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.

Cyber Resilience Act: Achievements and Pending Actions

Digital Innovation Hub Trakia

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT Open-Source Cyber Resilience Act Tools

Implementation Status of the Cyber Resilience Act

A snapshot of achievements and gaps (as of mid-2025)

Delegated Acts

- **Status**: Not yet adopted.
- **Context**: Article 8 and Article 61 authorize the European Commission to issue delegated acts to specify which critical products require mandatory EU certification (with at least “substantial” assurance).
- **Current Situation**: No such acts have been published so far.

Single Reporting Platform

- **Status**: Not yet operational.
- **Evidence**: ENISA has launched a tender for the SRP development — budgeted at €11 million for a 4-year build — but the platform is still not live.

European Vulnerability Database (EUVD)

- **Status**: Operational.
- **Evidence**: ENISA's **EU Vulnerability Database** (EUVD) is now fully functional and provides a centralized repository of cybersecurity. vulnerabilities, with features such as dashboards on critical and actively exploited vulnerabilities.

Development of Standards

- **Status**: In progress.
- **Evidence**: ENISA and the Joint Research Centre (JRC) published a mapping of CRA requirements to existing standards in April 2024 to support future harmonized standards.

European Certification Schemes

- **Status**: Under development.
- **Evidence**: Article 8 allows for EU-level cybersecurity certification. schemes (e.g., EUCC). However, no fully adopted schemes are yet in place; the process is ongoing.

Declaration of Conformity

- **Status**: Not available in official form.
- **Context**: CRA provides model templates in Annex V (standard) and Annex VI (simplified). Although outlined in regulation, no published, standardized form from EU authorities is available yet.

Conformity Assessment Procedures

- **Status**: Available.
- **Evidence**: CRA includes procedures for self-assessment and third-party assessment for compliance (Article 32–41). It also defines roles: Commission, ENISA, national notifying authorities, notified bodies, and market surveillance authorities.

SME Support
Simplified Technical Documentation

- **Status**: Not yet implemented.
- **Context**: While CRA envisages simplified approaches for micro, small, and medium enterprises, no official simplified template for technical documentation exists to date.

Notified Bodies

- **Status**: In progress — by end of 2026 all Member States must have them.
- **Evidence**: CRA requires each Member State to designate notified bodies by 11 December 2026; the establishment process is underway.

National Authorities

- **Status**: Confirmed.
- **Evidence**: CRA mandates national notifying authorities and market surveillance bodies. Member States have designated institutions accordingly (e.g., NCCA, national COM authority) under Article 36+.

Administrative Sanctions

- **Status**: Implementation ongoing.
- **Evidence**: CRA stipulates fines of up to €15 million or 2.5% of global turnover (Article 64), but transposition in national legislation is still in process.

Reporting Obligations

- **Status**: Partly applicable after 11 Dec 2027.
- **Evidence**: CRA enforces vulnerability and incident reporting deadlines (within 24h/72h/month), yet the full set of requirements become enforceable after 11 December 2027.

Implementation Status

Delegated Acts	Not yet
Single Reporting Platform (SRP)	Not yet
European Vulnerability Database	Yes (Operational)
Harmonized Standards	In progress
EU Certification Schemes	In development
Declaration of Conformity (EU form)	Not yet
Conformity Assessment Procedures	Yes
SME Simplified Documentation	Not yet
Notified Bodies	In progress
National Notification Authorities	Established
Administrative Sanctions	National process
Reporting Obligations	Not yet applied

Next Topic
Scope and Obligations under CRA

- Which products are covered: IoT, software, embedded hardware.
- Roles & responsibilities: manufacturers, importers, distributors.
- EUCS (Cloud Services Scheme) – regulating cloud providers.
- Case study: CRA impact on IoT manufacturers.
- Obligations: declarations of conformity, vulnerability reporting.
- Sanctions and consequences of non-compliance.

Thank you!

Miroslav Mitev, PhD
+359 896 198 875
m.mitrev@dihtrakia.org