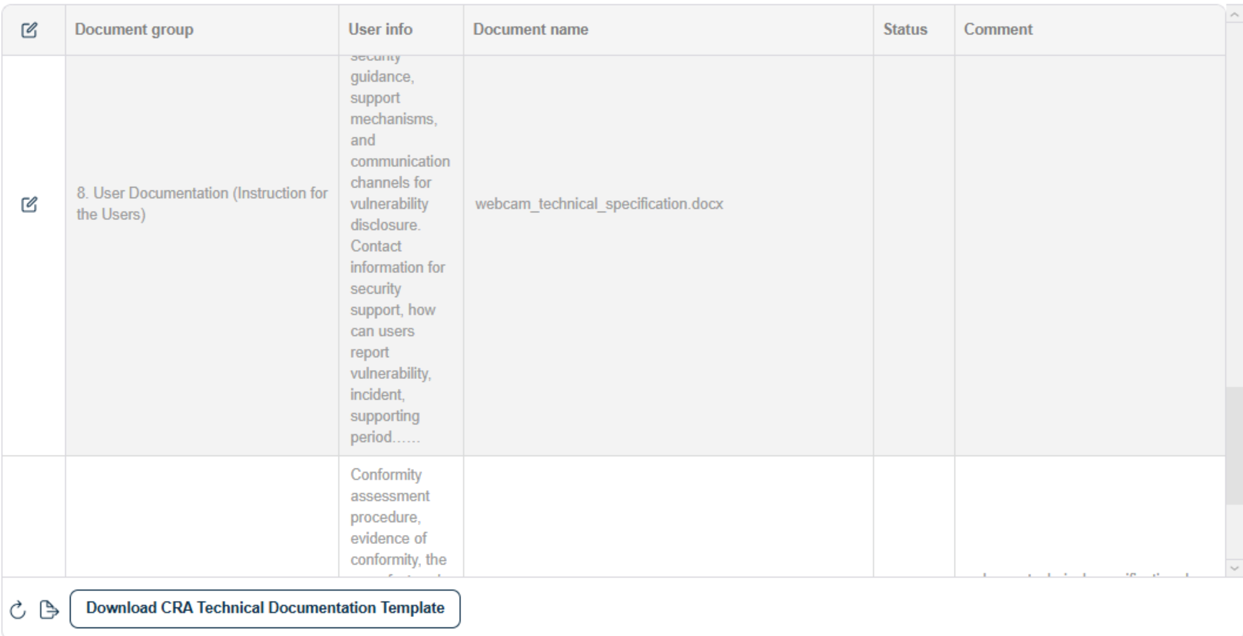
- **User** — who performed the action
- **Action Performed** — for example, **UPLOAD** or **DOWNLOAD**
- **Action date** — date and time of the action
- **Document name**
- **Version number**

- **Download** — available for upload actions

Example: User performed **UPLOAD** for webcam_technical_specification.docx vers ion **1.0**.

Documentation requirements checklist

The right-hand table lists the documentation types required for compliance. Each row represents one required documentation item.



	Document group	User info	Document name	Status	Comment
	8. User Documentation (Instruction for the Users)	guidance, support mechanisms, and communication channels for vulnerability disclosure. Contact information for security support, how can users report vulnerability, incident, supporting period......	webcam_technical_specification.docx		
		Conformity assessment procedure, evidence of conformity, the			

Download CRA Technical Documentation Template

Column	Description
Edit	Opens options for this requirement (**Upload** / **Later** / **Not applicable**)
Document group	Name and number of the required documentation group
User info	Guidance describing what should be provided
Document name	File mapped to this requirement, if any
Status	Current status of the requirement
Comment	User notes and/or system validation feedback for the documentation requirement

Required documentation groups include:

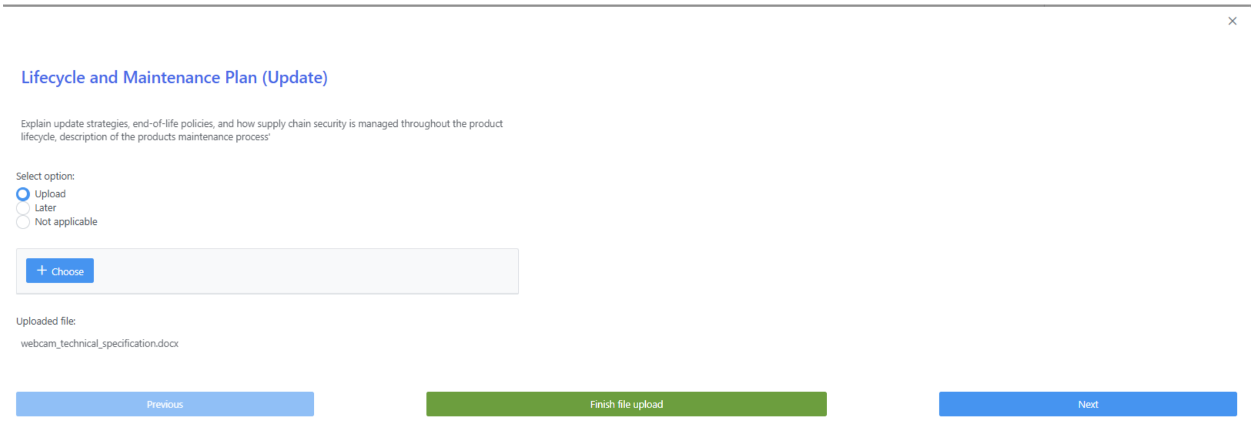
1. **Technical Details – Design and Development Information** — product architecture, architecture diagram, version control, and secure development practices
2. **Technical Details – SBOM** — software bill of materials in **JSON – SPDX 2.3 format**
3. **List of harmonized standards applied**
4. **Vulnerability Management**
5. **Cybersecurity Requirements/Measures (by Design)**
6. **Testing and Validation Results**
7. **User Documentation (Instruction for the Users)**
8. **Conformity Assessment and Declaration of Conformity**
9. **Lifecycle and Maintenance Plan (Update)** — update strategies, end-of-life policies, and supply chain security throughout the product lifecycle

One uploaded file (for example, webcam_technical_specification.docx) may be mapped to several documentation groups.

The **Comment** column may contain a user note or system validation feedback when content is incomplete (for example, that a document lacks a conformity assessment procedure, evidence of conformity, or the manufacturer's declaration of conformity).

Editing a documentation requirement

By clicking the **Edit** icon in a row of the requirements checklist, a dialog opens for that documentation group.



The dialog shows:

- the **document group title**
- guidance text explaining what should be provided
- **Select option:**

- **Upload** — upload a document for this requirement (default)
- **Later** — postpone the upload
- **Not applicable** — mark the requirement as not applicable to this product

If **Upload** is selected:

1. Click **+ Choose**.
2. Select a file from the local file system.
3. Confirm that the file is listed under **Uploaded file**.

Supported formats:

- **Technical Details – SBOM: JSON – SPDX 2.3 format** (.json)
- **Other documentation types: PDF**, **DOCX**, or **DOC**

Navigation buttons at the bottom of the dialog:

- **Previous** — go to the previous documentation group
- **Next** — go to the next documentation group
- **Finish file upload** — close the dialog and save the selected options

Example: For *Lifecycle and Maintenance Plan (Update)*, the user selects **Upload** and attaches webcam_technical_specification.docx, then clicks **Finish file upload**.

Depending on the selected option, the status of the requirement is updated (for example, uploaded, postponed, or not applicable).

Note: If a documentation requirement remains set to **Later**, the **Documentation** step in the product evaluation may result in **Failed**. Before starting evaluation, each requirement should be set to **Upload** (with a file provided) or **Not applicable**.

CRA Technical Documentation Template

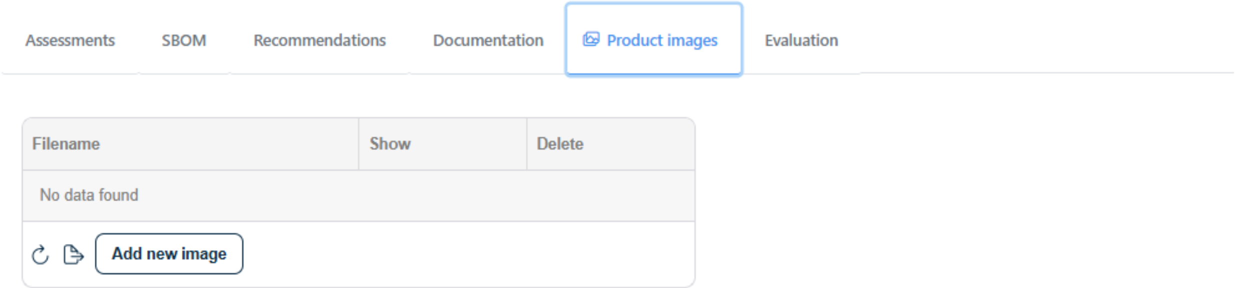
At the bottom of the requirements checklist, the **Download CRA Technical Documentation Template** button allows the user to download a template that can be used as a starting point for preparing CRA technical documentation.

Relationship with SBOM tab

If an SBOM file in **JSON – SPDX 2.3 format** was uploaded, the system automatically starts SBOM evaluation. Results are displayed on the **SBOM** tab once processing is complete.

Product images tab

Product images should be uploaded before running the final evaluation. Images uploaded on this tab are displayed on the generated EU Declaration of Conformity. Up to four images can be shown on the declaration.



Opening the Product images tab

On the product overview screen, open the **Product images** tab.

Initially, if no images have been uploaded, the table displays **No data found**.

The table contains the following columns:

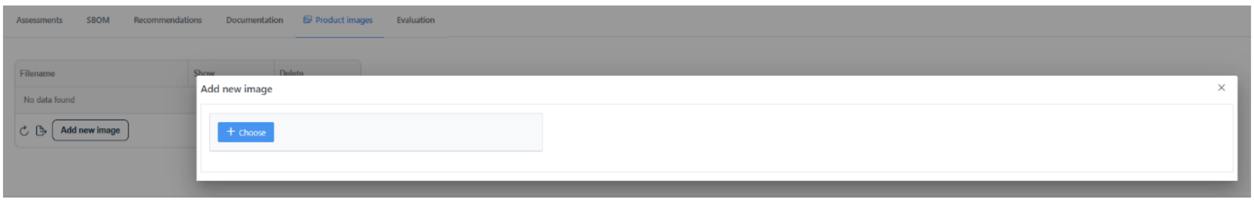
- **Filename**
- **Show**
- **Delete**

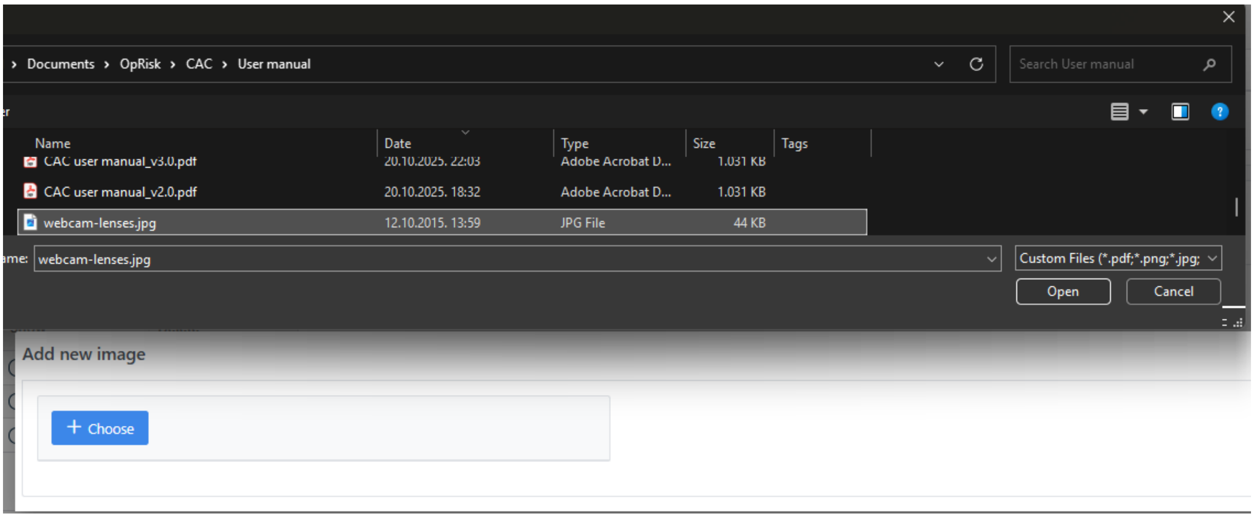
At the bottom of the table, the **Add new image** button is available.

Adding product images

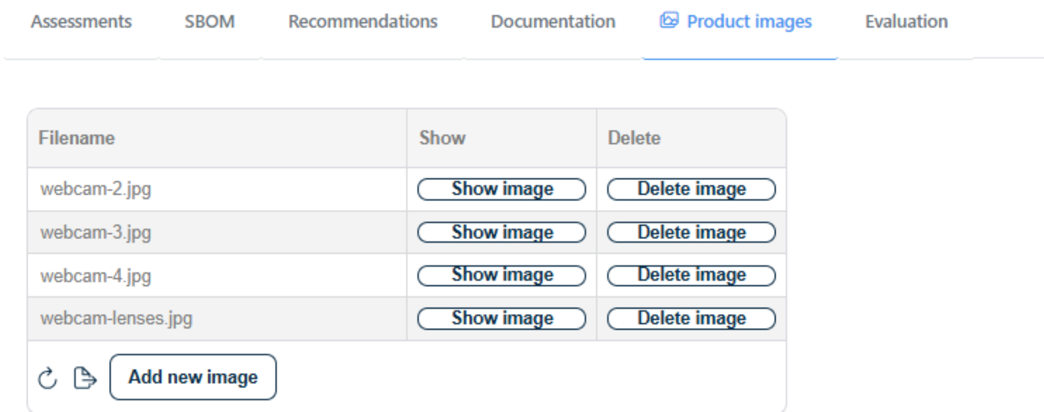
To upload images:

1. Click **Add new image**.
2. The **Add new image** dialog opens.
3. Click **+ Choose**.
4. Select one or more image files in the system file chooser.
5. Confirm the selection.





After upload, the images appear in the Product images table.



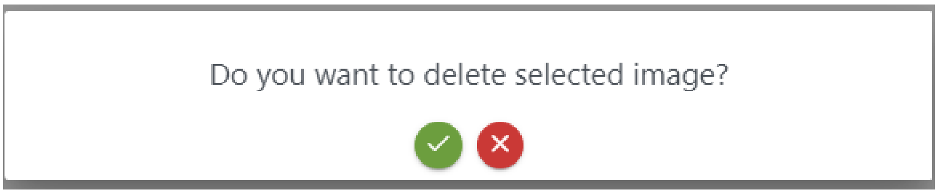
Viewing and deleting images

For each uploaded image, the following actions are available:

- **Show image** — opens the image in a new browser tab
- **Delete image** — removes the image from the product

To delete an image:

1. Click **Delete image** for the selected file.
2. Confirm the deletion in the confirmation dialog.

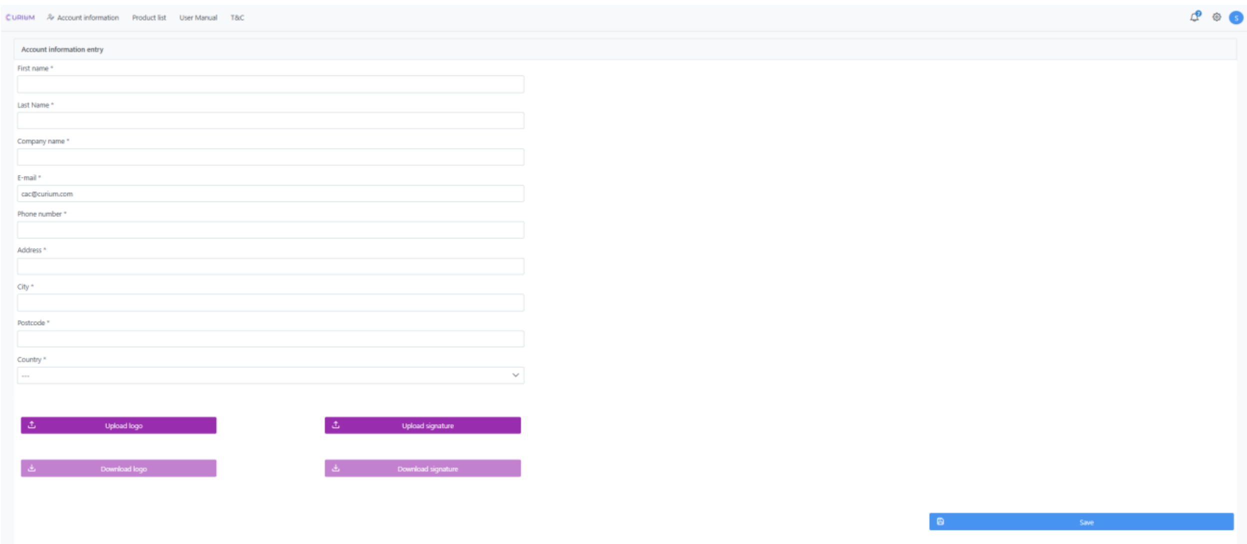


Notes

- Product images should be uploaded **before** running evaluation and generating the EU Declaration of Conformity.
- Up to **four** images can be displayed on the declaration.
- The user can add more images later using **Add new image**.

Account information

Before generating a Declaration of Conformity, the user should complete the Account information page. This page is available from the top navigation bar after login.



Required fields

The following fields are mandatory (marked with an asterisk *):

- First name
- Last name
- Company name
- E-mail
- Phone number
- Address
- City
- Postcode
- Country

Country is selected from a dropdown list.

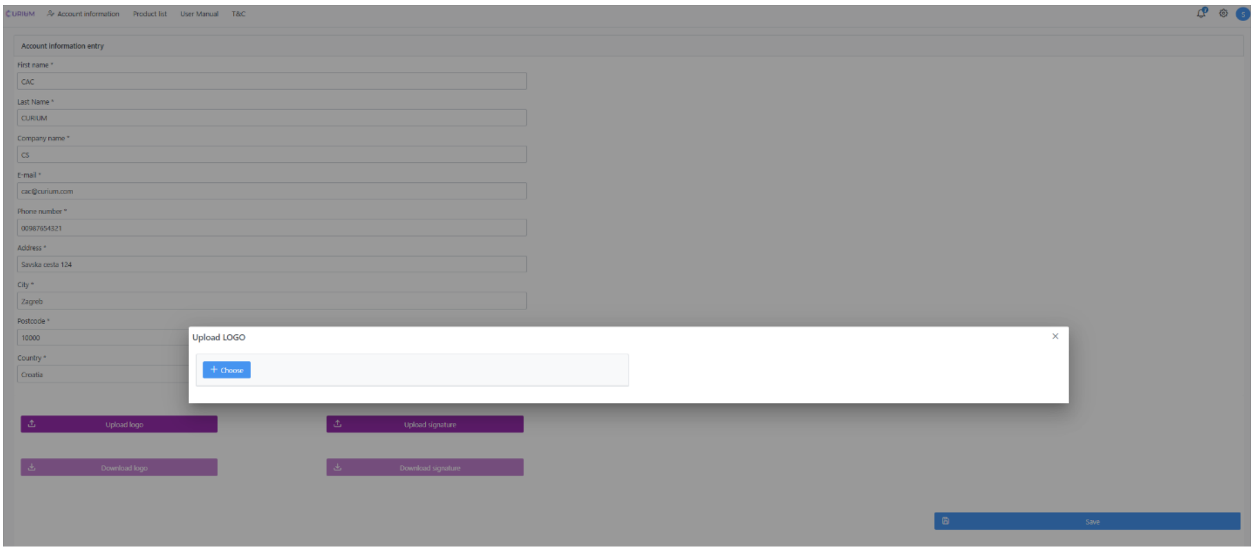
Uploading logo and signature

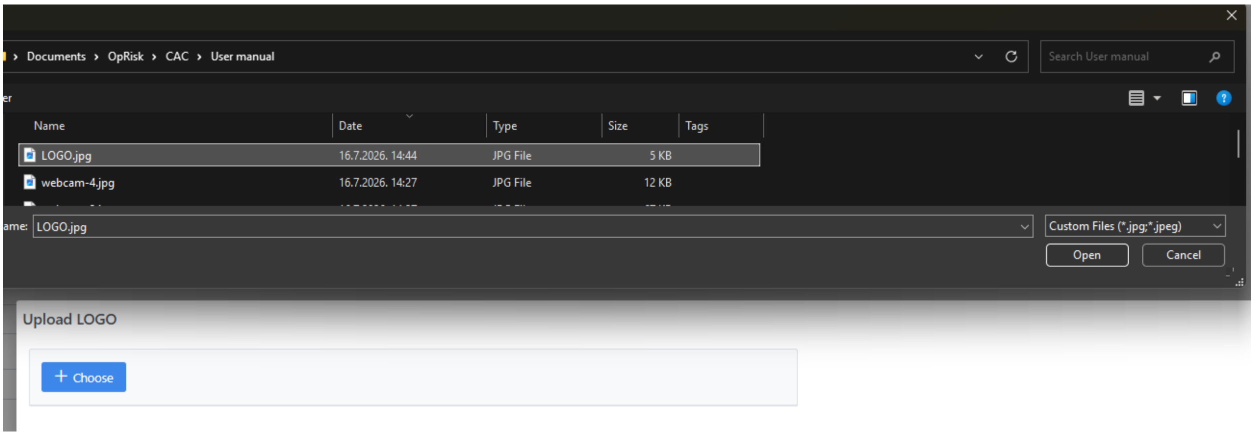
Below the form fields, the following upload actions are available:

- Upload logo — uploads the company logo used on the EU Declaration of Conformity
- Upload signature — uploads the authorised signature used on the EU Declaration of Conformity

Uploading a logo

1. Click Upload logo.
2. The Upload LOGO dialog opens.
3. Click + Choose.
4. Select an image file in the system file chooser (for example, LOGO.jpg).
5. Confirm with Open.
6. Click Save on the Account information page to store the changes.





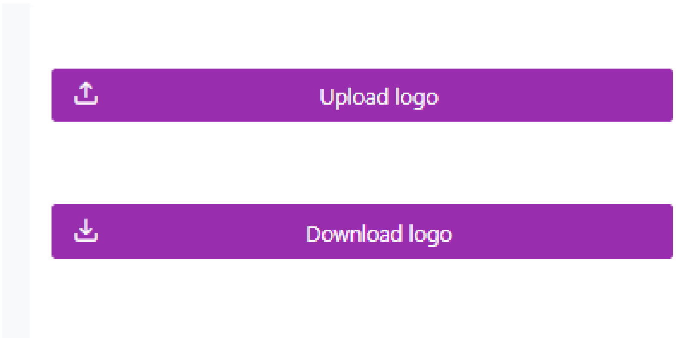
Uploading a signature follows the same steps using Upload signature.

Downloading logo and signature

Download logo and Download signature become available only after the corresponding file has been uploaded.

- Download logo — available after a logo has been uploaded; downloads the stored logo file
- Download signature — available after a signature has been uploaded; downloads the stored signature file

If a logo or signature has not yet been uploaded, the related download action is not available for use.



Saving

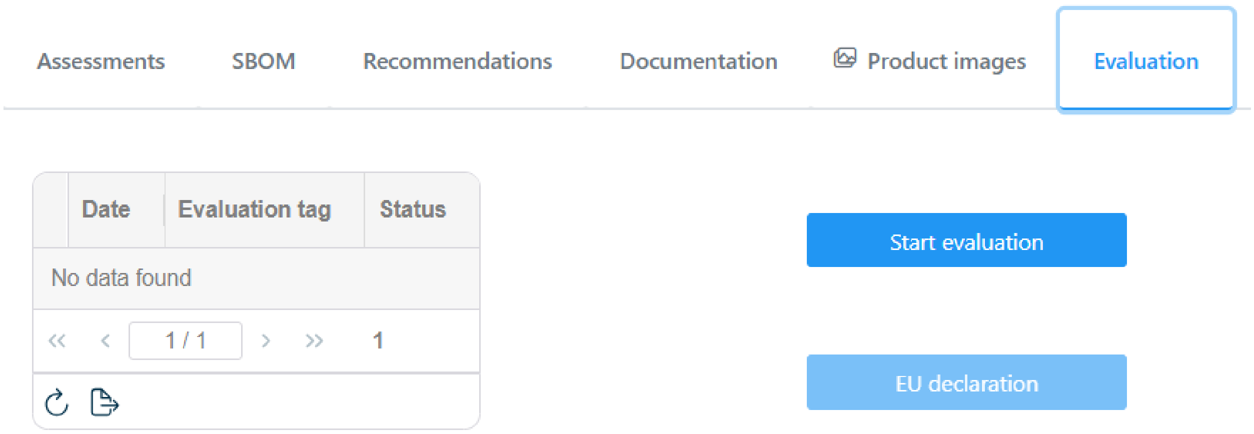
After entering or changing data, or after uploading a logo or signature, click Save (bottom right).

A success notification is shown when the data or uploaded files are saved successfully.

Note: Logo and signature uploaded on this page are used when generating the EU Declaration of Conformity. Company name is entered here; it is not collected during CURIUM portal registration.

Evaluation tab

The Evaluation tab is used to run the overall product compliance evaluation and to generate the EU Declaration of Conformity.



The tab contains:

- an evaluation history table on the left
- action buttons on the right: **Start evaluation** and **EU declaration**

Initially, if no evaluation has been run, the table displays No data found.

Evaluation history

The evaluation history table contains the following columns:

- Date — date of the evaluation
- Evaluation tag — identifier of the evaluation run
- Status — result of the evaluation (Passed or Failed)

When an evaluation record is selected, additional details for that evaluation are shown (evaluation steps and their status).

Evaluation steps

For a selected evaluation, the system checks the following steps:

- **Assessment** — the latest assessment result must be Good or Excellent, or a valid manual override must exist
- **Recommendation** — an action must be recorded for every recommendation (Acknowledged or Not applicable)
- **Documentation** — all required documentation that is not marked as **Not applicable** or postponed (Later) must be uploaded
- All steps must be **Passed** for the overall evaluation to be Passed.

Starting an evaluation

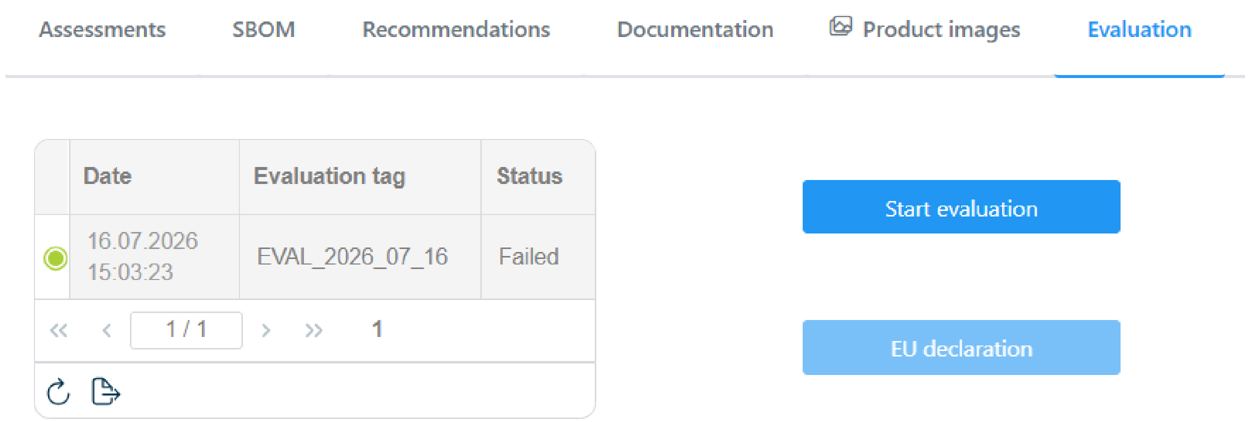
1. Open the Evaluation tab.
2. Click Start evaluation.
3. Wait for the evaluation to complete.

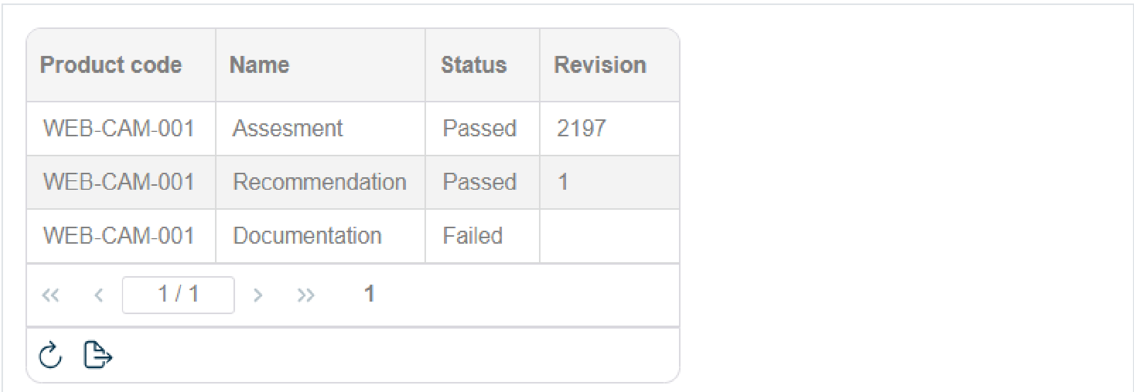
Review the new row in the evaluation history table and its Status (Passed or Failed).

If the evaluation status is Failed, review the failed step(s), correct the issues (assessment, recommendations, or documentation), and start a new evaluation.

Example: Failed evaluation

After clicking **Start evaluation**, a new row appears in the evaluation history table.





Select the evaluation row to display the evaluation steps in the lower table.

In this example:

- **Assessment** passed
- **Recommendation** passed
- **Documentation** failed → overall evaluation status is **Failed**

When a step fails, the user should:

1. Open the related tab (for example, **Documentation**).
2. Correct the missing or incomplete items.
3. Return to the **Evaluation** tab.
4. Click **Start evaluation** again.

The **EU declaration** remains unavailable until the latest evaluation status is **Passed**.

Example: Passed evaluation

When all evaluation steps are successful, the evaluation history shows status **Passed**.

Product code	Name	Status	Revision
WEB-CAM-001	Assesment	Passed	2197
WEB-CAM-001	Recommendation	Passed	1
WEB-CAM-001	Documentation	Passed	

1 / 1 1

In this case, Assessment, Recommendation, and Documentation are all **Passed**, so the overall evaluation status is **Passed**. The user can then click **EU declaration** to generate the Declaration of Conformity.

EU declaration

The **EU declaration** button generates the Declaration of Conformity.

Downloading or opening the declaration is only possible if the latest evaluation status is **Passed**.

For the contents of the PDF, preconditions, and download file name, see **Declaration of Conformity**.

Declaration of Conformity

After the latest product evaluation status is **Passed**, the user can generate the EU Declaration of Conformity.

On the **Evaluation** tab, click **EU declaration**. The system generates a PDF declaration for the selected product.

Example of Declaration of conformity

EU declaration of conformity

Company name: CS
Postal address: Savska cesta 129
Postal code: 1000
City: Zagreb
Phone number: 00987654321

Declare that the DoC is issued under our sole responsibility and belongs to the following product:

Product: Web camera
Type: SMART_HOME
Batch: 1
Serial number: 12390910

The object of the DoC described above is in conformance with the relevant EU harmonized legislation:

EU Regulation on Software Product Risk Management (EU-SPRM) 2025/789

The following harmonized standards and technical specifications have been applied:

EN ISO 34567-1:2024 — Software Risk Assessment Methods, EN 78901-2:2023 — Cybersecurity Requirements for Software Products, EN ISO 45210-3:2025 — Functional Safety in Software Development, EN 56789-4:2024 — Quality Assurance for Risk Evaluation Tools

Object of the declaration (identification of the product allowing traceability, may include color images, where necessary for the identification of the product)

Notified body

Additional information

Signed from and on behalf of

Zagreb	16.07.2026	CAC CURIUM

Preconditions

Before generating the declaration, ensure that:

- the latest evaluation status is **Passed**
- **Account information** is completed (company details, logo, signature)

- product data is entered (name, type, batch, serial number, legislation, standards)
- product images are uploaded on the **Product images** tab (up to four images)

Contents of the EU Declaration of Conformity

The generated PDF contains:

- **Title:** EU declaration of conformity
- **Manufacturer / company details** from Account information (company name, postal address, postcode, city, phone number)
- **Company logo** and authorised **signature** from Account information
- **Product identification:**
    - Product name (for example, Web camera)
    - Product code / type
    - Batch
    - Serial number
- **Statement** that the declaration is issued under the manufacturer's sole responsibility
- **Relevant EU legislation** (for example, EU Regulation on Software Product Risk Management (EU-SPRM) 2025/789)
- **Harmonized standards** applied (for example, EN ISO 34567-1:2024, EN 78901-2:2023, EN ISO 45210-3:2025, EN 56789-4:2024)
- **Product images** for identification / traceability (from Product images tab)
- **Notified body** and **Additional information**, if provided
- Place and date of issue, and signature block

Downloading the declaration

The declaration is downloaded as a PDF file named after the product code, for example:
WEB-CAM-001_EU_DECLARATION.pdf

The user can open, store, and attach this file as official proof of the completed evaluation process.

Note:
If **EU declaration** is unavailable or the generated document is incomplete, check:

1. Evaluation status is **Passed**
2. Account information (logo/signature uploaded and saved)
3. Product images uploaded
4. Product legislation and standards filled in