



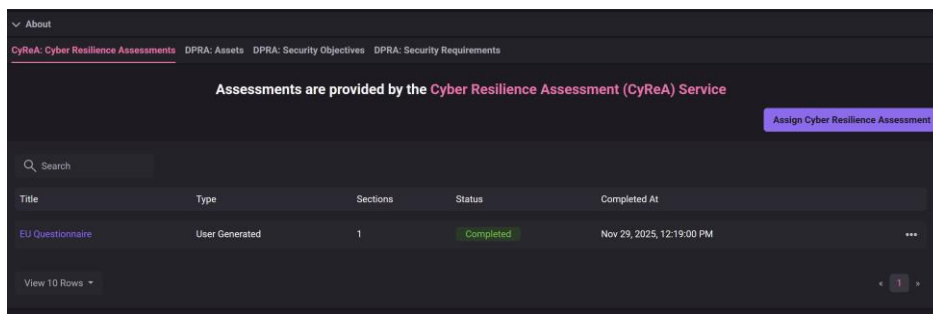
CyReA – Cyber Resilience Assessment



CyReA – Cyber Resilience Assessment

CyReA tool aims to systematically verified that ICT products with digital elements (ICT products) have been robustly assessed and comply with the essential requirements mandated by the CRA. It provides structured questionnaire-based wizard designed to facilitate and streamline the compliance assessment of their Products with Digital Elements (ICT products) against the requirements of the EU Cyber Resilience Act (CRA).

User dashboard: Upon successful login, the legitimate user is immediately directed to the main dashboard, as shown below Figure 1, to perform the response for the questionnaire-based wizard.

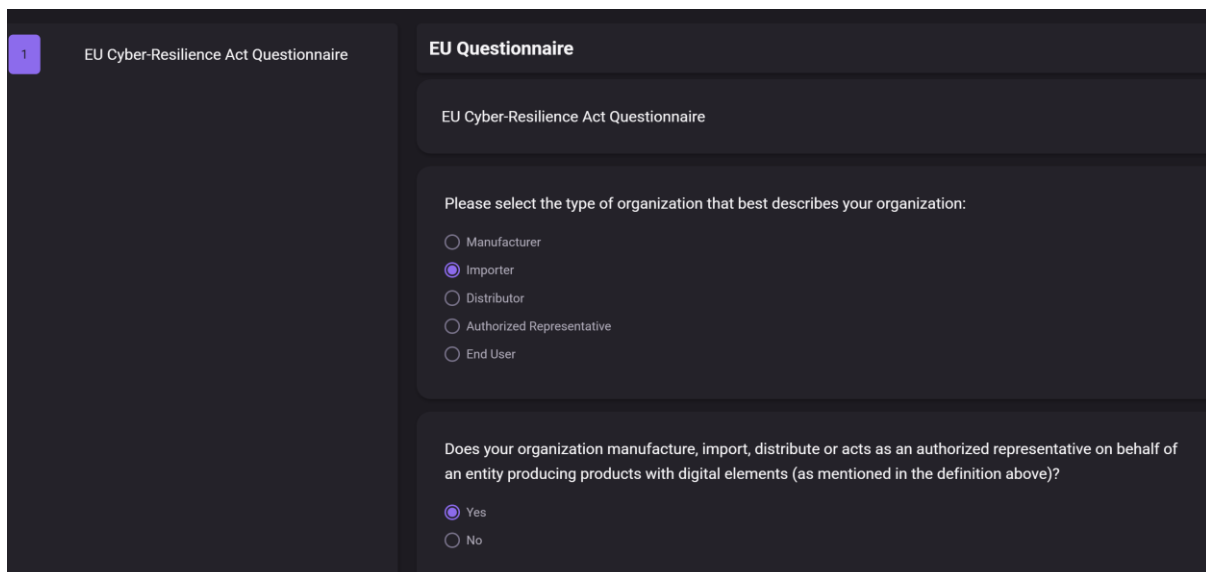


The screenshot shows the CyReA dashboard with a dark theme. At the top, there's a navigation bar with 'About', 'CyReA: Cyber Resilience Assessments', 'DPRA: Assets', 'DPRA: Security Objectives', and 'DPRA: Security Requirements'. Below this, a message states 'Assessments are provided by the Cyber Resilience Assessment (CyReA) Service' with an 'Assign Cyber Resilience Assessment' button. A search bar is present. A table lists assessments with columns: Title, Type, Sections, Status, and Completed At. One entry is visible: 'EU Questionnaire', 'User Generated', '1', 'Completed', and 'Nov 29, 2025, 12:19:00 PM'. At the bottom, there's a 'View 10 Rows' link and a pagination control showing '1'.

Title	Type	Sections	Status	Completed At
EU Questionnaire	User Generated	1	Completed	Nov 29, 2025, 12:19:00 PM

Figure 1: CyReA Dashboard

Scope & Role Determination: The initial step of CyReA is to determine the scope of CRA for the organisation based on their legal role including Manufacturer, Importer, Distributor, Authorized Representative, and End User under the CRA. If End User is selected specific option as shown in Figure 2, it is not necessary to continue with the remaining questions regarding product classification, conformity assessment, or self-assessment. The CRA provides obligations primarily on Manufacturers, Importers, Distributors, and Authorized Representatives who are involved in products with digital elements.

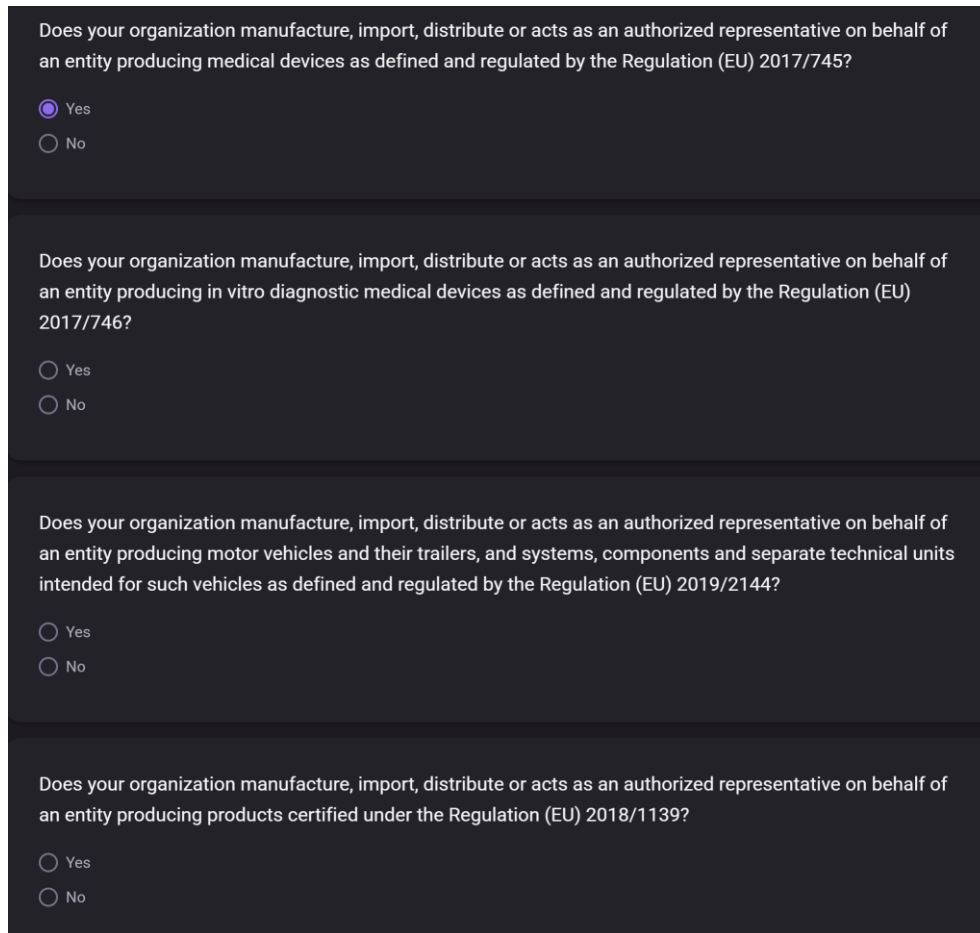


The screenshot shows the 'EU Questionnaire' form. It has a sidebar with '1 EU Cyber-Resilience Act Questionnaire'. The main content area is titled 'EU Questionnaire' and contains the following text: 'EU Cyber-Resilience Act Questionnaire'. Below this, it asks 'Please select the type of organization that best describes your organization:' with radio button options: 'Manufacturer', 'Importer' (selected), 'Distributor', 'Authorized Representative', and 'End User'. At the bottom, it asks 'Does your organization manufacture, import, distribute or acts as an authorized representative on behalf of an entity producing products with digital elements (as mentioned in the definition above)?' with radio button options: 'Yes' (selected) and 'No'.

Figure 15: Scope and Role determination

Product Screening: If the organisation type is not end user, the step shall follow which aims to screen the ICT product as CRA specifically excludes products with specific types that covered by other EU regulations such as Medical Devices, military products. Therefore, answering yes to any of these questions typically means the CRA does not apply to that specific product. The exclusion includes Medical Device regulated by the Regulation (EU) 2017/745, Transport by regulation (EU) 2019/2144, Aviation regulated by (EU) 2018/1139, National Security, and Software as a Service.

If your answer from any of following questions is "Yes" as shown in Figure 3, product falls under a category that is explicitly excluded from the scope of the EU Cyber Resilience Act (CRA). The security requirements for your product are governed by the specific sectoral law depending on type of products, i.e., Medical Devices, Motor Vehicle, national security or military purposes, and Software-as-a-Service (SaaS) services.



Does your organization manufacture, import, distribute or acts as an authorized representative on behalf of an entity producing medical devices as defined and regulated by the Regulation (EU) 2017/745?

☒ Yes
☐ No

Does your organization manufacture, import, distribute or acts as an authorized representative on behalf of an entity producing in vitro diagnostic medical devices as defined and regulated by the Regulation (EU) 2017/746?

☐ Yes
☐ No

Does your organization manufacture, import, distribute or acts as an authorized representative on behalf of an entity producing motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles as defined and regulated by the Regulation (EU) 2019/2144?

☐ Yes
☐ No

Does your organization manufacture, import, distribute or acts as an authorized representative on behalf of an entity producing products certified under the Regulation (EU) 2018/1139?

☐ Yes
☐ No

Figure 3: Product screening

Product Classification: once the product is screen and within scope of CRA, then it is necessary to classify the product to determine the required level of conformity assessment.

Your product falls into the Class I category under the CRA as shown in Figure 4, which means users need to follow the standard procedure for demonstrating compliance by following Self-Assessment

approach. If you do not check any of these option, then please continue next question , otherwise skip the next question and process following one.

Does your organization manufacture, import, distribute or act as an authorized representative on behalf of an entity producing one or more of the following products?

- ☐ 1. Identity management systems software and privileged access management software;
- ☐ 2. Standalone and embedded browsers;
- ☐ 3. Password managers;
- ☐ 4. Software that searches for, removes, or quarantines malicious software;
- ☐ 5. Products with digital elements with the function of virtual private network (VPN);
- ☐ 6. Network management systems;
- ☐ 7. Network configuration management tools;
- ☐ 8. Network traffic monitoring systems;
- ☐ 9. Management of network resources;
- ☐ 10. Security information and event management (SIEM) systems;
- ☐ 11. Update/patch management, including boot managers;
- ☐ 12. Application configuration management systems;
- ☐ 13. Remote access/sharing software;
- ☐ 14. Mobile device management software;
- ☐ 15. Physical network interfaces;
- ☐ 16. Operating systems not covered by class II;
- ☐ 17. Firewalls, intrusion detection and/or prevention systems not covered by class II;
- ☐ 18. Routers, modems intended for the connection to the internet, and switches, not covered by class II;
- ☐ 19. Microprocessors not covered by class II;
- ☐ 20. Microcontrollers;
- ☐ 21. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];
- ☐ 22. Industrial Automation & Control Systems (IACS) not covered by class II, such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);
- ☐ 23. Industrial Internet of Things not covered by class II.
- ☐ No

Figure 4: Class I Product Classification

If your product falls into the Class II category under the CRA as shown in Figure 5, it means the product is the highest risk category and mandates a more rigorous conformity assessment procedure. For Class II products, the CRA mandates the use of a Notified Body (a third-party Conformity Assessment Body) to verify compliance.

Does your organization manufacture, import, distribute or act as an authorized representative on behalf of an entity producing one or more of the following products?

- ☒ 1. Operating systems for servers, desktops, and mobile devices;
- ☒ 2. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments;
- ☒ 3. Public key infrastructure and digital certificate issuers;
- ☒ 4. Firewalls, intrusion detection and/or prevention systems intended for industrial use;
- ☒ 5. General purpose microprocessors;
- ☒ 6. Microprocessors intended for integration in programmable logic controllers and secure elements;
- ☒ 7. Routers, modems intended for the connection to the internet, and switches, intended for industrial use;
- ☒ 8. Secure elements;
- ☒ 9. Hardware Security Modules (HSMs);
- ☒ 10. Secure cryptoprocessors;
- ☒ 11. Smartcards, smartcard readers and tokens;
- ☒ 12. Industrial Automation & Control Systems (IACS) intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)], such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);
- ☒ 13. Industrial Internet of Things devices intended for the use by essential entities of the type referred to in [Annex I to the Directive 2022/2555 (NIS2)];
- ☒ 14. Robot sensing and actuator components and robot controllers;
- ☒ 15. Smart meters.
- ☐ No

Your product(s), is classified as a Class 1, CRITICAL PRODUCTS WITH DIGITAL ELEMENTS.

According to the EU CRA, Critical products with digital elements should be subject to stricter conformity assessment procedures, while keeping a proportionate approach. For this purpose, critical products with digital elements are divided into two classes, reflecting the level of cybersecurity risk linked to these categories of products. A potential cyber incident involving products in class II might lead to greater negative impacts than an incident involving products in class I, for instance due to the nature of their cybersecurity-related function or intended use in sensitive environments, and therefore should undergo a stricter conformity assessment procedure.

The manufacturer shall perform a conformity assessment of the Class I, critical product with digital elements and the processes put in place by the manufacturer to determine whether the essential requirements set out in Annex I are met. The manufacturer or the manufacturer's authorised representative shall demonstrate conformity with the essential requirements by using one of the following procedures:

(a) EU-type examination procedure (based on module B) provided for in Annex VI followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VI; or

(b) conformity assessment based on full quality assurance (based on module H) set out in Annex VI.

Figure 5: Class II Product Classification and Explanation

Conformity Assessment Readiness: The final step of CyReA aims to assess the ability to successfully execute the required assessment through either internal self-assessment or preparation for third-party assessment based on their resources, processes, and experience with risk assessment. The responses of these questions mainly focus on readiness and capability for the chosen conformity assessment route. You need to focus on Risk Assessment, Internal Testing, Internal Capability, and Confidence Level for successfully completing of CRA compliance as shown in Figure 6.



Do you perform a self-assessment or self-testing of your ICT services in relation to cybersecurity?

☐ Yes. Structured following international best practices

☐ Yes. Following a methodology created by us

☐ No

Have you performed risk assessment to the product, as part of the self-assessment or third party assessment process?

☐ I have not performed risk assessment

☐ I have performed risk assessment using an established methodology

☐ I have performed risk assessment using an interactive tool

☐ I have performed risk assessment using a template (i.e., word, excel etc)

☐ A third party has performed a risk assessment on the product and provided the results

In relation to the performance of Risk Assessment on your product, which if the following are true?

☐ The risk assessment takes into consideration the components of the product and their current vulnerabilities

☐ The risk assessment takes into consideration the security objectives and assurance level of the product

☐ The risk assessment takes into consideration the controls already implemented

Figure 6: Readiness Assessment

Based on the outcomes of the question response, CyReA provides Classification & Conformity Route and Readiness through following properties and shows the status complete as shown in Figure 7

- Your Organization's Role: [Manufacturer/Importer/Distributor/AR]
- Product Classification: [: Default/Class I/Class II]
- Required Compliance Route: [Self-Assessment (Internal Control) / Third-Party Assessment (Notified Body)]
- Risk Assessment, Internal Testing, Internal Capability, and confidence level

 **EU Questionnaire** ...

Cyber Resilience Assessment Status : Completed

▼ About

Basic Information

EU Cyber-Resilience Act Questionnaire

Welcome to the Cyber Resilience Act (CRA) Assessment Questionnaire.

This questionnaire helps you understand the basic characteristics and scope of the EU Cyber Resilience Act (EU CRA - proposed).

By filling in this questionnaire you will be able to determine whether your organization needs to implement specific actions regarding the assessment or the identification of products with digital elements.

To facilitate the understanding of the subject of the Cyber Resilience Act, the following definition is provided:

A Product with digital elements means any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately.

Figure 7: Completion Status