Approvals

CRA & RED Explained: Compliance, Timelines, & Impact

Nejra Lalić, Business Development Engineer

30. October 2025

Agenda

- Awareness of CRA and RED
- Cyber Resilience Act (CRA)
- What to Do While Awaiting Notified Body Accreditation?
- Radio Equipment Directive (RED) and RED-DA (Delegated Act)
- Overview FM Approvals Cybersecurity Certifications
- Q&A

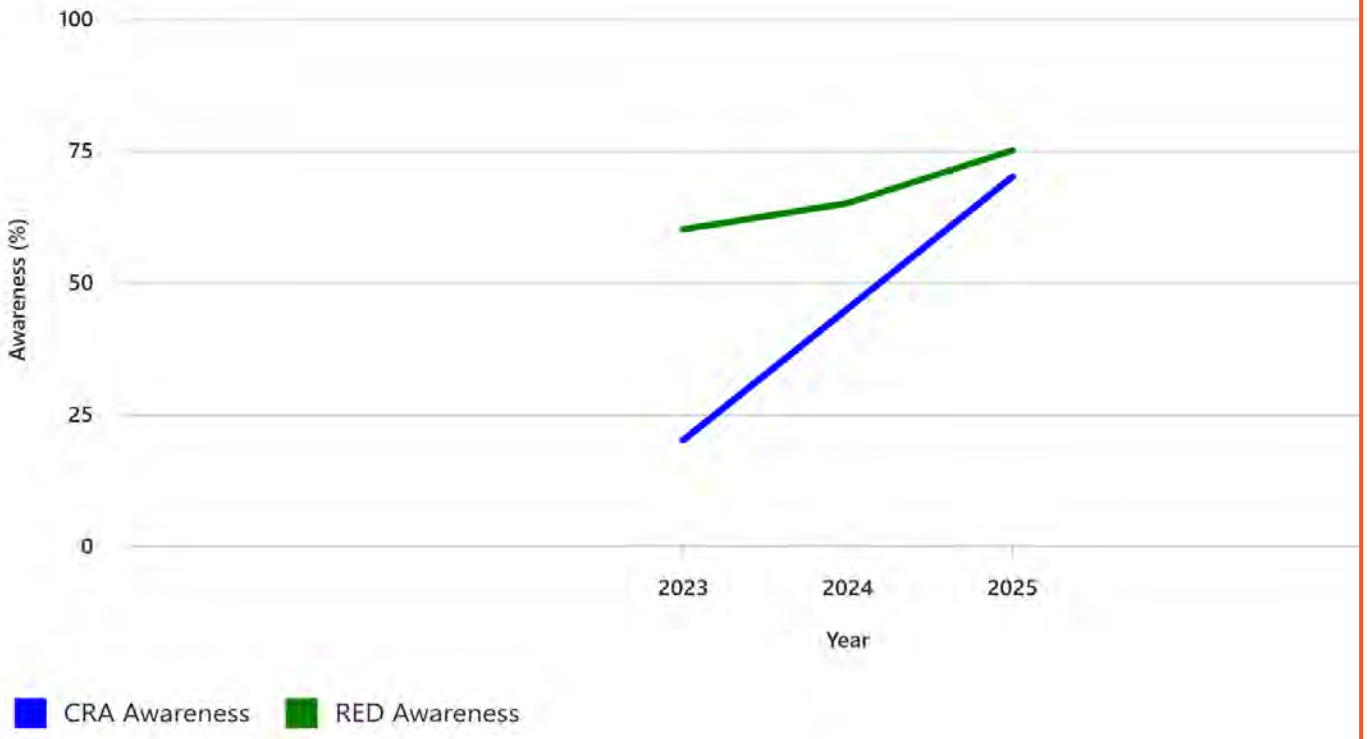
Market Awareness of CRA

2024

2025

Market Awareness CRA vs. RED in the Last 3 Years

CRA's awareness has risen rapidly due to new cybersecurity obligations, while RED remains stable as an established directive.



- **CRA (Cyber Resilience Act)**

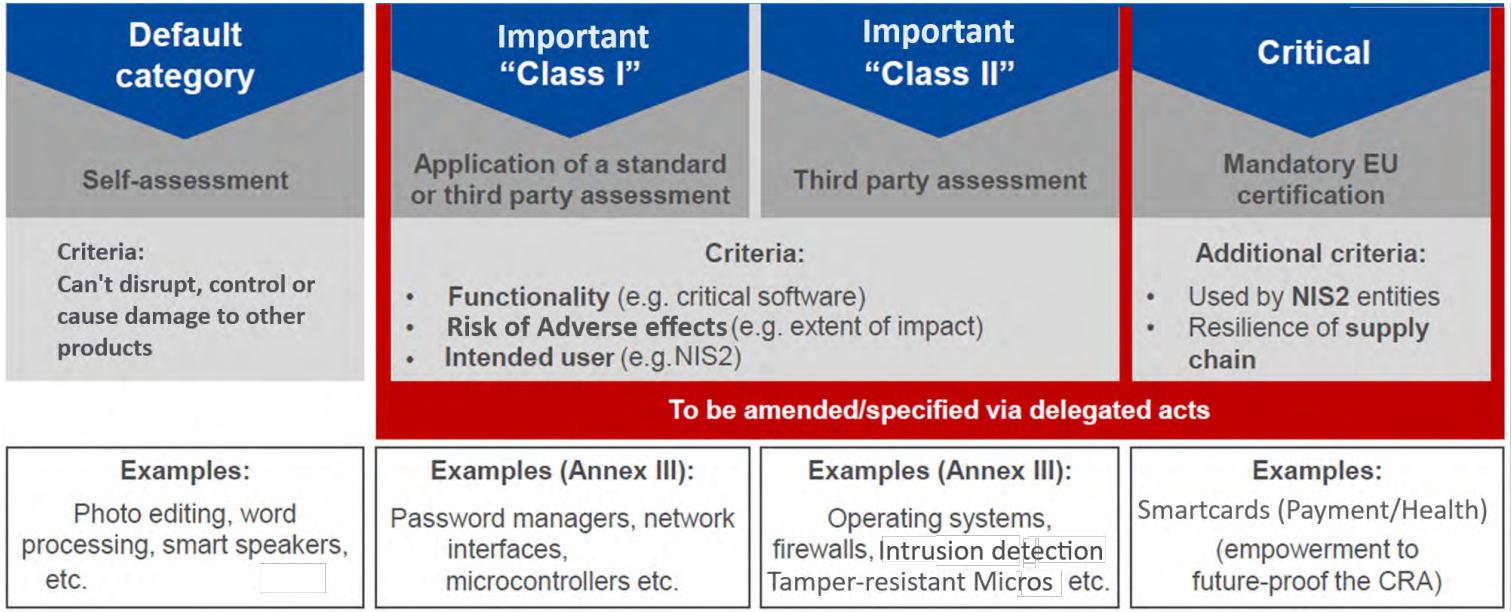
shows a steep growth in awareness:
- 2023: ~20%
- 2024: ~45%
- 2025: ~70%

- **RED (Radio Equipment Directive)**

maintains higher but slower growth:
- 2023: ~60%
- 2024: ~65%
- 2025: ~75%

Cyber Resilience Act (CRA) in the EU

- The first **EU-wide regulation** introducing **mandatory cybersecurity requirements for products with digital elements** (hardware, software, IoT)
- **ISA/IEC 62443** – basis for harmonized standards
- Applies to **manufacturers, software developers, importers, and distributors** in the EU - security of the whole supply chain
- Covers the **entire product lifecycle**
- **CE marking:** conformity with the CRA
- **Fines** - up to €15 million or 2.5% of global turnover
- **Effective dates:**



Does CRA Apply to My Product?

Does the product include or contain software or firmware?

✓ → Is the software an open-source product and non-commercial?

✗ → Excluded from the scope of the CRA

✓ → *Excluded from the scope of the CRA

✗ → Is the product a SaaS or a cloud offering?

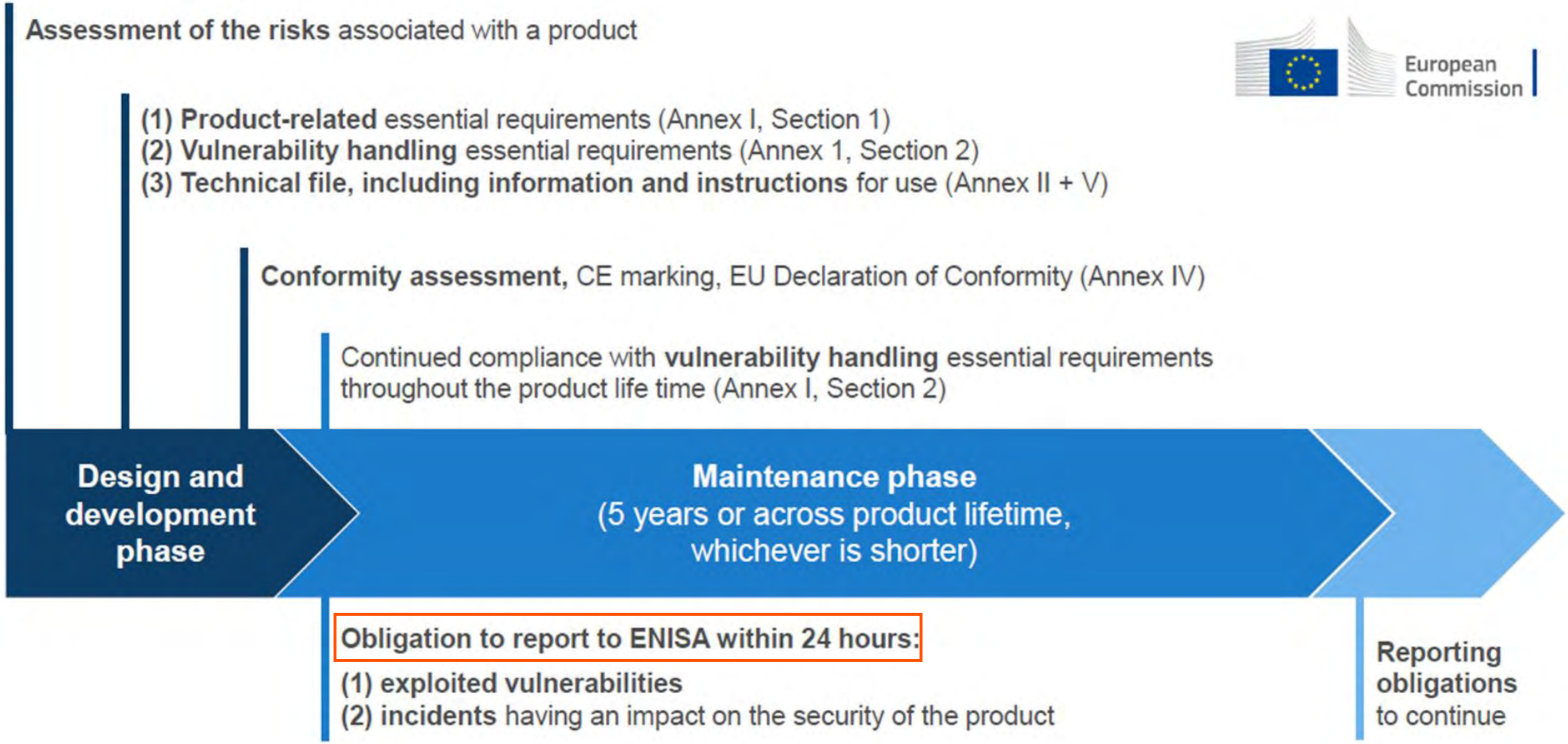
✗ → Must comply with the CRA

✓ → Is there another product based on the service?

✗ → Excluded from the scope of the CRA (take a look at NIS2)

✓ → Must comply with the CRA

CRA – Manufacturer Obligations



CRA – Assessment Types

Assessment Type	Conditions	Applicable Products (examples)	CRA References
Self-Assessment	- **Manufacturer** applies harmonized standards, common specifications, or EU cybersecurity certification schemes - **Product is not Important or Critical**	- Word processing software - Basic fitness trackers - Smart bulbs	Article 32(1) Annex VIII Part I Annex III & IV (exclusion)
Third-Party	- Manufacturer does not apply harmonized standards or certification schemes for Important Class I products - **Always required for Important Class II products**	- Password managers - Network interfaces - Operating systems - Firewalls (Class II)	Article 32(2), 32(3) Annex III Annex VIII Parts II & III
Notified Body	- **Product is a Critical product** - Commission adopts delegated act requiring mandatory certification - **Certification** must be at assurance level ‘substantial’ or higher	- Security gateways - Industrial control system components - Remote access solution for critical infrastructure	Article 8(1), 32(4) Annex IV

CRA - Timeline

The CRA entered into force on 10. Dec. 2024, with obligations becoming applicable from 11. Dec. 2027. There are also transitional periods for implementing specific requirements, such as vulnerability reporting - the obligations to report vulnerabilities will apply from 11. Sep. 2026.

The obligations concerning the notified bodies will be applied as from 11. June 2026, 18 months after the entry into force of the Regulation.

European Commission

What Can Manufacturers Do in the Absence of Accredited NBs?

- Prepare comprehensive technical documentation:
  - SBOM (software bill of materials)
  - Risk assessments
  - Secure-by-design and secure-by-default configurations
  - Vulnerability handling procedures
  - Lifecycle support plans (min. 5 years, updates available for 10 years)
- Start with SDLA certification ASAP to be prepared for a smooth transition from ISA/IEC 62443 certification to future CE marking - *recommended*
- Use self-assessment where permitted (default/low-risk category of products)
- Follow harmonized standards (once published) or common specifications
- Monitor CRA timeline, some of key dates:
  - 11. Sep. 2026: vulnerability and incident reporting begin
  - 11. Dec. 2027: full compliance required
- Stay engaged with regulatory updates

CRA - Summary

- Applies to **all digital products** (hardware, software, remote data processing solutions)

Key Manufacturer Obligations

- Risk assessment and cybersecurity by design
- Vulnerability management and incident reporting
- Security updates for at least 5 years
- CE marking and conformity assessment
- Software Bill of Materials (SBOM) required
- Technical documentation and user guidance

Product Classification & Testing

- Product categories:
  - Default
  - Important (Class I & II)
  - Critical
- Conformity assessment types:
  - Self-assessment for default
  - Third-party evaluation for higher-risk classes
  - EU Cybersecurity Certification for critical products

Reporting & Penalties

- Vulnerabilities must be reported within:
  - 24h (initial alert)
  - 72h (detailed report)
  - 14 days (mitigation plan)
- Fines:
  - Up to €15 million or 2.5% of global turnover for serious violations

Preparation & Support

- Third-party assessment:
  - SDLA, CSA, SSA (ISA/IEC 62443) – CRA Readiness
- Manufacturers should:
  - Determine product classification
  - Prepare technical documentation, risk assessments, and SBOMs
  - Follow the existing standards

Products Covered by Radio Equipment Directive (RED)

Core Features Required by RED:

- Wireless Communication Capability
- Safety and Health Protection
- Electromagnetic Compatibility (EMC)
- Efficient Use of the Radio Spectrum
- Cybersecurity
  - Network Protection
  - Privacy and Data Protection
  - Fraud Prevention

RED-DA supplement to RED!

Product Type	Technologies Used	RED-Relevant Features
Smartphones & Tablets	LTE, Wi-Fi, Bluetooth, GPS	Radio transmission, cybersecurity, data privacy
Smartwatches & Wearables	BLE, Wi-Fi, GPS	Health tracking, secure connectivity
IoT Devices	Zigbee, LoRa, Wi-Fi	Remote control, secure updates
Baby Monitors	RF, Wi-Fi	Audio/video transmission, privacy safeguards
Wi-Fi Routers	Wi-Fi 6, WPA3	Network integrity, secure configuration
GPS Trackers	GNSS, cellular	Location tracking, secure data transmission
POS Terminals	NFC, Bluetooth, Wi-Fi	Financial transaction protection
Smart Home Devices	Zigbee, Z-Wave, Wi-Fi	Automation, interoperability, fraud protection

RED and RED-DA (Delegated Act)

Aspect	Radio Equipment Directive (RED) – 2014/53/EU	RED Delegated Act (RED-DA) – EU 2022/30
Legal Type	Directive General framework	Delegated Act (**supplement to RED** - **Articles 3.3 (d), (e), (f)**
Purpose	Establishes the **baseline regulatory framework** for placing radio equipment on the EU market	Supplements the RED by **activating specific cybersecurity-related provisions**
Scope	Applies to **all radio equipment**	Applies specifically to **internet-connected radio equipment**
Requirements	General safety, electromagnetic compatibility EMC, spectrum use	**Cybersecurity for internet-connected devices**
Mandatory?	Yes, **for all radio equipment**	Yes, **for internet-connected radio equipment from 1. Aug. 2025**
Examples of Covered Devices	All radio equipment	**Devices that initiate internet communication** (e.g., Wi-Fi-enabled thermostats, smart home devices, IoT modules, smart toys and wearables)

RED-DA (Radio Equipment Directive Delegated Act) Withdrawal

- **Cybersecurity requirements of internet-connected radio equipment**

Mandatory compliance with RED-DA started 1. Aug. 2025 and will be valid until 11. Dec. 2027, when CRA will take over – to avoid double regulation

The **harmonized standards for RED-DA** (**EN 18031**) will likely form **the basis for CRA harmonized standards:**

EN 18031-1:

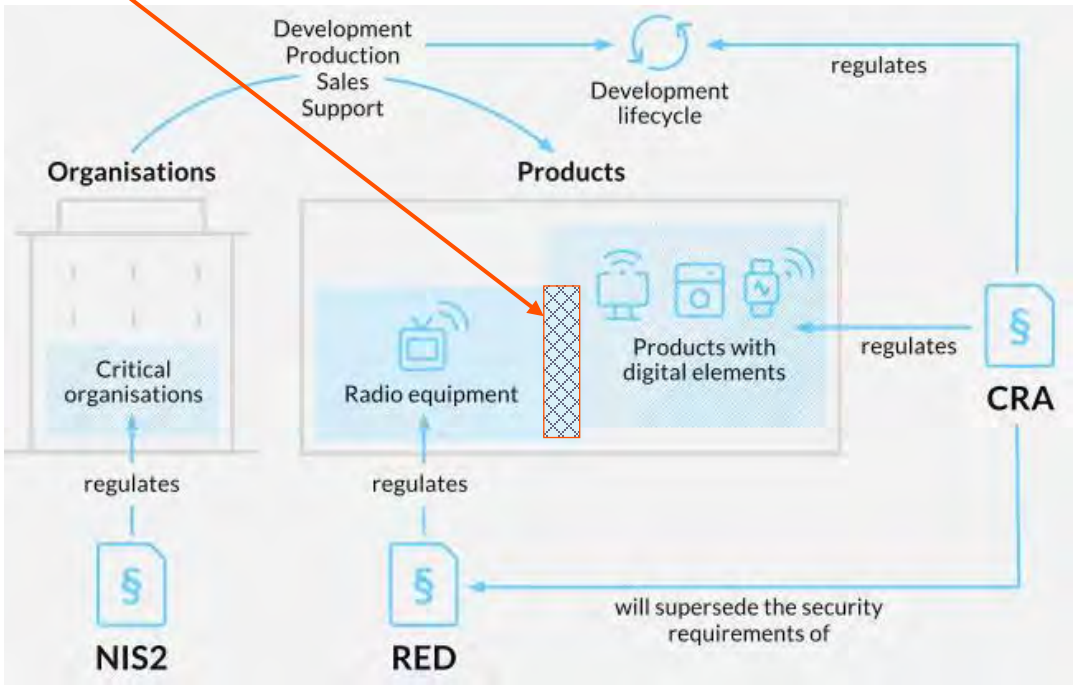
- Network protection

EN 18031-2:

- Privacy protection

EN 18031-3:

- Fraud prevention



Importance of Harmonized Standards

- **Presumption of Conformity**: Compliance with these standards provides a presumption of conformity with the RED-DA requirements, simplifying the certification process
- **Notified Body Involvement**: optional; full compliance allows manufacturers to self-declare conformity

CE Marking - Current Status

Combined Impact for Manufacturers:

Since **1. Aug. 2025**, **CE marking** for many wireless and connected products requires:

- **RED cybersecurity compliance** (mandatory)
- **CRA preparation** (ahead of 2027 enforcement)

Key Requirements for CE Marking under RED:

- Network protection (3.3 d)
- Privacy protection (3.3 e)
- Fraud prevention (3.3 f)

Key Requirements for CE Marking under CRA:

- Essential Cybersecurity Requirements
- Cybersecurity Risk Assessment
- Technical Documentation
- Conformity Assessment Procedure
  - EU Declaration of Conformity
  - Affixing the CE Marking
- Incident & Vulnerability Reporting

While manufacturers can currently self-declare cybersecurity compliance under the RED directive, starting in December 2027 the CRA will require third-party assessment or Notified Body certification for certain product categories!

Meeting the Requirements - Challenges and Solutions

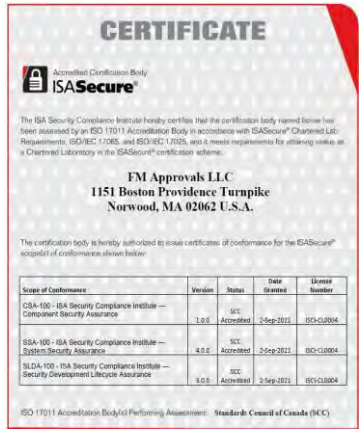
Manufacturers are **adapting their processes** to meet the RED and CRA requirements by embedding cybersecurity into every stage of the product lifecycle.

Key Challenges
Complexity of Compliance
Legacy Systems and Outdated Practices
Resource Constraints
Reporting Obligations
Supply Chain Risks
Lifecycle Support

Solutions
Early Gap Analysis
Secure Development Practices
Automated Vulnerability Management
SBOM and Documentation
Internal Reporting Workflow
Supply Chain Due Diligence

FM Approvals & Third-Party Assessment

ISASecure® is a third-party conformity assessment scheme based on the ISA/IEC 62443 series of standards.


CERTIFICATE

Accredited Certification Body
ISASecure®

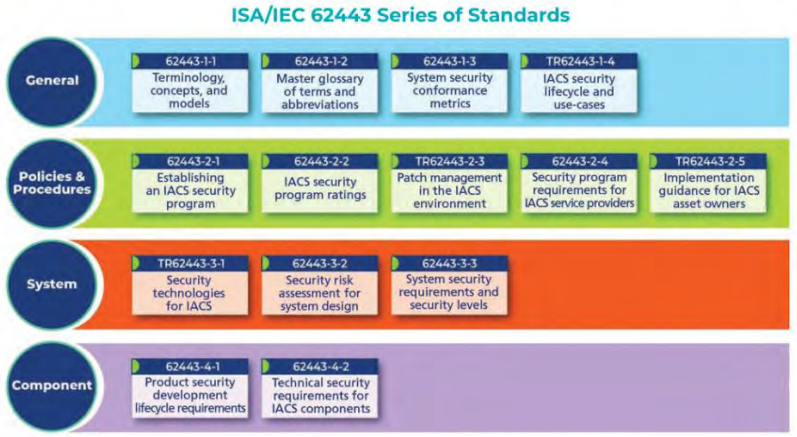
The ISA Security Compliance Institute hereby certifies that the certification body named below has been assessed by an ISO 17011 Accreditation Body in accordance with ISASecure® Chartered Lab Requirements, ISO/IEC 17065, and ISO/IEC 17025, and it meets requirements for obtaining status as a Chartered Laboratory in the ISASecure® certification scheme.

FM Approvals LLC
1151 Boston Providence Turnpike
Norwood, MA 02062 U.S.A.

The certification body is hereby authorized to issue certificates of conformance for the ISASecure® scope(s) of conformance shown below:

Scope of Conformance	Version	Status	Date Granted	Licensed Number
CSA-100 - ISA Security Compliance Institute — Component Security Assurance	1.0.0	SCC Accredited	2-Sep-2021	ISCI-CL0004
SSA-100 - ISA Security Compliance Institute — System Security Assurance	4.0.0	SCC Accredited	2-Sep-2021	ISCI-CL0004
SLDA-100 - ISA Security Compliance Institute — Security Development Lifecycle Assurance	3.0.0	SCC Accredited	2-Sep-2021	ISCI-CL0004

ISO 17011 Accreditation Body(s) Performing Assessment: Standards Council of Canada (SCC)

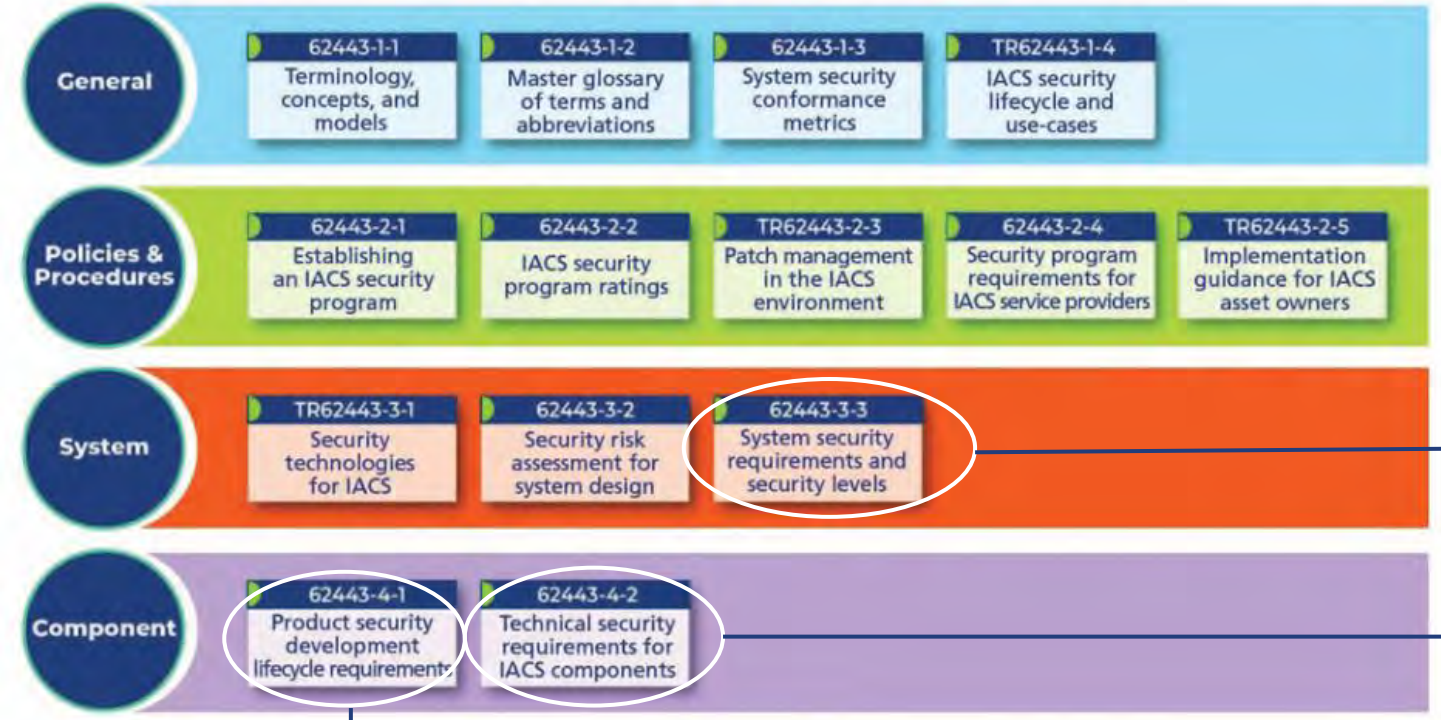


CRA Harmonized standards based on ICE 62443!

- **FM Approvals** can already perform **third-party assessments!**
- When **FM Approvals is accredited as a Notified Body (NB):**
  - Certificates may be easily converted
  - Labels need to be updated with the NB number

CE 9999

FM Approvals Cybersecurity Certification Programs for ICS and IIoT Products According to ISA/IEC 62443



FM APPROVED
SL4 CYBER SECURE

ISA

Certified Component ISASecure
Certified System ISASecure
Certified Site ISASecure

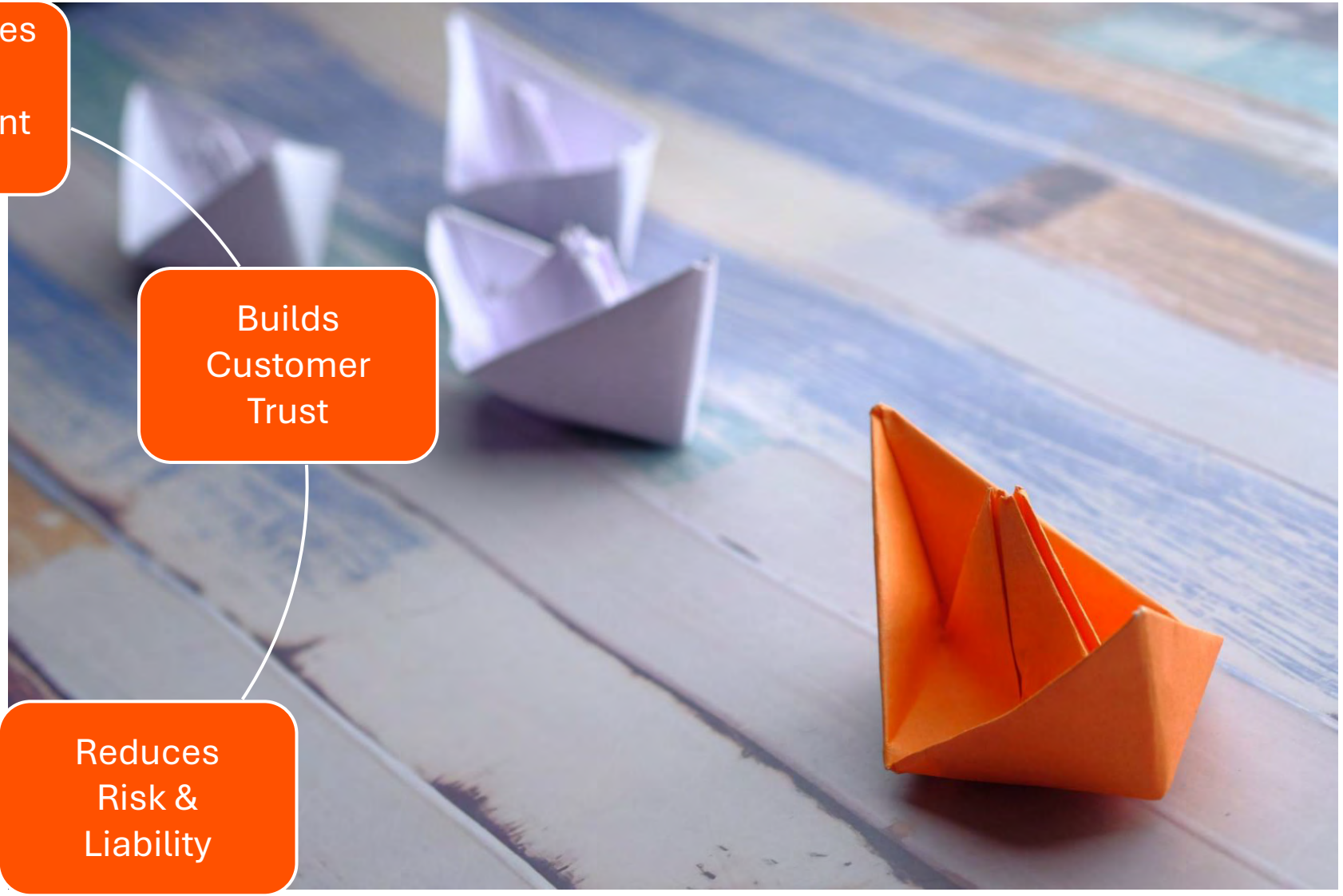
SSA – System Security Assurance:
ISA/IEC **62443-3-3**

CSA – Component Security Assurance:
ISA/IEC **62443-4-2** (ISASecure IIoT Scheme)

SDLA – Security Development Lifecycle Assurance:
ISA/IEC **62443-4-1 - prerequisite**

- **Gap Analysis** (questionnaire, report)
- **SDLA Readiness** (GA, certification valid for 1 year)
- **Full SDLA** (artifacts, processes used for development)

Benefits of SDLA and Cybersecurity Certification in General



Key Takeaways

Cybersecurity certification is an assessment of the design and the product.

Cybersecurity assessment and reporting is becoming a global requirement.

Early adoption of ISA/IEC 62443 has many benefits.

Region	US	EU
Products /Year	2023**	2026*/2027**
Elevators & Escalators	ASME 17.1	CRA
FAB Equipment	SEMI E187-0122	CRA
Life Safety	NEC/NFPA 72	CRA
Remote Access Breakers	NEC	CRA
COPS	NEC	CRA
Digital Elements		CRA

*Requires reporting of vulnerabilities

**Requires Cybersecurity Assessment

Products with digital elements that have been placed on the market before… [36 months from the date of entry into force of this Regulation], shall be subject to requirements of this Regulation only if, from that date, those products are subject to substantial modifications.

CRA – Useful Links for Download

You can download the official **CRA** text from the **EUR-Lex website**, which hosts the authentic version of **Regulation (EU) 2024/2847**:

•Direct link to the official text (HTML and PDF):

EUR-Lex: Regulation (EU) 2024/2847 – Cyber Resilience Act [eur-lex.europa.eu]

•PDF version of the Official Journal:

Download PDF [eur-lex.europa.eu]

Direct Annex Links:

Cyber Resilience Act Annexes – Official EU Source

EUR-Lex Official Regulation (EU) 2024/2847

Detailed Annex Overview

Annex I – Essential cybersecurity requirements

Annex II – Information and instructions to the user

Annex III – Important products with digital elements (Classes I & II)

Annex IV – Critical products with digital elements

Annex V – EU Declaration of Conformity

Annex VI – Simplified EU Declaration of Conformity

Annex VII – Content of the technical documentation

Annex VIII – Conformity assessment procedures

Some Common Questions

Is the certified product secure enough?

Certified products are free of known vulnerabilities. They have security features designed into them (at their targeted security levels).

Can we certify a product which has SDLA from another lab?

Yes — new products can be certified as long as SDLA certification remains valid.

If certified products can be involved in cybersecurity incidents, what is the value of product certification?

Certified products decrease the attack surface and hence the overall risk of an ICS system.

What is the value of certified products if threats are constantly changing?

Adoption and practice of SDLA processes includes future planning to address vulnerabilities as they are found.

Do the products need re-certification? What if there is a new software version?

Products do not need re-certification if no changes are made to it; 2 types of changes:

- **Updates**: bug-fixes and patches; no new functionality or features — **do not need** re-certification.
- **Upgrades**: new features and functionality — **need** re-certification.

Thank you!

nejra.lalic@fmapprovals.com

FM Approvals

Approvals