Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

Regulation (EU) 2024/2847

How Organizations Should Prepare for the Cyber Resilience Act

December 2025

Digital Innovation Hub
Trakia

Introduction

Sashka Boncheva

Cybersecurity Expert at EDIH Trakia, Bulgaria

Trainer and Consultant

ISO/IEC 27001 Lead Auditor

General Manager – Elegant Systems Ltd.

Women4Cyber Bulgaria, Co-founder

s.boncheva@dihtrakia.org

How Organizations Should Prepare for the Cyber Resilience Act

Gap Analysis & Internal Policies

CRA: What It Really Requires

Cyber Risk Assessment as Part of Technical Documentation

- Strong cybersecurity requirements for the product (Annex I Part I)
- Strong cybersecurity processes inside the organization (Annex I Part II)
- Risk assessment & vulnerability handling (Article 13)
- Reporting obligations for exploited vulnerabilities & incidents (Article 14)
- Evidence, documentation & CE marking readiness (Articles 31–44)

Why You Need a CRA Gap Analysis

A CRA gap analysis helps you understand:

- What CRA actually requires
- Where your current controls fall short
- What processes are missing
- What documentation is not yet available
- What must be fixed before CE marking is possible

What Your CRA Gap Analysis Must Cover?

1. Product cybersecurity requirements

— Secure-by-default, no known exploitable vulnerabilities, data protection (Annex I Part I)

2. Organizational process requirements

— Secure development, updates, testing, logging, vulnerability handling (Annex I Part II)

3. Article 13 readiness

— Cybersecurity risk assessment
— Support period
— Vulnerability handling capabilities

4. Article 14 readiness

— Ability to report exploited vulnerabilities and incidents within deadlines

5. Documentation & CE marking readiness

— Technical file (Annex VII)
— Evidence of security controls

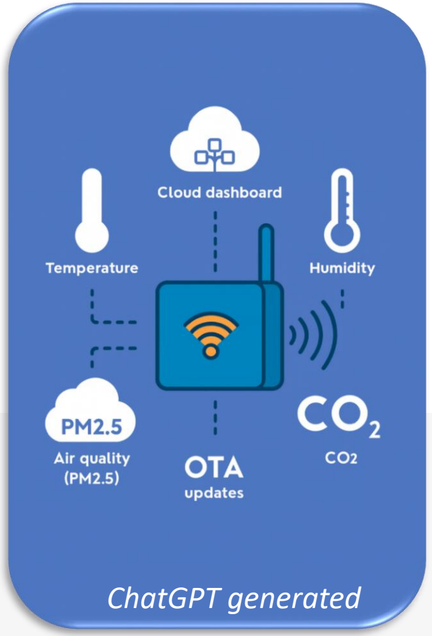
Product Context: IoT Environmental Sensor

Example Product:

An IoT environmental sensor measuring temperature, humidity, air quality (PM2.5), and CO_2 levels. Data is sent to a cloud dashboard. Device supports OTA updates.

Includes:

- Embedded firmware
- Wireless connectivity
- Mobile or web app
- Backend API
- OTA update mechanism
- Cloud platform for monitoring



CRA relevance:

IoT devices fall directly under the CRA because they contain:

- *digital elements*
- *connectivity*
- *software components (firmware + cloud)*
- *security-sensitive data*

CRA GAP Analysis — IoT Environmental Sensor

PRODUCT REQUIREMENTS (Annex I Part I)

CRA Reference	Requirement	Current State	GAP	Impact	Priority
Annex I Part I(2)(a)	No known exploitable vulnerabilities	No automated vulnerability scanning	Missing automated firmware scanning & CVE tracking	High likelihood of unnoticed vulnerabilities	**High**
Annex I Part I(2)(b)	Secure-by-default	Device ships with default admin password	Not secure-by-default; no forced password change	Device takeover possible	**Critical**
Annex I Part I(2)(c)	Minimize attack surface	Open debug port (UART) left active	Insecure design	Physical & remote attacks easier	**High**
Annex I Part I(3)	Protect data	Weak encryption (AES-128 without key rotation)	No key lifecycle	Data confidentiality risk	**Medium–High**

CRA GAP Analysis — IoT Environmental Sensor

PROCESS REQUIREMENTS (Annex I Part II)

CRA Reference	Requirement	Current State	GAP	Impact	Priority
Annex I Part II(1)	Secure Development Lifecycle (SDL)	Developers follow informal coding practices	No SDL policy, no threat modeling	Quality & security inconsistent	**High**
Annex I Part II(1)(b)	SBOM	Dependencies known internally but not exported	No automated SBOM for firmware or cloud	Cannot track component vulnerabilities	**High**
Annex I Part II(5)	Coordinated Vulnerability Disclosure (CVD)	No security.txt file; no reporting mechanism	No CVD policy	Cannot intake external reports	**Critical**
Annex I Part II(7)	Logging & monitoring	Minimal device logs; no tamper detection	Insufficient monitoring capability	Hard to detect exploitation	**Medium**
Annex I Part II(8)	Secure updates	OTA updates not signed	Insecure update channel	Firmware injection possible	**Critical**

CRA GAP Analysis — IoT Environmental Sensor

ARTICLE 13 — RISK ASSESSMENT & VULNERABILITY HANDLING

Requirement	Current State	GAP	Priority
Cybersecurity risk assessment	Not performed	No documented method	**High**
Support period (≥5 years recommended)	Unspecified	Missing a formal decision	**Medium**
Vulnerability handling process	Handled informally via email	Missing triage, SLA, documentation	**Critical**

CRA GAP Analysis — IoT Environmental Sensor

ARTICLE 14 — REPORTING OBLIGATIONS

Requirement	Current State	GAP	Priority
24-hour Early Warning to ENISA	No defined workflow	Cannot comply with CRA deadlines	**Critical**
72-hour Vulnerability Report	No template / SLA	Missing entire reporting structure	**High**
Final remediation report	Not implemented	No tracking of vulnerability lifecycle	**Medium–High**

CRA GAP Analysis — IoT Environmental Sensor

ANNEX VII — TECHNICAL DOCUMENTATION

Requirement	Current State	GAP	Priority
Risk assessment documentation	Missing	Cannot produce technical file	**High**
Architecture diagrams	Fragmented	Needs formal structure	**Medium**
SBOM	Missing machine-readable SBOM	Required for CE	**High**
Evidence (tests, updates, logs)	Minimal	Must be collected systematically	**High**

CRA-Required Internal Policies

To comply with CRA, organizations need internal policies for:

- Cybersecurity Risk Assessment (Art. 13)
- Vulnerability Handling Process (Art. 13 + Annex I Part II)
- Coordinated Vulnerability Disclosure (CVD) (Annex I Part II(5))
- Secure Development & Secure Lifecycle Management (Annex I Part II(1))
- Security Update Management (Annex I Part II(8))
- Monitoring & Logging Requirements (Annex I Part II)
- Incident Notification Procedure (Art. 14)
- Technical Documentation Management (Annex VII)

What These Policies Should Actually Contain

- **Risk Assessment Policy** – Method, scope, responsibilities, support period determination
- **Vulnerability Handling Procedure** – Identification > triage > remediation > communication > evidence
- **CVD Policy** – Public contact point, intake procedures, response timelines
- **Secure Development Policy** – Coding standards, reviews, testing, supply-chain controls
- **Update Management Policy** – Secure delivery, signing, rollback, update logs
- **Incident Notification Procedure** – Internal escalation + CRA 24/72h requirements

Typical Gaps We See in Organizations

- No secure development lifecycle (SDL)
- No formal vulnerability handling workflow
- No SBOM creation or maintenance
- No documented risk assessment per Article 13
- No public CVD channel
- No internal capability to report exploited vulnerabilities within 24 hours
- Missing technical documentation required for CE marking

Next: How to Create a CRA Compliance Roadmap — A Practical Walkthrough

THANK YOU

FOR YOUR ATTENTION

December 2025

Sashka Boncheva

m: +359 888 800 222

s.boncheva@dihtrakia.org

CYBER 4 ALL STAR

WOMEN 4CYBER EUROPEAN CYBER SECURITY ORGANISATION BULGARIA

Digital Innovation Hub Trakia