AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

CYBER RESILIENCE ACT

Overview and Status

Christoph Schmittner

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

CYBER RESILIENCE ACT – CORE POINTS

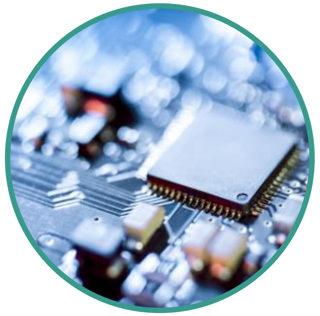
CYBER RESILIENCE ACT

Default category

- **Self assessment**
- Examples: Smart Speakers, Toys, Hard drives, Photo editor, Word processor

Class I – (critical) products

- **Self-assessment or third party (based on harmonized standard)**
- Routers, Microcontrollers, Anti-virus software, Password manager, Network interfaces, Firewalls



Class II – (highly critical) products

- **Third-party assessment (based on harmonized standard)**
- CPUs, Smartcards, Operating system, HSMs, Industrial firewalls, Smartcards, Smartcard readers, Secure elements

Risk Assessment: Functionality, Intended use, Impact

European Cyber Resilience Act (CRA) (european-cyber-resilience-act.com)

APPLICABILITY OF THE CYBER RESILIENCE ACT

Cyber Resilience Act applies to all products with digital elements

Excluded: Domains with pre-existing cybersecurity requirements

✓ Requirements depend on criticality

PRODUCTS WITH DIGITAL ELEMENTS

- Non exhaustive list:
  - Smartphones and Tablets
  - Computers and Laptops
  - Internet of Things (IoT) Devices
  - Wearable Technology
  - Networking Equipment
  - Software and Applications
  - Smart Vehicles
  - Medical Devices with Digital Elements
  - Gaming Consoles and Virtual Reality (VR) Headsets
  - Smart Industrial Equipment
  - Microcontroller
  - ….

CRA INTERACTION WITH SECTOR-SPECIFIC CYBERSECURITY

CRA Exemptions:

- Devices under existing sector-specific legislation may be exempt from CRA.

Sectoral Precedence:

- If a sector has dedicated cybersecurity regulations, these might supersede or complement CRA's requirements.

Future Legislation Potential:

- CRA allows for introduction of future sector-specific EU rules, affecting various domains.

EU Cybersecurity Framework Integration:

- CRA forms part of a wider EU framework, aiming to enhance product lifecycle security, relevant across sectors.

RATING OF CRITICALITY

Cybersecurity-Related Functionality

Authentication

Access Control

Intrusion Prevention

Endpoint Security

Network Protection

Core System Functions

Network Management

Configuration Control

Virtualization

Personal Data Processing

Disruption Potential

CRA REQUIREMENTS

Risk Assessments:

- Continuous mandatory risk assessments throughout the product's lifecycle to identify and manage potential cybersecurity vulnerabilities.

Vulnerability Management:

- Active management of identified vulnerabilities, including timely fixes and updates.

Automatic Security Updates:

- Provision of security updates automatically to all users, with an option for users to opt out.

External Audits for Critical Products:

- Products deemed critical must be subjected to external audits to ensure compliance with high cybersecurity standards.

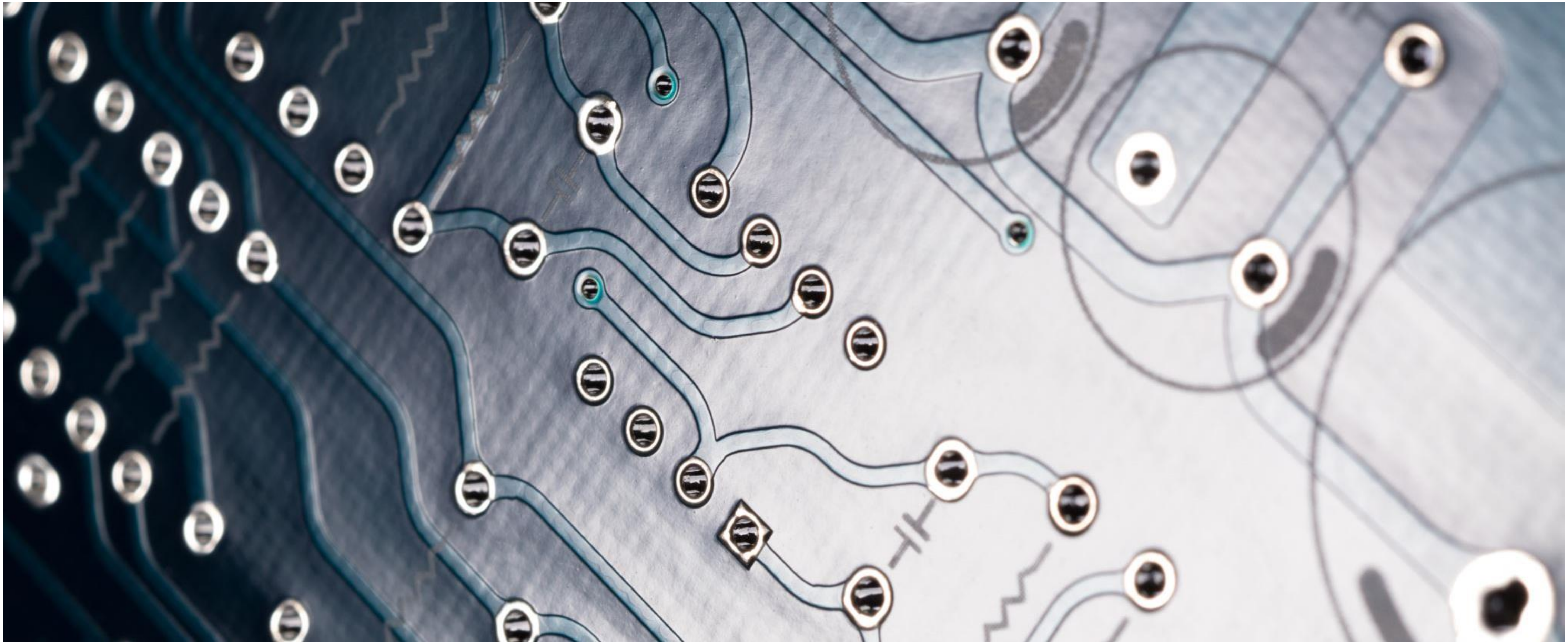
Rapid Incident Reporting:

- Obligation to report cybersecurity incidents to ENISA within 24 hours of detection, ensuring swift response and mitigation.

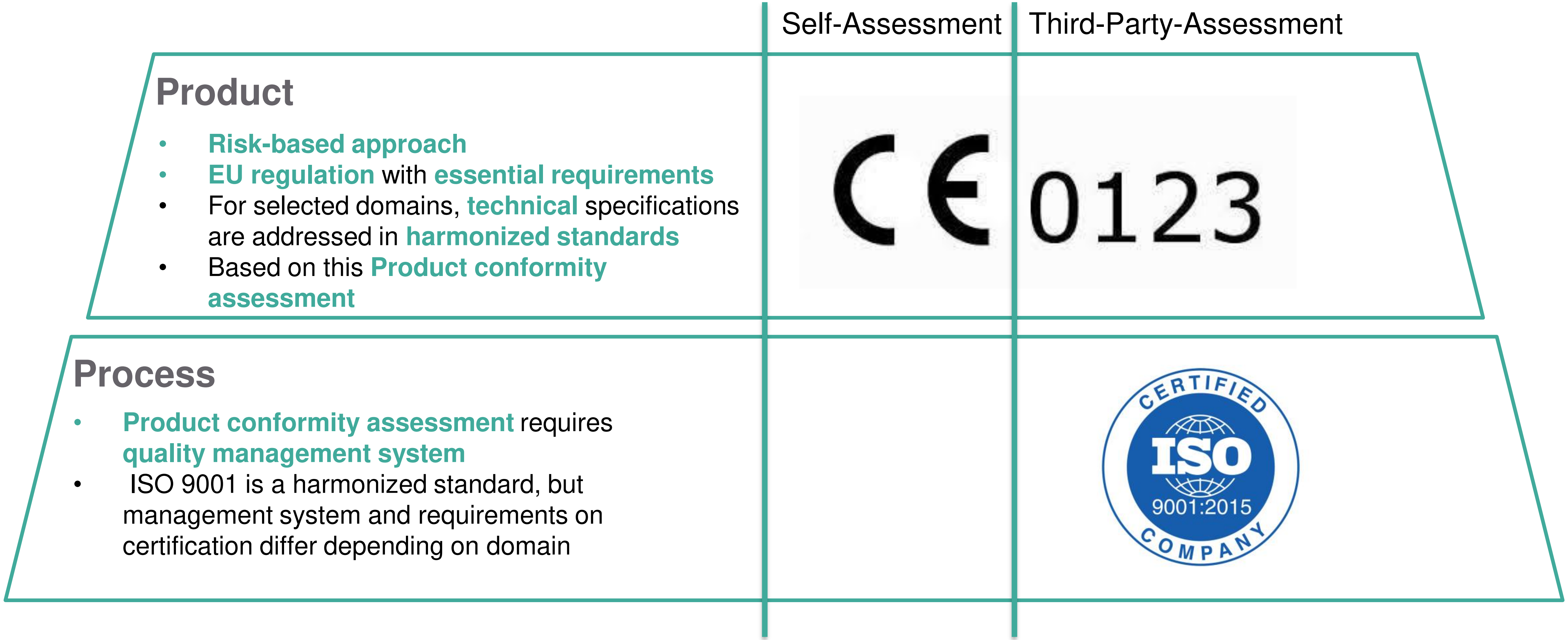
TIMELINE FOR COMPLIANCE

15.09.2022	Legislative proposal by the European Commission
19.07.2023	Council reaches common position.
19.07.2023	Start of trilogue negotiations with Parliament
T0	Regulation is adapted
(T0+12M	Reporting of vulnerabilities within 12 months)
T0+24M	Adaptation period for new requirements
(T0+36M	Full implementation including vulnerability and incident reporting)

CYBER RESILIENCE ACT IN THE EUROPEAN REGULATORY FRAMEWORK



EUROPEAN APPROACH TO REGULATION



Self-Assessment

Third-Party-Assessment

Product

- **Risk-based approach**
- **EU regulation** with **essential requirements**
- For selected domains, **technical** specifications are addressed in **harmonized standards**
- Based on this **Product conformity assessment**

Process

- **Product conformity assessment** requires **quality management system**
- ISO 9001 is a harmonized standard, but management system and requirements on certification differ depending on domain

EUR-Lex - 52016XC0726(02) - EN - EUR-Lex (europa.eu)

Proposal 2022/0272(COD) “Cyber Resilience Act”

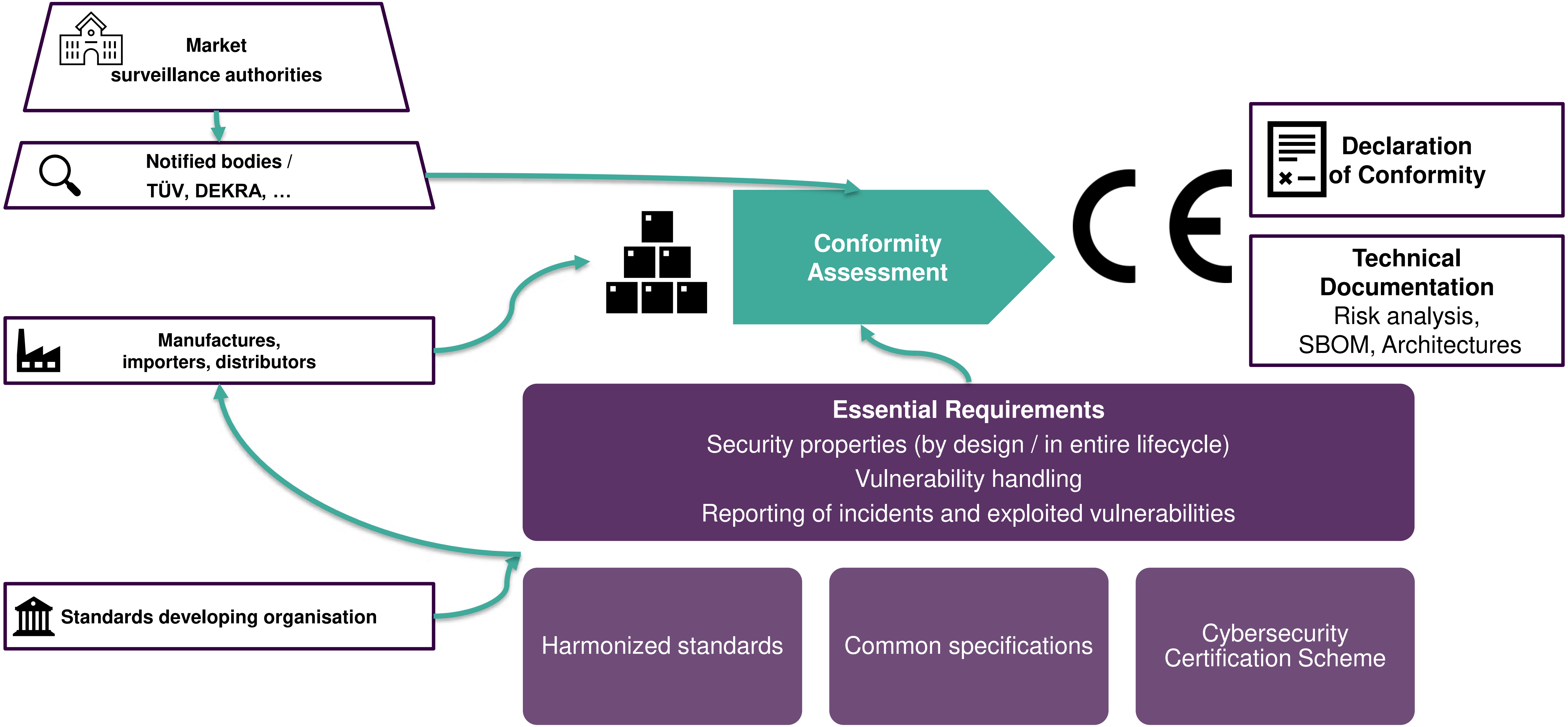
Regulation 2019/881 “Cybersecurity Act”

Proposal 2020/0359/(COD) “NIS2”

Regulation 765/2008 “CE marking”

Regulation 768/2008/EC “conformity assessment procedures”

FRAMEWORK



Market surveillance authorities

Notified bodies / TÜV, DEKRA, …

Manufactures, importers, distributors

Standards developing organisation

Conformity Assessment

Declaration of Conformity

Technical Documentation
Risk analysis,
SBOM, Architectures

Essential Requirements
Security properties (by design / in entire lifecycle)
Vulnerability handling
Reporting of incidents and exploited vulnerabilities

Harmonized standards

Common specifications

Cybersecurity Certification Scheme

CYBER RESILIENCE ACT - SUMMARY

Goals

Enhance cybersecurity and resilience within the EU.

Protect businesses and consumers from cyber threats.

Establish common cybersecurity standards for digital products.

Scope

Applies to manufacturers and retailers of products with digital elements.

Products whose use involves direct or indirect data connections.

Covers hardware, software, and IoT devices.

Core Requirements:

Risk assessments and vulnerability management throughout the product lifecycle.

Automatic security updates by default (with user opt-out option).

Critical products must undergo external audits.

Incident reporting

CYBERSECURITY BY DESIGN

CRA – AIT offers

AIT SOLUTIONS FOR CRA COMPLIANCE

Encryption Support: Advanced encryption algorithms and solutions to enhance data security.

Training & Exercises: Comprehensive training programs and cyber range exercises for team preparedness.

Product Testing: Rigorous testing services to ensure product compliance with CRA standards.

Risk Management with ThreatGet: Automated, model-based tool for proactive security by design, including certification support.

Security Monitoring with ÆCID: Cutting-edge Automatic Event Correlation for real-time incident detection and response.

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

THANK YOU!

Christoph Schmittner,