FLECS

COMPREHENSIVE GUIDE

EU Cyber Resilience Act Compliance for Industrial Automation

Clear guidance based on official EU sources, Linux Foundation research, and industry best practices. Everything you need to understand and prepare for CRA compliance.

21	Dec 2027	~90%
Essential Requirements	Full Enforcement	Self-Assessment

Executive Summary

The EU Cyber Resilience Act (CRA) represents the most significant regulatory shift for industrial automation in a decade. Entered into force on 10 December 2024, it mandates cybersecurity requirements for all products with digital elements sold in the European Union by 11 December 2027.

> *"62% of respondents are 'not familiar at all' or only 'slightly familiar' with the CRA. Only 25% correctly identified 2027 as the target year for full compliance."*
>
> **— Linux Foundation Research, "Unaware and Uncertain", March 2025**

This guide provides transparent, education-first CRA guidance—showing exactly what the regulation requires, when it's required, and how industrial automation manufacturers can prepare for compliance.

What is the EU Cyber Resilience Act?

The Cyber Resilience Act (CRA) is an EU regulation that establishes mandatory cybersecurity requirements for all products with digital elements sold in the European Union. Unlike previous regulations, the CRA requires security by design throughout the entire product lifecycle.

Key Facts

- Entered into force: 10 December 2024
- Full enforcement: 11 December 2027
- Applies to: Hardware & software with network connectivity
- Scope: Manufacturers, importers & distributors

What's New

- Security by design throughout lifecycle
- Mandatory vulnerability reporting (24h)
- Software Bill of Materials (SBOM)
- CE marking for cybersecurity compliance

Who's Affected?

Industrial automation products are explicitly in scope. This includes IoT devices, PLCs, controllers, gateways, and connected software. The regulation applies to all manufacturers, importers, and distributors placing products on the EU market.

CRA Implementation Timeline

The CRA provides a 36-month transition period with phased milestones. Understanding these dates is critical for planning your compliance journey.

Dec 2024	Jun 2026	Sep 2026	Dec 2027
CRA entered into force	Conformity bodies notification	Vulnerability reporting begins	Full enforcement

Key Milestone: September 2026

From 11 September 2026, manufacturers must report actively exploited vulnerabilities to ENISA within 24 hours. This is the first mandatory compliance milestone before full enforcement.

Industry Reality: Current CRA Readiness

Research from the Linux Foundation (March 2025) reveals significant gaps in CRA awareness and preparedness across the industry:

62%	34%	46%	~90%
Unfamiliar with CRA requirements	Produce comprehensive SBOMs	Rely on upstream for security	Products eligible for self-assessment

> *"Only 34% of manufacturers produce comprehensive SBOMs. 46% passively rely on upstream projects for security fixes."*
> **— Linux Foundation, "Unaware and Uncertain: The Stark Realities of CRA Readiness in Open Source"**

These statistics highlight both the challenge and opportunity for manufacturers who act early. Organizations that prepare now will have a competitive advantage when full enforcement begins.

CRA Annex I: The 21 Essential Requirements

CRA Annex I defines the specific cybersecurity requirements that all products with digital elements must comply with. These are organized into two parts: Product Security Requirements (13) and Vulnerability Handling Requirements (8).

21 Requirements in 2 Categories

Part I: Product Security (13) | Part II: Vulnerability Handling (8)

Part I: Product Security Requirements (13)

Ref	Requirement	Summary
I.1	**No known vulnerabilities**	Ship without exploitable vulnerabilities
I.2a	**Secure by default**	Secure configuration out of the box
I.2b	**Minimal attack surface**	Only necessary components enabled
I.2c	**Data protection**	Protect stored data appropriately
I.2d	**Secure communications**	Encrypted data in transit
I.2e	**Access control**	Authentication and authorization
I.2f	**Integrity protection**	Detect unauthorized modifications
I.2g	**Security logging**	Audit trails for security events
I.2h	**Recovery capability**	Backup and restore functions
I.2i	**Network isolation**	Don't compromise other systems
I.2j	**Minimal interfaces**	Reduce exposed attack vectors
I.2k	**Incident containment**	Limit breach impact
I.2l	**Monitoring opt-out**	User control over telemetry

Part II: Vulnerability Handling Requirements (8)

Part II focuses on how manufacturers must handle vulnerabilities throughout the product lifecycle, including documentation, disclosure, and communication with authorities.

Ref	Requirement	Summary
II.1	**SBOM documentation**	Machine-readable component inventory
II.2	**Separate security patches**	Decouple security from features
II.3	**Security testing**	Regular pentests and assessments
II.4	**Vulnerability disclosure**	Publish fixed vulnerabilities
II.5	**Disclosure policy**	Process for security reports
II.6	**ENISA communication**	24h reporting to EU agency
II.7	**Signed updates**	Cryptographic verification
II.8	**Free security updates**	No charge for patches

Software Bill of Materials (SBOM)

The CRA requires manufacturers to maintain an SBOM—a complete inventory of software components in your product. This is specified in Part II, Requirement 1.

SBOM Requirements

- Machine-readable format (SPDX, CycloneDX, or SWID)
- Minimum: top-level dependencies
- Provide to market surveillance on request
- Not required to be publicly available

Why SBOM Matters

- Traces all components included
- Identifies deployed versions
- Enables vulnerability tracking
- Ensures license compliance

CRA Article 6 & Annexes III/IV: Product Classification

The CRA categorizes products based on cybersecurity risk. Your category determines the conformity assessment procedure required. Understanding your classification is essential for compliance planning.

Default Category

~90% of products

Assessment: Self-assessment (Module A)

Products not listed in Annex III or IV. Manufacturers can self-declare conformity using internal control procedures.

Examples: Basic HMI panels, Simple sensors, Data loggers, Industrial monitors, Basic edge devices

Important Class I

~8% of products

Assessment: Harmonised standards or third-party

If harmonised standards exist and are applied, self-assessment is permitted. Otherwise, third-party assessment required.

Examples: Identity management systems, VPN devices, Network management, SIEM systems, Update/patch management tools

Important Class II

~1.5% of products

Assessment: Third-party required

Mandatory third-party conformity assessment by notified bodies. No self-assessment option regardless of standards.

Examples: Hypervisors, Container runtimes, Industrial firewalls, Intrusion detection/prevention, Tamper-resistant microcontrollers

Critical

<0.5% of products

Assessment: European cybersecurity certification

Products for critical infrastructure. Require certification under EU cybersecurity certification schemes.

Examples: Hardware Security Modules (HSMs), Smart meter gateways, Secure elements for critical systems

Key Insight: Most Products Qualify for Self-Assessment

Approximately 90% of products fall into the Default category, allowing manufacturers to self-declare conformity using internal control procedures (Module A). This significantly reduces the compliance burden for most industrial automation products.

FLECS Platform: CRA Compliance Status

FLECS provides transparent tracking of our CRA compliance capabilities. Below is our current status against all 21 Annex I requirements.

12 of 21 Requirements Covered

Full CRA Coverage Planned by December 2027

Part I: Product Security — FLECS Status

Ref	Requirement	Summary	FLECS
I.1	**No known vulnerabilities**	Ship without exploitable vulnerabilities	Coming Soon
I.2a	**Secure by default**	Secure configuration out of the box	Covered
I.2b	**Minimal attack surface**	Only necessary components enabled	Covered
I.2c	**Data protection**	Protect stored data appropriately	Covered
I.2d	**Secure communications**	Encrypted data in transit	Covered
I.2e	**Access control**	Authentication and authorization	Covered
I.2f	**Integrity protection**	Detect unauthorized modifications	Coming Soon
I.2g	**Security logging**	Audit trails for security events	Beta
I.2h	**Recovery capability**	Backup and restore functions	Covered
I.2i	**Network isolation**	Don't compromise other systems	Covered
I.2j	**Minimal interfaces**	Reduce exposed attack vectors	Covered
I.2k	**Incident containment**	Limit breach impact	Covered
I.2l	**Monitoring opt-out**	User control over telemetry	Covered

Part II: Vulnerability Handling — FLECS Status

Ref	Requirement	Summary	FLECS
II.1	**SBOM documentation**	Machine-readable component inventory	Coming Soon
II.2	**Separate security patches**	Decouple security from features	Covered
II.3	**Security testing**	Regular pentests and assessments	Coming Soon
II.4	**Vulnerability disclosure**	Publish fixed vulnerabilities	Coming Soon
II.5	**Disclosure policy**	Process for security reports	Coming Soon
II.6	**ENISA communication**	24h reporting to EU agency	Coming Soon
II.7	**Signed updates**	Cryptographic verification	Coming Soon
II.8	**Free security updates**	No charge for patches	Covered

21 Requirements. One Platform.

FLECS simplifies CRA compliance for industrial automation manufacturers.

D On the Device

Active

Managed Operating System I.2a II.7
Maintained, update-capable OS with defined update channels

App Lifecycle Management II.2 II.8
Fully automated installation, updates & maintenance

Security by Design I.2e I.2f
RBAC & certificate-based communication built-in

App Ecosystem I.2b I.2j
60+ standard apps for rapid controller extension

P Central Service Portal

Active

Download Portal II.7 II.8
Tools, drivers & firmware for all systems

License Management I.2e
Secure license provisioning & activation

Structured Distribution II.2 II.4
Support for existing update processes

Automated Release II.3 II.7
CI/CD pipeline with security testing

C Compliance Management

Coming Soon

SBOM Integration II.1
Automated Software Bill of Materials generation

CVE Scanning I.1 II.6
Automated vulnerability detection & ENISA reporting

Update Notifications II.4 II.5
Proactive alerts & coordinated disclosure

Resources & Referenced Standards

Official EU Sources

- **Regulation (EU) 2024/2847** — Official Journal of the EU, November 20, 2024
- **EU CRA Policy Page:** digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
- **CRA Summary:** digital-strategy.ec.europa.eu/en/policies/cra-summary

Linux Foundation & OpenSSF

- **"Unaware and Uncertain" (Mar 2025)** — CRA readiness research: 62% unfamiliarity, 34% SBOM rate
- **Free Course LFEL1001** — 90-minute training at training.linuxfoundation.org
- **Open Regulatory Compliance WG** — Community resources at orcwg.org/cra
- **SBOM Catalog** — SBOM formats and guidance at sbom-catalog.openssf.org

Industry Standards Referenced in CRA

Standard	Description	CRA Relevance
IEC 62443	Industrial Automation Security	Annex I alignment
SPDX / CycloneDX	SBOM Formats	Part II (1) requirement
BSI TR-03183	German SBOM Guideline	Implementation
ENISA Mapping	Standards Alignment	Verification

Additional Resources

From FLECS

- CRA Requirements Checklist (PDF)
- Product Classification Quiz
- CRA Landing Page at flecs.tech

Industry Analysis

- TÜV Rheinland CRA Overview
- Pilz CRA Requirements Page
- VDMA/ZVEI Industry Guidance

Next Steps: Your CRA Compliance Journey

The EU Cyber Resilience Act represents a significant regulatory shift, but with proper preparation, compliance is achievable for industrial automation manufacturers. Here's how to get started:

1. Understand Your Classification

Use the CRA product classification framework to determine which category your products fall into. Remember that ~90% of products qualify for self-assessment under the Default category.

2. Assess Your Current State

Review the 21 Annex I requirements against your current product security practices. Identify gaps and prioritize based on your product classification and the CRA timeline.

3. Start SBOM Implementation

Begin documenting your software components using SPDX or CycloneDX format. This is a foundational requirement that enables vulnerability tracking and compliance documentation.

4. Prepare for September 2026

Establish processes for vulnerability reporting to ENISA within 24 hours. This is the first mandatory milestone before full enforcement in December 2027.

Ready to Learn More?

See how FLECS simplifies CRA compliance for industrial automation with built-in security updates, automated vulnerability tracking, and ready-to-use conformity documentation.

Contact FLECS

- Website: flecs.tech
- CRA Resources: info.flecs.tech/cra-compliance
- Documentation: docs.flecs.tech

This guide is provided for informational purposes based on official EU sources and industry research. Always verify requirements against the official CRA regulation text. FLECS Technologies GmbH makes no warranties regarding the completeness or accuracy of this information for your specific compliance needs. Consult with qualified legal and technical advisors for your organization's compliance strategy.