Security Testing

DEKRA

100 YEARS SECURING THE FUTURE 1925 – 2025

Cybersecurity Asset Owners

- NIS2
- CRA
- IEC 62443/ISO 27001

Todays Topics

1 DEKRA Cybersecurity

2 Overview: Cybersecurity

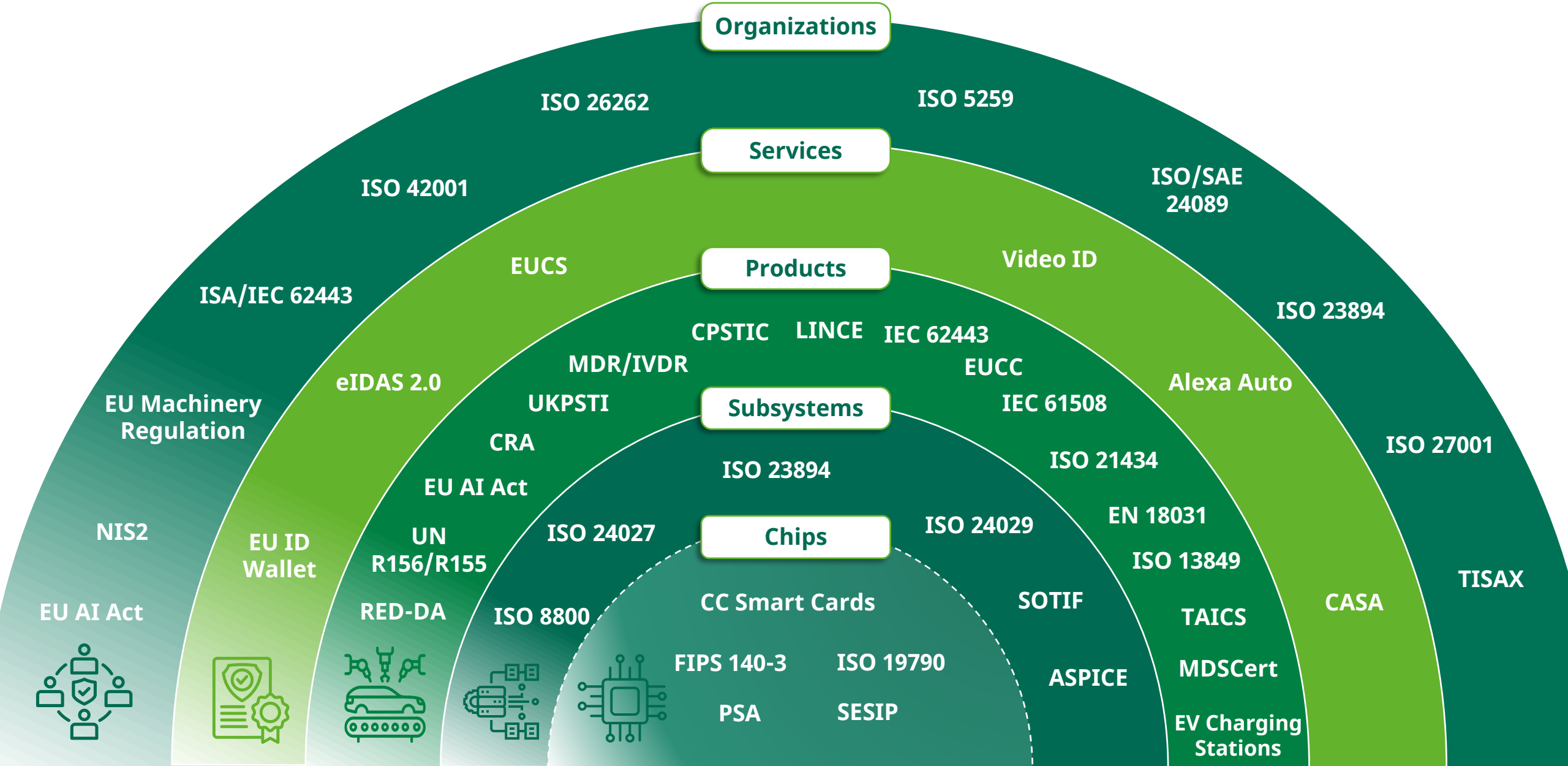
3 Overview: NIS2

4 NIS2: How Asset Owners can utilize IEC 62443

GLU Cybersecurity

100 YEARS SECURING THE FUTURE 1925 – 2025

Our Holistic Approach



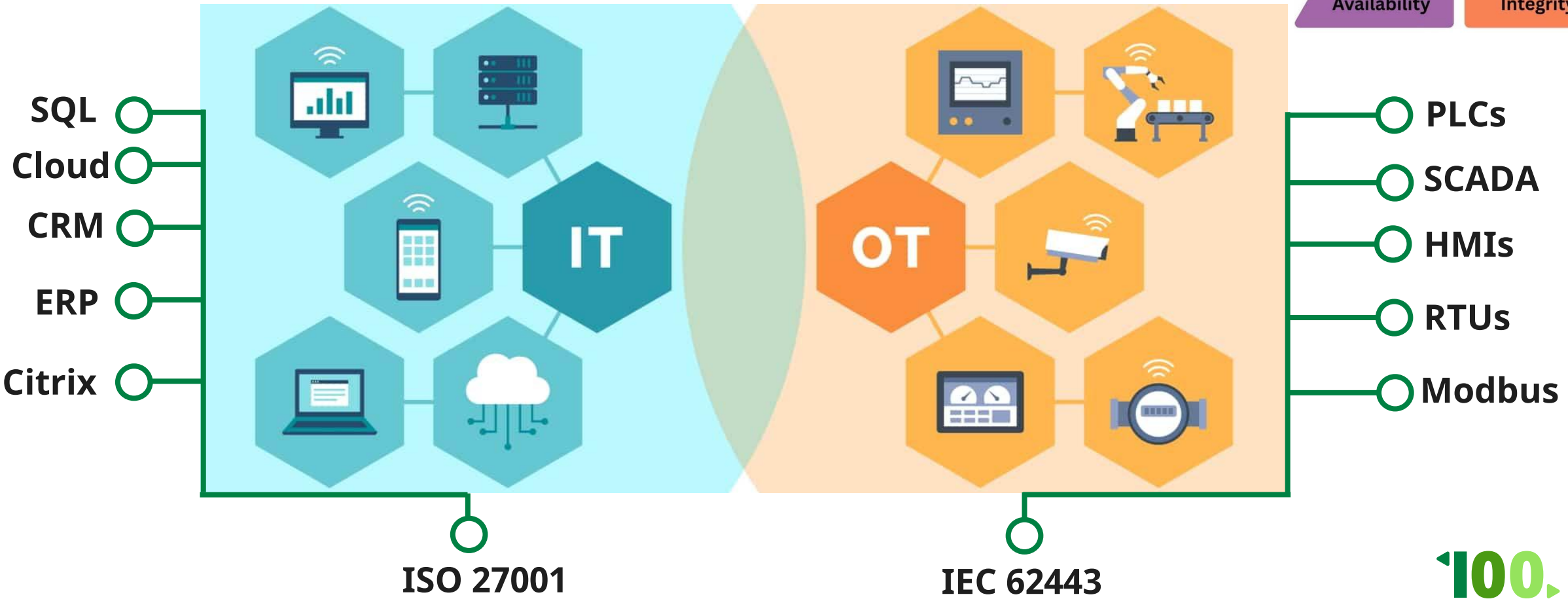
Overview: Cybersecurity

Cybersecurity is the practice of protecting computers, networks, data, and systems from digital attacks, unauthorized access, or damage. The goal is to **ensure confidentiality, integrity, and availability** of information.

- **Confidentiality:** Keeping information secret and accessible only to authorized people.
  Example: Using passwords, encryption, and access controls.
- **Integrity:** Ensuring data isn't altered or tampered with
  Example: Checksums, digital signatures, and version control.
- **Availability:** Making sure systems and data are available when needed.
  Example: Backups, redundancy, and protection against DDoS attacks.

IT / OT

NIS2 – Both IT & OT

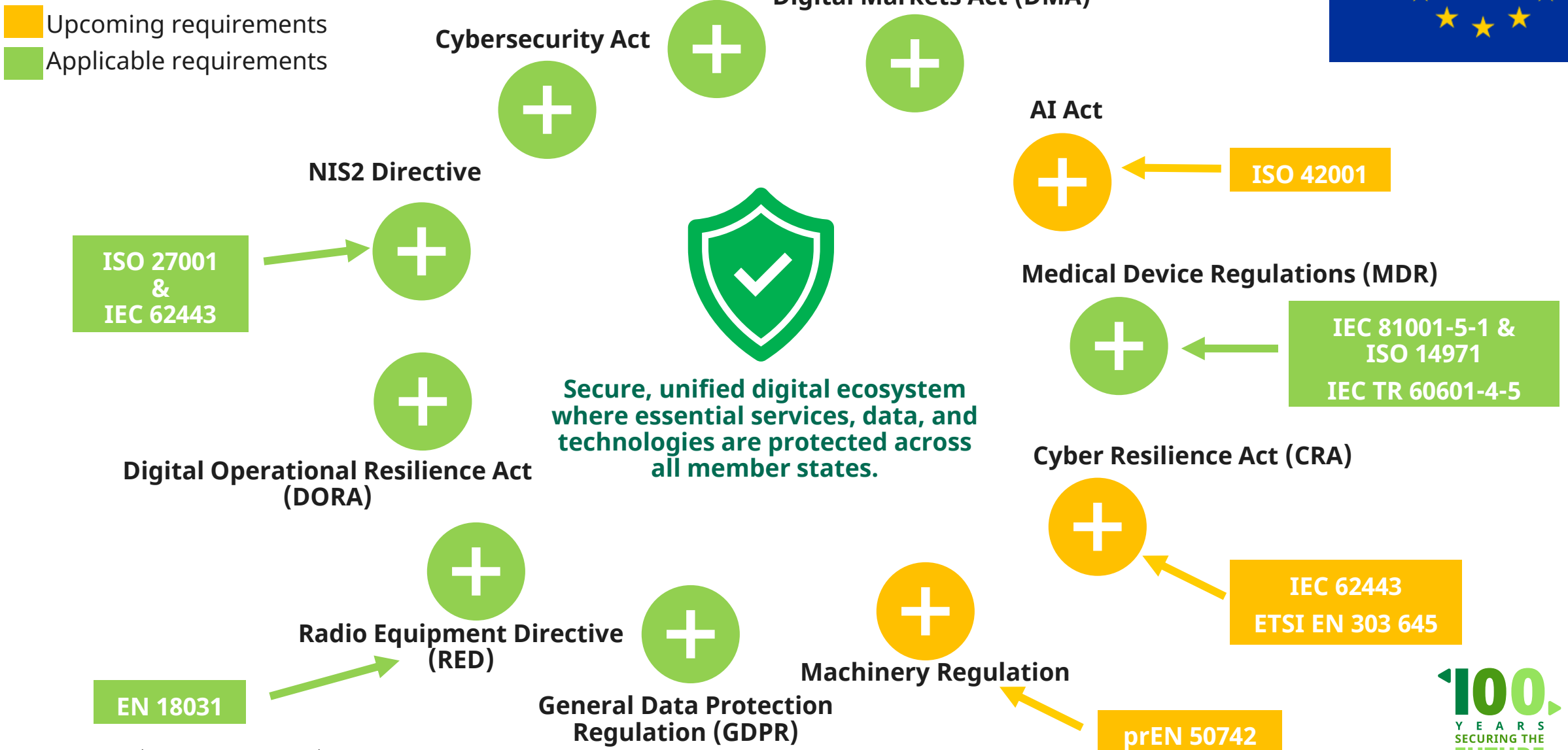


100 YEARS SECURING THE FUTURE 1925 – 2025

Different focus areas IT & OT

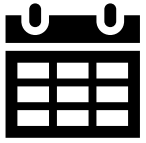
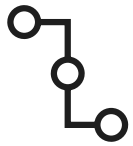
Aspect	IT (Information Technology)	OT (Operational Technology)
Primary Goal	Managing and securing data and information systems	Managing and securing physical processes and machinery
Typical Environment	Offices, Data centers, Cloud systems	Industrial plants, Manufacturing floors, Energy grids, Transportation infrastructure etc..
Main concern	Data confidentiality and integrity	Safety, System availability, Reliability
Examples	Email servers, ERP Systems, Databases	SCADA Systems, PLCs, Sensors, Industrial robots
Worst scenario	Data theft, stopping business processes, Reputational damage	Explosions, Fatalities, Equipment failures, environmental damage
Recovery time	Hours/Days	Weeks or months

EU Cybersecurity Regulations suite



EU Regulations connections/focus

In relation to CRA

	Cyber Resilience Act	RED-DA	NIS2	Machinery Regulation	AI Act
Requirements 	Cybersecurity requirements for hardware and software products with digital elements	Cybersecurity requirements for wireless and radio devices (Direct or Indirect)	Cybersecurity risk management measures and reporting obligations for organizations	Safety and Cybersecurity requirements for machinery and related products	Cybersecurity aspects of artificial intelligence, focusing on high-risk AI systems
Regulated entities 	Manufacturers, distributors, and importers of products with digital elements in the EU **(CE-Mark)**	Manufacturers of connected devices such as Smartphones, IoT devices **(CE-Mark)**	Operators of important and essential services in the EU	Manufacturers, importers, and distributors of machinery in the EU **(CE-Mark)**	AI developers, providers, and deployers in the EU **(CE-Mark)**
Compliance deadlines 	Reporting obligations **11 September 2026** Fully applicable **11 December 2027**	Fully applicable: **1 August 2025**	Fully applicable: **17 October 2024** *(Pending national implementation)*	Fully applicable: **20 January 2027**	AI Literacy requirements & Ban of unacceptable risk AI systems: **2 February 2025** Fully applicable: **2 August 2026**
Relation to CRA 		Both require security-by-design; RED-DA covers radio equipment, while the CRA applies to all digital devices with stronger focus on secure development.	NIS2 addresses cybersecurity at the organizational level, whereas the CRA focuses on secure products and systems. Their requirements are interconnected and mutually impactful.	Focuses on machinery safety and ties closely to functional safety. The CRA has a broader scope across all digital products, with some overlap — the two complement each other.	AI act and CRA mandate cybersecurity or robustness for AI-enabled products. The EU AI Act takes a holistic approach specifically to AI, while the CRA applies broadly to all digital products.

Overview: CRA

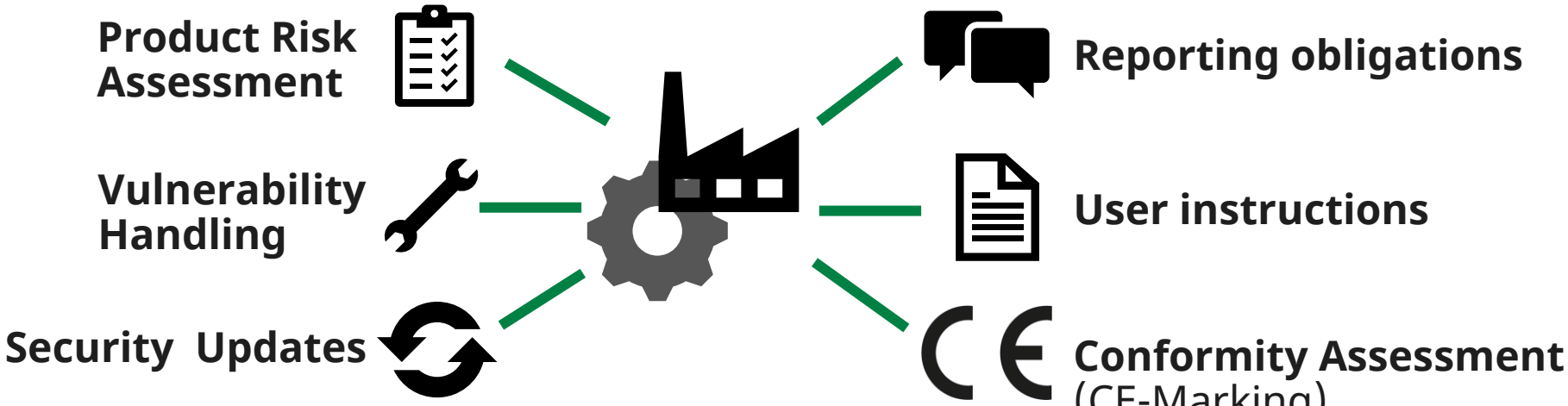
Cyber resilience Act

Cyber Resilience Act (CRA)

What is Cyber Resilience Act?

- European regulation introducing mandatory Cybersecurity requirements for all products with **Digital Elements**.
- Including their **building blocks**: **Hardware** and **Software** and their **remote data processing solutions** (Back-end/Cloud).

Manufacturers need to ensure **cybersecurity throughout** the **entire product lifecycle**



Products out of scope

Services
(incl. Standalone SaaS, Websites, Web-based)
NIS2

Non-commercial products
(Hobby products)

Products that fall under:
MDR, UNECE R155…
(Cars, Medical devices, Marine equipment)

CRA Requirements on manufactures

Development and after-sales services

- Assess a **product cybersecurity risks** and **requirements** in detail at all stages of development
- **Conduct regular audits/tests** and **evaluations** to verify the security of the products **during support period**
- Ensure that **3rd parties** (e.g. suppliers) and **open source components** do not **compromise product security**
- Track product components and vulnerabilities and create a **Software Bill of materials**
- Products are support for **minimal 5 years**

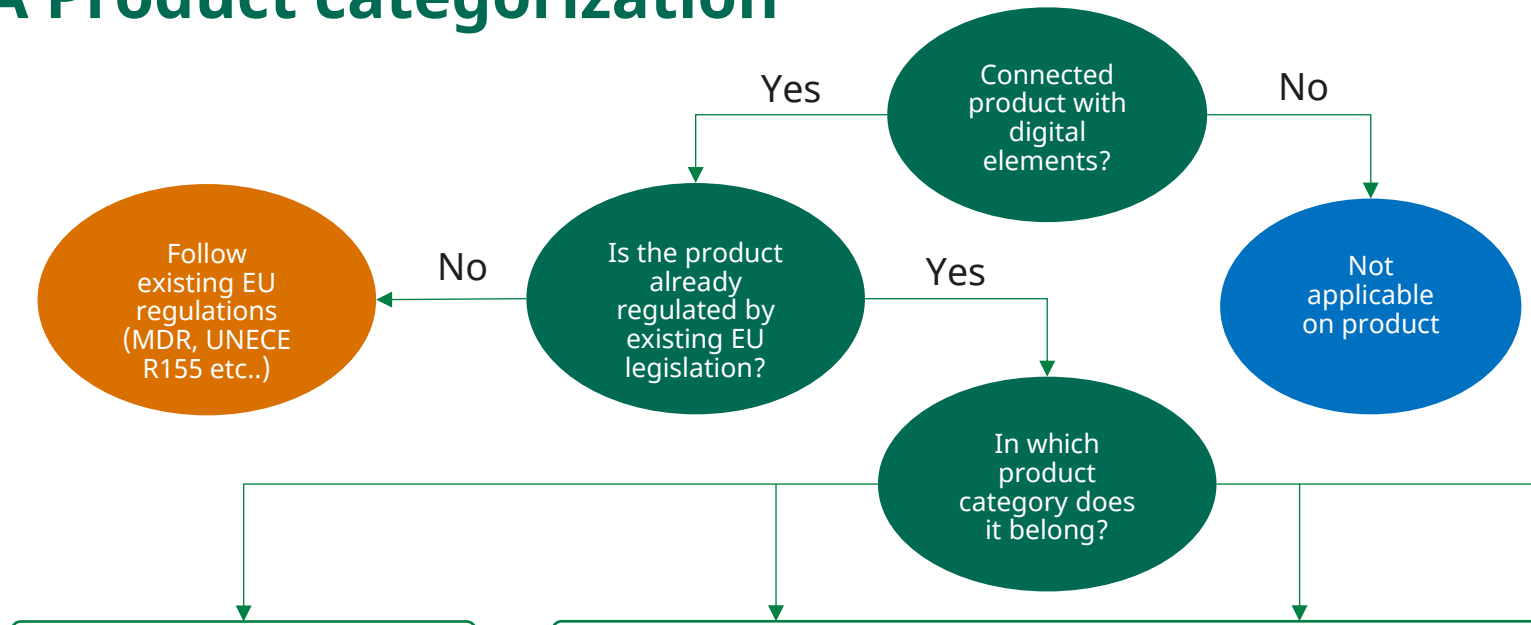
Vulnerability management

- Suppliers need processes for **managing vulnerabilities**
- Suppliers need a platform for **communication of vulnerabilities**
  - EU Central reporting point (ENISA)
  - For customers to report them
- If possible automated security updates
- Vulnerabilities handling is required at **11 September 2026**

Vulnerability handling requirements

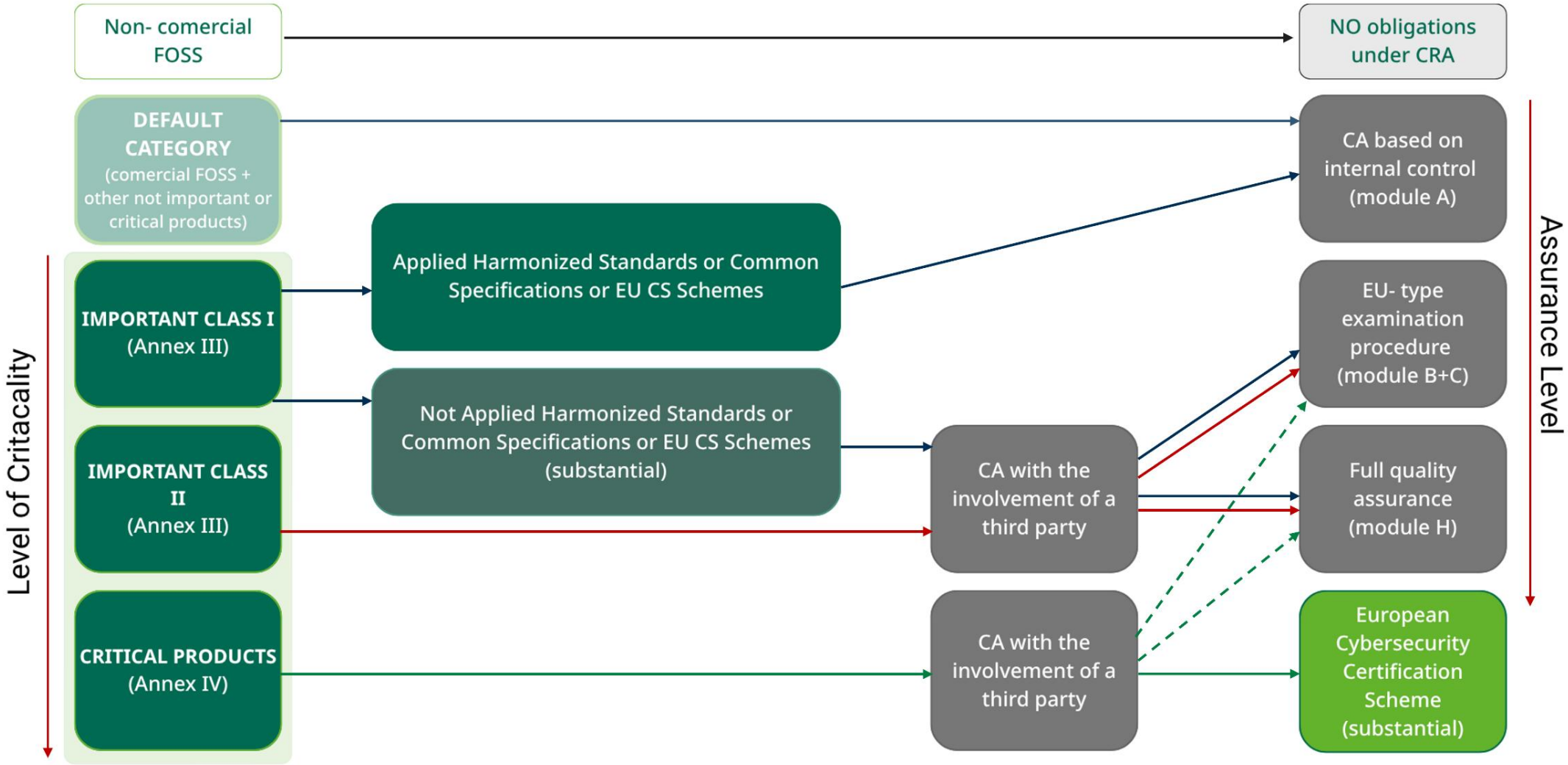
- Identify and document dependencies and vulnerabilities, including SBOM
- Test the security of digital products
- Coordinated vulnerability disclosure policy
- Mechanisms allowing the secure updating
- No known vulnerabilities and address vulnerabilities without delay
- Publicly disclose information about fixed vulnerabilities
- Facilitate the sharing of information about potential vulnerabilities
- Patches are delivered without delay, free of charge and with advisory messages

CRA Product categorization



90% of products	10% of products		
Default category	**Critical "Class I"**	**Critical "Class II"**	**Critical Products**
No special cybersecurity features, no significant negative impacts	Basic cybersecurity function or function with moderate risk of adverse impacts	Enhanced cybersecurity capability or higher risk of harmful impact capabilities	Are critical to cybersecurity and carry significant risk
▪ Games ▪ Photo editing ▪ Word processing	▪ Password managers ▪ Network interfaces ▪ Firewalls	▪ Operating systems ▪ Industrial Firewalls ▪ Secure elements	▪ Smart meter gateways ▪ Hardware devices with security boxes

CRA Compliance check



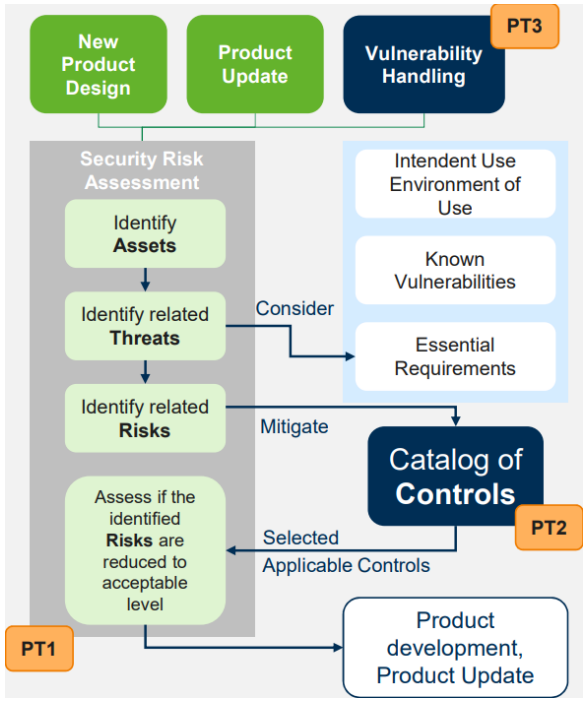
Current status Standardizations

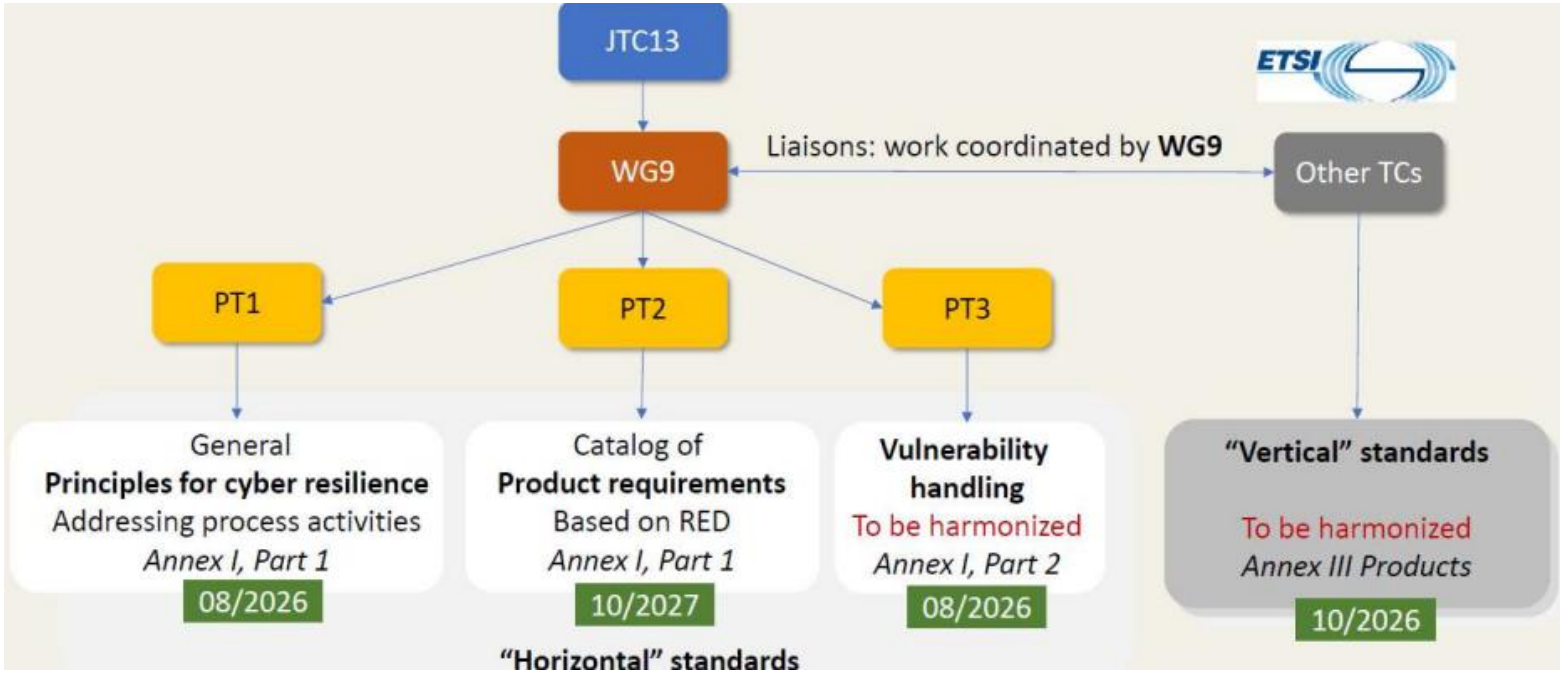
Overview

CEN-CENELEC will develop **3 horizontal standards** that will focus on:

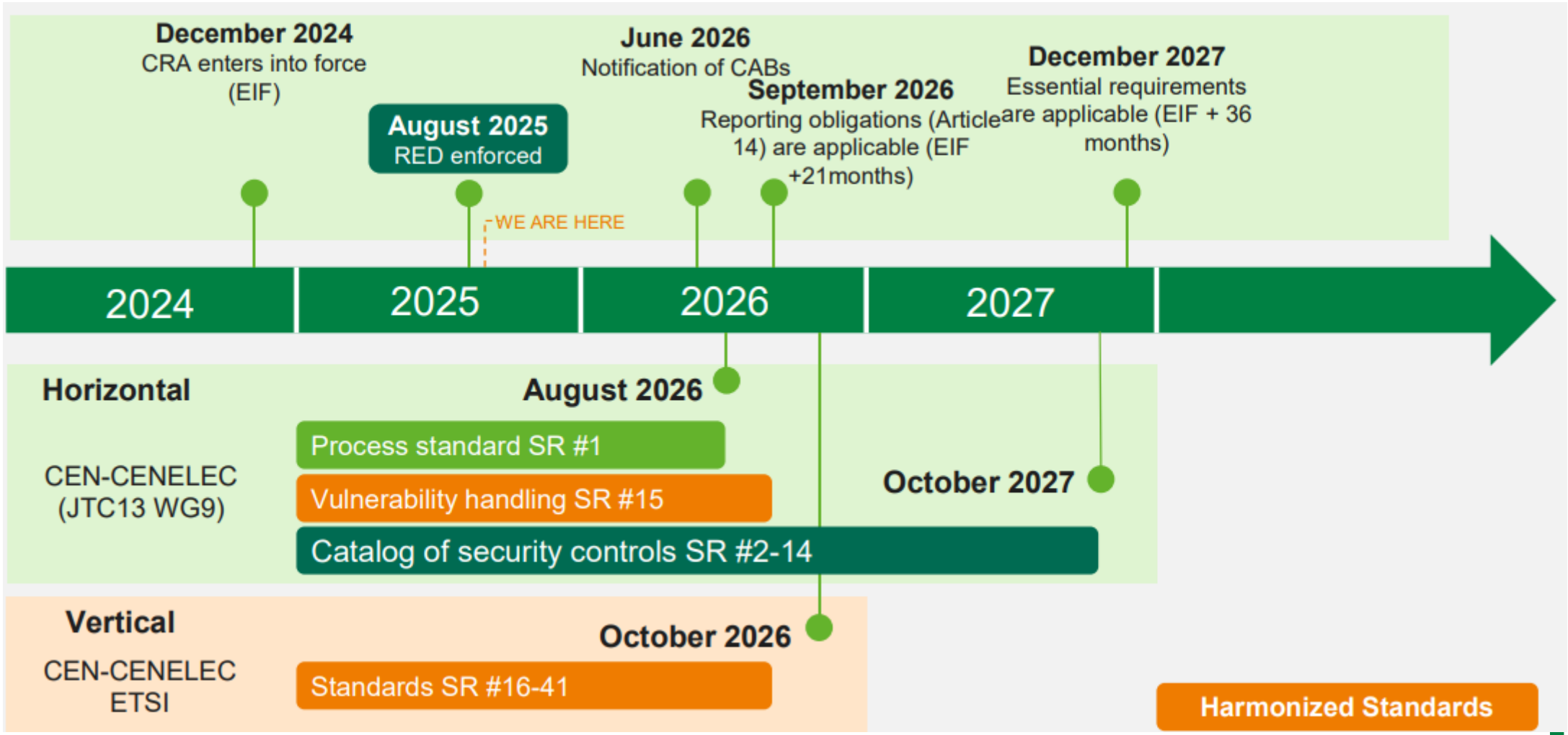
- **PT1**: Total product lifecycle
- **PT2**: Basic product security requirements
- **PT3**: Vulnerability handling

ETSI will develop **41 vertical product specific standards** with additional requirements per product





Timeline CRA

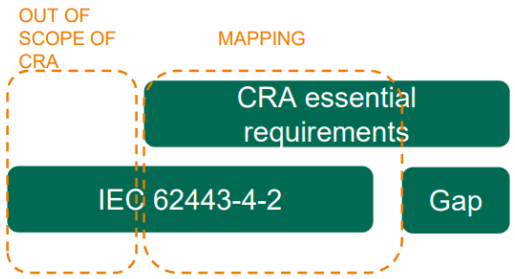


DEKRA compliance proposal for CRA with no harmonized standards 1/2

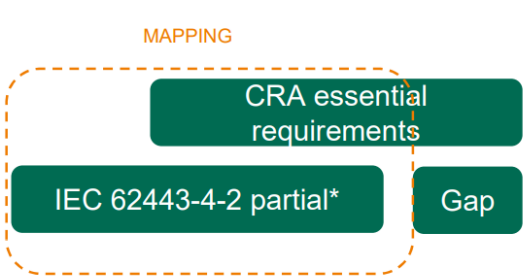
Industrial manufacturers

In the absence of harmonized standards, DEKRA recommends applying **IEC 62443-4-1** and **-4-2** to achieve conformity ahead of regulation enforcement.

- **IEC 62443-4-1** for compliance with SDLC requirements
- **IEC 62443-4-2** for compliance with product requirements, mapping with Essential requirements of CRA



For products intended to comply with IEC 62443-4-2 certification.



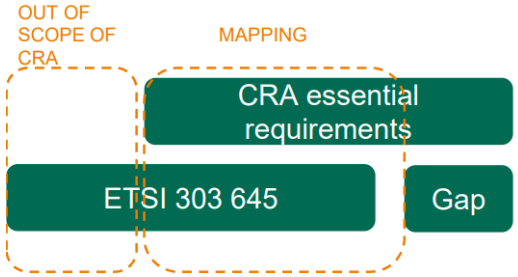
For products **NOT** initially intended to comply with IEC 62443-4-2.

** partial compliance can be reused if IEC 62443-4-2 certification is required afterwards.*

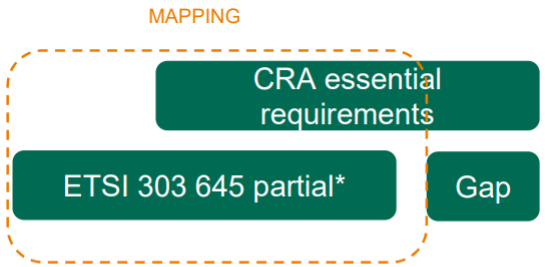
Consumer IoT manufacturers

As harmonized standards are still in development, DEKRA recommends using **ETSI EN 303 645** to demonstrate conformity for consumer IoT products and ensure timely compliance.

- **ETSI EN 303 645** for compliance with product requirements, mapping with Essential requirements CRA
- **ETSI EN 303 645** complemented with **IEC 62433-4-1** for compliance with SDLC requirements



For products intended to comply with ETSI 303 645 certification.



For products **NOT** initially intended to comply with ETSI 303 645.

** partial compliance can be reused if ETSI 303 645 certification is required afterwards.*

DEKRA compliance proposal for CRA with no harmonized standards 2/2

Pilot program

Pilot program overview

Program to close the gap and show compliance for the upcoming Cyber resilience Act. The program will include:

- **1 Hour workshop** with certificate of attendance
- **Categorization** for up to **3 products** (Anex III & IV)
- **Checklist for compliance** (Risk assessment, SDLC, Vulnerability monitoring)
- **Evaluation according** to **draft harmonized standard**, or **essential requirements** for **1 product**
- Attestation of Conformity (AoC)

- **Valid until June 2026**
- Limited to 50 entries
- 1 Pilot per customer

Other DEKRA Services

DEKRA holds **accreditation** and can offer **CB certificates** for:

- **ETSI EN 303 645**
- **IEC 62443 (-4-1, -4-2, -3-3, -2-4)**

DEKRA Can also support with training/workshops

Expected DEKRA Services

	Risk Assessment	SDLC	Product	Continuos Monitoring
Training	✓	🔨	🔨	✓
Testing	✗	✗	✓	🔨
Assessment	🔨	✓	🔨	✗
Certification	✗	✓	✓	✗

Overview: NIS2

Cyberbeveiligingswet (NL)

NIS2

What is Network and Information Systems (NIS2)?

- European Union law aimed at strengthening cybersecurity across member states by setting stricter security requirements and **mandatory incident reporting** for a wider range of companies, especially those in **critical** and **important sectors**. It expands upon the original NIS directive and **enhances enforcement**, including significant fines for non-compliance and **personal liability** for executives

NIS2 overview objectives

- Standard set of cybersecurity requirements across all EU members
- Stronger enforcement measures
- Expended scope of original NIS including more sectors
- Affected sectors responsible for their own cybersecurity levels
- Stricter incident reporting obligations
- Supply-chain cybersecurity requirements
- Better collaboration and information sharing between member states
- NIS2 basis for each member state that can be expended on

NIS2 requirements can differ in each different EU member state

Who is affected by NIS2?

Essential Business Sectors

Energy
- Electricity
- Gas
- Oil
- Hydrogen
- District Heating & Cooling

Transport
- Air
- Rail
- Water
- Road

Health
- Healthcare Providers
- Pharmaceutical Industry

Space

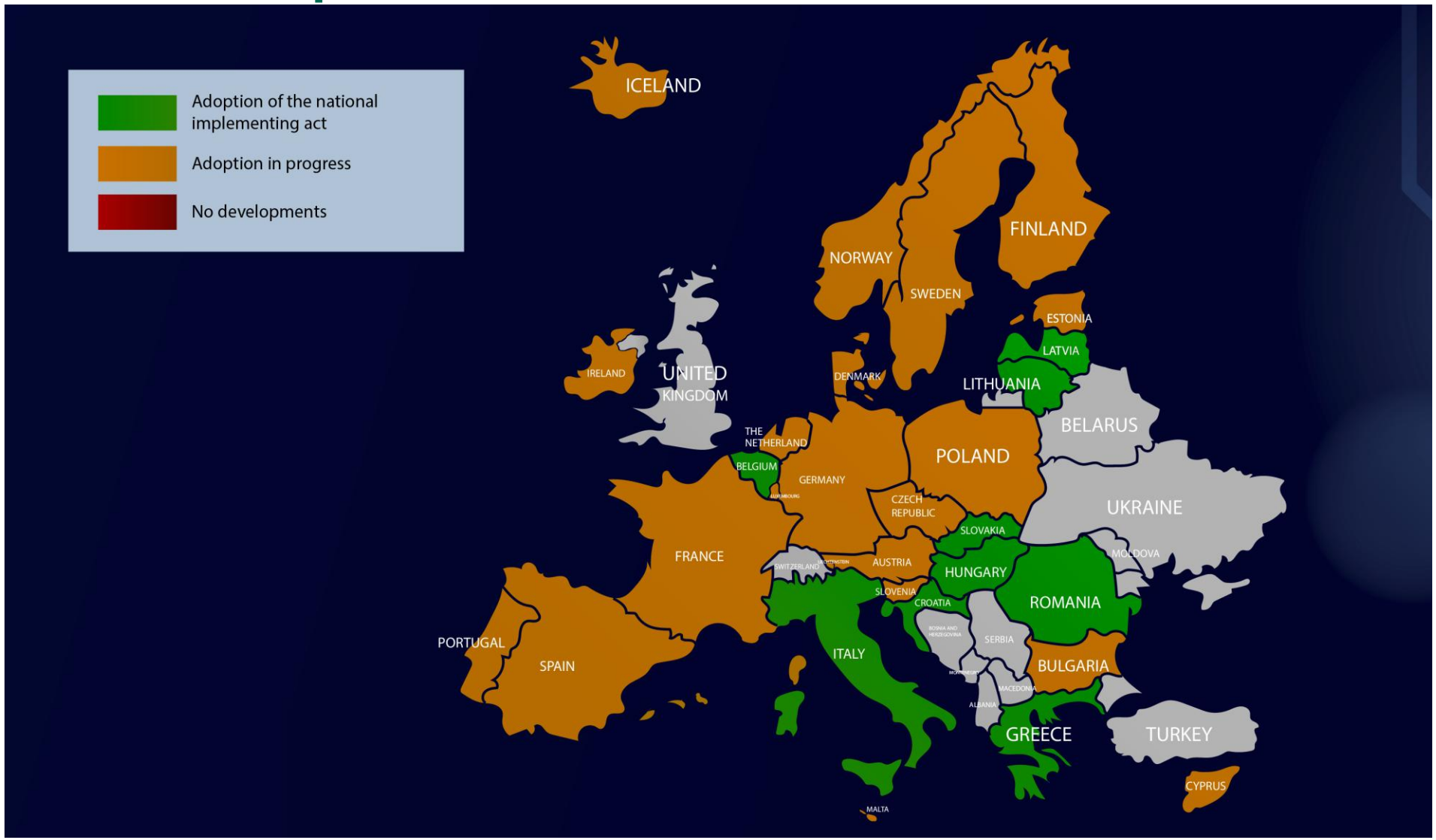
- **Drinking Water**
- **Waste Water**
- **Public Administration**
- **Digital Infrastructure**
- **Banking**
- **Financial Market Infrastructures**
- **ICT Service Mgmt (B-to-B)**

Important Business Sectors

- **Postal & Courier Services**
- **Waste Management**
- **Digital Providers**
  - Online Marketplaces
  - Online Search Engines
  - Social Networking Service Platforms
- **Chemicals**
  - Manufacture, Production & Distribution
- **Food**
  - Production, Processing & Distribution
- **Research**

Manufacturing
- Manufacture of Medical Devices & *In Vitro* Diagnostic Medical Devices
- Manufacture of Computer, Electronic & Optical Products
- Manufacture of Electrical Equipment
- Manufacture of Machinery & Equipment n.e.c.
- Manufacture of Motor Vehicles, Trailers & Semi-Trailers
- Manufacture of Other Transport Equipment

Status of NIS2 implementation across the EU



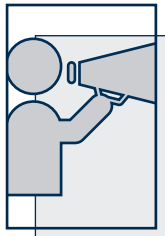
Source: https://nis2cybersecurity.org/about-nis2/

NIS2 requirements for businesses

Main commitments

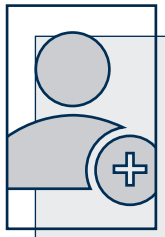
Duty to care

Organizations must take appropriate **technical and organizational security measures** to manage cyber risks, risk management, access control, incident response, and business continuity.



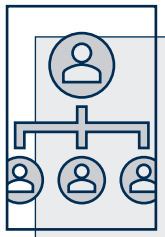
Duty to report

Significant **cyber incidents must be reported quickly** to the national authority or CSIRT (usually within 24 hours for early warning, 72 hours for details).



Duty to register

Entities covered by NIS2 must **register with the national competent authority**, providing details such as their services, contact points, and sector classification.



Management Accountability

Company management (**CISO**) is **personally accountable** for cybersecurity compliance. They must approve, oversee, and can be held **liable** for failing to implement proper measures.

Summary NIS2 Requirements for Businesses

Requirements for Management Bodies

- Appoint a CISO (Chief Information Security Officer) that has oversight over all Cybersecurity processes/Assets
- Oversee both the IT (Information Technology) and OT (Operational Technology) teams and secure both information systems and assets
- Approval and oversight of Cybersecurity Risk Mitigation measures (liability reason)
- Mandatory Cybersecurity training

Stricter Oversight from Authorities

- Mandatory registration with National Cybersecurity authority
- Regular audits (Including onsite)
- Financial penalties if not in compliance:
  - Essential Sector: up to 10 Million or 2% Worldwide annual turnover
  - Critical Sector: Up to 7 million or 1,4% Worldwide annual turnover

Reporting Obligations to Authorities

- Early Warning: Within 24 hours of discovering a *Significant incident* (e.q. High impact, Large extent)
- Detailed Report: Within 72 hours
- Final Report: Within one month or upon incident resolution

Practical Advice for NIS2 Compliance

Check IT – OT

- Check if your organization only has IT or also OT assets

GAP Analysis

- Make GAP from all NIS2 regulations (Countries) your organization is active and needs to comply.

Risk assessment

- Identify all the risks and make a mapping of requirements based on the GAP from countries and needs for the sector/organization.

Implement recommended standards

- If IT start with ISO 27001 and with OT check the IEC 62443-2-1 and IEC 62443-2-4 standards to fill the requirements for the Risk assessment

Prepare extended statement of Applicability (SoA)

- which expends on the shorter SoA used in ISO 27001 by including NIS2 specific requirements and controls

Focus first on ISMS implementation

- Establish based of the ISO 27001 the ISMS and if OT assets needs to be included expand on the existing ISMS with IEC 62443

Standards for NIS2 compliance

IEC 62443 Framework

Roles (4)

- Asset Owner
- Maintenance Service provider
- Integration service provider
- Product Supplier

Policies and procedures

- IACS Security Management System (-2-1)
- Security Management Implementation Guide (-2-2)
- Patch Management Guidelines (-2-3)
- IACS Supplier Requirements (-2-4)

Systems

- Security Levels for Zones and Conduits (-3-2)
- System security Controls and Risk Levels (-3-3)

Components/products

- Security for Industrial automation and Control systems (-4-1)
- Technical Requirements for the Security of IACS components (-4-2)

OT

IT

NIS2

ISO 27001

Organizational controls (37)

- Establishing a security policy
- Defining roles and responsibilities
- Internal Risk Assessments
- Incident Response management

People controls (8)

- Application screening
- Security Awareness trainings
- Job-sensitive Access Controls

Physical controls (14)

- Securing physical locations
- Access Control Management
- Protecting against Natural Hazards

Technological controls (34)

- Network and Information Security Management
- Ensuring Availability, Integrity and Security of systems and data
- Software and Backup Management

How to demonstrate compliance?

Affected Sector?

Essential Entity

>250 employees or

>€ 50M. Annual turnover

Important entity

>50 - 249 employees or

>€ 10M – 50M. Annual turnover

Risk Assessment & GAP Analysis

Implement recommended standards & get certified

ISO 27001 / IEC 62443 certification

Certification by an accredited conformity assessment body demonstrates control

Implement recommendations and document and maintain them

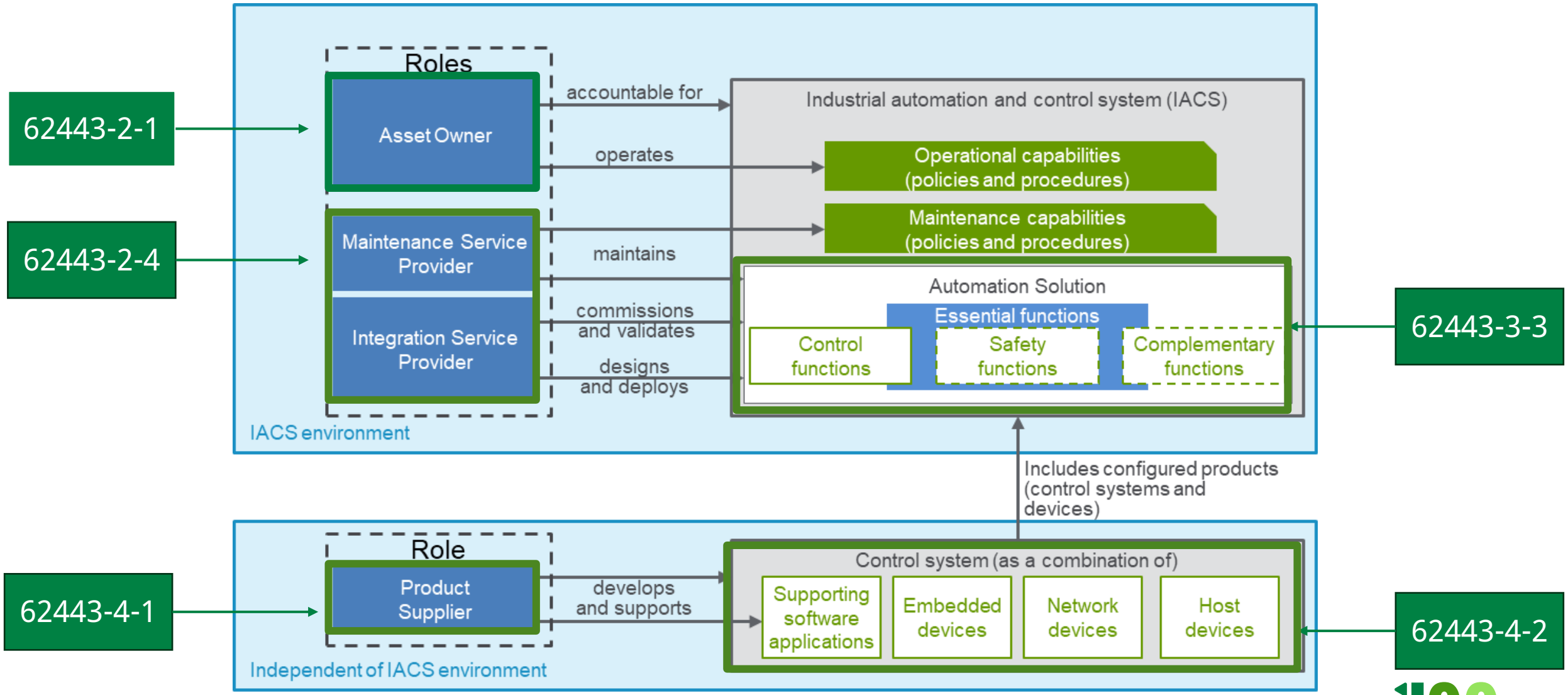
NIS2 conformity

Demonstrable conformity on closing the gaps identified in NIS2 Risk Assessment reports, and maintaining and continually improving the ISMS & IACS

NIS2: How Asset Owners can utilize IEC 62443

IEC 62443 Framework

IEC 62443 standard with certification scheme



IEC 62443-2-1

Overview

defines the requirements for setting up and maintaining an Industrial Automation and Control System (IACS) cybersecurity **management system** (Security Programs). It provides a **structured** approach to **governance**, **risk management**, and **continuous improvement** of **security** within **industrial environments**.

8 key security practices containing **87 individual process requirements**, **ensuring** that **organizations implement** a **systematic** and **sustainable approach** to industrial cybersecurity.

Purpose

stablishes a management-system foundation for industrial cybersecurity, comparable to an ISMS (ISO 27001) but focused on operational technology (OT). **Consistent**, **measurable**, and **auditable** cybersecurity **governance** across their **industrial environments**.

Benefits

- Align Key aspects CRA & NIS2
- Worldwide accepted Certificates
- Quality improvement on System design
- Specific Cyber resilience for OT environments
- Maturity levels

8 Security practices Asset Owner

- **Organizational security measures**
  ensure that the organization is prepared to adequately address IACS security.
- **Configuration management**
  ensure that the asset owner documents the IACS architecture, maintains an inventory of its hardware and software components and controls changes
- **Network and communications security**
  ensure that the IACS is protected from attacks conducted through the network and through communications capabilities
- **Component security**
  ensure that the IACS and its components are appropriately protected from attacks
- **Protection of data**
  ensure that data is protected from disclosure and tampering
- **User access control**
  ensure that users are assigned accounts that are used to control access to the IACS and its resources and commands.
- **Event and incident management**
  support detection, logging and analysis of security related events and compromises
- **System integrity and availability**
  ensure that the integrity and availability of the IACS are protected, and that the appropriate capabilities are present to recover the system to a previous state when necessary

IEC 62443-2-4

Overview

defines the security capabilities and processes required from **service providers**, such as **system integrators** and **maintenance contractors**, who **design**, **implement**, or **support** industrial automation and control systems (IACS).

12 key security practices comprising **124 individual process requirements**, ensuring that all **service activities** are performed in a **consistent**, **secure**, and **auditable** manner throughout the **system lifecycle**.

Purpose

Ensures that service providers **deliver**, **integrate**, and **maintain** industrial systems securely, reducing the risk of introducing vulnerabilities during deployment and operations, and enhancing both system quality and trustworthiness.

Benefits

- Align Key aspects CRA & NIS2
- Worldwide accepted Certificates
- Quality improvement on System design
- Specific Cyber resilience for OT environments
- Maturity levels

12 Security practices service provider

- **Solution staffing**
  assignment of personnel by the service provider to Automation Solution related activities
- **Assurance**
  providing confidence that the Automation Solution security policy is enforced
- **Architecture**
  providing confidence that the Automation Solution security policy is enforced
- **Wireless**
  use of wireless in the Automation Solution
- **SIS (safety instrumented system)**
  integration of SIS into the Automation Solution
- **Configuration management**
  configuration control of the Automation Solution
- **Remote access**
  remote access to the Automation Solution
- **Event management**
  event handling in the Automation Solution
- **Account management**
  administration of user accounts in the Automation Solution
- **Malware protection**
  anti-malware software in the Automation Solution
- **Patch management**
  security aspects of approving and installing software patches
- **Backup/restore**
  security aspects of backup and restore

IEC 62443-4-1

Overview

It defines a structured framework to ensure that security is built in from the earliest **design** phase through **maintenance** and **decommissioning**.

8 key secure development practices, encompassing **47 individual process requirements**, that guide **manufacturers** and **developers** in creating trustworthy, resilient industrial products.

Purpose

Ensures that all vendors and developers of industrial products follow a **repeatable**, auditable, and **measurable** secure **development process** for IACS (OT) environments.

Benefits

- Align Key aspects CRA & NIS2
- Worldwide accepted Certificates
- Quality improvement on System design
- Specific Cyber resilience for OT environments
- Maturity levels

8 Secure Development practices

- **Security Management**

Establish and maintain a formal security management system for product development.

- **Specification of Security Requirements**

Identify and document security needs based on risk assessment and use cases.

- **Secure by Design**

Integrate security principles into architecture, design, and coding practices.

- **Secure Implementation**

Apply secure coding standards, vulnerability prevention, and verification during development.

- **Security Verification and Validation testing**

Test and verify that security functions work as intended and meet defined requirements.

- **Management of Security-Related Issues**

Detect, assess, and remediate vulnerabilities or security defects during development.

- **Security Update Management**

Define processes for delivering and maintaining security patches and updates throughout product life.

- **Security Guidelines and Documentation**

Provide customers and integrators with clear, accurate security configuration and usage instructions.

DEKRA Seals

Process

Yearly audits on basis of IEC 62443 (Roles) requirements. A subsection (10-20) of these requirements are being audited. The audit takes 2-days and will be remotely done.

Maturity

The seal shows the maturity level of the organization.

Benefits

- Transparent visibility to customers
- Yearly third-party check
- DEKRA branding
- Visible Maturity Level on seal
- High certainty for Maturity Level increase
- Accredited Cyber Trust seal

Thank you!

Boris Zandstra
Accountmanager Cybersecurity

Boris.zandstra@dekra.com
+31 6 25274739

Jurgen Rottjers
Industrial Cybersecurity Expert

jurgen.rottjers@dekra.com

innovating safety & security