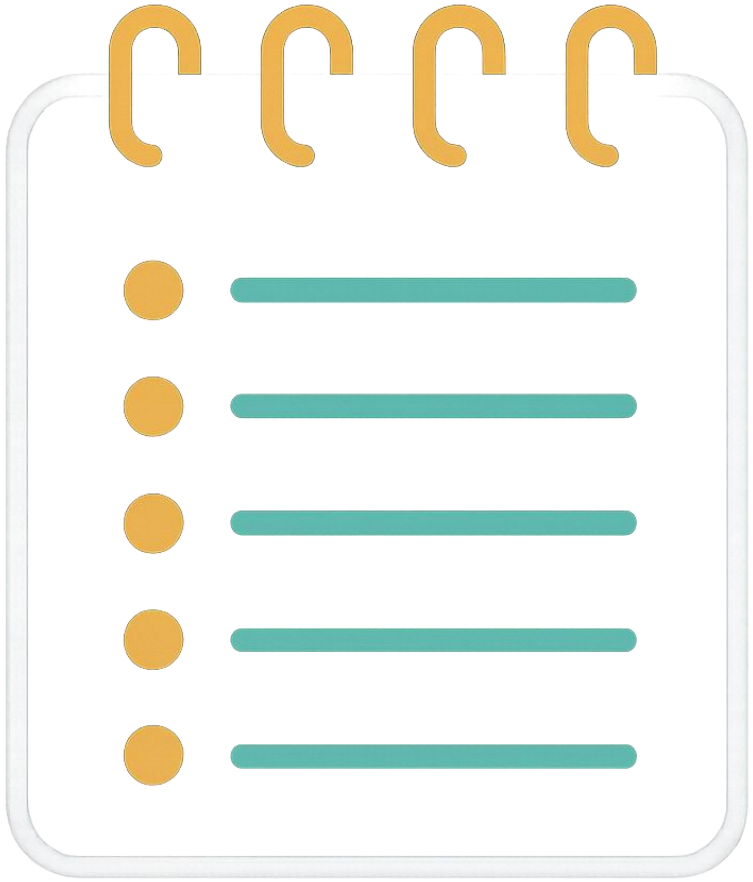
EU Cyber Resilience Act (CRA)

Agenda

- What is the EU CRA?
- Timelines for EU CRA
- Categorization
- Conformity Assessment Expectations
- Exemptions
- Next Steps



What is EU CRA?

- CRA – Cyber Resilience Act ((EU)2024/2847)
- Addresses cybersecurity challenges by passing this regulation
- Makes users aware of cyber issues in products and helps them choose products appropriately
- **Mandatory** for all products with digital elements
- To have fewer vulnerabilities & to ensure manufactures take security seriously
- Creates a harmonized regulatory framework

Timelines for EU CRA

- 23rd October 2024 – EU signs the regulation
- 10th December 2024 – Regulation came into force
- 11th September 2026 - Reporting obligations of Manufacturers (Manufacturer shall notify any actively exploited vulnerability)
- 11th December 2027 – Regulation becomes applicable and all manufacturers should follow the same

Categorization

Important (Class I)*

- Boot Managers
- Operating Systems
- MPU/MCU with security-related functionalities
- ASIC & FPGA with security-related functionalities
- Smart Home general purpose virtual assistants
- Smart Home products with security functionalities
- …….

Important (Class II)

- Hypervisors
- Firewalls, Intrusion detection & prevention systems
- Tamper-resistant microprocessors
- Tamper-resistant microcontrollers

Critical

- HW devices with security boxes
- Smart Meter Gateways
- Smart Cards or similar device, including secure elements

Default

- Any product not listed in the 'Important' or 'Critical' category

* List given is incomplete. Please refer to Annex III for complete list

Conformity Assessment Expectations

- Default Category
  - Manufacturer self-assessment is sufficient
- Important (Class I)*
  - 3rd party assessment
- Important (Class II)*
  - 3rd party assessment
- Critical
  - 3rd party EU certification

* There are some subtle differences between Class I & Class II and not covered here

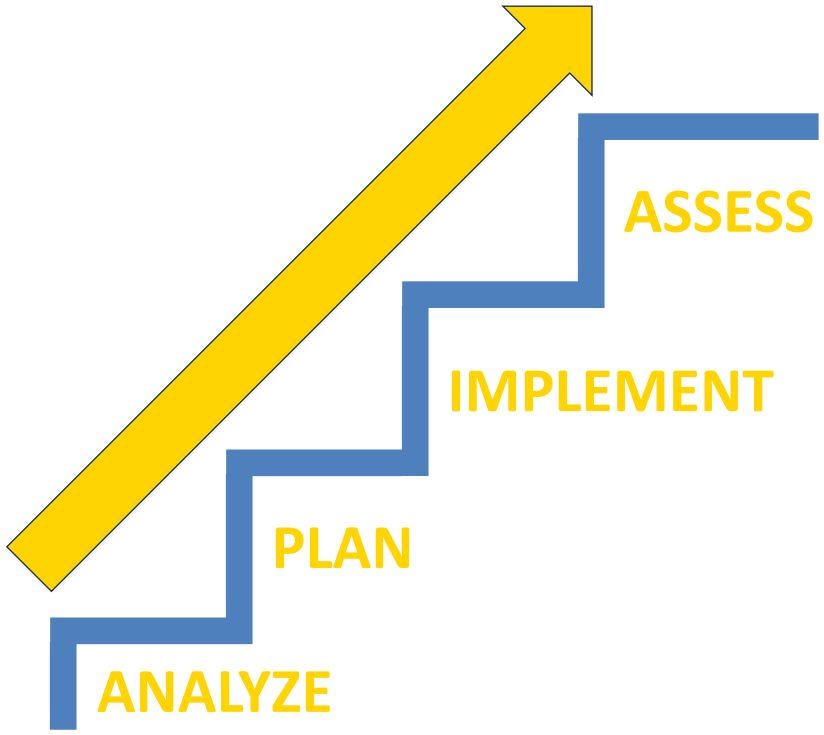
 www.Drivvize.com

Exemptions

Below products are already covered under separate cybersecurity standard and hence no additional evidence is required

- Medical Devices
- In vitro diagnostic medical devices
- Motor Vehicles
- Civil Aviation
- Marine Equipment

Next Steps



- Perform a ‘Gap Analysis’ to identify current state
- Update or create process framework to align with EU CRA expectations
- Implement cybersecurity related mechanisms (If identified as a gap from ‘Gap Analysis’)
- Plan audit (Internal or External based on product categorization)

Disclaimer

Important Note: The EU CRA Act contains a lot of information and some of them seem to be written with a legal perspective in mind. What we have tried to provide here is a summary of this information based on our understanding. While we have done our best to remain factual and accurate, please do your due diligence when trying to determine the best course of action for your product.

Disclaimer

Thanks!

Consultation

Knowledge

 www.Drivvize.com