Impact of EU CRA and Cyber Regulations on FPGA

A Leading Provider of Smart, Connected and Secure Embedded Control Solutions

Ian Pearson

01July25

Regulations and Standards

Disclaimer

The following slides provide a subjective interpretation of the relevant regulations and are intended for informational purposes only. They do not constitute legal advice. For specific legal guidance, please consult a qualified professional.

Eu Cyber Resilience Act

Agenda

- **EU CRA**
  - Basics and scope
  - Placing on the Market
  - Conformance Classes
  - Essential Requirements
  - Reporting Obligations
  - Timeline
- **How does this affect me?**
  - Secure by Design process flow
- **Does this affect FPGA/SoC based Designs?**

CRA Overview

Broad overview of CRA

- **Covers ALL in scope Products with Digital Elements – Hardware and Software – placed on the EU Market**
  - Risk based assessment
  - Excludes Medical, Automotive, Maritime, Military/Aerospace, National Security products (which have their own segment regulations)
- **Aim is to improve Product Cyber Security**
  - including resilience to attack and reliability/robustness if/when attacked
  - Increase product security posture from Product Concept through to End of Life
- **Implemented via**
  - Broad product security 'Essential Requirements' for ALL conformance categories
  - Enhanced 'Secure by Design, Secure by Default' practices
- **Obligations on 'Economic Operators' (Manufacturers, Importers, Distributors)**
  - To ensure products 'placed on the market' meet the regulations
- **Vulnerability Management system in place to maintain continuous compliance**
  - Reporting Obligations - timely reporting and resolution of incidents
- **Support Considerations**
  - Provide security updates for min. 5yrs from placing product on the market
- **Requires new CE mark**
  - Declaration of Conformance signed by suitably responsible person
  - Legally binding
- **Fines up to 15M Euro or 2.5% of revenue for non-compliance**

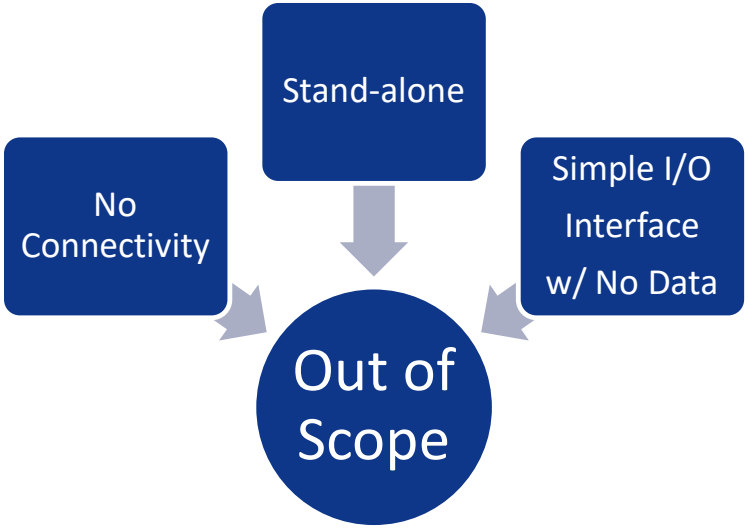
MICROCHIP

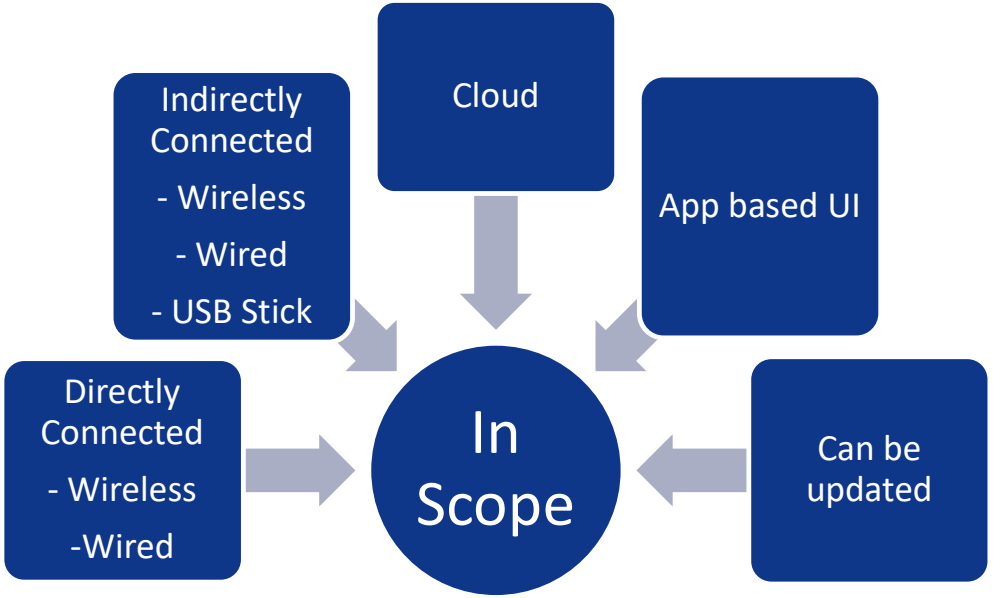
Cyber Resilience Act

What is in Scope?

- **Cyber Resilience Act covers <u>ALL</u> connected devices <u>unless</u> given an exemption**
  - Article 2 - Scope

All ‘Products with Digital Elements’ made available on the market, [hardware or software], where the intended purpose or reasonably foreseeable use of which includes a direct or indirect, logical or physical data connection to a device or network.

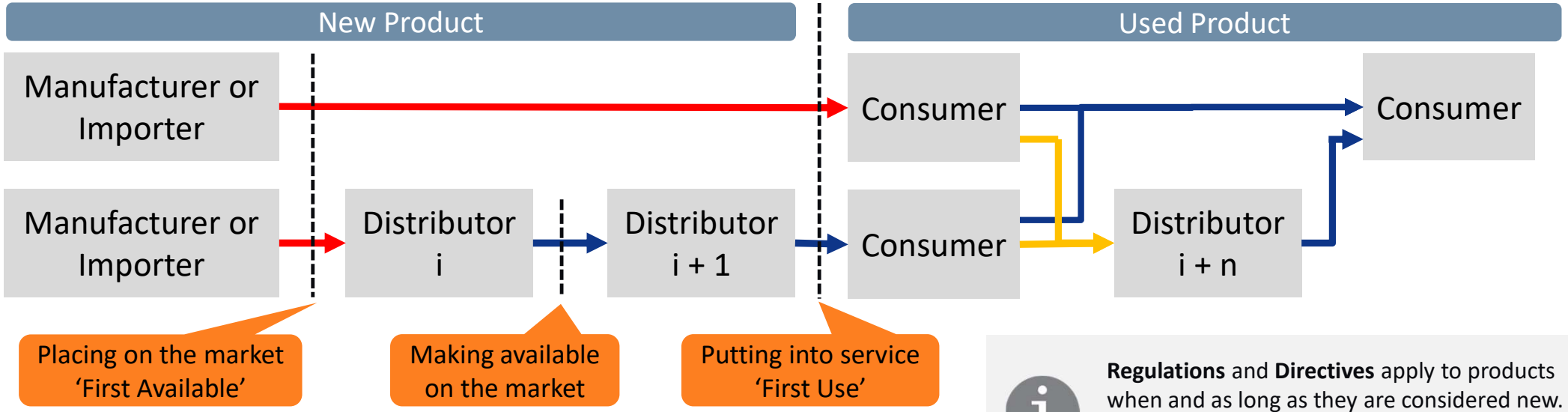




Protection of IP and security measures to mitigate cyber related safety issues still required at product level

EU Blue Guide

Explanation of ‘Placed’ and ‘Making Available’ on the market



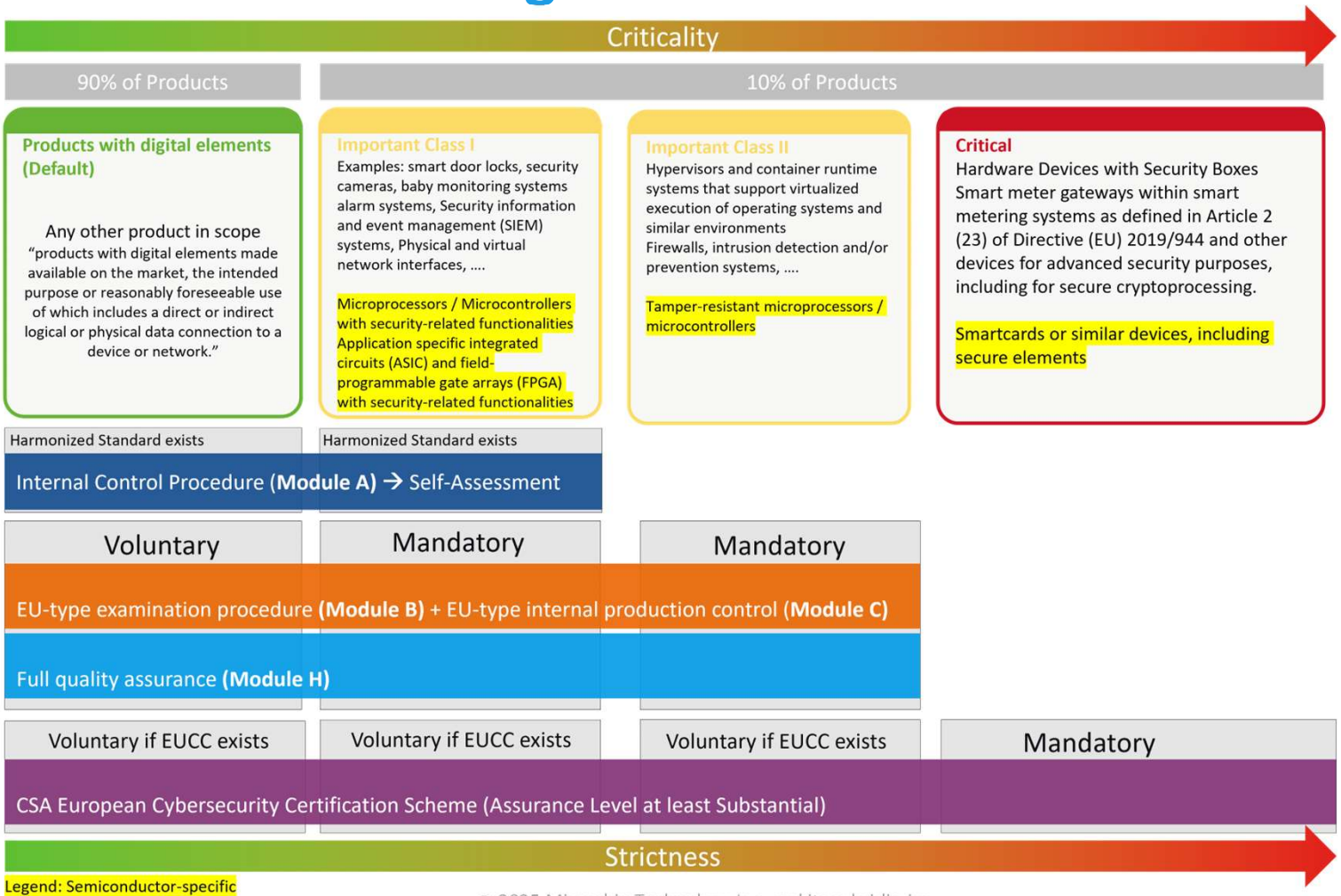
- **As per Blue Guide,**
  - ‘Placed on the market’ when [individual item] first made available
  - Placement has NO historic inheritance of type or serial
  - Performed by Manufacturer or Importer
  - Subsequent operation defined as ‘making available’

Regulations and **Directives** apply to products when and as long as they are considered new.
→ A product is considered new until its first use by the intended end-user.

Products must **meet all regulatory requirements at the time they are placed on the market** within the EU or EEA territory.

EU Cyber Resilience Act

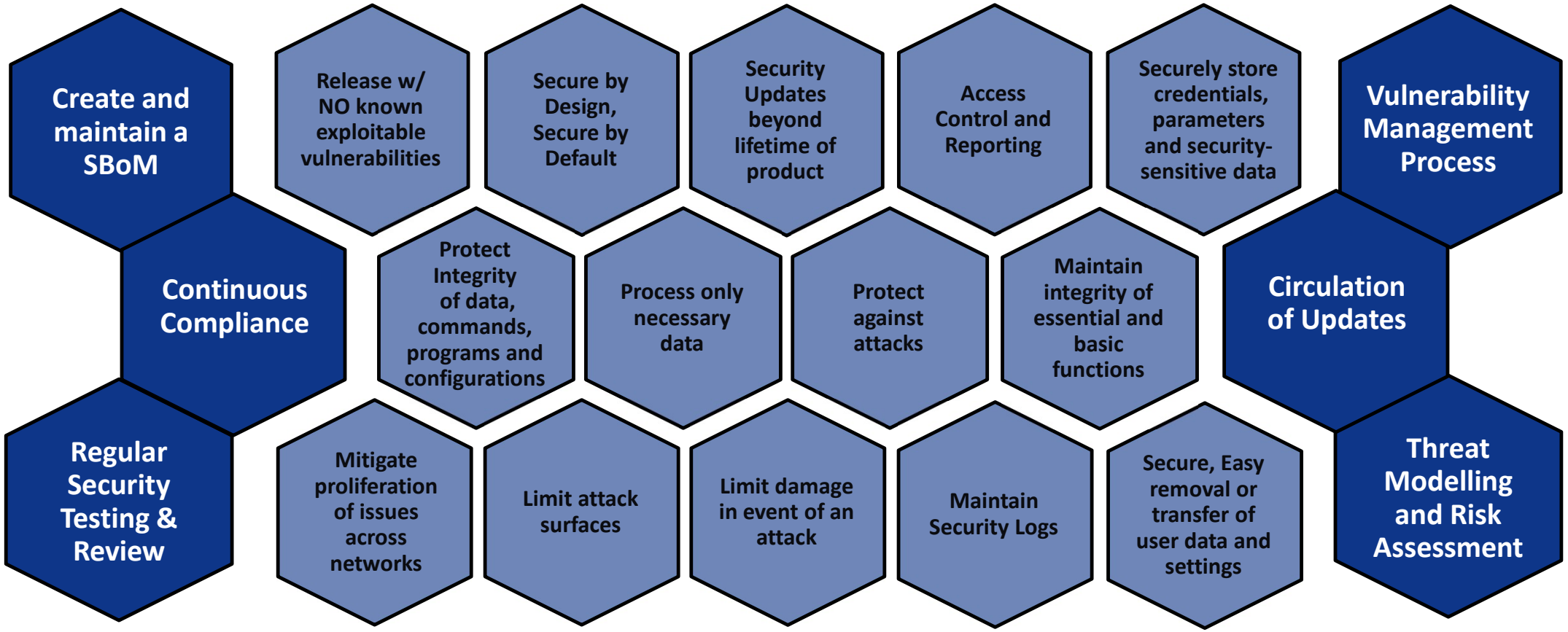
Product Conformance Categories



Legend: Semiconductor-specific

EU Cyber Resilience Act (CRA)

Key Requirements and Essential Requirements



Consider here the impact on the product development process

MICROCHIP

In Scope Products

Impact on Product Design, Manufacture and Lifetime Support

- **A Product with Digital Elements is expected to….**

‘***protect the availability, authenticity, integrity and confidentiality of sensitive or important data or functions***’ (from article 14, 5c relating to an event having severe impact)

- The inability to achieve these requirements is deemed a ‘**severe vulnerability**’ and is expected to be rectified asap inline with the vulnerability reporting obligations

‘***Be designed to ensure an appropriate level of cybersecurity based on the risks***’

- Follow ‘Secure by Design, Secure by Default’ guidelines
- Threat Analysis and Risk Assessment to determine product risk category
  - Performed from product concept thro’ end of life
  - Business Risks should form part of this assessment

MICROCHIP

EU Cyber Resilience Act

Reporting obligations (Article 11)

A **manufacturer** shall **notify** any **actively exploited vulnerability** contained in the product with digital elements that it becomes aware of simultaneously **to the CSIRT** designated as coordinator, in accordance with paragraph 7 of this Article, and **to ENISA**. The **manufacturer** shall **notify** that actively exploited vulnerability via the **single reporting platform** established in Article 11b.

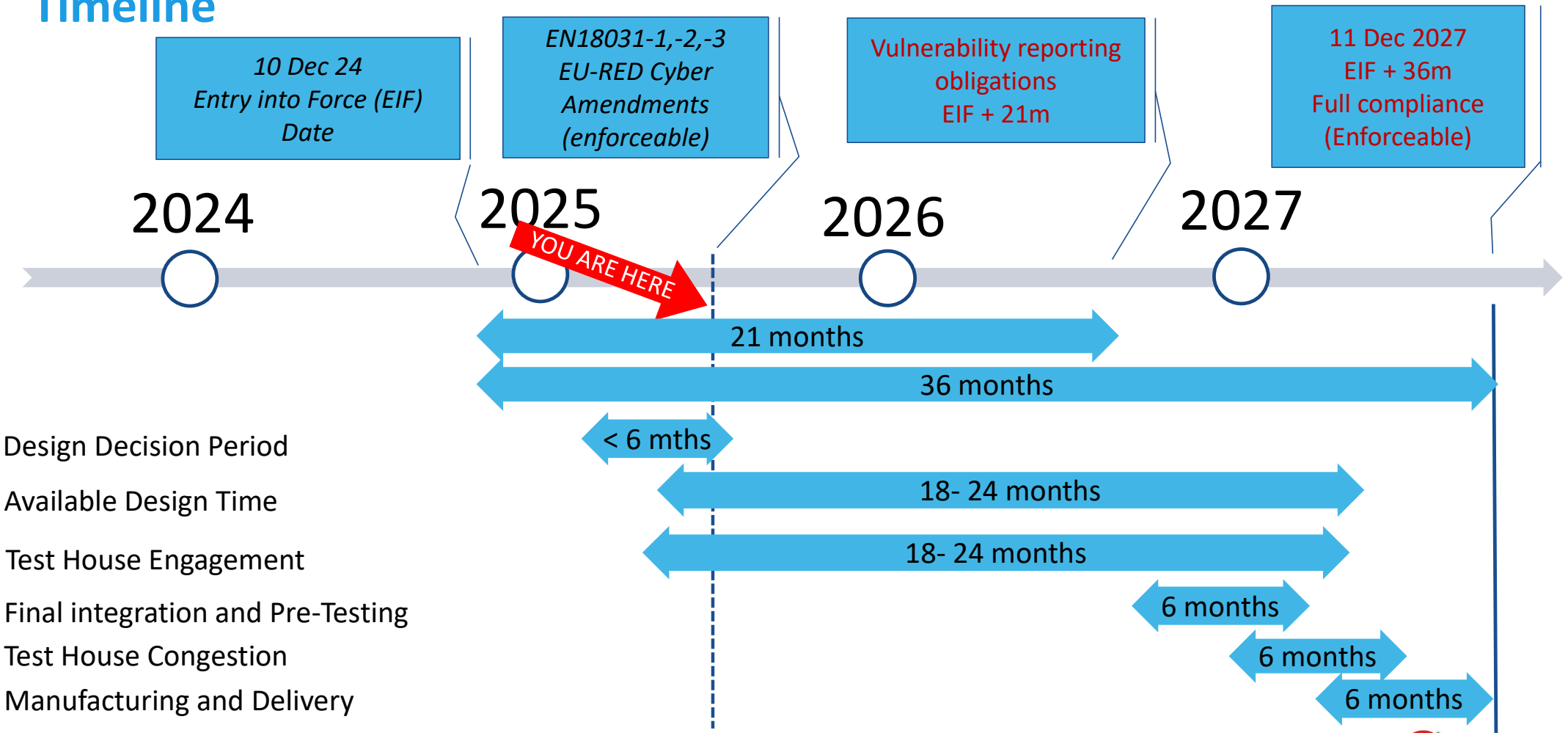
Type of reporting	Actively exploited vulnerabilities	**Severe incidents** ***negatively affects availability, authenticity, integrity or confidentiality of sensitive or important data or functions or has led or is capable to lead to the execution of malicious code***
Early warning	< 24 h	< 24 h
Notification	< 72 h	< 72 h
Final report incl. 1. a detailed description of the incident, including its severity and impact. 2. the type of threat or root cause that is likely to have triggered the incident. 3. applied and ongoing mitigation measures.	< 14 days after availability of solution / patch / fix	< 1 month after submission of the notification

Date of applicability: 21 months after entry into force of the regulation

MICROCHIP

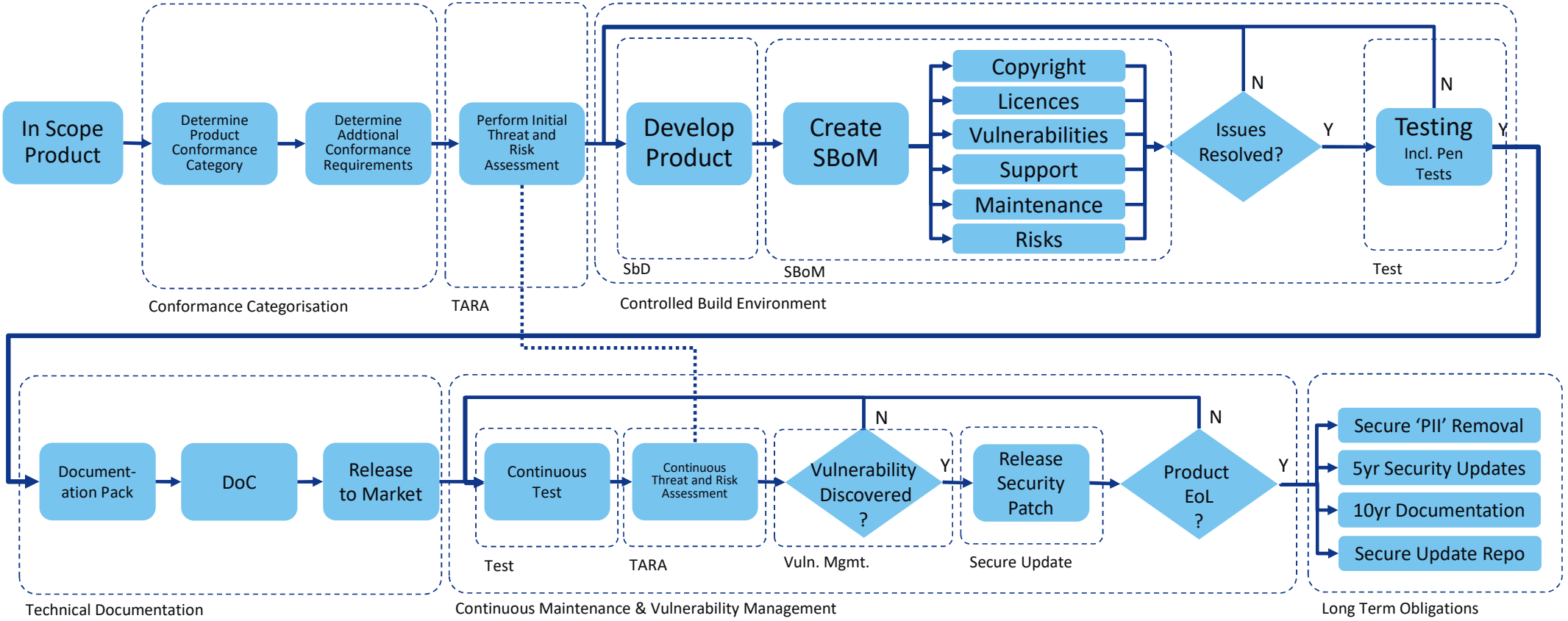
Cyber Resilience Act (CRA)

Timeline



CRA Design Process

Simplified ‘Secure by Design’ process for CRA



EU Cyber Resilience Act

Does this affect FPGA based Designs?

- **Does CRA affect FPGA based designs?**

EU Cyber Resilience Act

Does this affect FPGA/SoC based Designs?

- **If your design is in scope then, yes.**

- **Many additional requirements**
  - Product, Process, Testing, Support, Maintenance

- **Additional Design Considerations**
  - Threat Modeling, Risk Analysis, SBoM,

- **Additional Business Considerations**
  - Long term support and continuous compliance obligations, development complexity impact, new skills required, legal obligations on the company and DoC signatory

EU Cyber Resilience Act

Wrap-Up

- **EU CRA enforcement starts on 11Dec27**
- **It has a significant impact on how a product can be placed on the EU Market**
- **The cyber aspect of design has legal obligations on the manufacturer**
- **The time to engage is now**

MICROCHIP

Thank You!