CURIUM CONTINUUM

CyReA
Cyber Resilience Assessment

User Manual for CURIUM Compliance Continuum Cyber Resilience Assessment (CyReA) – Tool

This User Manual is an open-source document licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. You are free to share and adapt this material under the condition that you provide appropriate credit, use it for non-commercial purposes, and distribute your contributions under this same license.

User Manual for CyReA Tool © 2026 by **NeaLogic** is licensed under **CC BY-NC-SA 4.0**. To view a copy of this license, visit: https://creativecommons.org/licenses/by-nc-sa/4.0/

The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC

CyReA – Cyber Resilience Assessment

The CyReA tool aims to systematically verify that ICT products with digital elements (ICT products) have been robustly assessed and comply with the essential requirements mandated by the CRA. It provides a 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 in Figure 1, to complete the questionnaire-based wizard.

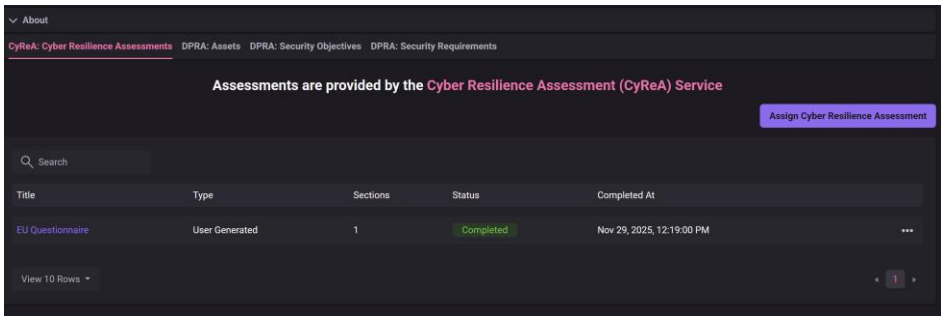


Figure 1: CyReA Dashboard

Scope & Role Determination: The initial step of CyReA is to determine the scope of the CRA for the organisation based on their legal role including Manufacturer, Importer, Distributor, Authorized Representative, and End User under the CRA. If the End User option is selected, 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 CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC

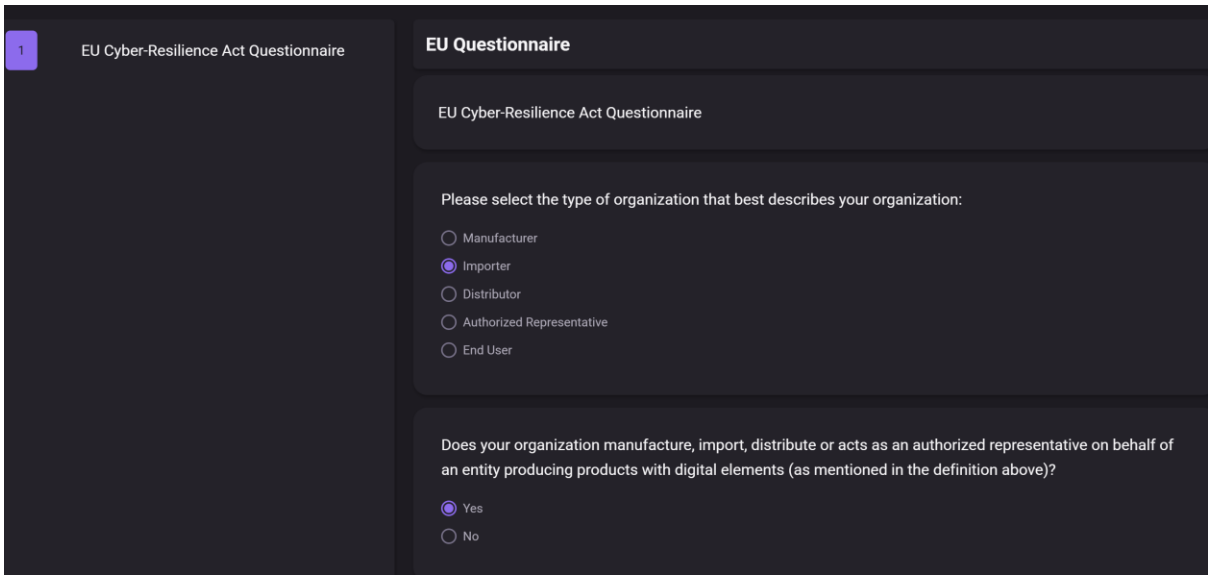


Figure 2: Scope and Role determination

Product Screening:

If the organisation is not an End User, the next step screens the ICT product to determine whether it falls within the scope of the CRA. Certain products, such as medical devices and military products, are excluded because they are covered by other EU regulations.

Therefore, answering “yes” to any of these questions typically means the CRA does not apply to that specific product. The exclusion includes Medical Devices regulated by 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 to any of following questions is "Yes" as shown in Figure 3, the 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.

The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC

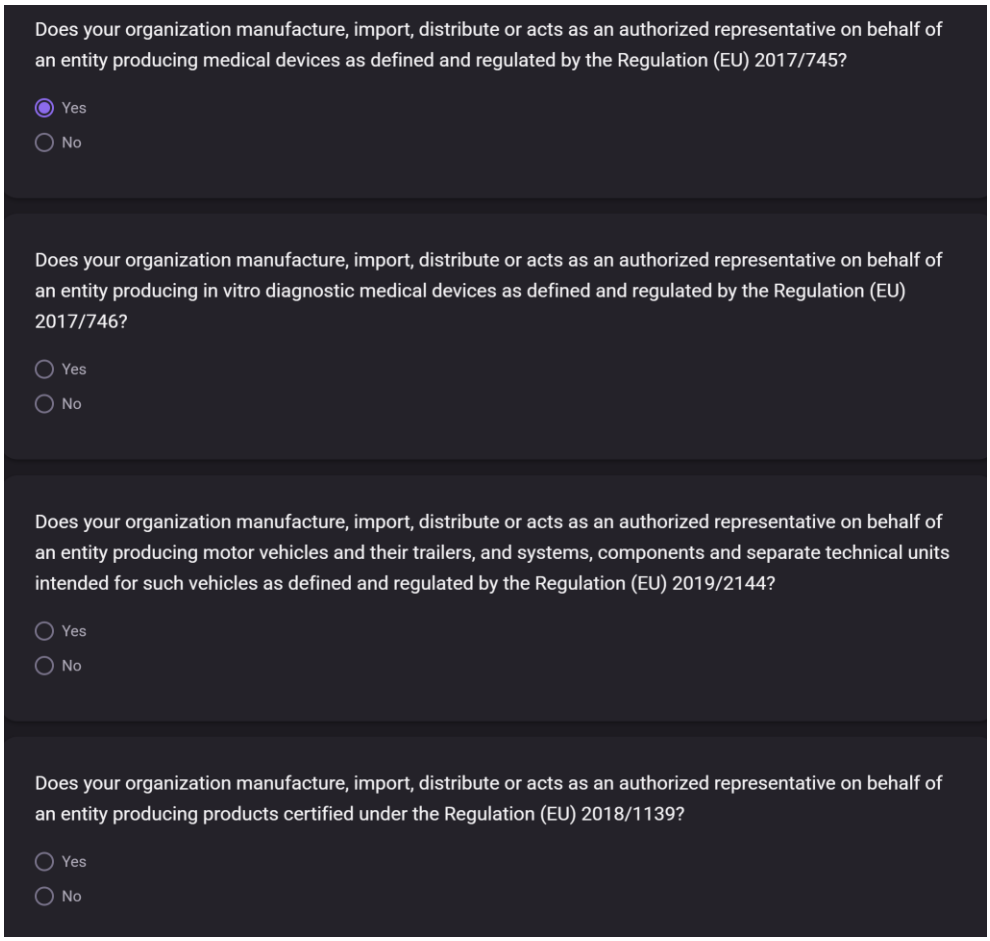


Figure 3: Product screening

Once the product has been screened and confirmed to fall within the scope of the CRA, it must be classified to determine the applicable conformity assessment procedure.

If you select any of the options shown in Figure 4, your product falls into the Class I category under the CRA. You can then proceed with the self-assessment approach to demonstrate compliance and skip the next question. If you do not select any of these options, please continue with the next question.

The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC

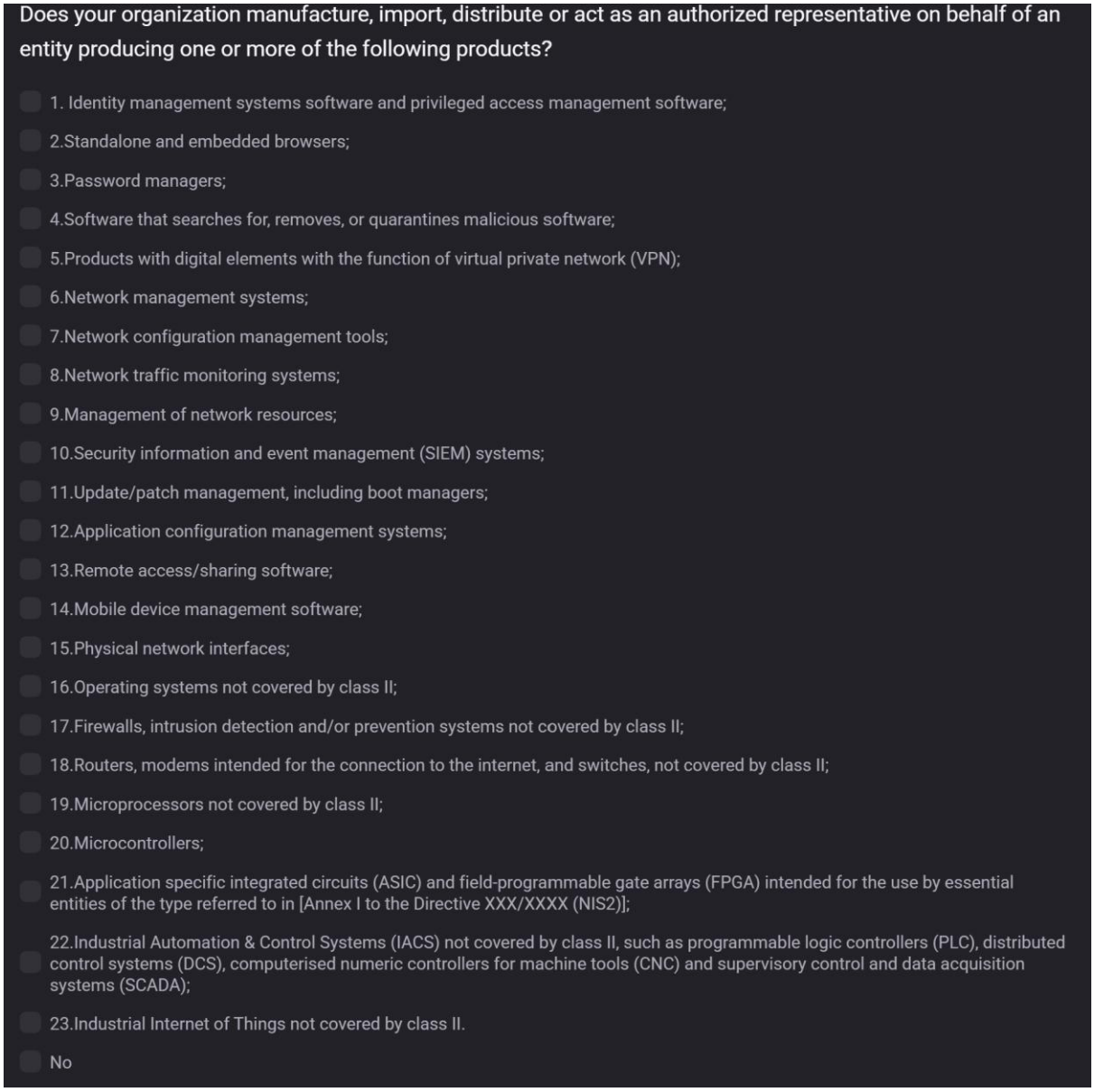
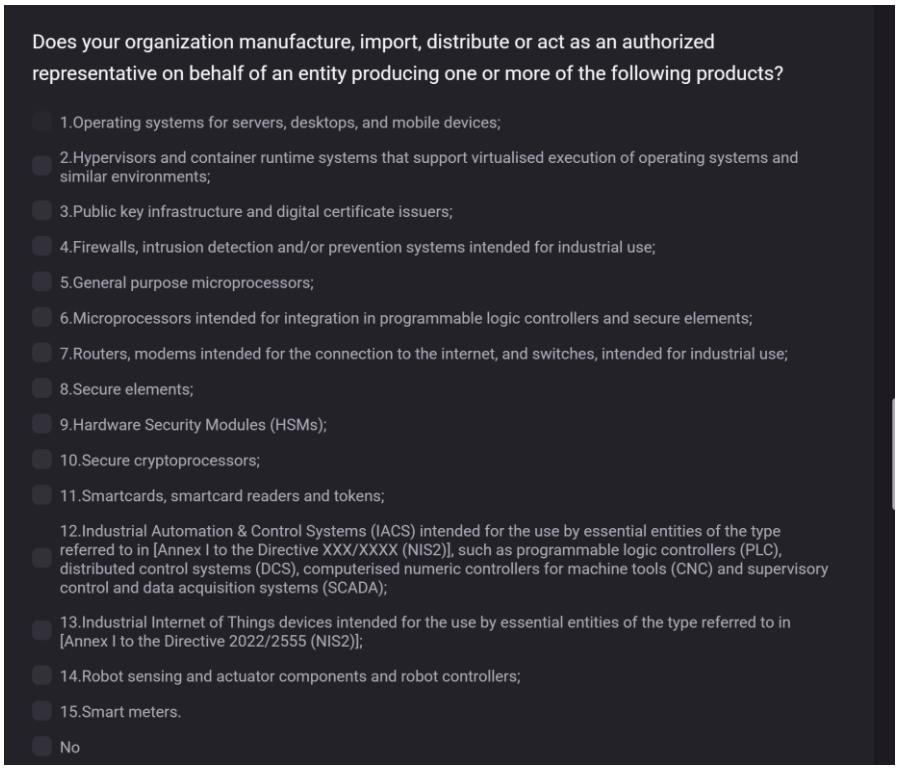


Figure 4: Class I Product Classification

If your product falls into the Class II category under the CRA as shown in Figure 5, it means the product is in 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.

The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC



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

The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC

The final step in CyReA assesses the organisation's readiness to follow the applicable conformity assessment route, whether through internal self-assessment or preparation for a third-party assessment. The questions focus on its resources, processes, and experience with risk assessment. As shown in Figure 6, consider your organisation's risk assessment, internal testing, internal capabilities, and confidence in completing the assessment required for CRA compliance.

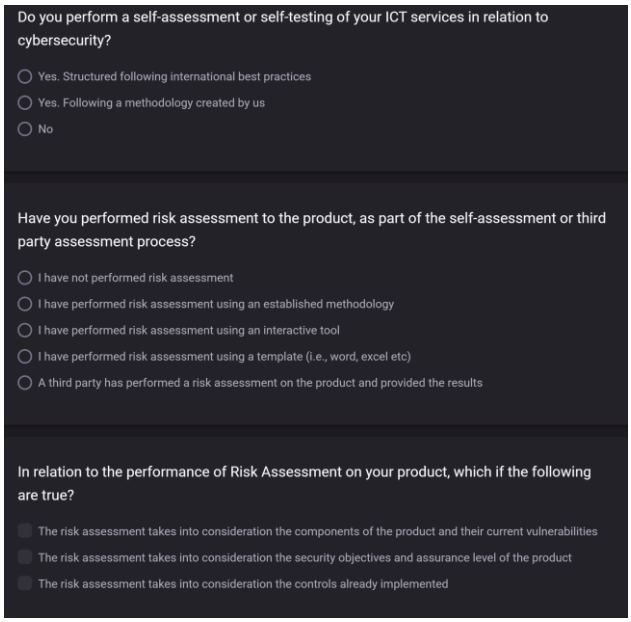


Figure 6: Readiness Assessment

Based on the outcomes of the question response, CyReA provides Classification & Conformity Route and Readiness through the 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

The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC

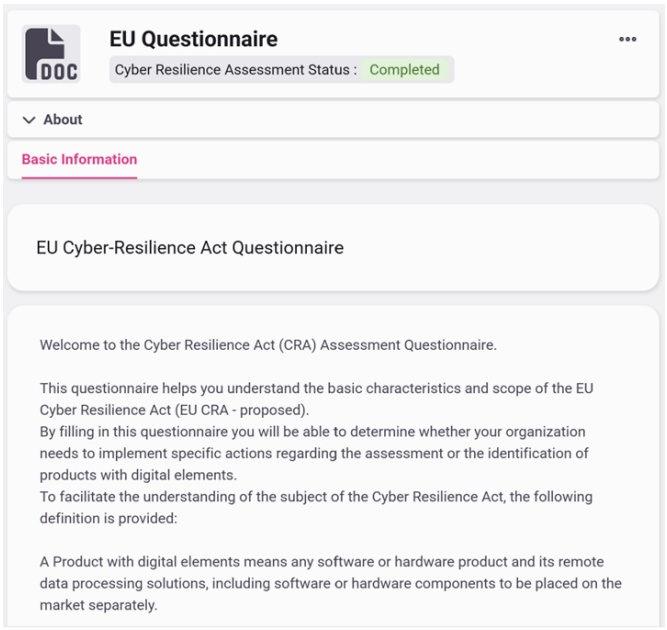


Figure 7: Completion Status

User Manual for CyReA Tool © 2026 by **NeaLogic** is licensed under **CC BY-NC-SA 4.0**. To view a copy of this license, visit https://creativecommons.org/licenses/by-nc-sa/4.0/

The CURIUM project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) under Grant Agreement No. 101190372. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the ECCC