



Cyber Resilience Act (CRA) Compliance and Awareness

Sphynx Cyber Range Material

Platform Overview

The [Sphynx Cyber Range Platform](#) is an advanced training platform designed to support organisations in addressing modern cybersecurity and privacy challenges. It provides customizable, scenario-based exercises tailored to the specific assets, threat landscape, and risk profile of each organisation. Through realistic and interactive environments, the platform enables users to develop practical skills, strengthen decision-making capabilities, and enhance their readiness to effectively prevent, detect, and respond to cybersecurity incidents in line with evolving regulatory requirements such as the Cyber Resilience Act (CRA).

Programme Introduction

Title

Cyber Resilience Act (CRA) Compliance and Awareness

Overview

This online programme provides practical awareness and understanding of the EU Cyber Resilience Act (CRA). It is designed to help users, including SMEs and digital product stakeholders, understand whether their products fall within the scope of the CRA and how to meet its cybersecurity requirements. Parts of this programme's material are made available for public access through the CURIUM Portal.

What You Will Learn

By completing this programme, you will be able to:

- Determine whether a product falls within the scope of the CRA
- Understand key cybersecurity obligations under the CRA

- Apply vulnerability handling and incident reporting practices
- Recognize lifecycle responsibilities and compliance requirements
- Support secure-by-design and secure-by-default implementation

Programme Structure

This programme consists of one interactive scenario combining training and assessment:

- **A set of training questions**
- **A set of scored assessment questions**
- **Maximum Score:** 100 points
- **Difficulty Level:** Intermediate
- **Assessment Duration:** 75 minutes

Scenario Introduction

Title

CRA Scope, Obligations, and Compliance

Overview

In this scenario, you will work through a series of realistic situations related to the EU Cyber Resilience Act (CRA). You will assess whether products fall within scope, identify applicable obligations, and make decisions related to vulnerability management, incident reporting, and compliance.

Target Audience

- SMEs developing or distributing digital products
- Software developers and system designers
- Cybersecurity and compliance professionals
- Technical trainers and instructors

Developed Skills

- Cybersecurity Fundamentals

- Vulnerability Assessment and Management
- Incident Response
- Security Policies and Standards
- Software Development
- Systems Analysis
- Training, Education, and Awareness

Bibliography

- EU Cyber Resilience Act (CRA) Official - <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>
- European Commission CRA Implementation - <https://digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation>

Training and Assessment Approach

Participants will complete training questions followed by a structured assessment designed to evaluate their understanding of CRA scope, obligations, and practical application. The assessment includes scenario-based questions that simulate real-world decision-making related to vulnerability management, incident reporting, and compliance. A representative subset of questions is presented within this material, while the complete question bank is maintained internally.

Sample Training Questions

Section 1: CRA Fundamentals

TQ-1.1 (Single Choice)

What does CRA stand for?

- A. Cyber Resilience Authorization
- B. Cyber Resilience Act
- C. Cybersecurity Requirements Assessment
- D. Critical Risk Administration

Correct Answer: B

TQ-1.2 (Multiple Choice)

**Which of the following are considered “products with digital elements” under the CRA?
(There are 2 correct answers)**

- A. Standalone web applications not placed on the market
- B. Smartphones and laptops
- C. Smart home devices (e.g., cameras, locks)
- D. Marketing websites with no dynamic functionality
- E. Cloud storage services (SaaS)

Correct Answer: B, C

Section 2: Products Classification and Scope

TQ-2.1 (Multiple Choice)

Which of the following are CRA scope exclusions? (There are 3 correct answers)

- A. Free and open-source software (FOSS) that is not monetized
- B. All mobile applications
- C. In-vitro diagnostic medical devices
- D. Spare parts manufactured to identical specifications
- E. All software as a service (SaaS) offerings

Correct Answer: A, C, D

Section 3: Essential Cybersecurity Requirements

TQ-3.1 (Interactive Bucket - Drag and Drop)

Classify each security requirement by its correct implementation phase:

Items to classify:

- Products shall be made available without known exploitable vulnerabilities
- Protect the confidentiality of stored, transmitted data
- Minimize attack surfaces

- Ensure data minimization
- Share vulnerability information as part of coordinated vulnerability disclosure
- Apply effective and regular security testing and reviews

Correct Categorization:

- **Design Phase (Architecture and pre-market security foundations):**
 - Protect the confidentiality of stored and transmitted data
 - Minimize attack surfaces
 - Ensure data minimization
- **Operations Phase (Post-market monitoring, updates, and disclosure):**
 - Products shall be made available without known exploitable vulnerabilities
 - Share vulnerability information as part of coordinated vulnerability disclosure
 - Apply effective and regular security testing and reviews

Section 4: Economic Operators and Obligations

TQ-4.1 (Single Choice)

Which of the following is NOT considered an economic operator under the CRA?

- A. Manufacturer
- B. Importer
- C. End consumer purchasing for personal use
- D. Distributor

Correct Answer: C

TQ-4.2 (Multiple Choice)

Which obligations apply to manufacturers under the CRA? (There are 5 correct answers)

- A. Conduct cybersecurity risk assessment throughout product lifecycle
- B. Draw up technical documentation before market placement
- C. Define and maintain support period (minimum 5 years)

- D. Perform all distribution activities directly
- E. Provide security updates for the defined support period
- F. Report actively exploited vulnerabilities to CSIRT

Correct Answer: A, B, C, E, F

Section 5: Conformity Assessment

TQ-5.1 (Single Choice)

Which conformity assessment procedure is used for default category products (non-critical)?

- A. Internal Control (Module A) - Self-Assessment
- B. EU-Type Examination (Module B)
- C. Full Quality Assurance (Module H)
- D. Third-party certification mandatory

Correct Answer: A

TQ-5.2 (Interactive Bucket - Drag and Drop)

Classify each product type by the correct category:

Items to classify:

- Operating system (Important - Class I)
- Generic IoT sensor (Default category)
- Smart meter gateway (Critical)
- Custom authentication software (Important - Class I)
- Basic temperature sensor (Default category)
- Hardware security module (Critical)

Correct Categorization:

- **Self-Assessment Required:**
 - Generic IoT sensor (Default category)
 - Basic temperature sensor (Default category)

- **Third-Party Assessment:**
 - Operating system (Important - Class I)
 - Smart meter gateway (Critical)
 - Custom authentication software (Important - Class I)
 - Hardware security module (Critical)

Section 6: Technical Documentation

TQ-6.1 (Single Choice)

When must technical documentation be prepared according to the CRA?

- A. After the product is placed on the market
- B. Only if third-party assessment is required
- C. Before the product is placed on the market and continuously updated during support period
- D. Documentation is optional for default category products

Correct Answer: C

TQ-6.2 (Multiple Choice)

Which of the following must be included in technical documentation per Article 31? (There are 4 correct answers)

- A. General description of the product including intended purpose
- B. Complete source code of the product
- C. Description of design, development, and production processes
- D. Cybersecurity risk assessment
- E. SBOM (Software Bill of Materials)
- F. Warranty terms and prices

Correct Answer: A, C, D, E

Section 7: Vulnerability Handling

TQ-7.1 (Single Choice)

Under the CRA, as a manufacturer, what is the mandatory timeline to report in detail a severe incident once aware of it?

- A. 24 hours
- B. 48 hours
- C. 72 hours
- D. 7 days

Correct Answer: C

Section 8: Product Lifecycle

TQ-8.1 (Single Choice)

What is the minimum support period a manufacturer must define for a product, unless its expected lifetime is shorter?

- A. 2 years
- B. 3 years
- C. 5 years
- D. 10 years

Correct Answer: C

TQ-8.2 (Interactive Bucket - Drag and Drop)

Classify each obligation by the correct category, as either Pre-Market or Post-Market:

Items to classify:

- Conduct cybersecurity risk assessment
- Define support period
- Ensure secure by default configuration
- Make security updates available
- Notify CSIRT of actively exploited vulnerabilities

- Maintain technical documentation
- Receive and respond to vulnerability reports
- Plan product decommissioning and data removal
- Provide user guidance on secure use

Correct Categorization:

- **Pre-Market Obligations:**
 - Conduct cybersecurity risk assessment
 - Define support period
 - Ensure secure by default configuration
 - Maintain technical documentation
- **Post-Market Obligations:**
 - Make security updates available
 - Notify CSIRT of actively exploited vulnerabilities
 - Receive and respond to vulnerability reports
 - Plan product decommissioning and data removal
 - Provide user guidance on secure use

Section 9: Supply Chain and Third-Party Components

TQ-9.1 (Single Choice)

Manufacturers are responsible for ensuring that:

- A. Only third-party components they directly developed
- B. Only open-source software components are secure
- C. Third-party components, including free and open-source software, do not compromise cybersecurity
- D. All vulnerabilities in third-party components are reported by component providers

Correct Answer: C

TQ-9.2 (Single Choice)

Which statement best reflects the CRA's approach to open-source software?

- A. Open-source software stewards are treated as manufacturers
- B. CRA obligations apply when open-source software is used in commercial products placed on the market
- C. Open-source software is excluded from the CRA entirely
- D. Open-source communities must provide security updates under the CRA

Correct Answer: B

Section 10: Regulatory Compliance and Market Surveillance

TQ-10.1 (Single Choice)

Which authority is responsible for ensuring effective implementation of the CRA in EU Member States?

- A. Each Member State's designated market surveillance authority
- B. European Commission only
- C. ENISA only
- D. Manufacturers' associations

Correct Answer: A

Sample Assessment Questions

Section 1: CRA Fundamentals

AQ-1.1 (Single Choice, 5 points)

Which of the following best defines a "product with digital elements" according to the Cyber Resilience Act?

- A. Software or hardware product that has or is able to have a data or network connection (5 points)
- B. Only hardware devices manufactured in the EU (0 points)
- C. Products that exclusively process personal data (0 points)

Correct Answer: A

Section 2: Products Classification and Scope

AQ-2.1 (Single Choice, 6 points)

A manufacturer produces both a standalone firewall software and a network management system that includes firewall capabilities as one feature. How are these classified?

- A. Both classified as Important (Class II) (0 points)
- B. Firewall = Important (Class II), Network system = Default if firewall is not a core functionality (6 points)
- C. Both classified as Default (0 points)
- D. The inclusion of firewall automatically makes both Critical (0 points)

Correct Answer: B

Section 3: Essential Cybersecurity Requirements

AQ-3.1 (Multiple Choice, 8 points)

According to Part II of Annex I, which of the following are manufacturer obligations regarding vulnerability handling?

- A. Identify and document vulnerabilities and create an SBOM (2 points)
- B. Address vulnerabilities without delay with security updates (2 points)
- C. Apply effective and regular security testing and reviews (2 points)
- D. Maintain vulnerabilities in secret indefinitely (-1 point)
- E. Share and publicly disclose vulnerability information (2 points)
- F. Use only external security companies for all testing (-1 point)

Correct Answers: A, B, C, E

Section 4: Economic Operators and Obligations

AQ-4.1 (Single Choice, 4 points)

An importer discovers that a product they are about to distribute does not have proper CE marking. What is their obligation under the CRA?

- A. Proceed with distribution and notify the manufacturer after market placement (0 points)
- B. Refrain from placing the product on the market until proper conformity is demonstrated (4 points)
- C. Add their own marking to the product (0 points)
- D. Notify market surveillance authorities only after issues are reported (0 points)

Correct Answer: B

Section 5: Conformity Assessment

AQ-5.1 (Single Choice, 5 points)

A critical product manufacturer has undergone EU-Type Examination by a notified body. What must they do next before placing products on the market?

- A. Immediately begin production without additional steps (0 points)
- B. Implement production control measures (Module C) and affix CE marking (5 points)
- C. Only maintain the EU-type certificate (0 points)
- D. Conduct additional self-assessments for each product (0 points)

Correct Answer: B

Section 6: Technical Documentation

AQ-6.1 (Multiple Choice, 8 points)

A manufacturer must include an SBOM (Software Bill of Materials) in their technical documentation. Which of the following are correct requirements for the SBOM?

- A. Must be in a commonly used and machine-readable format (2 points)
- B. Must cover at least the top-level dependencies of the product (2 points)
- C. Must include all transitive dependencies regardless of depth (-1 point)
- D. Should support identification of known vulnerabilities in components (2 points)
- E. Must be provided to market surveillance authorities if requested (2 points)

Correct Answers: A, B, D, E

Section 7: Vulnerability Handling

AQ-7.1 (Single Choice, 6 points)

A manufacturer discovers a vulnerability in their product that is actively exploited by attackers. What is the correct sequence of actions?

- A. Develop fix, Test, Notify users, Report to CSIRT (0 points)
- B. Report to CSIRT (within 24h), Develop fix, Test, Notify users, Final report (6 points)
- C. Notify users, Develop fix, Report to CSIRT (0 points)
- D. Keep vulnerability secret until fully patched (0 points)

Correct Answer: B

Section 8: Product Lifecycle

AQ-8.1 (Multiple Choice, 8 points)

Which obligations apply to manufacturers regarding the product lifecycle?

- A. Define support period with clear criteria for determination (2 points)
- B. Maintain technical documentation throughout support period (2 points)
- C. Provide free security updates (addressing identified security issues) (2 points)
- D. Charge premium prices for critical security updates (-1 point)
- E. Clearly communicate end of support period to users (2 points)

Correct Answers: A, B, C, E

Section 9: Supply Chain and Third-Party Components

AQ-9.1 (Single Choice, 6 points)

A manufacturer discovers a vulnerability in an open-source library they have integrated into their product. What is their primary responsibility?

- A. Do nothing as it is the open-source project's responsibility (0 points)
- B. Develop and validate a patch/workaround and provide it to users as a security update, while following CRA reporting obligations (6 points)
- C. Remove the library immediately from the product (0 points)

- D. Inform the open-source project and wait for their fix (0 points)

Correct Answer: B

Section 10: Regulatory Compliance and Market Surveillance

AQ-10.1 (Single Choice, 5 points)

What must a manufacturer do immediately upon discovering their product contains a non-compliant component or process?

- A. Continue selling until stock is exhausted (0 points)
- B. Take corrective measures, including withdrawal or recall if necessary (5 points)
- C. Notify only the component supplier (0 points)
- D. Wait for market surveillance authority to discover the issue (0 points)

Correct Answer: B



Cyber Range Training Material © 2026 by SPHYNX is licensed under CC BY-NC-SA 4.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by-nc-sa/4.0/>