FORTEIA

EU Cyber Resilience Act

Practical Implementation Guide

A Business & Technical Readiness Guide for Digital Products

W H I T E P A P E R

May 2026

Prepared by FORTEIA

Trust · Governance · Security

Global Presence: Europe (France, Belgium) · India (Pune, Mumbai)

Contents

Foreword

CRA accountability begins in the boardroom – not the security operations centre.

Late on a Friday afternoon in March 2026, a Brussels–based product director discovers that one of her firm's connected devices – sold across the EU for the past six years – contains a vulnerability now being actively exploited by a threat actor known to European cybersecurity authorities. From the moment her team becomes aware, she has 24 hours to file an early–warning notification with national authorities. Once reporting obligations apply, the regulation provides very limited operational tolerance for delayed notification.

That scenario is not hypothetical. It is the operational reality created by Regulation (EU) 2024/2847 – the EU Cyber Resilience Act – which entered into force on 10 December 2024 and begins enforcing its first major obligations on 11 September 2026.

The CRA does not simply add a new compliance layer to existing cybersecurity frameworks. It rewrites the relationship between digital products and the markets that consume them. For the first time in the European Union, manufacturers become directly subject to cybersecurity accountability and market–surveillance enforcement obligations.

This whitepaper has been prepared for the executives, security leaders, and product owners who will carry the weight of that accountability. Our intent is to translate regulation into structured, achievable action – what to do this quarter, what to plan for next year, and where the genuine risks lie.

Every statistic in the pages that follow is anchored to a primary institutional source, independently verifiable from the original publisher.

Executive Summary

The Cyber Resilience Act is among the most consequential cybersecurity regulations introduced by the European Union for digital products. Adopted by the European Parliament and Council on 23 October 2024 and published in the Official Journal three weeks later, the regulation is now binding law across all 27 Member States. Unlike a directive, it requires no national transposition. Implementation timelines are already in effect.

Three dates matter. The CRA entered into force on 10 December 2024. From 11 September 2026, manufacturers must submit the required CRA early–warning notification within 24 hours of becoming aware of an actively exploited vulnerability – a hard, non–negotiable deadline that applies to legacy products as much as to new ones. Then, on 11 December 2027, the full body of obligations takes effect: secure–by–design engineering, conformity assessment, CE marking, lifecycle support, and Software Bill of Materials transparency. The September 2026 milestone is the one most organisations underestimate. It pulls the practical readiness deadline forward by roughly fifteen months.

10 Dec 2024

CRA Enters Into Force

Directly applicable in all 27 EU Member States. No transposition required.

11 Sep 2026

Reporting Obligations Begin

24–hour early-warning notification obligations for actively exploited vulnerabilities – including legacy products.

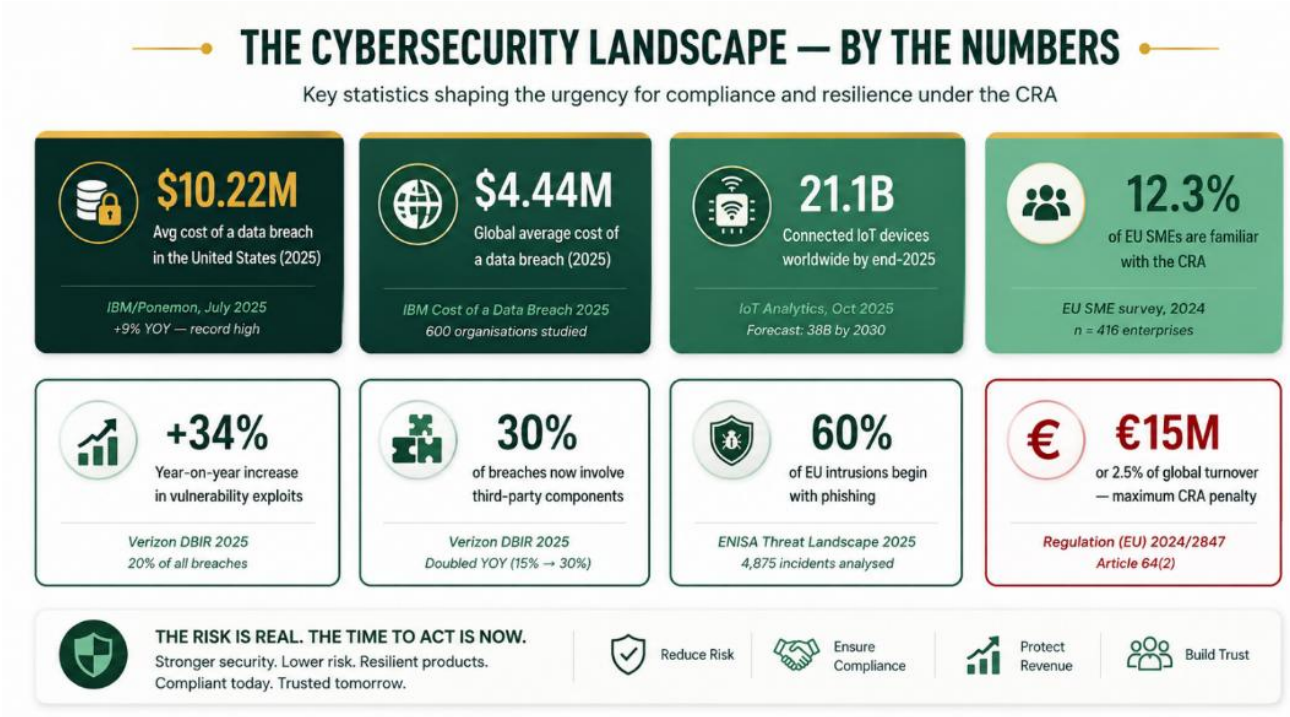
11 Dec 2027

Full Compliance Mandatory

CE marking, secure–by–design, SBOM, conformity assessment and lifecycle support all required.

The economic argument for acting now is unambiguous. The IBM Cost of a Data Breach Report 2025 – IBM's 20th annual study, conducted by Ponemon Institute across 600 breached organisations between March 2024 and February 2025 – placed the global average breach cost at USD 4.44 million. In the United States, where regulators have begun pursuing significant penalties, the figure climbed 9% year–on–year to a record USD 10.22 million. European organisations would do well to read the U.S. trajectory as a forecast of what active CRA enforcement may eventually look like.

Awareness, however, has not kept pace with obligation. An academic survey of 416 European SMEs published in 2024 found that only 12.3% were familiar with the Cyber Resilience Act – a gap that ENISA's ongoing SME cybersecurity initiatives continue to reinforce growing concerns regarding SME preparedness across Europe. FORTEIA's field experience confirms this gap extends well into mid–market and enterprise organisations, particularly for products embedded inside larger systems, SaaS offerings with downloadable agents, and AI–enabled features integrated into existing applications.



Eight statistics that frame the CRA opportunity – and the cost of inaction.

What the CRA Actually Requires

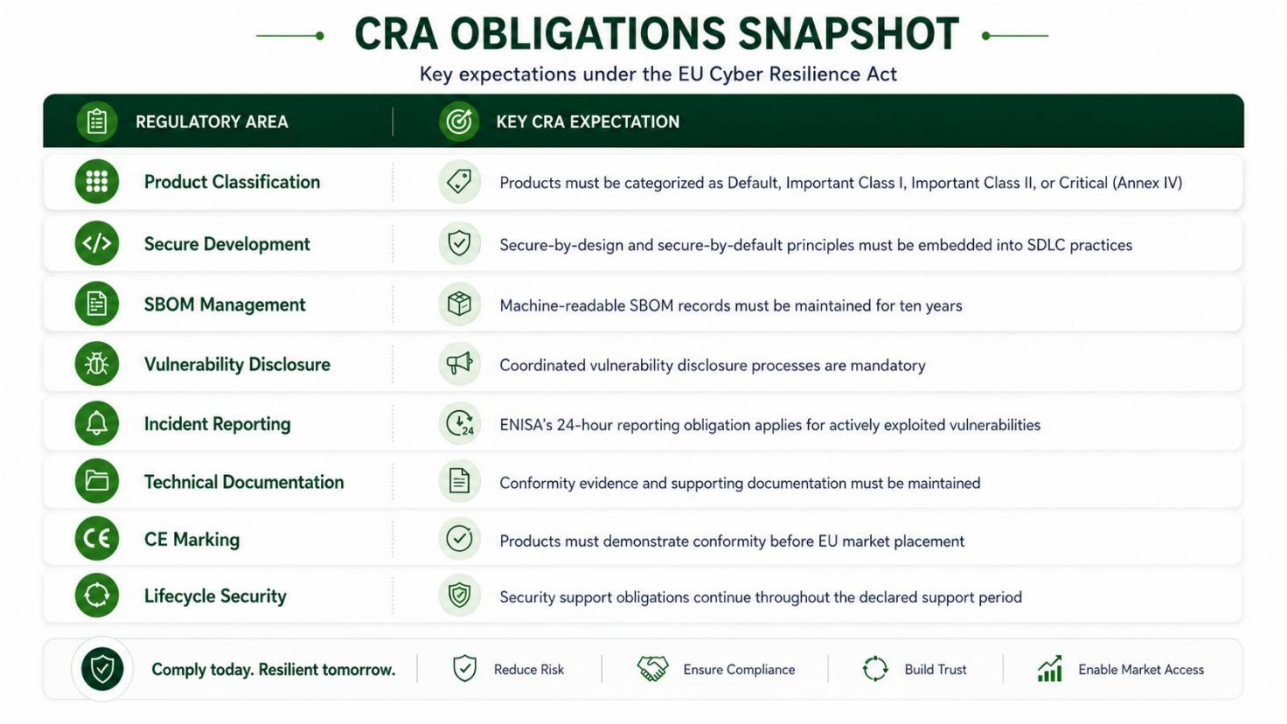
The regulation imposes structured obligations across the product lifecycle. Manufacturers must classify their products into one of four risk tiers – ***Default, Important Class I, Important Class II, or Critical*** – each with distinct conformity assessment routes. They must adopt secure software development practices and ship with secure–by–default configurations. They must maintain a machine–readable Software Bill of Materials and retain it for ten years after the product is placed on the market.

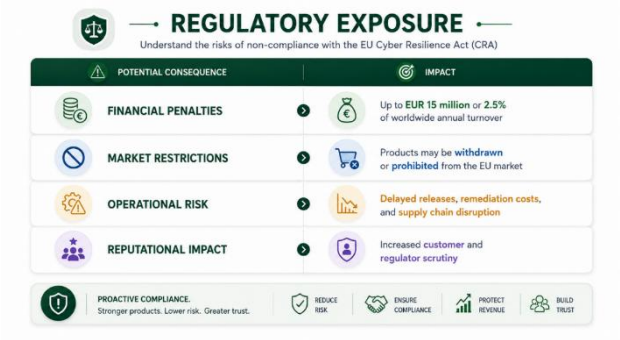
They must operate a coordinated vulnerability disclosure programme and meet the CRA's 24-hour early-warning notification obligations. They must affix CE marking, maintain technical documentation, and stand behind the security of their products throughout their declared support period.

Penalties for non–compliance reach EUR 15 million or 2.5% of total worldwide annual turnover, whichever is higher. Market surveillance authorities may restrict, withdraw, recall, or prohibit non–conformant products from the EU market. For organisations with material European revenue, the business risk is immediate and operationally significant.

FORTEIA's recommendation is straightforward: treat the CRA as a programme of operational maturity rather than a compliance project. Organisations that take this view typically emerge with stronger products, more loyal customers, and a clearer security posture. Those that delay tend to encounter regulatory risk and competitive disadvantage simultaneously.

> ***The CRA is not reacting to a future problem – it is responding to an already measurable failure in digital product security.***





Business Impact

CRA enforcement risk extends beyond fines. Product withdrawal, delayed market access, reputational erosion, and incident–response pressure create measurable business exposure for organisations operating in the EU digital market.

Organisations that delay governance alignment often underestimate the operational effort required to maintain vulnerability reporting, SBOM governance, and supplier oversight simultaneously.

1. Why the CRA – and Why Now

> ***The Cyber Resilience Act is not merely a cybersecurity regulation – it is the European Union's attempt to redefine digital trust, product accountability, and market resilience at scale.***

A Threat Landscape That Demanded Regulation

The Cyber Resilience Act did not arrive in a vacuum. It is the European Union's structured response to a measurable, sustained deterioration in the security posture of digital products entering its market. ENISA's Threat Landscape report for 2025, published in October, analysed 4,875 cybersecurity incidents observed between July 2024 and June 2025 – the most comprehensive recent picture of what European defenders are facing. Phishing has become the single dominant initial intrusion vector. Connected mobile devices feature in roughly two–fifths of observed threats. The pace and sophistication of supply chain compromise has continued to accelerate.

60%

of EU cyber intrusions begin with phishing – the dominant initial intrusion vector across all ENISA–observed sectors in 2024–2025.
Source: ENISA Threat Landscape 2025

Verizon's 2025 Data Breach Investigations Report, released on 23 April 2025 in its eighteenth annual edition, reinforces the picture from a different angle. Its analysis of more than 22,000 security incidents and 12,195 confirmed breaches, gathered across 139 countries, identified four shifts that should concern any organisation placing digital products on the EU market:

- Vulnerability exploitation grew +34% year–on–year, now 20% of all breaches
- Edge–device exploitation (firewalls, VPNs, routers) rose nearly eightfold – from 3% to 22%
- Third–party involvement doubled in a single year, rising from 15% to 30%
- Ransomware present in 44% of breaches, median ransom USD 115,000

+34%

year–on–year increase in vulnerability exploitation as an initial breach vector. Now the second–most–common entry point.
Source: Verizon DBIR 2025

Each of these trends maps directly onto a specific CRA obligation. Edge–device exploitation is precisely why network routers and firewalls sit in the Important (Class I) category. The doubling of third–party involvement is why the regulation's SBOM requirement is mandatory rather than recommended. And the 34% surge in vulnerability exploitation is why the 24–hour reporting clock starts in September 2026.

The Economic Stakes

USD 4.44M

global average breach cost in 2025. U.S. organisations averaged USD 10.22M – an all–time record. The U.S. trajectory is a credible forecast for post–CRA enforcement in Europe.
Source: IBM Cost of a Data Breach Report 2025

The financial consequences of cyber incidents continue to escalate even as security investment grows. The IBM Cost of a Data Breach Report 2025 – IBM's twentieth annual edition, conducted by Ponemon Institute across 600 organisations between March 2024 and February 2025 – reported that the global average cost of a breach declined for the first time in five years, falling 9% to USD 4.44 million. Much of that improvement was driven by faster detection and containment in organisations that have deployed security AI and automation extensively.

The U.S. trajectory is moving in the opposite direction. American organisations now face an average breach cost of USD 10.22 million, an all–time record and a 9% increase year–on–year. The drivers are higher regulatory fines, longer detection cycles, and increased post–breach customer support costs. For European companies, the pattern functions as a credible warning: once enforcement under the CRA begins in earnest, breach economics in the EU may follow a similar arc.

The Connected–Product Surface

The volume of products to which the CRA applies is growing relentlessly. IoT Analytics' State of IoT 2025 report, published in October 2025, places the global count of connected IoT devices at 18.5 billion in 2024 and forecasts 21.1 billion by the end of 2025 – a 14% year–on–year increase. The same forecast projects 39 billion devices by 2030. Each is a potential product with digital elements; each, where placed on the EU market, a potential CRA obligation.

The Awareness Gap

The most striking finding in the EU's preparedness picture is how few organisations are ready. An academic study published in 2024 – "Ensuring Cybersecurity Compliance: Assessing SME Awareness and Preparedness for the Cyber Resilience Act" – surveyed 416 European small and medium–sized enterprises and found that only 12.3% were familiar with the regulation. ENISA's SME cybersecurity initiatives further reinforce growing concerns regarding cybersecurity preparedness across European SMEs, and FORTEIA's engagement experience suggests these challenges extend meaningfully into mid–market and enterprise organisations as well.

12.3 %

of EU SMEs surveyed were familiar with the Cyber Resilience Act in 2024. Awareness has improved since but remains far below the level needed for sector–wide readiness by 2026.
Source: Mauri et al., 2024 (n=416). ENISA SME Cybersecurity guidance corroborates the trend.

The pattern is consistent: CRA scope is most often underestimated for products embedded inside larger systems, for SaaS offerings with downloadable agents, and for AI–enabled features bolted onto existing applications. The first phase of any FORTEIA CRA engagement is therefore not technical – it is investigative.

2. Understanding the Cyber Resilience Act

What the CRA Is

The Cyber Resilience Act establishes mandatory cybersecurity requirements for products with digital elements placed on the EU market. Enacted as Regulation (EU) 2024/2847, it is directly applicable in all Member States – there is no national transposition step. This makes the CRA more uniform in application than directives such as NIS2.

Scope of Application

Unlike previous EU cybersecurity legislation, the CRA is product–centric. It places security accountability directly on those who design, manufacture, and distribute digital products – from IoT devices and industrial control systems to enterprise software and consumer applications.

Non–EU manufacturers selling into the EU must comply. Importers and distributors bear their own obligations to verify conformity before placing products on the market.

Products exempt from the CRA include: medical devices under (EU) 2017/745; motor vehicles under (EU) 2019/2144; aviation products under (EU) 2018/1139; and products used exclusively for military or national security purposes.

Pure SaaS services are generally considered outside the CRA's primary scope unless they form an integral component of a product with digital elements. Furthermore Open–source software without commercial intent is exempt; manufacturers commercially integrating OSS components are not.

Key obligations under the CRA

The Cyber Resilience Act establishes mandatory security, governance, vulnerability management, and lifecycle obligations for all products with digital elements placed on the EU market.

Critical CRA deadlines

The September 2026 reporting milestone effectively accelerates operational readiness requirements by more than a year. Organisations delaying preparation until 2027 risk entering compliance programmes after mandatory reporting obligations have already begun.

By September 2026, many organisations will discover that vulnerability reporting readiness is already too late to build.

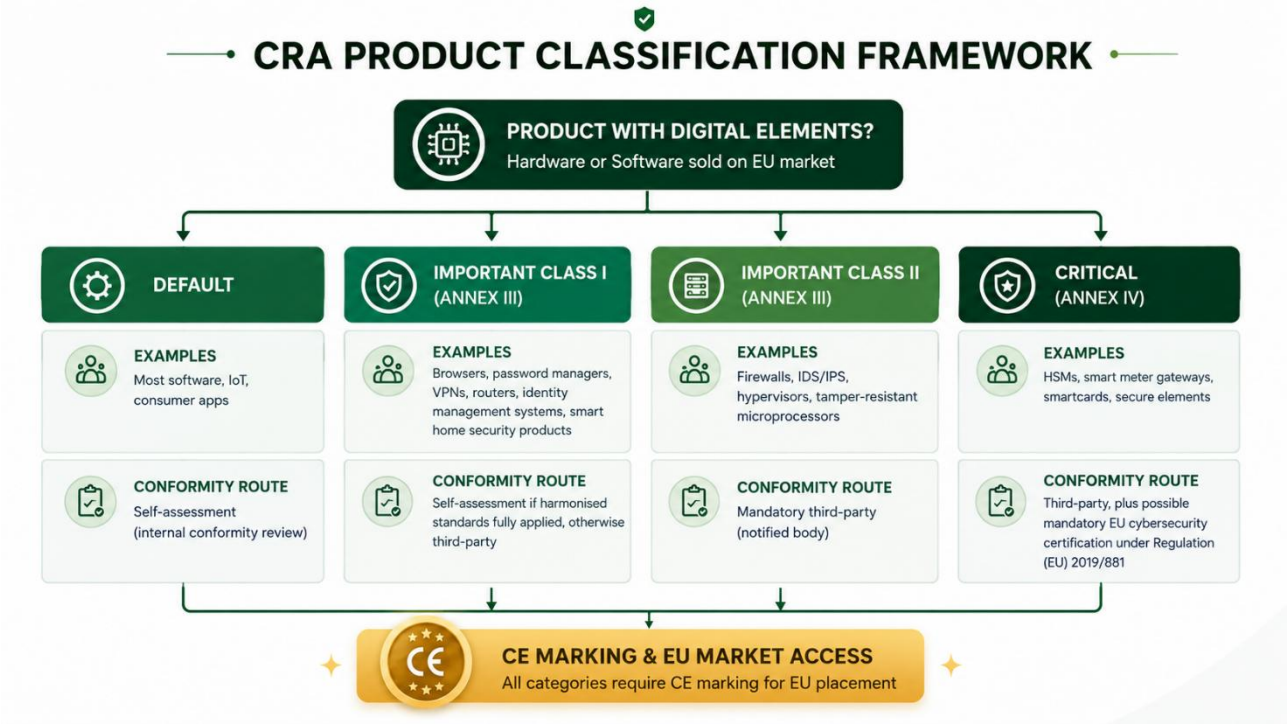
3. Product Classification & Scope Assessment

The Four Risk Tiers

The CRA establishes four risk tiers for products with digital elements, each with distinct conformity assessment requirements.

- Default products are not listed in Annex III or Annex IV.
- Important products are listed in Annex III and are split into Class I (e.g. browsers, password managers, VPNs, routers, identity management systems) and the higher-risk Class II (e.g. firewalls, intrusion detection and prevention systems, hypervisors, tamper-resistant microprocessors).
- Critical products are listed in Annex IV (e.g. hardware security modules, smart meter gateways, smartcards, secure elements).

The tier determines whether a manufacturer can self-declare compliance, must apply harmonised standards, must engage a notified body, or – for certain Critical products – may be required to obtain a European cybersecurity certificate under Regulation (EU) 2019/881.



Implementing Regulation 2025/2392

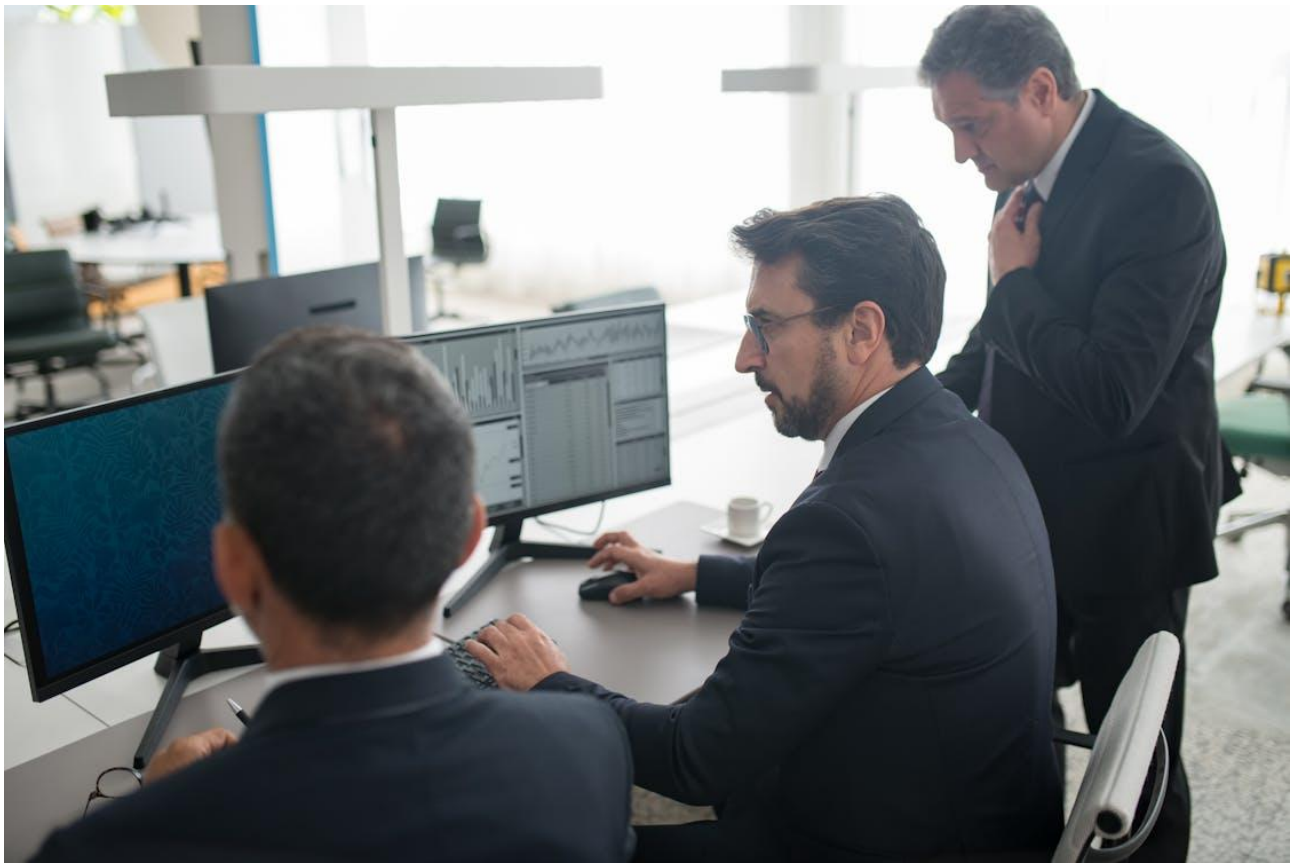
On 28 November 2025, the European Commission adopted Implementing Regulation (EU) 2025/2392, providing the definitive technical description of important and critical product categories with non–exhaustive examples. This is now the primary reference for applying the 'core functionality' test to determine product classification.

Open–Source Software

The CRA includes a specific and nuanced treatment of open–source software (OSS). OSS maintainers who do not monetize their software are generally not considered manufacturers under the CRA and therefore fall outside its direct scope. The regulation introduces the concept of an *"open–source software steward"* for community projects with commercial support.

However, organizations that commercially integrate open–source components into their products – as virtually all software vendors do today – bear the full weight of CRA obligations for those components. This includes dependency management, vulnerability tracking, SBOM documentation, and continuous monitoring.

FORTEIA recommends that organizations map all OSS dependencies during their initial Discover phase and assess their obligations under the CRA's commercial integration rules. The Verizon DBIR 2025 finding that 30% of breaches now involve third–party components reinforces the importance of this exercise.



Open–source software may be developed outside regulatory scope – but the moment it becomes part of a commercial product, accountability shifts from the community to the manufacturer.

4. Key Implementation Challenges

Many organizations understand the theoretical objectives of the CRA but encounter significant operational challenges when moving toward implementation. Drawing on FORTEIA's engagement experience and supporting industry data, the following areas typically require the most attention.

Product Scope & Applicability Assessment

Determining CRA scope requires structured analysis of all products, SaaS integrations, embedded components, and open–source dependencies. Misclassification carries severe regulatory risk. A formal applicability assessment before committing resources is the recommended first step.

Secure Software Development Lifecyle

FORTEIA's assessments consistently identify gaps in secure development practices, including:

- Inconsistent or absent threat modeling
- Weak dependency and open–source component management
- Limited static and dynamic application security testing
- Poor secrets management and credential hygiene
- Inadequate security gates in CI/CD pipelines
- Lack of security review during product design

Industry research consistently identifies third–party code as a leading source of security debt, and the time required to remediate identified vulnerabilities continues to lengthen. The Verizon DBIR 2025 finding that 30% of breaches now involve third–party components – double the 2024 figure – reinforces that point from a complementary angle: dependency hygiene is no longer optional. The CRA materially raises expectations across all of these areas.

Vulnerability Management & PSIRT

Vulnerability handling is one of the most critical operational challenges under the CRA. Organizations must establish formal processes for vulnerability identification, disclosure, advisory communication, patch management, and continuous monitoring.

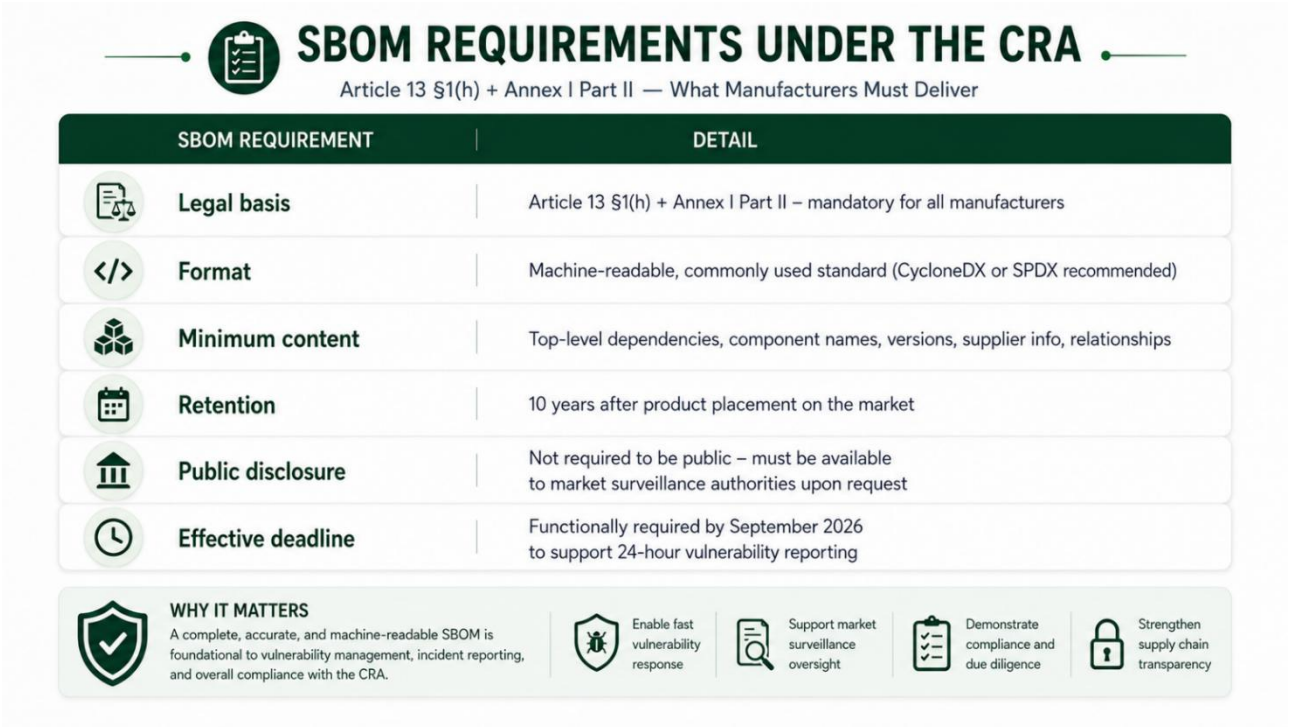
Most organisations lack a formal Product Security Incident Response Team or coordinated vulnerability disclosure programme. With ENISA reporting obligations beginning 11 September 2026, establishing these capabilities is now urgent.

24h

mandatory early-warning notification window for actively exploited vulnerabilities under CRA – applies to all products including legacy.
Source: CRA Article 14 (effective 11 Sep 2026)

Software Bill of Materials (SBOM)

The CRA creates a legally binding SBOM requirement. Technical documentation – including the SBOM – must be maintained for a minimum of 10 years after market placement. SBOM must be machine–readable (CycloneDX or SPDX).



Supply Chain & Third–Party Risk

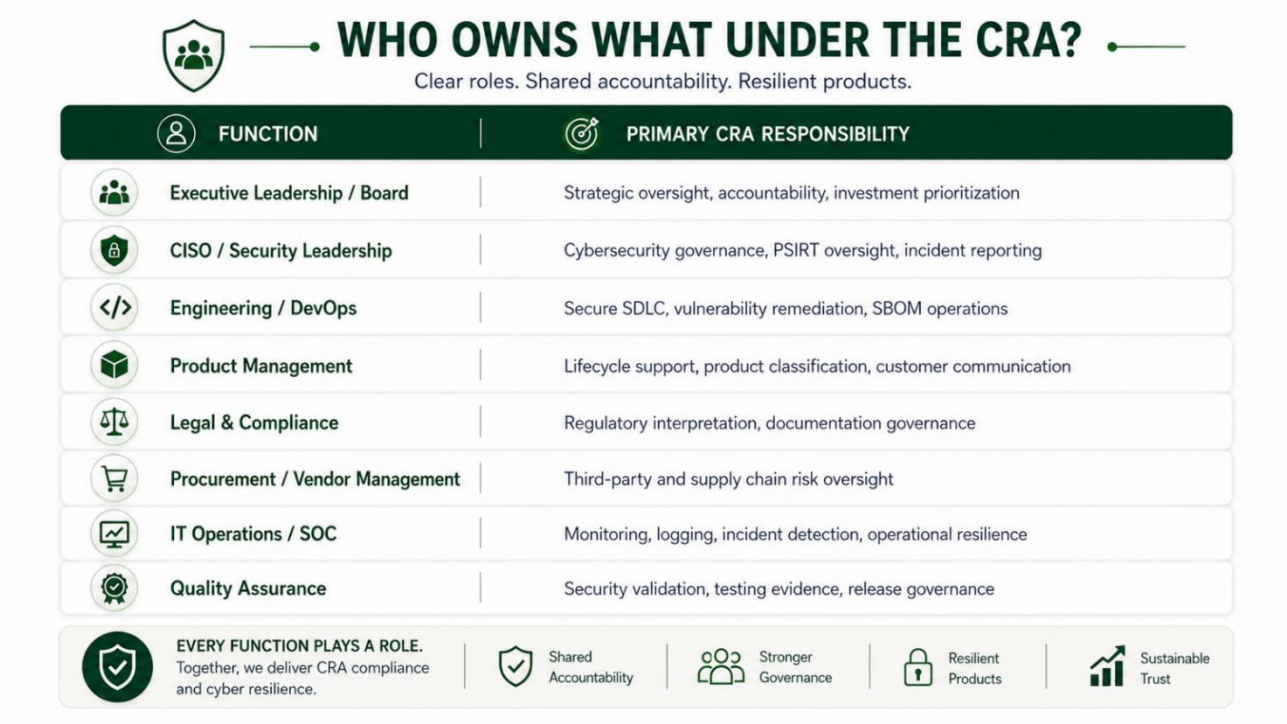
Modern products depend extensively on open–source components, external APIs, cloud services, third–party libraries, and managed service providers. The CRA places explicit obligations on manufacturers to understand, manage, and document this dependency landscape.

30%

of 2025 breaches involved third–party components – double the 15% reported in 2024. Supply chain compromise is now a leading vector.
Source: Verizon DBIR 2025

Governance & Accountability

Successful CRA implementation requires clear ownership and cross–functional coordination across security, engineering, product management, legal, compliance, and executive leadership. Organizations that lack defined accountability structures will struggle to sustain compliance over time and to respond effectively to the 24–hour reporting clock.



The complexity of CRA implementation means that isolated compliance activities are rarely sufficient. Organisations require a structured operational framework capable of aligning governance, engineering, vulnerability management, supply–chain oversight, and lifecycle security into a measurable and sustainable compliance programme.

> ***Under the CRA, the greatest implementation risk is rarely the absence of security tools – it is the absence of operational ownership, process discipline, and continuous visibility across the product lifecycle.***

5. FORTEIA Implementation Framework (CRORF)

FORTEIA's CRA Readiness & Operational Resilience Framework (CRORF) provides a structured, phased path to compliance. Cross–functional alignment – security, engineering, legal, and product – is essential throughout.

1

Discover – Scope & Applicability Assessment

Identify all products, systems, and services potentially impacted by the CRA. Conduct product inventory, SaaS and cloud applicability analysis, third–party dependency mapping, AI feature identification, and regulatory overlap mapping (NIS2, GDPR, DORA).

Deliverables: *CRA applicability matrix · Product classification overview · Initial risk profile · Executive briefing*

2

Assess – Gap Analysis & Maturity Evaluation

Evaluate current cybersecurity posture against CRA expectations. Assessment covers governance maturity, secure SDLC practices, vulnerability management and PSIRT readiness, incident response capabilities, supply chain security, and technical documentation completeness.

Deliverables: *CRA gap assessment report · Maturity heatmap · Risk prioritisation matrix · Compliance roadmap*

3

Secure – Technical Remediation

Address identified gaps through targeted enhancements. Focus areas: SAST/DAST/SCA tooling integration; SBOM tooling (CycloneDX/SPDX); DevSecOps and CI/CD hardening; encryption, authentication, and secure update mechanisms; container and infrastructure security.

Deliverables: *Technical remediation roadmap · Security architecture improvements · DevSecOps enhancement plan*

4

Govern – Policies & Operational Readiness

Establish governance for ongoing CRA obligations. Includes: PSIRT setup and operational procedures; coordinated vulnerability disclosure policy; CRA-aligned vulnerability and incident reporting workflows; supplier risk management framework; executive reporting model.

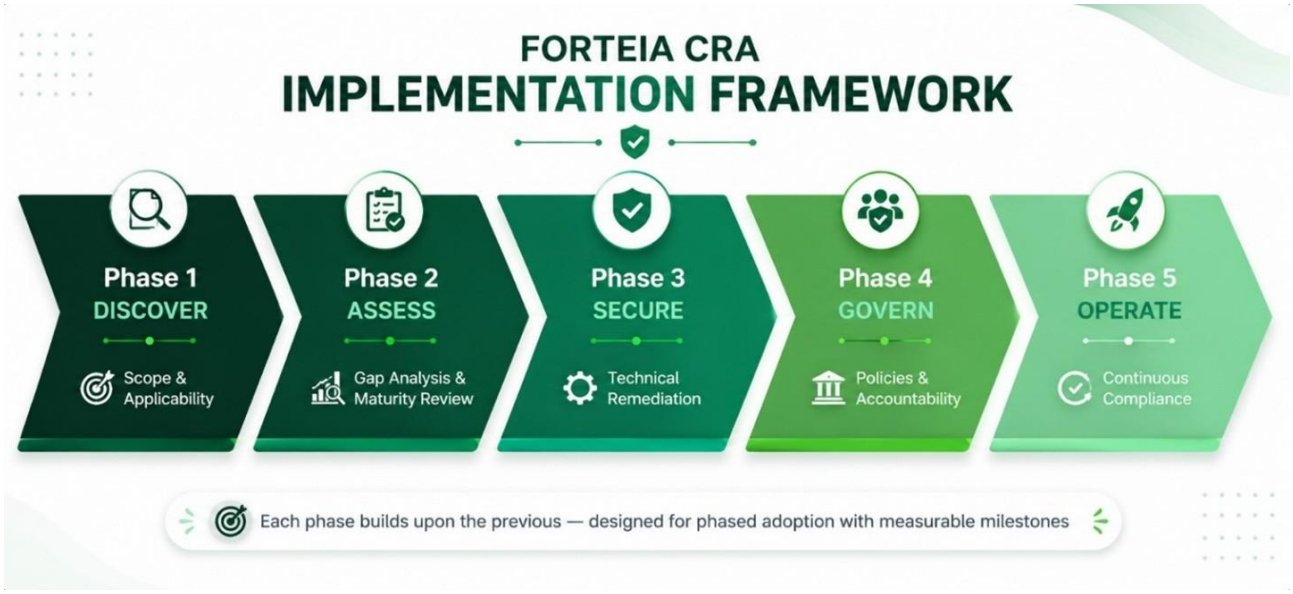
Deliverables: *Governance framework · Vulnerability disclosure policy · Incident response playbooks*

5

Operate – Continuous Compliance & Lifecycle Security

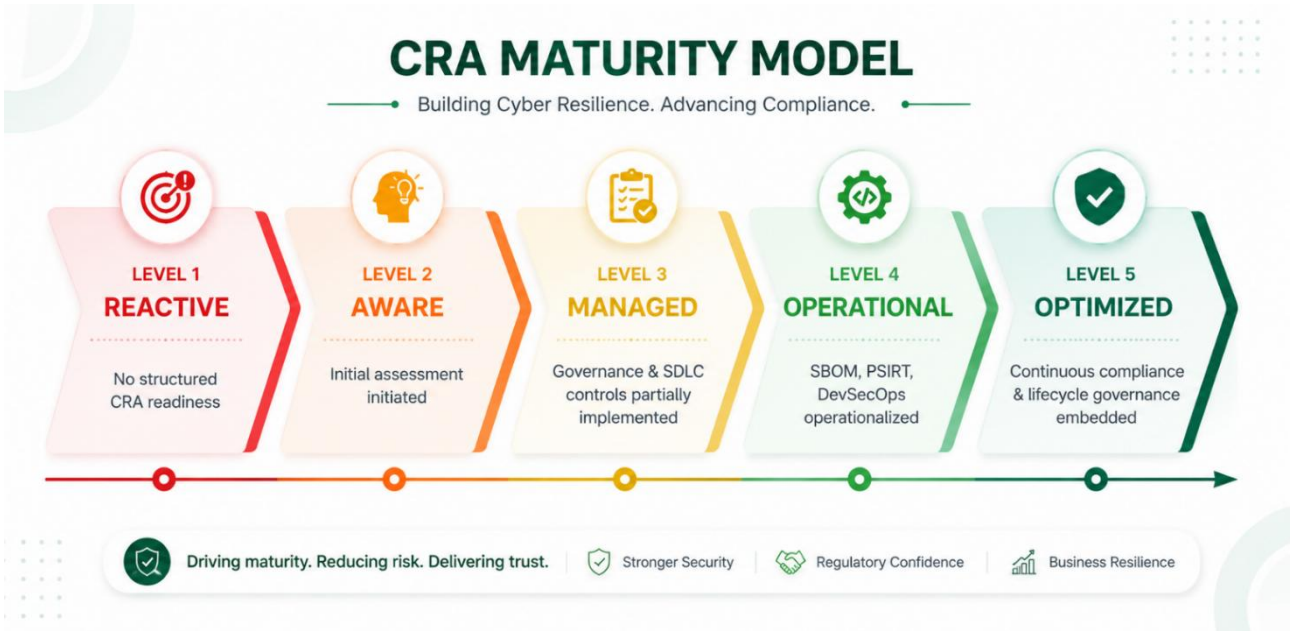
CRA compliance is not a one–time exercise. Continuous vulnerability monitoring and CVE tracking, security patch management, incident response, periodic supplier reassessment, security advisory publication, and ongoing documentation maintenance.

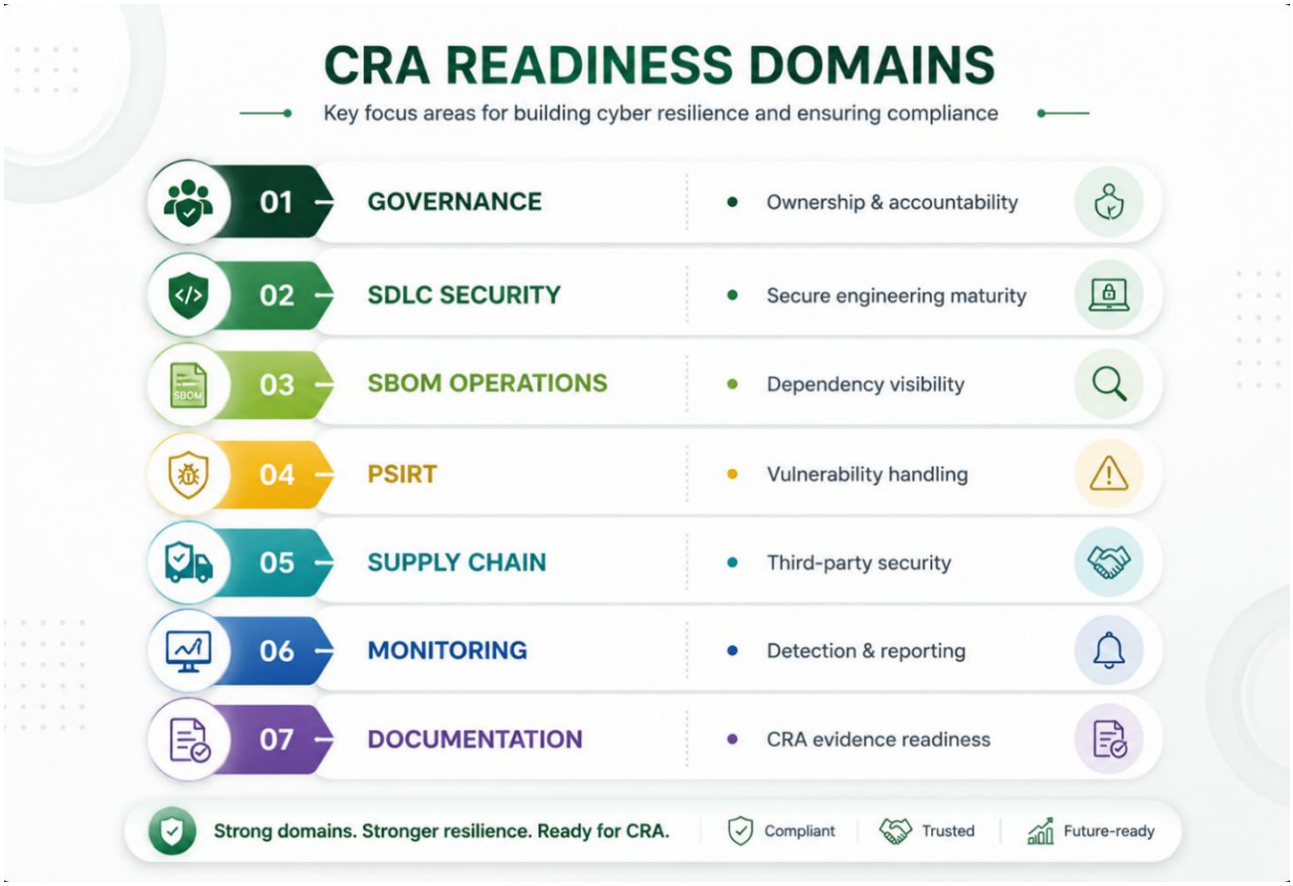
Deliverables: *Continuous compliance model · Governance dashboards · Audit readiness programme*



FORTEIA CRA Readiness Index

The FORTEIA CRA Readiness Index provides a structured maturity framework for assessing organizational preparedness across governance, engineering, operational resilience, and lifecycle security domains. CRA readiness cannot be evaluated through documentation alone. Organisations must demonstrate operational maturity across governance, engineering, vulnerability management, and lifecycle security capabilities.

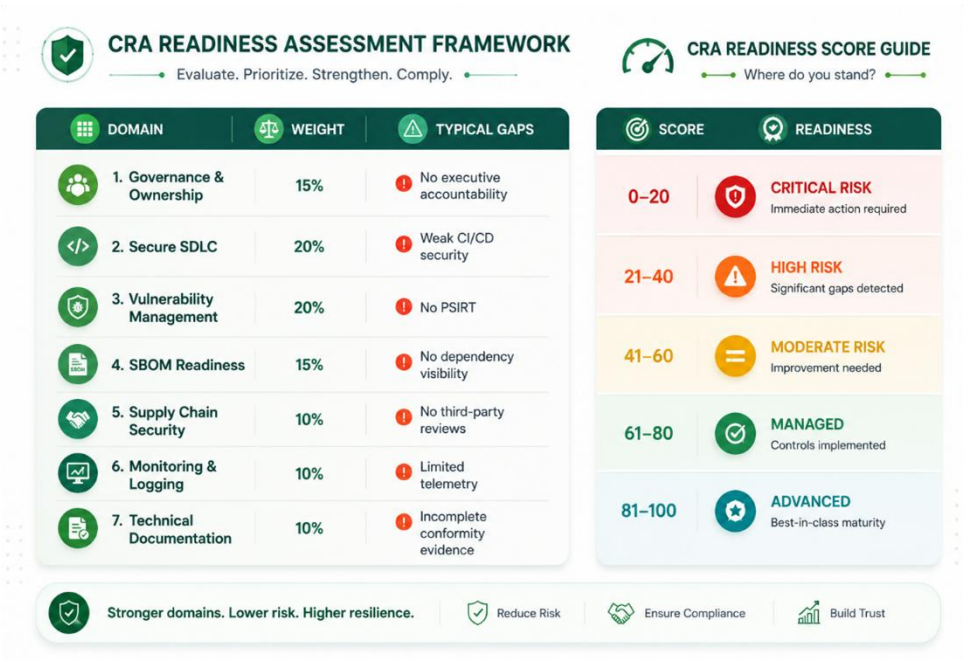




FORTEIA CRA Readiness Scoring Model

FORTEIA's early CRA assessments suggest that organizations typically score lowest in SBOM operational readiness, vulnerability disclosure governance, and technical documentation maturity.

Organizations are evaluated across weighted operational domains aligned to CRA implementation maturity. Scores are derived through structured assessment workshops, documentation review, technical control evaluation, and governance interviews.



6. Technical Security Considerations

Organizations implementing CRA readiness must evaluate and strengthen multiple technical security domains. The following areas represent the most significant technical focus, supported by industry data.

6.1 DevSecOps Integration

Modern development environments require security to be embedded throughout the software development lifecycle – not applied as a final checkpoint before release. CRA compliance demands that security controls are integrated into development workflows, toolchains, and team responsibilities.

Recommended Controls:

- Static Application Security Testing (SAST) integrated into code review
- Dynamic Application Security Testing (DAST) during staging and pre–production
- Dependency scanning and software composition analysis (SCA)
- Infrastructure–as–Code security validation
- Container image scanning and runtime security
- CI/CD pipeline security gates with enforced policy thresholds
- Secrets management and credential lifecycle controls

USD 1.9M

average breach–cost saving for organisations using security AI and automation extensively. AI–enabled prevention associated with lifecycles 80 days shorter than baseline.
Source: IBM Cost of a Data Breach Report 2025

SBOM Operations

SBOM implementation should be an operational security capability, not a compliance artifact. An actionable programme includes: automated SBOM generation at each build (CycloneDX or SPDX); real–time correlation with NVD/OSV; cryptographic signing; secure sharing with regulators; 10–year retention policy per CRA Article 13.

An actionable SBOM programme includes:

- Automated SBOM generation at each build cycle (CycloneDX or SPDX format)
- Real–time correlation of SBOM components with known vulnerability databases (NVD, OSV)
- Dependency tree visualization for supply chain risk assessment
- Cryptographic signing of SBOMs to ensure integrity and provenance
- Secure SBOM sharing workflows with regulators and enterprise customers
- 10–year retention policy aligned with CRA Article 13 obligations

Practical finding: *A European SaaS provider reduced SBOM generation time by ~70% after integrating automated generation into CI/CD using CycloneDX tooling.*

Identity & Access Management

Strong identity security controls underpin secure product operation. The Verizon DBIR 2025 found that 22% of breaches still begin with credential abuse, and that 88% of attacks against basic web applications involved stolen credentials. Organizations should review and strengthen:

- Multi–factor authentication across product interfaces and internal systems
- Privileged access management for production and critical systems
- Least–privilege enforcement for all service accounts and developer access
- Remote access security and zero–trust architecture alignment
- Identity lifecycle management (joiner–mover–leaver processes)

6.4 Cloud & Infrastructure Security

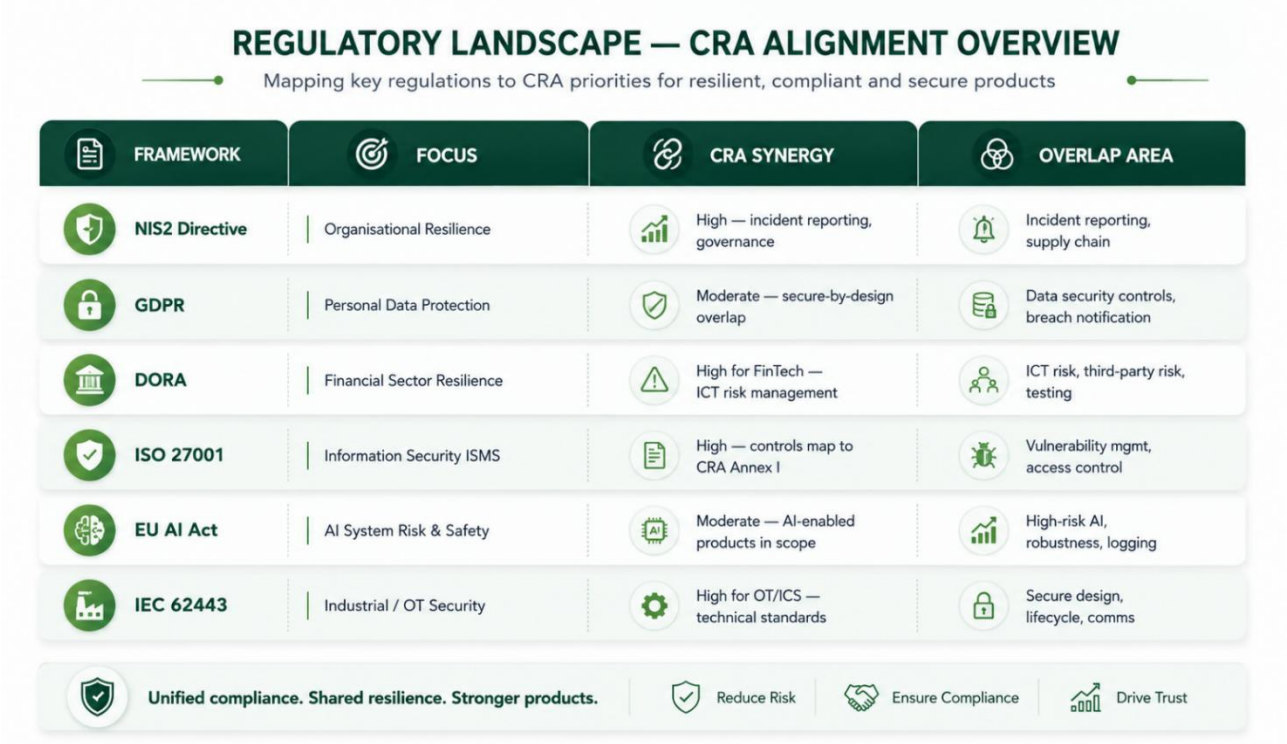
Breaches involving public cloud averaged USD 5.17M in 2025 – materially above the global mean. Focus areas: cloud configuration posture management; centralised SIEM; network segmentation; encryption at rest and in transit; API security; Kubernetes hardening.

6.5 Open–Source Risk Management

Open–source software has become foundational to modern digital products, but under the CRA, organisations remain fully accountable for the security, maintenance, vulnerability management, and lifecycle governance of all commercially integrated OSS components. Effective open–source risk management therefore requires continuous dependency visibility, software composition analysis (SCA), vulnerability monitoring, and supply–chain governance across both direct and transitive dependencies.

7. Regulatory Alignment

Organisations in the EU face overlapping regulatory obligations. A unified cybersecurity governance strategy significantly reduces duplication. FORTEIA recommends developing a unified control mapping across CRA Annex I, ISO 27001, NIS2, and applicable sector frameworks – reducing audit overhead and accelerating time to compliance.



Important: The mappings above represent practical control–level overlap only. Only the CRA itself defines binding obligations under Annex I. Organisations should seek qualified legal and compliance counsel for specific obligations applicable to their products and sectors.

FORTEIA recommends developing a unified control mapping that demonstrates compliance with CRA Annex I requirements alongside relevant ISO 27001 controls, NIS2 obligations, and applicable sector–specific frameworks. This approach reduces audit overhead, simplifies governance reporting, and accelerates time to compliance.

Practical Synergies

On 28 November 2025, the European Commission adopted Implementing Regulation (EU) 2025/2392. Where existing regulatory infrastructure is already in place, organisations can typically reuse a substantial portion of evidence and process artefacts when extending into CRA scope. The mappings below should be understood as practical control–level overlap; only the CRA itself defines binding obligations under Annex I.

- NIS2 incident-reporting workflows can be extended to support CRA reporting obligations with minimal new infrastructure.
- GDPR Data Protection Impact Assessments (DPIAs) can be extended to include software vulnerability handling under CRA.

- ISO/IEC 27001:2022 vulnerability–management controls (notably A.8.8 and A.5.7) provide a strong foundation for CRA Annex I obligations, though ISO 27001 is an organisational ISMS standard and not a CRA–specific framework.
- DORA ICT risk–management controls overlap substantially with CRA secure–development obligations for organisations in financial services.
- ISA/IEC 62443 secure–design practices map directly to CRA Annex I.1 essential cybersecurity requirements for industrial control systems and OT environments; the standard is sector–specific to industrial automation.

> ***The organisations that achieve CRA readiness fastest will not be those building entirely new compliance programmes – but those intelligently aligning and operationalising the controls they already possess.***

8. CE Marking & Conformity Assessment

> ***Under the CRA, CE marking is no longer a symbolic market–access label – it becomes a visible declaration of cybersecurity accountability across the entire product lifecycle.***

All products with digital elements placed on the EU market must carry CE marking demonstrating CRA conformity. The assessment route depends on product classification. Technical documentation must be maintained throughout the support period and for a minimum of 10 years after market placement.

Product Class	Assessment Route	Key Requirements
Critical (Class II)	Mandatory third-party conformity assessment by Notified Body	✓ External audit ✓ Harmonised standard compliance ✓ EC Declaration of Conformity
Important (Class I)	Third-party assessment or self-assessment using harmonised standards	✓ Technical documentation ✓ Harmonised standard alignment ✓ Declaration of Conformity
Default	Internal self-assessment against Annex I requirements	✓ Technical documentation ✓ Vulnerability handling process ✓ Declaration of Conformity

Declaration of Conformity

Upon successful conformity verification, manufacturers must complete a Declaration of Conformity (DoC) for each product. The DoC must reference the applicable Annex and be kept current throughout the product lifecycle.

Technical Documentation – Annex VII

Required contents: product description and design; security risk assessment; SBOM; vulnerability handling process; test results; Declaration of Conformity reference. Must be kept up to date and retained for 10 years.

9. Recommendations

Organizations initiating CRA readiness programmes should structure their activities across three time horizons. The 11 September 2026 vulnerability reporting deadline creates a near–term implicit obligation that demands immediate attention.

Immediate Priorities – 0 to 6 Months

→ Conduct a formal CRA applicability and product classification assessment
→ Establish cybersecurity governance ownership and executive accountability
→ Evaluate current secure development practices against CRA Annex I requirements
→ Assess vulnerability management maturity and PSIRT readiness
→ Initiate SBOM tooling evaluation and proof–of–concept implementation
→ Review incident response readiness against CRA reporting requirements
→ Map regulatory overlaps with NIS2, GDPR, and sector–specific obligations

Medium–Term Priorities – 6 to 18 Months

→ Implement DevSecOps practices including SAST, DAST, and SCA tooling
→ Establish and operationalise a formal PSIRT function
→ Deploy SBOM generation, maintenance, and vulnerability correlation workflows
→ Strengthen supply chain security assessments for critical third–party components
→ Formalise compliance governance, documentation, and audit readiness
→ Prepare technical documentation and conformity assessment evidence packages
→ For Class II products: engage a Notified Body and begin pre–assessment

Long–Term Priorities – 18+ Months

→ Establish continuous compliance monitoring and executive dashboards
→ Integrate security into product lifecycle governance
→ Complete CE marking and Declaration of Conformity submission
→ Conduct full compliance validation against all CRA Annex I requirements
→ Build ongoing cybersecurity resilience maturity across all product lines

10. Conclusion

> ***The CRA represents a structural shift in how cybersecurity accountability will be measured across the European digital economy.***

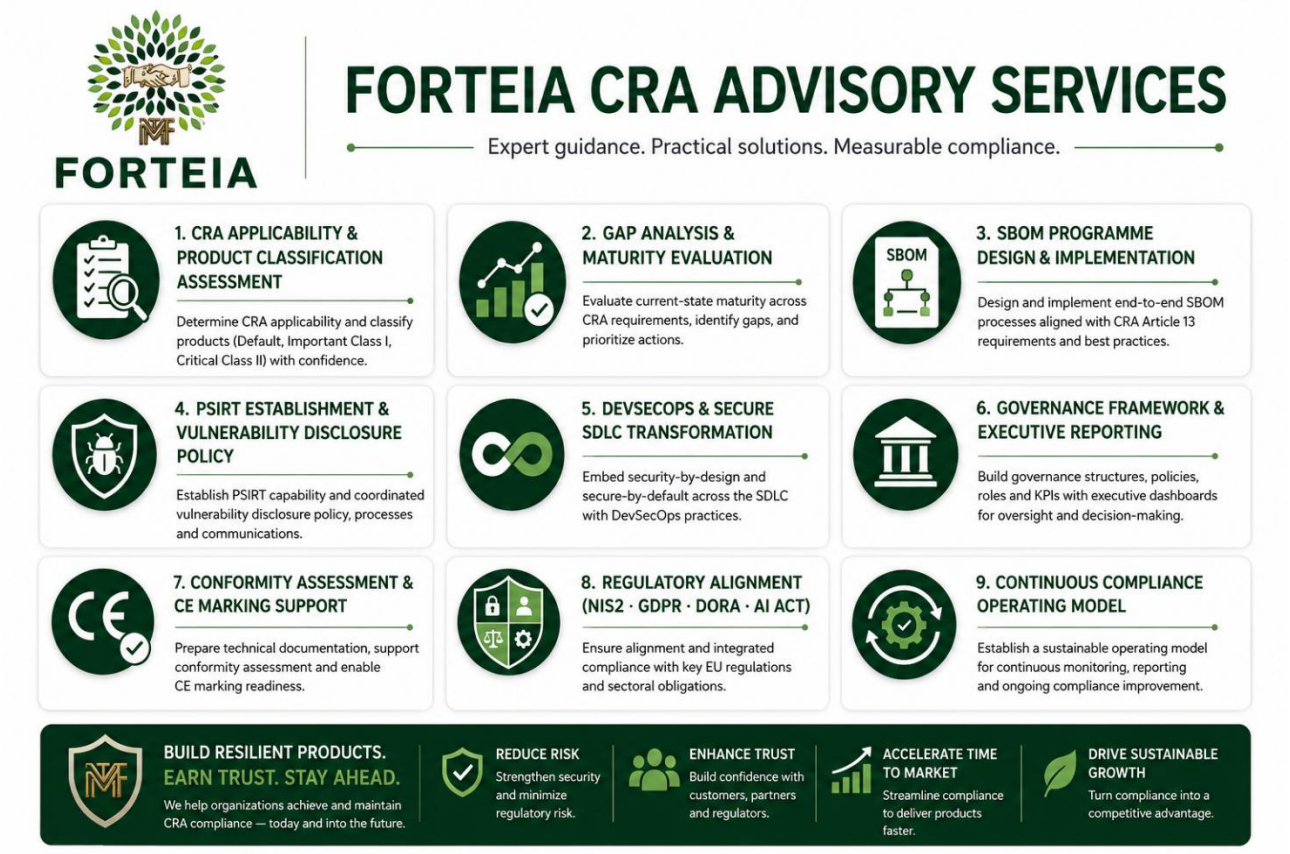
The Cyber Resilience Act is the most significant evolution in European product cybersecurity regulation to date. Vulnerability exploitation as a breach vector grew 34% in a single year, while third–party involvement in breaches doubled (Verizon DBIR 2025). Edge devices went from 3% to 22% of all breach starting points.

The average cost of a breach now sits at USD 4.44 million globally, with U.S. organisations averaging USD 10.22 million as enforcement intensifies. And against this backdrop, only 12.3% of EU SMEs surveyed in 2024 were familiar with the regulation about to govern them.

The 11 September 2026 vulnerability reporting deadline effectively mandates SBOM and monitoring readiness 12 to 15 months before the headline December 2027 full compliance date. Organisations that wait until 2027 will already be late.

Those who treat the CRA as an opportunity tend to emerge with stronger products, greater customer trust, and more resilient operations. In practice, the differentiator is rarely budget alone – it is institutional prioritisation, operational discipline, and executive ownership.

Practical implementation, executive alignment, and sustainable governance are the critical success factors. FORTEIA stands ready to support organisations through every phase of that journey.



Cheat Sheet: Key Points on the EU Cyber Resilience Act

Topic	Key Point
Regulation	Regulation (EU) 2024/2847 – directly applicable in all 27 Member States. No national transposition required.
Entry into Force	10 December 2024 – the 36–month implementation clock began.
Reporting Deadline	11 September 2026 – 24-hour early-warning notification obligations for actively exploited vulnerabilities (all products, including legacy).
Full Compliance	11 December 2027 – all obligations apply: CE marking, SBOM, secure–by–design, conformity assessment.
Who Is In Scope	Any manufacturer, importer, or distributor placing products with digital elements on the EU market – regardless of HQ location.
Product Categories	Default (self-assessment) · Important Class I – Annex III (self-assessment if harmonised standards applied, otherwise third-party) · Important Class II – Annex III (mandatory third-party) · Critical – Annex IV (third-party, with possible mandatory EU cybersecurity certification).
Penalties	Up to €15M or 2.5% of global annual turnover – whichever is higher. Products can be banned from EU market.
SBOM	Machine–readable SBOM required. Must be retained for 10 years after market placement.
Security Updates	Free of charge over the declared support period (generally minimum 5 years). Cannot be paywalled.
Technical Documentation	Must include risk assessment, SBOM, test results, vulnerability process, Declaration of Conformity. Retained 10 years.
CE Marking	Required for all in–scope products. Affixed only after successful conformity assessment.
Open Source	OSS without commercial intent is exempt. Manufacturers integrating OSS commercially bear full CRA obligations.
NIS2 / DORA Overlap	Incident reporting workflows, risk management controls and governance models can be extended across both.
First Step	Conduct a formal CRA applicability and product classification assessment before committing resources to remediation.

Sources & References

All claims in this whitepaper are anchored to authoritative public sources. FORTEIA cites only primary or institutional sources. Every URL was validated in May 2026.

Primary EU & Institutional Sources

1	Regulation (EU) 2024/2847 – Cyber Resilience Act. European Parliament & Council, 23 October 2024. https://eur–lex.europa.eu/eli/reg/2024/2847/oj
2	European Commission – Cyber Resilience Act (official policy portal). https://digital–strategy.ec.europa.eu/en/policies/cyber–resilience–act
3	Commission Implementing Regulation (EU) 2025/2392, adopted 28 November 2025. https://eur–lex.europa.eu/eli/reg_impl/2025/2392/oj
4	ENISA & JRC – CRA Requirements Standards Mapping. April 2024 (JRC137340). https://www.enisa.europa.eu/publications/cyber–resilience–act–requirements–standards–mapping
5	ENISA – Threat Landscape 2025. October 2025. 4,875 incidents analysed. https://www.enisa.europa.eu/publications/enisa–threat–landscape–2025
6	IBM Security & Ponemon Institute – Cost of a Data Breach Report 2025. 600 organisations. Global avg: USD 4.44M. https://www.ibm.com/reports/data–breach
7	Verizon Business – 2025 Data Breach Investigations Report. 22,052 incidents; 12,195 breaches; 139 countries. https://www.verizon.com/business/resources/reports/dbir/
8	IoT Analytics – State of IoT 2025. 18.5 billion connected devices in 2024; 39 billion forecast by 2030. https://iot–analytics.com/number–connected–iot–devices/
9	Mauri, L. et al. (2024) – "Ensuring Cybersecurity Compliance: Assessing SME Awareness and Preparedness for the CRA." 416 European SMEs.
10	ISO/IEC 27001:2022 – Information security management systems. | ISO 18974 – OSS security. | ISA/IEC 62443 – ICS security.

Legal Disclaimer: This document is provided for informational purposes only and does not constitute legal advice, regulatory certification, or formal conformity assessment guidance. Organisations should seek independent legal, regulatory, and technical advice specific to their products, sectors, and jurisdictions. FORTEIA does not act as a Notified Body, certification authority, or legal representative under the CRA.

This page intentionally left blank.

About FORTEIA

Who We Are

FORTEIA is a cybersecurity, governance, privacy, AI security, and digital trust advisory organization helping enterprises strengthen resilience, manage regulatory obligations, and operationalize security across modern digital ecosystems. We support organisations in aligning cybersecurity strategy, governance, compliance, and engineering practices with evolving global regulatory frameworks including the EU Cyber Resilience Act (CRA), NIS2, DORA, GDPR, and AI governance requirements.

Vision

To enable trusted, resilient, and secure digital ecosystems through governance, cybersecurity, and operational excellence.

Mission

To help organisations operationalise cybersecurity, governance, privacy, and AI trust through practical, measurable, and business-aligned advisory services.

Core Capabilities

FORTEIA delivers advisory and operational cybersecurity capabilities across governance, resilience, engineering security, regulatory readiness, and digital trust domains.

- Cybersecurity & Resilience Advisory
- Governance, Risk & Compliance (GRC)
- EU CRA, NIS2 & DORA Readiness
- Privacy & Data Protection Governance
- AI Security & AI Governance
- Secure SDLC & DevSecOps Advisory
- Vulnerability Management & PSIRT
- Supply Chain & Third-Party Risk
- Security Architecture & Assessments
- Executive Cybersecurity Strategy

Contact & Engagement

Website: www.forteia.com

Email: engage@forteia.com

Global Presence: Europe (France, Belgium) · India (Pune, Mumbai) · www.forteia.com