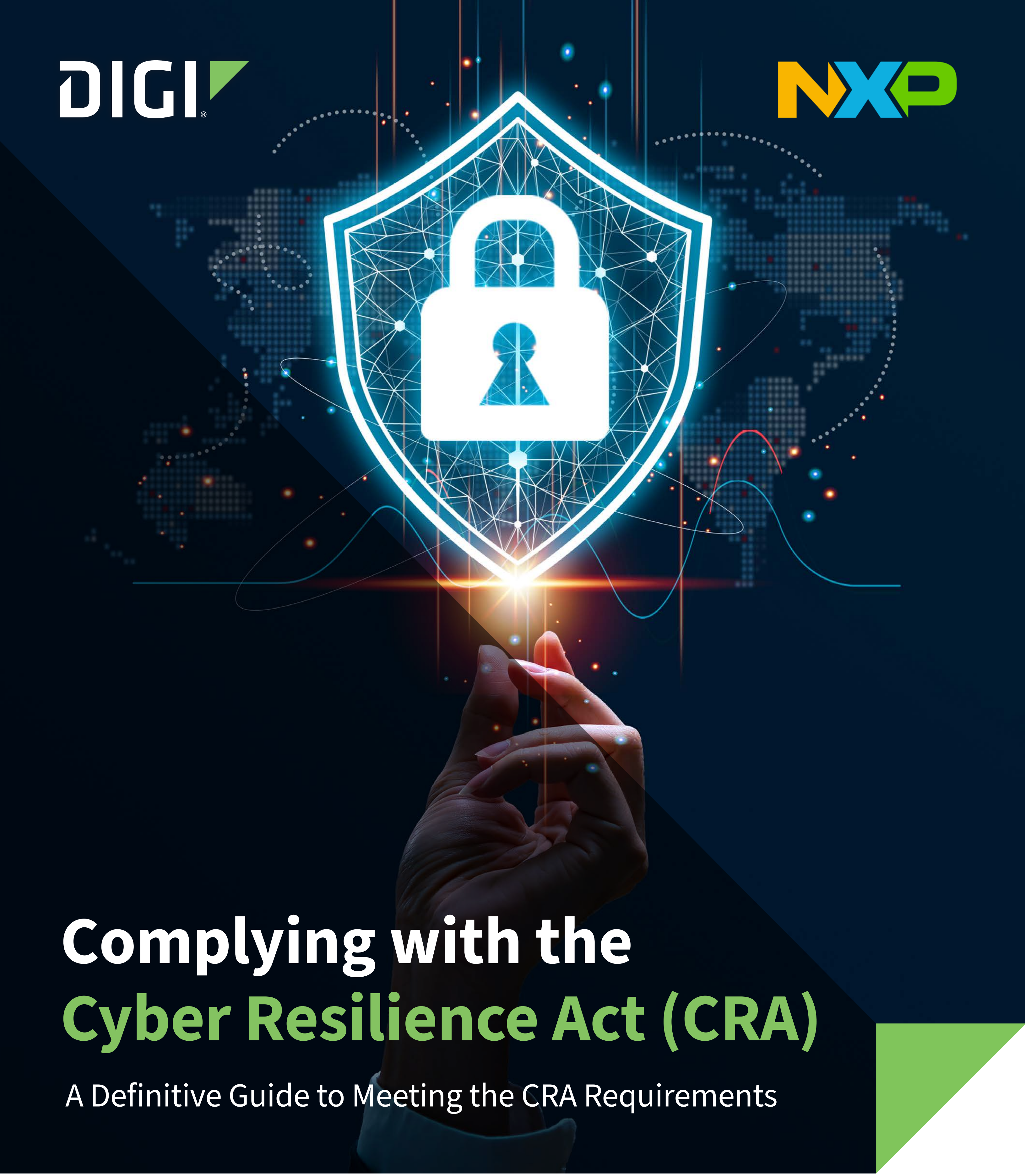


Complying with the Cyber Resilience Act (CRA)

A Definitive Guide to Meeting the CRA Requirements

Table of Contents

Introduction

The **Cyber Resilience Act (CRA)** significantly reshapes the global product compliance landscape by embedding strict cybersecurity obligations into the framework for Conformité Européenne (CE) marking. These requirements potentially impact any OEM product, regardless of origin, that is intended to be sold in the EU. Formally known as Regulation (EU) 2024/2847, the CRA applies to any product containing digital elements whose intended purpose or foreseeable use includes a direct or indirect data connection — either logically or physically — to a network or device. This hands-on guide from Digi and NXP provides a walkthrough of the requirements and how to comply.

Under this regulation, all products that are capable of connecting to a device or network must meet defined cybersecurity requirements in order to receive CE marking, which is a legal prerequisite for sale within the EU. Products that do not comply cannot be placed on the EU market.

At the heart of the CRA is a response to persistent cybersecurity shortcomings. Although many products claim to be secure, there is often no reliable way for consumers or businesses to verify such claims or to ensure ongoing protection. The CRA provides a unified, mandatory framework for cybersecurity compliance that spans the entire product lifecycle.

To that end, the regulation establishes:

- Common requirements for launching products or software with digital elements, ensuring a consistent starting point for all manufacturers
- A single cybersecurity framework for the planning, design, development, and upkeep of connectable products
- A duty of care that applies throughout the product's lifecycle — not just at the point of sale

This framework is meant to facilitate compliance not only for manufacturers of finished products, but also those supplying hardware and software components.

As with previous EU legislation, other countries are already following in the CRA's footsteps. For instance, the United States **introduced the U.S. Cyber Trust Mark in September, 2024**. Overseen by the Federal Communications Commission (FCC), this voluntary labeling program is intended to incentivize the development of more secure connected products.

The good news is that conforming to CRA requirements will help ensure your products also align with security measures being rolled out elsewhere. More importantly, understanding the CRA will help your organization avoid potentially costly rework or having products pulled from the market.

What Are the Risks of CRA Non-Compliance?

Compliance with the CRA is mandatory. If a product covered by the act does not qualify for a CE marking, it cannot legally be sold in the EU. Regulators have the authority to withdraw non-compliant products from the market and issue recalls, potentially crippling an organization's market presence.

Regulators may also choose to issue penalties for non-compliance, with each violation of the CRA carrying a potential fine of either €15 million or 2.5% of an organization's annual global turnover — whichever is higher.

Despite the harsh consequences, there are still widespread misconceptions about the CRA. One common misunderstanding concerns the timeline. While many manufacturers believe the regulation does not take effect until 2027, the CRA has already entered into force. Key compliance deadlines are approaching rapidly — see **"Countdown to CRA Compliance" on page 5** for details.

> While many manufacturers believe the regulation does not take effect until 2027, the CRA has already entered into force.
>
> See "Countdown to CRA Compliance" on page 5 for details.

There is also ongoing confusion about the scope of the regulation — specifically, which products it applies to, who is responsible, and what steps are required to maintain compliance. Some of the most pressing questions are addressed in **"Misconceptions About the Cyber Resilience Act" on page 4**. Understanding these details is crucial for manufacturers, purchasing managers, and development teams.

More broadly, a thorough review of CRA fundamentals is essential to keep your organization, supply chain, and product development in compliance with this significant regulation.

Disclaimer: *This article is for informational purposes only and does not constitute legal advice. Readers should not act upon any information presented herein without seeking professional counsel. For advice regarding your specific situation or for interpretation of applicable laws, please consult a qualified attorney.*

Misconceptions About the Cyber Resilience Act

Misconception	Reality
The CRA only applies to companies based in Europe.	**All manufacturers, importers, and distributors who place products on the European market must adhere to the CRA, regardless of where they are headquartered.**
Products already on the market when the CRA comes into effect are exempt.	**Any commercial product, legacy or otherwise, that is substantially modified after 11 December 2027 will need to meet the CRA requirements.** **Likewise, manufacturers must bear in mind an exception in Article 69, "Transitional provisions." The obligations set out in Article 14, "Reporting obligations of manufacturers," will apply to all products falling within the scope of this regulation and placed on the market before 11 December 2027.**
Only OEMs are responsible for CRA compliance.	**The CRA applies to the entire supply chain, from manufacturers to importers, distributors, and suppliers, and all parties are liable for compliance. It is applicable to hardware and software products, both as a final appliance or components. Hereafter we will refer to these groups and individuals as "the responsible parties." Note that this document only addresses responsibilities of manufacturers.**
Only IT or communication devices are covered by the CRA.	**The CRA covers the majority of commercial products with digital elements, from IoT devices to industrial control systems.** **However, some products are excluded from CRA compliance requirements, as they are covered by other regulations already in force. For example, these include:** • **Medical devices** • **Automotive systems and components** • **Aviation-related equipment** • **Marine equipment** • **Spare parts to replace identical components in products with digital elements** • **Products related to defense, national security, or designed to process classified information**
Open-source products are exempt from the CRA.	**Whether or not a product contains open-source components is irrelevant, if the product would otherwise require CRA compliance.**
The CRA only applies to products that incorporate software.	**If a commercial product requires a cloud platform or remote data processing solution as part of its core functionality, it falls under the purview of the CRA.**
Products that are offline most of the time do not need to be CRA compliant.	**Any product with digital elements capable of even potentially establishing a data connection to a device or network must comply with the CRA.**
Products only need to be tested or certified once.	**The CRA requires ongoing maintenance, compliance, and adherence throughout a product's lifecycle, not solely at the point of market entry.**

Fundamentals of the CRA

Unlike previous regulations, the CRA introduces concrete technical requirements, clear obligations, and defined deadlines — establishing accountability across the entire supply chain. These new rules are built on six foundational pillars:

- ✓ **Strict cybersecurity**: The CRA sets high security requirements for design, development, maintenance, and post-market support. Manufacturers must monitor for vulnerabilities in their products, address vulnerabilities proactively and provide regular updates.
- ✓ **Conformity assessments**: Products must undergo detailed assessments to verify compliance with essential cybersecurity requirements before entering the EU market.
- ✓ **Early vulnerability and incident notifications**: Any actively exploited vulnerability and severe incident must be reported to designated authorities within twenty-four hours of detection to enable rapid response.
- ✓ **Product classification**: Products are categorized by cybersecurity risk — default, important, or critical — with specific conformity assessment procedures to ensure proportionate security evaluations.
- ✓ **Supervision and audits**: Compliance must be maintained throughout the product lifecycle by way of active oversight and auditing, not just at market entry.
- ✓ **Transparency and communication**: OEMs must provide clear, current information about product security features, vulnerabilities, and remediation measures to users and authorities.

> Article 13, paragraph 19: "Manufacturers shall ensure that the end date of the support period referred to in paragraph 8, including at least the month and the year, is clearly and understandably specified at the time of purchase in an easily accessible manner and, where applicable, on the product with digital elements, its packaging or by digital means.
>
> Where technically feasible in light of the nature of the product with digital elements, manufacturers shall display a notification to users informing them that their product with digital elements has reached the end of its support period."

Together, these pillars create a standardized approach to cybersecurity, helping ensure connectable products meet essential cybersecurity requirements before reaching end users and throughout their entire lifecycle.

> Manufacturers must begin work immediately to ensure compliance within the mandated timeline.

Countdown to CRA Compliance

Part of the 2020 EU Cybersecurity Strategy, the CRA was intended to complement the **NIS2 Framework**. The act was officially signed by the European Parliament and the Council of the European Union on 23 October 2024 and **published on 20 November 2024**.

10 December 2024

The CRA is officially adopted into EU legislation with a grace period before full adoption is mandatory.

11 June 2026

Conformity assessment bodies responsible for verifying CRA compliance become operational, as outlined in Chapter IV, Articles 35-51.

Organizations should begin familiarizing themselves with the conformity assessment procedures and determine whether their product category requires formal engagement with a conformity assessment body or if voluntary collaboration is appropriate to support compliance efforts ahead of the 2027 deadline.

11 September 2026

Manufacturers are now obligated to simultaneously report actively exploited vulnerabilities and severe incidents in applicable products to both their "designated as coordinator" Computer Security Incident Response Team (CSIRT) and the European Union Agency for Cybersecurity (ENISA) within 24 hours of discovery, as outlined in Article 14.

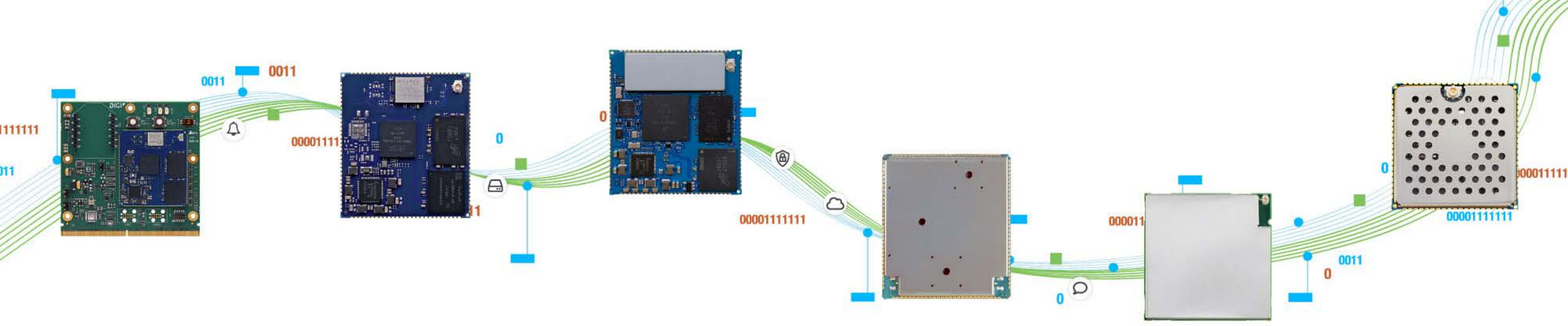
11 December 2027

The Cyber Resilience Act officially comes into effect. From this date onward, all applicable products require a CE marking to be authorized for sale in the EU.

Key Requirements for Compliance (Annex I)

The CRA mandates cybersecurity compliance "from cradle to grave," requiring both secure product design and ongoing protection throughout the entire product lifecycle. This means cybersecurity must be addressed at the earliest stages of development and maintained well beyond product launch. (**See the Support Period section on 7 for more information**.)

To support this objective, Annex I of the CRA outlines two categories of cybersecurity requirements: Part I, which focuses on the properties of products with digital elements, and Part II, which sets out rules for vulnerability handling and lifecycle management.



Part I: Product-Related Cybersecurity Requirements

During the design phase, organizations are expected to conduct a thorough cybersecurity risk assessment and establish an adequate level of cybersecurity based on potential risks (Annex I, Part I.1). From here their products with digital elements must:

- Be free of known exploitable vulnerabilities at the time of release (Annex I, Part I.2(a))
- Be shipped with a "secure by default" configuration (Annex I, Part I.2(b))
- Ensure that vulnerabilities can be addressed through security updates, which should be automatic and enabled by default (Annex I, Part I.2(c))
- Protect from unauthorized access with appropriate authentication, identity, or access management systems (Annex I, Part I.2(d))
- Shield data confidentiality by, for example, encrypting data at rest or in transit using cutting-edge mechanisms (Annex I, Part I.2(e))
- Safeguard the integrity of stored, transmitted or processed data, commands, programs and configuration against any unauthorized tampering, and report cases of data corruption (Annex I, Part I.2(f))
- Only process data strictly relevant to its intended use (Annex I, Part I.2(g))
- Protect essential functions from denial-of-service (DoS) attacks (Annex I, Part I.2(h))
- Minimize potential impacts by themselves or connected devices on services provided by other devices or networks (Annex I, Part I.2(i))
- Limit attack surfaces, including external interfaces (Annex I, Part I.2(j))
- Incorporate exploitation mitigation mechanisms to reduce the impact of security incidents (Annex I, Part I.2(k))
- Provide security-relevant information by monitoring and recording internal activities such as access to or modification of data, services, or functions — though they must also give users the ability to opt out (Annex I, Part I.2(l))
- Ensure all data and settings can be securely deleted or transferred to other products on request by users (Annex I, Part I.2(m))

Part II: Vulnerability Handling Requirements

Secure design alone is not sufficient. The CRA also establishes several requirements for managing and remediating vulnerabilities. Manufacturers must identify and document all vulnerabilities and components contained in each product. This includes maintaining an up-to-date, machine-readable software bill of materials (SBOM) that catalogs, at minimum, a product's top-level dependencies (Annex I, Part II.1). In addition, manufacturers must:

- Address and remediate vulnerabilities without delay by providing security updates (Annex I, Part II.2)
- Apply effective and regular tests and reviews of the security of the product (Annex I, Part II.3)
- Share and publicly disclose information about fixed vulnerabilities (Annex I, Part II.4)
- Put in place and enforce a policy on coordinated vulnerability disclosure (Annex I, Part II.5)
- Provide a contact address for reporting discovered vulnerabilities (Annex I, Part II.6)
- Implement mechanisms to securely distribute updates to ensure vulnerabilities are fixed or mitigated in a timely manner (Annex I, Part II.7)
- Ensure security updates are disseminated without delay, free of charge, and with advisory messages that provide relevant information to users (Annex I, Part II.8)

These vulnerability-handling practices are intended to ensure that products remain protected and compliant well after their initial release, through coordinated efforts across the product's support period and beyond.

Key Obligations (Articles 13 and 14)

In addition to cybersecurity requirements for product design, development, production, and maintenance, the CRA outlines several key obligations for manufacturers. (Note that some of the obligations apply to responsible parties across the supply chain. However, this document focuses solely on manufacturer responsibilities.) These are defined in CRA Articles 13 and 14, “Obligations of manufacturers” and “Reporting obligations of manufacturers,” respectively, which specify procedures that must be followed to ensure products meet the essential cybersecurity requirements set forth in Annex I, Parts I and II.

CRA Article 13: Obligations of Manufacturers

Article 13 sets out the obligations of manufacturers. Let's break down manufacturers' obligations into three phases: design and development, the support period, and the availability of security updates.

Design and Development

During the first phase, design and development, this regulation establishes a series of obligations:

- Ensure that the product has been designed, developed, and produced in compliance with the essential cybersecurity requirements set out in Annex I, Part I.

- Conduct a cybersecurity risk assessment associated with the product which will be documented and updated during the support period.

- The cybersecurity risk assessment must consider the product’s intended purpose, potential uses, the conditions of use, such as the operating environment, or the assets that must be protected, and its support period. The cybersecurity risk assessment will indicate whether the essential cybersecurity requirements set out in Annex I, Parts I and II, are applicable to the product in question, and how those requirements are implemented in practice.

- The results of the cybersecurity risk assessment must be included in the product’s technical documentation (Article 31 and Annex VII), along with a clear justification for the exclusion of any essential cybersecurity requirements. These results must guide decisions and actions throughout the product’s planning, design, development, production, delivery, and maintenance phases.

- It should also be emphasized that manufacturers must exercise due diligence when integrating third-party components so that those components do not compromise the product security, including free and open-source software components not commercially available on the market.

- They shall also implement or have implemented the conformity assessment procedures of their choice referred to in Article 32.

- Once a manufacturer has demonstrated product conformity against the essential cybersecurity requirements in Annex I, Part I and II, manufacturers shall draw up the EU declaration of conformity in accordance with Article 28 and affix the CE marking in accordance with Article 30.

> Article 13, paragraphs 5, 6, and 8 state that manufacturers must exercise due diligence when integrating third-party components so that those components do not compromise the product security, including free and open-source software components not commercially available on the market.

Support Period

Let's move on to the next phase, the support period.

- The product has already been placed on the market and the support period begins — during which the manufacturer is obliged to ensure that the vulnerabilities of the product are handled effectively and in compliance with the essential cybersecurity requirements formulated in Annex I, Part II.

- Manufacturers shall specify the support period to reflect the length of time during which the product is expected to be in use, being at least five years as a general rule. They must determine the support period taking into account user expectations, the nature of the product, its intended purpose, support periods for products with similar functionality introduced into the market by other manufacturers, the availability of the operating environment and the support periods of integrated components that provide the main features and are obtained from third parties, among other considerations.

- Manufacturers shall include in the technical documentation set out in Annex VII the information that was taken into account to determine the support period of the product.

- Note that the support period starts when a product is placed on the market. The end date of the support period is the last time the product is sold on the market, plus five years. So, the support period is still five years, but its end is a rolling deadline as long as the product is placed on the market. In fact, the countdown of the support period starts when the last batch of the product is sold. But actually, the support period goes till the product end of life or the last delivery to customers on the EU market, plus five years.

- Importantly, manufacturers bear full responsibility for vulnerability identification, handling, and disclosure across all components, including those sourced from third parties. When vulnerabilities in third-party components are remediated, manufacturers must share relevant documentation or code with the component maintainer.

- Article 13 also requires manufacturers to document relevant aspects relating to the product cybersecurity including any vulnerabilities they are aware of, and any relevant information provided by third parties. Manufacturers must maintain comprehensive records of their products' cybersecurity elements, with documentation specifically tailored to each product’s risk profile.

- Additionally, manufacturers must implement suitable policies and procedures for receiving, processing, and responding to vulnerability reports submitted by third parties. This creates an effective feedback loop that supports ongoing security improvements.

- Manufacturers must maintain technical documentation and the EU declaration of conformity at the disposal of market surveillance authorities for at least ten years from the product launch, or for the duration of the support period, whichever is longer.

- They must also keep the information and instructions to the user (Annex II) available to users and market surveillance authorities for at least ten years after the product has been placed on the market, or for the duration of the support period, whichever is longer.

- During the support period, manufacturers who become aware that their product or processes do not comply with the essential cybersecurity requirements set out in Annex I must immediately implement corrective measures, or withdraw or recall the product from the market.

- Manufacturers must provision SBOMs to market surveillance authorities upon request for EU-wide software dependency assessments, especially on free and open-source software components, on specific product categories.

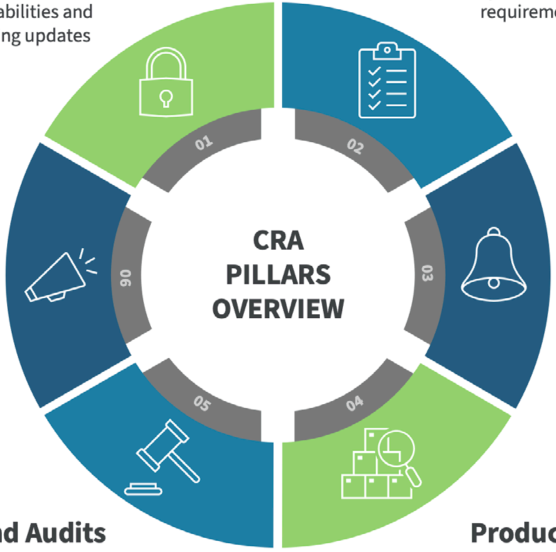
> The support period for a product begins when the product is **placed on the market.**
>
> Its end is determined by the last time the product is sold or delivered in the EU, plus five additional years.
>
> The five-year countdown begins only after the product is no longer placed on the market — meaning the support period extends as long as sales or deliveries continue, making it a rolling deadline.

Availability of Security Updates

Finally, the availability of security updates:

- Manufacturers shall ensure that each security update referred to in Annex I, Part II, point 8, that has been made available to users during the support period remains available after its release for a minimum period of ten years or for the remainder of the support period, if this period is longer.

- Manufacturers may ensure compliance with the essential cybersecurity requirement set out in Annex I, Part II, point (2), only for the latest released version, provided that users of previous versions have access to the latest version free of charge and do not incur additional costs.



Strict Cybersecurity
Design, development, maintenance and EOL; proactive removal of vulnerabilities and recurring updates

Conformity Assessments
More detailed to ensure compliance with cybersecurity requirements

Transparency and Communication
Clear and up-to-date information on product security features and any relevant security issues

Early Vulnerability and Incident Notifications
Any actively exploited vulnerability and severe incident discovered must be reported to authorities within 24 hours of its detection

Supervision and Audits
More intensive to ensure continued compliance with cybersecurity requirements

Product Classification
Different categories according to their level of risk (default, important and critical)

Reporting Obligations of Manufacturers (Article 14)

A manufacturer must report actively exploited vulnerabilities and severe incidents **within 24 hours of discovery**. An actively exploited vulnerability is a known weakness that, based on reliable evidence, is being used by malicious actors to compromise systems. A severe incident is an event that can have serious consequences for the product, its users, or connected systems — such as outages, breaches, or data leaks.

In both cases, an early warning notification must be shared simultaneously with ENISA and the CSIRT designated as the coordinator in each member state. The notification must indicate the member states in which the product has been made available. In the case of severe incidents, it will also include at least whether it is suspected to be due to illegal or malicious acts. That notification will be submitted via a platform established by ENISA (Article 16).

The manufacturer is also obligated to release a notification within 72 hours that contains:

- General information about the vulnerability or incident
- What has been done to remediate or correct the issue
- What users can do to mitigate the damage
- An initial assessment of the incident
- The manufacturer's assessment of how sensitive or confidential the reported information is

Finally, the manufacturer must submit a final report for both actively exploited vulnerabilities and severe incidents.

In the case of actively exploited vulnerabilities, a final report must be submitted no later than fourteen days after a corrective or mitigating measure is available, which must include, at a minimum:

- Description of the vulnerability, including its severity and consequences
- Information about any malicious actors who have exploited or are exploiting the vulnerability
- Details regarding the security update or other available corrective measures

For severe incidents, a final report must be submitted within one month after presenting the seventy-two-hour notification of the incident, which must include at least the following:

- Detailed description of the incident, including its severity and repercussions
- Type of threat or root cause that likely triggered the incident
- Mitigation measures applied and in progress

Important Notes on Compliance and Product Lifecycle

Every applicable product on the EU market must adhere to the CRA reporting obligations, including products that were commercially available prior to 11 December 2027. These requirements apply to the full lifecycle of all products bearing the CE mark.

Therefore, developer teams must continuously monitor and analyze potential vulnerabilities in their products, document them properly, and report them to ENISA and CSIRT. For all identified vulnerabilities, the developers must create or obtain patches and apply them in a timely manner. This means manufacturers must integrate the ability to access and update every connectable device over the lifetime of the product to remain in compliance.

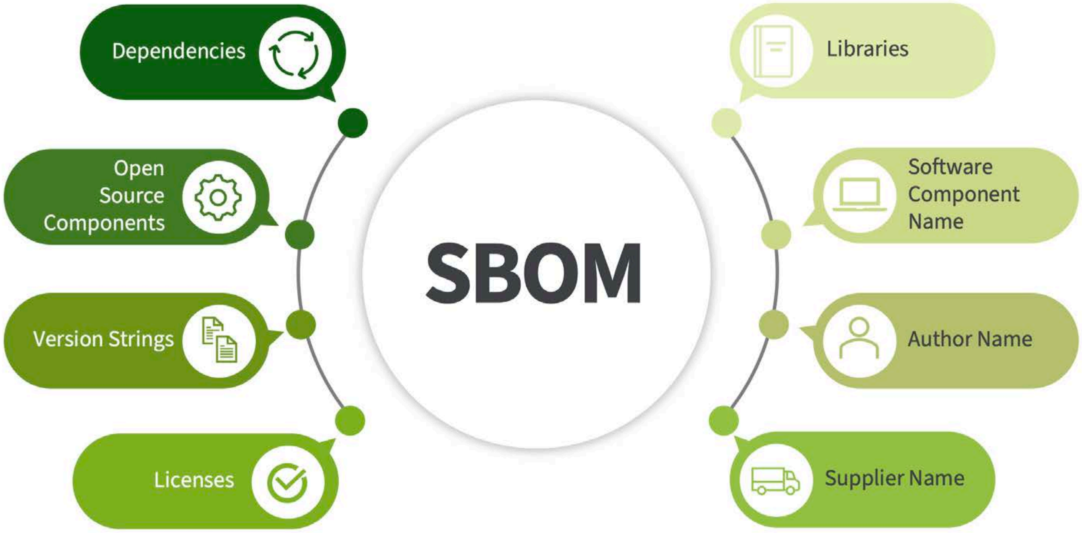
See **Digi's CRA Compliance End-to-End Support on page 13** to learn how Digi solutions support these requirements.

Requirements for Technical Documentation

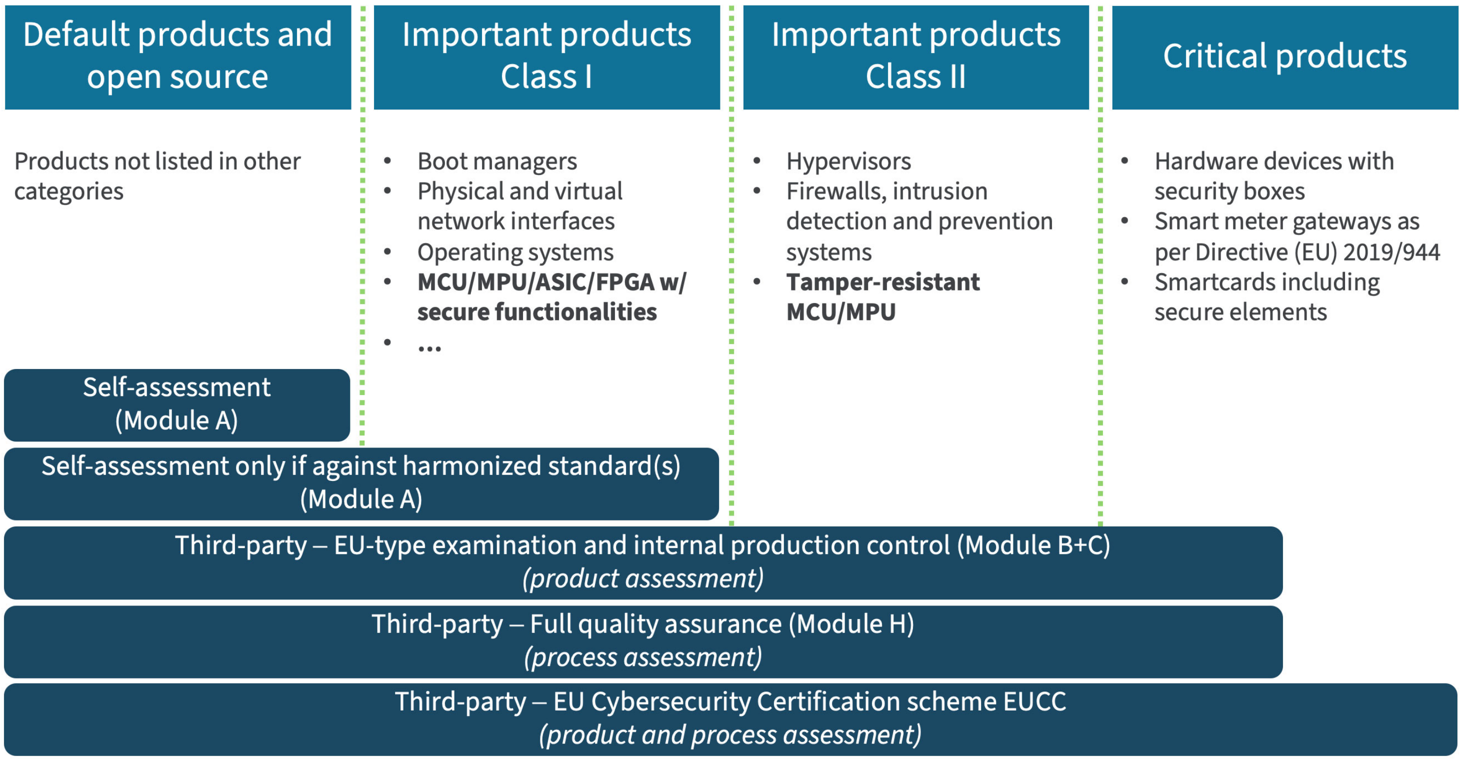
As referred to in Article 31 and outlined in Annex VII of the CRA, manufacturers are obligated to maintain documentation that includes the following:

- A general description of their product, including its intended purpose, software versioning information, photographs showing the external features and markings as well as the internal layout, and user information and instructions listed in Annex II
- Details on design, development, production, and vulnerability handling processes
- Information about the product design and development: drawings/schematics and a description of the system architecture that explains how the software components interoperate and integrate into the overall processing
- Specifications on vulnerability handling processes, including the software bill of materials, the coordinated vulnerability disclosure policy, a contact address for vulnerability notification, and a description of the solutions selected for the secure delivery of updates
- Information on production and monitoring processes, and the validation of said processes
- The cybersecurity risk assessment mentioned in Article 13, including how the essential cybersecurity requirements formulated in Annex I, Part I are applicable
- Information on how the manufacturer determined their product's support period pursuant to Article 13(8)
- Any EU-published harmonized standards that fully or partially apply to the product, including cybersecurity certification schemes and common specifications
- Reports of the tests conducted to verify the conformity of the product and of the vulnerability handling processes with the applicable essential cybersecurity requirements
- A copy of the product's EU declaration of conformity, and an SBOM, if applicable, by request of a market surveillance authority

Technical documentation requirements include product descriptions, vulnerability processes, risk assessments, and SBOMs — kept at the disposal of market surveillance authorities for at least ten years.



Product Categories and Conformity Assessment Procedures



Default products and open source

Products not listed in other categories

Important products Class I

- Boot managers
- Physical and virtual network interfaces
- Operating systems
- **MCU/MPU/ASIC/FPGA w/ secure functionalities**
- ...

Important products Class II

- Hypervisors
- Firewalls, intrusion detection and prevention systems
- **Tamper-resistant MCU/MPU**

Critical products

- Hardware devices with security boxes
- Smart meter gateways as per Directive (EU) 2019/944
- Smartcards including secure elements

Self-assessment (Module A)

Self-assessment only if against harmonized standard(s) (Module A)

Third-party – EU-type examination and internal production control (Module B+C) *(product assessment)*

Third-party – Full quality assurance (Module H) *(process assessment)*

Third-party – EU Cybersecurity Certification scheme EUCC *(product and process assessment)*

Conformity Assessment Procedures (Article 32)

Per Article 32, all products falling within the scope of the CRA must undergo a conformity assessment to demonstrate compliance with the essential cybersecurity requirements outlined in Annex I. Manufacturers must implement at least one of the CRA's established conformity assessment procedures. This includes accounting for changes to products, updates to harmonized standards, and evolving cybersecurity certifications.

The type and scope of this assessment depends on the classification of the product. At present, the available information on product categories remains incomplete. In accordance with Article 7(4), the European Commission is expected to adopt an implementing act by 11 December 2025 to define the technical descriptions of Classes I and II of important products set out in Annex III, as well as the critical product category listed in Annex IV. A draft of that act is currently in development.

Default

If the product is not listed as important or critical, the manufacturer can perform an internal conformity assessment. The majority of covered products fall under this umbrella. This also applies to free and open-source software associated with commercial products.

Note that services are exempted from the CRA unless they are integral to a product's functionality.

Important Products, Class I

The manufacturer can perform an internal assessment only if they apply harmonized standards, common specifications, or European cybersecurity certification schemes. Examples of Class I products include password managers, products with the function of a virtual private network (VPN), network management systems, and general-purpose smart home virtual assistants.

Important Products, Class II

Class II products always require a third-party conformity assessment. They include hypervisors, tamper-resistant microprocessors, and microcontrollers.

Critical

Critical products must either obtain a European cybersecurity certificate pursuant to Regulation (EU) 2019/881, the 2019 EU Cybersecurity Act, or follow the same conformity assessment processes as Class II products.

Once a manufacturer has completed a conformity assessment for their product, they must then draft a declaration of conformity in the languages of the member state where the product is sold. They can then affix a CE marking to their product, its packaging, accompanying documentation, and website.

Working Together for Compliance

The CRA has fundamentally altered the landscape of product compliance in the EU. Navigating the CRA and its complex requirements represents one of the biggest challenges OEMs face in getting secure products to market in the European Union that have the potential to be Internet connected.

> The combination of NXP's advanced secure processors and Digi's comprehensive solutions delivers security building blocks that enable OEMs to meet CRA requirements.

NXP and Digi — Building Next-Generation Processors and SOM Solutions

Digi International collaborates with manufacturers such as NXP Semiconductors to deliver developer building blocks that leverage advanced processors and security methods — and thereby support OEMs in building secure-by-design products that meet requirements such as those of the CRA and other regulations.

NXP's Security Posture: CRA Ready

NXP's EdgeLock® Assurance Program was created by NXP for addressing the mature security posture from the organization. It serves as a foundation for customers to meet security standards and regulations, supporting the product developer's security process along with delivering product security capabilities.

This program includes the implementation of industry best practices for secure development and a robust company culture addressing physical and logical security, as well continuous staff trainings. Secure product development processes are an integral part of the program, certified by external 3rd parties against industry standards like ISO 21434, IEC 62443-4-1 and IEC 80001-5-1.

NXP products with security functionality are verified during the development process by a group of experts from the in-house Vulnerability Analysis laboratory to ensure that NXP products are hardened against the most common risk scenarios. Additionally, NXP ensures their security claims are verified by independent third parties, following strict industry standards such as SESIP (EN 17927) and Common Criteria (ISO 15408), ensuring that NXP's components meet the highest standards of assurance and resilience. The independent third parties verify the security claims of NXP products, the robustness of such implementations against specific attack potentials, as well as verification against publicly known vulnerabilities, delivering state-of-the-art security for each applicable risk level.

Scalable Security Architecture and CRA Requirement Mapping

To further support CRA compliance, NXP product security capabilities can be mapped to the CRA's Essential Cybersecurity Requirements, including product configuration, authentication, access control, data protection, monitoring, vulnerability management, and incident response. NXP's security solutions are available in a range of security functionality, from entry level to advanced — allowing OEMs to scale protections based on risk levels. Key technologies such as the **EdgeLock Secure Enclave**, **Secure Elements**, and **EdgeLock 2GO** services provide robust credential protection, lifecycle security management, and turnkey provisioning.

NXP's Security Solutions for CRA Conformant Applications

In order to build a secure and robust system, first of all, we need to put the anchor of the entire system to something that we trust. A silicon with its security protection rooted in hardware is hard to attack because it is inherently trustworthy. A silicon is the foundation and the base for all software running on top of it. Software — like firmware, communication stacks, the operating system and other applications — can be modified and compromised, but the silicon is not easily compromised. We call the silicon the Root of Trust (RoT) of the system.

There is no absolute security, given the extremely large spectrum of possible attacks, but also the growing complexity of applications significantly increases the attack surface.

As a result, it is important to work with a solution provider like Digi that integrates NXP's secure processors into its **Digi ConnectCore® system-on-modules** and delivers complete, secure-by-design solutions and building blocks — like **Digi ConnectCore Cloud Services** and **Digi ConnectCore Security Services** — that enable OEMs to design and deliver secure end products, along with the ability to remotely monitor and manage their solutions, meet the requirements of the CRA, and even add additional streams of revenue to their organization's business model.

Digi's CRA Compliance End-to-End Support

European and international businesses alike need practical, actionable guidance on the CRA — and on how to design products for compliance from the ground up.

Digi has **a keen focus on cybersecurity** and has been following the CRA since it was first announced, leveraging our experience in security, and mapping our security building blocks to the requirements of this important regulation. We also take a unique approach with our services that addresses each aspect of the CRA, with detailed step-by-step guidance on implementation.

"When we spoke to Digi, it was the first time someone really talked about what we had to do to comply with the CRA," notes one customer. "When we met with other vendors, they only provided general overviews of the law."

Digi's embedded solutions and services are intentionally designed to help customers comply with CRA requirements and obligations, and Digi works with each customer to put together a service package that meets their specific needs.

Digi's Compliance-Focused Ecosystem

Digi offers a **full suite** of cloud-to-connectivity services, including **Digi ConnectCore system-on-modules** (SOMs), software and tools, as well as **Digi ConnectCore Security Services** and **Digi ConnectCore Cloud Services** that form an integrated ecosystem with security built in. Our solutions assist in creating compliant, secure-by-design digital products with proactive vulnerability management, secure software updates, and remote configuration, monitoring, and maintenance.

With Digi's complete ecosystem, OEMs can confidently maintain CRA compliance throughout their product lifecycles while reducing both complexity and time to market. Our integrated approach not only helps address current requirements, but also positions organizations to adapt seamlessly to future regulatory changes.

Alongside our purpose-built portfolio and services, Digi also offers several educational resources, including a one-hour webinar that addresses **how engineers can overcome the challenges of the CRA**.

Digi TrustFence

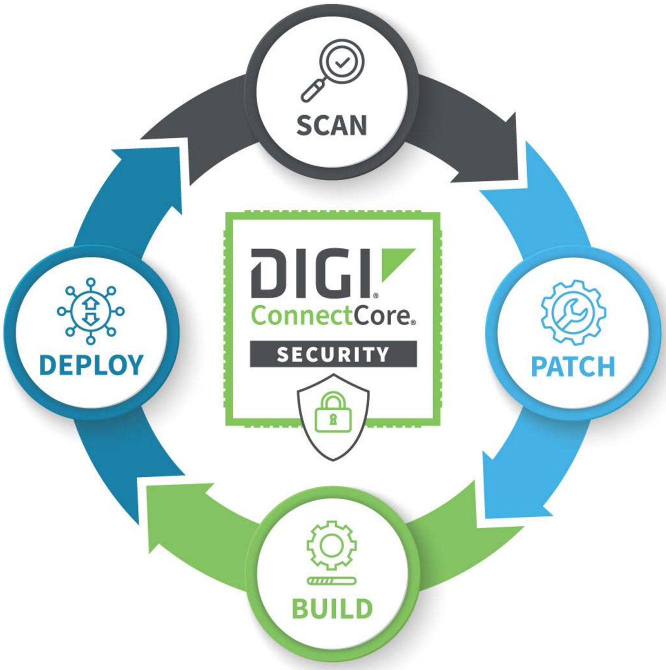
Designed for mission-critical applications, **Digi TrustFence®** helps developers build dynamic, adaptive security directly into IoT devices, supporting both security-by-design and secure configuration through features such as secure boot, secure console, secure software updates, encrypted file system, and protected hardware and pins.

TrustFence is fully integrated into Digi's **cellular routers**, **XBee® RF modules and cellular modems**, **infrastructure management devices**, and **Digi ConnectCore SOMs**. Digi Embedded Yocto (DEY) also incorporates TrustFence.

Digi ConnectCore Security Services

Digi ConnectCore Security Services feature a range of tools to help organizations address the CRA's vulnerability management and disclosure requirements, including 24-hour reporting obligations for actively exploited vulnerabilities and severe incidents.

This includes consistently analyzing and monitoring a custom SBOM running on Digi ConnectCore SOMs for security vulnerabilities. To help remediate critical issues, the services provide a curated vulnerability report, a security software layer with patches and fixes for common vulnerabilities, and expert consulting and support services.



Digi ConnectCore Cloud Services

Digi ConnectCore Cloud Services based on the Digi Remote Manager® (Digi RM) platform help manufacturers keep their devices up-to-date and provides extensive process automation, monitoring, and remote device management capabilities.

Combining proven off-the-shelf hardware with Digi's industry-leading knowledge and experience, ConnectCore Cloud Services empower OEMs to develop compliant connected devices that provide superior quality and ease of use to customers through automated mass firmware and software updates, bi-directional communication, real-time alerts, and detailed reports on device conditions and network health.

DIGI
ConnectCore
CLOUD
120
60
72°

Digi Wireless Design Services

If you are working with Digi embedded solutions and need engineering support, our **Wireless Design Services** (WDS) team can help. WDS can support your development team at any point along the way, whether you need product design and build services, certifications, software development, rapid time-to-market support, or ongoing engagements to ensure your products remain in compliance.

This team of talented engineers and project managers has deep experience in every aspect of product development, including board redesigns and product rescues, and has a fully equipped lab for engineering, testing, and go-to-manufacturing support.

Digi Embedded Yocto (DEY)

An open-source Linux distribution based on the Yocto Project™, **Digi Embedded Yocto** (DEY) is designed specifically for our SOMs. It helps embedded developers fulfill their CRA compliance obligations through a combination of Digi-owned software maintenance, robust **patch policy**, and full integration with Digi TrustFence and Digi ConnectCore Security and Cloud Services.

Digi offers comprehensive CRA compliance support including automated vulnerability scanning, secure remote updates, and expert consulting throughout the product lifecycle.

Complying with CRA: Leveraging Digi Security Building Blocks

Let’s look at exactly how the Digi ConnectCore solution helps you meet the requirements of the CRA.

Part I: Product-Related Cybersecurity Requirements

In the tables on the following pages we have included the fourteen cybersecurity requirements relating to product properties, per Annex I, Part I. We have rolled up our sleeves and mapped each of the requirements to Digi TrustFence, Digi ConnectCore Security Services, Digi ConnectCore Cloud Services and, of course, our DEY operating system. Let's take a closer look at a couple of requirements.

- **Annex I, Part I.2(a).** Products will ship without known exploitable vulnerabilities. Digi ConnectCore Security Services facilitate custom software bill of materials (SBOM) scans to triage common vulnerabilities and exposures (CVEs), removing false positives and enabling OEMs to focus on the most critical issues. Additionally, OEMs can take advantage of our meta-digi-security layer that includes a collection of pre-integrated security patches for DEY, board support package (BSP), Linux kernel and bootloader.
- **Annex I, Part I.2(c).** Vulnerabilities can be addressed leveraging the secure software update feature included in Digi TrustFence and our Digi ConnectCore Cloud Services to securely and reliably deploy such patches and fixes remotely over-the-air (OTA).

It is a thorough and careful assessment that pinpoints our software, tools, features, and procedures available to help OEM customers confidently comply with this legislation, reducing time to market and, more importantly, maintaining compliance over the product lifecycle.

There are some requirements that do not apply to the Digi security building blocks, but that could apply to a ConnectCore-based end product. For example, an OEM that builds an application using a Digi ConnectCore SOM must fulfill the CRA requirements in the end product. In fact, OEM customers own end products with potentially vulnerable hardware and software, so they will need to carefully consider what work they need to undertake during the CRA journey.

Part II: Vulnerability Handling Requirements

The last table includes the eight vulnerability handling requirements of Annex 1, Part II. Following the same approach as Part I, we have meticulously mapped each of the requirements to our security building blocks. Let's take a deep dive into a couple of requirements.

- **Annex I, Part II.1.** Our proven methodology, together with DEY and Digi ConnectCore Security Services, makes it easier for manufacturers to identify and document vulnerabilities and components contained in products by drawing up a custom SBOM covering at the very least the top-level dependencies.
- **Annex I, Part II.7.** Digi TrustFence and Digi ConnectCore Cloud Services also provide mechanisms to securely distribute product updates to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automated manner. Our cloud services ensure secure edge-to-cloud communications supporting TLS (Transport Layer Security), certificate-based authentication and encryption. Additionally, with the template functionality, OEM device fleets can be automatically scanned, updated, and maintained in compliance with the established configuration. By leveraging templates, OEM customers can save time, reduce errors, minimize effort, and manage scale when configuration updates are needed, as well as ensure consistency and standardization across all devices deployed in the field.

The scope of this review is focused on Digi ConnectCore. OEM customers who design products based on our SOMs will be able to take advantage of our value-added solutions but will have to dedicate certain efforts to meet CRA obligations and requirements and its milestones to launch a product to market or continue selling existing products.

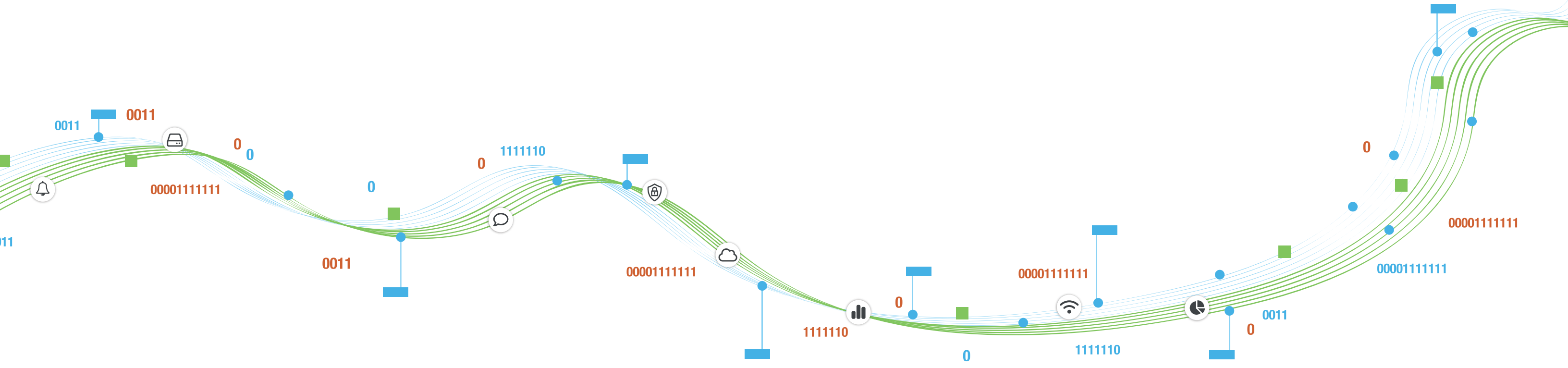
Of course, we can arrange a call with your sales representative to conduct a deep dive into these requirements and how to implement Digi security building blocks for a specific project.

Complying with CRA: Leveraging Digi Security Building Blocks (I)

Part I	Description	Digi TrustFence	Digi ConnectCore Security Services	Digi ConnectCore Cloud Services	Digi Embedded Yocto
(1)	Products shall be designed, developed and produced ensuring an appropriate level of cybersecurity based on the risks	TrustFence overall	Security services overall	Cloud services overall	DEY overall
(2) (a)	Products shall be made available without known exploitable vulnerabilities	N/A	Custom SBOM scans, meta-digi-security	**Digi RM Vulnerability Patch Policy**	**Digi owned software maintenance**
(2) (b)	Products shall be made available with a secure by default configuration	TrustFence overall	N/A	N/A	Hardened DEY
(2) (c)	Products shall ensure that vulnerabilities can be addressed through security updates	Secure software update	meta-digi-security, consulting and support	Secure remote OTA software updates	Secure software update, dual boot configuration
(2) (d)	Products shall ensure protection from unauthorized access	Secure console, secure JTAG	N/A	N/A	SSH/TLS
(2) (e)	Products shall protect the confidentiality of stored, transmitted or otherwise processed data, personal or other	Encrypted file system / files (hardware bound)	N/A	File system access, TLS, certificate-based authentication and encryption	Encryption, WPA3, FIPS 140-2/3 (additional cost)
(2) (f)	Products shall protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration	Secure boot / authenticated file system	N/A	File system access, TLS, certificate-based authentication and encryption	TLS, read-only file system
(2) (g)	Products shall process only data, personal or other, that are adequate, relevant and limited to what is necessary	N/A	N/A	Custom data streams	N/A
(2) (h)	Products shall protect the availability of essential and basic functions against denial-of-service attacks	N/A	N/A	N/A	Embedded systems security best practices
(2) (i)	Products shall minimize the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks	N/A	N/A	N/A	Embedded systems security best practices
(2) (j)	Products shall be designed, developed and produced to limit attack surfaces, including external interfaces	Secure boot, secure console, secure JTAG, tamper detection	meta-digi-security, consulting and support	N/A	N/A
(2) (k)	Products shall be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques	Tamper detection	N/A	Templates	N/A
(2) (l)	Products shall provide security related information by recording and monitoring relevant internal activity	Tamper detection	N/A	Security monitoring agent	N/A
(2) (m)	Products shall provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner	N/A	N/A	File system access, Digi RM data/settings management	N/A

Complying with CRA: Leveraging Digi Security Building Blocks (II)

Part II	Description	Digi TrustFence	Digi ConnectCore Security Services	Digi ConnectCore Cloud Services	Digi Embedded Yocto
(1)	Manufacturers shall draw up a software bill of materials in a commonly used and machine-readable format	N/A	Custom SBOM creation	N/A	DEY SBOM
(2)	Manufacturers shall address and remediate vulnerabilities without delay	N/A	meta-digi-security, consulting and support	Secure remote OTA software updates, templates	DEY regular releases
(3)	Manufacturers shall apply effective and regular tests and reviews of the security of the product	N/A	Custom SBOM scans	Digi RM Vulnerability Patch Policy	DEY Patch Policy
(4)	Manufacturers shall share and publicly disclose information about fixed vulnerabilities	N/A	Security Services overall	Digi Security Center	Digi Security Center
(5)	Manufacturers shall put in place and enforce a policy on coordinated vulnerability disclosure	N/A	N/A	Digi RM Vulnerability Patch Policy, Digi Security Center	DEY Patch Policy, Digi Embedded GitHub, Digi Security Center
(6)	Manufacturers shall facilitate the sharing of information about potential vulnerabilities including by providing a contact address for the reporting of the vulnerabilities discovered	N/A	N/A	Digi security form	Digi security form
(7)	Manufacturers shall provide for mechanisms to securely distribute updates to ensure that vulnerabilities are fixed or mitigated in a timely manner	Secure software update	N/A	Secure remote OTA software updates, templates, TLS, certificate-based authentication and encryption	N/A
(8)	Manufacturers shall ensure that, where security updates are available, they are disseminated without delay and, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken	N/A	N/A	Secure remote OTA software updates, templates	DEY Patch Policy, Digi Embedded GitHub



The Digi Ecosystem: Integrated CRA Compliance

One of the greatest strengths of the Digi portfolio is its integrated approach to CRA compliance. Digi solutions are secure by design and supported by Digi TrustFence, Digi ConnectCore Security Services, Digi ConnectCore Cloud Services, and Digi Embedded Yocto (DEY). These form an integrated hardware and software solution with security built in from the ground up.

The Digi ecosystem provides comprehensive coverage for key CRA requirements:

- ✓ **SBOM management:** Tools for creating and maintaining a software bill of materials
- ✓ **Vulnerability handling:** Frequent scanning for vulnerabilities that arise after the initial product release
- ✓ **Reporting tools:** Includes curated vulnerability reports that highlight critical issues
- ✓ **Vulnerability remediation:** Security software layer that includes patches and fixes for common vulnerabilities
- ✓ **Security maintenance:** Secure and reliable remote OTA software updates
- ✓ **Device fleet management:** Enabling process automation, monitoring, remote device management and cost reduction
- ✓ **Expert support:** Consulting and support services for patches and fixes integration

With Digi's complete ecosystem of SOMs, software, tools and services, OEMs can confidently accelerate their compliance with this legislation, reducing time to market and, more importantly, maintaining compliance throughout their products' lifecycle. This integrated approach not only addresses current CRA requirements but positions organizations to adapt seamlessly to future regulatory changes.

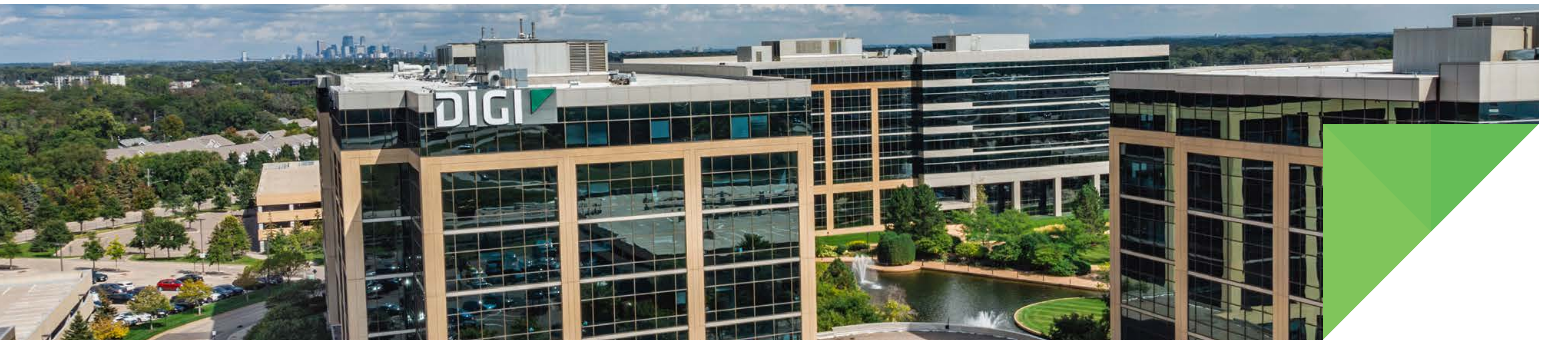
Conclusion

The CRA represents a fundamental shift in the digital product landscape. It establishes cybersecurity as a foundational, non-negotiable element of product design and lifecycle management.

While the CRA originated in Europe, its influence is already extending globally. By adopting its principles now, organizations can prepare for emerging regulations in other regions — transforming compliance from a challenge into an opportunity for sustainable growth and long-term market leadership.

Organizations that approach CRA compliance strategically will also discover opportunities beyond regulatory adherence. By embedding security throughout the product lifecycle — from conception through development, production, deployment, and maintenance — manufacturers can build deeper customer trust, reduce costly security incidents, and create more resilient products that stand the test of time.

[Request a free one-hour Digi security consultation](#) →



Why Digi?

Digi is a complete IoT solutions provider, supporting every aspect of your project, from mission-critical communications equipment to design and deployment services to get your application designed, installed, tested, and functioning securely, reliably and at peak performance.

Digi builds its products for high reliability, high performance, security, scalability, and versatility so customers can expect extended service life, quickly adapt to evolving system requirements, and adopt future technologies as they emerge. Digi embedded modules, routers, gateways, and infrastructure management solutions support the latest connected applications across verticals, from the enterprise to transportation, energy, industrial and smart cities use cases.

Our solutions enable connectivity to standards-based and proprietary equipment, devices, and sensors, and ensure reliable communications over virtually every form of wireless or wired systems. Our integrated remote management platform helps accelerate deployment and provide optimal security using highly efficient network operations for mission-critical functions such as mass configuration and firmware updates, as well as system-wide monitoring with dashboards, alarms, and performance metrics.

Company Background

- Digi has been connecting the “Internet of Things” — devices, vehicles, equipment and assets – since 1985
- Digi is publicly traded on the NASDAQ stock exchange: DGII
- Headquartered in the Twin Cities of Minnesota, Digi employs over 800 people globally, and has connected over 100 million devices worldwide

As an IoT solutions provider, Digi puts proven technology to work for our customers so they can light up networks and launch new products. Machine connectivity that’s relentlessly reliable, secure, scalable and managed — and always comes through when you need it most. That’s Digi.

Next Steps

- Ready to talk to a Digi expert? **Contact us**
- Want to hear more from Digi? **Sign up for our newsletter**
- Shop now for Digi solutions: **How to buy**

Contact a Digi expert and get started today

PH: 877-912-3444
www.digi.com

Digi International Worldwide Headquarters
9350 Excelsior Blvd. Suite 700
Hopkins, MN 55343

DIGI®

/digi.international @DigiDotCom /digi-international

While every reasonable effort has been made to ensure that this information is accurate, complete, and up-to-date, all information is provided “AS IS” without warranty of any kind. We disclaim liability for any reliance on this information. All registered trademarks or trademarks are property of their respective owners.