

DEKRA/Onward CRA Compliance Service



About DEKRA

Established in

1925

to ensure **road safety** in connection with rapidly developing mobility.

Today, DEKRA stands for safety on the road, at work, and at home and offers a broad service portfolio, including qualified and independent expert services in 60 countries.



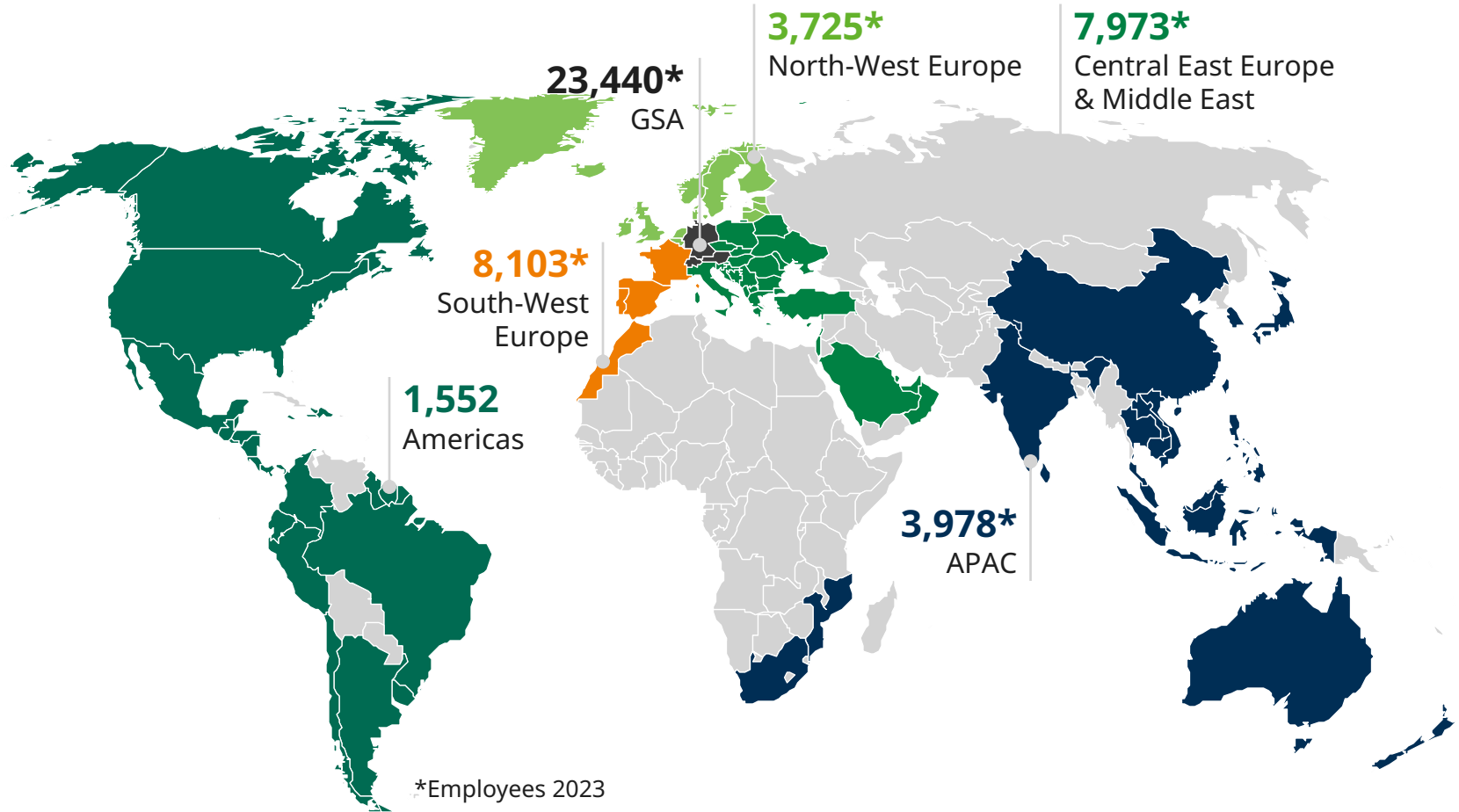
Safety expertise in 6 regions

in 60 countries



Services

-  Vehicle Inspection
-  Claims & Expertise
-  Digital & Product Solutions
-  Industrial Inspection
-  Audit
-  Advisory Services
-  Training
-  Personnel Services



About DEKRA Taiwan

DEKRA On the safe side

3
Legal entities



DEKRA Testing and Certification



DEKRA iST Reliability Service



Onward Security

6

Sites

TW HQ | HY IoT
LK EMC | HC IoV
DEKRA iST | Onward

Employees

580



4 Service Divisions

- | PRODUCT TESTING
- | ADVISORY & TRAINING SERVICES
- | INDUSTRIAL INSPECTION
- | AUDIT

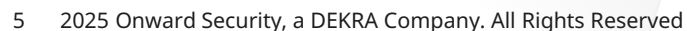
Our Mission

**“We ensure
safety, security
and sustainability”**

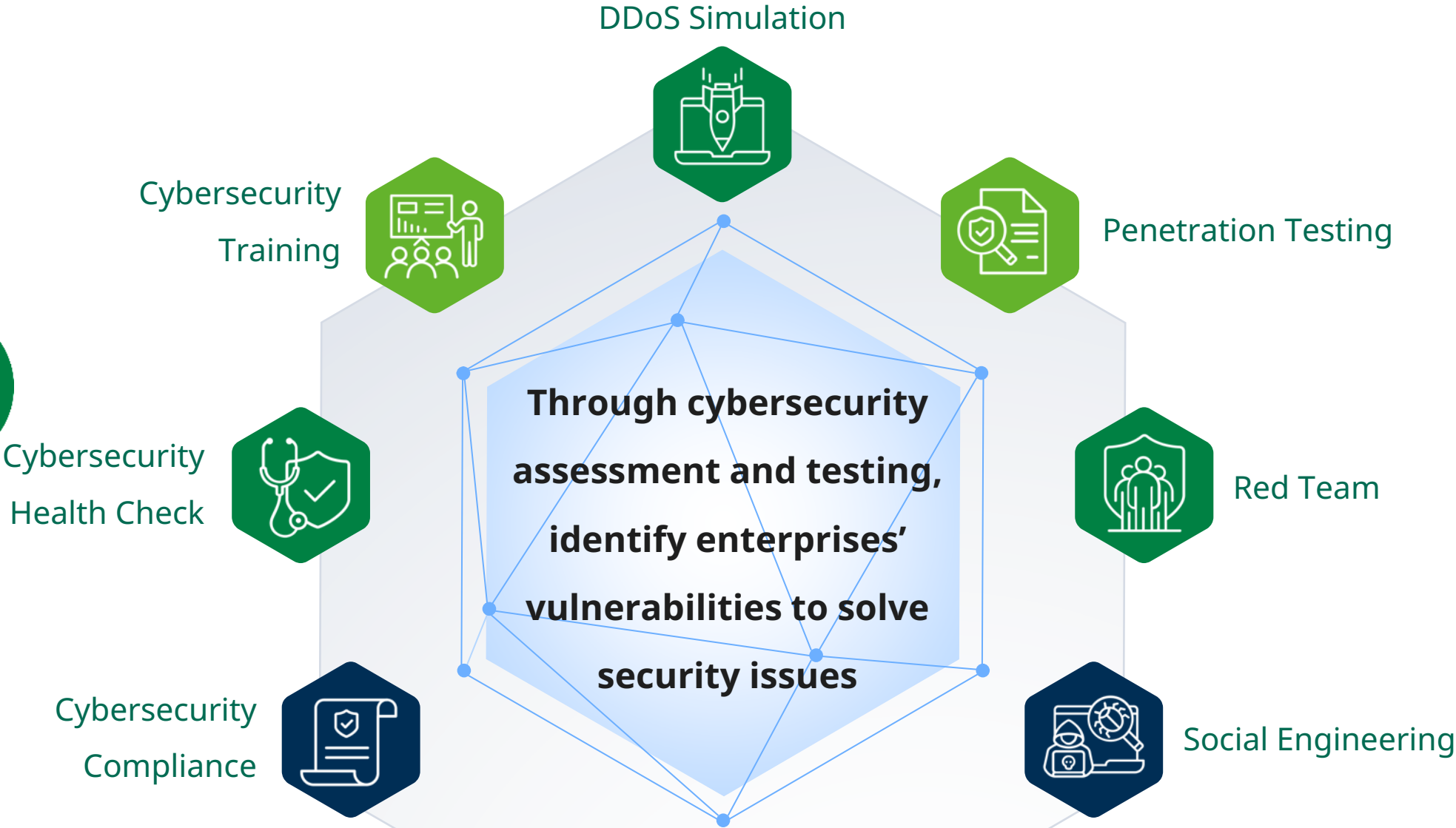


Our Vision

**“We will be the global partner for a safe,
secure and sustainable world”**



Enterprise Cybersecurity Services



Security Compliance Services

Secure-by-design, streamline cybersecurity compliance assessment



Gap Analysis

Review &
Comparison

Training

Assessment &
Improvement

Perfection

Audit &
Certification

- Automotive
- V2X
- ISMS
- PIMS
- AI
- ICT
- Cryptography
- Medical
- Data Protection
- System Security

Testing and Certification Services

Testing and Certification in 60+ countries

- Automotive
- Mobile App
- ICT
- IoT
- Medical
- Cryptography
- 5G
- Industrial
- SoC
- Telecom
- Drone



Cybersecurity Assessment Tools

HERCULE[⚡] SecSAM Security Assessment Management System for OSS



OSS Management



Product Risk Control

- ✓ Improve efficiency of vulnerability fix with CI/CD integration
- ✓ Manage vulnerability risk rating based on SBOM and CBOM structure
- ✓ Comply with global IoT security standards

**Meet IT and
Product
Security
Requirements**

HERCULE[⚡] SecDDoS DDoS Simulation System



Real Hacking Simulation



Cyber Threats Reduction

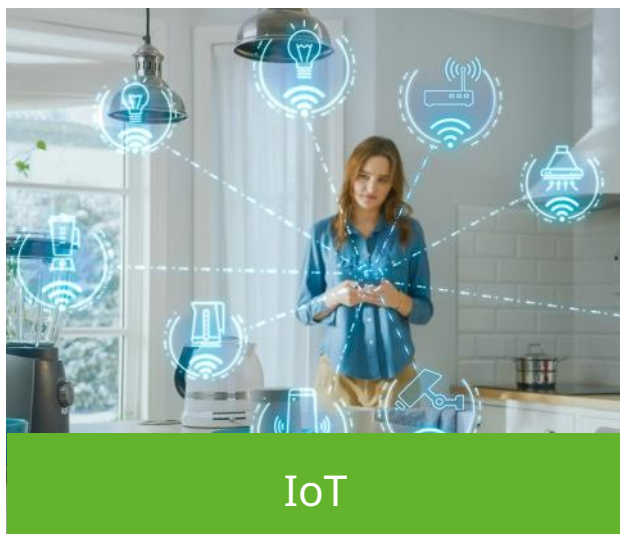
- ✓ Flexible testing options without time and location restrictions
- ✓ Instant feedback and analysis reports enable the system to respond to DDoS attacks effectively
- ✓ Pay according to usage to increase cost-effectiveness

Your Trusted Partner for IoT Cybersecurity

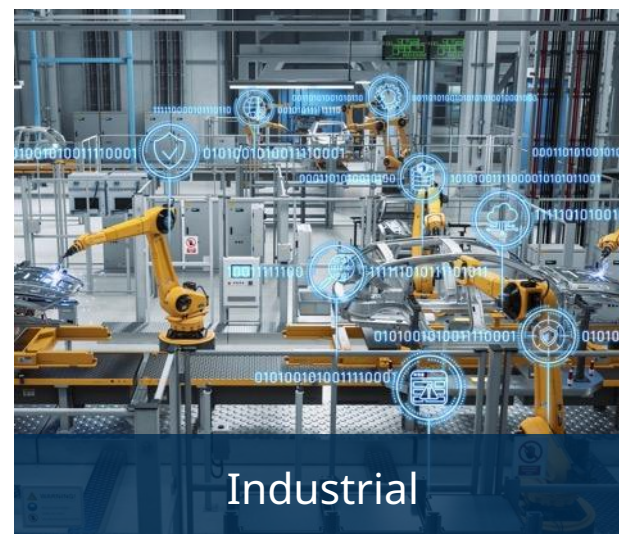
Realizing Ultimate Security | Global Testing and Certification in Action



Automotive



IoT



Industrial



Medical

Dedicated to IoT Product Security

- 200+ cybersecurity projects in IoT industry
- Tested 1000+ IoT product security

In-depth Cybersecurity Techniques

- Uncovered 50+ zero-day vulnerabilities (CVE)
- Discovered 3000+ IoT product vulnerabilities

Global Compliance and Certification Capability

- 500+ customers / 20+ countries certification obtained
- Compliance experience in Automotive, IoT, Industrial, and Medical sector

Portfolio of DEKRA CSH + Onward Security

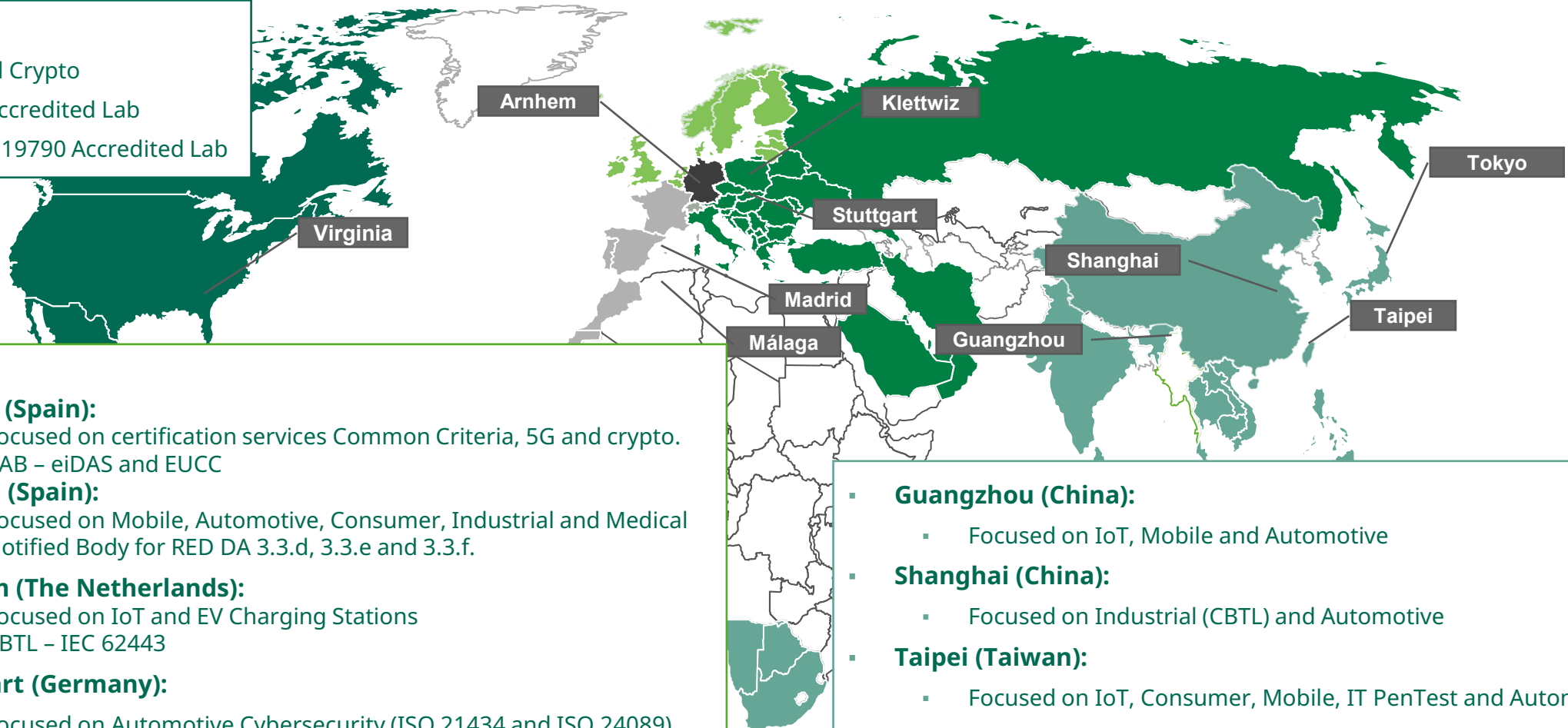


Application	SDO and Regulations	Services	Testing Tools
Automotive	- UNECE WP29 (R155 and R156) - OmniAir	- Assessment and Training - Product Security Evaluation - Automotive SPICE - ISO 21434 - ISO 24089 - TiSAX	- SecSAM (Security Assessment Management System for OSS) - SecDDoS (DDoS Simulation System)
AI	- EU AI Act - NIST - ENISA - OWASP - VDA QMC	- Readiness assessment - Compliance consulting (e.g., governance methodology/framework customization) - ISO 42001 Consulting (including training) - ISO 8800 Consulting (including training) - AI Model/Data Quality/Security Tests - Automotive SPICE v.4.0 Machine Learning Engineering (MLE) consulting (including training)	
IoT	- RED-DA - Cyber Resilience Act (CRA) - GSMA, PSTI - CSA-Singapore	- Product Security Evaluation (EN 18031) - Labelling Schemes (UK, Singapore, US) - Alexa Auto - Google's MASA program - US Cyber Trust Mark - SESIP, PSA	
ICT	- ICC - ENISA - Cybersecurity Act - NIST - FIPS	- Common Criteria / EUCC - NESAS / EU5G - Crypto - Lightweight Evaluations - Cloud Testing and Certification. (Google's CASA & EUCS)	
Industrial	- IECEE - ISASecure	- IEC 62443 - Product Security Evaluation	
Medical	- UL 2900 - EU-MDR/IVDR - FDA	- UL 2900-2-1 - MDR/IVDR Assessment - FDA Cybersecurity - IEC 81001-5-1, IEC 60601-4-5	

DEKRA CSH + Onward Security in Europe, APAC, and Americas

Virginia (US):

- Focused on ICT and Crypto
- Common Criteria Accredited Lab
- FIPS 140-3 and ISO 19790 Accredited Lab



- **Madrid (Spain):**
 - Focused on certification services Common Criteria, 5G and crypto.
 - CAB – eIDAS and EUCC
- **Málaga (Spain):**
 - Focused on Mobile, Automotive, Consumer, Industrial and Medical
 - Notified Body for RED DA 3.3.d, 3.3.e and 3.3.f.
- **Arnhem (The Netherlands):**
 - Focused on IoT and EV Charging Stations
 - CBTL – IEC 62443
- **Stuttgart (Germany):**
 - Focused on Automotive Cybersecurity (ISO 21434 and ISO 24089)
- **Klettwitz (Germany):**
 - Technical Office for UN R155 and UN R156

- **Guangzhou (China):**
 - Focused on IoT, Mobile and Automotive
- **Shanghai (China):**
 - Focused on Industrial (CBTL) and Automotive
- **Taipei (Taiwan):**
 - Focused on IoT, Consumer, Mobile, IT PenTest and Automotive
- **Tokyo (Japan):**
 - Focused on IoT



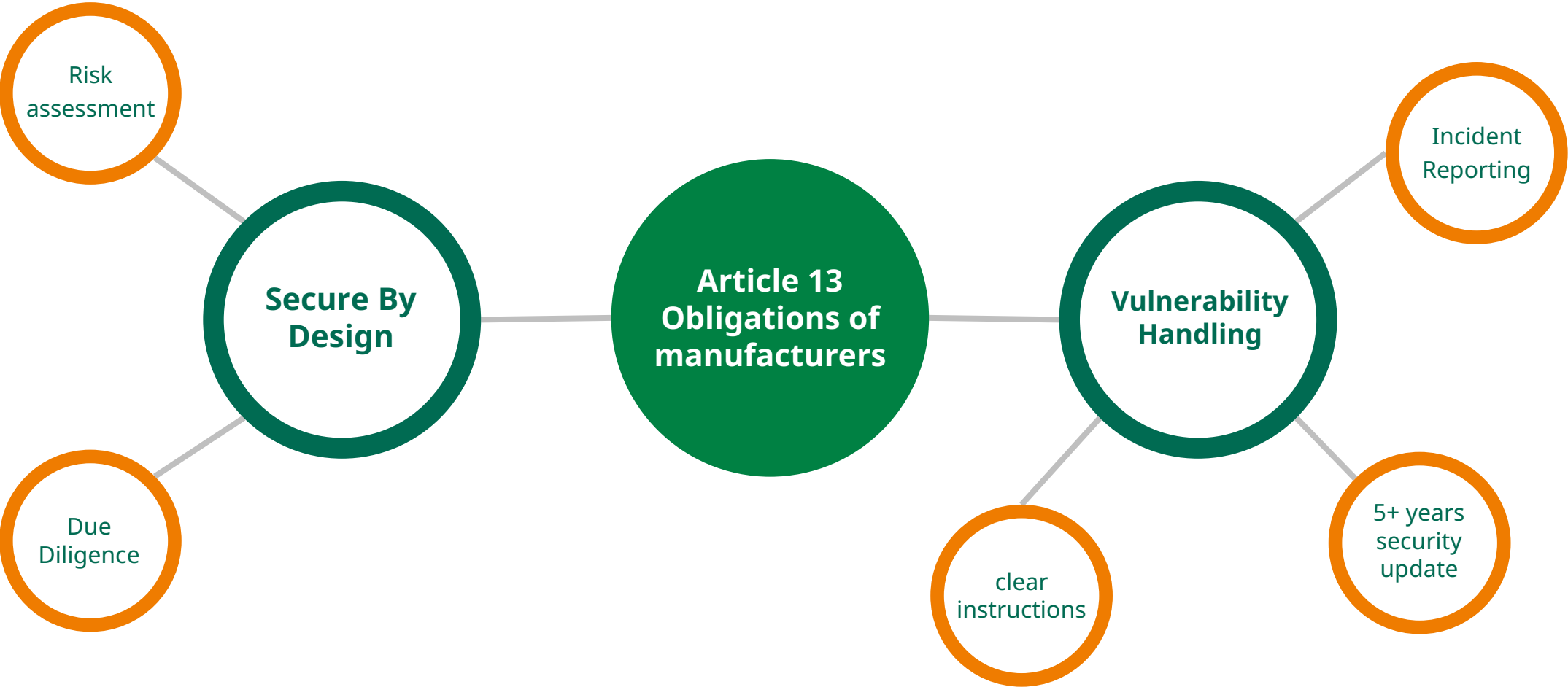
Regulation (EU) 2024/2847 Cyber Resilience Act (CRA)

RED and CRA

Items	RED (Radio Equipment Directive) Directive 2014/53/EU, Regulation (EU) 2022/30	CRA (Cyber Resilience Act) Regulation (EU) 2024/2847
Scope	- radio equipment - communicate itself over the internet	- products with digital elements (include hardware, software, and RDPS) - direct or indirect logical or physical data connection to a device or network
Essential Requirement	Health and Safety, EMC, RF, additional (cyber)	Cybersecurity
Core Cybersecurity Requirement	Product features to prevent network misuse, privacy protection, and fraud	- Process of secure by design and vulnerability handling - Product features to mitigate identified threats
Harmonized Standard (Cyber)	EN 18031 series	- EN 40000 series ^{*1} - EN 304 600 series, EN 50764-767, EN 50770 series ^{*2}
Effective Date	June 13, 2016 (August 1, 2025)	December 11, 2027

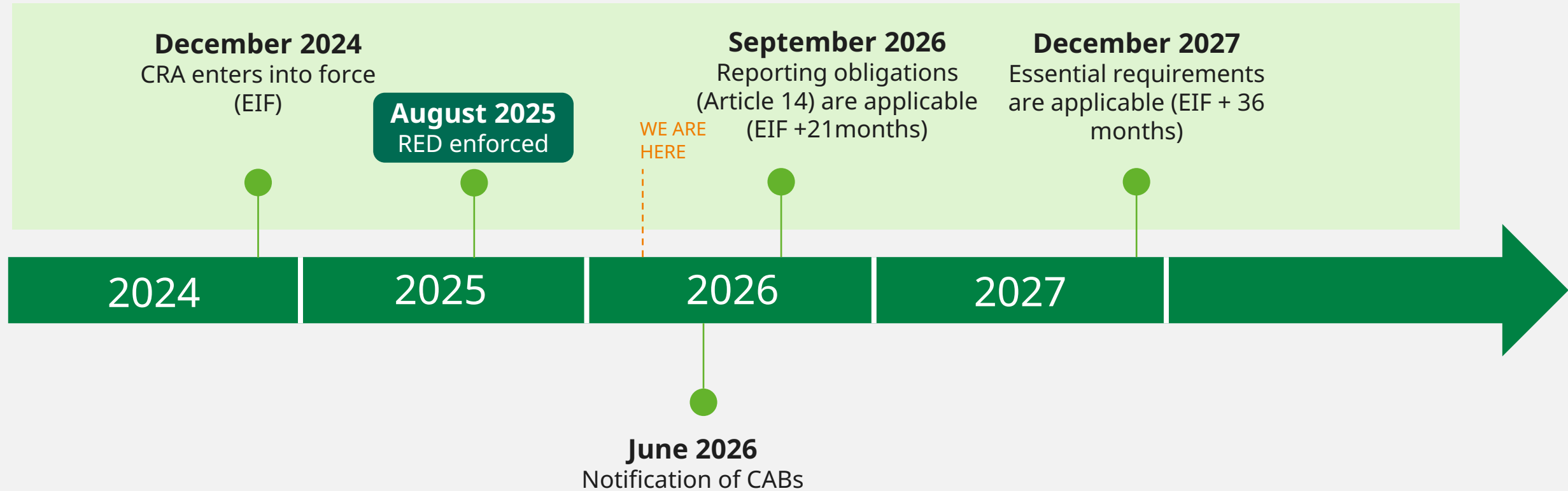
**1 horizontal*
**2 vertical*

Navigating Manufacturer Responsibilities



Timeline

Article 71 - Entry into force and application



Vulnerability Reporting

Article 14 - Reporting obligations of manufacturers

when

1. **actively exploited vulnerability**
2. **severe incident**

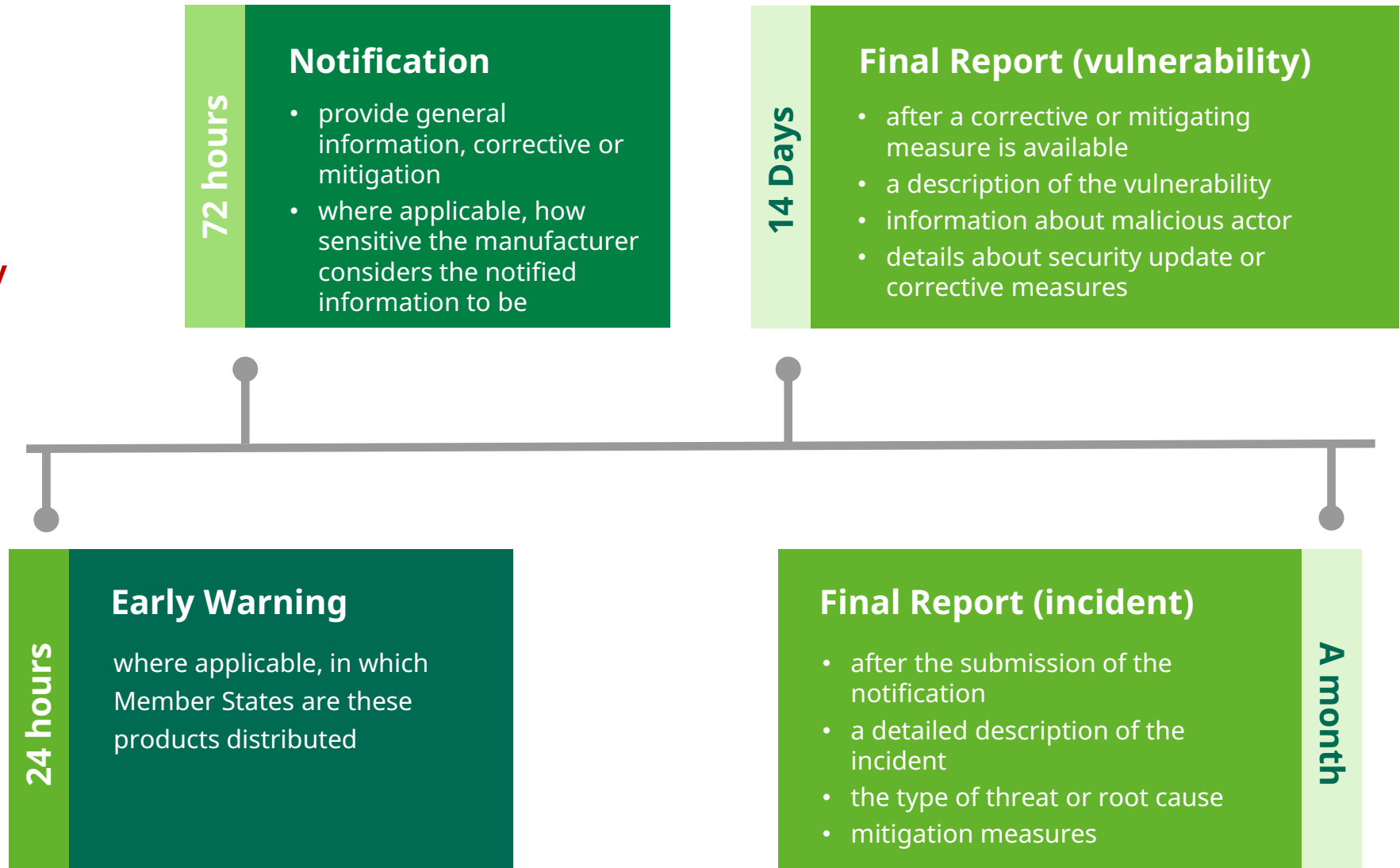
- Negative affect the the ability to protect CIA of sensitive or impotant data/function
- Introduce or execution of malicious code

become aware

via the single reporting platform

notify

- designated CSIRT
- ENISA



Product Category

Article 7 - Important products with digital elements (Annex III), Article 8 - Critical products with digital elements (Annex IV)

IMPORTANT CLASS I

Complete list of products that fall into Important Class I can be found in Annex III of the CRA, this includes:

- Identity management systems, privileged access management software & hardware, and access control readers
- Standalone & embedded browsers
- Password managers
- Software that searches for, removes or quarantines malicious software
- Products with virtual private network function
- Network management systems
- Boot managers
- Operating systems
- Routers and modems intended to connect to the internet and switches

IMPORTANT CLASS II

- Hypervisors and container runtime systems supporting virtualized execution of operating systems
- Firewalls, intrusion detection & prevention systems
- Tamper-resistant microprocessors & microcontrollers

CRITICAL CLASS

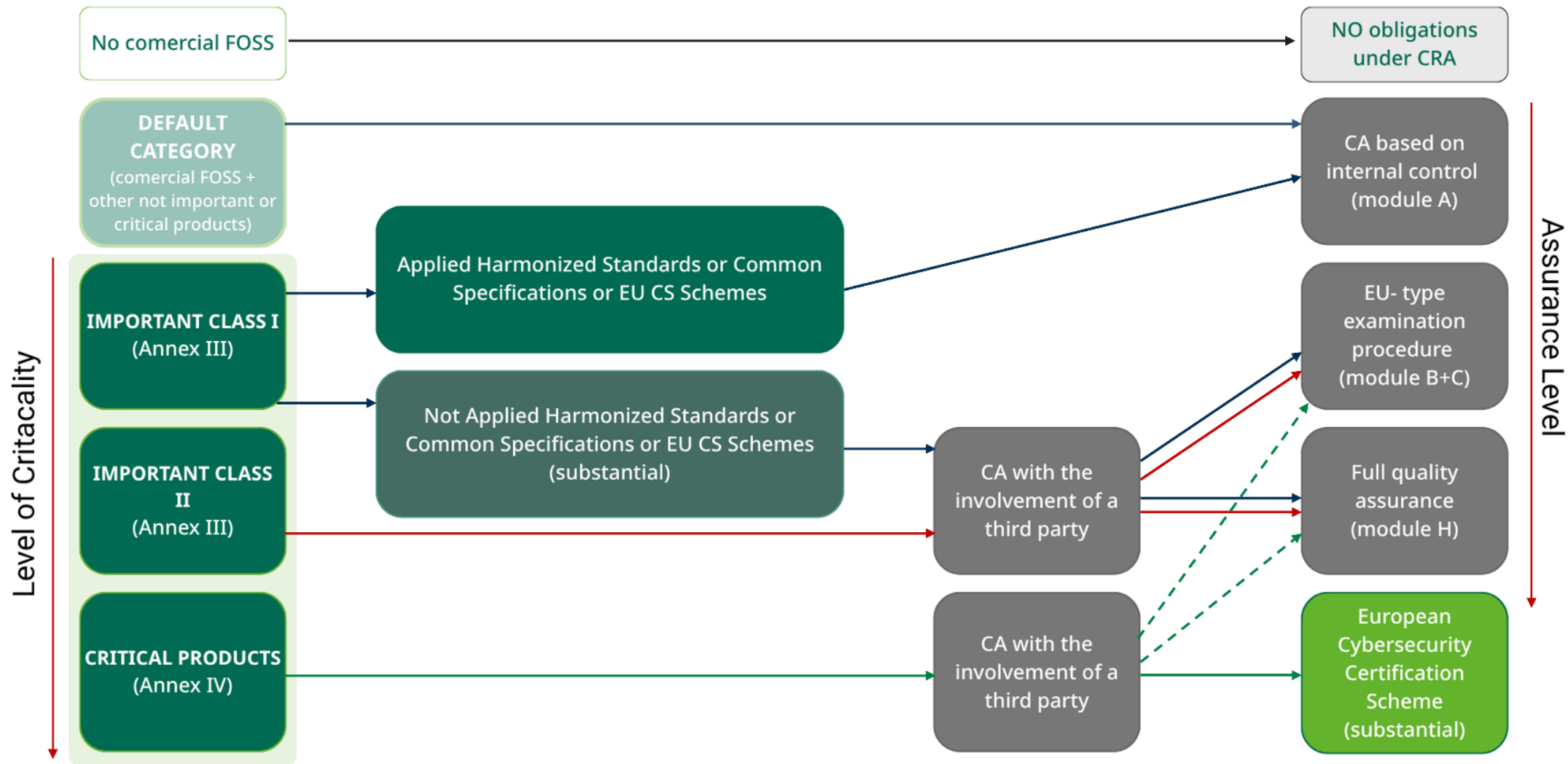
- Hardware devices with security boxes
- Smart meter gateways
- Smart cards or similar devices including secure elements
- Other devices for advanced security purposes, including secure crypto processing

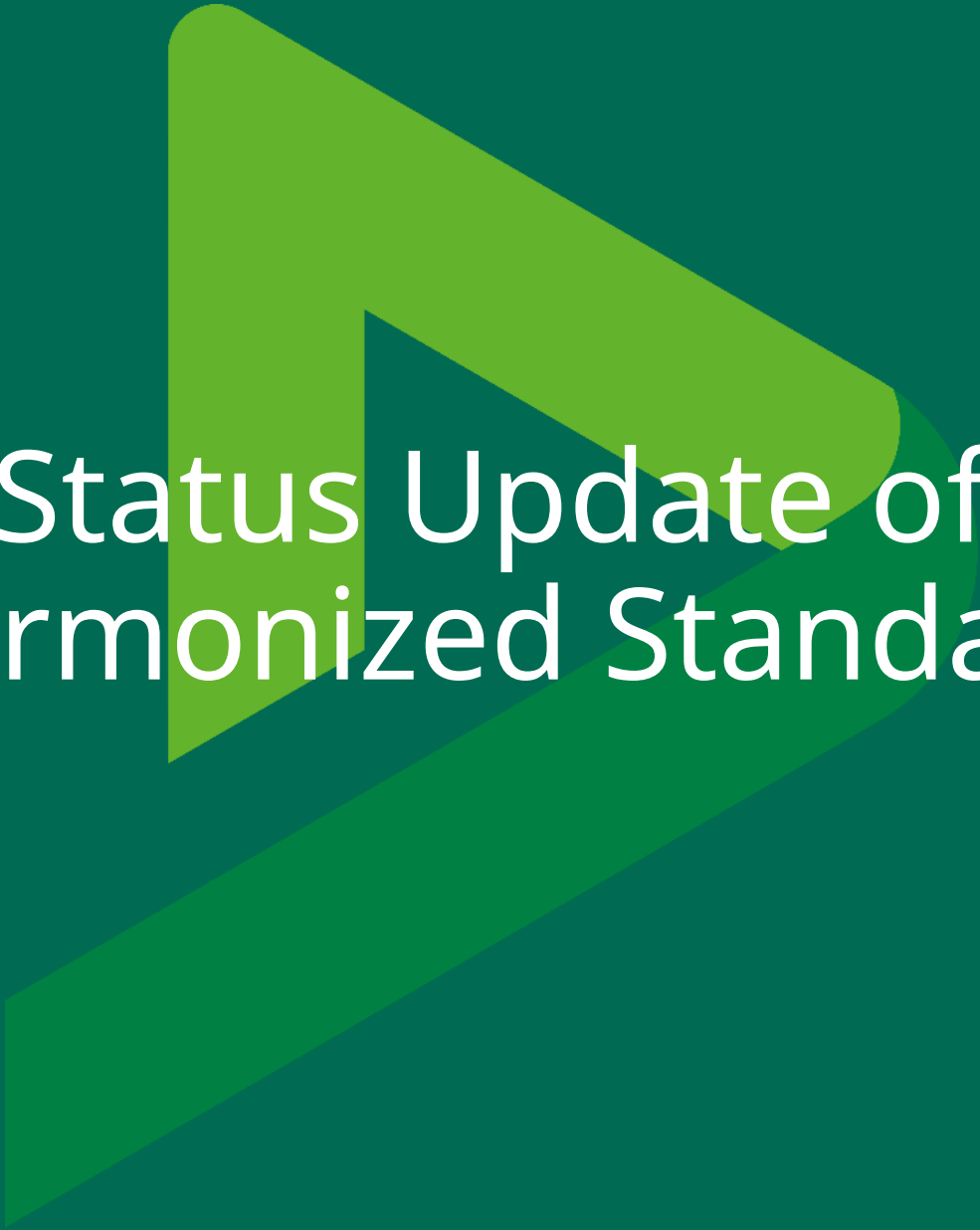
Implementation Regulation (EU) 2025/2392

technical description of the categories of important and critical products with digital elements

Conformity Assessment Procedure

Article 32 - Conformity assessment procedures for products with digital elements





Status Update of Harmonized Standard

CRA - Product Requirements

Article 6 - Requirements for products with digital elements

Products with digital elements shall be made available on the market only where:

- (a) they meet the essential cybersecurity requirements set out in Part I of Annex I, provided that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, the necessary security updates have been installed; and
- (b) the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in Part II of Annex I.

Annex I – Essential Cybersecurity Requirements (ECRs)

Part I Cybersecurity requirements relating to the properties of products with digital elements

- (1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.
- (2) On the basis of the cybersecurity risk assessment and where applicable, products with digital elements shall:
 - a) be made available on the market without known exploitable vulnerabilities;
 - b) ...
 - m) provide the possibility for users to securely and easily remove on a permanent basis all data and settings, ensure that this is done in a secure manner.

Part II Vulnerability handling requirements

Manufacturers of products with digital elements shall:

- (1) drawing up a software bill of materials
- (2) address and remediate vulnerabilities without delay
- (3) apply effective and regular tests
- ...
- (8) ensure that, where security updates are available, they are disseminated without delay and free of charge

Overview of CRA horizontal and vertical standards

CEN-CLC JTC 13 Cybersecurity and Data Protection WG9

EN 40000-1-1
Vocabulary

EN 40000-1-5
Threats and
Security Objectives

EN 40000-1-2
Principle for cyber
resilience

EN 40000-1-3
Vulnerability
Handling

EN 40000-1-4
Generic Security
Requirements

CLC TC 47 X
Semiconductors and Trusted Chips Implementation

CENELEC TC 65X
Industrial-process measurement, control and automation

CENELEC JTC 13 WG6
Smart meter gateway

ETSI Technical Committee on Cyber Security

EN 304 617
Browser

EN 304 618
Password Manager

EN 304 619
Antivirus

EN 304 620
VPN

EN 304 621
NMS

EN 304 622
SIEM

EN 304 623
Boot Manager

EN 304 624
PKI

EN 304 625
Network Interface

EN 304 626
Operating System

EN 304 627
Router, modem,
and switches

EN 304 631
Smart home
assistants

EN 304 632
Smart home
security

EN 304 633
Internet connected
toys

EN 304 634
Personal
wearables

EN 304 635
Hypervisors

EN 304 636
Firewall, IDS, IPS

EN 304 642
Network function
telecom

Status of Standardization for CRA: CEN-CLC JTC 13

Working Group 9 - Special Working Group on Cyber Resilience Act

Project reference	Status	Initial Date	Current Stage	Next Stage	Forecasted voting date
prEN 40000-1-1 (WI=JT013095) Cybersecurity requirements for products with digital elements - Vocabulary	Under Approval	2025-07-28	2026-01-01	2026-06-08	2026-06-08
prEN 40000-1-2 (WI=JT013089) Cybersecurity requirements for products with digital elements - Part 1-2: Principles for cyber resilience	Under Approval	2025-03-05	2026-01-01	2026-08-27	2026-08-27
prEN 40000-1-3 (WI=JT013090) Cybersecurity requirements for products with digital elements - Part 1-3: Vulnerability Handling	Under Approval	2025-03-05	2026-03-05	2025-06-06	2025-06-06
prEN XXX (WI=JT013091) Cybersecurity requirements for products with digital elements – Generic Security Requirements	Under Drafting	2025-03-05	2025-03-05		2026-09-20
(WI=JT013097) Cybersecurity requirements for products with digital elements —Threats and Security Objectives	Under Drafting	2025-08-06	2026-03-10	2026-09-08	

Horizontal Standards

Standard ID	Standard Name	CRA	Purpose
EN 40000-1-2	Principles for cyber resilience	Annex I, Part I (1)	• <u>Process standard</u> to ensure products are developed and maintained with a risk-based approach to cover any security risks • Implementation demonstrated via documented process outputs
EN 40000-1-4	Generic security requirements	Annex I, Part I (2)	• <u>Product standard</u> addressing a specific set of security requirements by mapping security objectives to a catalog of possible security controls • Implementation demonstrated via the product itself and/or supported by technical documentation
EN 40000-1-3	Vulnerability handling	Annex I, Part II	• <u>Process standard</u> to ensure products are maintained in a secure state using a risk-based approach • Implementation demonstrated via documented process outputs and actions in the market (updates, notifications, recalls, etc.)

Status of Standardization for CRA: ETSI TC CYBER

	IDENTIFICATION	TITLE (Formal only)	STATUS
1	Doc. Nb. EN 304 642 Ver. 0.0.10 Ref. DEN/CYBER-EUS-0019 Technical Body: CYBER EUSR Directives: 2024/2847 Details and Download	CYBER; CRA; Cybersecurity Requirements for Network Functions of Telecommunications Systems	Drafting Stage Current Status: Early draft (2026-02-18) Next Status: Stable draft (2026-06-30)
2	Doc. Nb. EN 304 636 Ver. 0.0.9 Ref. DEN/CYBER-EUS-0020 Technical Body: CYBER EUSR Directives: 2024/2847 Details and Download	CYBER; CRA; Cybersecurity requirements for firewalls, intrusion detection and/or prevention systems	Drafting Stage Current Status: Mature draft sent to EC and recognised o (2025-12-15) Next Status: EC Assessment Received (2026-02-02)
3	Doc. Nb. EN 304 635 Ver. 0.0.10 Ref. DEN/CYBER-EUS-0016 Technical Body: CYBER EUSR Directives: 2024/2847 Details and Download	CYBER; CRA; Cybersecurity requirements for hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments	Drafting Stage Current Status: Mature draft sent to EC and recognised o (2025-12-09) Next Status: EC Assessment Received (2026-01-28)
4	Doc. Nb. EN 304 634 Ver. 0.2.2 Ref. DEN/CYBER-EUS-003 Technical Body: CYBER EUSR Directives: 2024/2847 Details and Download	CYBER; CRA; Cybersecurity requirements for personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/746 or Regulation (EU) 2017/746 do not apply; Or personal wearable products that are intended for the use by and for children	Drafting Stage Current Status: Mature draft (2026-02-02) Next Status: Mature draft sent to EC and recognised o (2026-02-23)
5	Doc. Nb. EN 304 633 Ver. 0.2.3 Ref. DEN/CYBER-EUS-004 Technical Body: CYBER EUSR Directives: 2024/2847 Details and Download	CYBER; CRA; Cybersecurity requirements for Internet connected toys covered by Directive 2009/48/EC that have social interactive features (e.g. speaking or filming) or that have location tracking features	Drafting Stage Current Status: Mature draft sent to EC and recognised o (2026-02-05) Next Status: EC Assessment Received (2026-03-13)
6	Doc. Nb. EN 304 632 Ver. 0.2.1 Ref. DEN/CYBER-EUS-0014 Technical Body: CYBER EUSR Directives: 2024/2847 Details and Download	CYBER; CRA; Cybersecurity requirements for smart home products with security functionalities; including smart door locks, security cameras, baby monitoring systems and alarm systems	Drafting Stage Current Status: Mature draft sent to EC and recognised o (2026-02-05) Next Status: EC Assessment Received (2026-03-13)
7	Doc. Nb. EN 304 631 Ver. 0.2.1 Ref. DEN/CYBER-EUS-0011 Technical Body: CYBER EUSR Directives: 2024/2847 Details and Download	CYBER; CRA; Cybersecurity requirements for smart home general purpose virtual assistants	Drafting Stage Current Status: Mature draft sent to EC and recognised o (2026-02-05) Next Status: EC Assessment Received (2026-03-13)
8	Doc. Nb. EN 304 627 Ver. 0.0.11 Ref. DEN/CYBER-EUS-0013 Technical Body: CYBER EUSR Directives: 2024/2847 Details and Download	CYBER; CRA; Cybersecurity requirements for routers, modems intended for the connection to the internet, and switches	Drafting Stage Current Status: EC Assessment Received (2026-01-19) Next Status: Final draft (2026-02-15)

Status of Standardization for CRA: CLC/TC 65X

Industrial-process measurement, control and automation

Developments based on [EN IEC 62443](#) based on the existing project to update the broad vertical (WI= 81487 – EN IEC 62443-4-1:2018/prAA and WI= 79973 EN IEC 62443-4-2:2019/prAA) using the scheme by the EN IEC 62443-1-5

Project reference 	Status 	Initial Date	Current Stage	Next Stage	Forecasted voting date
prEN 50770-1 (pr=81649) Security for Operational Technologies - Part 1: Security Profile for firewalls and intrusion detection and prevention systems (based on EN IEC 62443)	Under Drafting	2025-10-21	2025-10-21	2026-02-17	2027-08-03
prEN 50770-3 (pr=81651) (prEN 50770-3) Security for Operational Technologies - Part 3: Security Profile for physical and virtual network interfaces (based on EN IEC 62443)	Under Drafting	2025-12-27	2025-12-27	2026-03-22	2027-08-03
prEN 50770-4 (pr=81652) (prEN 50770-4) Security for Operational Technologies - Part 4: Security Profile for products with digital elements with the function of virtual private network (VPN)	Under Drafting	2025-10-21	2025-10-21	2026-02-17	2027-08-03
prEN 50770-5 (pr=81653) Security for Operational Technologies - Part 5: Security Profile for routers, modems intended for the connection to the internet, and switches (based on EN IEC 62443)	Under Drafting	2025-10-21	2025-10-21	2026-02-17	2027-08-03
prEN 50770-6 (pr=81654) Security for Operational Technologies - Part 6: Security Profile for security information and event management (SIEM) systems (based on EN IEC 62443)	Under Drafting	2025-10-21	2025-10-21	2026-02-17	2027-08-03
prEN 50XXX-2 (pr=81650) (prEN 50770-2) Security for Operational Technologies - Part 2: Security Profile for network management systems (based on EN IEC 62443)	Under Drafting		2025-08-14		

Status of Standardization for CRA: CLC/TC 47X

Semiconductors and Trusted Chips Implementation

Working group	Title				
CLC/TC 47X/WG 01	Microprocessors and Microcontrollers with security related functionalities				
CLC/TC 47X/WG 02	Tamper resistant Microprocessors and Microcontrollers				
CLC/TC 47X/WG 03	SmartCards and Secure Element Platforms				
CLC/TC 47X/WG 04	ASIC and FPGA with security-related functionalities				
CLC/TC 47X/WG CRA	TC47X - CRA				

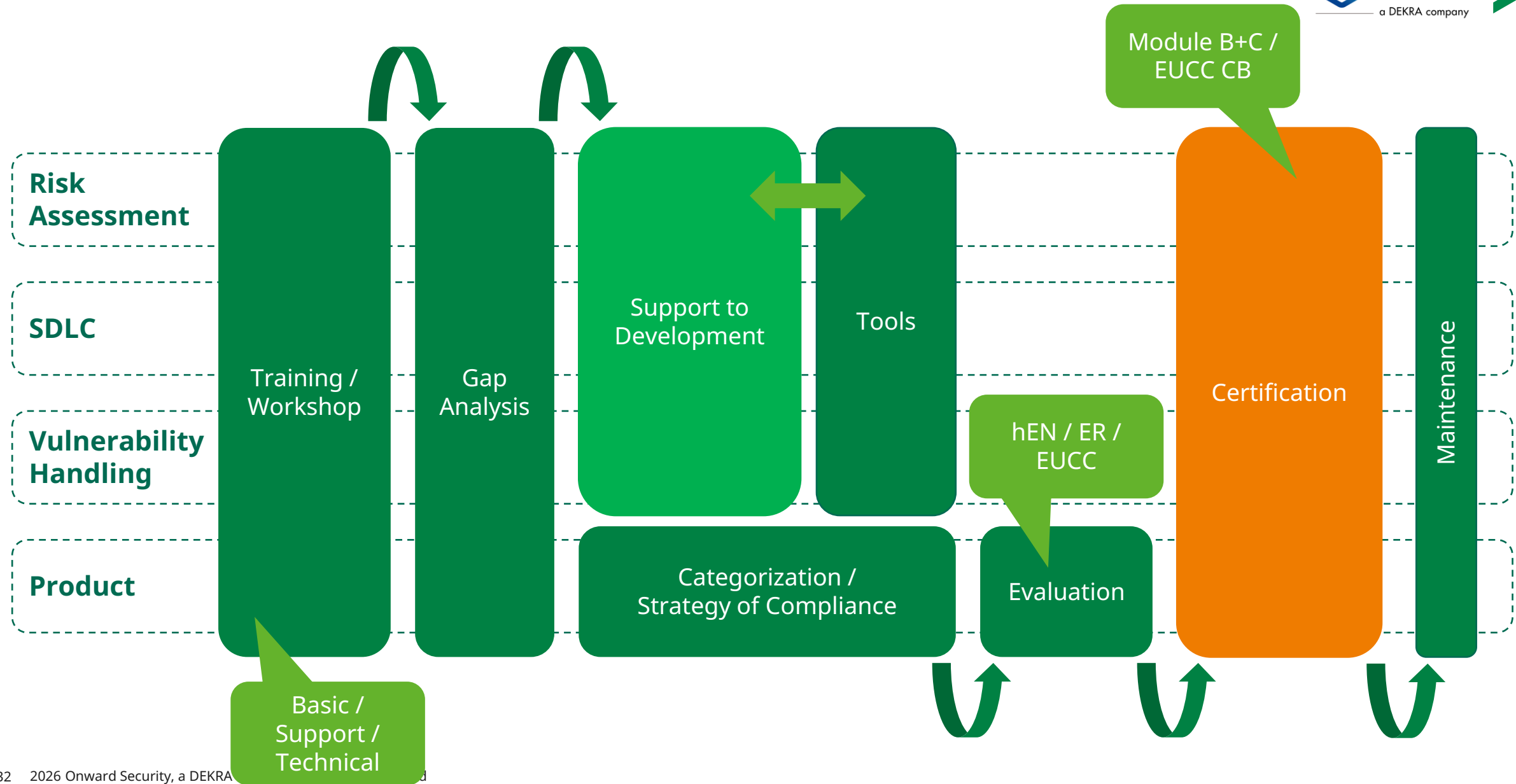
Project reference	Status	Initial Date	Current Stage	Next Stage	Forecasted voting date
prEN 50764:2026 (pr=80922) Cybersecurity requirements for platforms of smartcards and similar devices including secure elements	Under Enquiry	2025-02-02	2026-01-16	2026-04-10	2026-08-13
prEN 50765:2026 (pr=80923) Cybersecurity requirements for microprocessors and microcontrollers with security-related functionalities	Under Enquiry	2025-01-23	2026-01-16	2026-04-10	2026-08-13
prEN 50766:2026 (pr=80924) Cybersecurity requirements for tamper-resistant microprocessors and microcontrollers	Under Enquiry	2025-01-03	2026-01-16	2026-04-10	2026-08-13
prEN 50767 (pr=82281) prEN 50767: Technical Security Standards for Application Specific Integrated Circuits (ASICs) and Field-Programmable Gate Arrays (FPGAs) with Security-related Functionalities	Under Drafting	2025-09-22	2025-09-22	2026-01-03	2027-06-28



CRA Compliance Service

- 01** Participation in **CEN/CENELEC JTC13/WG9** and **ETSI CYBER WG** for development of standards for CRA.
- 02** Participation in **European Commission Special WG** on CRA (2 delegates).
- 03** DEKRA is accredited **Laboratory and Certification Body for EUCC**: compliance with CRA through EUCC.
- 04** DEKRA has been selected by **ENISA** as supporting entity for the project "Support to Pilot the EUCC CRA Interplay" to perform pilots to evaluate the compliance with CRA through EUCC.

DEKRA CRA Services



Services Catalogue

Supporting / Tool

Type	Service	Description
Workshop	Workshop (basic)	1-2 hours workshop (Language: Mandarin) - Introduction of CRA and latest update
	Workshop (advance)	- additional 1-2 hours advisory service (Language: Mandarin) - include content from basic workshop - Detailed explanation of CRA article and practice suggestion
Gap analysis	SDL	Perform interview and gap analysis of SDL requirement (Language: Mandarin)
	Vulnerability handling	Perform interview and gap analysis of vulnerability handling requirement (Language: Mandarin)
Advisory service	SDL	- Document template (optional) expert service
	Vulnerability handling	- Document template (optional) expert service
	Reporting obligation	Document template and training
Tool	SecSAM	- SaaS SBOM management tool - license of 5 users and 25 products

Services Catalogue

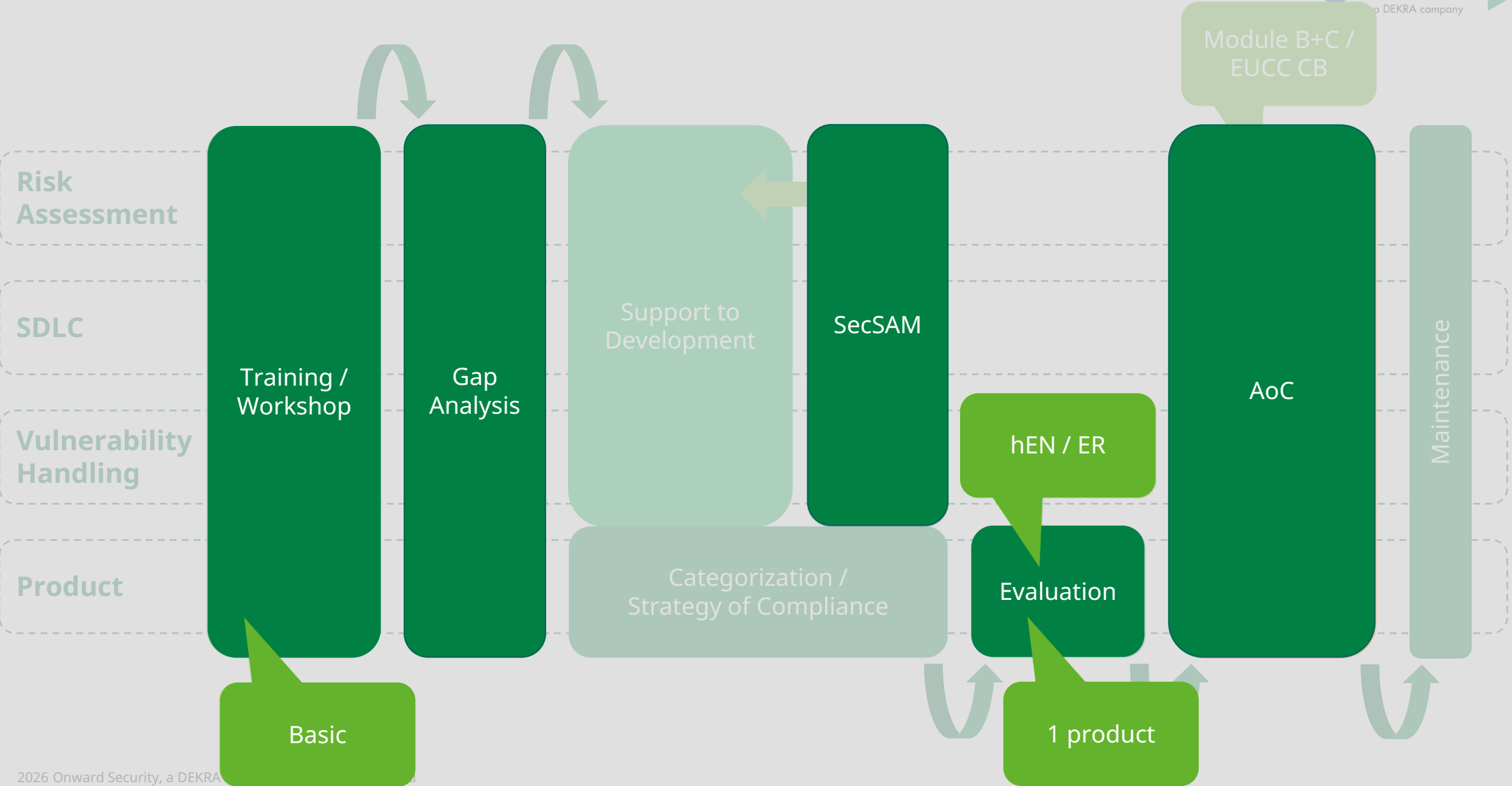
Evaluation / Certification

Type	Service	Description
Evaluation	Product Evaluation (Light)	Product evaluation based on essential requirements and reference standards
	Product Evaluation (Default)	Product evaluation based on horizontal harmonized standards
	Product Evaluation (Important)	Product evaluation based on vertical harmonized standards
	EUCC Evaluation	Product evaluation based on EUCC substantial level
Certification	Attestation of certificate	Based on the result of evaluation report, issue appropriate AoC by testing laboratory
	Nobo cert for products (Module B)	EU-TEC issued by notified body for product which meet CRA regulation
	Nobo cert for QMS (Module H)	Certificate issued by notified body for quality system of manufacturer can ensure that their quality system make product meet CRA regulation
	CB certification for EUCC	EUCC certificate issued by EUCC certification body for product



CRA Pre-assessment Service

DEKRA CRA Solutions Pre-assessment Services



What's included

Workshop

- 1 workshop
 - 2 hours for EU CRA regulation detailed introduction and Q&A

Gap Analysis *1

- development lifecycle (inhouse methodology based on DEKRA knowledge, expertise, ISO/IEC standard, and latest draft hEN if any)
- vulnerability handling (inhouse methodology based on DEKRA knowledge, expertise, ISO/IEC standard, and latest draft hEN if any)

Product Evaluation *2

- 1 product testing (inhouse test cases based on DEKRA knowledge, expertise, ISO/IEC standard, and latest draft hEN if any)

SBOM Tools

- 1 SBOM monitoring tools

Deliverable

- | | | | |
|--|---|--|---|
| <ul style="list-style-type: none">• Workshop material (digital format)• Attendance of Certificate | <ul style="list-style-type: none">• 2 Gap analysis reports• Up to 6 hours supporting service | <ul style="list-style-type: none">• Total of 1 product evaluation reports• Up to 3 hours supporting service• Attestation of Conformity | <ul style="list-style-type: none">• 3 months of trial license |
|--|---|--|---|

**1 1 product family specific by the manufacturer*

**2 include 1 round of verification testing*

CRA Supporting Service

EN 40000-1-2 / EN 40000-1-3 輔導流程



1. Interview

1. 依照 EN 40000-1-2, EN 40000-1-3 的安全要求，審查廠商是否提供相對應之文件
2. 針對導入產品開發作業進行作業訪查
3. 開發人員訪談，以瞭解產品實際開發暨更新流程
4. 檢視現有開發系統及相關工具
5. 開發端廠房實地訪查確認

2. Gap Analysis

1. 依上述實際訪談內容產出可行性評估報告及產品開發各階段所需之資安控制措施建議

3. Design

1. 建立安全作業管控流程
2. 提供產品開發安全管理作業參考指引
3. 根據作業訪談結果調整文件設計

4. Implement

1. 建立產品開發生命週期安全管理機制
2. 將參考全組織現況與業務權責提出建議制定產品開發安全開發之任務與目標
3. 協助產品安全任務編組以定期進行產品安全之管理與審查
4. 建立符合公司目標之產品安全開發政策
5. 建立符合產品安全開發政策之安全作業流程

5. Review

1. 根據開發流程改善建議提出產品規劃、設計、開發、測試、維運之諮詢服務以符合SSDL要求
2. 依照產品導入EN 40000-1-2 / EN 40000-1-3 訂定的流程，確認開發程序確實符合既定流程並產出相對應紀錄
3. 產品導入期間提供諮詢服務，並檢視產品安全開發紀錄，

7. External Assessment

1. 由 DEKRA 獨立團隊執行外部評估
2. 評估之後，即可取得 AoC 證明開發流程與漏洞管理滿足 EN 40000-1-2 與 EN 40000-1-3- 要求

8 ~ 10 month

2 ~ 4 weeks

Feasibility Assessment

Implementation

Review

Assessment

EN 40000-1-2 / EN 40000-1-3 輔導內容



制度建立

- 建立產品安全開發作業流程
- 提供程序書文件範本
- 建立產品資安事件應變作業
- 確認EN 40000-1-2, EN 40000-1-3 流程合規符合性

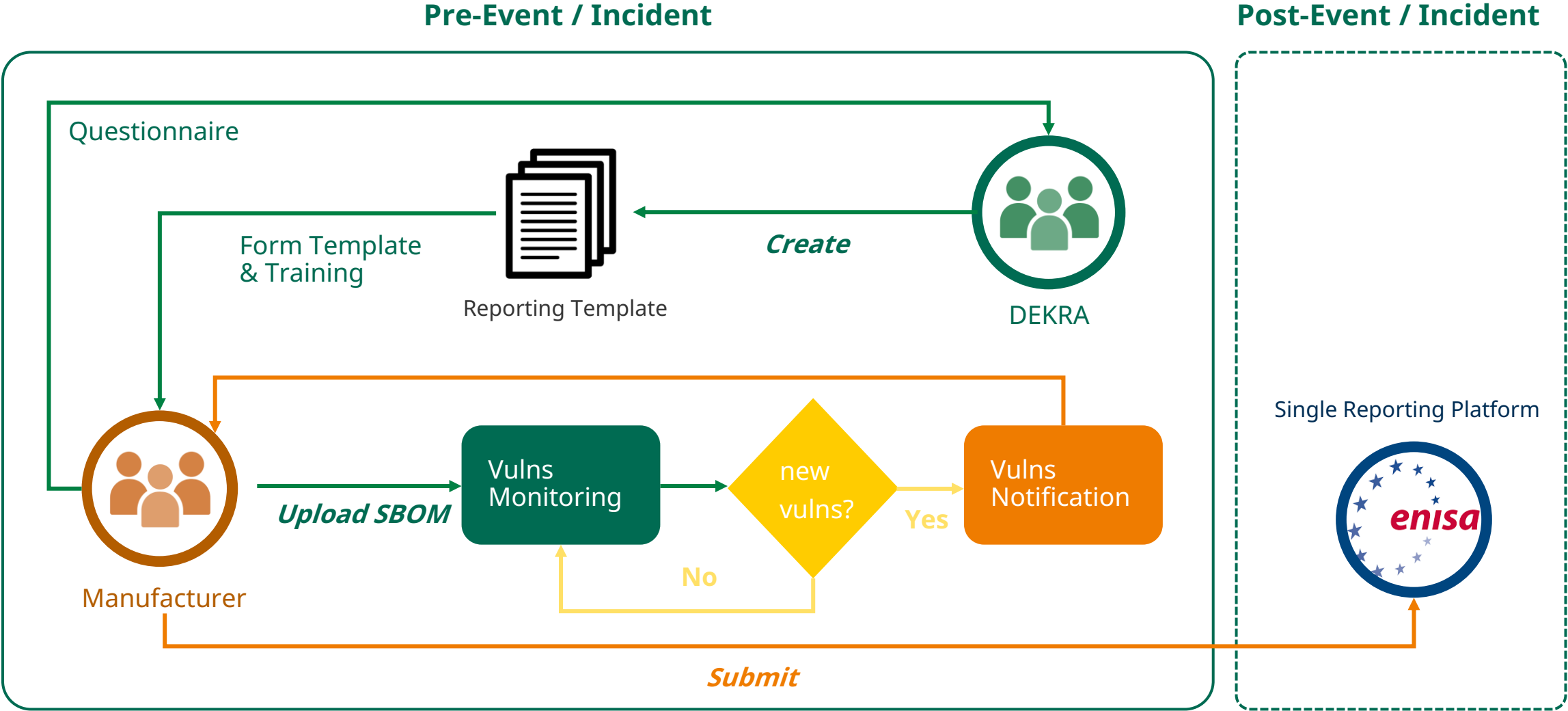
諮詢服務

- 施行現況訪談
- 導入期間每月安排1-2人天的文件增修討論
- 導入期間提供以電話與電子郵件管理制度與資安技術諮詢服務

教育訓練

- 提供課程規劃
- 每次至少2小時訓練, 含教材、試題
- 協助受稽人員熟悉 IEC 62443-4-1 標準作業流程

CRA Reporting Supporting Service (1/2)



CRA Reporting Supporting Service (2/2)

add-on services



Local Deployment

- On-premise SBOM Infrastructure: Dedicated local instance to ensure data sovereignty and security
- Private Instance Deployment: Fully isolated environment for internal SBOM management and analysis

SBOM Generation

- Blackbox approach
 - Automated SBOM generation using industry-leading tools (e.g., Black Duck) with only firmware images required
- Whitebox approach
 - Deep-dive scanning using advanced static code analysis tools (e.g., LucentSky) for comprehensive visibility into software components

Assessment

- Systematic evaluation of reporting processes against CRA Article 14 regulatory requirements
- Formal issuance of AoC upon fulfilling CRA mandates, validating your cybersecurity posture
- Strategic support for OEMs to demonstrate robust reporting capabilities to their customers

◀ 100 ▶
YEARS
SECURING THE
FUTURE
1925 - 2025

Thank you.

✉ contact.onward@dekra.com

🌐 www.onwardsecurity.com



Onward Security 🔍

Realize Ultimate Security | every step starts with the labs