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 Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

Economic Operators under the Cyber Resilience Act: Roles and Responsibilities

Digital Innovation Hub Trakia

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT Open-Source Cyber Resilience Act Tools

Context

CRA defines who is responsible for cybersecurity at every stage of a product's life cycle.

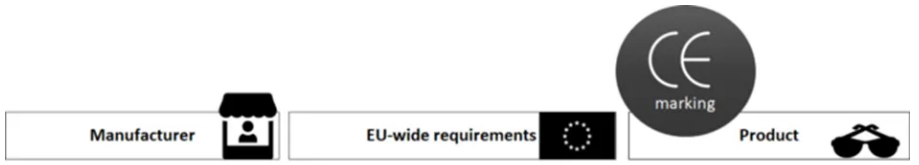
Introduce the three key actors: **Manufacturer, Importer, Distributor**.

Why Economic Operators Matter

- Cybersecurity accountability must exist across the supply chain.
- CRA closes the gap between product design, import, and distribution.
- Links to the EU's *"secure-by-design and by-default"* principles.
- Reference ENISA's statement: *"Security cannot stop at the factory gate."*

Overview of Roles

- **Manufacturers.**
- **Importers.**
- **Distributors.**



Manufacturer: Primary Responsibility

Full responsibility for product compliance.

Tasks:

- Design and develop according to essential cybersecurity requirements (Annex I).
- Prepare **Technical Documentation**.
- Conduct **Conformity Assessment**.
- Issue **EU Declaration of Conformity (DoC)**.
- Affix **CE marking**.
- Ongoing duty to monitor and fix vulnerabilities.

Manufacturer: After Placing on the Market

- Post-market surveillance and incident response.
- Reporting vulnerabilities to **ENISA** and national authorities (within 24 hours if actively exploited).
- Provide software updates during the support period.
- Maintain records and cooperate with authorities.

Importer: Gatekeeper to the EU Market

- Product has **DoC** and **CE marking**.
- Manufacturer followed CRA obligations.
- Technical documentation is available in EU language.
- Cannot place product on market if non-compliant.
- Ensures traceability (contact details, batch numbers, etc.).

Distributor: Last Link to the User

- Checks visible compliance: CE marking, labeling, instructions.
- Must act if a product seems unsafe or modified.
- Must cooperate with manufacturers/importers during recalls or incident handling.
- Communication role – must inform users and authorities when risks are found.

Shared Responsibilities

- Cybersecurity is **collective**: each operator contributes to the same product lifecycle.
- Duties overlap – communication and traceability are key.
- All operators must support vulnerability handling and updates.
- Visual: Venn diagram of shared obligations (Security | Compliance | Reporting).

Information Flow & Traceability

1

ENISA model: “Information must flow both upstream and downstream.”

2

Importance of clear contacts, version control, update channels.

Conformity Assessment & Documentation

- CRA, Annex VI – self-assessment vs. third-party certification.
- When a **Notified Body** is required (for critical products).
- What documentation each operator must store and for how long (10 years).

Vulnerability Reporting Duties

- CRA, article 11 – mandatory vulnerability handling process.
- Timeline for notification (ENISA / CSIRTs).
- Coordination between manufacturer and distributors for patches.

DISCOVERY → REPORT → FIX → NOTIFY

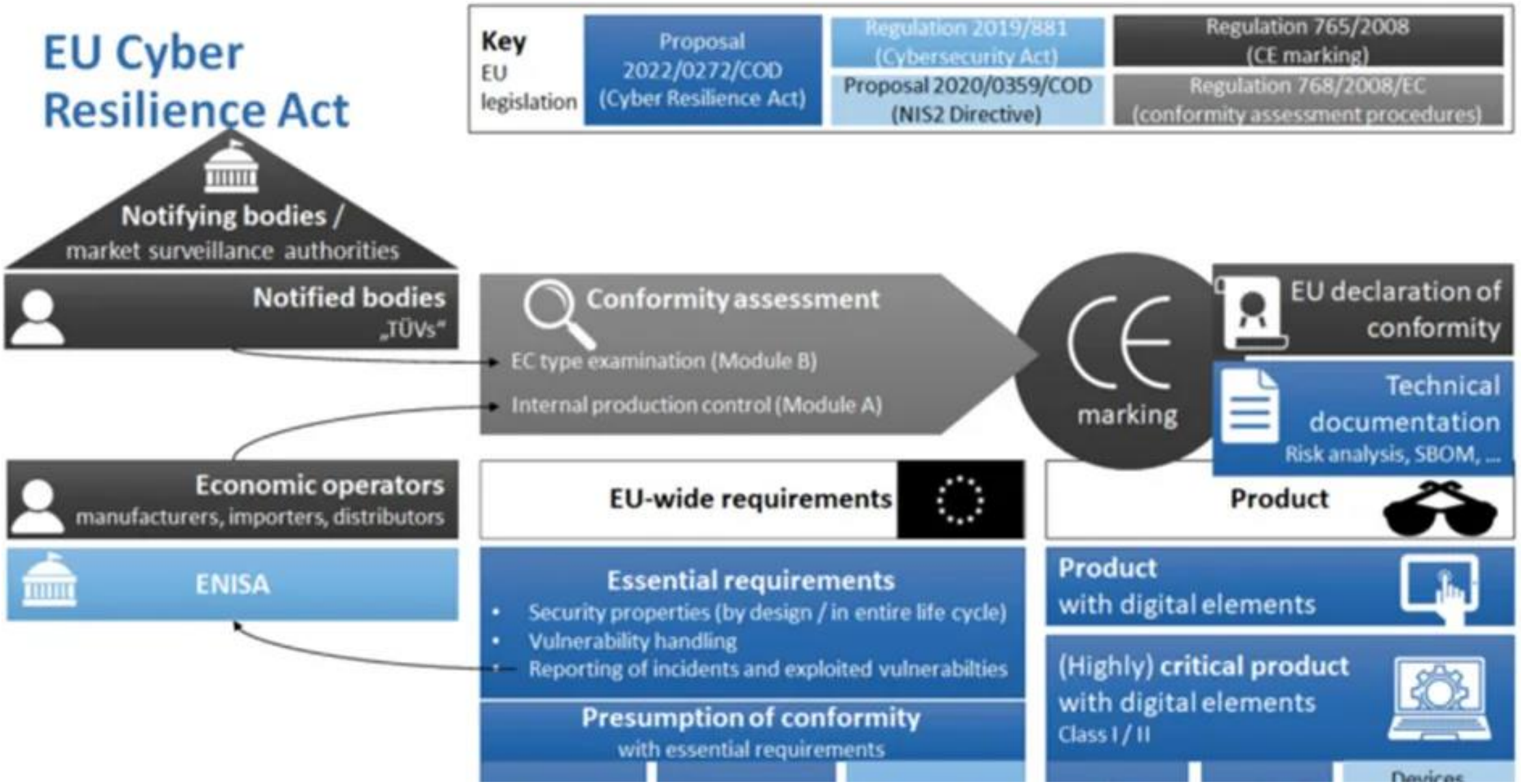
Who Does What – Responsibilities Across the Product Lifecycle

Who	What (Main Responsibilities)	When (Timing / Condition)
 Manufacturer	• Design and develop product according to cybersecurity requirements (Annex I). • Prepare Technical Documentation & EU Declaration of Conformity (DoC). • Affix CE marking. • Set up vulnerability handling & update process. • Report exploited vulnerabilities to ENISA & CSIRTs. • Keep records & cooperate with authorities.	▶ Before placing on the market (design, documentation). ▶ After placing – monitor, patch, report.
 Importer	• Verify CE marking & Declaration of Conformity. • Ensure manufacturer follows CRA. • Check technical documentation (EU language). • Maintain traceability (contact, serials). • Stop sale if non-compliant.	▶ Before placing on EU market. ▶ During issues – inform manufacturer & authority.
 Distributor	• Check visible compliance (CE mark, instructions). • Don’t sell unsafe or modified product. • Cooperate in recalls or incidents. • Inform users & authorities about risks.	▶ Before sale – verify compliance. ▶ During distribution – monitor security & recalls.

Market Surveillance & Enforcement

- National authorities' role.
- Powers to request documentation, stop sales, or order recalls.
- Sanctions under Article 53 – penalties proportional to turnover.
- Example from ENISA: alignment with the EU Market Surveillance Regulation 2019/1020.

EU Cyber Resilience Act



Practical Examples

- Case 1: Importer finds missing documentation → cannot release product.
- Case 2: Distributor reports exploited vulnerability → manufacturer issues patch.
- Case 3: Authority inspects conformity documentation after complaint.

Key Takeaways

Manufacturers → design and maintain security.

Importers → verify and ensure documentation.

Distributors → monitor, communicate, cooperate.

Shared goal: a trustworthy digital single market.

Thank you!

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