INTRODUCING THE CYBER RESILIENCE ACT (CRA)

The European regulatory landscape is undergoing a major transformation with the adoption of the Cyber Resilience Act (CRA). This regulation came into force in December 2024 and represents a decisive step in securing digital products marketed in the European Union. For manufacturers of machinery, industrial equipment and connected products, this regulation introduces new obligations that profoundly transform design and marketing practices.

What is the CRA?

The Cyber Resilience Act (EU Regulation 2024/2847) is a directly applicable European regulation that establishes harmonised cybersecurity requirements for all "products with digital elements" made available on the European Union market. Unlike directives that require national transposition, the CRA applies uniformly in all Member States from the time of its entry into force.

A directly applicable regulation

The directly applicable nature of the CRA means that no national transposition is necessary. Manufacturers, whether established in the EU or in third countries, must comply with the same requirements to market their products on the European market. This standardization aims to create a homogeneous level of safety and to avoid regulatory fragmentation.

Scope of application

The ARC applies to any product with digital elements, i.e. any hardware or software capable of processing digital data. This includes:

- Consumer products (smartphones, laptops, connected objects, home automation)
- Connected industrial equipment (machines, robots, PLCs)
- Control systems (PLC, SCADA, DCS)
- IoT and IIoT devices
- Embedded software and firmware
- The cybersecurity components themselves

The regulation covers the entire life cycle of the product, from its design to its decommissioning, distribution and use.

What are the objectives of the CRA?

The Cyber Resilience Act pursues several strategic objectives that reflect current cybersecurity challenges in a context of increasing interconnection of industrial and consumer systems.

Strengthen security by design

The central objective of the CRA is to impose a "security by design" approach for all digital products. This philosophy requires that cybersecurity be integrated from the earliest stages of development, not added as an additional layer after the fact. Manufacturers must anticipate threats, assess risks and implement appropriate protection mechanisms even before they are released to the market.

Improving transparency and trust

The ARC aims to create an environment of trust by requiring manufacturers to clearly communicate the safety features of their products. Users and integrators should be able to easily identify compliant products with the CE mark and have detailed information on implemented security measures, known vulnerabilities and available updates.

Creating a chain of responsibility

By making all economic actors (manufacturers, importers, distributors) responsible, the regulation establishes a clear chain of responsibility. Each stakeholder must ensure that the products they make available meet the requirements of the ARC, creating

an ecosystem where cybersecurity becomes a shared concern.

Harmonising requirements at European level

Regulatory harmonization avoids the proliferation of divergent national standards that would complicate cross-border marketing. A CRA compliant product can be freely marketed throughout the European Union, simplifying the process for manufacturers while ensuring a uniform level of protection for users.

What is changing with the CRA?

The coming into force of the Cyber Resilience Act marks a paradigm shift for the manufacturing industry and software companies. The obligations imposed profoundly transform established practices.

A restrictive regulatory approach

Contrary to the recommendations and voluntary good practices that prevailed until now, the CRA imposes legally binding obligations. Manufacturers can no longer choose to ignore cybersecurity: it is becoming a legal condition for accessing the European market, in the same way as functional safety or electromagnetic compatibility.

Proactive vulnerability management

One of the major innovations of the CRA concerns vulnerability management. The regulation distinguishes between two types of vulnerabilities that require a rapid response:

- **Actively exploited vulnerabilities** : When a manufacturer discovers that a vulnerability in their product is being exploited maliciously in real-world conditions, they have 24 hours to make an initial notification, 72 hours to provide initial corrective actions, and 14 days to submit a final report.
- **Exploitable vulnerabilities** : These vulnerabilities have the potential to be exploited under practical operational conditions. Although the CRA does not impose strict deadlines for their processing, they must no longer be present in products marketed after the date of full application of the regulation.

The obligation to support over the long term

The ARC requires manufacturers to provide security updates for a minimum period of 5 years after placing on the market. This obligation transforms the business model of many manufacturers who are used to a single sales logic, by forcing them to maintain a continuous relationship with their products and customers.

Traceability and documentation

Documentary requirements become considerably more important. Manufacturers must compile and maintain detailed technical documentation, including:

- Cybersecurity risk analysis
- Description of security features
- Test and evaluation results
- The vulnerability management process
- Safe installation and use instructions

This documentation must be kept for 10 years and made available to the supervisory authorities upon request.

Who is concerned by the CRA?

The scope of application of the Cyber Resilience Act is deliberately broad to cover all economic actors involved in the provision of digital products.

Manufacturers

Manufacturers are the category of actors most directly concerned. The following are considered to be manufacturers:

- Companies that design and produce products with digital elements
- Companies that have such products designed or manufactured and market them under their name or brand name

- Importers who introduce products from manufacturers established outside the EU into the European market
- Distributors who become liable when they substantially modify a product or make it available when it is manifestly non-compliant

This broad definition includes large industrial groups as well as SMEs and startups developing connected solutions.

Industrial sectors particularly affected

Several sectors are particularly concerned by the CRA:

Manufacturing : Manufacturers of machine tools, production equipment, industrial robots, and programmable logic controllers are on the front line. Their products, which are increasingly connected and integrated into IIoT architectures, are fully within the scope of the regulation.

Industrial automation : Manufacturers of control systems (SCADA, DCS, PLC), smart sensors, and human-machine interfaces (HMI) must adapt their development processes to meet CRA requirements.

IoT and consumer electronics : Connected products for individuals (connected objects, home automation equipment, surveillance devices) are also subject to the regulation.

Software vendors : Developers of operating systems, firmware, industrial applications, and cybersecurity solutions themselves must comply with the CRA.

Product classification

The CRA establishes a classification of products according to their criticality, with differentiated requirements and evaluation procedures:

Standard Products : The majority of products with digital elements fall into this category. They are subject to a self-conformity assessment by the manufacturer (Module A), which can be based on harmonised standards once they are published.

Class I (Important) Products : This category includes certain products for identity management, access control, virtual private networks, and systems that detect vulnerabilities. They require self-assessment with compliance with harmonised standards where they exist.

Class II (Important) Products : Includes, but is not limited to, operating systems, secure microprocessors, and some intrusion detection systems. They require a type examination by a notified body (Module B+C).

Critical Products : The most sensitive products (e.g. certain security components for critical infrastructure) may be subject to a European cybersecurity certification scheme.

The actors indirectly concerned

Beyond manufacturers, other stakeholders are impacted:

- **System integrators** who assemble digital products in complex installations must ensure that the components used are compliant
- **It** is in the interest of industrial operators to require CRA compliance from their suppliers to secure their facilities
- **Subcontractors and suppliers** involved in the development chain must adapt their practices to allow the final product to comply

What are the main obligations for industrial organizations?

The CRA imposes a set of obligations that structure the cybersecurity approach throughout the product life cycle. These requirements are divided into several complementary categories.

Essential cybersecurity requirements

The essential requirements set out in Annex I of the CRA constitute the safety framework that all products must meet. They include:

Security by design : Products should be designed, developed, and produced in a way that ensures an appropriate level of risk-based cybersecurity. This involves a formalised risk analysis, the identification of critical assets and potential threats, and the implementation of proportionate protection measures.

Defense in depth : The regulation encourages the adoption of multi-layered security architectures,

where several protection mechanisms reinforce each other. This approach, well known in OT environments as "defense in depth", limits the impact of a one-time compromise.

Reduced attack surface: Manufacturers should minimize unnecessary functionality, disable non-essential services, and limit access privileges to what is strictly necessary. Software and hardware components should be chosen with the fewest known vulnerabilities in mind.

Update management : Products must be able to receive security updates throughout their support period. These updates should be secure (signed, authenticated), easy to apply, and not degrade product functionality.

Vulnerability Management

Vulnerability management is one of the most demanding obligations of the ARC. Manufacturers must establish and maintain a comprehensive process that includes:

Identification and Reception : Establishment of a single point of contact to receive vulnerability reports (security.txt in accordance with RFC 9116). Manufacturers should actively monitor vulnerability databases (CVEs, NVDs) for the components they embed.

Analysis and assessment : Each vulnerability should be analyzed to determine its exploitability in the specific context of the product. This assessment must consider the intended environment of use, existing protective measures and practical operating conditions. A theoretical vulnerability in a component may not be exploitable if that component is isolated from the network or protected by other mechanisms.

Processing and remediation : Depending on criticality and operability, the manufacturer must develop and deploy patches, workarounds, or compensatory measures. The regulation recognises the concept of "virtual patching", which is particularly relevant for OT environments where software updates can be difficult to apply.

Communication : Manufacturers must communicate transparently about vulnerabilities and remediation. This communication must be both proactive (notifications to users) and reactive (responses to requests for information).

Documentation technique

The constitution of complete and up-to-date technical documentation is mandatory. This documentation should include:

- An EU declaration of conformity attesting to compliance with the essential requirements
- Documentation of cybersecurity risk analysis
- Detailed description of the product's safety properties
- Instructions for safe installation, configuration and use
- The vulnerability and update management policy
- The results of the security tests and evaluations carried out

CE marking and declaration of conformity

Before marketing a product, the manufacturer must:

- Carry out the conformity assessment according to the applicable procedure (Module A, A with harmonised standard, or B+C depending on the class)
- Draw up the EU declaration of conformity
- Affix the CE mark to the product
- Provide the necessary instructions and safety information

Support and maintenance obligations

The core obligations will not take full effect until December 11, 2027, but manufacturers should plan their long-term support strategy now. The requirement to provide security updates for at least 5 years transforms the customer relationship model and requires a dedicated organization for post-sales support.

What are the penalties provided for by the CRA?

The Cyber Resilience Act provides for a dissuasive sanctions regime to guarantee the effectiveness of the obligations imposed. National supervisory authorities have extensive powers of investigation, injunction and sanction.

Financial penalties

Fines can be as high as €15 million or 2.5% of annual worldwide turnover. This dual approach makes it possible to adapt the sanction to the size of the company: large organisations incur fines proportional to their turnover, while a floor of €15 million guarantees a deterrent effect even for smaller companies.

The proportionality of the sanctions depends on several criteria:

- The nature, seriousness and duration of the breach
- Whether the offence was intentional or negligent
- Measures taken to mitigate the damage
- The degree of cooperation with the authorities
- Any previous breaches
- The consequences of the breach on users and society

Administrative penalties

In addition to financial fines, supervisors can take various measures:

Injunctions : Obligation to bring the product into compliance within a specified period, to provide additional information, or to correct non-compliant practices.

Recall and recall : In the event of a serious breach, the authority may require the product to be withdrawn from the market and recalled from end-users. This measure, which is particularly costly and damaging to the company's image, is a major deterrent sanction.

Marketing ban : Non-compliant products may be banned from the European market until their compliance is demonstrated.

Publication of sanctions: The authorities can make the sanctions issued public, with a significant reputational impact for the companies concerned.

Civil and commercial liability

In addition to administrative penalties, manufacturers are also exposed to:

- Civil liability actions by users who have suffered damage
- A loss of trust and brand image
- Exclusion from public contracts or sectoral certifications
- Business challenges with customers demanding compliance

How to prepare for the application of the ARC?

Preparing for CRA compliance requires a methodical and phased approach. Although the main obligations apply from 11 December 2027, it is essential to start now, given the scale of the transformations to be made.

Step 1: Condition assessment

The first step is to carry out a precise diagnosis of the current situation:

Product Inventory : Identify all products with digital elements that are marketed or in development. For each product, determine its potential classification (standard, class I, class II, critical).

Gap analysis : Compare current practices with ARC requirements. Identify existing processes (secure development, vulnerability management, support) and gaps that need to be addressed.

Impact Assessment : Estimate the resources needed (human, technical, financial) to achieve compliance, as well as realistic timelines for implementation.

Step 2: Implementation of cybersecurity risk management

Risk management is the foundation of the compliance approach. It is a question of adopting a structured approach, ideally based on recognized standards such as the IEC 62443-4-1 standard for the development of secure products:

Define the system under consideration : Precisely delimit the scope of analysis (hardware components, software, interfaces, intended environment of use).

Identify assets and interfaces : List all elements of the system that are likely to be targeted by an attack (data, critical functions, communication components).

Analyze impacts: Assess the criticality of each asset in terms of confidentiality, integrity, availability and safety.

Identify threats : Use structured methodologies (Microsoft STRIDE, MITRE ATT&CK for ICS) to identify relevant threats according to the context of use.

Assess plausibility : Determine the likelihood of each threat occurring based on attacker motivation, attack opportunities, and existing protection measures.

Calculate and prioritize risks : Cross-reference impact and likelihood to obtain a level of risk, then prioritize the risks to be addressed.

Define and implement mitigation measures : Select appropriate technical and organizational measures to reduce risks to an acceptable level.

Assess the residual risk : Verify that the risks remaining after treatment are acceptable with regard to the context of use.

Step 3: Integrate security into the development lifecycle

Security must be integrated into every phase of the product lifecycle, using a Secure Development Lifecycle (SDL) approach:

Design : Define security requirements, design secure architecture, select components with security in mind.

Development : Apply secure coding practices, use static and dynamic analysis tools, perform security-oriented code reviews.

Testing and validation : Perform security tests (penetration tests, fuzzing), verify resistance to attacks identified in the risk analysis.

Placing on the market : Compile the technical documentation, carry out the conformity assessment, establish the EU declaration of conformity.

Support and maintenance : Monitor vulnerabilities, develop and deploy patches, communicate with users.

End of life : Notify users of the end of security support, provide recommendations for migration or secure retirement.

Step 4: Setting up the vulnerability management process

A robust vulnerability management process is a must:

Create a point of contact : Publish a security.txt file (RFC 9116) at the root of the company's website, indicating how to report vulnerabilities responsibly.

Vulnerability Intelligence : Monitor CVE/NVD databases for third-party components used, track vendor security advisories, participate in threat exchange communities (ISAC).

Contextual Scan : For each vulnerability identified, assess its actual exploitability in the specific context of the product. A vulnerability affecting a component that is not exposed or protected by compensatory measures may not require urgent patching.

Patch development : Prioritize patch development based on criticality and exploitability, test patches to avoid regressions, prepare Vulnerability Exploitability eXchange (VEX) documents specifying the status of each vulnerability.

Deployment and communication : Notify customers of patch availability, provide clear instructions for their application, propose workarounds if necessary.

CRA Compliance : Implement contingency procedures to meet strict deadlines for actively exploited vulnerabilities (initial notification within 24 hours, full report within 14 days).

Step 5: Organization and skills

CRA compliance requires specific skills and an adapted organization:

Designate a security product manager : Identify a person who is responsible for the subject at the executive level, with the necessary authority and resources.

Train teams : Raise awareness among all development teams, train in secure development practices, develop expertise in risk analysis and vulnerability management.

Create or strengthen the PSIRT : Establish a Product Security Incident Response Team (PSIRT) responsible for managing vulnerabilities and security incidents.

Structure governance : Define roles and responsibilities, establish decision-making processes, and set up compliance monitoring indicators.

Step 6: Collaborate with the ecosystem

Compliance cannot be achieved in isolation:

Supplier requirements : Include security clauses in contracts with component suppliers, require the provision of vulnerability and patch information (SBOM, VEX).

Communication with customers : Provide comprehensive security documentation, support integrators in secure deployment, establish communication channels for security issues.

Participation in sectoral initiatives : Join professional working groups (VDMA, other industry associations), participate in standardization work, exchange best practices.

OT/IoT Operational Checklist: 10 Key Actions

To structure your compliance approach, here is a pragmatic checklist of priority actions to implement:

1. Carry out an exhaustive inventory of the products concerned

Identify all your products with digital elements for the European market. For each, document the hardware and software components, communication interfaces, firmware versions, and determine the applicable CRA classification.

2. Perform cybersecurity risk analysis on a product-by-product basis

Apply a structured methodology (IEC 62443-4-1, ISO/SAE 21434 for vehicle-connected products) to identify critical assets, relevant threats, assess risks, and define appropriate protective measures. Formally document this analysis.

3. Implement defense-in-depth and segmentation

Adopt a multi-layered security architecture: network segmentation to isolate critical areas, firewalls and IPS to control flows, strict access control, strong authentication. This approach significantly reduces the attack surface and exploitability of vulnerabilities.

4. Deploy native OT cybersecurity solutions

OT environments require specific solutions that are different from traditional IT tools. Choose:

- Endpoint protection solutions adapted to industrial systems (support for legacy OS, no reboot required, OT whitelisting)
- IPS with deep inspection of industrial protocols (DPI over Modbus, Profinet, EtherNet/IP, etc.)
- Virtual patching solutions to protect non-patchable systems
- Removable Media (USB) Control Tools for Production Environments

5. Establish the vulnerability management process

Implement the necessary infrastructure: secure point of contact (security.txt), automated CVE monitoring, analysis and prioritization processes, the ability to develop and deploy patches in an emergency, and structured communication with customers.

6. Implement a secure update system

Design a mechanism to deploy security updates in a way that is secure (cryptographic signing, authenticated channel), simple (automation possible),

and without prolonged production disruption. Provide rollback mechanisms in case of problems.

7. Compile the technical documentation of compliance

Gather and formalize all the required documentation: risk analysis, security specifications, test results, secure configuration procedures, vulnerability management policy, secure user manual. This documentation must be kept up-to-date throughout the life cycle.

8. Define the conditions of secure use and responsibilities

Specify in the product documentation the intended context of use, the security assumptions (network environment, expected physical access controls), and the limits of liability. Some security measures are the responsibility of the end operator: clarify these responsibilities contractually.

9. Train and structure teams

Invest in skills development: training in secure development, certification in industrial cybersecurity (ISA/IEC 62443 Cybersecurity Expert), recruitment of specialized profiles if necessary. Structure the organization with dedicated roles (product security officer, PSIRT).

10. Anticipate long-term support

Plan the support strategy by design for a minimum of 5 years: architecture allowing updates, provisioning of human and technical resources for post-sales support, economic model including the cost of security support. Anticipate component obsolescence management.

How does AKENATECH support you?

Faced with the complexity and scale of the requirements of the Cyber Resilience Act, we have developed a comprehensive support approach that covers your entire compliance journey.

Recognized expertise in OT cybersecurity and regulatory compliance

Our unique positioning combines in-depth technical expertise in cybersecurity of industrial environments (OT/IoT) with a mastery of regulatory compliance issues. We are familiar with the specificities of control systems, the availability constraints of production environments, and the requirements of the IEC 62443 and ISO 27001 standards, which constitute the technical basis of CRA compliance.

End-to-end support: Strategy → Implementation → Operations

Our three-phase approach ensures a sustainable and effective transformation:

Strategy Phase - GRC Consulting

We start with an in-depth analysis of your situation:

- CRA compliance diagnosis: identification of the products concerned, assessment of deviations from requirements
- Definition of the compliance strategy: prioritization of actions, resource planning, cost estimation
- Implementation of cybersecurity risk management according to IEC 62443-4-1: product risk analysis methodology, support on your first pilot products
- Support in the preparation of technical documentation and conformity assessment procedures
- Support for CE marking for products with digital elements

This consulting phase allows you to build a clear and realistic roadmap, aligned with your business constraints and your business objectives.

Implementation Phase - Solution Integration

Once the strategy has been defined, we move on to the concrete implementation:

- **Endpoint protection** : deployment of native cybersecurity solutions for OT, adapted to industrial and legacy systems (Windows 2000/XP and Linux support, no reboot required, automatic whitelisting of OT applications)
- **Visibility and detection** : implementation of network monitoring solutions with in-depth inspection of industrial protocols (DPI on 200+ OT protocols), anomaly and intrusion detection
- **Hardening systems** : application of secure configuration best practices, disabling unnecessary services, enhanced access control
- **Sealing and integrity** : solutions to protect against unauthorized modification, removable media (USB) control suitable for production environments
- **Segmentation and defense in depth** : secure network architecture with IPS/IDS, industrial firewalls, critical area isolation

We favor proven solutions in OT environments, with recognized technology partners such as TXOne Networks, which offer virtual patching mechanisms that are particularly adapted to the constraints of the CRA.

Operations Phase - Managed Services

CRA compliance is not a one-time project but a long-term commitment. We ensure the continuity of your compliance:

- **Time-sharing CISO** : provision of an experienced Information Systems Security Manager to manage your product security approach without recruiting internally
- **Semi-outsourced PSIRT** : operational management of your vulnerabilities, automated CVE monitoring, exploitability analysis, coordination of development and deployment of patches, communication with customers and authorities
- Ongoing support for the evolution of your documentation and processes

A pragmatic and operational approach

Our methodology is designed to be pragmatic and adapted to industrial realities:

- Consideration of production constraints (availability, legacy, air-gapped environments)
- Phased and prioritized approach to controlling investments
- Skills transfer to empower your teams
- Reuse of existing analyses and investments (ISO 27001, NIS2, IEC 62443)

Synergy with other regulations

The CRA does not apply in isolation. We help you create synergies with your other compliance efforts:

- **Machinery Regulation 2023/1230** : coordination of common cybersecurity requirements with the CRA
- **NIS2** : Alignment of Organizational and Technical Measures for Critical Operators
- **ISO 27001** : Integrating product security into your information security management system
- **IEC 62443** : a reference technical standard for industrial cybersecurity, recognized as a solid foundation for CRA compliance

FAQ

When does the CRA really come into force?

The Cyber Resilience Act came into force on December 10, 2024. However, the obligations are gradually being applied:

- **September 11, 2026** : Obligation to report actively exploited vulnerabilities and serious security incidents
- **December 11, 2027** : Full enforcement of all requirements, including a ban on marketing products with known exploitable vulnerabilities

It is therefore crucial to start your process now, because the necessary transformations take time.

Is my product covered by the CRA?

If your product has digital elements (hardware or software capable of processing digital data) and is intended to be marketed in the European Union, it is most likely affected. This includes:

- Consumer products incorporating digital elements
- Industrial machines with programmable logic controllers
- Connected equipment (IoT/IIoT)
- Control systems (SCADA, DCS, PLC)
- Electronic components with firmware
- Embedded software and industrial applications

Some exemptions exist (medical devices, vehicles, aeronautics already covered by other specific regulations), but they are limited.

What is the difference between the ARC and the Machinery Regulations?

The **Machinery Regulation (EU) 2023/1230** applies specifically to machinery and establishes functional safety requirements that now include cybersecurity aspects. The **ARC** applies horizontally to all products with digital elements, regardless of whether they are machines or not.

For a machine manufacturer, the two regulations apply in a complementary way:

- The Machinery Regulation covers the overall functional safety of the machine (mechanical, electrical, cybersecurity risks affecting safety)
- The ARC covers all aspects of cybersecurity of the digital elements of the machine

The requirements overlap to some extent, and a well-conducted risk analysis makes it possible to meet both regulations simultaneously.

Do I need to address all CVE vulnerabilities affecting my components?

No, the ARC approach is based on risk and operability in real-world conditions. A CVE vulnerability affecting a component you use may not be exploitable in your product, depending on:

- Your security architecture (segmentation, defense in depth)
- The context of use (component not exposed to the network, physical access required for operation)
- Features actually used (vulnerability on a server function when you only use client mode)

It is precisely the risk analysis that makes it possible to determine the real operability and to prioritize remediation actions. Vulnerability Exploitability eXchange (VEX) documents help to clearly communicate the status of each vulnerability.

What if I can't patch a legacy system?

OT environments often have legacy systems that cannot be updated without the risk of malfunction. The CRA recognizes this reality and allows the use of **compensatory measures** :

- **Virtual patching** : use of IPS/IDS that can block attempts to exploit known vulnerabilities, without modifying the vulnerable system
- **Network segmentation** : isolation of the legacy system in a secure area with strict flow control
- **Enhanced access control** : limiting physical and logical access to the system
- **Intensive monitoring** : increased monitoring to detect any exploitation attempts

These defense-in-depth approaches help reduce the exploitability of vulnerabilities without patching the system itself.

How do I manage security support over 5 years?

The 5-year minimum support obligation represents a significant change. Several strategies are possible:

- **Anticipate by design** : choose components with long-term support, design a modular architecture that facilitates updates
- **Integrate cost into the business model** : explicitly charge for security support, offer maintenance contracts that include patches
- **Outsource the PSIRT** : use a specialized service provider for operational vulnerability management and patch development
- **Pooling resources** : for SMEs, sector-specific pooling solutions are beginning to emerge

Does the CRA apply to products that are already on the market?

The regulation provides for a principle of non-retroactivity: products already placed on the market before 11 December 2027 are not subject to the initial compliance requirements. However:

- The obligation to report actively exploited vulnerabilities applies from September 11, 2026, **including for products already on the market**
- Manufacturers retain a general safety obligation for products in service
- It is strongly recommended to provide security patches even for previous products, for liability and image reasons

Can I rely on standards to demonstrate compliance?

Yes, the CRA explicitly provides for the use of **harmonised standards**. When a harmonised standard is published in the Official Journal of the European Union, compliance with it creates a presumption of conformity with the corresponding essential requirements.

The IEC **62443** series standards (cybersecurity of industrial automation and control systems) are particularly relevant and should be harmonized under the ARC:

- IEC 62443-4-1: Requirements for the development of secure products
- IEC 62443-4-2: Technical requirements for component safety

Other standards such as **ISO/IEC 27001** (information security management system) can also help demonstrate organizational compliance.

What are the first actions to take now?

To get started effectively:

1. **Inventory your affected products** and determine their CRA classification
2. **Set up your security contact point** (security.txt) to be reachable from September 2026
3. **Initiate risk analysis** on your priority products to identify vulnerabilities and threats
4. **Train your teams** in the challenges of ARC and secure development practices
5. **Evaluate your suppliers** and integrate security clauses into your contracts

We recommend that you get support to structure this process and avoid costly mistakes.

Conclusion

The Cyber Resilience Act represents a major turning point in the approach to cybersecurity of industrial and connected products. Beyond the regulatory constraint, it is an opportunity for commercial differentiation for manufacturers who will be able to transform this requirement into a competitive advantage.

CRA compliance requires a profound transformation of product design, development, and support practices. This transformation is a long-term one that requires significant investments in skills, processes and technologies. However, it is essential to continue marketing on the European market, which represents a key outlet for the global manufacturing industry.

The deadlines are fast approaching: September 2026 for vulnerability reporting, December 2027 for all requirements. Manufacturers need to act now to prepare effectively. A structured approach, based on risk analysis and recognized standards such as IEC 62443, makes it possible to progress methodically and optimize investments.

At AKENATECH, we support manufacturers in this transformation by combining technical expertise in OT cybersecurity, knowledge of production environments and mastery of regulatory issues. Our end-to-end approach – from strategy to operation to implementation – enables you to build sustainable compliance while maintaining business performance.

Don't let time slip away. CRA compliance is built today to be ready tomorrow.

Contact us to discuss your specific situation and build your Cyber Resilience Act compliance roadmap together.