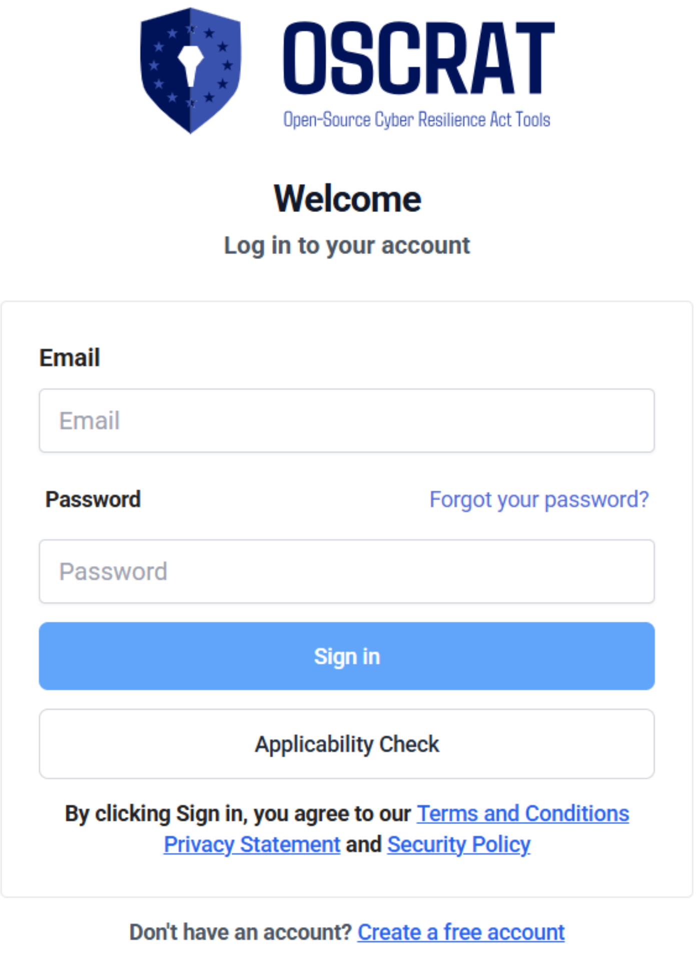
OSCART WORKSHOP
THE OSCART PLATFORM

Yasen Tanev

Registration and Log in



OSCRAT

Open-Source Cyber Resilience Act Tools

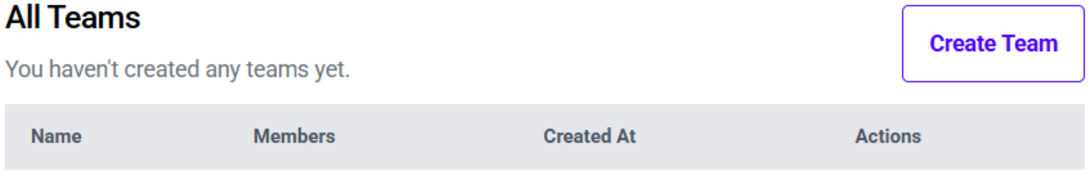
Welcome

Log in to your account

By clicking Sign in, you agree to our Terms and Conditions Privacy Statement and Security Policy

Don't have an account? Create a free account

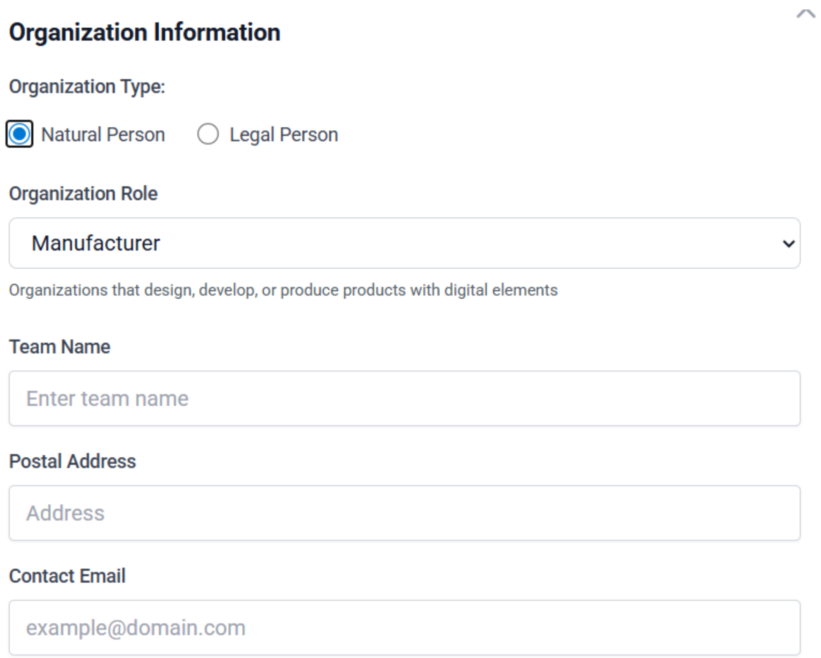
Team in the core of the project



All Teams

You haven't created any teams yet.

Name	Members	Created At	Actions



Organization Information

Organization Type:

● Natural Person ○ Legal Person

Organization Role

Manufacturer

Organizations that design, develop, or produce products with digital elements

Team Name

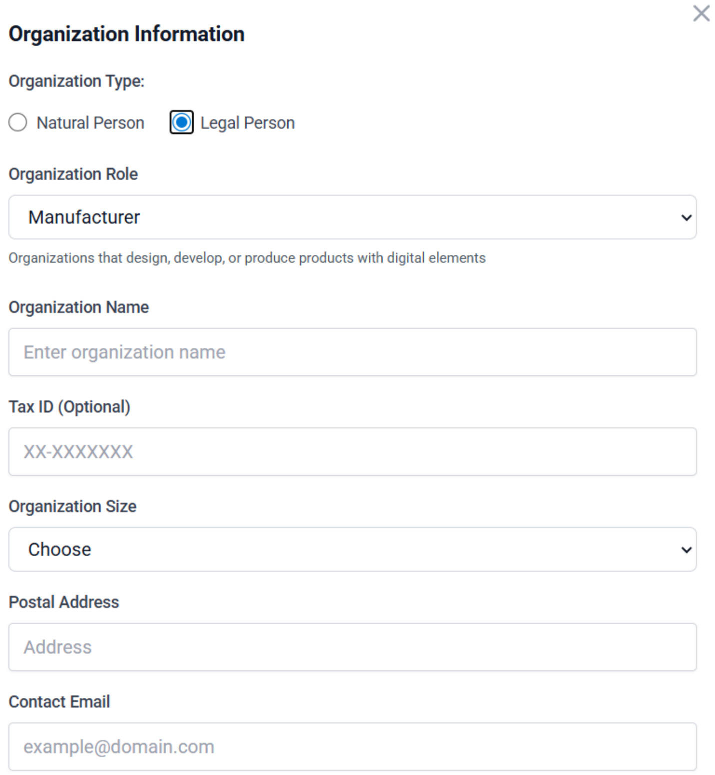
Enter team name

Postal Address

Address

Contact Email

example@domain.com



Organization Information

Organization Type:

○ Natural Person ● Legal Person

Organization Role

Manufacturer

Organizations that design, develop, or produce products with digital elements

Organization Name

Enter organization name

Tax ID (Optional)

XX-XXXXXXX

Organization Size

Choose

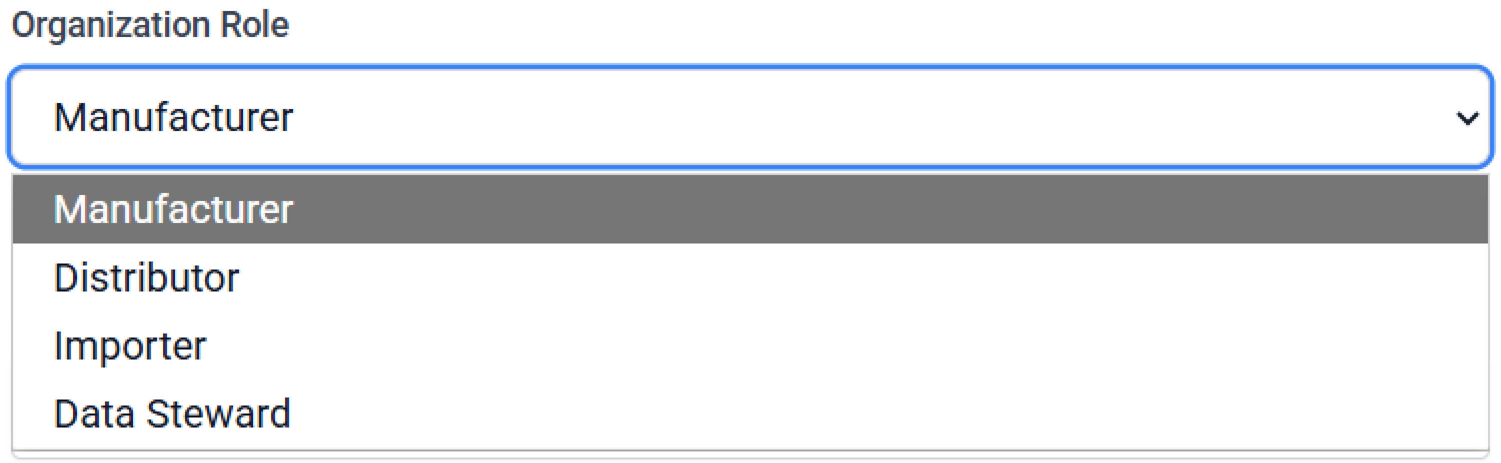
Postal Address

Address

Contact Email

example@domain.com

Specific roles = specific needs



Organization Role

Manufacturer

How to Choose

- If you **make the product** → Manufacturer
- If you **resell domestically sourced products** → Distributor
- If you **bring products across borders** → Importer
- If you **manage product or compliance data on behalf of others** → Data Steward

Organization Role Definitions

- Manufacturer

Select this if your organization produces or assembles the product. This includes companies that design, fabricate, or brand goods under their own name and are responsible for production specifications and compliance at the point of manufacture.

- Distributor

Choose this if your organization purchases finished products and resells them to retailers, wholesalers, or end customers, without materially altering the product.

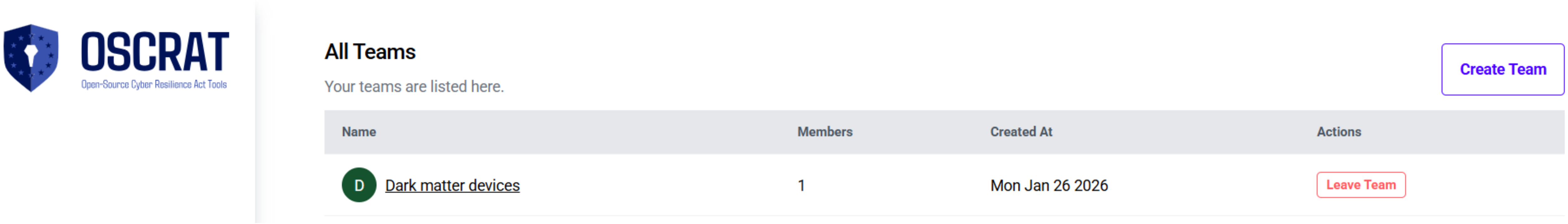
- Importer

This role applies if your organization brings products into a country from abroad and is legally responsible for customs clearance, regulatory compliance, and related import obligations, regardless of whether you manufactured the product.

- Data Steward

Select this if your organization’s responsibility is managing, maintaining, or submitting product data (e.g., regulatory filings, product catalogs, compliance records) rather than manufacturing, selling, or importing the product itself.

When team is ready, it is time for activities

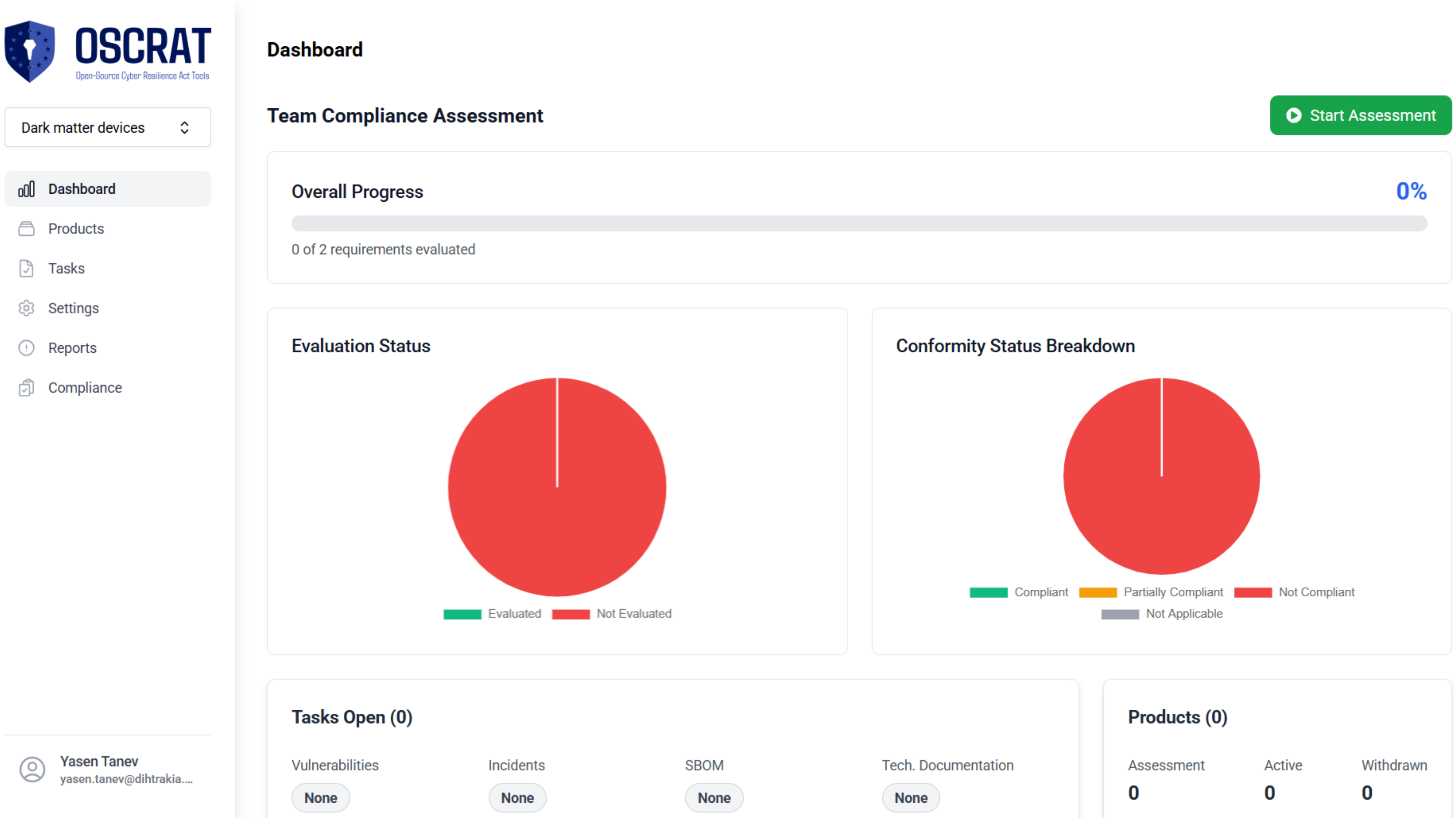


All Teams

Your teams are listed here.

Name	Members	Created At	Actions
D Dark matter devices	1	Mon Jan 26 2026	Leave Team

Operational dashboard – the hearth of compliance



OSCRAT
Open-Source Cyber Resilience Act Tools

Dark matter devices

- Dashboard
- Products
- Tasks
- Settings
- Reports
- Compliance

Yasen Tanev
yasen.tanev@dihtrakia....

Dashboard

Team Compliance Assessment

▶ Start Assessment

Overall Progress 0%

0 of 2 requirements evaluated

Evaluation Status

🟩 Evaluated 🟥 Not Evaluated

Conformity Status Breakdown

🟩 Compliant 🟧 Partially Compliant 🟥 Not Compliant
⬜ Not Applicable

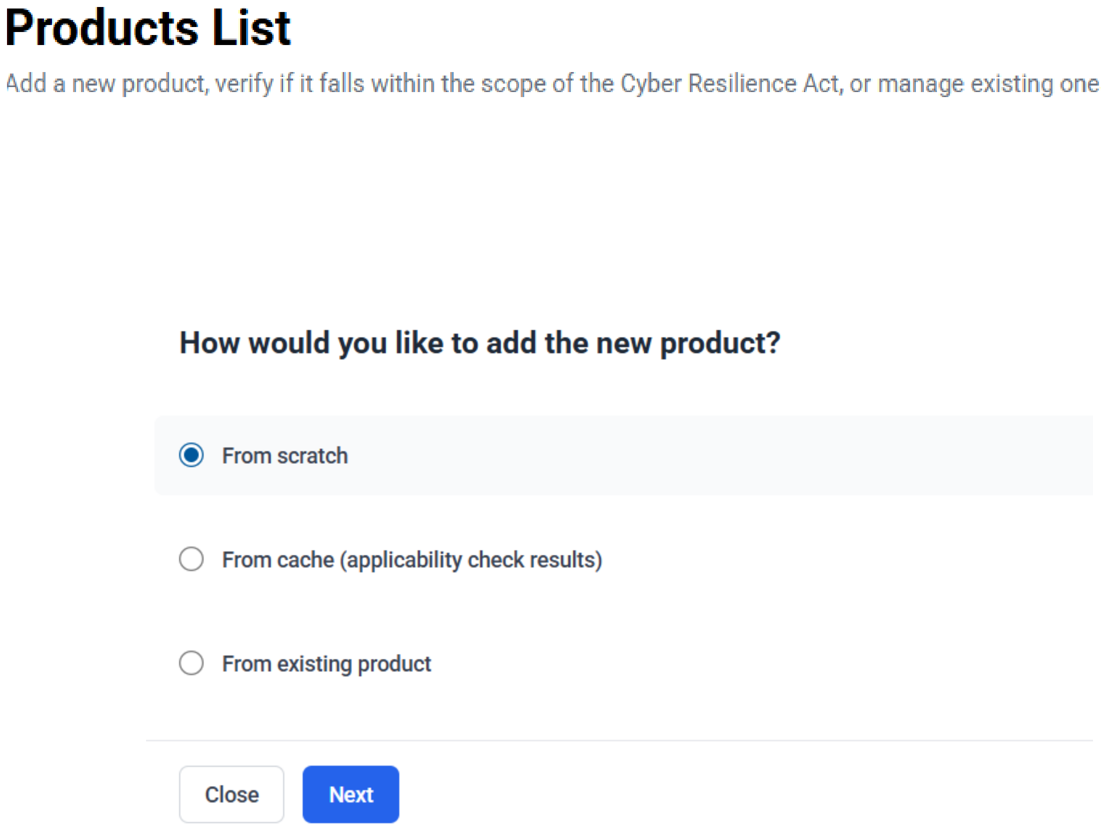
Tasks Open (0)

Vulnerabilities	Incidents	SBOM	Tech. Documentation
None	None	None	None

Products (0)

Assessment	Active	Withdrawn
0	0	0

CRA is about the products



Products List

Add a new product, verify if it falls within the scope of the Cyber Resilience Act, or manage existing ones.

How would you like to add the new product?

● From scratch

○ From cache (applicability check results)

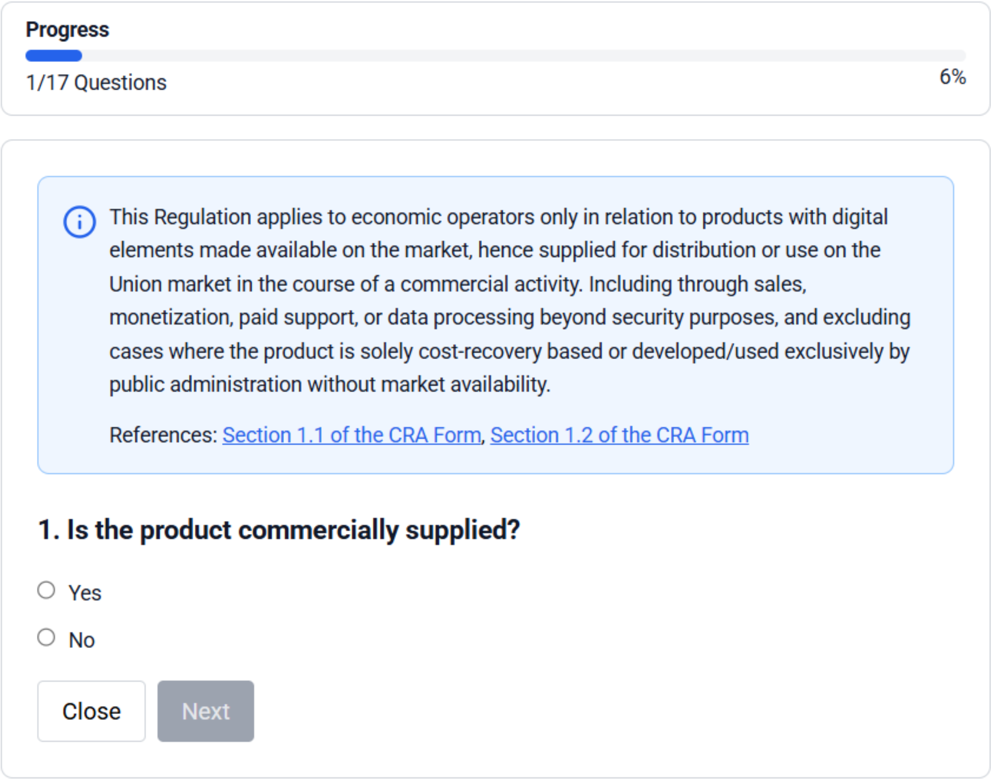
○ From existing product

From scratch
Create a new product by first completing the applicability survey. Once the survey is finished, a new product template is generated based on the survey results.

From cache (applicability check results)
Create a new product using a previously completed applicability survey that is already stored in the system. The survey does not need to be repeated, and no product has been created from it yet.

From existing product
Create a new product by copying data from an existing product. The new product will be pre-populated with the existing product's information and can be adjusted as needed.

From scratch – 17 questions



Progress

1/17 Questions 6%

This Regulation applies to economic operators only in relation to products with digital elements made available on the market, hence supplied for distribution or use on the Union market in the course of a commercial activity. Including through sales, monetization, paid support, or data processing beyond security purposes, and excluding cases where the product is solely cost-recovery based or developed/used exclusively by public administration without market availability.

References: Section 1.1 of the CRA Form, Section 1.2 of the CRA Form

1. Is the product commercially supplied?

○ Yes

○ No

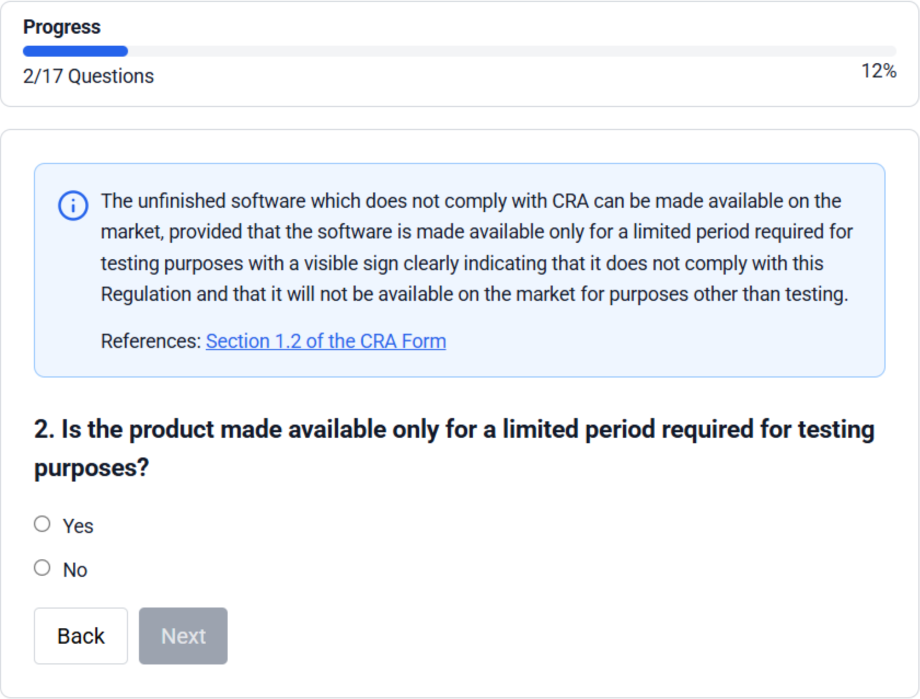
Answer "Yes" if:

- The product is sold, licensed, or subscribed to
- The product generates revenue directly or indirectly
- The product is made available on the EU market to customers or users

Answer "No" if:

- The product is used only internally
- The product is provided only at cost-recovery
- The product is used exclusively by public authorities and not placed on the market

Question 2 – for Q1 – No only



Progress

2/17 Questions 12%

The unfinished software which does not comply with CRA can be made available on the market, provided that the software is made available only for a limited period required for testing purposes with a visible sign clearly indicating that it does not comply with this Regulation and that it will not be available on the market for purposes other than testing.

References: Section 1.2 of the CRA Form

2. Is the product made available only for a limited period required for testing purposes?

○ Yes

○ No

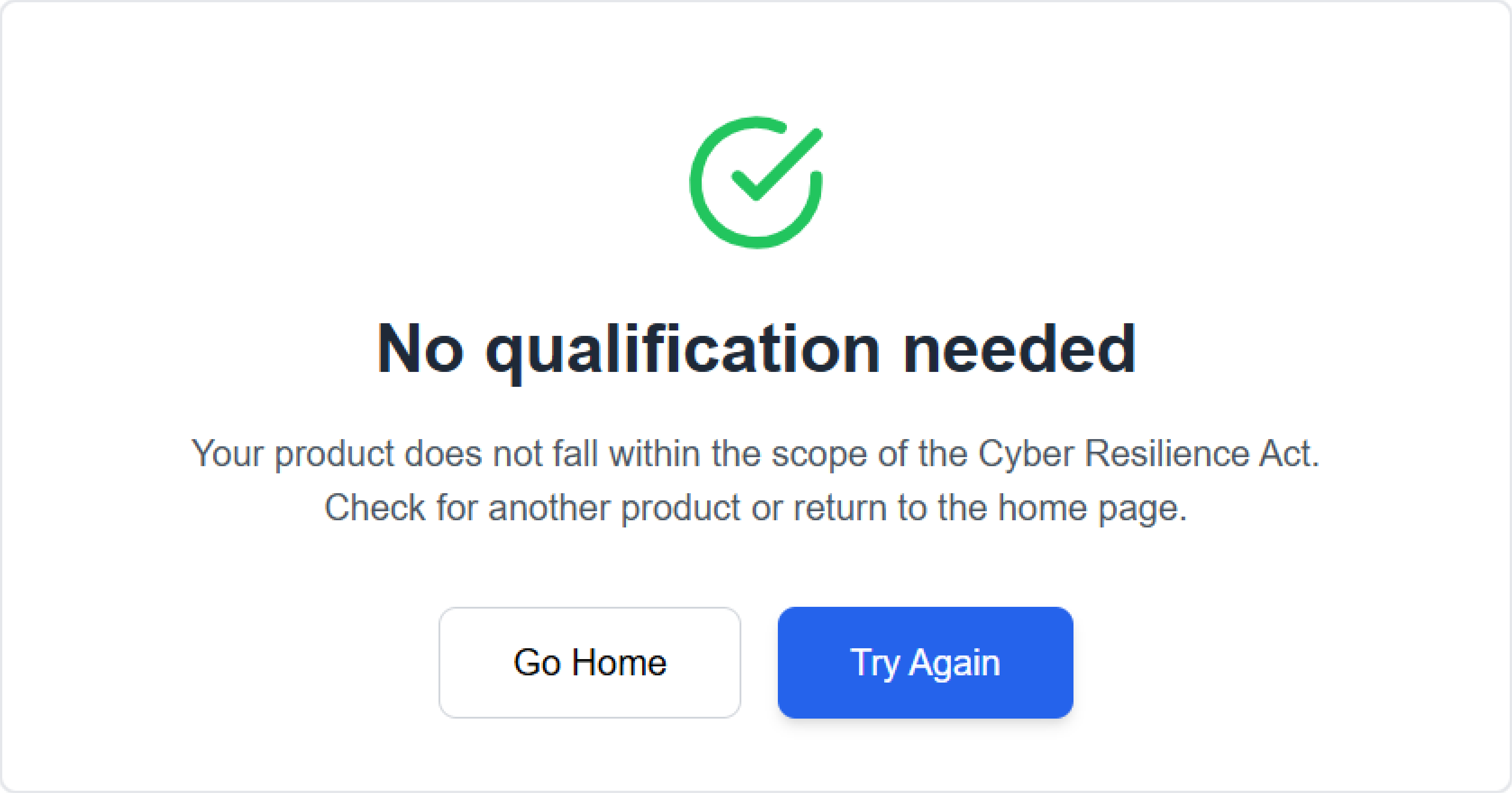
Answer “Yes” if:

- The product is unfinished or pre-release
- It is provided **only for testing or evaluation**
- Access is limited to a **defined, short time period**
- It is clearly labeled as **non-compliant and for testing only**

Answer “No” if:

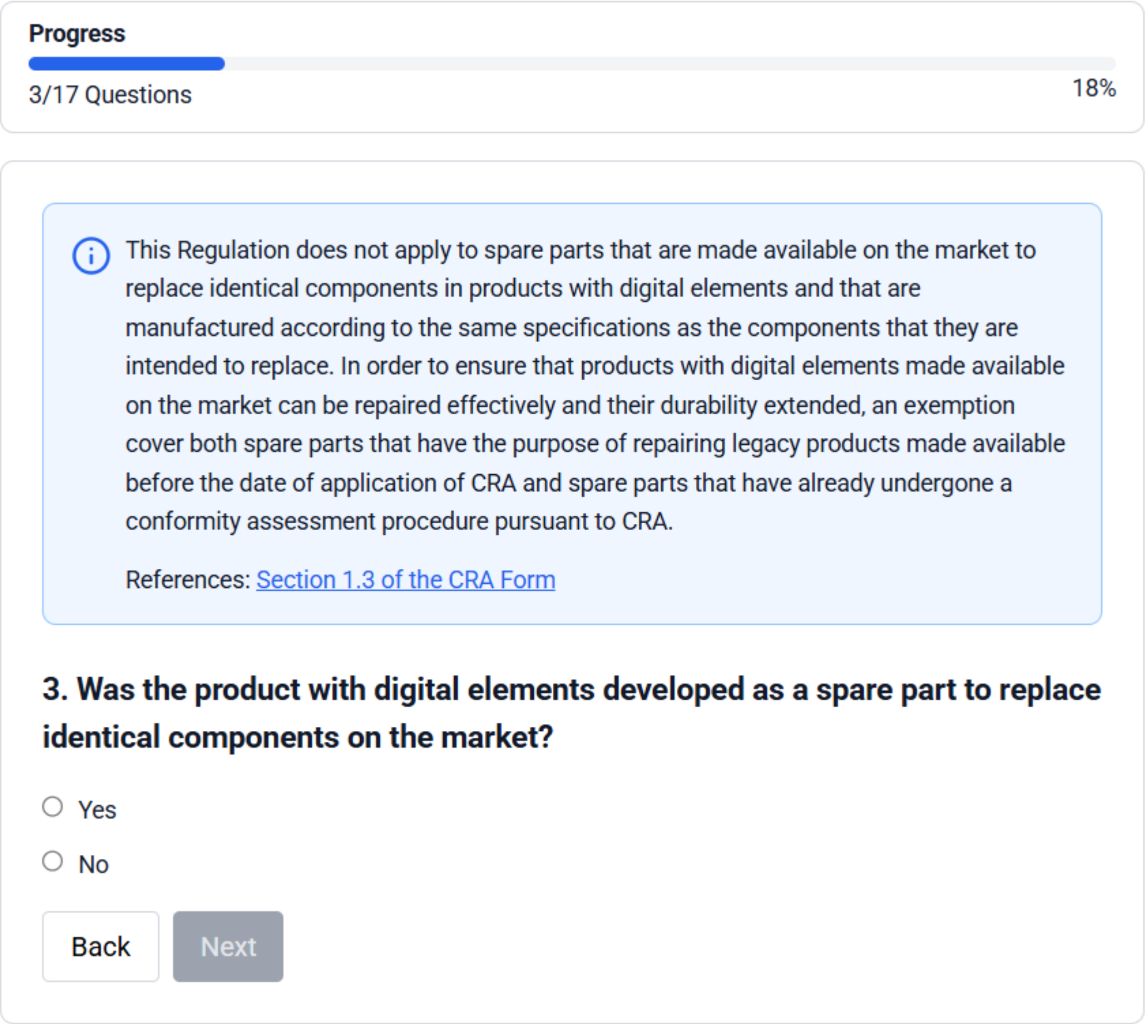
- The product is intended for regular use
- It is available beyond testing purposes
- It is or will be placed on the market for normal operation

If Q2 is yes, then product is out of scope



No qualification needed

Your product does not fall within the scope of the Cyber Resilience Act. Check for another product or return to the home page.



This Regulation does not apply to spare parts that are made available on the market to replace identical components in products with digital elements and that are manufactured according to the same specifications as the components that they are intended to replace. In order to ensure that products with digital elements made available on the market can be repaired effectively and their durability extended, an exemption cover both spare parts that have the purpose of repairing legacy products made available before the date of application of CRA and spare parts that have already undergone a conformity assessment procedure pursuant to CRA.

References: Section 1.3 of the CRA Form

3. Was the product with digital elements developed as a spare part to replace identical components on the market?

○ Yes

○ No

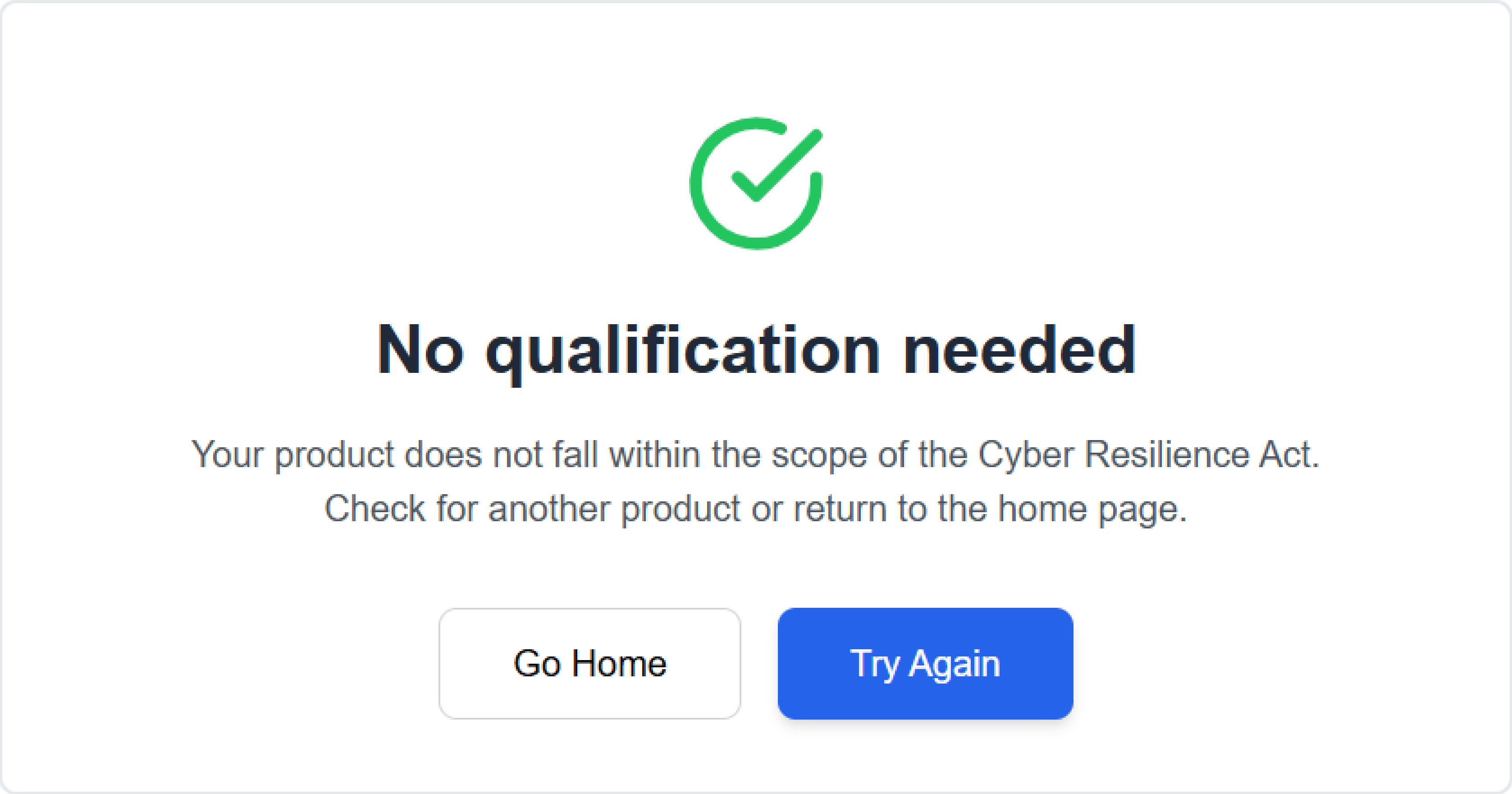
Answer "Yes" if:

- The product is a **spare or replacement part**
- It replaces an **identical component** in an existing product
- It is manufactured to the **same specifications** as the original component
- It is intended to **repair or maintain** an existing product on the market

Answer "No" if:

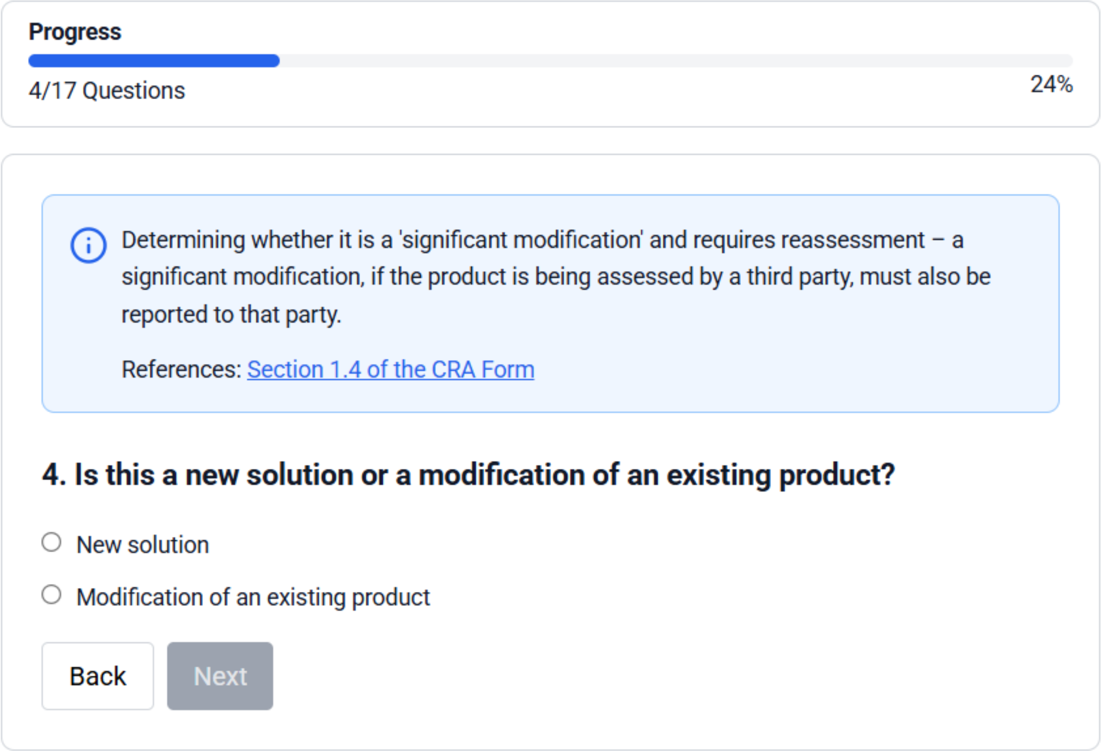
- The product is a **new or upgraded component**
- It adds new functionality or changes behavior
- It is not identical to the component being replaced
- It is intended for **new products**, not repairs

If Q3 is yes, then product is out of scope



No qualification needed

Your product does not fall within the scope of the Cyber Resilience Act.
Check for another product or return to the home page.



Determining whether it is a 'significant modification' and requires reassessment – a significant modification, if the product is being assessed by a third party, must also be reported to that party.

References: Section 1.4 of the CRA Form

4. Is this a new solution or a modification of an existing product?

○ New solution

○ Modification of an existing product

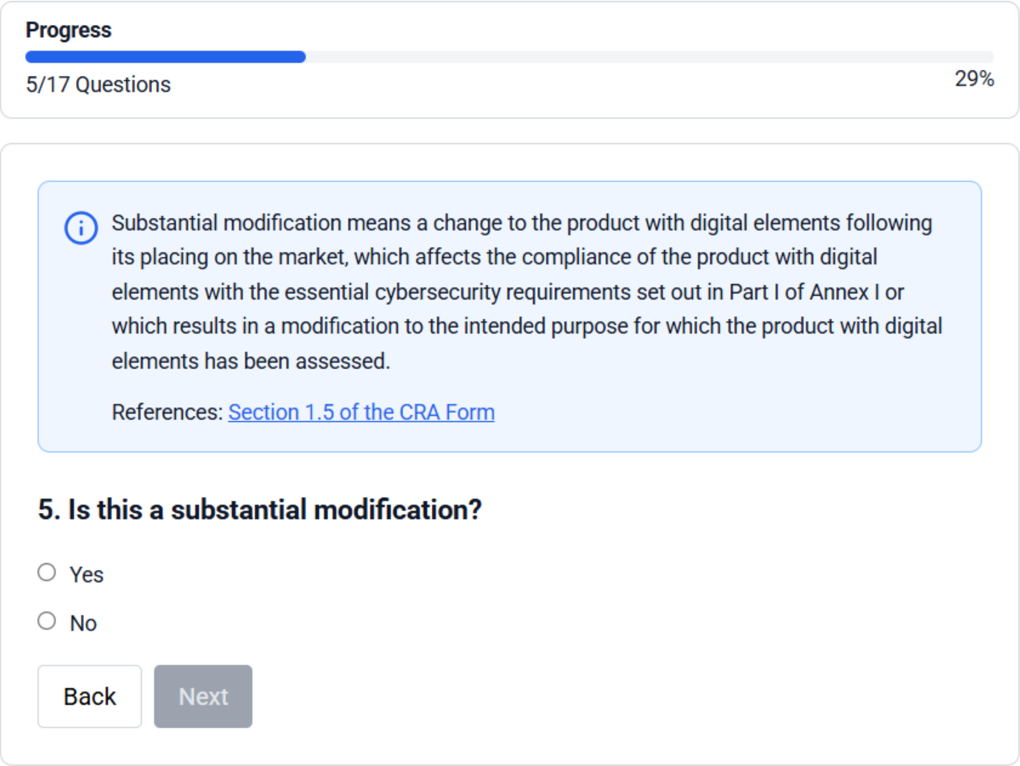
Select "New solution" if:

- The product has **not been placed on the market before**
- It is a **new product or new product line**
- It is not based on an already certified or marketed product

Select "Modification of an existing product" if:

- The product already exists on the market
- You have **changed, updated, or enhanced** an existing product
- The change may affect functionality, security, or compliance

Modification of an existing product – YES then Q5



Progress

5/17 Questions 29%

Substantial modification means a change to the product with digital elements following its placing on the market, which affects the compliance of the product with digital elements with the essential cybersecurity requirements set out in Part I of Annex I or which results in a modification to the intended purpose for which the product with digital elements has been assessed.

References: Section 1.5 of the CRA Form

5. Is this a substantial modification?

○ Yes

○ No

Answer "Yes" if the change:

•Was made after the product was placed on the market

•Affects cybersecurity compliance or essential security requirements

•Changes the intended purpose or use of the product

•Introduces new functionality that impacts security or risk

Answer "No" if the change:

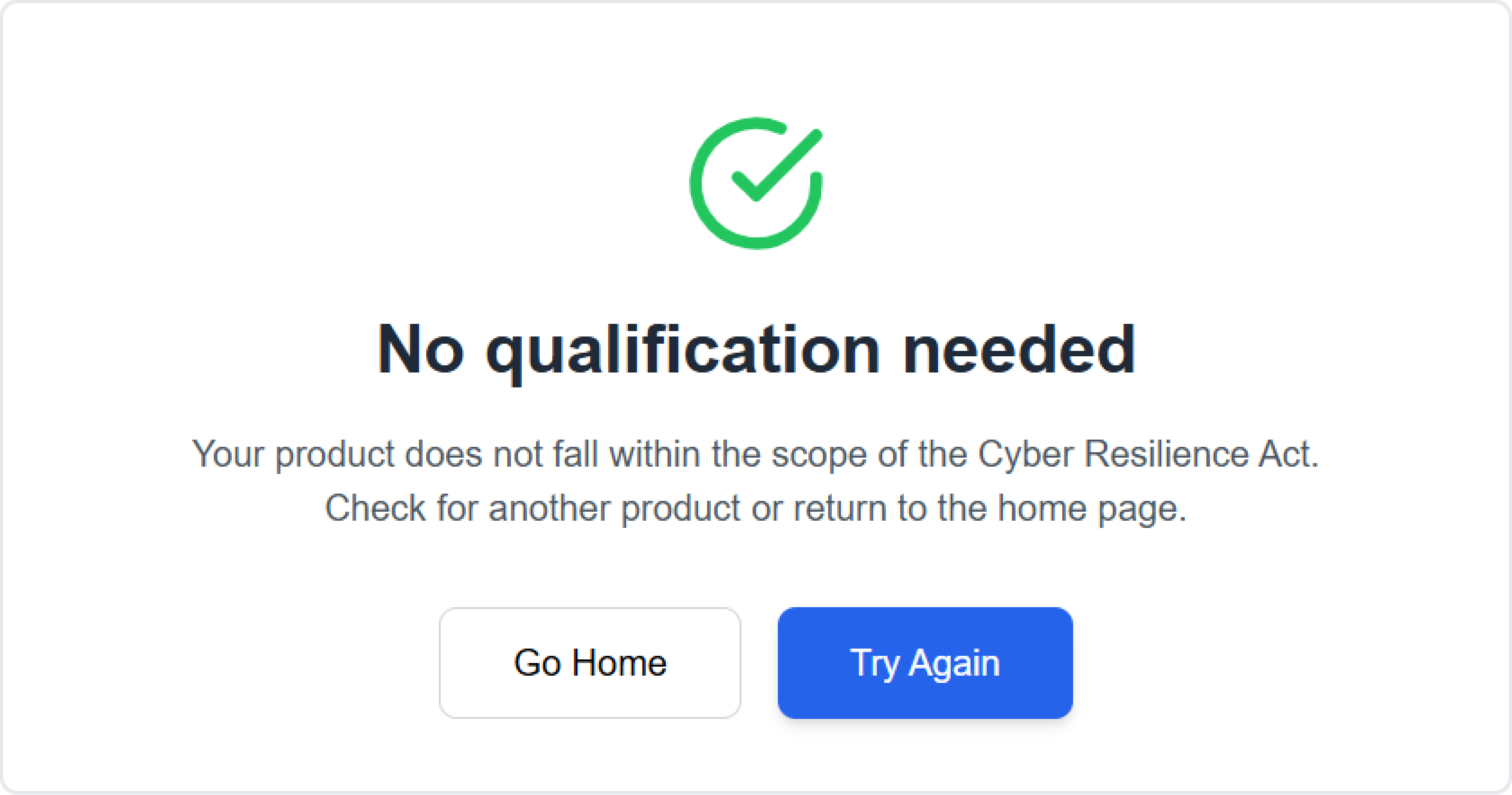
•Is a minor update or bug fix

•Does not affect security or compliance

•Does not change the intended purpose

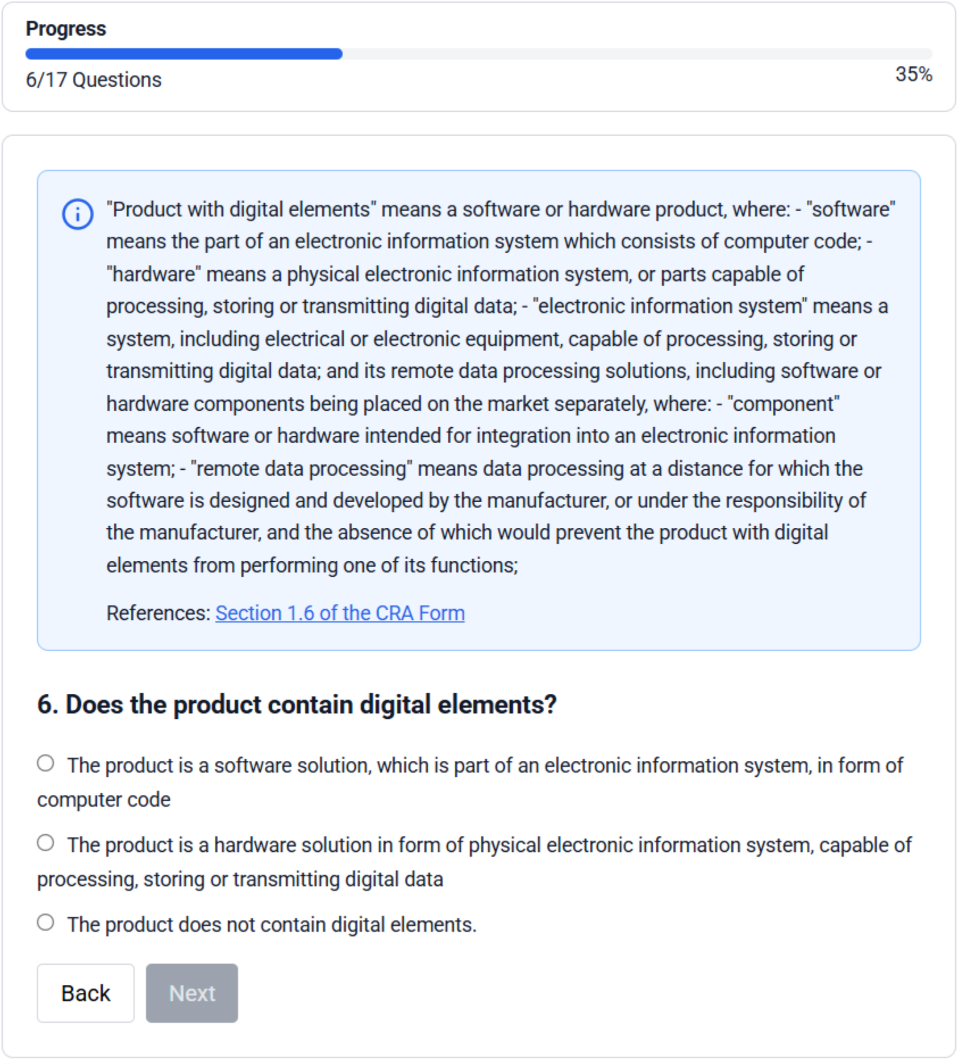
•Is routine maintenance or patching

If Q5 is no, then product is out of scope



No qualification needed

Your product does not fall within the scope of the Cyber Resilience Act.
Check for another product or return to the home page.



"Product with digital elements" means a software or hardware product, where: - "software" means the part of an electronic information system which consists of computer code; - "hardware" means a physical electronic information system, or parts capable of processing, storing or transmitting digital data; - "electronic information system" means a system, including electrical or electronic equipment, capable of processing, storing or transmitting digital data; and its remote data processing solutions, including software or hardware components being placed on the market separately, where: - "component" means software or hardware intended for integration into an electronic information system; - "remote data processing" means data processing at a distance for which the software is designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions;

References: Section 1.6 of the CRA Form

6. Does the product contain digital elements?

○ The product is a software solution, which is part of an electronic information system, in form of computer code

○ The product is a hardware solution in form of physical electronic information system, capable of processing, storing or transmitting digital data

○ The product does not contain digital elements.

Select “Software solution” if:

- The product consists of **software or code**
- It runs on or is part of an electronic information system
- It provides functionality through digital processing

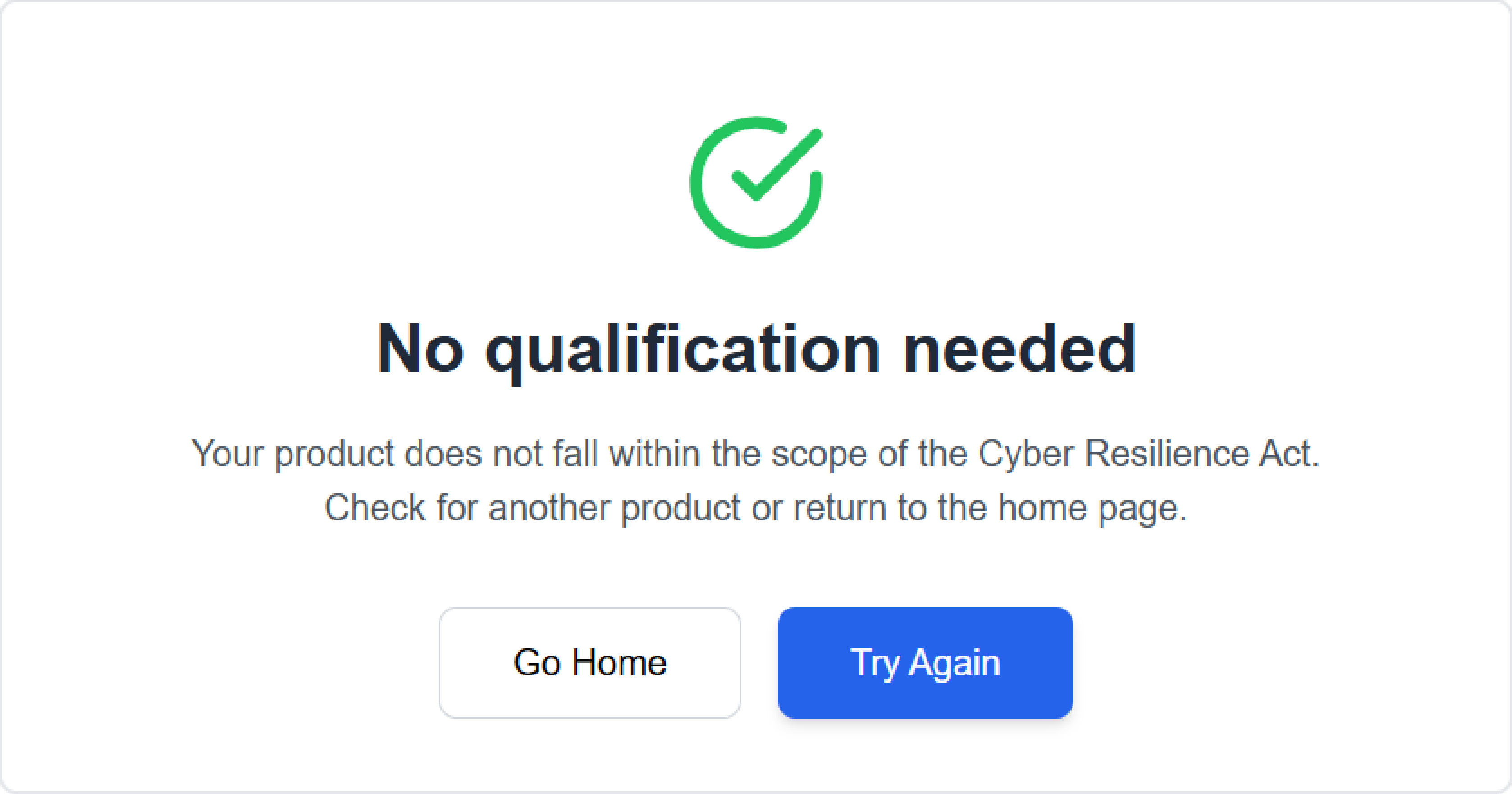
Select “Hardware solution” if:

- The product is **physical electronic equipment**
- It processes, stores, or transmits digital data
- It contains embedded software or firmware

Select “Does not contain digital elements” if:

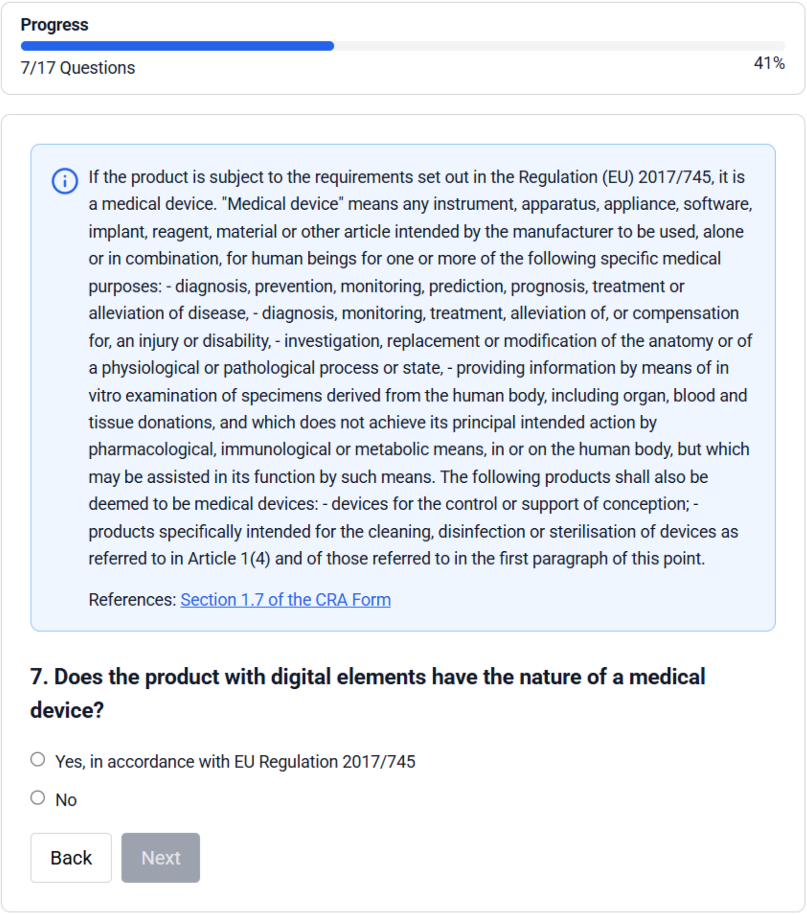
- The product is **purely mechanical or analog**
- It does not process, store, or transmit digital data
- It contains no software, firmware, or digital components

If Q6 is The product does not contain digital elements, then product is out of scope



No qualification needed

Your product does not fall within the scope of the Cyber Resilience Act.
Check for another product or return to the home page.



If the product is subject to the requirements set out in the Regulation (EU) 2017/745, it is a medical device. "Medical device" means any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes: - diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease, - diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability, - investigation, replacement or modification of the anatomy or of a physiological or pathological process or state, - providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations, and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means. The following products shall also be deemed to be medical devices: - devices for the control or support of conception; - products specifically intended for the cleaning, disinfection or sterilisation of devices as referred to in Article 1(4) and of those referred to in the first paragraph of this point.

References: Section 1.7 of the CRA Form

7. Does the product with digital elements have the nature of a medical device?

○ Yes, in accordance with EU Regulation 2017/745

○ No

Answer “Yes” if:

•The product is intended for **medical use on humans**

•It supports **diagnosis, monitoring, treatment, or prevention**

•It is regulated as a **medical device under EU MDR (2017/745)**

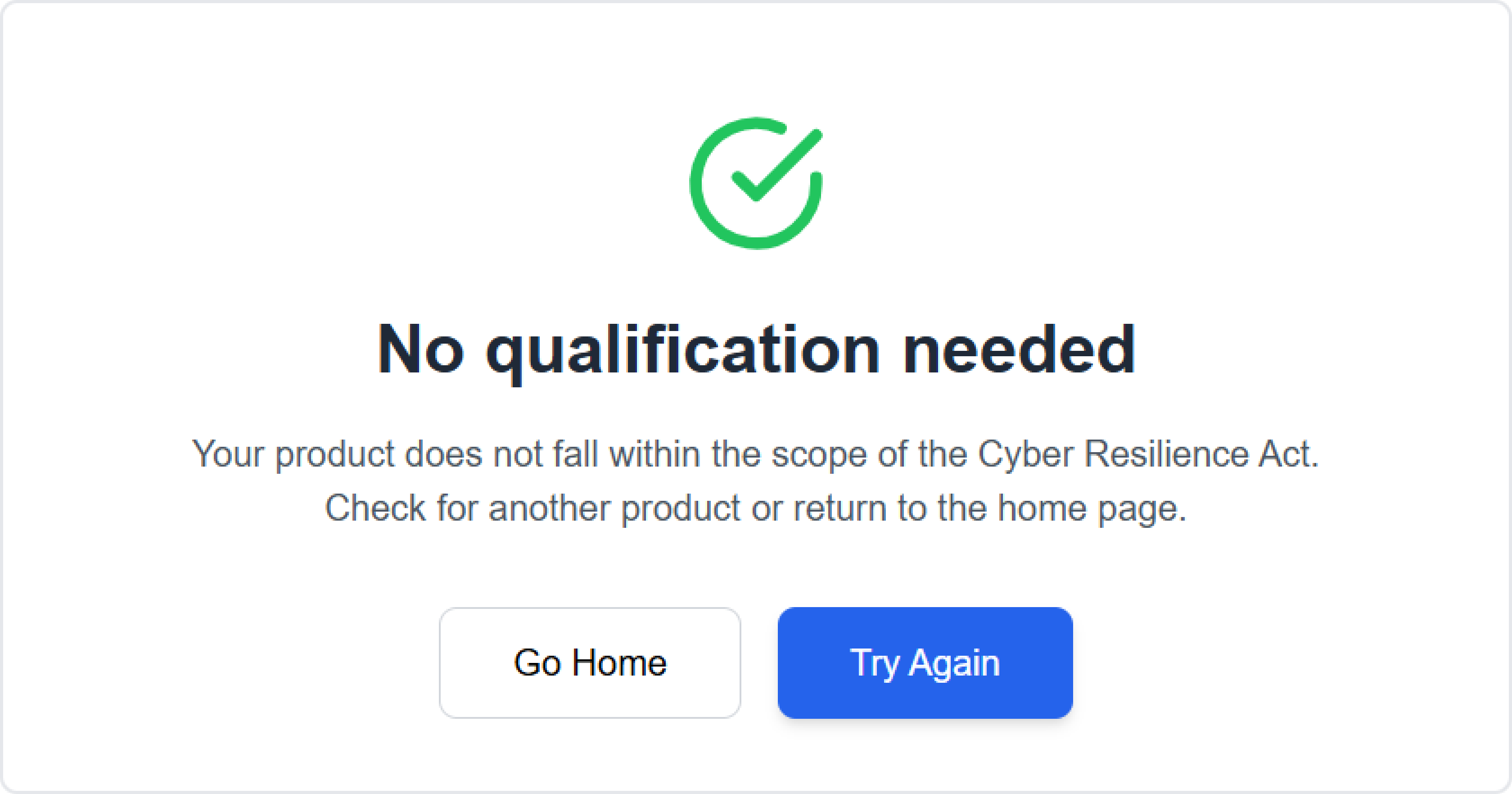
Answer “No” if:

•The product has **no medical purpose**

•It is not regulated under the **EU Medical Device Regulation**

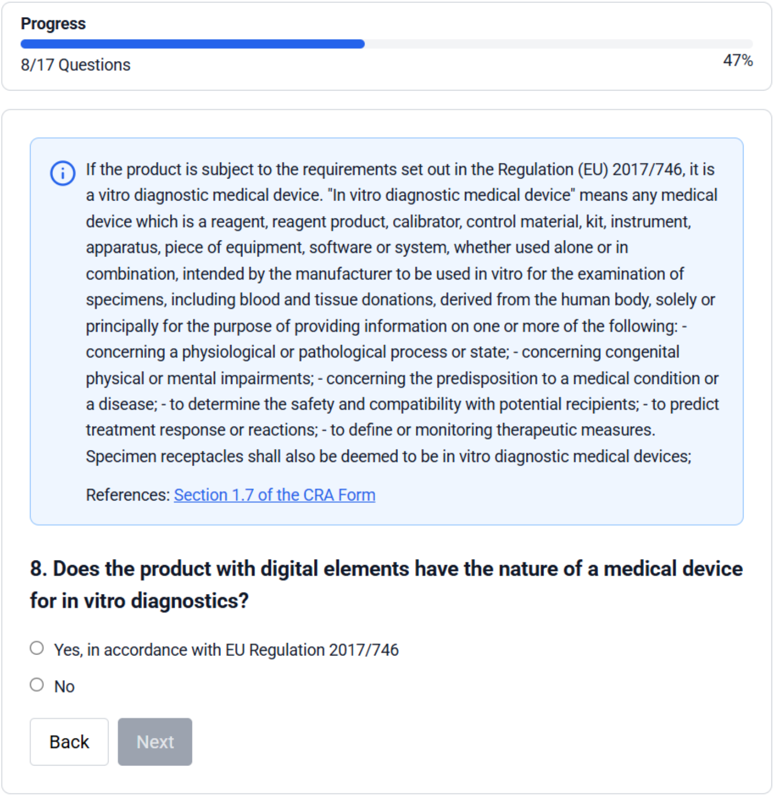
This keeps the guidance minimal while remaining accurate for CRA applicability.

If Q7 is Yes, in accordance with EU Regulation 2017/745



No qualification needed

Your product does not fall within the scope of the Cyber Resilience Act.
Check for another product or return to the home page.



If the product is subject to the requirements set out in the Regulation (EU) 2017/746, it is a vitro diagnostic medical device. "In vitro diagnostic medical device" means any medical device which is a reagent, reagent product, calibrator, control material, kit, instrument, apparatus, piece of equipment, software or system, whether used alone or in combination, intended by the manufacturer to be used in vitro for the examination of specimens, including blood and tissue donations, derived from the human body, solely or principally for the purpose of providing information on one or more of the following: - concerning a physiological or pathological process or state; - concerning congenital physical or mental impairments; - concerning the predisposition to a medical condition or a disease; - to determine the safety and compatibility with potential recipients; - to predict treatment response or reactions; - to define or monitoring therapeutic measures. Specimen receptacles shall also be deemed to be in vitro diagnostic medical devices;

References: Section 1.7 of the CRA Form

8. Does the product with digital elements have the nature of a medical device for in vitro diagnostics?

○ Yes, in accordance with EU Regulation 2017/746

○ No

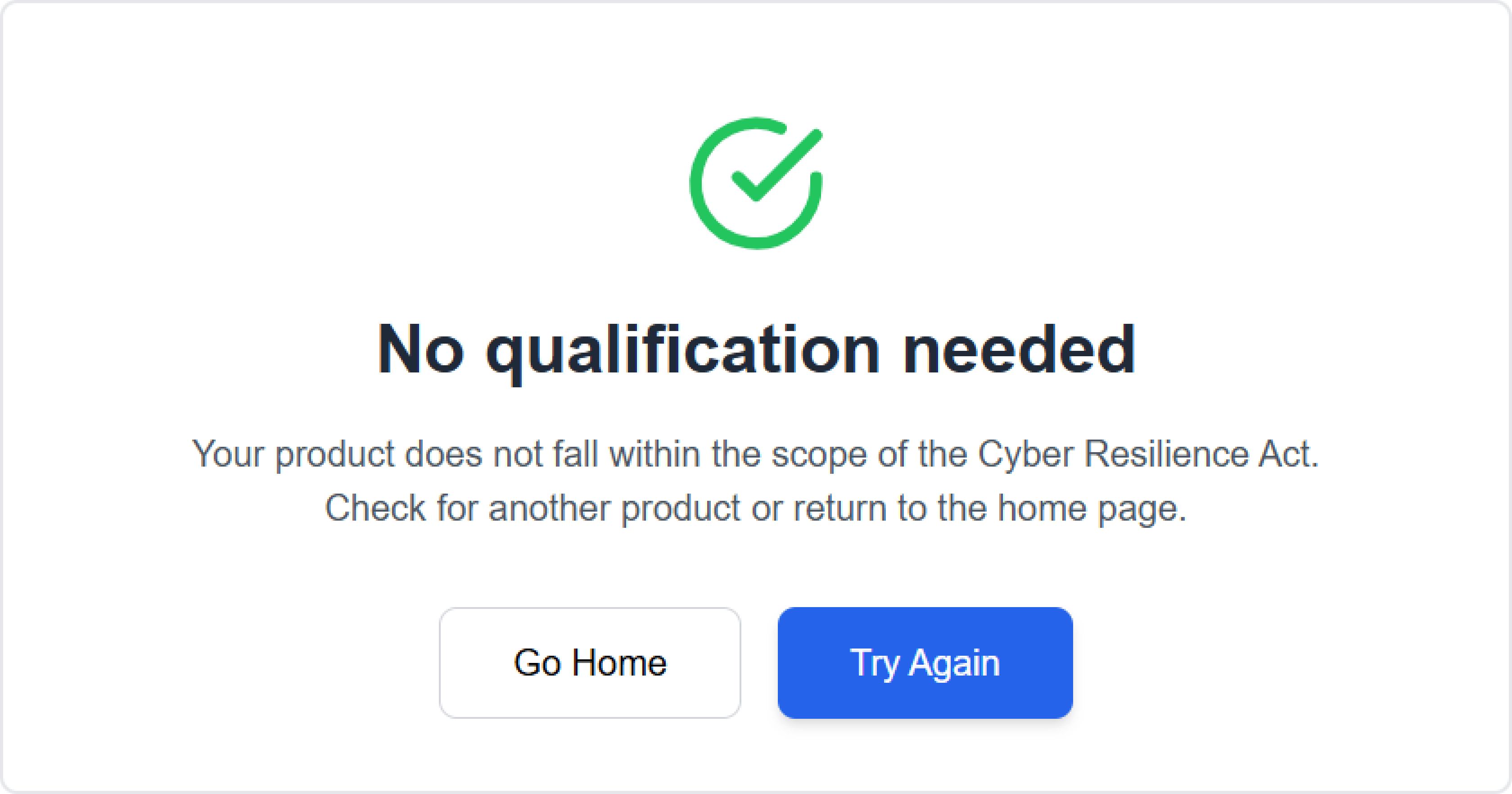
Answer "Yes" if:

- The product is intended for **in vitro examination of human specimens** (e.g. blood, tissue)
- It provides medical information for **diagnosis, monitoring, prediction, or treatment decisions**
- It is regulated as an **IVD medical device under EU Regulation 2017/746 (IVDR)**

Answer "No" if:

- The product is not used for **in vitro diagnostic purposes**
- It does not analyze or support analysis of human specimens
- It is not regulated under the **IVDR**

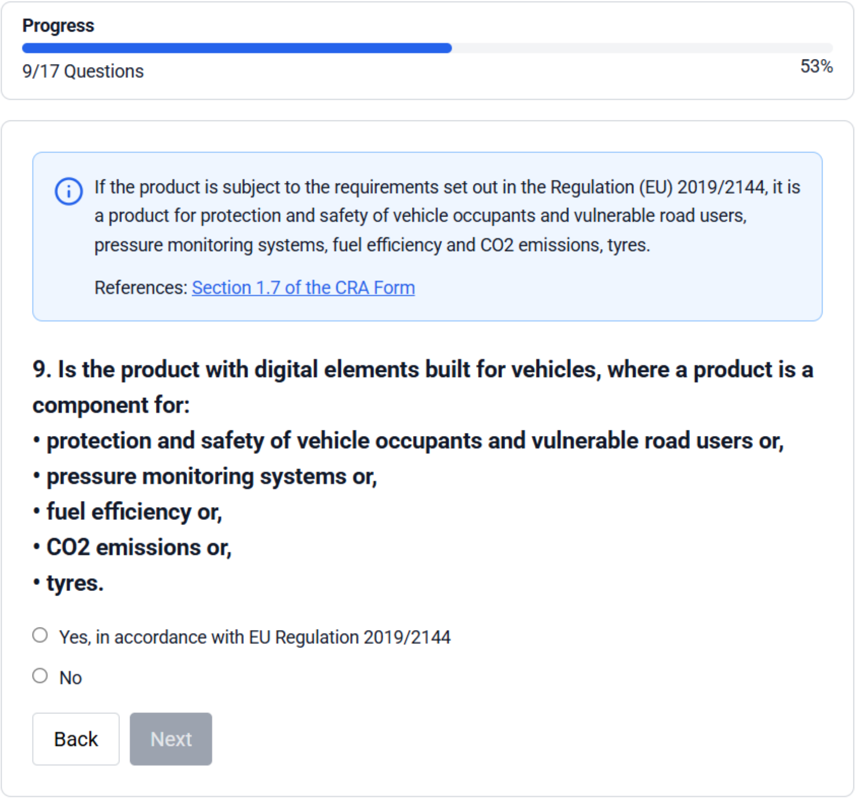
If Q8 is Yes, in accordance with EU Regulation 2017/746



✓

No qualification needed

Your product does not fall within the scope of the Cyber Resilience Act.
Check for another product or return to the home page.



Progress

9/17 Questions 53%

ⓘ If the product is subject to the requirements set out in the Regulation (EU) 2019/2144, it is a product for protection and safety of vehicle occupants and vulnerable road users, pressure monitoring systems, fuel efficiency and CO2 emissions, tyres.

References: Section 1.7 of the CRA Form

9. Is the product with digital elements built for vehicles, where a product is a component for:
• protection and safety of vehicle occupants and vulnerable road users or,
• pressure monitoring systems or,
• fuel efficiency or,
• CO2 emissions or,
• tyres.

○ Yes, in accordance with EU Regulation 2019/2144

○ No

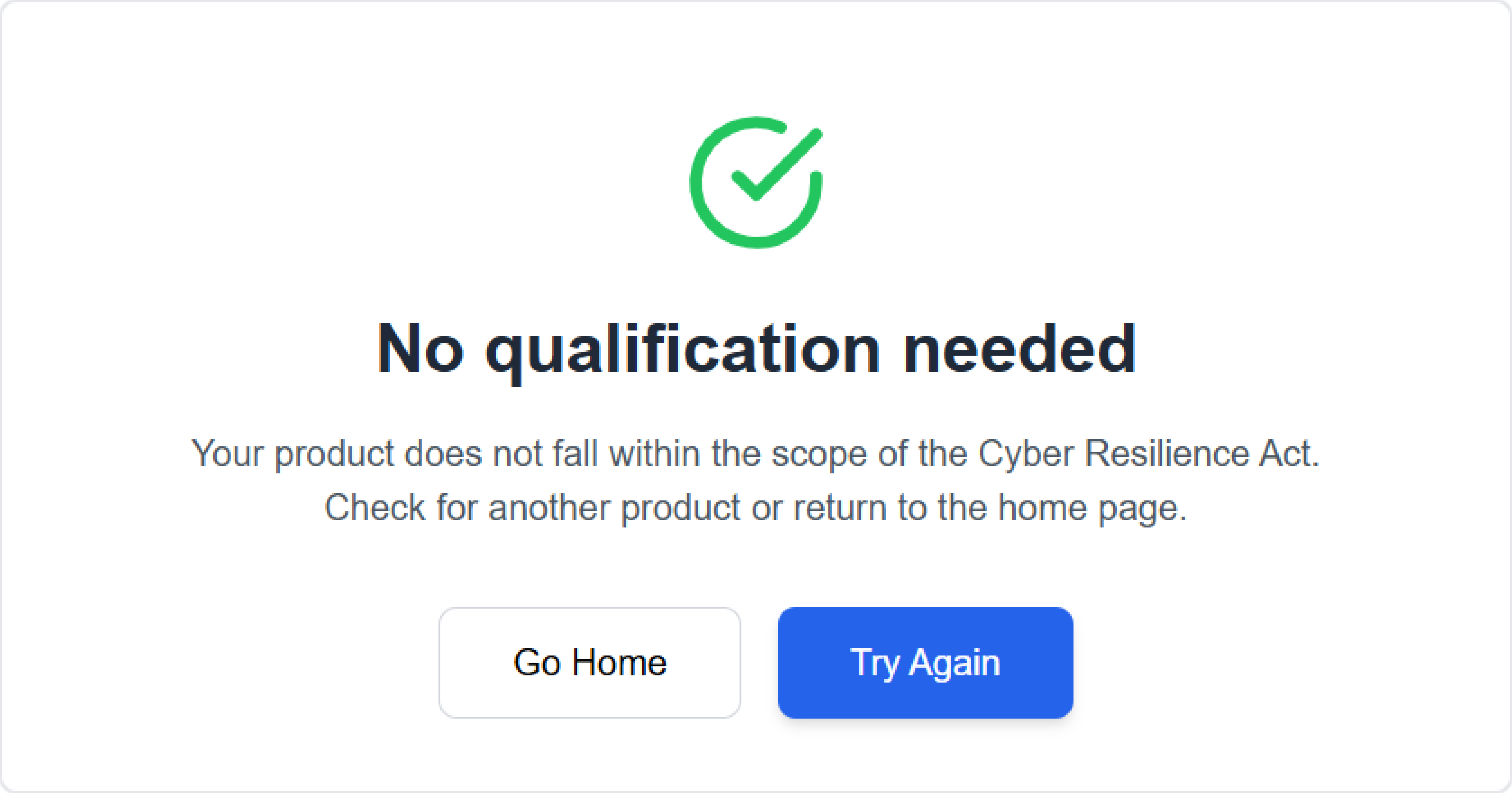
Answer "Yes" if:

- The product is **designed for use in vehicles**
- It is a **vehicle component** related to:
  - occupant or road-user **safety or protection**, or
  - **tyre pressure monitoring systems (TPMS)**, or
  - **fuel efficiency** or **CO_2 emissions**, or
  - **tyres**
- It is regulated under **EU Regulation 2019/2144**

Answer "No" if:

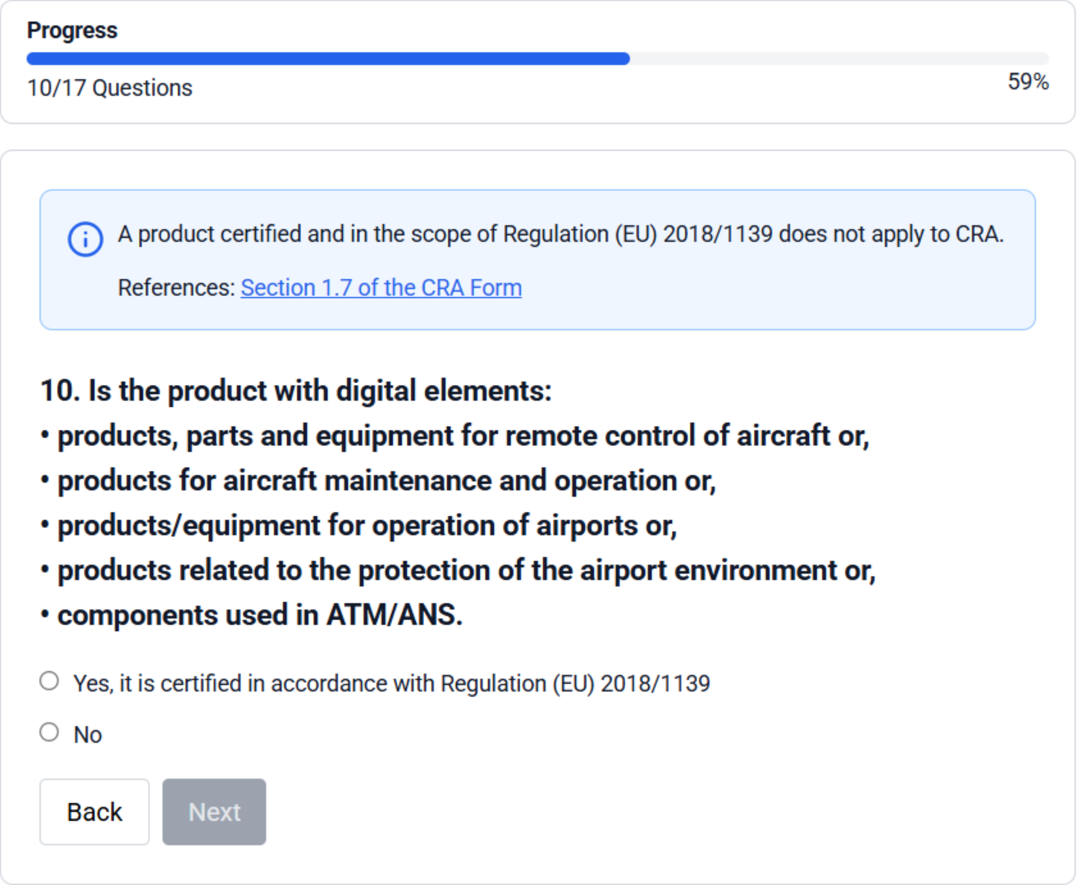
- The product is **not vehicle-specific**
- It is not a regulated vehicle safety, emissions, or tyre component
- It does not fall under **EU Regulation 2019/2144**

If Q9 is Yes, in accordance with EU Regulation 2019/2144



No qualification needed

Your product does not fall within the scope of the Cyber Resilience Act.
Check for another product or return to the home page.



Progress

10/17 Questions 59%

ⓘ A product certified and in the scope of Regulation (EU) 2018/1139 does not apply to CRA.

References: Section 1.7 of the CRA Form

10. Is the product with digital elements:

- **products, parts and equipment for remote control of aircraft or,**
- **products for aircraft maintenance and operation or,**
- **products/equipment for operation of airports or,**
- **products related to the protection of the airport environment or,**
- **components used in ATM/ANS.**

○ Yes, it is certified in accordance with Regulation (EU) 2018/1139

○ No

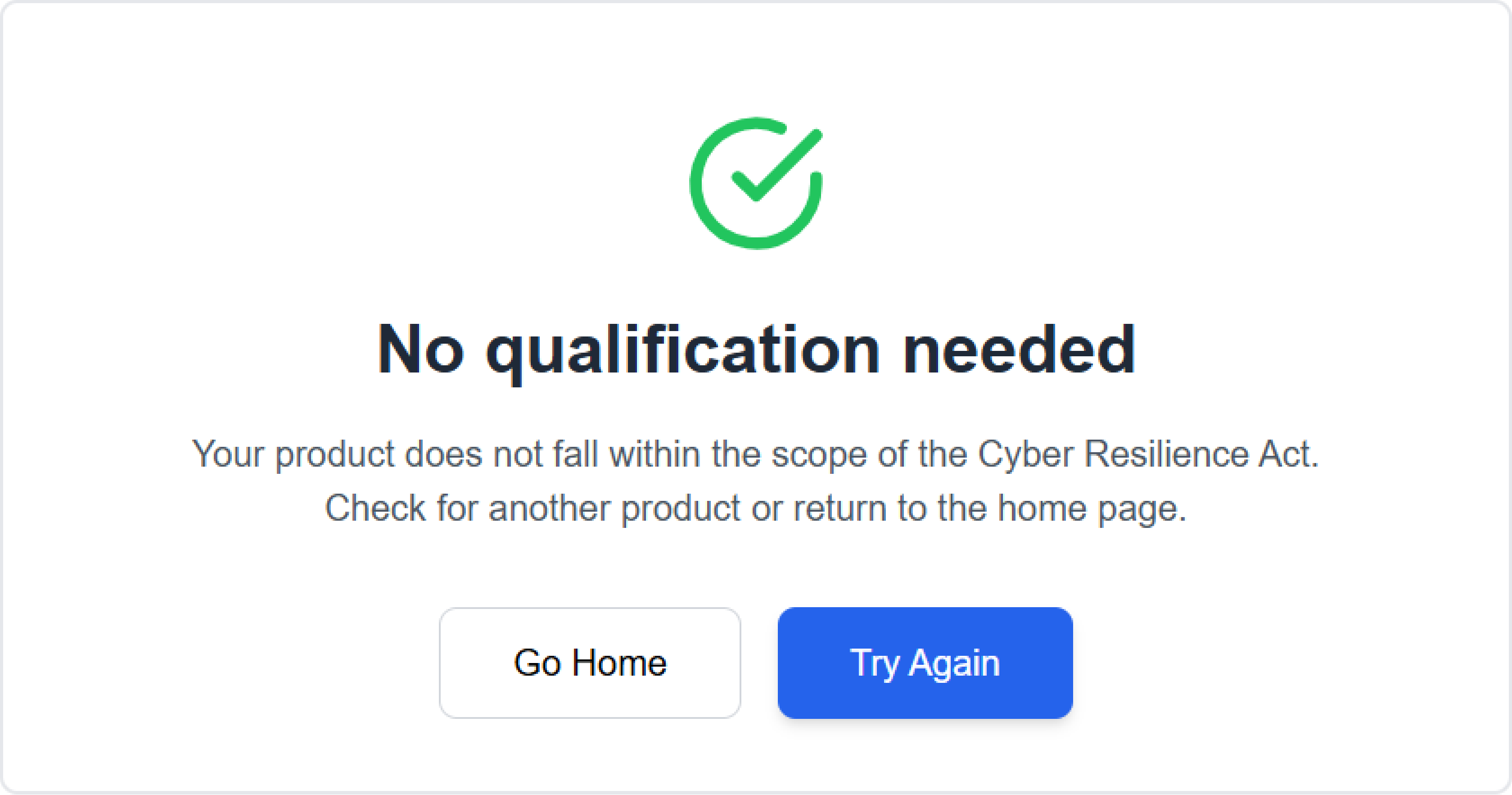
Answer “Yes” if:

- The product is **designed for use in vehicles**
- It is a **vehicle component** related to:
  - occupant or road-user **safety or protection**, or
  - **tyre pressure monitoring systems (TPMS)**, or
  - **fuel efficiency** or **CO_2 emissions**, or
  - **tyres**
- It is regulated under **EU Regulation 2019/2144**

Answer “No” if:

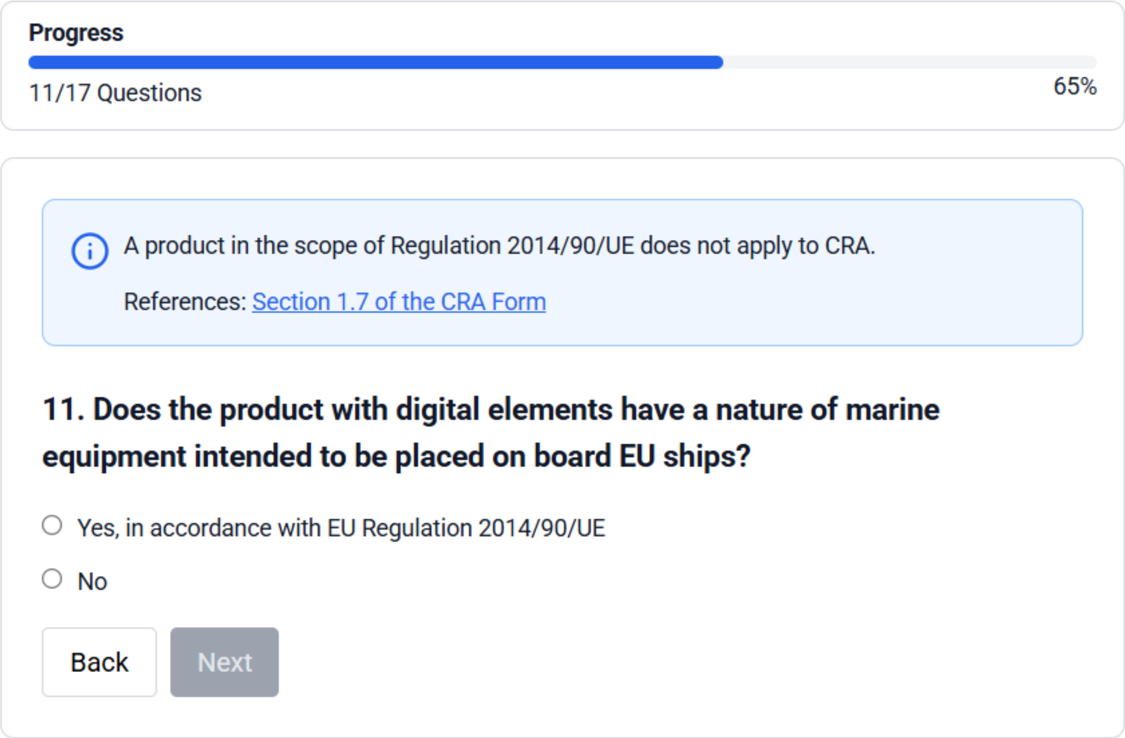
- The product is **not vehicle-specific**
- It is not a regulated **vehicle safety, emissions, or tyre component**
- It does not fall under **EU Regulation 2019/2144**

If Q10 is Yes, it is certified in accordance with Regulation (EU) 2018/1139



No qualification needed

Your product does not fall within the scope of the Cyber Resilience Act.
Check for another product or return to the home page.



A product in the scope of Regulation 2014/90/UE does not apply to CRA.

References: Section 1.7 of the CRA Form

11. Does the product with digital elements have a nature of marine equipment intended to be placed on board EU ships?

○ Yes, in accordance with EU Regulation 2014/90/UE

○ No

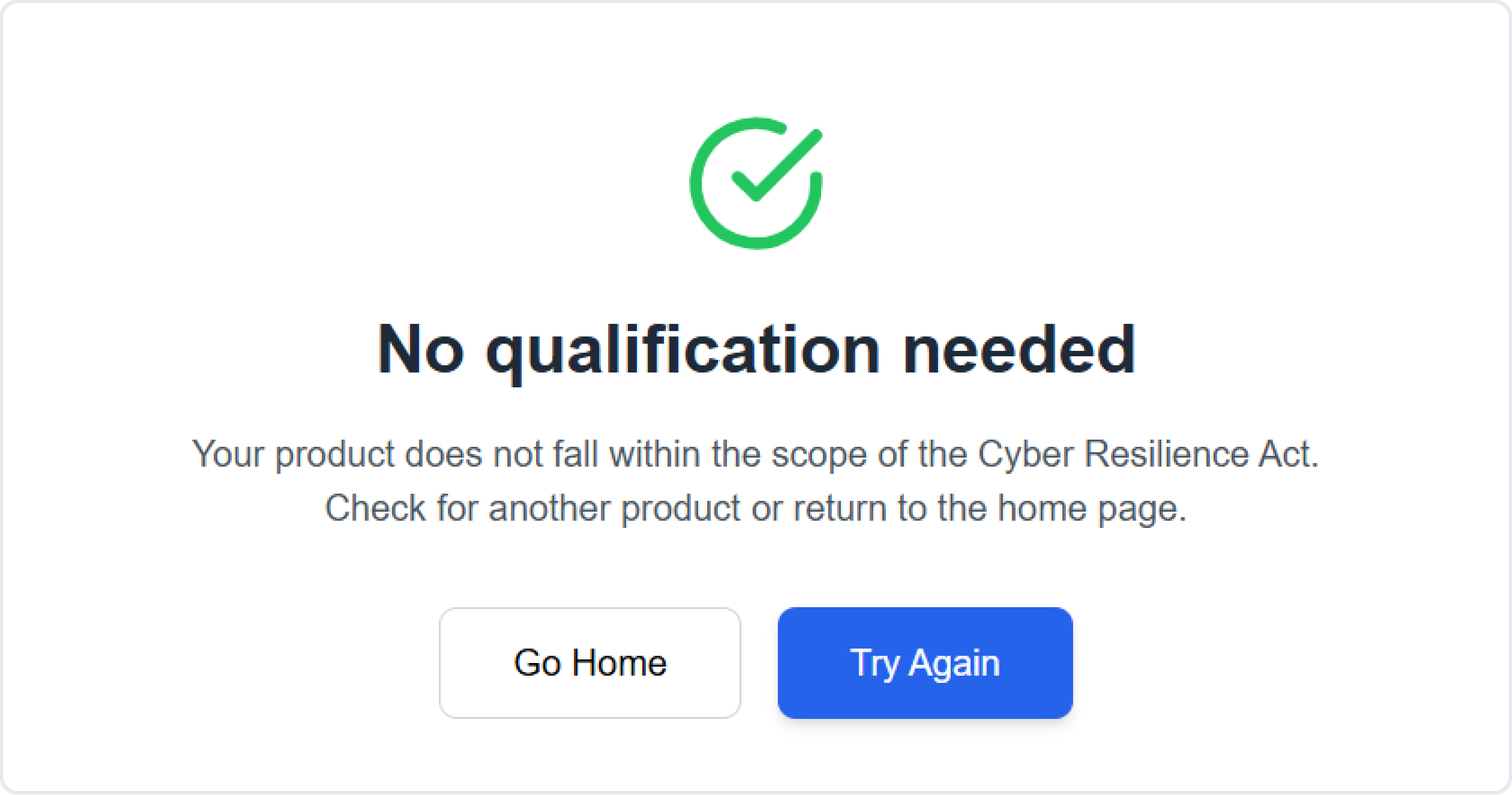
Answer "Yes" if:

- The product is **marine equipment** intended to be placed on board **EU ships**
- It is covered by **EU Regulation 2014/90/EU** (Marine Equipment Directive)
- It requires **certification or conformity** under that Regulation

Answer "No" if:

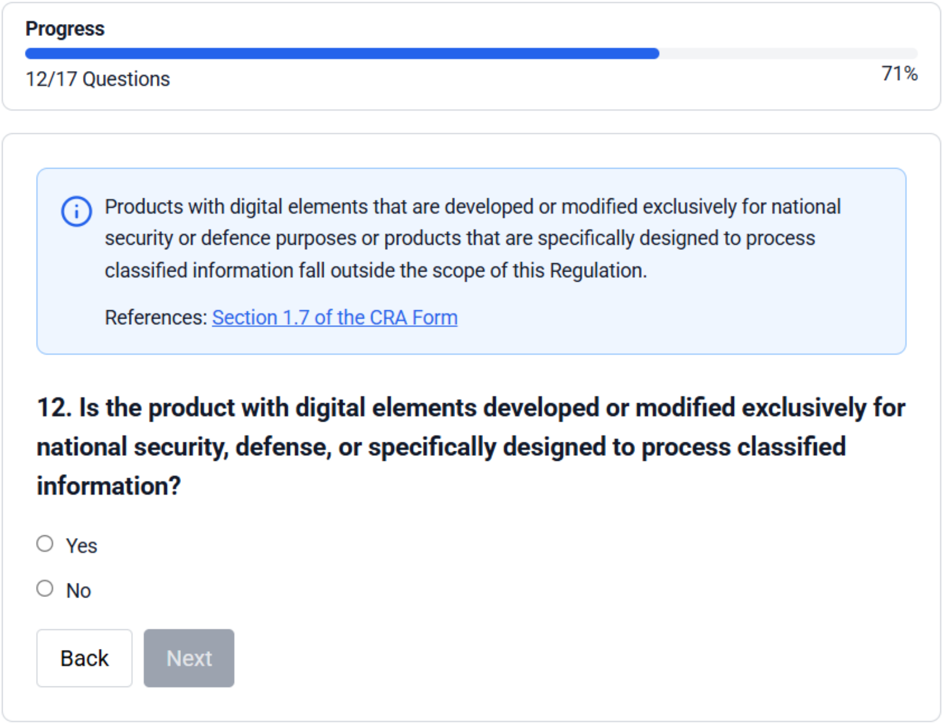
- The product is **not marine equipment**
- It is not intended to be placed on board EU ships
- It does not fall under **EU Regulation 2014/90/EU**

If Q11 is Yes, in accordance with EU Regulation 2014/90/UE



No qualification needed

Your product does not fall within the scope of the Cyber Resilience Act.
Check for another product or return to the home page.



Products with digital elements that are developed or modified exclusively for national security or defence purposes or products that are specifically designed to process classified information fall outside the scope of this Regulation.

References: Section 1.7 of the CRA Form

12. Is the product with digital elements developed or modified exclusively for national security, defense, or specifically designed to process classified information?

○ Yes

○ No

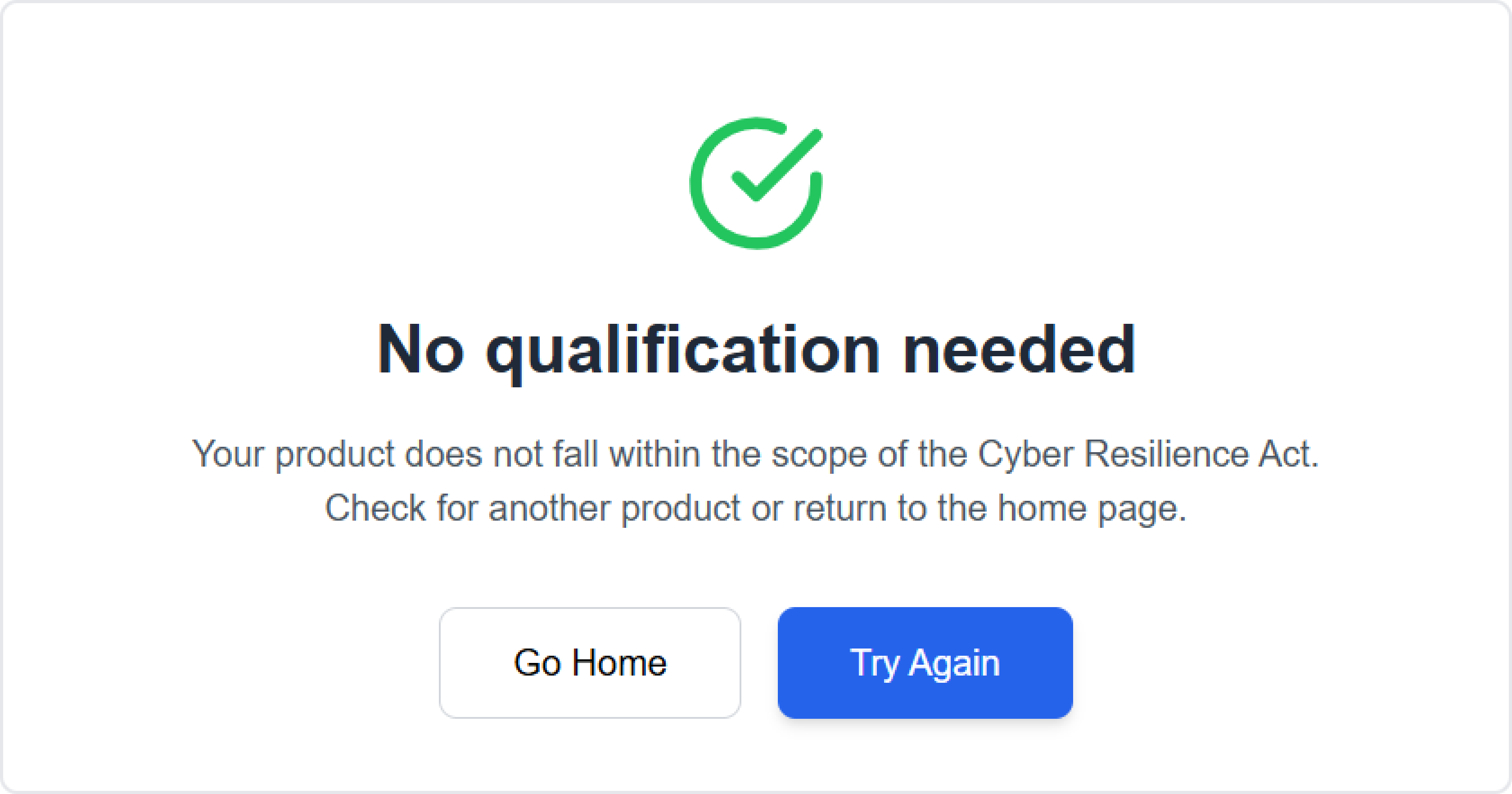
Answer "Yes" if:

- The product is developed or modified **exclusively for national security or defence purposes**
- The product is **specifically designed to process classified information**
- The product is not intended for civilian or commercial use

Answer "No" if:

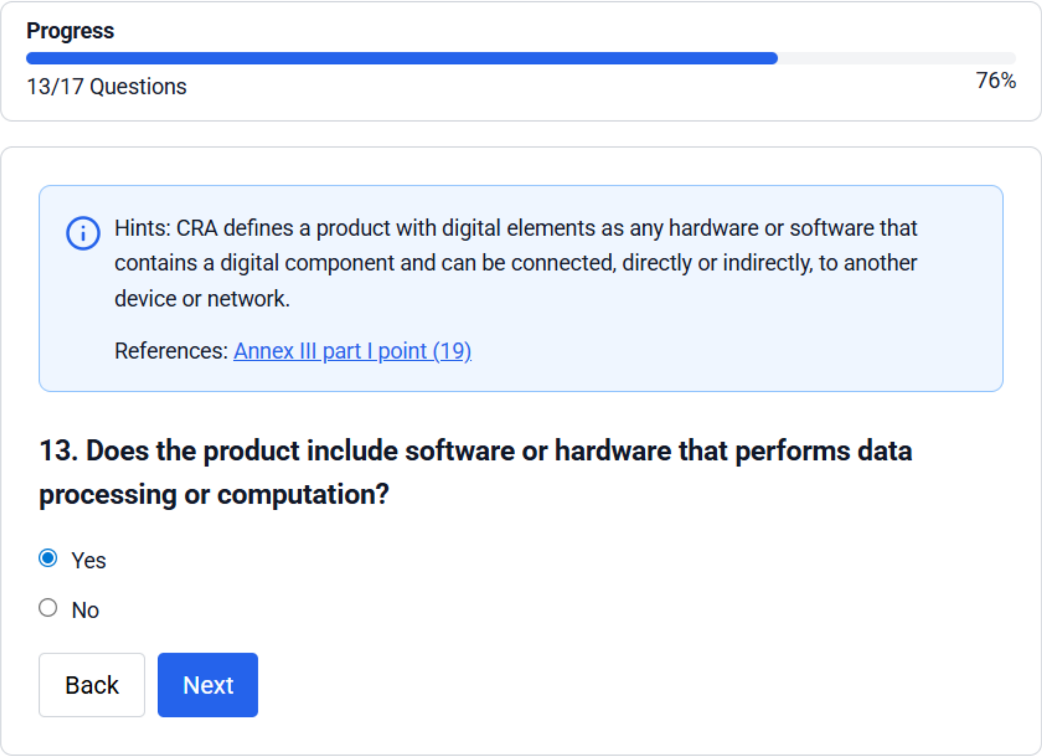
- The product has **civilian or commercial use**
- It is not exclusively developed for defence or national security
- It is not specifically designed to process classified information

If Q12 is Yes



No qualification needed

Your product does not fall within the scope of the Cyber Resilience Act. Check for another product or return to the home page.



Progress

13/17 Questions 76%

Hints: CRA defines a product with digital elements as any hardware or software that contains a digital component and can be connected, directly or indirectly, to another device or network.

References: Annex III part I point (19)

13. Does the product include software or hardware that performs data processing or computation?

● Yes

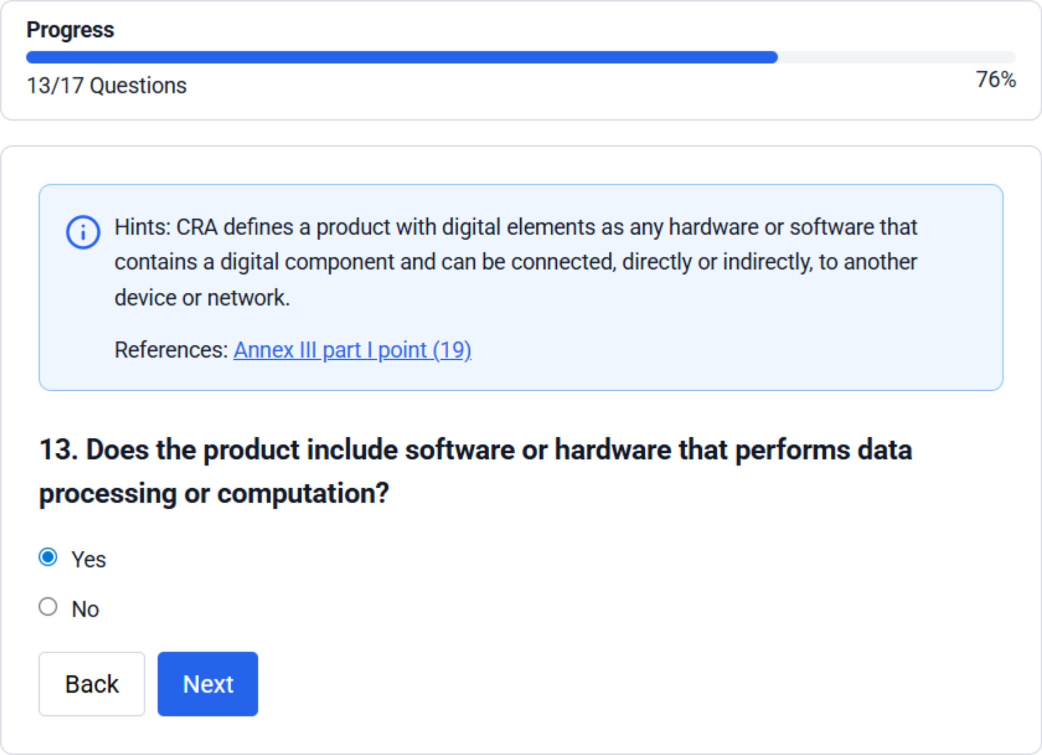
○ No

Answer “Yes” if the product:

- Includes **software or firmware that actively processes data**
- Performs **logical decisions, analytics, control logic, or transformations**
- Executes **code** that affects product behavior or outputs
- Uses a processor, microcontroller, or software stack to provide functionality

Examples:

- Embedded systems running firmware
- Software applications
- Devices performing signal processing, decision-making, or automation
- Products relying on backend or cloud computation



Hints: CRA defines a product with digital elements as any hardware or software that contains a digital component and can be connected, directly or indirectly, to another device or network.

References: Annex III part I point (19)

13. Does the product include software or hardware that performs data processing or computation?

● Yes

○ No

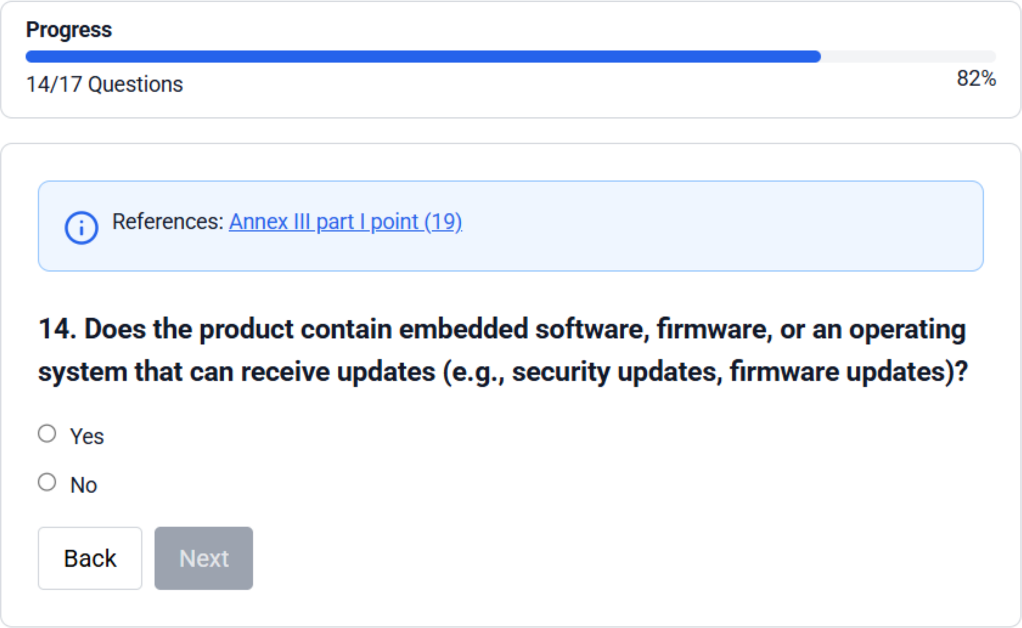
Answer "No" if the product:

- Does **not perform meaningful digital processing**
- Uses electronics only for **basic signaling or fixed control**
- Has no programmable logic that affects behavior
- Is primarily **mechanical or analog**, even if it contains simple electronics

Examples:

- Simple sensors with fixed output
- Devices with non-programmable control circuits
- Products where electronics do not process or compute data in a functional way

If the answer on Q13 is No – Q14 / Yes – Q17



Progress

14/17 Questions

82%

References: Annex III part I point (19)

14. Does the product contain embedded software, firmware, or an operating system that can receive updates (e.g., security updates, firmware updates)?

○ Yes

○ No

Answer “Yes” if:

- The product includes **embedded software, firmware, or an operating system**
- The software or firmware can **receive updates** (e.g. security patches, bug fixes, firmware updates)
- Updates can be delivered **locally or remotely** (manual, OTA, service tool, etc.)

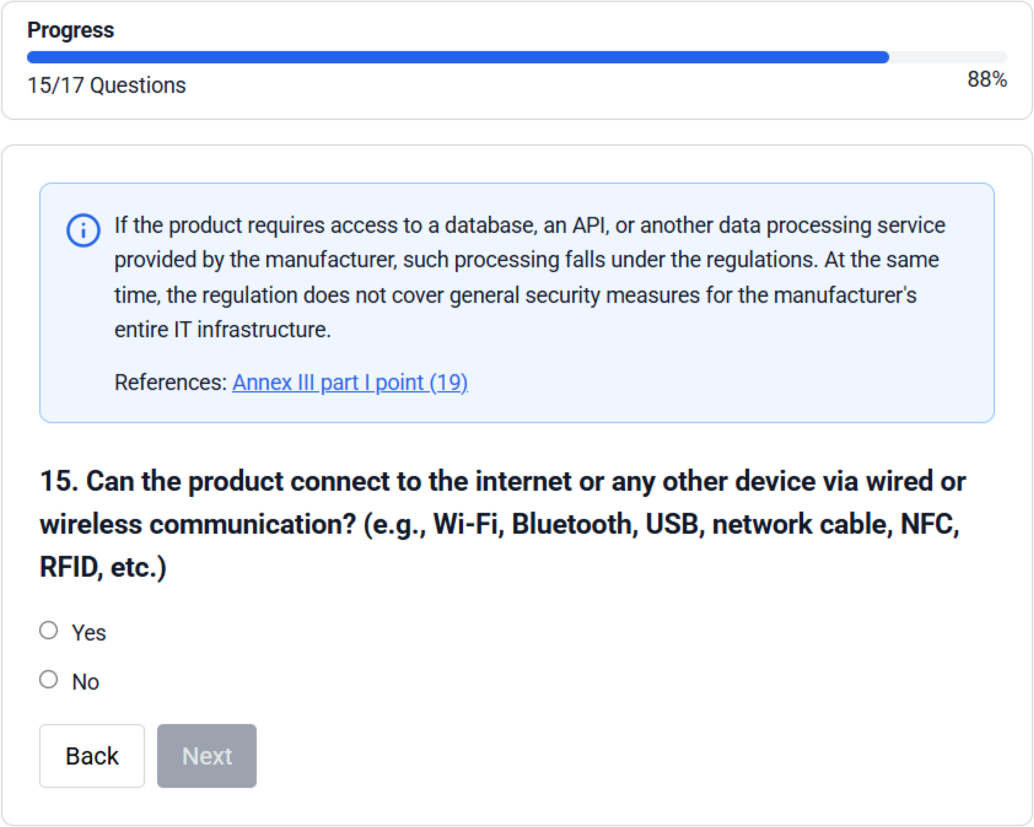
Yes: in the scope of the CRA

Answer “No” if:

- The product has **no software, firmware, or operating system**
- Any embedded logic **cannot be updated** after the product is placed on the market
- The product is purely **static, mechanical, or analog**

No: not in the scope of the CRA

If Q14 is No / Q14 is Yes – Q17



Progress

15/17 Questions

88%

If the product requires access to a database, an API, or another data processing service provided by the manufacturer, such processing falls under the regulations. At the same time, the regulation does not cover general security measures for the manufacturer's entire IT infrastructure.

References: Annex III part I point (19)

15. Can the product connect to the internet or any other device via wired or wireless communication? (e.g., Wi-Fi, Bluetooth, USB, network cable, NFC, RFID, etc.)

○ Yes

○ No

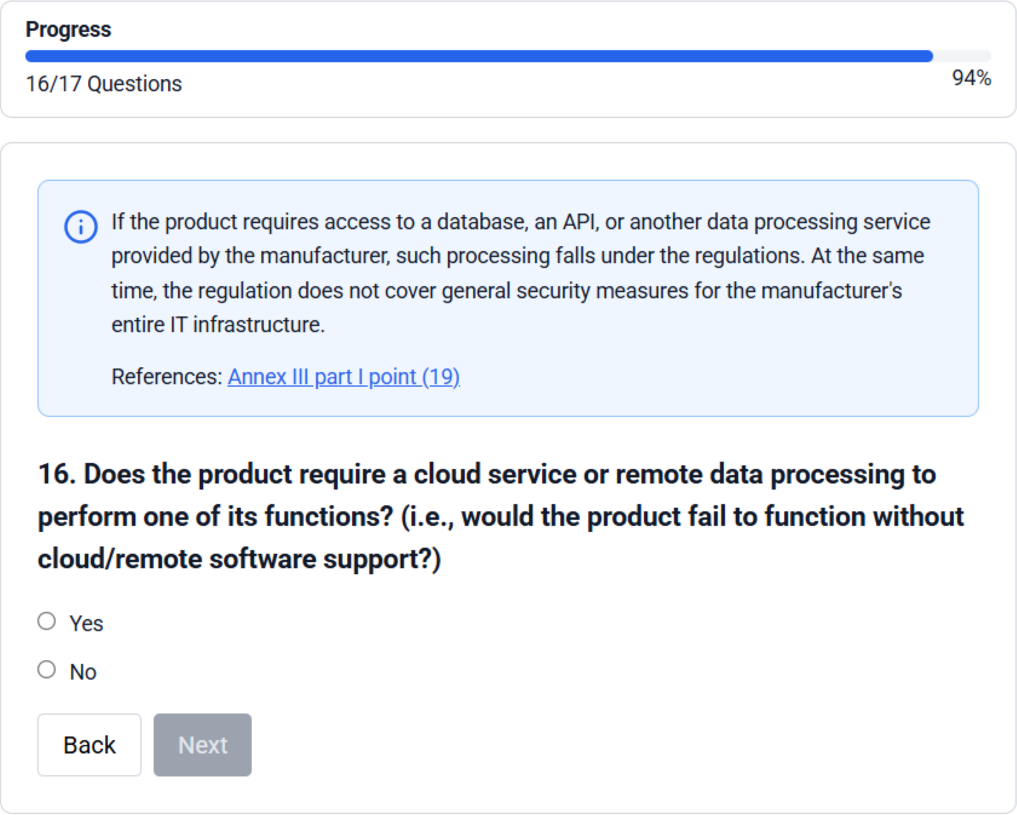
Answer "Yes" if:

- The product can connect to the **internet**
- The product can connect to **other devices or systems**
- Connection is possible via **wired or wireless interfaces** (e.g. Wi-Fi, Bluetooth, USB, Ethernet, NFC, RFID)
- The product accesses **APIs, databases, cloud services, or remote services** provided by the manufacturer

Answer "No" if:

- The product has **no connectivity**
- It cannot connect to the internet or to other devices
- It operates **fully offline** with no external communication interfaces

If Q15 is No



Progress

16/17 Questions

94%

If the product requires access to a database, an API, or another data processing service provided by the manufacturer, such processing falls under the regulations. At the same time, the regulation does not cover general security measures for the manufacturer's entire IT infrastructure.

References: Annex III part I point (19)

16. Does the product require a cloud service or remote data processing to perform one of its functions? (i.e., would the product fail to function without cloud/remote software support?)

○ Yes

○ No

Answer "Yes" if:

- The product **requires** a cloud service or remote backend to function
- One or more **essential functions fail** without cloud or remote processing
- The product depends on **manufacturer-operated APIs, databases, or services**

Answer "No" if:

- The product does **not require** cloud or remote data processing to function
- It can still operate without backend services

Q17 – Device category

Why these categories are important under the CRA
Products in these categories:

- Perform **core security, trust, or control functions**, or
- Are **deeply embedded in digital infrastructure**, or
- Are used in **high-risk contexts** (networks, identity, children, homes, critical systems)

Because a vulnerability in these products can have **system-wide or safety impacts**, the CRA applies **enhanced cybersecurity requirements** to them.
Selecting one of these categories means:

- The product **is in scope of the CRA**
- The product is subject to **higher assurance, stricter controls, and stronger lifecycle obligations**

Annex III / Annex IV Categories (as listed in the dropdown)

Hardware Devices with Security Boxes
Hardware that includes dedicated secure components (e.g. HSMs, trusted execution environments) to protect sensitive operations such as key storage or cryptographic processing.

Smart meter gateways within smart metering systems as defined in Article 2, point (23) of Directive (EU) 2019/944 of the European Parliament and of the Council (1) and other devices for advanced security purposes, including for secure cryptoprocessing
Devices that securely manage and transmit metering data or perform advanced cryptographic security functions.

Smartcards or similar devices, including secure elements
Physical cards or embedded chips used to securely store credentials, identities, or cryptographic keys.

Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments
Software that enables virtualization or containerization, allowing multiple systems or workloads to run securely on shared hardware.

Firewalls, intrusion detection and prevention systems
Security products that monitor, detect, block, or prevent unauthorized access or malicious activity.

Tamper-resistant microprocessors
Microprocessors designed to resist physical or logical tampering and protect sensitive operations.

Tamper-resistant microcontrollers
Microcontrollers with built-in protections against tampering, commonly used in embedded and security-critical systems.

Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers
Products that manage identities, control access rights, or authenticate users, including biometric systems.

Standalone and embedded browsers
Browsers used as independent applications or embedded within devices to access web-based content or services.

Password managers
Software or hardware used to securely store and manage user credentials.

Software that searches for, removes, or quarantines malicious software
Security software such as antivirus, anti-malware, or endpoint protection solutions.

Network management systems
Products used to monitor, configure, and manage network devices and network performance.

Security information and event management (SIEM) systems
Systems that collect, correlate, and analyze security events and logs to detect threats and incidents.

Boot managers
Software responsible for starting or loading an operating system during device startup.

Public key infrastructure and digital certificate issuance software
Systems used to issue, manage, and validate digital certificates and cryptographic trust relationships.

Physical and virtual network interfaces
Components that enable network connectivity, either through physical hardware or virtual interfaces.

Operating systems
Core software that manages hardware resources and provides the execution environment for applications.

Routers, modems intended for the connection to the internet, and switches
Network devices that route, transmit, or manage data traffic.

Microcontrollers with security-related functionalities
Microcontrollers that include security features such as secure boot, encryption, or access control.

Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related functionalities
Custom or programmable chips designed to perform security-critical functions.

Smart home general purpose virtual assistants
Voice-controlled or AI-based assistants used in smart home environments.

Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems
Connected home devices that provide security, monitoring, or safety functions.

Internet connected toys covered by Directive 2009/48/EC of the European Parliament and of the Council (1) that have social interactive features (e.g. speaking or filming) or that have location tracking features
Connected toys that interact socially or track location, often used by children.

Personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745 or (EU) No 2017/746 do not apply, or personal wearable products that are intended for the use by and for children
Wearable devices that monitor health or are designed for children but are not regulated as medical devices.

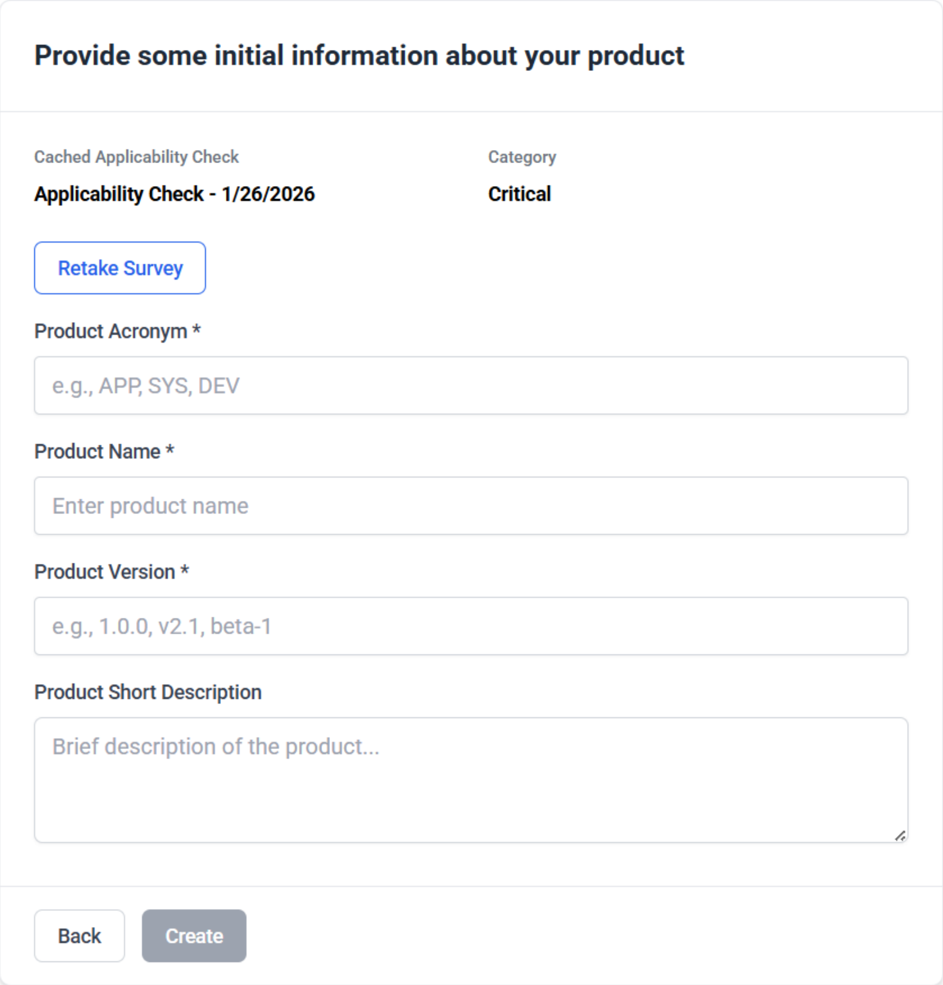
Key reminder (for users)

- **All listed categories are in scope of the CRA**

- Selecting one means **enhanced CRA requirements apply**

- Not selecting one means **standard CRA requirements apply**

Ready to create product



Provide some initial information about your product

Cached Applicability Check	Category
Applicability Check - 1/26/2026	**Critical**

Product Acronym *

e.g., APP, SYS, DEV

Product Name *

Enter product name

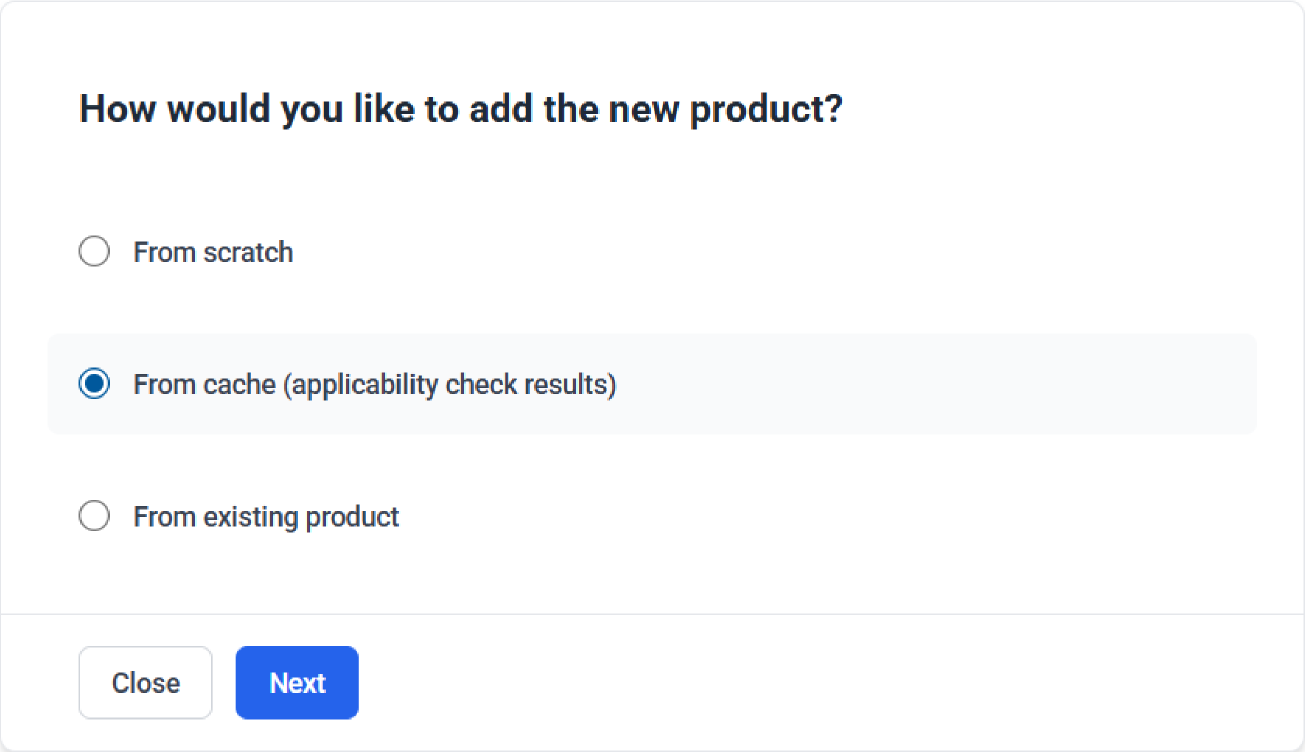
Product Version *

e.g., 1.0.0, v2.1, beta-1

Product Short Description

Brief description of the product...

Ready to create product – existing check list

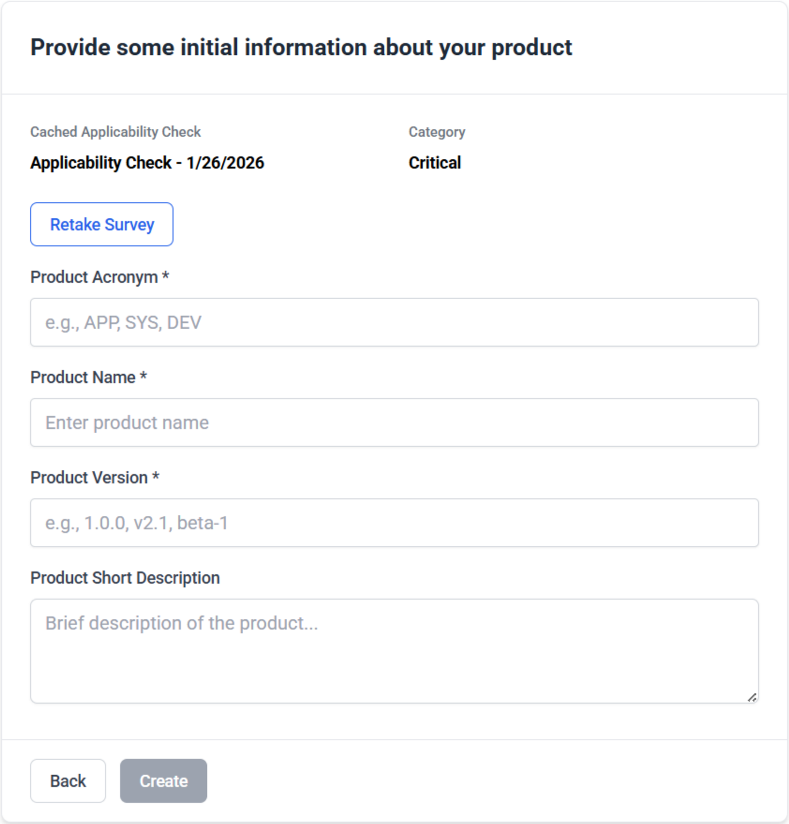


How would you like to add the new product?

○ From scratch

● From cache (applicability check results)

○ From existing product



Provide some initial information about your product

Cached Applicability Check	Category
Applicability Check - 1/26/2026	Critical

Product Acronym *

e.g., APP, SYS, DEV

Product Name *

Enter product name

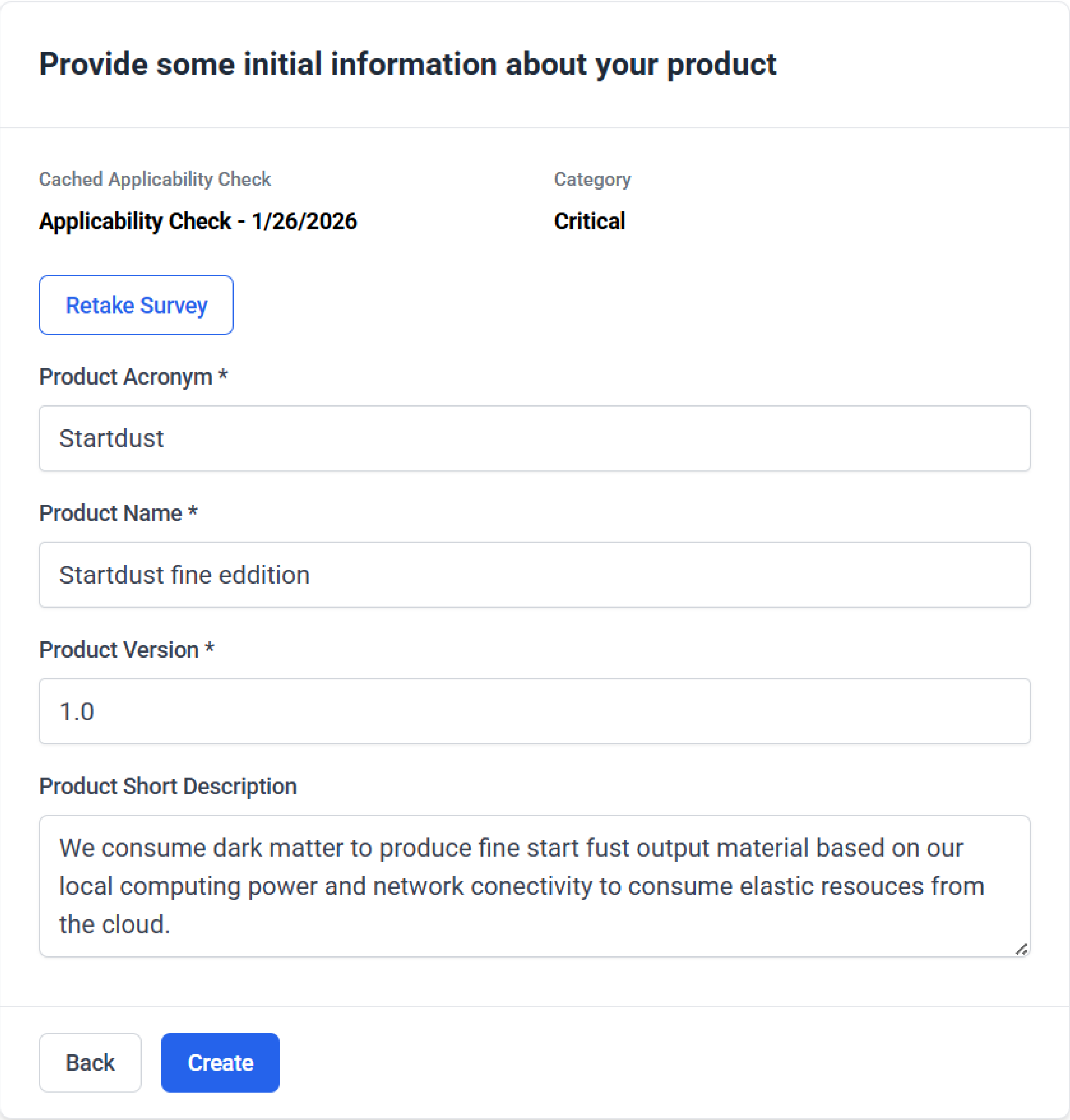
Product Version *

e.g., 1.0.0, v2.1, beta-1

Product Short Description

Brief description of the product...

We have product



Provide some initial information about your product

Cached Applicability Check
Applicability Check - 1/26/2026

Category
Critical

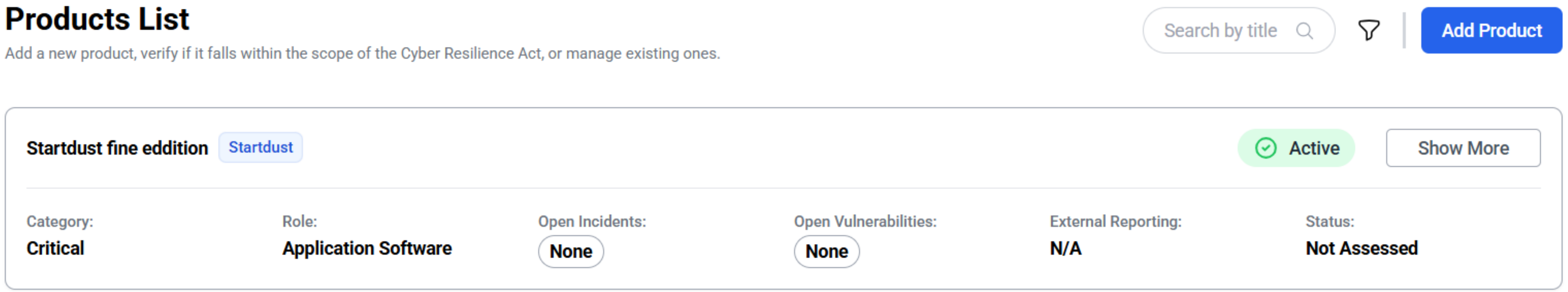
Product Acronym *
Startdust

Product Name *
Startdust fine eddition

Product Version *
1.0

Product Short Description
We consume dark matter to produce fine start fust output material based on our local computing power and network conectivity to consume elastic resouces from the cloud.

Product page

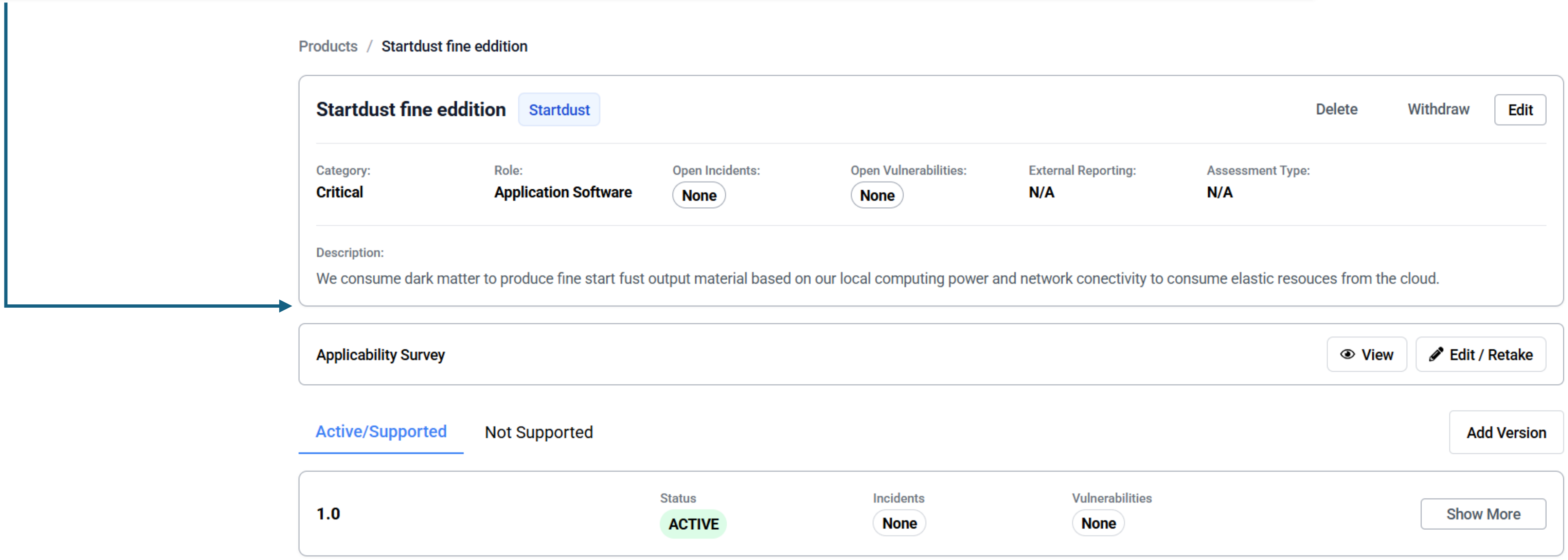


Products List

Add a new product, verify if it falls within the scope of the Cyber Resilience Act, or manage existing ones.

Startdust fine eddition Startdust

Category:	Role:	Open Incidents:	Open Vulnerabilities:	External Reporting:	Status:
Critical	Application Software	None	None	N/A	Not Assessed



Products / Startdust fine eddition

Startdust fine eddition Startdust

Category:	Role:	Open Incidents:	Open Vulnerabilities:	External Reporting:	Assessment Type:
Critical	Application Software	None	None	N/A	N/A

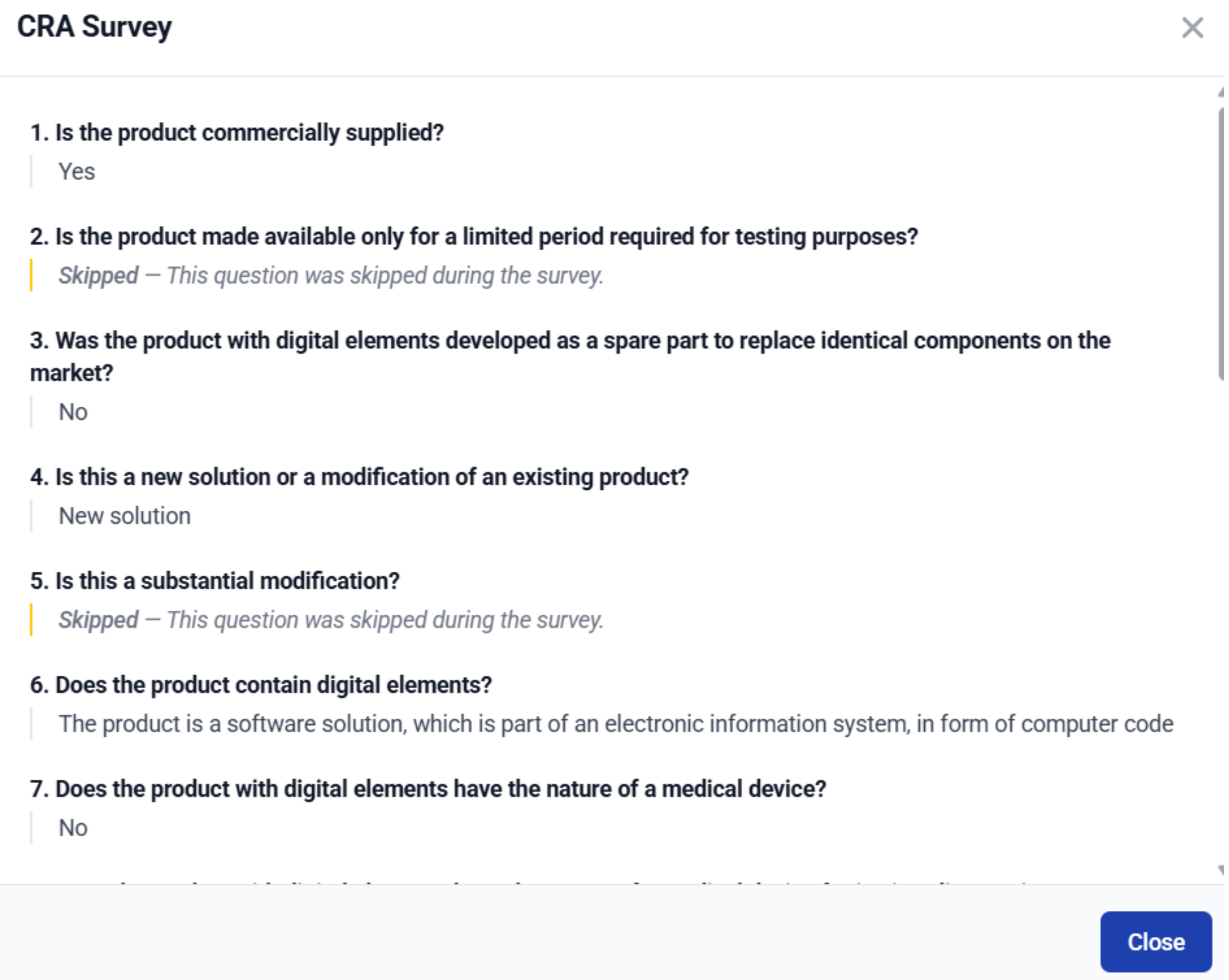
Description:

We consume dark matter to produce fine start fust output material based on our local computing power and network conectivity to consume elastic resouces from the cloud.

Applicability Survey

	Status	Incidents	Vulnerabilities
1.0	ACTIVE	None	None

Applicability Survey



CRA Survey

1. Is the product commercially supplied?

   Yes

2. Is the product made available only for a limited period required for testing purposes?

   Skipped — This question was skipped during the survey.

3. Was the product with digital elements developed as a spare part to replace identical components on the market?

   No

4. Is this a new solution or a modification of an existing product?

   New solution

5. Is this a substantial modification?

   Skipped — This question was skipped during the survey.

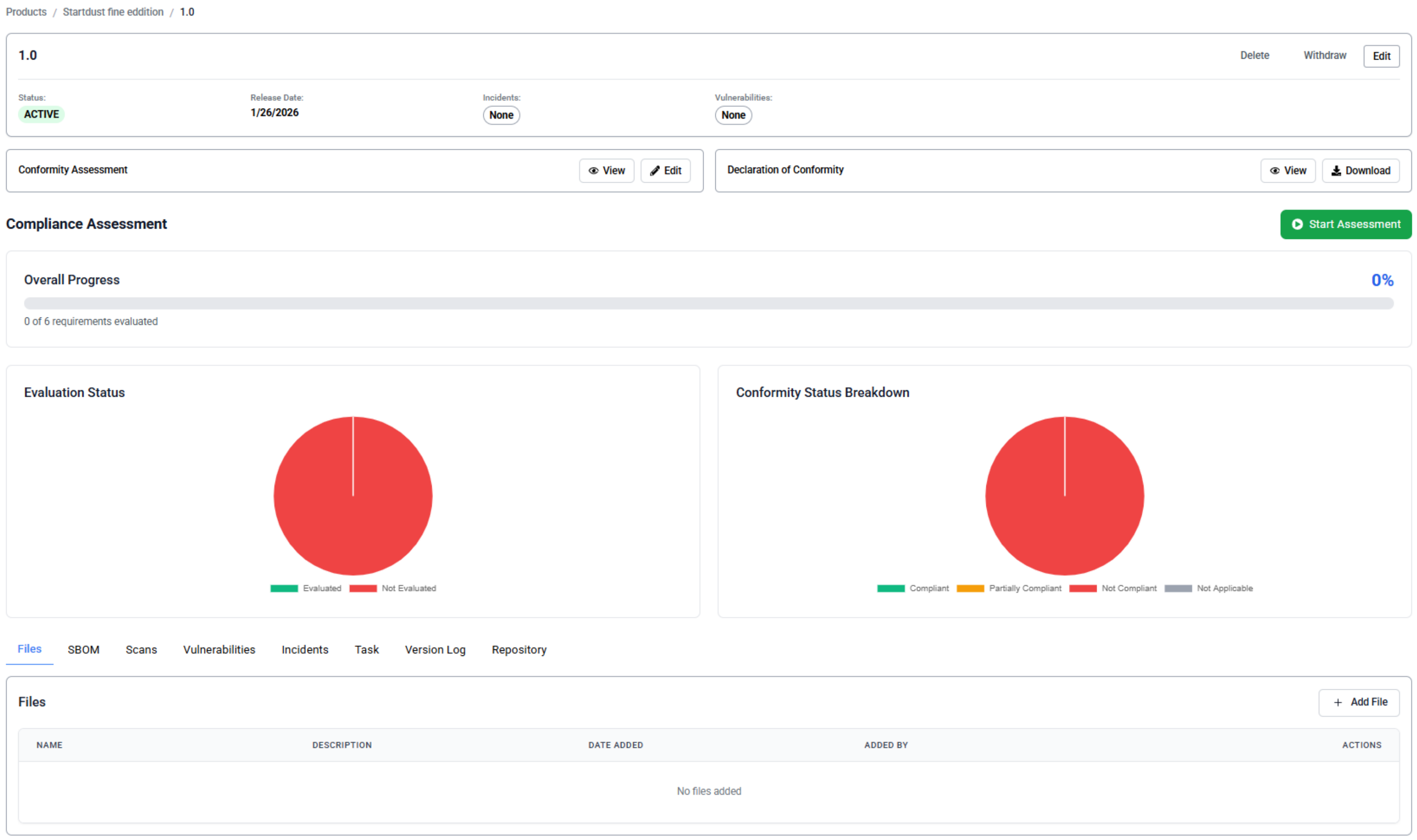
6. Does the product contain digital elements?

   The product is a software solution, which is part of an electronic information system, in form of computer code

7. Does the product with digital elements have the nature of a medical device?

   No

Show even more



Products / Startdust fine eddition / 1.0

1.0

Delete Withdraw Edit

Status:	Release Date:	Incidents:	Vulnerabilities:
ACTIVE	1/26/2026	None	None

Conformity Assessment — View · Edit

Declaration of Conformity — View · Download

Compliance Assessment

Start Assessment

Overall Progress 0%

0 of 6 requirements evaluated

Evaluation Status

Conformity Status Breakdown

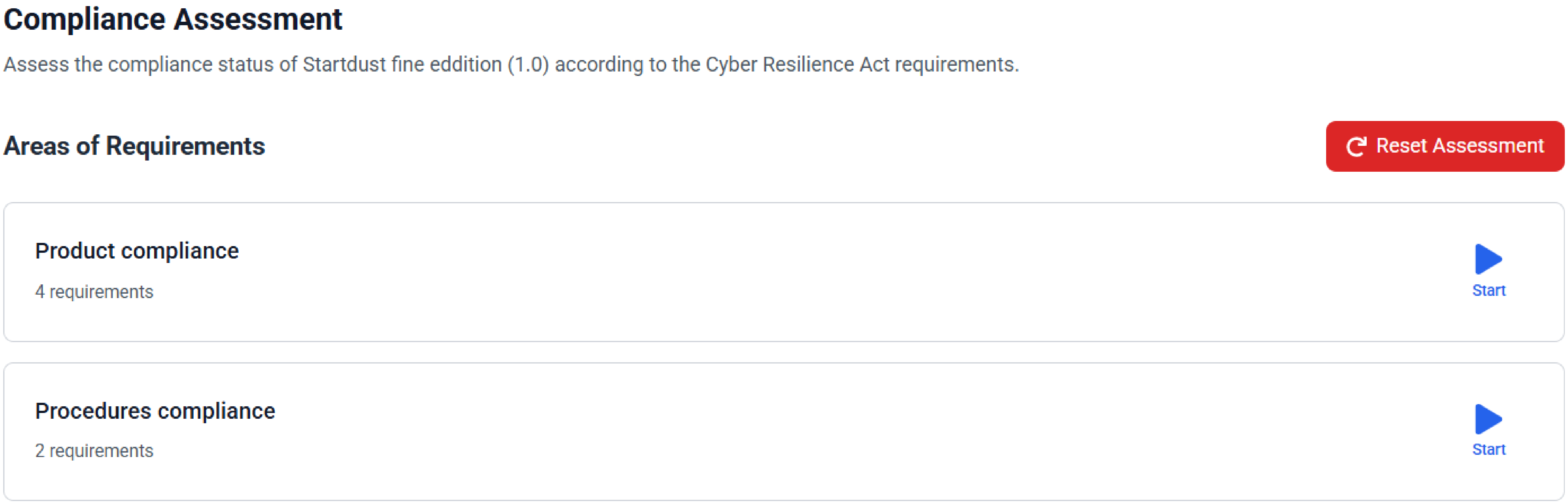
Files · SBOM · Scans · Vulnerabilities · Incidents · Task · Version Log · Repository

Files

+ Add File

NAME	DESCRIPTION	DATE ADDED	ADDED BY	ACTIONS
No files added				

More with the products



Compliance Assessment

Assess the compliance status of Startdust fine eddition (1.0) according to the Cyber Resilience Act requirements.

Areas of Requirements

Product compliance

4 requirements

Procedures compliance

2 requirements

We will proceed in next trainings with:

- SBOM, Scans, Vulnerabilities and tasks
- Compliance and conformity
- Reporting

and we will help you understand and be ready with your products for CRA