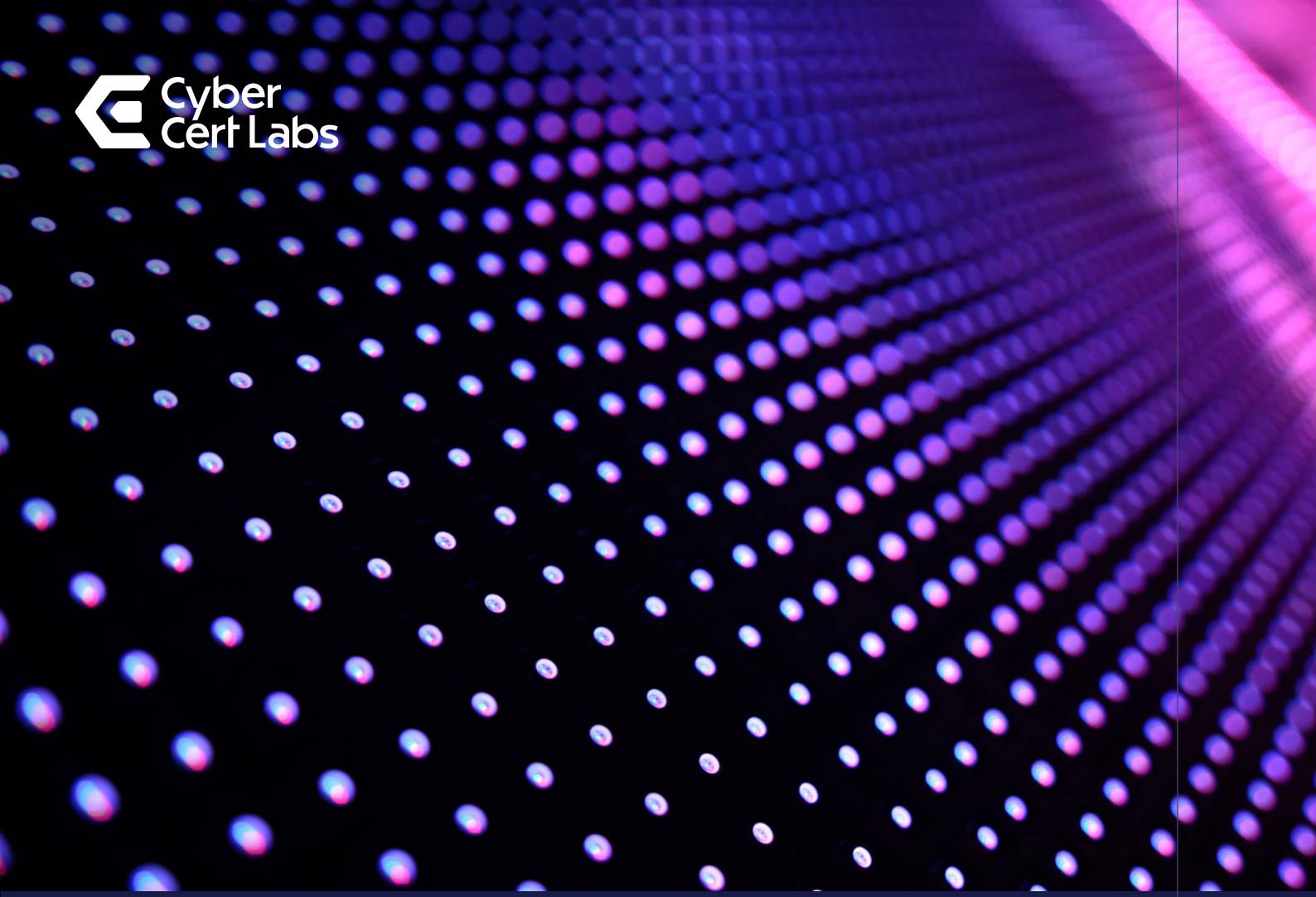
Cyber Cert Labs



Navigating the CRA

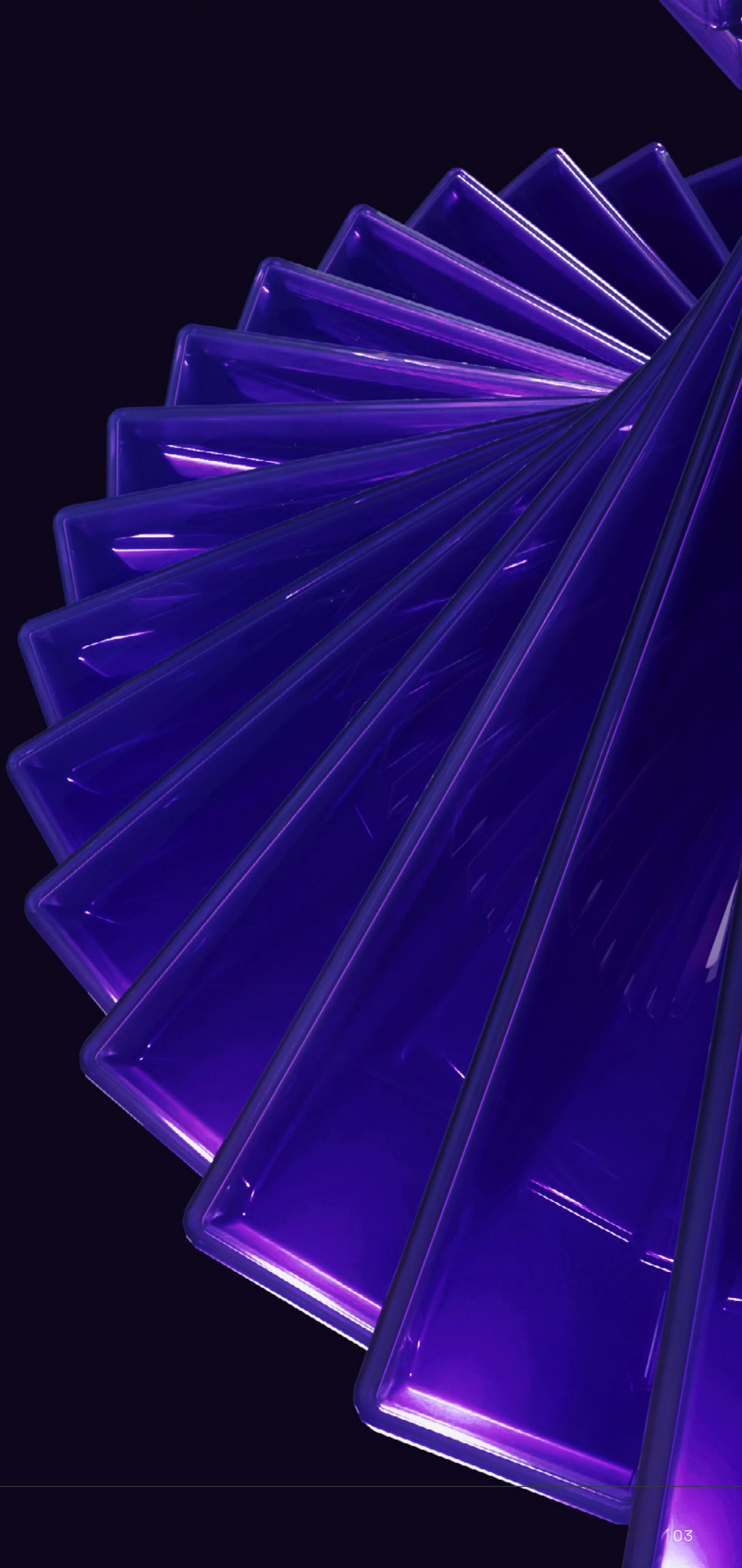
A Step-by-Step Guide for Digital Product Manufacturers

Cyber Cert Labs

Table of Contents

0.0//

Introduction



The Cyber Resilience Act

Introduction

0.1 //

The European Union has introduced a landmark regulation; the Cyber Resilience Act (CRA, Regulation (EU) 2024/2847), to safeguard the cybersecurity of products with digital elements placed on the EU single market.

The CRA establishes the first horizontal, cybersecurity baseline for products with digital elements, ensuring they are designed, developed, released and maintained with robust security from the outset. It applies to virtually all manufacturers of products with digital elements that make their products available on the EU market, regardless of size or sector. This ranges from connected consumer devices and industrial controllers to enterprise software, embedded firmware and the cloud back-ends that support them.

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

1. Inadequate Cybersecurity in Manufacturing: Products with digital elements are often designed, developed and manufactured with low levels of cybersecurity, creating widespread vulnerabilities. Outdated or missing security updates leave them, and the networks they connect to, exposed to cyber threats that cascade across supply chains.
2. Lack of Transparency and User Awareness: Buyers, integrators and consumers struggle to make informed decisions about the security of the products they purchase and connect to, making products with digital elements an attractive entry point for attackers.

Manufacturers of products with digital elements will have to adopt the essential cybersecurity requirements and vulnerability handling requirements set out in the CRA. To demonstrate compliance, manufacturers will affix the CE marking to their product and sign a declaration of conformity, legally attesting their product meets the essential security requirements set out by the CRA.

0.2 //

Timeline and Key Dates

The CRA entered into force on 10th December 2024, triggering a phased transition that gives manufacturers time to prepare. There are three key dates to note:

- 11th June 2026 - Provisions on the notification of conformity assessment bodies begin to apply, allowing the third-party assessment ecosystem to scale up ahead of full applicability.
- 11th September 2026 - Vulnerability and incident reporting obligations apply. Manufacturers must report actively exploited vulnerabilities and severe security incidents to ENISA and the relevant national CSIRT. Notably, this obligation also covers actively exploitable vulnerabilities in legacy products already on the market.

- 11th December 2027 - Full applicability. From this date, every product with digital elements placed on the EU market must meet all CRA essential requirements and carry the CE marking.

With less than two years until full applicability, manufacturers that begin their compliance journey now will be best positioned to maintain uninterrupted access to the EU market and to absorb the design, testing and documentation work without disrupting product roadmaps.

0.3 // The Global Product Security Regulatory Landscape

The CRA is the first comprehensive product security regulation of its kind anywhere in the world, but it is not the only one. Major markets including the United Kingdom, the United States, Singapore, Australia, Japan and several other Asian economies are rolling out their own product security regimes. For manufacturers of products with digital elements selling internationally, these schemes are quickly becoming part of the cost of doing business:

- United Kingdom - PSTI. The Product Security and Telecommunications Infrastructure regime sets baseline security requirements for consumer connectable products, including a ban on universal default passwords, a published vulnerability disclosure policy and clear minimum support periods.
- United States - U.S. Cyber Trust Mark. A voluntary, FCC-administered cybersecurity labelling scheme for consumer IoT, signalling to buyers that a product meets a defined baseline of security criteria.
- Singapore - Cybersecurity Labelling Scheme (CLS). A four-tier rating scheme for consumer smart devices, with mutual-recognition arrangements that extend its reach across the region.
- Other markets. Australia, Japan and a growing list of other countries are introducing voluntary or mandatory schemes of their own, most still focused primarily on consumer IoT.

Most of these schemes are deliberately light-touch and aimed primarily at consumer connected devices. The CRA sets a markedly higher bar including significantly stricter security requirements that apply across all categories of product with digital elements. By using CE marking as the conformity mechanism, the CRA makes product security a legal and commercial precondition for accessing the EU single market.

For manufacturers, the practical implication is clear: investing in CRA compliance positions a product to meet the world's most demanding product-security regime, while also providing a strong foundation to satisfy lighter-weight schemes such as PSTI, the U.S. Cyber Trust Mark and CLS as they continue to evolve.

0.4 // Why CE Marking Matters

CRA compliance, and the CE marking that comes with it, delivers benefits that extend far beyond avoiding fines and product recalls:

- **Continued access to the EU single market.** A precondition for selling, integrating or distributing products with digital elements anywhere in the EU.
- **Stronger customer trust and procurement competitiveness.** B2B buyers, integrators and public-sector procurers increasingly require demonstrable product security as part of the buying decision.
- **Reduced exposure to breach costs and reputational damage.** Early identification, remediation and disclosure of vulnerabilities limits incident impact and supply-chain risk.
- **A durable competitive edge.** In an increasingly security conscious market, a product with CE marking signals quality, accountability and long-term commitment to customers.

Treated as a strategic investment rather than a regulatory burden, CRA compliance turns product security into a measurable commercial advantage.

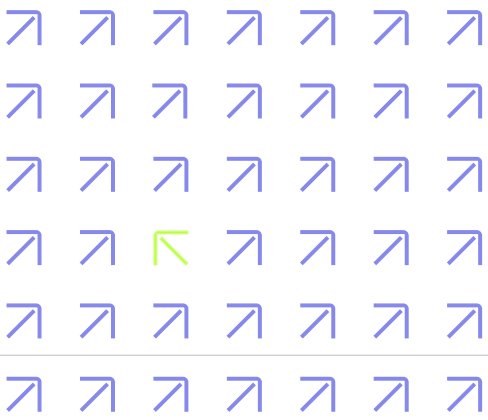
0.5 //

About Cyber Cert Labs

Cyber Cert Labs (CCL) helps manufacturers navigate the Cyber Resilience Act with practical, expert-led guidance. We translate complex regulatory text into clear, actionable steps that fit the way modern hardware and software teams actually work.

CCL leads CRA-AI, an EU co-funded project developing the next generation of tools for CRA compliance at scale. As part of this work, we are building an end-to-end product security and compliance platform called Attestra. Powered by AI and purpose-built for manufacturers of products with digital elements, Attestra covers scope and category determination, threat led risk assessment, security-by-design, security testing, technical documentation and evidence, vulnerability handling and post-market monitoring in a single workflow.

Alongside the platform, we operate the Attestra Academy, our training arm dedicated to upskilling product, engineering, quality, security and compliance teams on how to implement the CRA in practice. From foundational awareness through to role specific deep dives and product use cases, the Attestra Academy gives organisations the knowledge needed to embed CRA compliance into everyday product development.



CRA SECURITY & COMPLIANCE

Ship Secure Products. Faster.

The AI-powered platform purpose-built for Cyber Resilience Act conformity.

Attestra

One Platform. All CRA requirements.

Attestra turns the CRA from a regulatory burden into a structured, manageable programme of work. Built by product security experts, it guides manufacturers step by step from first obligation to CE Mark, deadlines are handled, not feared!

WHY MANUFACTURERS CHOOSE ATTESTRA

Purpose-built for CRA and CE Mark. Every workflow produces the evidence you need for conformity.

Lower cost of compliance. AI-guided workflows reduce reliance on consultants who cost €1,200–€1,800 a day.

September 2026 ready. Vulnerability and incident reporting is live now. Start meeting your obligations today.

Security embedded, not bolted on. Move from reactive security practices to secure lifecycle management that scale with your product.

// Get Started

Join the Attestra Early Adopter Programme for early access, expert-led workshops, free CRA guides, and discounted pricing.

Sign Up for Free Trial

NOW LIVE

VULNERABILITY HANDLING & REPORTING

Receive, triage, manage, and report vulnerabilities. AI-powered ENISA and CSIRT form pre-fill. Branded public portal for your coordinated vulnerability disclosure policy. Your Day 1 priority for September 2026.

RISK ASSESSMENT

Import your SBoM, build a digital twin of your product, run threat-led assessments, and document your security-by-design decisions, all mapped to the CRA essential requirements and emerging harmonised standards.

PRODUCT TESTING

Generate test cases from your security objectives, collect evidence, and produce the test reports needed for conformity assessment.

DOCUMENTATION & ATTESTATION

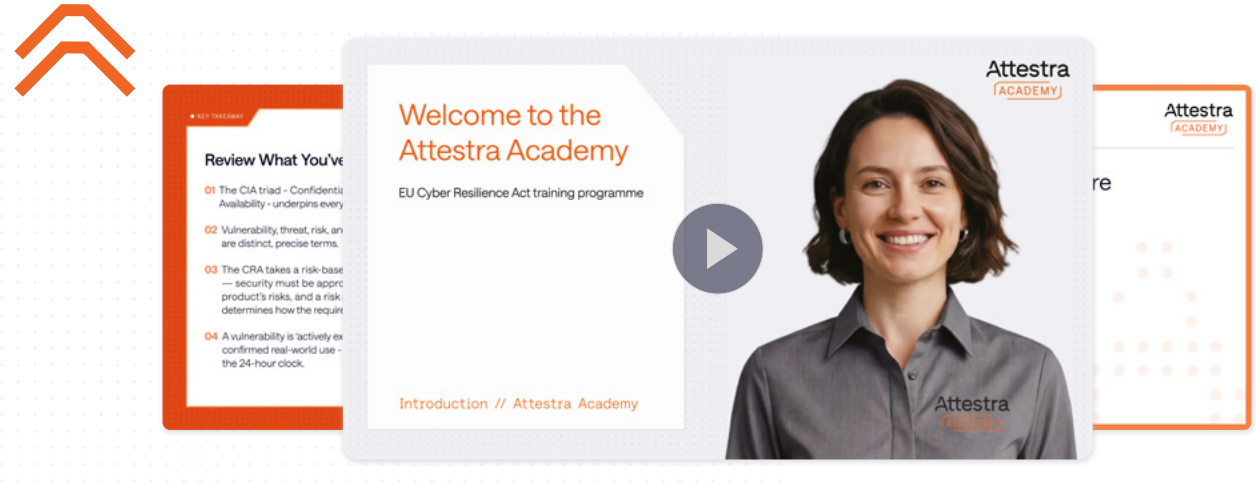
Auto-generate the technical documentation pack and Declaration of Conformity required for the CE Mark.

PRODUCT MAINTENANCE

Track fixes, update documentation, and loop through assessments as your product evolves across its support period.

Attestra ACADEMY

The complex, made simple.



The CRA is not a one-off project. It applies across the full product lifecycle embedding cybersecurity into your day-to-day operations. Your team needs to acquire the necessary skills and knowledge to bring the CRA obligations in house.

Attestra Academy gives product engineering and compliance teams the CRA knowledge to drive conformity internally. Courses are delivered through engaging video, available in multiple languages and updated as guidance from the European Commission and ENISA evolves.

WHAT YOUR TEAM GETS

End-to-end CRA Learning
From fundamentals through to post-market obligations.

In-house Capability
Stand over your product security and build in house expertise.

Always Current
Content updated as new guidance and harmonised standards are released.

Multi-lingual
Teams learn in their own language.

Resource Hub
Real product case studies showing the CRA applied across different product types. Create study notes, receive step-by-step guides, infographics and official reference materials.

WHAT YOUR TEAM LEARNS

CRA Fundamentals. Scope, obligations, product categories, conformity routes, and key deadlines.

Vulnerability Handling & Reporting. From coordinated disclosure policy to the 24-hour ENISA notification.

Risk Assessment & Product Security. Threat modelling, threat-led assessment, security-by-design principles and security testing.

Conformity & the CE Mark. Technical documentation, user documentation, evidence, Declaration of Conformity and what assessment bodies expect.

Post-Market Obligations. Vulnerability tracking, risk monitoring, security updates, and managing the five-year support period.

// Start Training Your Team

Explore the Attestra Academy and build your teams expertise.

Get Started

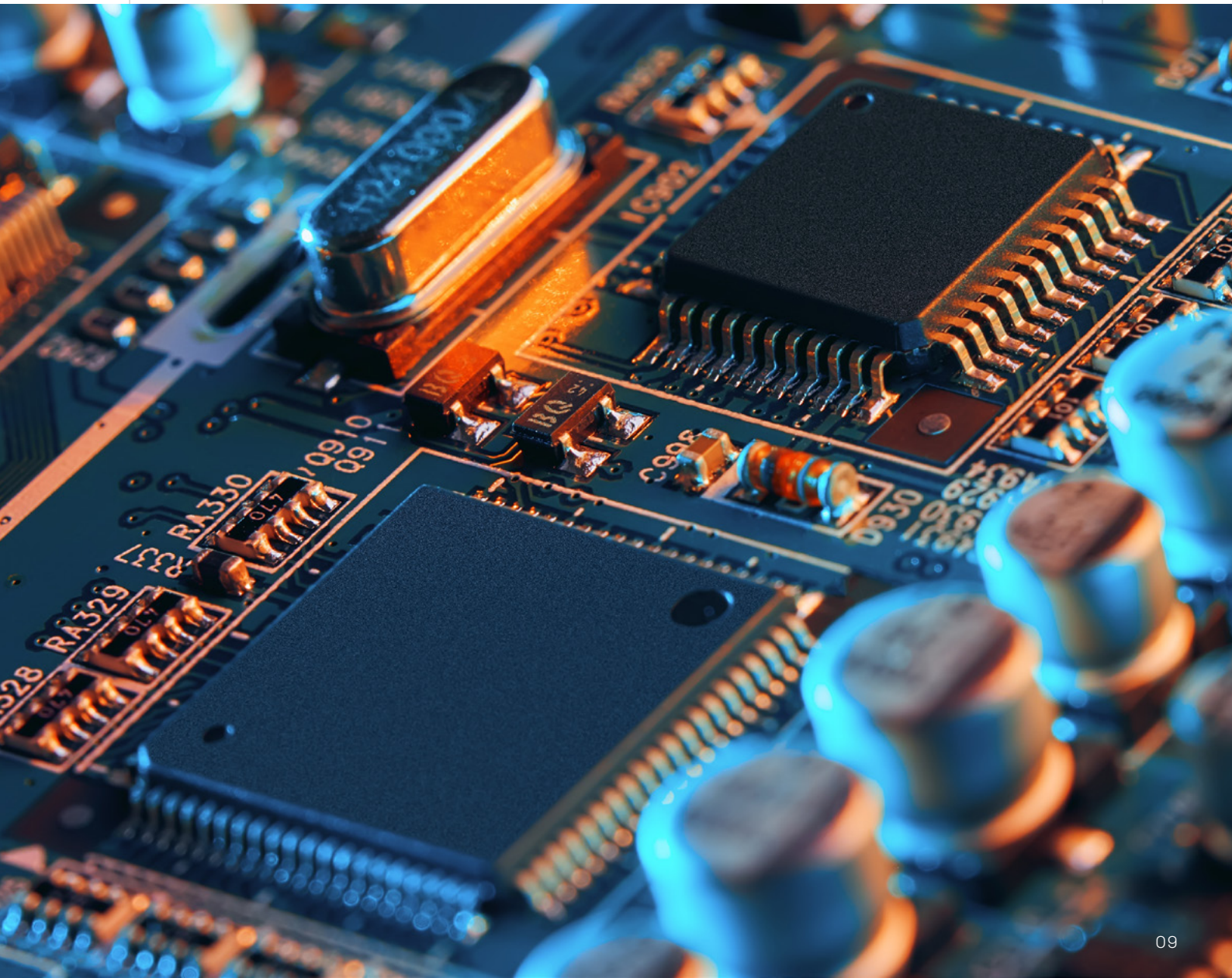
0.6 //

Understanding Your Journey to CRA Compliance

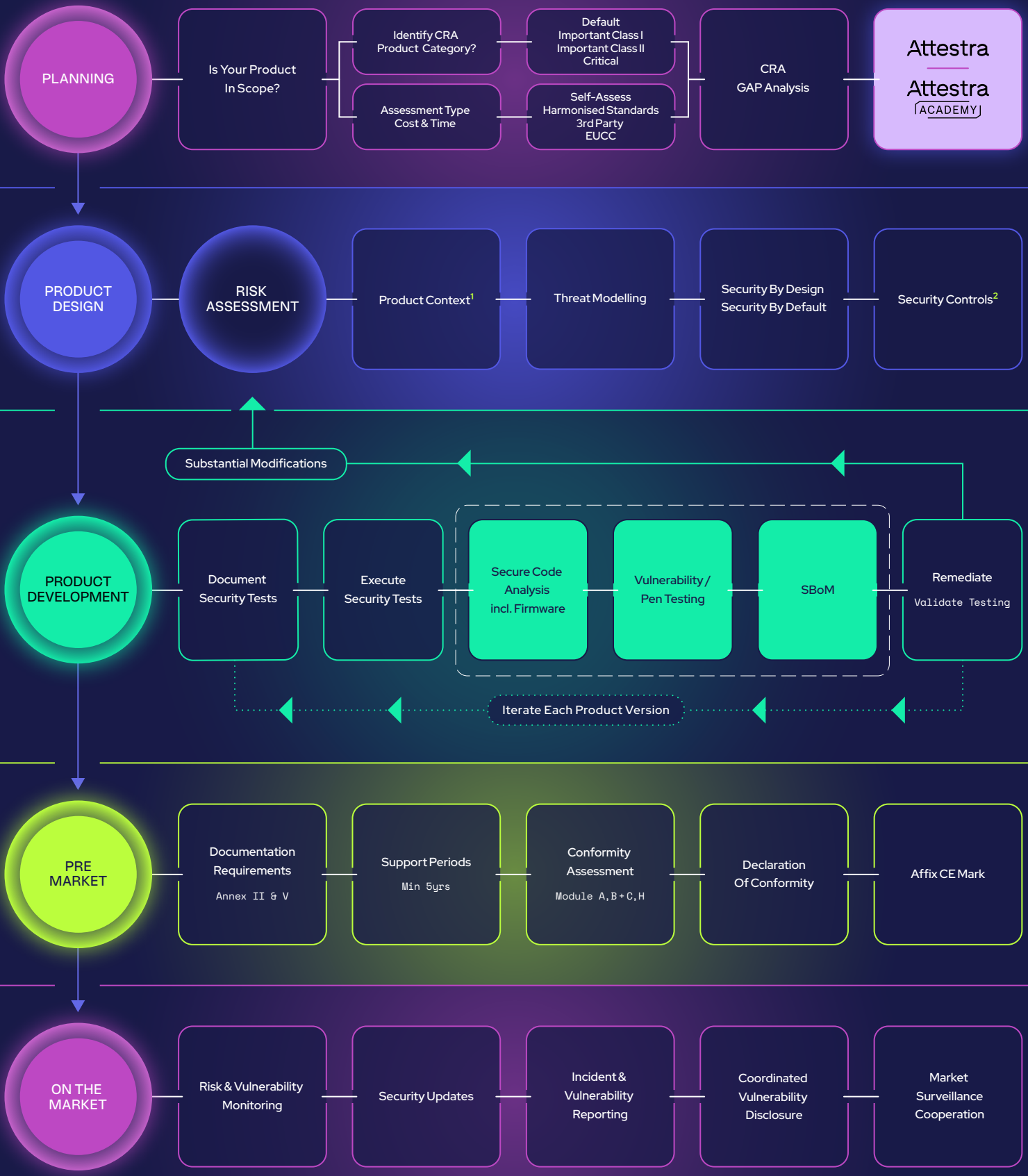
Our Step-by-Step Guide

To help manufacturers of products with digital elements navigate this new landscape, we have created an intuitive guide that aligns the CRA's requirements with a typical product development lifecycle. The infographic on the following page illustrates our approach to breaking the CRA down into manageable stages so that compliance becomes a structured, achievable programme of work rather than an overwhelming regulatory hurdle.

By understanding our approach to the CRA product lifecycle, manufacturers can prepare with confidence and make informed decisions about their product development processes.



Inside the Cyber Resilience Act



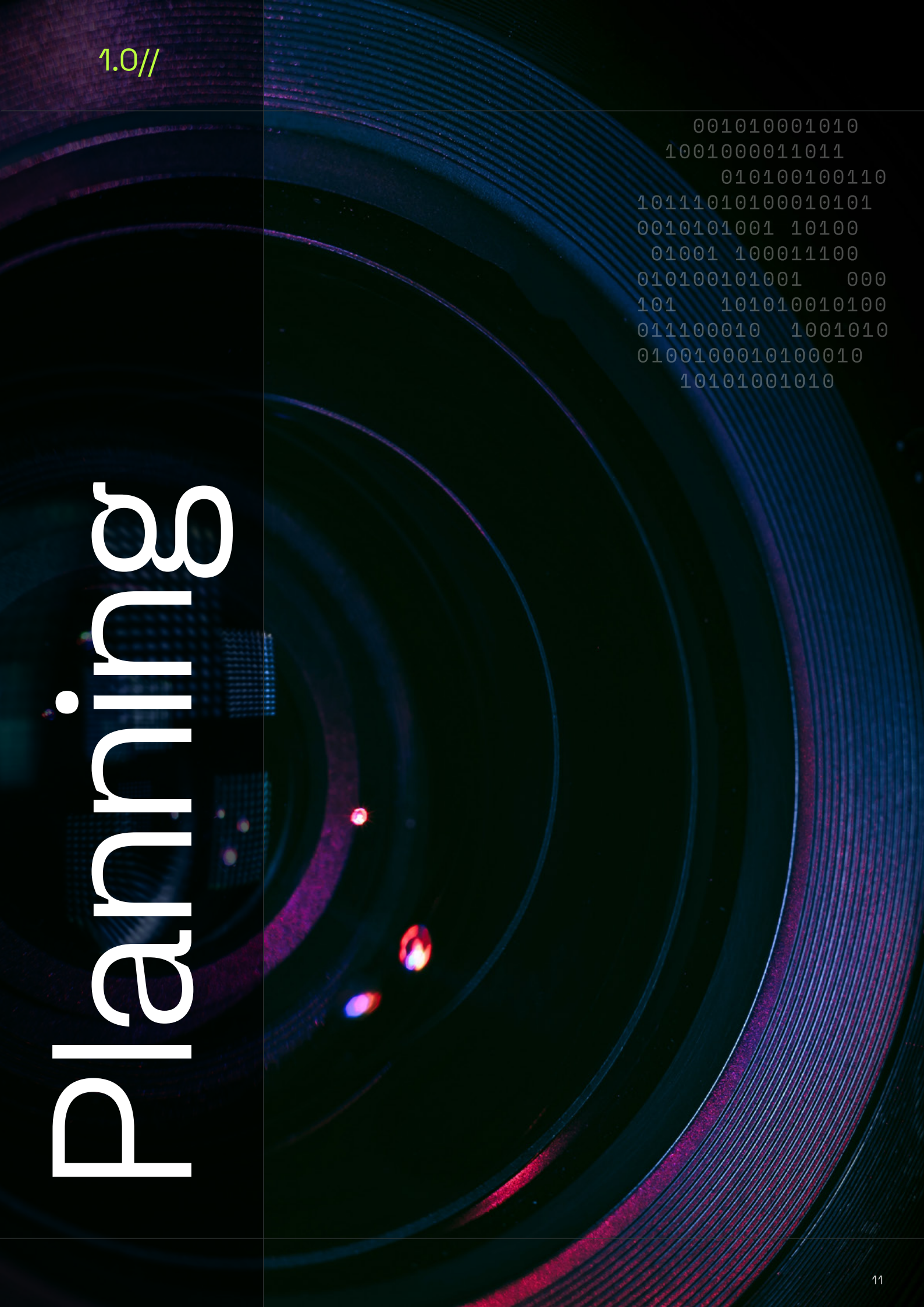
Information Key

1. Product Context // The product's intended purpose, reasonably foreseeable use, functions, operational environment, architecture, and users.

2. Security Controls // A document that defines the security controls that implement security by design/default and which are included in the user documentation.

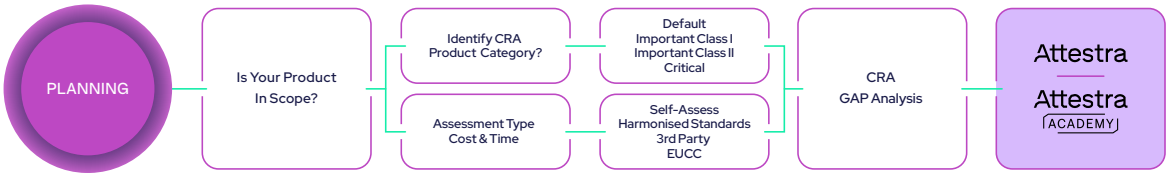
1.0//

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 CRA applies to products with digital elements that are made available on the EU market. This gives us two criteria to define scope by:

- What is a product with digital elements?
- How is 'made available on the market' defined?

A product with digital elements is defined in the CRA as 'a software or hardware product and its remote data processing solution' where the intended purpose or reasonably foreseeable use of the product includes a direct or indirect logical or physical data connection to a device or network. This includes products with third party software or hardware components not made by the manufacturer.

Remote data processing solution (RDPS) is defined as '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'. If a RDPS was not designed and developed by the manufacturer or was not tailor made for the manufacturer and instead was provided by an external service provider as a product or service, the RDPS does not come under the scope of the CRA.

Making available on the market is defined as: 'the supply of a product with digital elements for distribution or use on the EU market in the course of a commercial activity, whether in return for payment or free of charge'. **Commercial activity** encompasses more than just selling a product. Commercial activity is also defined as charging for technical support services that does not cover recuperation costs alone, requiring processing of personal data as a condition of use for reasons other than security, accepting donations exceeding the cost of product development or intention to monetise the product in other ways such as providing a software platform which the manufacturer uses to monetise other services. If your product meets these criteria, it is in scope for the CRA.

There are some exceptions that are out of scope of the CRA, these are:

- Software as a Service (SaaS) is out of scope unless it is used as a RDPS or the products functionality relies on the service.
- Medical devices and in vitro diagnostic devices.
- Motor vehicles and trailers.
- Aeronautical products, parts and equipment.
- Products with digital elements developed **exclusively** for national security or defence.

The EU Commission released guidance on the CRA to give more information and examples of the application of the legislation, more detail on the scope of the CRA can be found here.

1.2 // Regulatory Requirements for Open-Source Software

Free and open-source software (FOSS) is defined in the CRA as 'software the source code of which is openly shared, and which is made available under a free and open-source licence which provides for all rights to make it freely accessible, usable, modifiable and redistributable'.

The CRA only applies to products with digital elements that are placed on the market in the course of commercial activity. If FOSS does not meet the requirements of being placed on the market it does not have to adhere to the CRAs essential requirements and instead must comply with light touch requirements. This also means FOSS cannot bear the CE marking and so it is the responsibility of manufacturers that use open-source software as part of their product with digital elements to ensure that any open-source software components comply with the CRA.

The CRA refers to an **'Open-Source Steward'**, this is a legal person who publishes or supports FOSS intended for integration with products to be placed on the market. Open-source stewards have to follow light touch security requirements outlined in the CRA but do not have the same responsibilities as a manufacturer. FOSS security requirements are:

- Creation and documentation of a cybersecurity policy to promote the development of a secure product with digital elements;
- Implementation of a vulnerability handling process;
- 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 assigned assessment method depends on the product category. The EU Commission outlines the conformity assessment type to be used in Annex VIII. The conformity assessment procedures can be found in full here.

It is important to understand when deciding what category a product falls into, what the **products core functionality** is. A product's core functionality refers to the product's main features and technical capabilities, without which it would not be able to meet its intended purpose. For example, a smart phone manufacturer integrates an operating system as part of the product, but the smart phones core functionality is not the same as an operating system, it is an ancillary function that allows the smart phones core function (enabling users to communicate and access software applications) to work. Therefore, the smartphone as a product does not automatically fall into the same category as an operating system.

The EU Commission release an implementing regulation to give technical descriptions of the important and critical class products to help manufacturers understand what the core functionality is for these products, the regulation can be found here.

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	THIRD PARTY ASSESSMENT	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 **Module A** of the conformity assessment procedure. This is a self-assessment to demonstrate compliance with CRA essential requirements.

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 **Module A** self-assess method to demonstrate compliance with the CRA essential requirements as long as they can fully 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.
- **Common Specification** – aa 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 has developed on behalf of the European Commission to create a framework to certify products with digital elements meet the essential requirements of the CRA, more detail can be found here.

If the manufacturer cannot use one of these schemes for their product, then self-assessment is not applicable. The manufacturer must comply with **Module B and C** of the conformity assessment procedure. Module B is a EU-type examination of the products design conducted by a notified body. Module C is conducted by the manufacturer to ensure the production of its

products meets the standard approved in Module B and provide the CE marking and declaration of conformity. Manufacturers can also opt to use **Module H** which is a full quality assurance assessment.

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

Important class II products cannot use self-assessment under any circumstances. A third-party conformity assessment is always required, either through **Module B and C, Module H**, or a **European cybersecurity certification scheme** at assurance level of at least "substantial." Manufacturers can still apply the relevant harmonised standards for their product type, which supports conformity with the regulation.

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 can align to the horizontal harmonised standards and the vertical harmonised standard for its product type but must also complete a third-party conformity assessment by a notified body following either **Module B and C or Module H**. Manufacturers of critical class products can also choose to complete a **European cybersecurity certification scheme** at assurance level of at least "substantial" to demonstrate compliance.

During the planning stage, 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.

1.4 // Harmonised Standards

The EU Commission issued a standardisation request to CEN, Cenelec and ETSI to develop 15 horizontal and 26 vertical harmonised standards for the CRA. The horizontal standards translate the essential cybersecurity requirements from Annex I of the CRA in specifications all manufacturers can apply

to their products. For products in the default category these are the only harmonised standards that can be applied.

For the vertical standards there is a standard for each product type in important class I, class II and critical category. The vertical standard for the product type and the horizontal standards must be applied for presumption of conformity to apply for important class I and II products.

The harmonised standards release is phased; the key dates are:

- Horizontal standard entry 1 (framework for security by design) & entry 15 (standard on vulnerability handling) – 30th August 2026
- All vertical standards entries (16-41) – 30th October 2026
- Remaining horizontal standards (entries 2-14) – 30th October 2027

Design

Product Design

Stage 2

In the planning phase the manufacturer established that their product is in scope for the CRA and what product category it falls into. The product design phase is where the manufacturer will outline the products purpose, features and architecture. Alongside that, the manufacturer must calculate the cybersecurity risk and incorporate cybersecurity principles into the design process.

2.1 //

Risk Assessment

A cybersecurity risk assessment is a mandatory requirement as defined in article 13(2) of the CRA. Manufacturers must identify all potential risks, and the associated threats and vulnerabilities that an end user of the product can be exposed to. This will inform the product's risk profile and determine what security controls are proportionate to address the associated risks. The risk assessment is a living document that should be updated over the product lifetime.

Product Context

Manufacturers must first understand the product's purpose and function, as well as the environment it is intended to operate in before they can assess the risks associated with the product. This is referred to as **product context** in the draft of prEN 40000-1-2, the first horizontal CRA harmonised standard. The product context consists of:

1. The intended purpose and reasonably foreseeable use of the product
2. The functions of the product
3. The environment the product is intended to be used in
4. The product architecture
5. The intended user of the product

The product context should include free and open-source software, third-party components the manufacturer intends to integrate into the product and remote data processing solutions.

Intended Purpose and Foreseeable Use/Misuse

As part of product context, the manufacturer must define how their product is meant to be used and the ways it might foreseeably be used in practice by users. Article 13(3) of the CRA requires the cybersecurity risk assessment to take these into account, and the CRA defines three distinct terms for them:

- **Intended Purpose:** the use for which the product is intended by the manufacturer, including the specific context and conditions of use, as specified in the instructions for use, promotional and sales materials, and technical documentation.
- **Reasonably Foreseeable Use:** use that is not necessarily what the manufacturer intends but is likely to result from reasonably foreseeable human behaviour, technical operations, or interactions.
- **Reasonably Foreseeable Misuse:** use that is not in accordance with the intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems.

Where reasonably foreseeable misuse may lead to significant cybersecurity risks, the manufacturer must communicate those risks to users in the information and instructions accompanying the product.

Risk Identification

Once the product context has 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.

2.2 // Security Design Principles

With the product context understood and the risks assessed, the manufacturer turns to the design decisions themselves. prEN 40000-1-2 sets out four cybersecurity principles that should be included in the product design decisions.

1. Risk-based Approach

The CRA requires cybersecurity measures to be proportionate to the risks identified in the risk assessment. This principle is what connects the risk assessment to the design, every security decision should correspond to a risk identified in the risk assessment.

2. Security By Design

Security by design treats security as a fundamental design input rather than a feature added at the end. The CRA expects this shift in mindset because retrofitting security into a finished product is more expensive and less effective than building it into the product design. Each security control in the product should trace back to a specific risk and a defined security objective from the risk assessment.

One method that could be used to implement security by design is threat modelling. 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.

3. Secure By Default

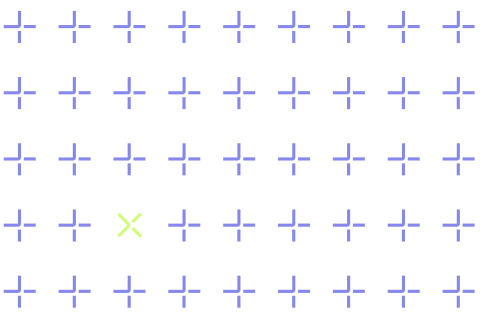
The CRA requires products to be delivered in their most secure configuration, removing the need for the end user to enable these features. In practice this means default-on protections, automatic security updates with a clear and easy opt-out, and the ability for users to reset the product to its original secure state. Designing for secure-by-default reduces the risk of misconfiguration by end users. Examples of secure by default configurations include; shipping the product with strong, unique credentials, enabling encryption by default and automatic updates or disabling unnecessary services or ports in the default state.

4. Transparency

Users need accurate information about the cybersecurity properties of the products they buy and use, and the CRA places specific obligations on manufacturers to provide user documentation. At the design phase this means planning for what needs to be documented and communicated. For example, default settings, configurable security options, company contact information, and the information needed to operate the product securely.

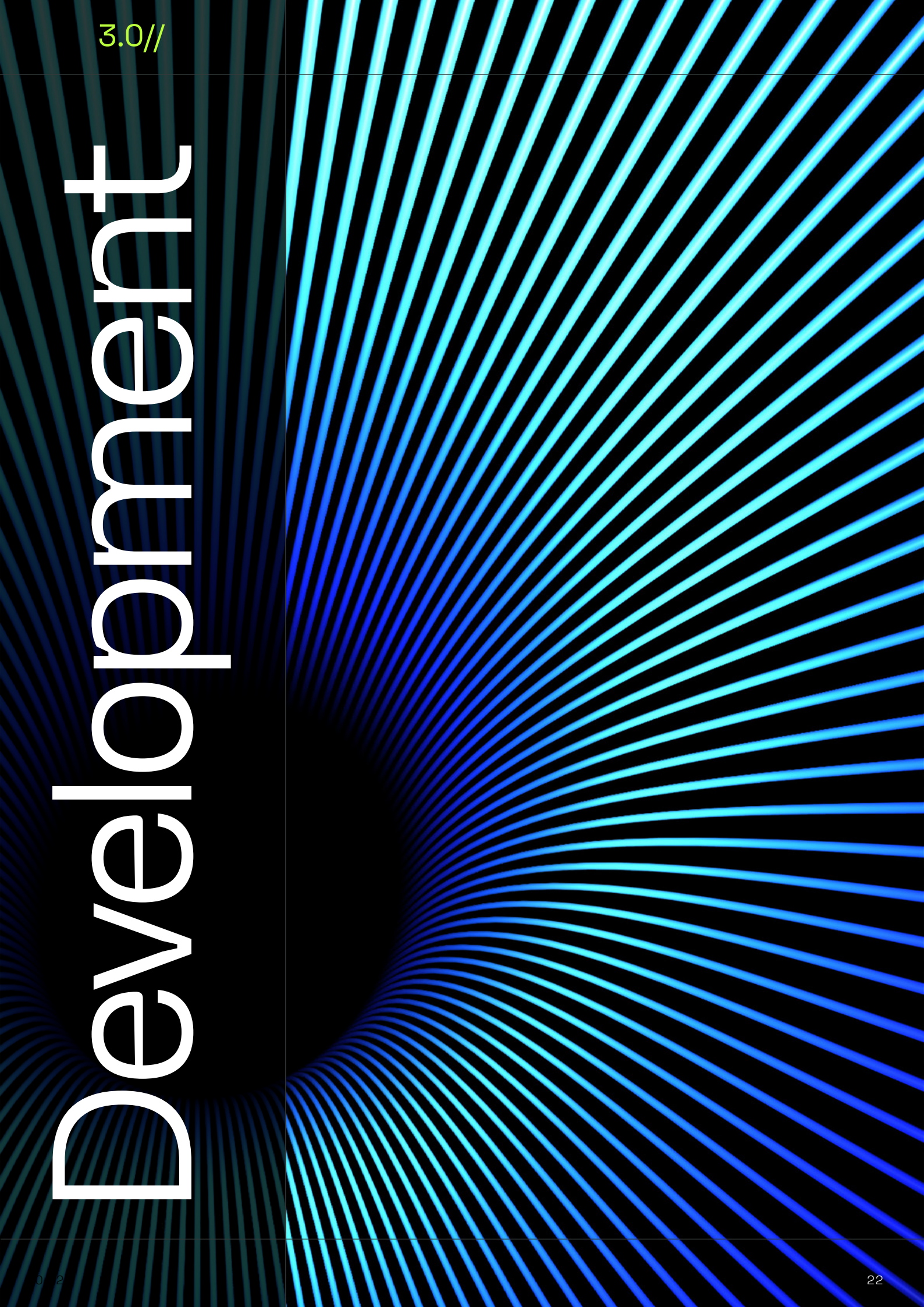
5. Minimisation

The manufacturer should only expose the functionality, ports, services, accounts and data flows that are needed to deliver the products intended purpose. Anything beyond that could be used as an attack surface by a threat actor. Removing unnecessary access during design is cheaper and more reliable than mitigating it later.



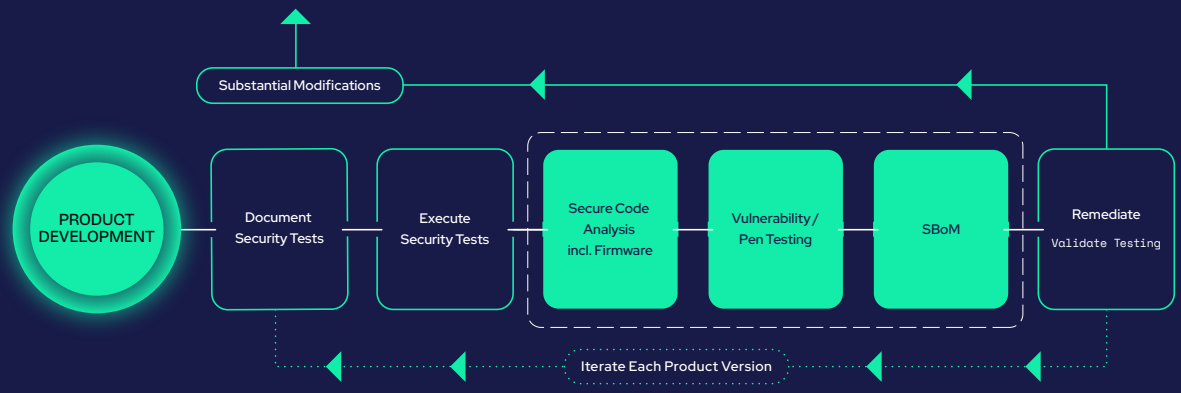
3.0//

Development



Product Development

Stage 3



3.1 // Security Testing and Validation

Throughout the product development lifecycle, it is essential to conduct various tests on the product to ensure 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 and the test outcome should be thoroughly documented.

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.
- Firmware Security Analysis
  This process involves extracting and analysing the firmware running on a hardware product to identify security weaknesses such as hard-coded credentials, weak cryptography, insecure update mechanisms or known vulnerable third-party components. 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 the identified vulnerabilities have been remediated, re-testing should be performed both to confirm that the fixes have fully addressed the vulnerabilities and to confirm that the fixes have not introduced new vulnerabilities or weakened controls.

Security testing should not be a one-time activity but rather an ongoing process that continues throughout the product lifecycle. Manufacturers must 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 throughout the product support period.

Software Bill of Materials (SBOM)

Manufacturers must create a software bill of materials (SBOM), an inventory of the software components contained in a product, including the software version and any third-party or open-source dependencies. This allows vulnerabilities in any component to be identified quickly when a vulnerability is disclosed. While the SBOM does not have to be supplied to users by default, it must be made available to market surveillance authorities upon request.

3.3 // 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. A substantial modification is defined as a change to the product with digital elements after it has been placed on the market that:

- Affects the product's compliance with the essential cybersecurity requirements,
- Results in a modification to the intended purpose for which the product has been assessed.

When a product is substantially modified it is considered a new product by the CRA and so making a substantially modified product available on the market constitutes a new placing on the market. If a company that was not the original manufacturer of a product, substantially modifies a product and places it on the market the secondary company is considered the manufacturer of the new product, not the original product's manufacturer. The CRA specifically calls out that most security updates and repairs using spare parts that are identical to the parts already present in the product do not count as substantial modifications.

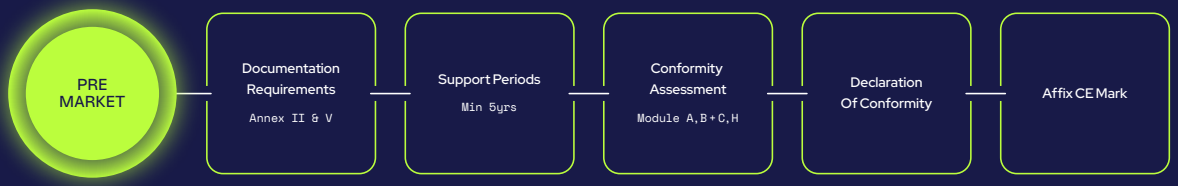
Where a modification qualifies as substantial, the manufacturer treats the modified product as a new placing on the market. In practice this means updating the technical documentation for the aspects affected by the modification; carrying out a fresh conformity assessment proportionate to the change, signing a new EU declaration of conformity and declaring a new support period of at least five years from that point. The original support period for the unmodified version continues to run for users that do not take up the modified version.

4.0//

Pre-Market

Pre-Market

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 create technical documentation and documentation to be shared with users. Technical documentation is held by the manufacturer for inspection by market surveillance authorities. User documentation is supplied with the product when it is placed on the market and informs the buyer. The user documentation also forms part of the technical documentation pack.

Technical Documentation

The manufacturer keeps this on file for market surveillance authorities. It must include:

- A general description of the product: intended purpose, software versions, hardware photos or illustrations, and the user-facing information.
- A description of the design, development and production process, and of the vulnerability handling processes.
- Cybersecurity risk assessment.
- The information used to determine the product's support period.
- A list of the harmonised standards, common specifications, or European cybersecurity certification schemes applied (in full or in part).
- Reports of the tests carried out to verify conformity with the essential requirements.
- A copy of the EU declaration of conformity.

User Documentation

This accompanies the product when it is placed on the market. It must include:

- The manufacturer's name, registered trade name or trademark, and contact details.
- A single point of contact for reporting vulnerabilities, and where to find the manufacturer's coordinated vulnerability disclosure policy.

- The product name, type, and any information needed to identify it uniquely.
- The intended purpose of the product, the security environment provided by the manufacturer, and the product's essential functionalities and security properties.
- Any known or foreseeable circumstances, under intended use or reasonably foreseeable misuse, that may lead to significant cybersecurity risks.
- The EU declaration of conformity or the internet address where it can be accessed.
- The type of technical security support offered and the end-date of the support period.
- Instructions for security features, updates and how to decommission 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. The full documentation requirements can be found in Annex II and Annex VII of the CRA.

The manufacturer is responsible for maintaining the product documentation throughout the support period of the product. Documentation must also be kept at the disposal of the market surveillance authorities for 10 years after the product has been placed on the market or for the support period whichever is longer.

4.2 // Conformity Assessment

Once all necessary documents are in place and the manufacturer has ensured conformity with CRA requirements, they can proceed with the appropriate conformity assessment for their product category. After completing the conformity assessment, manufacturers must sign the EU declaration of conformity, after which the CE marking can be affixed to the product.

CE Marking

The CE marking is the manufacturer's visible declaration that a product complies with all applicable EU harmonisation legislation, including the CRA's essential cybersecurity requirements. The CRA requires CE marking to be affixed visibly, legibly and indelibly to the product before it is placed on the market. For hardware, the CE marking is affixed on the product itself, or if that is not feasible, on the packaging and the EU declaration of conformity. For software products, the CE marking is affixed either on the EU declaration of conformity or on the website accompanying the software. The CE marking can only be applied once the manufacturer has completed the relevant conformity assessment procedure and signed the EU declaration of conformity.

EU Declaration of Conformity

Once conformity assessment procedures are complete, the manufacturer must draw up an EU Declaration of Conformity which states that the fulfilment of the essential cybersecurity requirements of the CRA have been demonstrated. This is a formal written statement following the structure set out in Annex V of the CRA that attests the product meets the essential requirements of the CRA, and the manufacturer assumes responsibility for the product's compliance with the regulation.

If the product is subject to more than one Union legal act that requires a Declaration of Conformity, a single declaration will be drawn up for all Union legal acts.

4.3 // Support Period

The support period is the length of time during which the manufacturer is required to fulfil the vulnerability handling obligations of the CRA. **The minimum support period is five years**; it may be shorter only where the product is genuinely expected to be in use for less than five years. The manufacturer determines the support period so that it reflects the length of time the product is expected to be in use. Determining the support period should take into account reasonable user expectations, the nature of the product, and any relevant Union law determining the lifetime of the product. The information used to determine the support period must be recorded in the technical documentation, and the end-date of the support period must be communicated to users in the documentation accompanying the product. Security updates issued during the support period must remain available **for at least 10 years** after issue or for the remainder of the support period, whichever is longer.

Market

On The Market

Stage 5

5.1 //

Ongoing Security Commitments During the Support Period

Throughout the support period of the product, manufacturers must provide free and 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 & Incident 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.

Severe Incident Reporting

Manufacturers must also report severe incidents that have an impact on the security of their products. The 24-hour early warning and the 72-hour notification follow the same pattern as vulnerability reporting. The final report, however, is due within one month of the 72-hour notification rather than 14 days from the availability of a corrective measure.

Becoming Aware

When a manufacturer detects a suspicious event or when an external party (a customer, a researcher, a CSIRT, a media report) brings one to its attention, the manufacturer must immediately assess whether it is in fact an actively exploited vulnerability or a severe cybersecurity incident impacting the product. Following Commission Guidance (paragraphs 195–196), the manufacturer is regarded as having "become aware" once that initial assessment gives them a reasonable degree of certainty that a vulnerability in their product is being actively exploited, or a severe incident has occurred and has compromised the security of the product. They will at this point have 24 hours to report the early warning notification to their designated CSIRT and ENISA.

5.3 // Vulnerability Disclosure

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

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

Once the vulnerability has been fixed and security update made available the manufacturer is required to publicly disclose the fixed vulnerability including a description, the products affected, the impact and severity, and clear remediation information for users.

5.4 // Coordinated Vulnerability Disclosure Policy (CVD)

Manufacturers are required to put in place a coordinated vulnerability disclosure policy (CVD). A CVD policy sets out a structured process for external individuals or entities to report vulnerabilities directly to the manufacturer or indirectly through a CSIRT designated as coordinator under the NIS2 Directive, so the manufacturer can diagnose and remedy the vulnerability before details are made public. Manufacturers may supplement their CVD policy with mechanisms such as bug bounty programmes to incentivise the reporting of vulnerabilities.

5.5 // Consequences of Non-Compliance

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

Administrative Fines

- **Up to €15 million or 2.5% of total worldwide annual turnover for the preceding financial year (whichever is higher)**—for non-compliance with the essential cybersecurity requirements in Annex I or with the manufacturer obligations in Articles 13 and 14, including vulnerability and incident reporting.
- **Up to €10 million or 2% of total worldwide annual turnover for the preceding financial year (whichever is higher)**—for non-compliance with other specified obligations of the CRA.
- **Up to €5 million or 1% of total worldwide annual turnover for the preceding financial year (whichever is higher)**—for supplying incorrect, incomplete or misleading information to notified bodies or market surveillance authorities.

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

5.6// Special Consideration for SMEs

The CRA includes a number of provisions designed to ease the burden on microenterprises and small and medium-sized enterprises (SMEs).

- **Penalty considerations** - when deciding on the amount of an administrative fine, market surveillance authorities must take the size of the enterprise into account. In addition, administrative fines do not apply to microenterprises or small enterprises for any failure to meet the 24-hour deadline for early warning notification of actively exploited vulnerabilities or severe incidents. Member States should also not impose other kinds of penalties of a pecuniary character on those entities for the same infringements.
- **Reduced conformity assessment fees** – the CRA outlines requirements that fees for conformity assessment procedures be reduced proportionately for SMEs. Notified bodies are also required, to operate on terms that take account of SME interests when setting their fees and conducting assessments.
- **Member State support measures** – where appropriate, Member States must organise SME-targeted awareness-raising and training, establish a dedicated communication channel for SMEs to receive advice on the CRA, and support SME testing and conformity assessment activities.
- **Regulatory sandboxes** - Member States can establish cyber resilience regulatory sandboxes, providing controlled testing environments where SMEs can develop, validate and test innovative products against the CRA before placing them on the market.

AN EU CO-FUNDED PROJECT

CRA-AI

// Your starting point for the Cyber Resilience Act.

CRA-AI is the EU co-funded project making CRA compliance achievable for the manufacturers that need it most. Backed by a €2.87M grant from the European Commission under the Digital Europe Programme and delivered by a consortium of CRA experts led by Cyber Cert Labs.

The CRA-AI projects main aim is to build Attestra an AI native product security and compliance CRA platform to support manufacturers who need to conform with the Cyber Resilience Act. It also provides free tools, expert guidance and training through the Attestra Academy to help digital product manufacturers understand their obligations and act on them.

Where to Start

Two free assessments answer the first two questions every manufacturer asks.

// Am I in scope?

FREE

CRA Scope Assessment.

A 5-minute self-assessment that tells you whether your product falls inside the scope of the CRA and which product category it belongs to.

Take Assessment

// How ready am I?

FREE

CRA Readiness Assessment.

A 30-minute guided assessment that scores your product security against the CRA essential requirements and gives you a tailored report with actionable recommendations.

Start Now

CRA - AI
CYBER RESILIENCE ACT
ARTIFICIAL INTELLIGENCE

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Follow the CRA-AI project on LinkedIn for webinars, events, case studies and early adopter updates. Click Here.

Co-funded by the European Union. Grant Agreement No. 101190243. The views and opinions expressed are those of the author(s) and do not necessarily reflect the views of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

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 free 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.

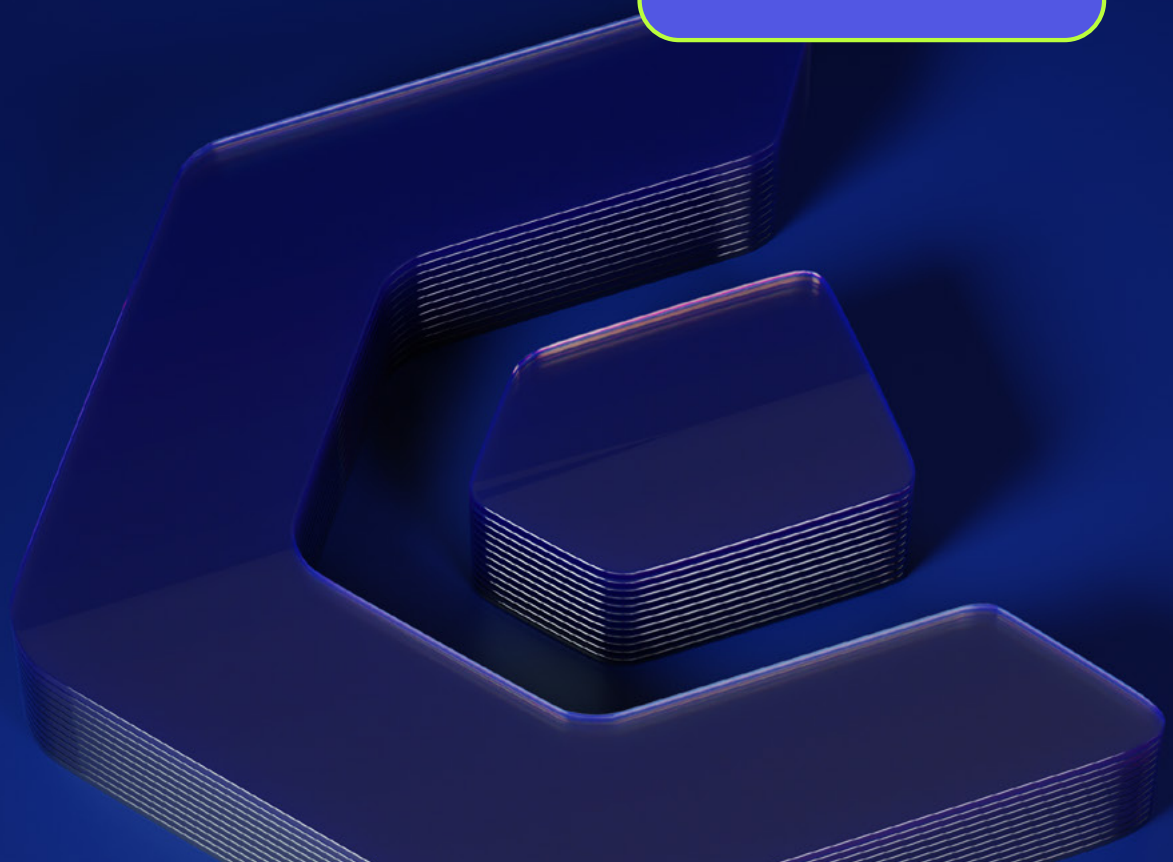
Ready to act?

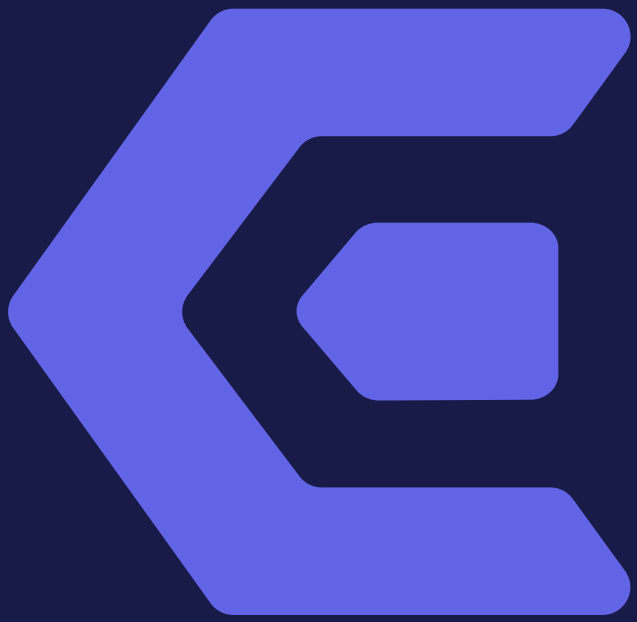
Fill in a Free Readiness Assessment.

Start Now

Need more guidance?
Speak with one of our experts.

contact@cybercertlabs.com





cybercertlabs.com