CERTAINITY

The European Cyber Resilience Act

Get your House in Order Before the New Legislation Hits

Partner | Head of Security Engineering
Michael Brunner, PhD.

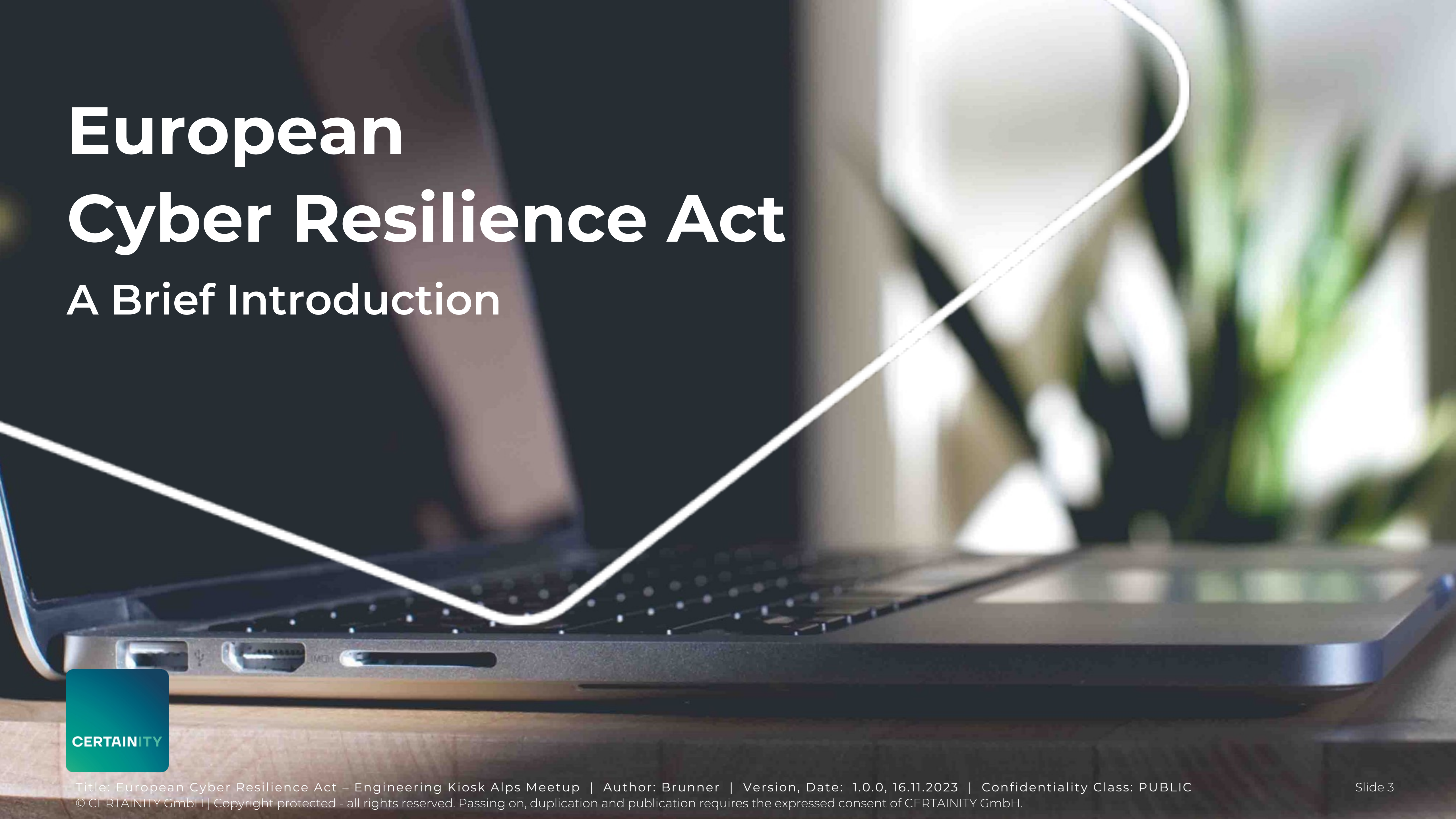
- Doctorate in computer science with focus on **information security and risk management**
- Over 15 years of professional experience working as IT, Management, and **Security Consultant** as well as **Software Engineer**
- Industry know-how: Financial service providers, transportation companies, energy suppliers, automotive manufacturers and suppliers

✉ michael.brunner@certainity.com | ☎ +43 664 9624028 | in Profile

Agenda

- **Who** is affected?
- **What** is required?
- **How** are you doing?
- **Why** should you start immediately with the preparation?

DISCLAIMER



European Cyber Resilience Act

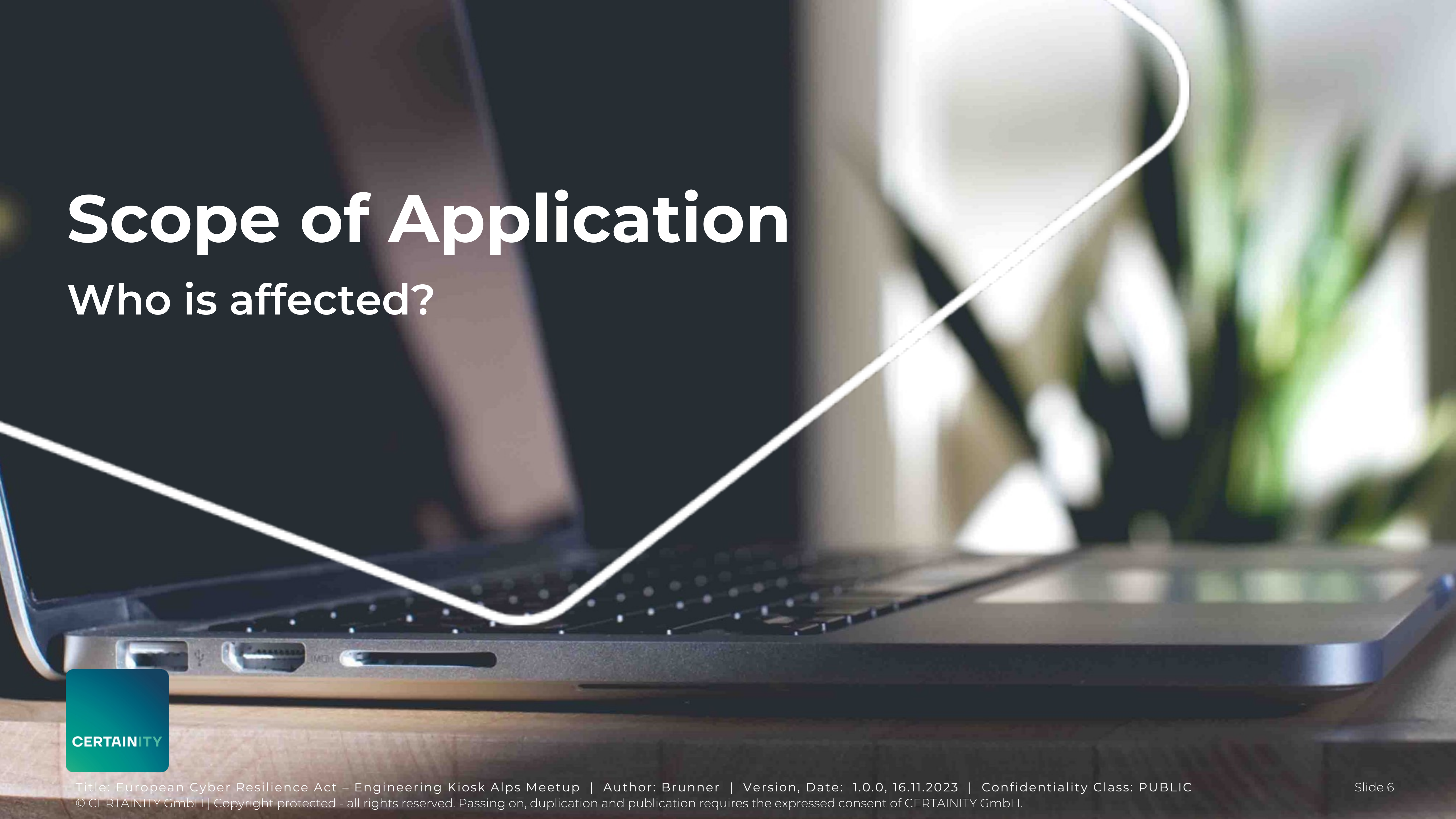
A Brief Introduction

CERTAINITY

European Cyber Resilience Act – The Big Picture

*Hardware and software products are increasingly affected by successful cyberattacks. The estimated global cost of cybercrime in 2021 was **5.5 Trillion EUR**.*

- The European Cyber Resilience Act is an essential component of the EU cyber security strategy
- Broadly regulates all products and industries that have not yet been covered by separate regulations - especially software development in the non-embedded area



Scope of Application

Who is affected?

CERTAINITY

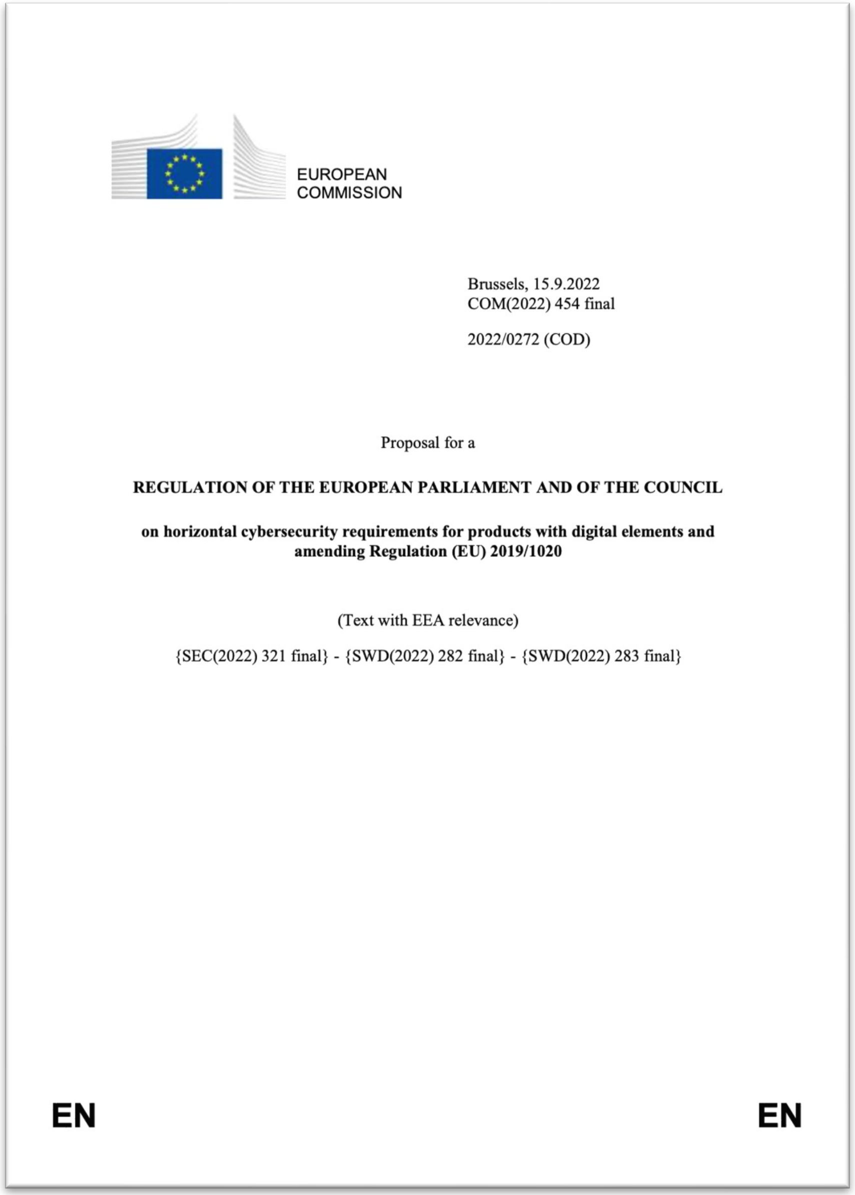
Scope in EU Legalese

This Regulation applies to products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network.

Definition **Product with digital elements**: *Any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately.*

Definition **Remote data processing**: any data processing at a distance for which the software is designed and developed by the manufacturer or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions

Exceptions: Products [..| to which the regulations (EU) 2017/745, 2017/746, 2019/2144 apply; products [..] certified in accordance with regulation (EU) 2018/1139, products [..] which are developed exclusively for national security or military purposes or to products specifically designed to process classified information, …



EUROPEAN
COMMISSION

Brussels, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

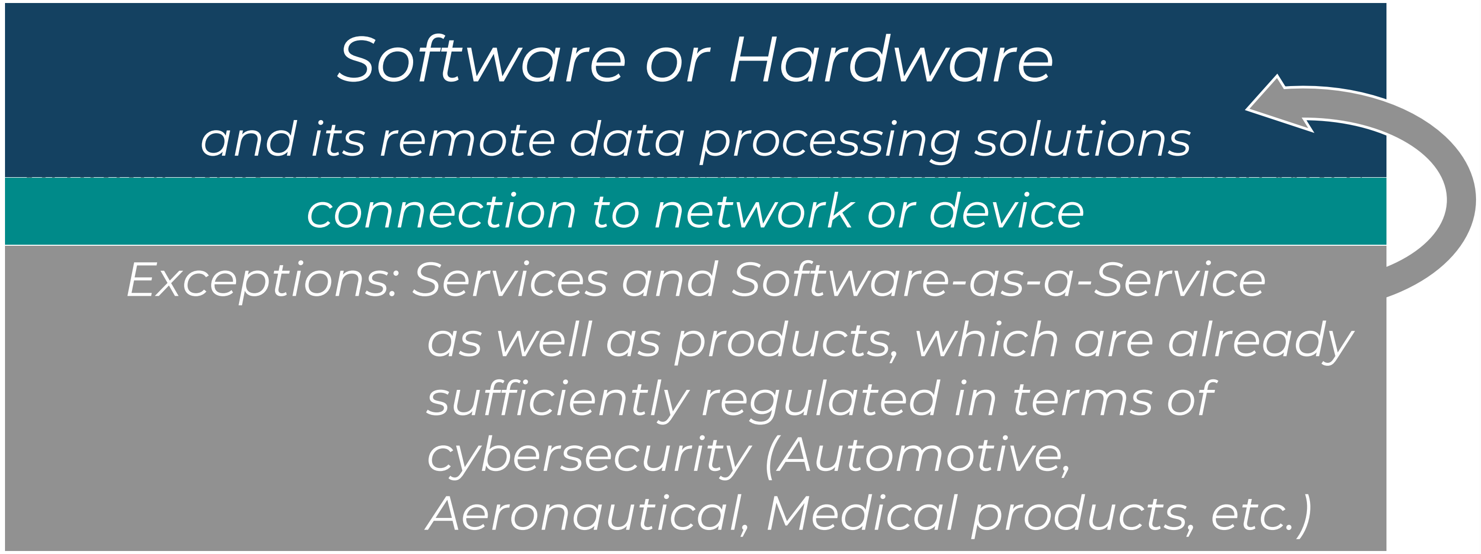
(Text with EEA relevance)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

EN EN

Scope in EU Legalese

This Regulation applies to products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network.



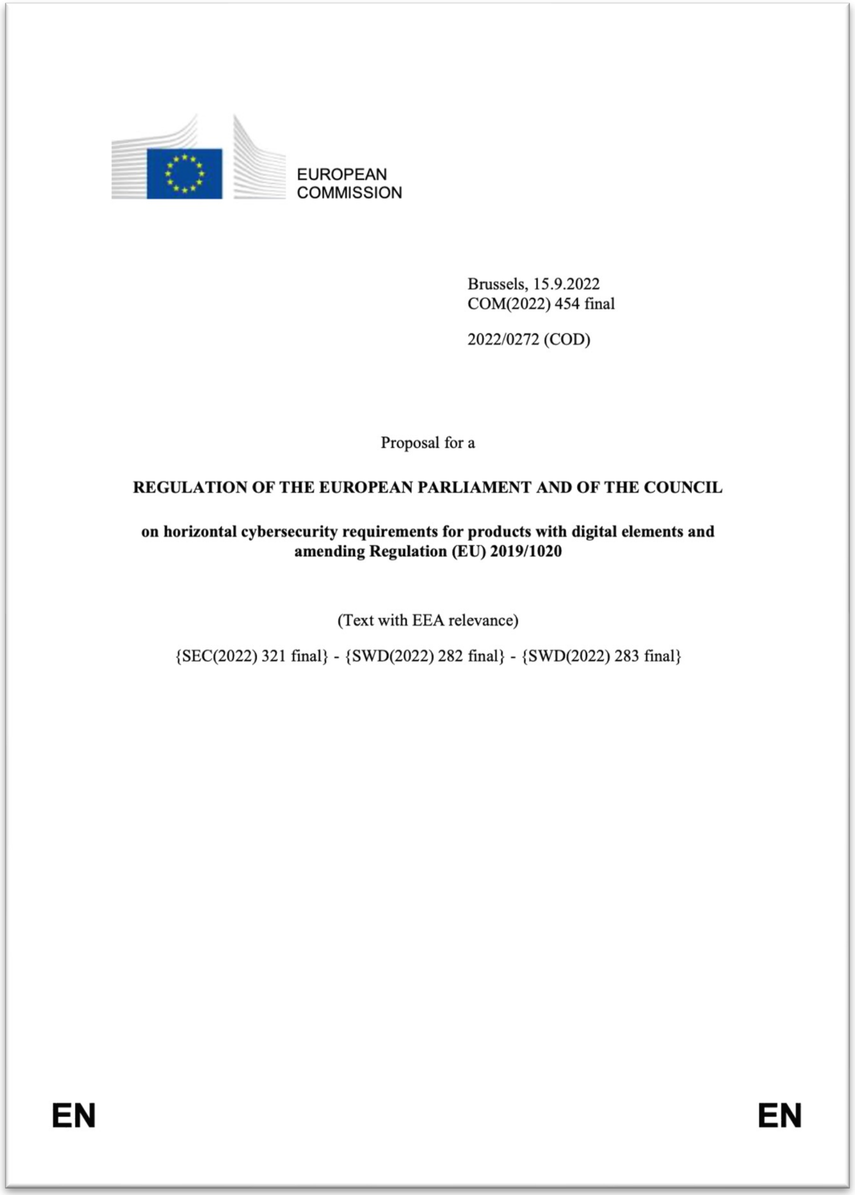
Software or Hardware

and its remote data processing solutions

connection to network or device

Exceptions: Services and Software-as-a-Service as well as products, which are already sufficiently regulated in terms of cybersecurity (Automotive, Aeronautical, Medical products, etc.)

Exceptions: Products [..| to which the regulations (EU) 2017/745, 2017/746, 2019/2144 apply; products [..] certified in accordance with regulation (EU) 2018/1139, products [..] which are developed exclusively for national security or military purposes or to products specifically designed to process classified information, ...



EUROPEAN
COMMISSION

Brussels, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

(Text with EEA relevance)

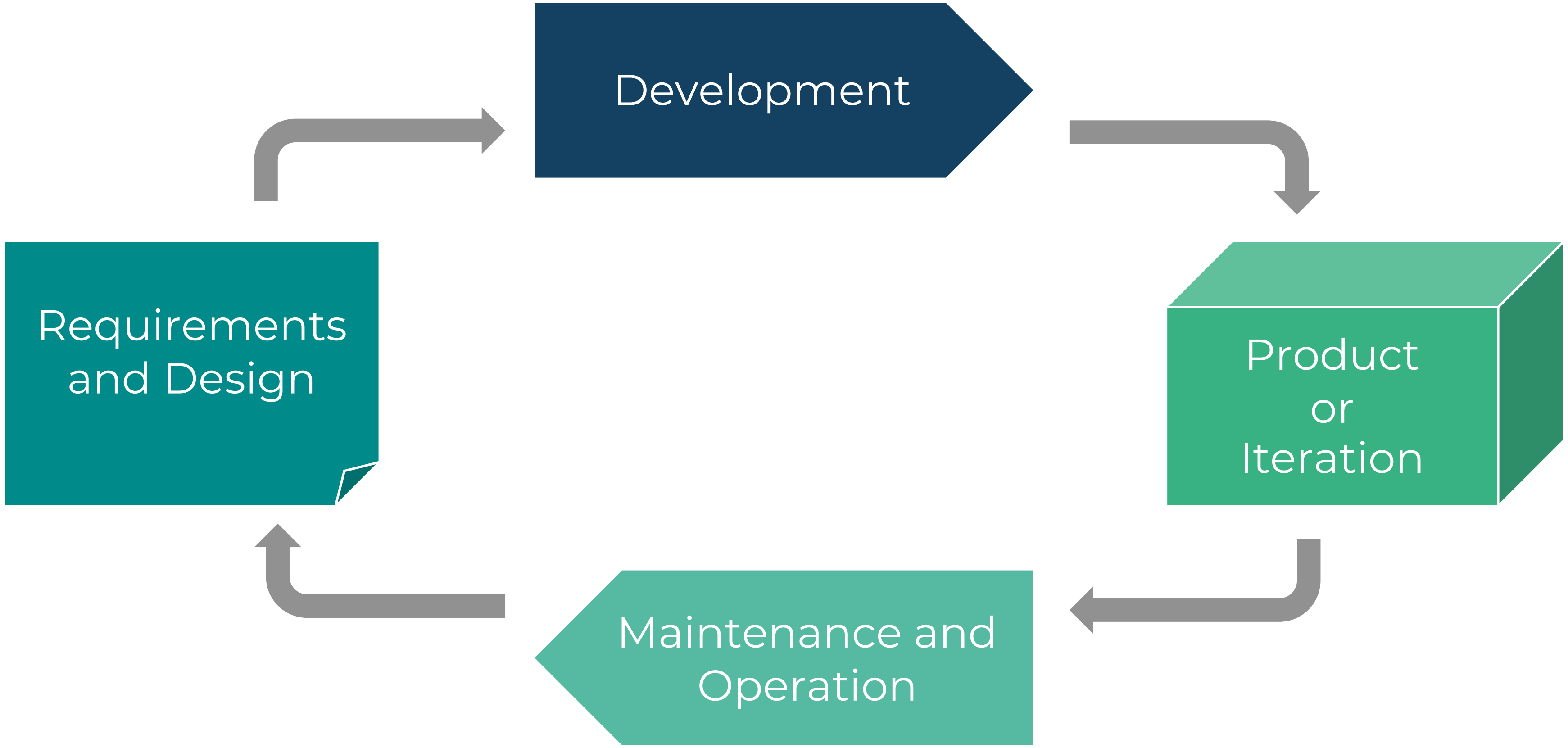
{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

EN **EN**

Requirements and Measures

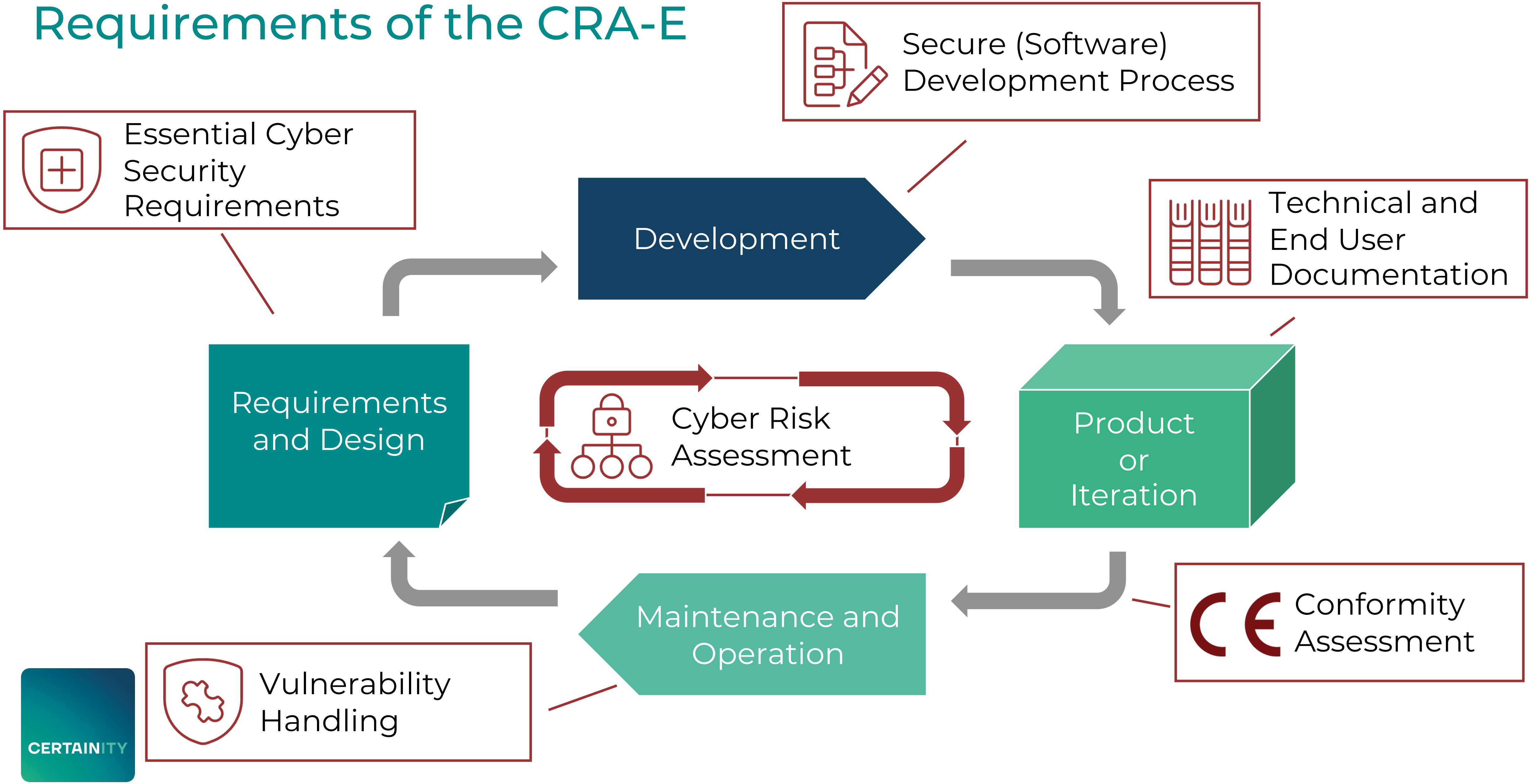
What is required?

Requirements of the CRA-E



CERTAINITY

Requirements of the CRA-E



Essential Cyber Security Requirements

Secure (Software) Development Process

Technical and End User Documentation

Conformity Assessment

Vulnerability Handling

Requirements and Design

Development

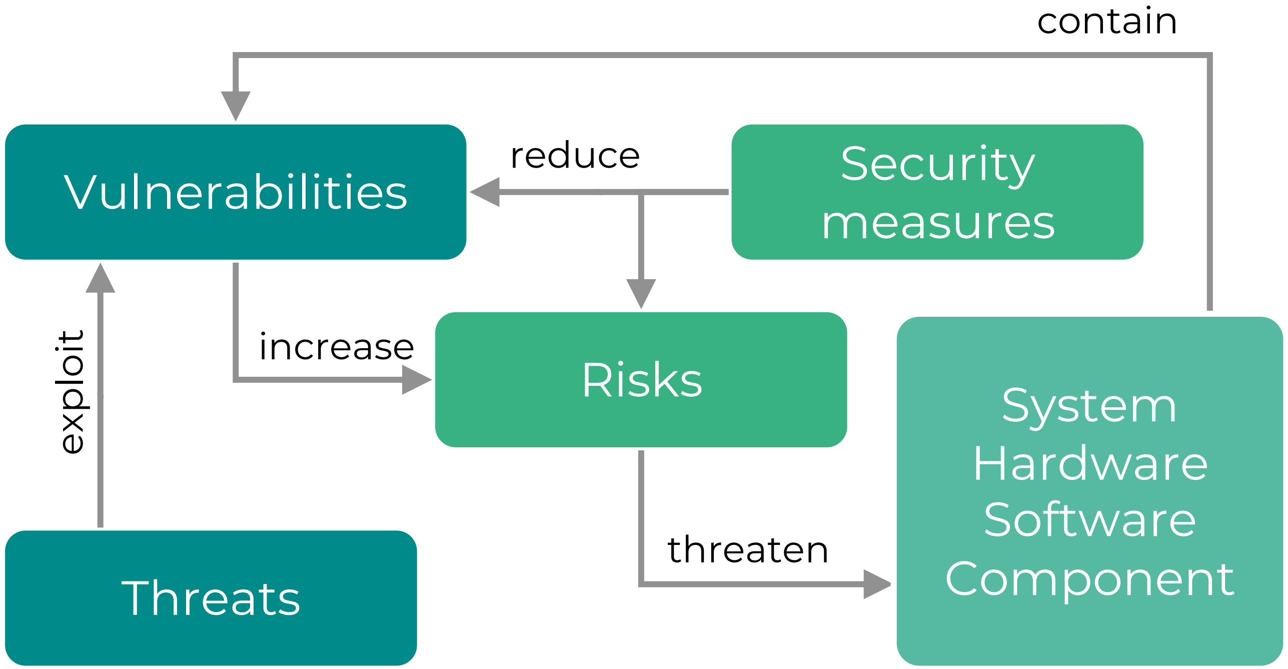
Product or Iteration

Maintenance and Operation

Cyber Risk Assessment

CERTAINITY

Cyber Security Risk Assessment



1 In addition to an intrinsic consideration, potential effects of security incidents on the health and safety of users must also be considered!

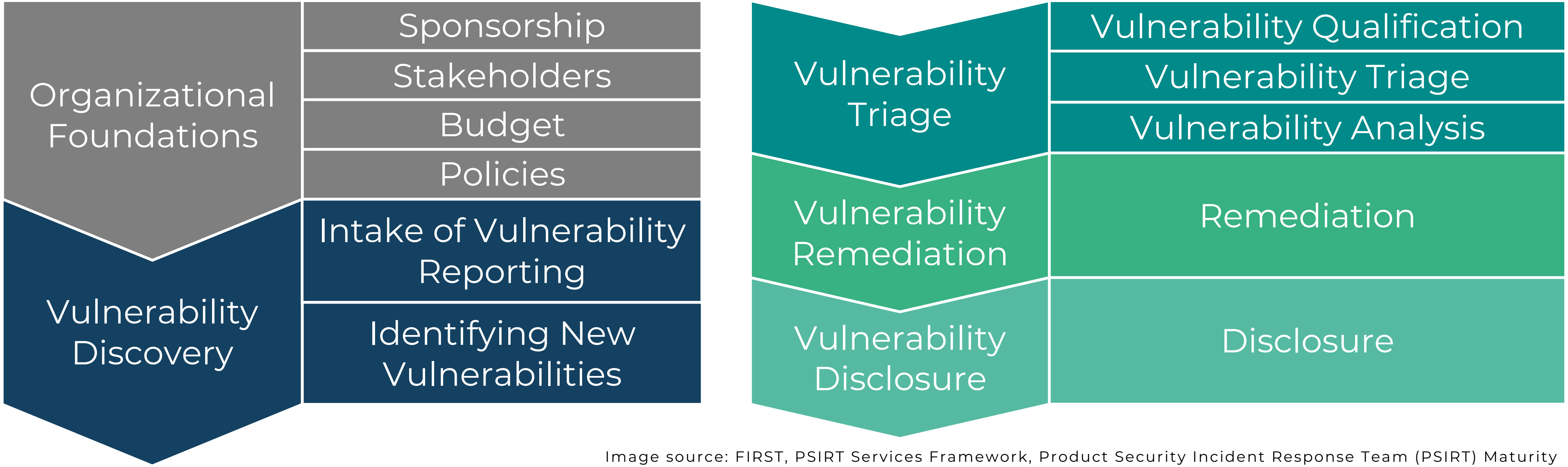
2 And: The own negative impact on the availability of services provided by other devices or networks.

3 Consideration of 3rd party and supply chain risks

- Due diligence when integrating 3rd party components
- No degradation of the security properties

Vulnerability handling requirements

Creation of the prerequisite for efficient vulnerability management through implementation of a Product Security Incident Response Team (PSIRT)



Organizational Foundations
- Sponsorship
- Stakeholders
- Budget
- Policies

Vulnerability Discovery
- Intake of Vulnerability Reporting
- Identifying New Vulnerabilities

Vulnerability Triage
- Vulnerability Qualification
- Vulnerability Triage
- Vulnerability Analysis

Vulnerability Remediation
- Remediation

Vulnerability Disclosure
- Disclosure

Image source: FIRST, PSIRT Services Framework, Product Security Incident Response Team (PSIRT) Maturity Document, available online at https://www.first.org/standards/frameworks/psirts/psirt_maturity_document

The European Cyber Resilience Act sets out 8 specific requirements for addressing vulnerabilities

Vulnerability handling requirements

Creation of the prerequisite for efficient vulnerability management through implementation of a Product Security Incident Response Team (PSIRT)

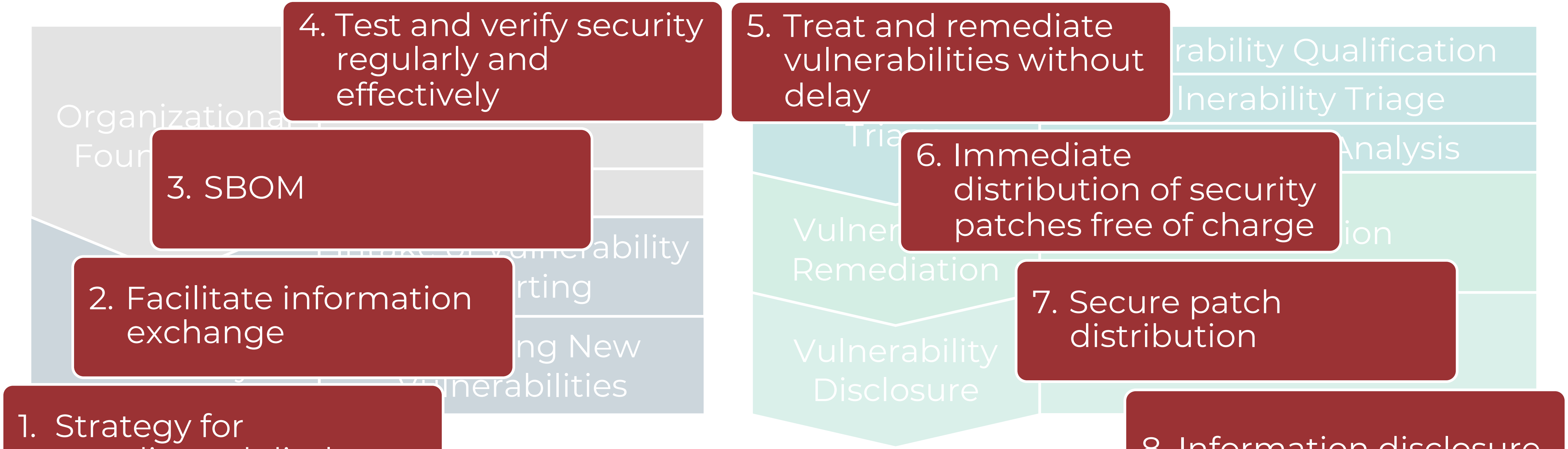
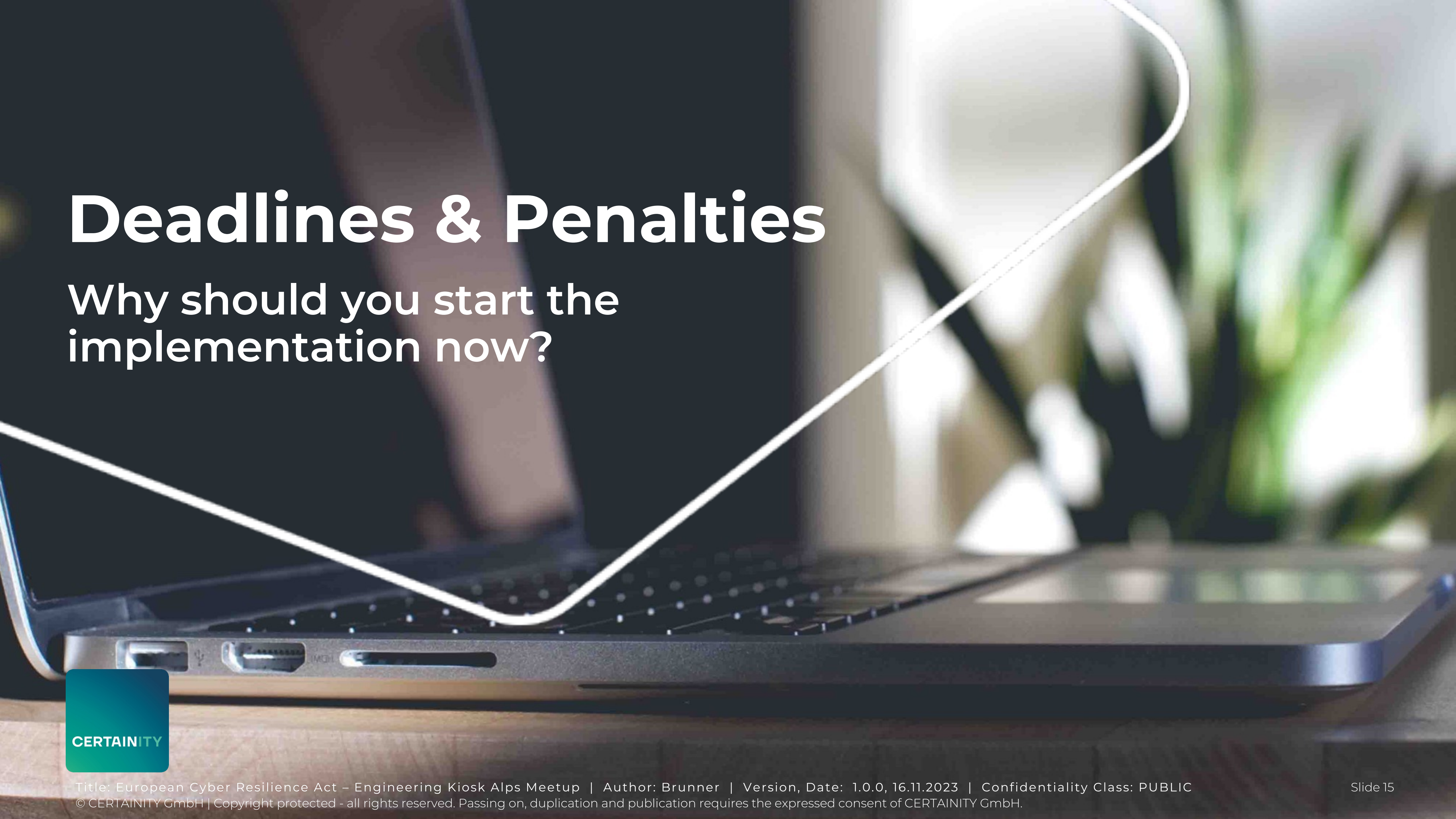


Image source: FIRST, PSIRT Services Framework, Product Se
Document, available online at https://www.first.org/standard

1. Strategy for coordinated disclosure
2. Facilitate information exchange
3. SBOM
4. Test and verify security regularly and effectively
5. Treat and remediate vulnerabilities without delay
6. Immediate distribution of security patches free of charge
7. Secure patch distribution
8. Information disclosure

The European Cyber Resilience Act sets out 8 specific requirements for addressing vulnerabilities

CERTAINITY



Deadlines & Penalties

Why should you start the implementation now?

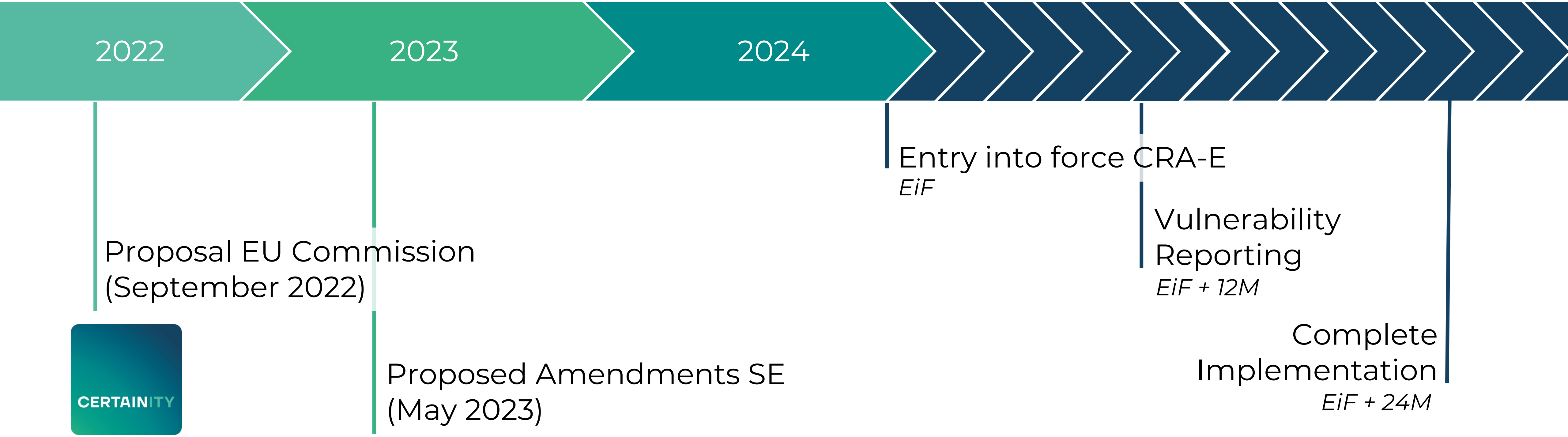
Penalities

Non-compliance with essential requirements and violations of specified duties	Non-compliance with other obligations	False, incomplete or misleading information provided to market surveillance authorities
€ 15.000.000 2,5 % Revenue (worldwide, prior year)	€ 10.000.000 2 % Revenue (worldwide, prior year)	€ 5.000.000 1 % Revenue (worldwide, prior year)

CERTAINITY

Deadlines for the implementation of the CRA-E requirements

- Based on current knowledge, the European Cyber Resilience Act is expected to come into force in 2024.
- Significant simplifications are not expected according to the latest amendment proposals and current developments



CERTAINITY

Cyber Resilience Act Preparedness Study – Challenges stated by participating companies

Development	Vulnerability Handling	Documentation
Personnel and Resources – Costs and Time Utilization | Qualification | Security Budget		
Management Support	Automation	Continuous Updates
Customer Expectations	Heterogeneous Tech Stacks in Complex Products	Varying Quality of Documentation
Heterogeneous Process Environment	Legacy Components	SBOM
Excessive Regulation	Communication Customers	Motivation
	Lack of Predictability	

CERTAINITY

universität innsbruck

Conclusio

CERTAINITY

CERTAINITY

CERTAINITY GmbH

reliable. trustworthy. bespoke.

Heiligenstädter Lände 27c | A – 1190 Wien
HG WIEN, FN 262176 D

office@certainity.com

https://certainity.com

Contact our experts immediately in the event of a cyber security incident

cert@certainity.com +43 664 888 44 686