CyReA – Cyber Resilience Assessment

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

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 questionary-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 questionary-based wizard.

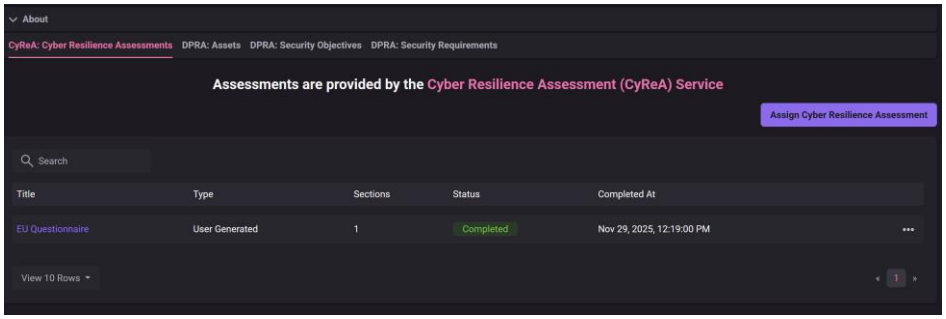

Figure 1: CyReA Dashboard

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.

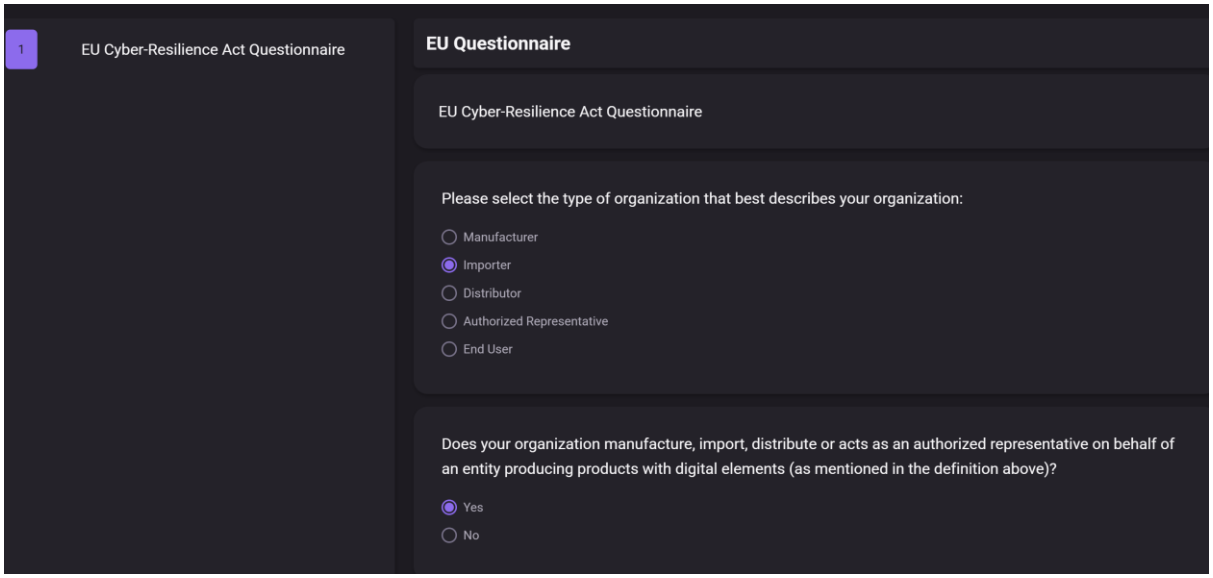

Figure 15: Scope and Role determination

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

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.

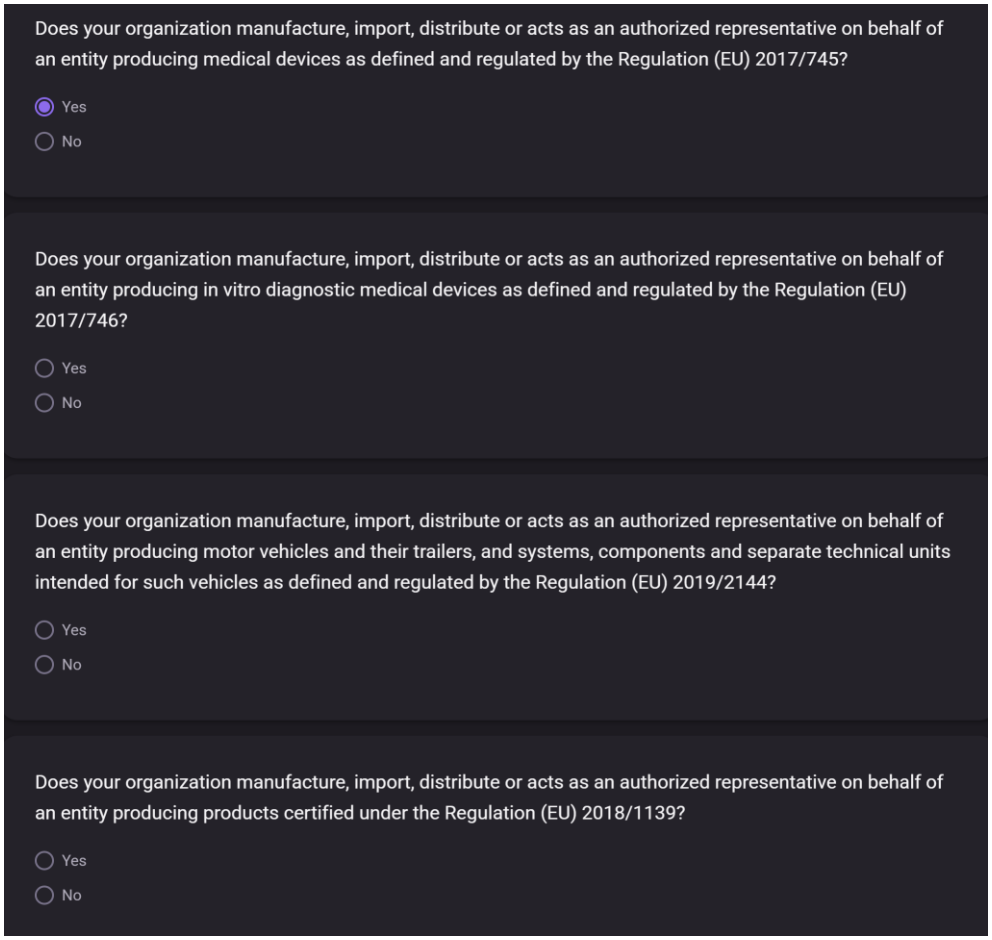

Figure 3: Product screening

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

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

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

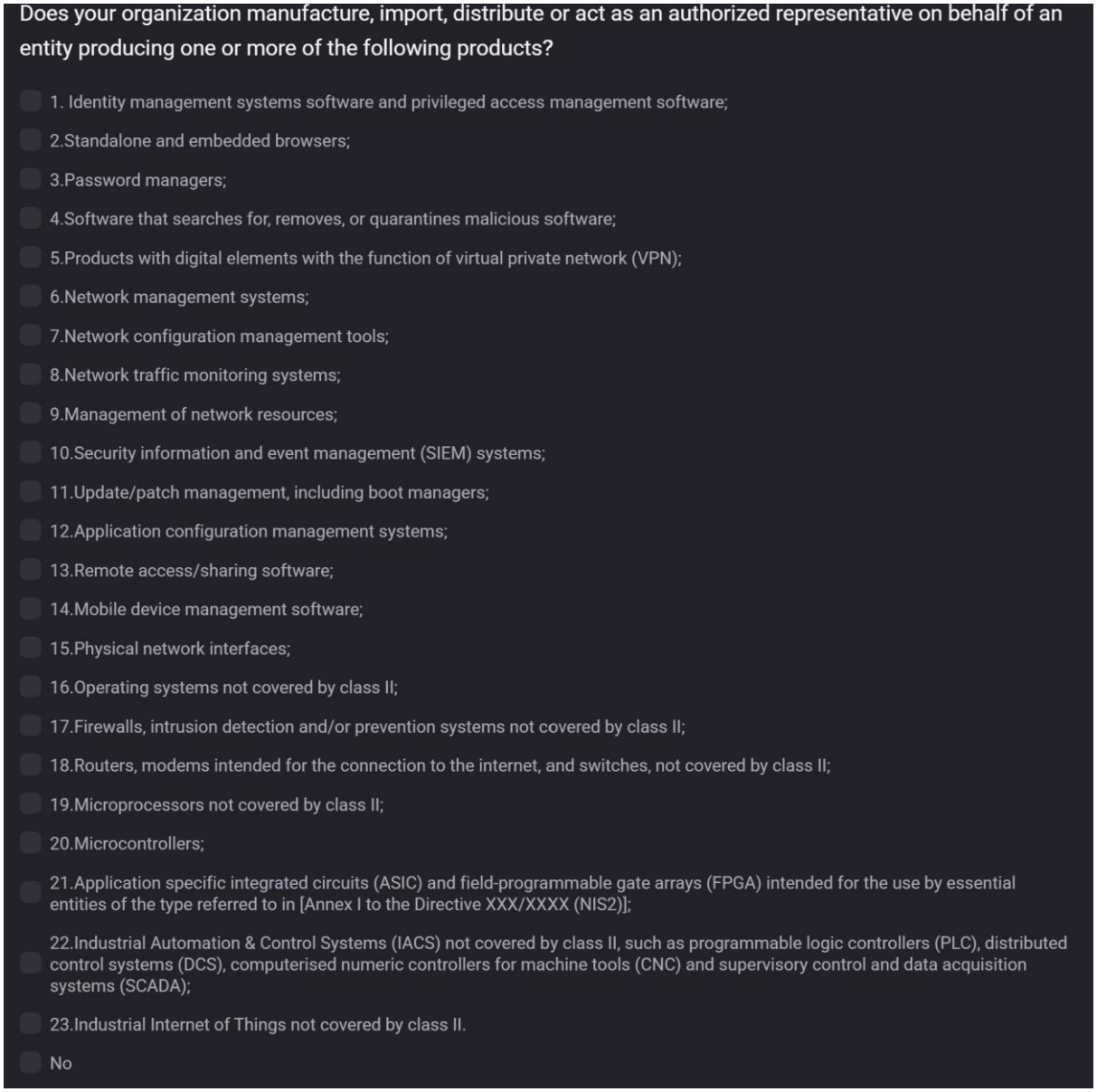

Figure 4: Class I Product Classification

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.

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

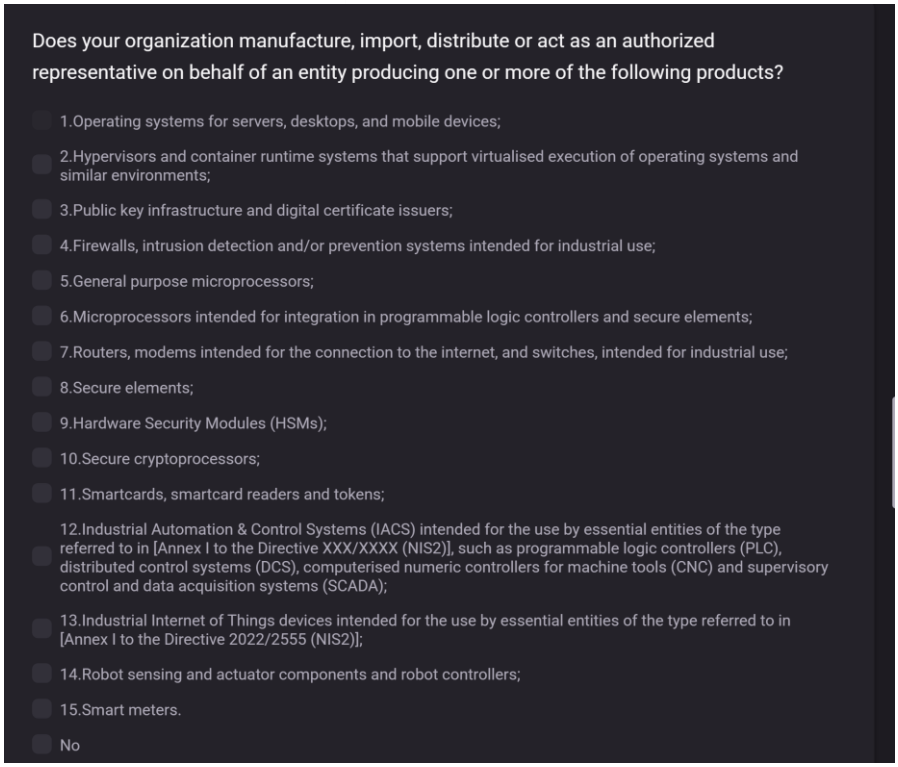

Figure 5: Class II Product Classification and Explanation

Conformity Assessment Readiness: The final step of CyReA aims to asses 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.

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

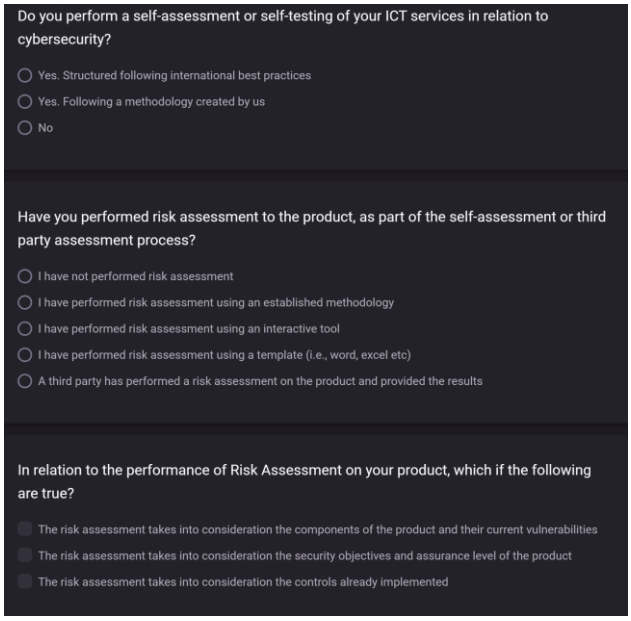

Figure 6: Readiness Assessment

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

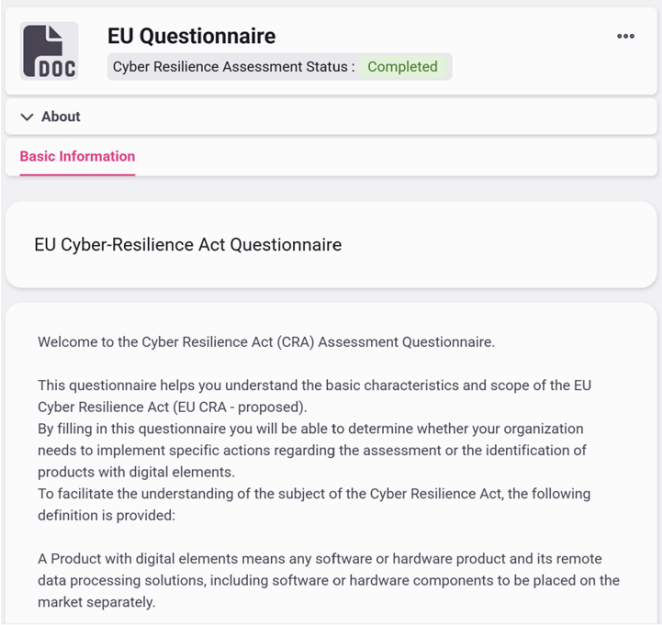

Figure 7: Completion Status

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