01 SCOPE

Noex

Does your machine fall under the CRA?

The Cyber Resilience Act (CRA) normally applies to products with **digital elements** that are intended for use or can reasonably be expected to be used, directly or indirectly, with a data connection.

1 STEP 1

Does the product have digital elements?

This means that the product contains software or hardware with digital functionality.

Examples

- PLC
- HMI
- Industrial PC
- Frequency converter
- Safety control system
- Embedded software

YES

2 STEP 2

Is the product connected?

This means that the product is directly or indirectly connected to a device or a network.

Examples

- Ethernet
- Profinet
- OPC UA
- USB
- WLAN
- Bluetooth
- Remote access

Type of connection

Logical connection
Via software or network protocols.

Physical connection
Via cable, radio waves or another physical interface.

Indirect connection
E.g., via factory network, gateway or cloud service.

YES

The CRA normally applies if both of the above criteria are met.

Even indirect connection via, for example, factory network or gateway can be covered.

3 STEP 3

Is the product excluded?

Some product categories are not covered by the CRA.

Examples of exclusions

- Medical devices
- In vitro diagnostic devices
- Certain vehicles
- Aerospace products
- Marine products, etc.

NO

IMPORTANT: TAKE ACTION NOW!

The product is normally covered by the CRA.

- Development requirements
- Security requirements
- Vulnerability management

Start working on ensuring compliance now and plan for continuous security throughout the product's lifecycle.

YES

The product is not covered by the CRA.

Document the assessment and the basis for the conclusion.

Important to consider

The assessment must be based on the product's intended purpose and reasonably foreseeable use. Some product categories covered by other sector-specific legislation may therefore be excluded.

Reference

CRA Article 2 (scope) and Article 3 (definitions).

02 REPORTING OBLIGATIONS • ARTICLES 14 & 16

Noex

Reporting obligations from 11 September 2026

From and including 11 September 2026, manufacturers must report:

- **Actively exploited vulnerabilities**
- **Serious incidents** that affect the security of products with digital elements

REPORTING TIMELINE

1. Early warning

≤ 24 hours

After the manufacturer becomes aware of:

- an actively exploited vulnerability or
- a serious incident that affects the security of the product

2. Formal notification

≤ 72 hours

Information on:

- the vulnerability or incident
- its impact
- measures taken or planned corrective actions
- measures that the user can take

3. Final report

(actively exploited vulnerability)

14 days

At the latest 14 days after corrective or risk-reducing measures have become available.

The report must include, among other things:

- description of the vulnerability
- consequences or severity level
- information on security updates or other corrective measures

4. Final report

(serious incident)

1 month

At the latest one month after the incident notification.

The report must include, among other things:

- detailed description of the incident
- root cause analysis
- corrective and preventive risk-reducing measures

Common reporting platform

Reporting must be done via **ENISA's common reporting platform** in accordance with Article 16.

The platform will forward the information to relevant CSIRT entities and Member State authorities to which the product is supplied, as well as other relevant authorities.

Affected users must be informed

The manufacturer must inform affected users, without undue delay, when informed about:

- the vulnerability or incident
- possible consequences
- risk-reducing measures
- available corrective measures

The information must, where possible, be provided in a **structured and machine-readable format**.

The deadlines are counted from the time the manufacturer becomes aware of the event. The reporting obligations are set out in **Article 14**. Reporting is done via the common reporting platform described in **Article 16**.

Source

Cyber Resilience Act (EU) 2024/2847, Articles 14 and 16

03 THE CHALLENGE

Noex

Many components – many potentiali vulnerabilities

A modern machine system often consists of many products with digital elements. Every component can be affected by its own cybersecurity risks, security updates and reporting obligations.

COMPONENTS IN A MACHINE SYSTEM

SENSORS

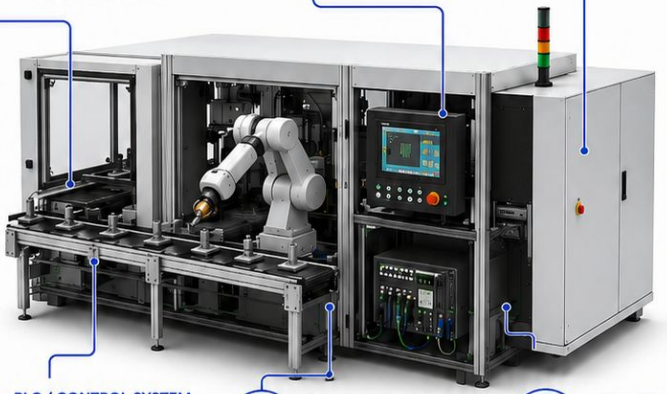
Collect data from the machine's environment, processes and status.

HMI / OPERATOR PANEL

Interface for monitoring and interaction between the operator and the machine.

DRIVE SYSTEM

Frequency converters, servo drives and other systems that control movement and power.



PLC / CONTROL SYSTEM

Programmable control that manages the machine's logic and functions.

GATEWAY / NETWORK

Connects various components enabling communication and data exchange.

INDUSTRIAL PC

Runs applications, stores data and handles local processing in the machine.

Every component must be assessed.

When new vulnerabilities become publicly known, manufacturers must determine:

- Whether the affected component is used in our product
- Whether the vulnerability affects our product
- Whether risk-reducing or corrective measures are required
- Whether reporting obligations under the CRA must be updated

Manual analysis is time-consuming

To identify, assess and follow up on vulnerabilities in a large number of digital components requires significant resources – which is why the deadlines of **24 and 72 hours** must be met.

Important to consider

Manufacturers are responsible for having a structured process and the necessary tools to manage vulnerabilities in all relevant components – on an ongoing basis.

Source

Cyber Resilience Act (EU) 2024/2847, Articles 14 and 16

04 THE SOLUTION • CSAF

Noex

CSAF – structured and machine-readable security information

CSAF

CSAF (Common Security Advisory Framework) is an open standard for publishing security information in a structured and machine-readable format. The standard enables automatic processing of vulnerabilities, security updates and affected products based on recommendations from multiple vendors.

1 Structured information

The vendor publishes security information about vulnerabilities, affected products and measures in CSAF format (JSON).

2 Machine-readable format

The information is structured and machine-readable, which enables automatic interpretation without manual intervention.

3 Automated processing

Systems and tools can automatically retrieve, filter and handle the information.

4 Identify affected products

It is easy to identify which products, components and versions are affected.

5 Recommended measures

Recommended actions and recommendations can be communicated and understood by the receiving system.

Faster and more effective vulnerability management

Structured and machine-readable information reduces manual handling, the risk of errors and the time from publication until action is taken.

Article 14.8 of the CRA requires that such information, when available, be made available in a format that can be automatically processed.

CSAF in brief

Open standard
CSAF is an open standard that anyone can use.

OASIS standard
Developed and governed within OASIS Open.

ISO/IEC 20153
CSAF is an international standard ISO/IEC 20153.

Machine-readable format
Security information is published in JSON format for easy processing and automation.

Benefits for your organization

- Less manual handling and faster processes
- Reduced risk of errors and critical oversight
- Better interoperability between systems and organizations
- Accurate and current information – at the right time
- Support for automation and scalable vulnerability management

Faster identification of affected components

When vendors publish security information in CSAF format, tools can automatically identify which components are affected and assess the impact on the product.
This reduces manual effort and streamlines the work with vulnerability management.

Source
Cyber Resilience Act (EU) 2024/2847, Article 14.8

05 IN PRACTICE

Noex

CSAF makes security information easier to use

When vendors publish security advisories in CSAF format, the information can be processed automatically and integrated into organizations' processes for vulnerability management.

This makes it easy to identify affected products, assess the impact on your products and handle security information from multiple vendors.

How it works in practice

1. **The vendor publishes a security advisory in CSAF format**
   Structured information on vulnerabilities, affected products and measures.
2. **The information is published**
   The advisory is made available via web servers or integration channels.
3. **Automatic processing**
   Systems and tools automatically retrieve, interpret and validate the CSAF data.
4. **Identification of affected products**
   Affected products, components and versions are matched against your environment.
5. **Recommended measures**
   Recommendations and measures are presented and can be integrated into workflows.

CSAF format – machine-readable

- Structured JSON format
- Designed for automatic processing
- Easy integration into tools and processes
- Supports speed and consistent information

PDF format – human-readable

- Suitable for manual reading
- Requires manual review and interpretation
- More difficult to integrate into systems
- Risk of missed or delayed information

More effective handling of security information

Machine-readable security information reduces manual work and provides faster access to relevant information about:

Affected products | Identified vulnerabilities | Recommended measures

Benefits of using CSAF in practice

Faster response
Automated handling shortens the time from publication until action is taken.

Higher accuracy
Exact matching against products and versions reduces the risk of errors.

Easy integration
Works well with existing tools and processes via open standards.

Scalable
Handles large volumes of information from multiple vendors simultaneously.

Improved security
The right information at the right time provides better decision-making and reduces risks.

By using CSAF format, organizations can create a more automated, reliable and scalable process for handling security information – regardless of the number of vendors.

Source
Cyber Resilience Act (EU) 2024/2847, Article 14.8

06 GET CONTROL OVER CRA REQUIREMENTS

Noex

From requirements to practical work

To comply with the Cyber Resilience Act (CRA), vendors need control over their components, cybersecurity risks, vulnerabilities and security updates **from development to the end of the product's support period.**

Below are six key areas that help you build a process for meeting the CRA's requirements in practice.

1 Control over components

Identify and document

- Hardware
- Software
- Open Source components
- Supplier components

Result

Software Bill of Materials (SBOM) and component inventory

CRA support: Annex I | Part II point 1

2 Identify vulnerabilities

Detect and assess risks

- Supplier advisories
- CVE databases
- CSAF advisories
- Reported vulnerabilities
- Contact point for vulnerability reporting (Article 13.17)

Result

Awareness of new security issues

CRA support: Annex I | Part II points 5–6

3 Assess impact

What is the impact?

- Does it affect our product?
- How critical is the issue?
- Is a fix needed?
- Is reporting required?

Result

Prioritized actions

CRA support: Article 13.2–13.4

4 Take action and test

Manage identified risks

- Security updates
- Security reviews
- Security tests

Result

Reduced cybersecurity risk

CRA support: Annex I | Part II points 2–3

5 Inform users

Share relevant information

- Security Advisories
- Affected products
- Recommended measures
- Security updates

Result

Users can take action in time

CRA support: Annex I | Part II point 4 Article 14.8

6 Manage the support period

Maintain security over time

- Security updates
- Documentation
- Contact point
- Reporting as required by Article 14
- Inform about the end of the support period (Article 13.19)

Result

End of support managed according to CRA

CRA support: Articles 13.8–13.23

GET CONTROL OVER CYBERSECURITY

Continuous management from development to the end of the support period

Important to keep in mind

The CRA is not only about reporting. Vendors must identify components, manage vulnerabilities, distribute security updates and inform users **from development to the end of the support period.**

Learn more about the CRA

- Article 13 – Obligations for vendors
- Article 14 – Reporting
- Annex I | Part I – Requirements for the characteristics
- Annex I | Part II – Vulnerability management requirements

Source

Cyber Resilience Act (EU) 2024/2847