

EU Cyber Resilience Act (CRA) for Embedded Systems

1 Day

DURATION

6

MODULES

22

TOPICS

AC6403

COURSE CODE

COURSE OVERVIEW

Build cybersecurity into the design of the embedded products you ship to the EU. The Cyber Resilience Act makes security a legal condition for selling in the EU, with full application from December 2027. This course shows what that means for firmware, vulnerability handling, and the supply chain behind a product. Contribute to CRA compliance on embedded products, from reporting exploited vulnerabilities to preparing technical documentation and the EU declaration of conformity. These are practical skills for engineering, product, and compliance roles as cybersecurity requirements for CE marking take effect.

WHO THIS COURSE IS FOR

- For embedded engineers, system architects, product managers, and compliance and test engineers who need to bring products sold in the EU into line with the CRA.

PREREQUISITES

- Basic knowledge of embedded systems, including firmware, boot, and update, and of the product development lifecycle. Familiarity with open source components and basic networking is helpful.

LEARNING OBJECTIVES

What You Will Learn

- Determine whether a product is in scope and which class it falls into, and turn the essential requirements into design choices. Set up vulnerability handling for the support period and recognize when a firmware update is a substantial modification.

6 Modules, 22 Topics

01

Introduction to the Cyber Resilience Act

TOPICS

- Introduction to the CRA
- CRA in Context
- How the CRA Classifies Products
- Relation to Existing EU Laws

02

Essential Cybersecurity Requirements

TOPICS

- Manufacturer Responsibilities
- Managing Vulnerabilities and Reporting
- Conformity
- Handling Substantial Modifications

03

Compliance and Conformity Assessment

TOPICS

- CE Marking and Conformity Procedures for Digital Products
- Classification of Products (Important vs. Critical)
- Case Study: Applying Conformity Assessments to Embedded Systems

04

Lifecycle Security Management

TOPICS

- Obligations for Manufacturers
- Securing Supply Chains and Third-Party Components
- Best Practices for Risk Assessments and Due Diligence

05

Implementations for Cyber Resilience Compliance

TOPICS

- Requirements and Platforms
- Secure Boot and Key Protection
- Hardening and Updates
- Tools and Automation
- Vulnerability Handling and Evidence

06

Communication Protocols and Network Systems

TOPICS

- CRA Requirements for Communication
- Hardening IP Networks and TLS
- Wireless and Low-Power Networks

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com



info@koenig-solutions.com