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.

# The Cyber Resilience Act: Turning Regulatory Challenges into Competitive Advantages

February 2026

Co-funded by the European Union
ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE
OSCRAT
Open-Source Cyber Resilience Act Tools

# Introduction

## Dafina Stefanova

Operational Technical Security Consultant

Cyber Resilience & Compliance Specialist

Data Security & Incident Response Expert

Former SOC Analyst,

Women4Cyber Bulgaria

dafistefanova7@gmail.com

Helping organizations transform compliance into operational resilience.

Co-funded by
the European Union

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

OSCRAT
Open-Source Cyber Resilience Act Tools

WOMEN
4CYBER
BULGARIA

# Why This Matters

Digital products have no “safety laws” until now

- ❑ CE marking protects physical devices
- ❑ CRA introduces a digital safety shield
- ❑ Security becomes a legal requirement from the first line of code
- ❑ Major cyber incidents have shown that weak security affects entire markets

# What CRA Covers

Any product that connects to the internet

- Software, apps, IoT, industrial systems

Two main risk levels:

- Default: basic requirements
- Critical: products holding “keys to the kingdom” (e.g., firewalls, password managers)
- Failure in critical products can cause systemic incidents

# My Role as a Consultant

Translate legal requirements into technical actions

- ❑ Work with engineers and leadership
- ❑ Build the “security shield” step by step

# Step 1: Deep-Dive Interviews

Meet with product creators

Identify security gaps in:

- ❑ Source code protection
- ❑ Incident response
- ❑ Access control
- ➢ Goal: find “open windows” before attackers do
- ➢ Unclear ownership during incidents increases damage exponentially

# Step 2: Architecture Review

Review system diagrams and data flows

- ❑ Check encryption and secure communication
- ❑ Ensure cloud connections are protected
- ➢ Poor architecture is often the root cause of large-scale breaches
- ➢ “Postcard vs. sealed letter” analogy

# Step 3: SBOM (Software Bill of Materials)

Full list of third-party components

- ❑ Identifies vulnerable libraries
- ❑ Enables fast response when new threats appear
- ❑ Without SBOM, organizations cannot respond fast to supply chain vulnerabilities (e.g., Log4Shell)
- ➢ "Ingredient list" analogy

# Building the Evidence

Penetration testing (“friendly hackers”)

- ➢ Automatic update capability
- ➢ Mapping technical controls to legal requirements
- ➢ Every feature must have proof

# GAP Analysis

Compares CRA requirements vs. current practices

- Identifies missing controls
- Architecture summary
- Vulnerability management
- Update processes
- Source code protection
- Incident response
- Forms the foundation of the compliance plan

# Risk Assessment

What can go wrong

- Likelihood
- Impact
- Mitigation actions
- Based on interviews, documentation, architecture diagrams, SBOM and test results
- No assumptions - only evidence

# Real-World Incidents That Shaped CRA

Log4Shell - global supply chain exposure

- ➢ SolarWinds - compromised update mechanism
- ➢ WannaCry -  failure to patch known vulnerability
- ➢ Colonial Pipeline - weak access control
- ❖ These incidents transformed cybersecurity from technical issue to regulatory obligation

# Evidence Package

GAP Analysis

- Risk Assessment
- SBOM
- Architecture overview
- Vulnerability management process
- Update/patching procedures
- Penetration test results
- Supporting evidence from the manufacturer

# Reporting to ENISA

Final documentation submitted to ENISA

- ENISA verifies compliance
- Ensures products entering the EU market are safe
- Mandatory for all CRA-covered products

# Support for Small Companies

EU grants available (up to €60,000)

- Programs: Secure, Cyberstand EU
- Helps companies hire experts and prepare documentation
- Reduces financial burden of compliance

# Conclusion

CRA reduces the probability and impact of the next major incident

- Security becomes a core requirement
- Early preparation = competitive advantage
- Protecting customers is the ultimate goal

# Thank you for your attention!

February 2026

**Dafina Stefanova**

**m: +359 888 448466**

dafistefanova7@gmail.com

WOMEN4CYBER
EUROPEAN CYBER SECURITY ORGANISATION
BULGARIA

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT
Open-Source Cyber Resilience Act Tools