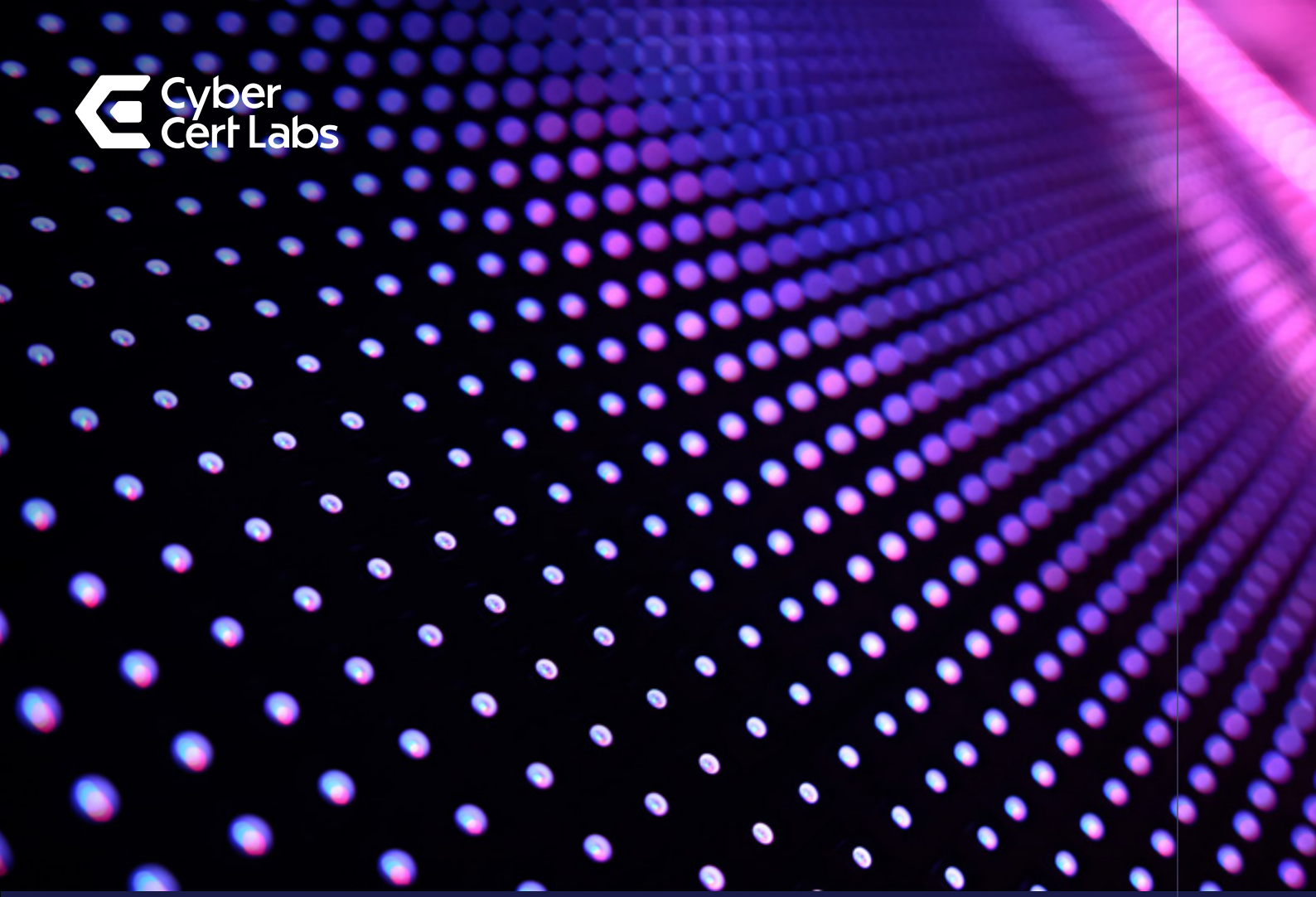
Cyber Cert Labs



Navigating the CRA

A Step-by-Step Guide for SMEs

cybercertlabs.com

Cyber Cert Labs

Table of Contents

03 Introduction

04// The Cyber Resilience Act.

08// CRA Readiness Assessment.

08 Planning

09// Is Your Product In Scope?

10// Understanding Product Categories.

13 Product Design Stage

14// What Is Security By Design And Default?

Risk Assessment.

17 Product Development Stage

18// Security Testing And Validation.

19// Substantial Modifications.

20 Product Release Stage

21// Documentation Obligations.

Support Periods.

22// Assessment.

23 Maintenance Stage

24// Ongoing Security Commitments During the Support Period.

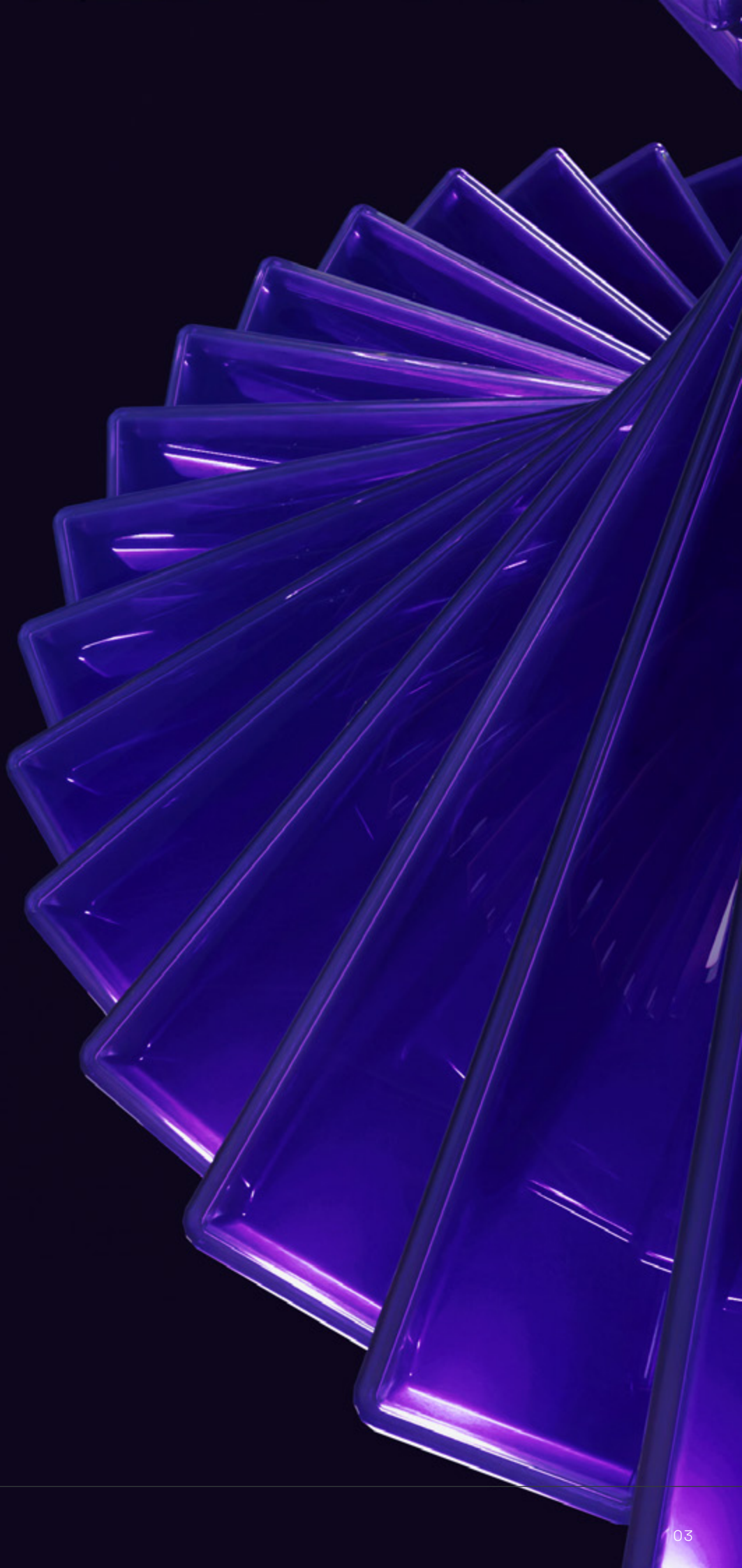
Vulnerability Reporting.

25// Vulnerability Disclosure.

Consequences Of Non-Compliance.

0.0//

Introduction



The Cyber Resilience Act

Introduction

0.1 //

The European Union has introduced a new regulation- the Cyber Resilience Act (CRA) - to safeguard the cybersecurity of products with digital elements.

This pioneering legislation sets a baseline cybersecurity standard for product with digital elements, ensuring they are designed with robust security features from the outset.

The CRA tackles two pressing issues that have compromised digital product security:

1. Inadequate Cybersecurity in Manufacturing: Digital products are often designed and developed with low levels of cybersecurity, resulting in widespread vulnerabilities. Outdated or missing security updates leave them open to cyber threats.
2. Lack of Transparency and User Awareness: Consumers struggle to make informed decisions about the security features of products with digital elements, making it easier for hackers to target these devices as entry points into larger networks.

The CRA is a horizontal regulation that applies across a broad array of sectors, ensuring all products with digital elements made available on the EU market meet essential cybersecurity standards. To show compliance, manufacturers will affix the CE mark for cybersecurity. In addition, distributors and importers in the EU or third countries will also be subject to the regulation.

A 36-month transition period after the adoption of the law will allow manufacturers time to prepare for CRA compliance. All newly released products must meet full CRA requirements after this timeframe. Vulnerability reporting obligations become mandatory 21 months into the transition period.

0.2 //

The Cyber Resilience Act

A New Reality for SMEs

The EU Commission's impact assessment on the Cyber Resilience Act (CRA) identified a significant challenge for small and medium-sized enterprises (SMEs) complying with the new cybersecurity regulation. The assessment highlighted that SMEs may struggle to meet the associated costs and gain access to cybersecurity expertise, which could hinder their ability to compete in an increasingly digital market.

0.3 //

Benefits Beyond Compliance

Why SMEs Should Care

While compliance might seem like a daunting task, the CRA offers benefits that extend far beyond adherence to regulations. By strengthening product security, SMEs can:

- Enhance customer confidence in their products
- Protect consumers against cyber threats
- Protect themselves against reputational damage
- Gain a competitive edge in an increasingly digital market

0.4 //

Gain a Competitive Edge

The CRA Readiness Assessment generates a comprehensive report that highlights your strengths and areas for improvement, providing actionable advice on how to improve your current product security posture. By leveraging our Readiness Assessment solution, you can:

- Gain knowledge and understanding of the impact of the Cyber Resilience Act on your products and processes
- Identify weaknesses and improvements in your current processes
- Develop high-level plans to meet your product security goals
- Start thinking about the cost of compliance to your organisation
- Start your planning early to gain competitive advantage

0.5 //

Understanding Your Journey to CRA Compliance

Our Step-by-Step Guide

To help SMEs navigate this new landscape, Cyber Cert Labs is offering expert guidance on what it means to comply with the CRA.

We have created an intuitive guide to help SME manufacturers navigate the complexities of the Cyber Resilience Act (CRA). The infographic below illustrates our approach to achieving compliance by seamlessly integrating new steps into the familiar product development lifecycle process. By breaking down the CRA requirements into manageable components, we aim to make compliance less daunting and more achievable for SMEs.

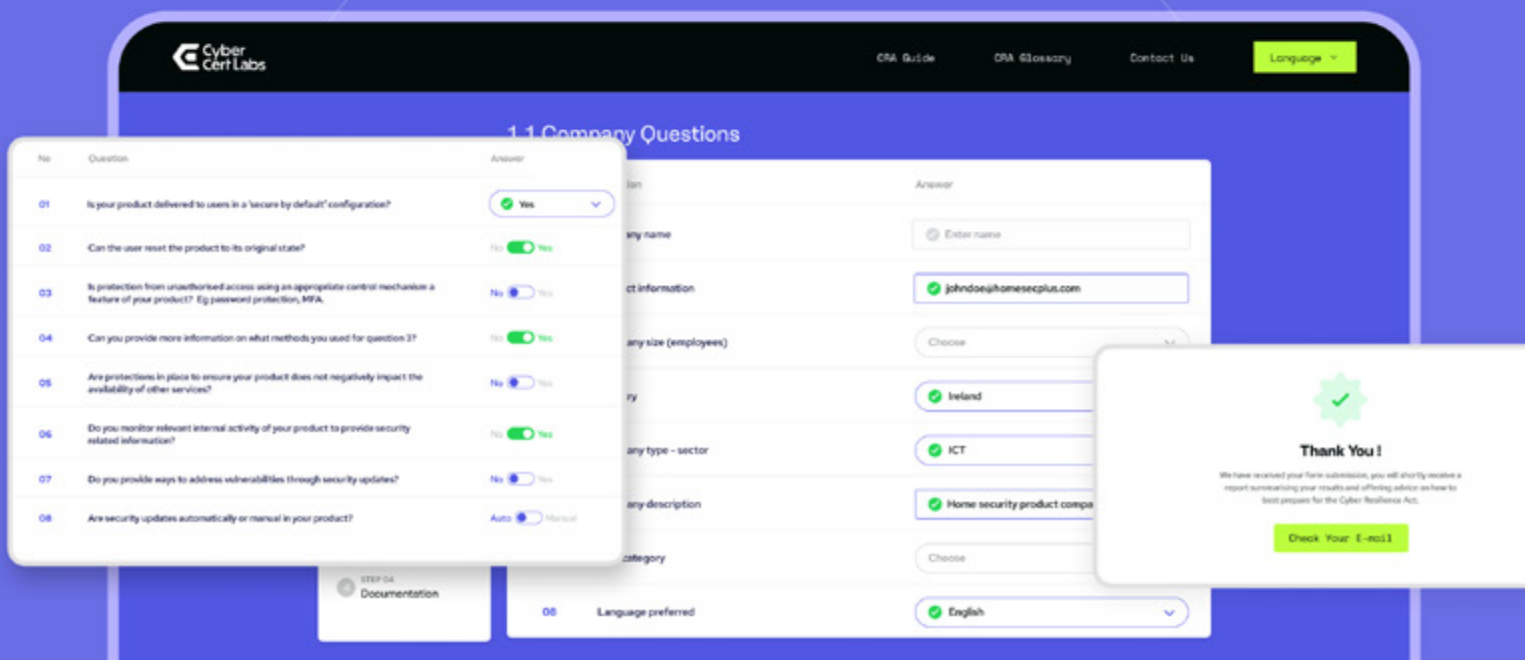
By understanding our approach to the CRA product lifecycle, SME manufacturers can better prepare themselves for compliance and make informed decisions about their product development processes.

Click the link below to find out more about our Readiness Assessment.

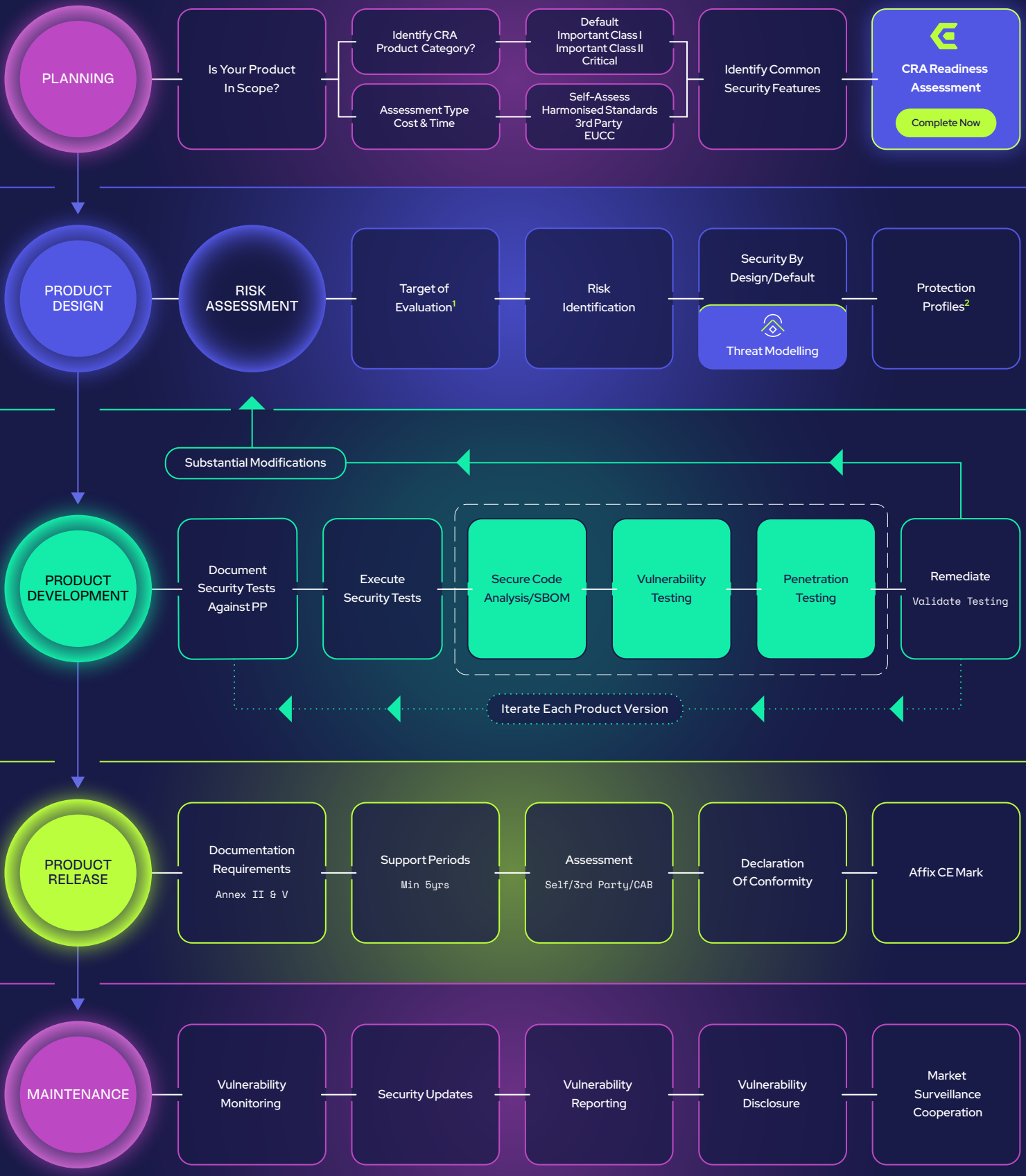
Learn More

Need more guidance?
Speak with one of our experts.

contact@cybercertlabs.com



Inside the Cyber Resilience Act



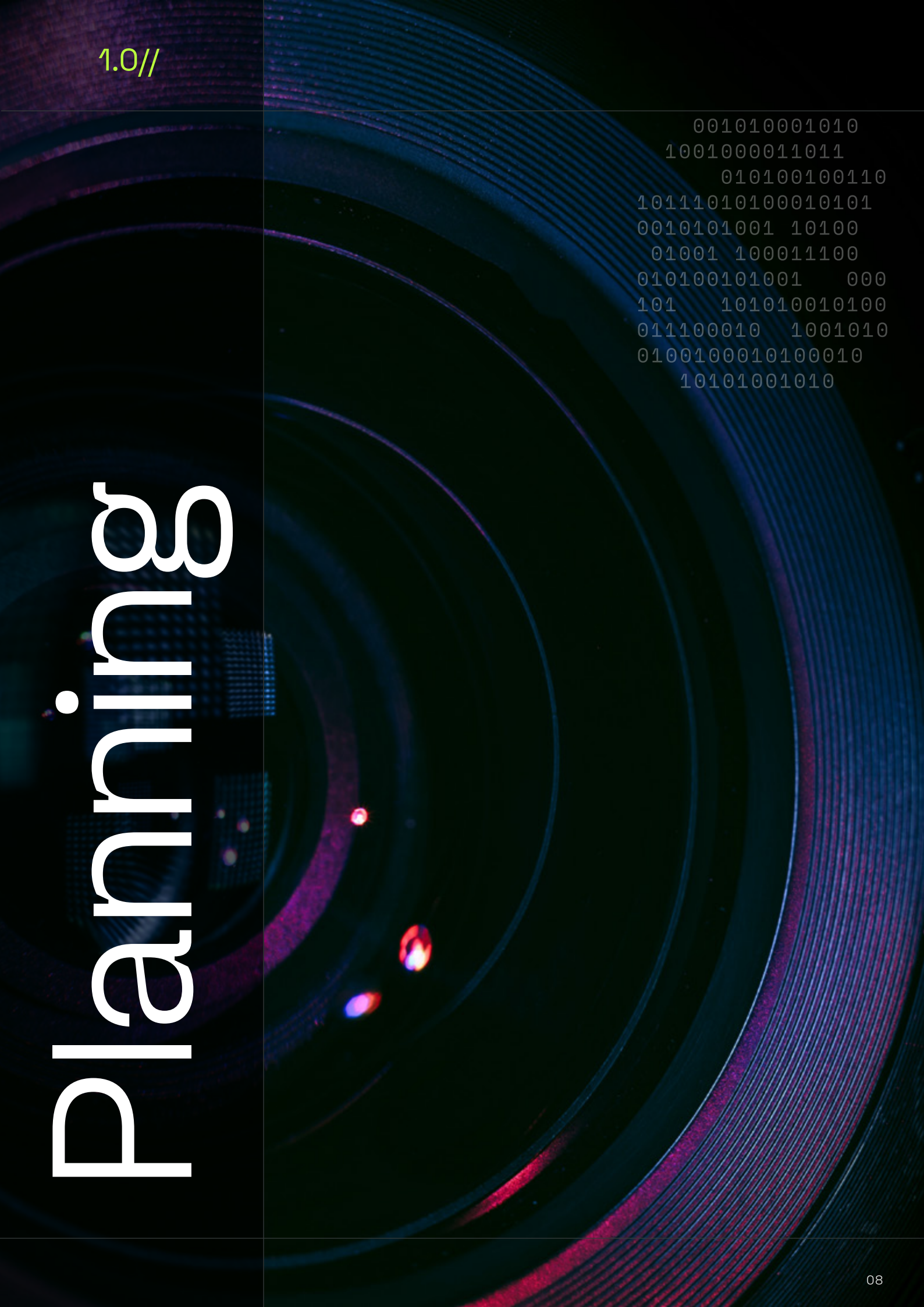
Information Key

1. Target of Evaluation // Defines the scope of what is being tested for security, in the case of the CRA this includes the entirety of the product and any remote processing solutions.

2. Protection Profile // A document that defines the security requirements and security controls needed to protect a particular product type to a specific assurance level.

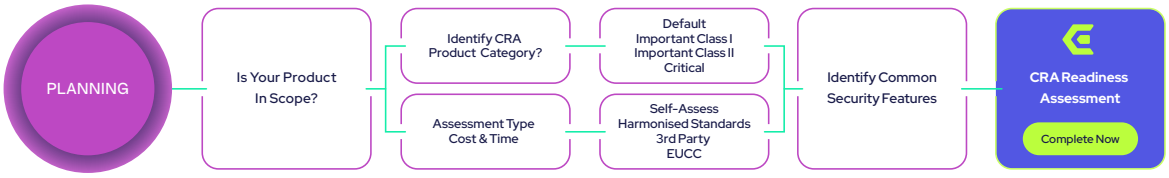
1.0//

Planning


001010001010
1001000011011
010100100110
1011101010010101
0010101001 10100
01001 100011100
010100101001 000
101 101010010100
011100010 1001010
0100100010100010
101010010 10

Planning

Stage 1 - Is your Product in Scope?



1.1 //

The first step in the product planning phase is to establish if the product falls within scope of the CRA. The tables below outline the definitions of products in scope and product out of scope.

In Scope
Products with Digital Elements
Software and/or hardware products and their associated remote data processing solutions.
Including third party software and/or hardware components
Products with a data connection to other devices or networks
Made available on the EU single market

Out of Scope
Software as a Service (SaaS) except for remote data processing solutions relating to a product with digital elements.
Medical devices & in vitro diagnostic devices
Civil aviation safety
Motor vehicles & trailers
Products with digital elements developed exclusively for national security or defence

1.2 //

Regulatory Requirements for Open-Source Software

The regulatory regime for open-source software will be light touch, which means it cannot bear the CE mark. Manufacturers that use open-source software as part of their product with digital elements must ensure that any open-source software components comply with the Cyber Resilience Act (CRA). For free and open-source software, the following requirements will apply:

- Creation and documentation of a cybersecurity policy to promote the development of a secure product with digital elements;
- Implementation of a vulnerability handling process; and
- Cooperation with market surveillance authorities

1.3 //

Understanding Product Categories

Once manufacturers determine their product is in scope for CRA compliance, they must identify which product category it belongs to. Products with digital elements are classified based on their risk level and criticality. While all products with digital elements must comply with the CRA essential requirements, the assessment method depends on the category assigned. There are four CRA categories.

Category	Default "Unclassified"	Important "Class I"	Important "Class II"	Critical Products
Examples See ANNEX III	Smart speakers, games, photo editing software, hard drives, mobile and desktops apps and everything else	IAM/PAM SW, OS, wearables, smart home, password managers, network management systems, microcontrollers, VPN, SIEM, anti virus	Hypervisors & container runtimes, firewalls, Intrusion Detection & / or Prevention, Tamper-resistant microprocessors & microcontrollers	Smart meter gateways smartcards or similar devices, including secure elements Hardware Security Modules
Conformance	SELF ASSESSMENT	HARMONISED STANDARDS Ensuring CRA principles are met	THIRD PARTY ASSESSMENT	EUCC

Default (Lowest Risk Category)

Approximately 90% of products fall into this category, which has a lower risk profile compared to other categories. Examples include:

- Smart home devices
- Printers
- Bluetooth speakers
- Media player software applications

Manufacturers with products in the Default category can use self-assessment to demonstrate compliance with CRA essential requirements (as outlined in Annex I of the CRA) and follow the self-assessment protocol detailed in CRA Annex VIII.

Important Class I

The complete list of products that fall into Important Class I can be found in Annex III of the CRA, this includes;

- Identity management systems, privileged access management software & hardware, and access control readers
- Standalone & embedded browsers
- Password managers
- Software that searches for, removes or quarantines malicious software
- Products with virtual private network function
- Network management systems
- Boot managers
- Operating systems
- Routers and modems intended to connect to the internet and switches

Manufacturers with products that fall into Important Class I can use the self-assess method to demonstrate compliance with the CRA essential requirements as long as they can apply one of the following:

- Harmonised Standard - a European standard developed by a recognised European Standards Organisation, following a request from the European Commission. Manufacturers can use harmonised standards to demonstrate that products comply with an EU legislation. Harmonised standards are currently being created specifically for the CRA.
- Common Specification – a detailed practical set of rules setting out how a product should comply with specific requirements adopted by the European Commission when no harmonised standards exist.
- European Cybersecurity Certification – a scheme ENISA is developing on behalf of the European Commission to create a framework to certify products with digital elements meet the essential requirements of the CRA.

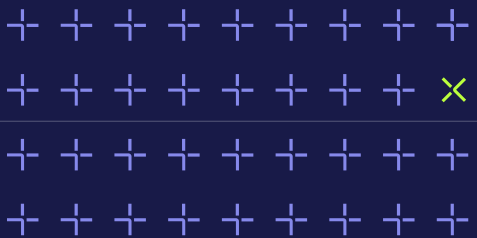
If the manufacturer cannot use one of these schemes for their product, they must apply to have their product assessed by a third-party conformity assessment body.

Important Class II

Product types that fall into Important Class II category include:

- Hypervisors and container runtime systems supporting virtualized execution of operating systems
- Firewalls, intrusion detection & prevention systems
- Tamper-resistant microprocessors & microcontrollers

Products in the Important Class II must complete a third-party conformity assessment even if they comply with harmonized standards, common specifications or a European cybersecurity certification scheme.



1.3 // Critical Class

The Critical Class includes products of the highest risk and therefore have the strictest compliance process. These include:

- Hardware devices with security boxes
- Smart meter gateways
- Smart cards or similar devices including secure elements
- Other devices for advanced security purposes, including secure crypto processing

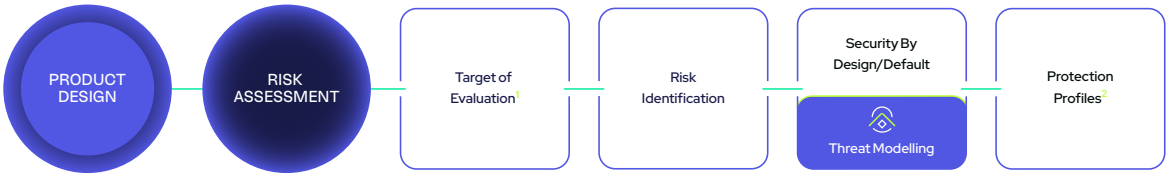
Products in the Critical Class must complete a European Common Criteria (EUCC) cybersecurity certification assessment conducted by a conformity assessment body.

Businesses should factor in the cost of compliance, as well as the additional time and effort required to bring new CRA compliant digital products to market successfully. Understanding which product category applies to their product is crucial, as this will determine the type of assessment they need to undergo, making it a key consideration when budgeting for future projects.

Design

Product Design

Stage 2



The CRA mandates that manufacturers implement security by design and default throughout the product lifecycle.

2.1 // What is Security by Design and Default?

Security by design

Refers to a concept where security is considered as a fundamental part of the design and development process, rather than being added later as an afterthought. The risk assessment required by the CRA provides the input into the design and development process. The security features that reduce the risk to an acceptable level should link back to clear security risks and defined security objectives. The goal is to build systems that are secure from the ground up, making them less vulnerable to attacks and reducing the risks of data breaches, vulnerabilities, or other security incidents.

Security by default

Is the principle that a product should be delivered to users with all security features enabled, removing the need for the end user to enable these features. This allows users who may not be well-versed in cybersecurity to start with a product in its most secure state. The first step to implementing security by design and default is to understand the risks and vulnerabilities a product is exposed to. Manufacturers are obligated to conduct a risk assessment to quantify these risks and vulnerabilities in order to comply with the CRA.

2.2 // Risk Assessment

The risk assessment allows manufacturers to identify all potential risks, and the associated threats and vulnerabilities that an end user of the product can be exposed to. This will inform what security controls need to be put in place to secure the product. The high-level steps of the risk assessment can be broken down into the following:

Target of Evaluation

The Target of Evaluation (TOE) is a critical concept in IT security, defined by ISO 15408 as the specific parts of a product that are in scope for evaluation. In the context of the CRA, the TOE encompasses not only the product itself but also any remote data processing solutions.

As per the CRA mandate, the entire product and its associated remote data processing solution must be compliant. Therefore, manufacturers should identify all components of the product, including third-party components, as part of the TOE. The documentation of the TOE must be complete enough that an independent body (such as a Conformity Assessment Body) can recreate the TOE for the purposes of testing the product.

Defining the TOE Environment

It is equally important for manufacturers to define the expected environment in which their product will operate. The TOE environment can significantly impact risk factors, and manufacturers should take this into account when designing and developing their products.

For example:

- A smart home security system designed for residential use might operate in a relatively low-risk environment.
- In contrast, a financial institution's network management system would likely be deployed in a high-security environment with strict access controls and monitoring protocols.

By understanding the TOE and its associated environment, manufacturers can take a more informed approach to product design, development, and evaluation, ultimately ensuring that their products meet the required security standards.

Risk Identification

Once the TOE and expected environment have been defined, manufacturers must enumerate the risks, threats and vulnerabilities the product may have innately or face when on the market and then assess the likelihood, severity, and impact of these risks. This involves considering factors such as:

- The probability of a particular risk event occurring
- The potential consequences of a risk event
- The consideration of the security features to prevent the risk event from occurring or to reduce the impact of the risk were it to occur
- An overall risk statement in relation to the product

By evaluating these factors, manufacturers can prioritise their efforts to mitigate, reduce and manage risks, ultimately ensuring that their products are more secure.

Implementing Security by Design and by Default

Threat modelling is a process that systematically identifies and evaluates potential threats that could impact the product. Using outputs from the risk identification stage to build the threat model and use it to model security threats so the proposed security features can be evaluated. This can help model different security features as part of the design phase reducing the cost of development and testing further down the development pipeline.

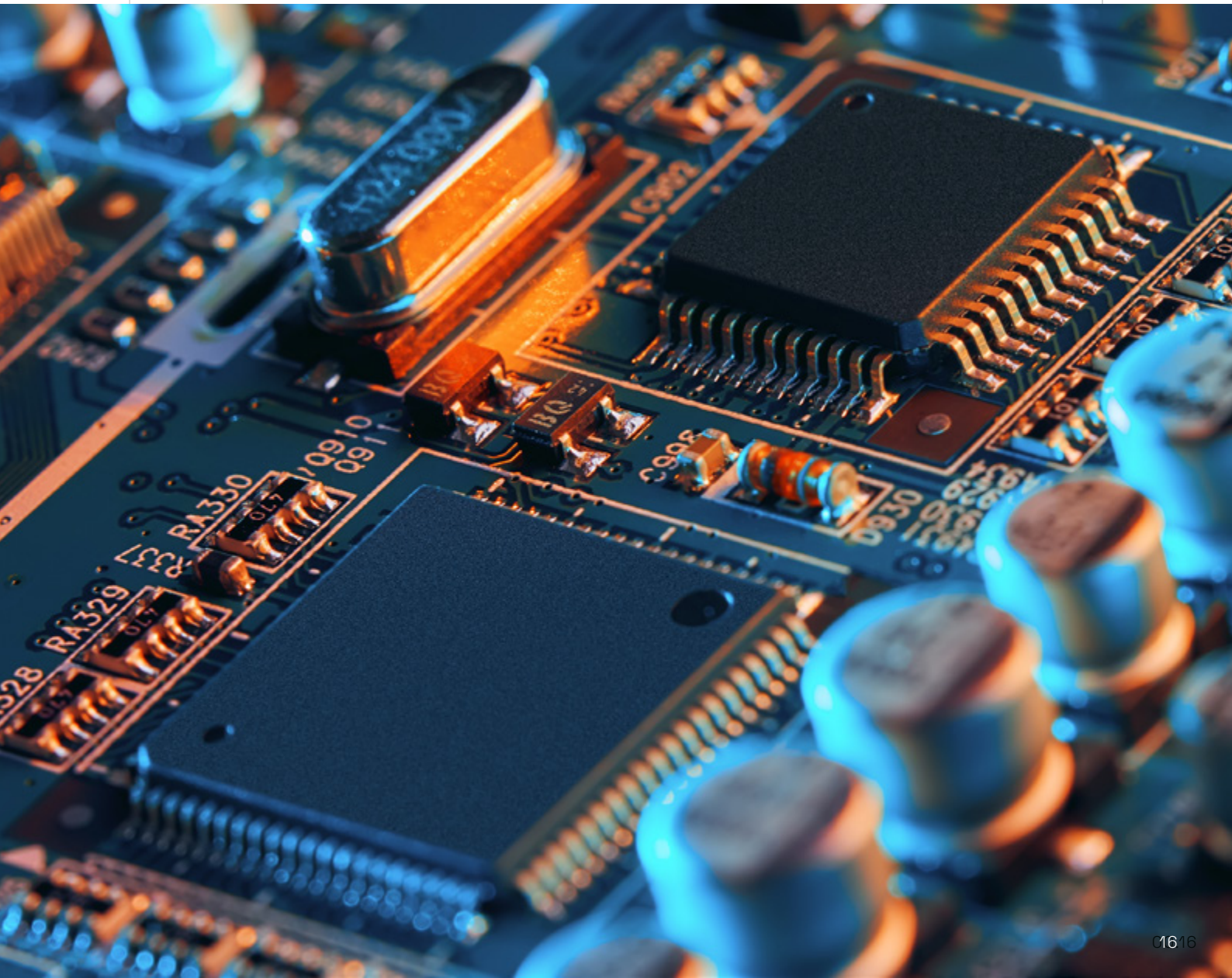
Vulnerability analysis compliments the threat modelling by identifying potential vulnerabilities or flaws in the product that could be exploited by threat actors. This analysis can help to refine the design of the security controls by providing more detail on the methods threat actors will use to compromise the security of the product.

These steps should be repeated throughout the product lifecycle to keep the threat model and risk database up to date as the product develops.

Protection Profile: The Blueprint for Security

A Protection Profile (PP) is a critical document that outlines the specific security controls needed to safeguard a particular product type. The PP serves as a blueprint for ensuring that the product meets the required assurance level, thereby protecting it from cyber threats and vulnerabilities.

The protection profile will describe what security features need to be put in place and the level of confidence needed in the security mechanisms to meet specified assurance levels. There are many published protection profiles for different product types, a manufacturer can choose to use an existing protection profile or write their own to fit their specific needs.

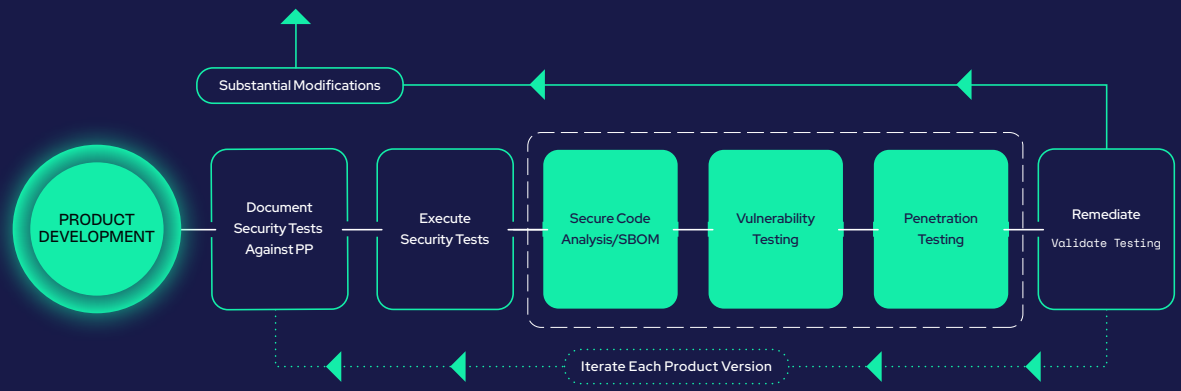


3.0//

Development

Product Development

Stage 3



3.1 // Security Testing and Validation

Throughout the product development lifecycle, it is essential to conduct various forms of testing on the product to ensure its correct functionality. Manufacturers should include security testing as part of their testing regime to verify that security controls are sufficient to meet the CRA's essential requirements. Security tests should be documented against the protection profile.

3.2 // Forms of Security Testing

Security testing encompasses a broad range of methodologies and techniques designed to identify potential vulnerabilities and security threats. Some key forms of security testing that manufacturers may want to consider include:

- **Secure Code Analysis**
  This process involves reviewing and analysing the source code of software or firmware products to identify any vulnerabilities, security flaws, or coding errors. Secure code analysis should be performed regularly, ideally every time the source code is significantly updated.
- **Vulnerability Testing**
  This methodology involves systematically scanning a product to identify and fix vulnerabilities. Vulnerability testing helps manufacturers ensure that their products are secure by identifying potential entry points for attackers.
- **Penetration Testing**
  Also known as "pen-testing," this security testing method simulates cyberattacks on a product to test its defences against malicious actors. Penetration testing provides valuable insights into the effectiveness of a product's security controls and helps manufacturers identify unpatched vulnerabilities.

Recording Test Outcomes

Before, during and after completing security testing, it is essential to record the test methodology, cases and outcomes. Based on the results, manufacturers should implement fixes or changes to

address identified vulnerabilities. Once all vulnerabilities have been remediated, re-testing should be performed to ensure that fixes have fully addressed the found vulnerabilities.

Security testing should not be a one-time activity but rather an ongoing process that continues throughout the product lifecycle. Manufacturers should repeat security testing whenever updates are made to the product, such as new version updates, to ensure that new vulnerabilities are not introduced. This is reflected in the CRA legislation as security testing and vulnerability handling must be kept up to date for the product support period.

Substantial Modifications and Risk Assessment

When substantial modifications are made to a product, manufacturers must revisit the risk assessment stage to identify potential new risks or changes in the attack surface. Significant changes to the product's intended purpose may expose it to new security threats, making it essential to reassess the risks associated with the updated product.

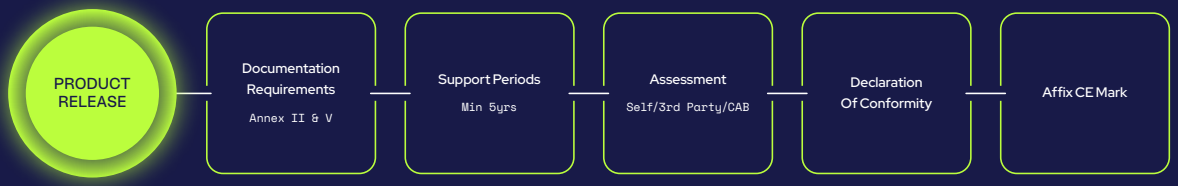
4.0//

Release


001010001010
1001000011011
010100100110
1011101010010101
0010101001 10100
01001 100011100
010100101001 000
101 101010010100
011100010 1001010
0100100010100010
10101001010

Product Release

Stage 4



Before a product with digital elements can be made available on the EU market, manufacturers must ensure they have completed the following essential steps:

4.1 // Documentation Obligations

The CRA requires manufacturers to share specific documents with users of their products. These documents include:

- Manufacturer Information: The manufacturer name/trademark, postal address or digital contact method.
- Product Description: A general description of the product, highlighting its features and functionalities.
- Vulnerability Handling Process: The single point of contact for information for vulnerability reporting and the manufacturers coordinated vulnerability disclosure policy
- Cybersecurity Risk Assessment: A comprehensive assessment of the potential cybersecurity risks associated with the product.
- Support Period: A statement outlining the support period (min 5 years) for the product, along with a justification for its length.
- Harmonized Standards and Certifications: A list of harmonized standards, common specifications, or European cybersecurity certification schemes applied to the product.
- Test Outputs and Evidence: Test outputs and evidence verifying conformity with the CRA requirements.
- EU Declaration of Conformity: The manufacturer's formal declaration that the product conforms to the relevant EU directives.

4.2 // Software Bill of Materials (SBOM)

In addition to these documents, manufacturers should create a software bill of materials (SBOM). While this document does not necessarily need to be made public or supplied to users, it must be available for market surveillance authorities upon request. The manufacturer is responsible for maintaining the technical documentation up to date throughout the support period of the product.

4.3 //

Conformity Assessment

Once all necessary documents are in place and the manufacturer has ensured conformity with CRA requirements, they can proceed with a self-assessment or assessment by a third-party conformity assessment body. After completing the conformity assessment, manufacturers must sign the EU declaration of conformity, after which the CE mark can be affixed to the product.

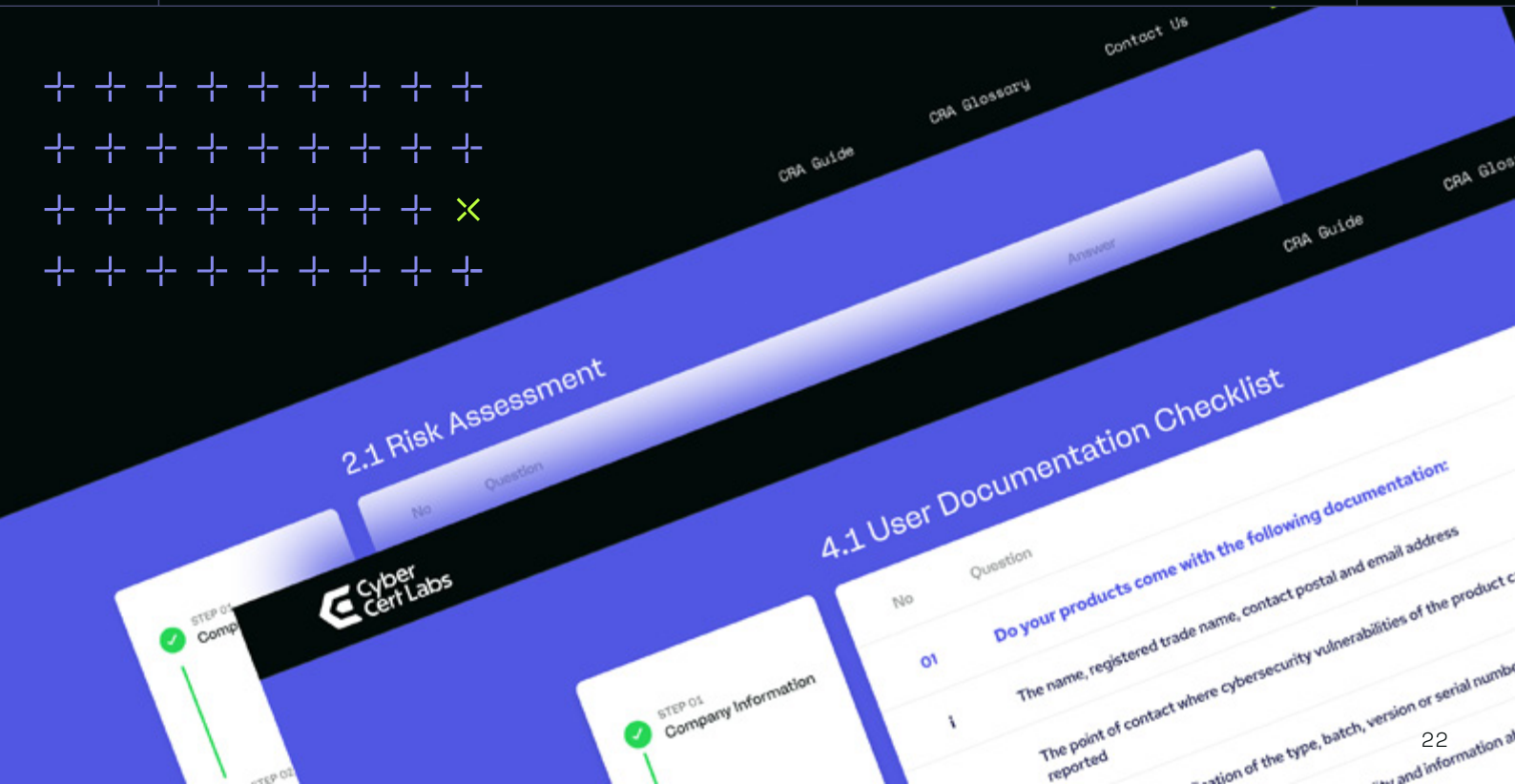
Please note that this is not an exhaustive list, and it's recommended to consult the official CRA guidelines for detailed information on these requirements.

Click the link below to find out more about our Readiness Assessment.

Learn More

Need more guidance?
Speak with one of our experts.

contact@cybercertlabs.com



Maintenance

Cyber Cert Labs

Maintenance

Stage 5

5.1 //

Ongoing Security Commitments During the Support Period

Throughout the support period of the product, which is a minimum of 5 years, manufacturers must provide ongoing security commitments to users, including:

- **Vulnerability Handling**
  Manufacturers must ensure that vulnerability handling and security updates are provided to users free of charge.
- **Continuous Security Testing**
  Continuous security testing should be conducted during the support period to detect emerging risks and check for exploited vulnerabilities.

5.2 //

Vulnerability Reporting Obligations

When an actively exploited vulnerability is found in a manufacturer's product, the CRA mandates specific reporting obligations.

Early Warning

Manufacturers must notify the CSIRT designated as the coordinator and the European Union Agency for Cybersecurity (ENISA) within 24 hours of becoming aware of an actively exploited vulnerability.

Vulnerability Notification

Within 72 hours, manufacturers must provide additional information about the vulnerability, including:

- General details about the product
- The nature of the exploit
- Any corrective or mitigating measures taken

Final Report

No later than 14 days after a corrective measure is available, manufacturers must submit a final report describing:

- The vulnerability and its severity
- Information about any malicious actors
- Details of the security update or corrective measures

ENISA is developing a single reporting platform to streamline vulnerability reporting for manufacturers.

5.3 // Vulnerability Disclosure

Manufacturers must also inform impacted users about actively exploited vulnerabilities. The information shared should include:

- Risk mitigation and corrective measures
- Any additional steps that can be taken to protect against the vulnerability

5.4 // Coordinated Vulnerability Disclosure Policy (CVD)

Manufacturers are required to put in place a coordinated vulnerability disclosure policy (CVD). This is a policy that allows external individuals or entities to report vulnerabilities in a product to a manufacturer directly or indirectly.

5.5 // Consequences of Non-Compliance

Failure to comply with the essential requirements of the Cybersecurity Act (CRA) or its implementing regulations, including vulnerability or incident reporting, may result in severe penalties.

Administrative Fines

- Up to €5 Million or 1% of global turnover: This is the maximum fine for non-compliance with CRA essential requirements.
- Up to €10 Million or 2% of global turnover: This is the maximum fine for non-compliance with other obligations, such as reporting vulnerabilities or incidents.
- Up to €15 Million or 2.5% of global turnover: This is the maximum fine for supplying misleading information to enforcement bodies or national CSIRT teams.

In extreme cases, EU authorities may require the recall or withdrawal of non-compliant products from the market.

Special Consideration for SMEs

Administrative fines do not apply to micro or small and medium-sized enterprises (SMEs) for failures to meet the 24-hour deadline for early warning notification. Member States should not impose other kinds of penalties with a pecuniary character on these entities.

Is Your Business CRA Ready? Be Proactive, Not Reactive.

The Cyber Resilience Act (CRA) is here. Don't wait until it's too late to secure your digital products!

Our **30-minute online Readiness Assessment** will help you get ahead of the curve.

How it works

- Answer key questions based on the CRA essential requirements.
- Get a comprehensive report highlighting your products security strengths and areas for improvement.
- Receive actionable recommendations to enhance your CRA preparedness and overall product security.

Protect users. Build trust.

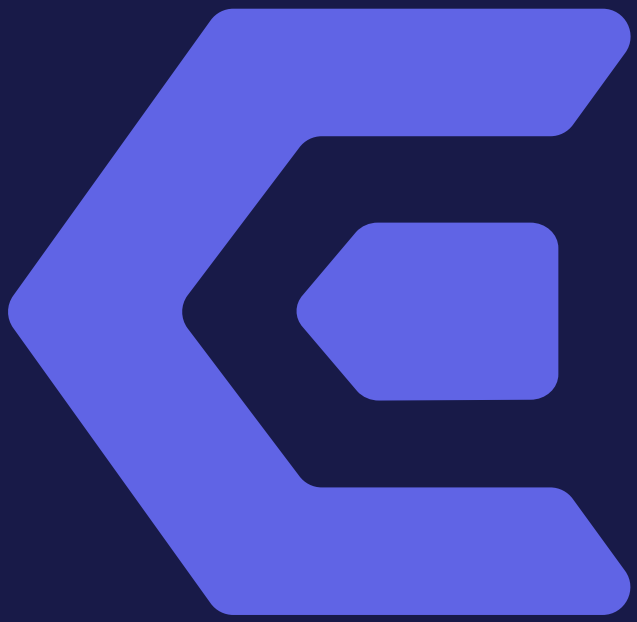
Ready to act?

Fill in a Readiness Assessment.

Start Now

Need more guidance?
Speak with one of our experts.

contact@cybercertlabs.com



cybercertlabs.com