resillion

GOVERNANCE, RISK AND COMPLIANCE

Cyber Resilience Act

Helping manufacturers prepare for the EU Cyber Resilience Act – through advisory, implementation, assurance and monitoring services.

Cyber Resilience Act services

Resillion helps customers prepare for the Cyber Resilience Act (CRA) through advisory, implementation, assurance, compliance and monitoring services. Our services cover product security, secure development, software composition analyses, vulnerability handling and compliance documentation. We can recommend suitable tools while remaining agnostic as to the final choice of tooling.

CRA TIMELINE

Dec 2024
Entered into force

11 Sep 2026
Reporting obligations start to apply

11 Dec 2027
Main obligations apply

What is covered by the CRA?

The CRA applies to products with digital elements — such as embedded software, mobile apps and connected services — placed on the EU market, and introduces lifecycle obligations across secure design, development, vulnerability handling, security updates, user information and technical documentation. It creates significant requirements for manufacturers and can materially affect market access, product governance and regulatory exposure, including substantial penalties for non-compliance.

Turning legal obligations into an operating model

For many manufacturers, the initial challenge is translating legal obligations into practical operational capabilities that can be sustained throughout the product lifecycle. The regulation introduces broad requirements, but many organisations don't yet have full visibility of their product estate, software supply chain, support periods and internal accountabilities in a form that supports compliance.

In practice, it's often tedious or complex to identify all software and third-party components, maintain evidence of product support commitments, run consistent secure development and vulnerability handling and post-market security processes, and maintain the documentation, patch governance and cross-functional coordination needed across product, engineering, security and compliance.

Without a systematic governance framework, clearly defined operational processes and appropriate automated tooling, these activities quickly become manual, fragmented and hard to sustain at scale, making it difficult to maintain accurate evidence, respond efficiently to vulnerabilities and demonstrate ongoing conformity with confidence.

The post-market obligations introduced by CRA can be particularly challenging because they are event-driven rather than project-driven. Manufacturers may need to rapidly triage vulnerability reports, distinguish routine vulnerabilities from potentially reportable events, gather sufficient technical evidence to determine when regulatory reporting obligations are triggered, and coordinate specialist technical and regulatory activities within demanding reporting timeframes.

Maintaining these capabilities internally can be disproportionate for many organisations, particularly where vulnerability reports occur unpredictably and specialist expertise is only required intermittently.

Limited estate visibility

Products, components and support periods aren't mapped in a compliance-ready form.

Complex supply chains

Third-party and open-source components are hard to identify and track over time.

Evidence and documentation

Maintaining accurate, current conformity evidence becomes manual and fragmented.

Event-driven reporting

Unpredictable vulnerability reports must be triaged within demanding timeframes.

Tailored, phased and built for sustainable ownership

We provide tailored services aligned to your business objectives and regulatory requirements, helping your teams build the internal capability and sustainable ownership needed for ongoing CRA compliance.

Our services can be delivered in phased packages, so you can increase or reduce assurance and monitoring support after implementation according to your internal capacity, business priorities and speed-to-market requirements.

FIVE SERVICE AREAS

1 Advisory
Classification, risk and gap assessment, governance and secure-by-design architecture.

2 Implementation
SBOM deployment, secure SDLC, vulnerability management, conformity documentation and training.

3 Assurance
Security assessment, fuzz testing, code assurance and independent readiness review.

4 Compliance
Compliance assessment and supplier assurance across your software supply chain.

5 Monitoring
CVD operations, regulatory reporting, managed vulnerability operations and patch governance.

01 Advisory

Product classification

Determine whether your product falls within the CRA, how it should be classified and which conformity assessment route applies. Our experts provide a clear classification rationale, helping you avoid unnecessary compliance activity and plan the appropriate route to market.

Product cyber security risk assessment

Understand the cyber security risks that matter most to your product and your route to compliance. Our experts perform a structured CRA-aligned risk assessment, considering intended and reasonably foreseeable use, product architecture, threat landscape and lifecycle obligations to help you prioritise investment, justify security decisions and build a stronger foundation for conformity.

Gap assessment

The assessment considers the product, supporting processes and available evidence across the full product lifecycle, including secure development, vulnerability handling, software supply-chain management, support-period obligations, technical documentation and conformity readiness. Beyond identifying compliance gaps, we help manufacturers make pragmatic decisions around legacy products, support commitments and engineering operating models, enabling sustainable compliance while minimising business disruption and implementation effort.

Governance framework

Establish clear ownership and effective decision-making for CRA compliance by building on your existing operating model. We help optimise governance arrangements, clarify roles and responsibilities, and integrate CRA obligations into existing management systems, engineering processes and organisational structures, leveraging recognised frameworks such as ISO 27001 and IEC/ISA 62443 where appropriate.

Secure-by-design product architecture

Embed cyber security into your product architecture before weaknesses become costly redesigns or barriers to market access. Our experts identify practical architectural improvements that reduce attack exposure, strengthen assurance and support your CRA conformity case.

TYPICAL OUTPUTS

Clear, risk-prioritised roadmap showing what needs to be done, why it matters and where to begin. It brings together classification, risk, compliance gaps, governance and product architecture into an actionable programme aligned with your regulatory deadlines and business priorities.

02 Implementation

Software Bill of Materials (SBOM) deployment

Automate software component inventory management and gain continuous visibility of your software supply chain. We implement practical SBOM generation, software composition analysis capabilities and supporting operational processes that improve vulnerability response, reduce manual effort and support ongoing CRA compliance.

Secure Software Development Life Cycle (S-SDLC) / DevSecOps process review and optimisation

Strengthen product security by embedding CRA security practices into your existing engineering lifecycle without slowing product delivery. We optimise Secure SDLC and DevSecOps processes by integrating security, vulnerability management, documentation and governance activities into established engineering workflows, improving software quality, reducing security risk and supporting sustainable CRA compliance.

Vulnerability management

Build a sustainable vulnerability management capability that enables your organisation to receive, assess, prioritise, remediate and disclose vulnerabilities confidently. We implement practical processes for vulnerability handling, coordinated disclosure, security update governance and regulatory reporting, helping manufacturers meet CRA post-market obligations while integrating these activities into normal business operations.

Conformity documentation

Develop complete, audit-ready documentation and governance evidence that demonstrates CRA conformity and supports efficient conformity assessment. We help integrate documentation, evidence management and governance activities into your existing engineering and management processes, reducing manual effort and simplifying ongoing compliance.

Secure development training

Equip engineering teams with the practical skills and secure development behaviours needed to embed security into everyday engineering practice. Our role-based training helps teams build more resilient products, reduce avoidable vulnerabilities and support sustainable CRA compliance throughout the software lifecycle.

TYPICAL OUTPUTS

A fully operational cybersecurity capability that embeds secure engineering, software supply-chain governance and vulnerability management into day-to-day product development—enabling teams to confidently maintain CRA compliance long after implementation.

03 Assurance

Security assessment

Gain independent assurance that your product is secure and resilient. We combine architecture review, threat analysis, security testing and feature-level validation to identify security weaknesses, verify the effectiveness of security controls and provide practical recommendations before your product reaches the market.

Fuzz testing

Discover vulnerabilities that conventional testing may never reveal. Combining Resillion's independent security expertise, proven fuzz testing methodologies and CRACY-funded specialist tooling, we uncover hidden software defects, unexpected behaviours and robustness weaknesses that strengthen product resilience and provide independent assurance of product security.

Code assurance

Go beyond automated code analysis with independent expert source code review. We identify implementation weaknesses, insecure coding practices and recurring vulnerability patterns that automated tools can miss, providing practical remediation guidance to improve software quality, security and long-term maintainability.

Conformity assessment support

Validate your readiness before declaring conformity. Our independent readiness review provides objective assurance that your product security evidence, technical documentation and supporting processes are sufficiently robust for Module A self-assessment, while highlighting practical improvements before declaration of conformity and CE marking.

Readiness review / internal audit support

Obtain an independent view of your organisation's CRA readiness. We review your governance, operational controls, engineering processes and product assurance activities, providing practical recommendations together with an independent assurance report suitable for management review, internal audit and continual improvement.

TYPICAL OUTPUTS

Independent assurance report that gives management confidence in product security, engineering quality and CRA readiness. The report highlights strengths, identifies residual risks and provides practical recommendations before market declaration or external assessment.

04 Compliance

Compliance assessment

Understand where you stand before declaring conformity. We assess your product, technical documentation and supporting evidence against applicable CRA requirements, identifying regulatory gaps and providing practical recommendations that strengthen your conformity evidence and support confident declaration.

Supplier assurance

Strengthen confidence across your software supply chain. We independently assess suppliers and third parties to identify security, operational and regulatory risks that could affect product conformity, enabling more informed supplier decisions and stronger supply-chain governance.

TYPICAL OUTPUTS

A consolidated view of conformity against applicable CRA requirements, covering product, technical documentation and supporting evidence, together with a supplier and third-party risk picture and prioritised recommendations to strengthen your conformity evidence before declaration.

05 Monitoring

Coordinated Vulnerability Disclosure (CVD) operations

Respond to reported vulnerabilities with confidence. We provide time-critical vulnerability triage, technical assessment and coordinated disclosure support to help you validate reported vulnerabilities, prioritise remediation and determine whether CRA post-market reporting obligations are triggered.

CRA regulatory reporting support

Meet CRA regulatory reporting obligations with confidence. We help you determine when regulatory reporting is required, coordinate the collection and validation of supporting evidence, and prepare professional submissions that meet CRA reporting deadlines and regulatory expectations.

Managed vulnerability operations

Extend your security team with continuous vulnerability management. We manage identified vulnerabilities throughout their lifecycle, from intake and risk assessment through remediation tracking and closure, helping you maintain audit-ready evidence and demonstrate effective post-market vulnerability management under the CRA.

Managed security operations

Identify security incidents before they become regulatory issues. Combining continuous security monitoring, threat detection and incident response with vulnerability operations, we help uncover emerging security events, investigate potential exploitation and respond rapidly to reduce business risk and support ongoing CRA compliance.

Patch governance

Turn security fixes into demonstrable compliance. We govern patch development, validation, release and deployment, helping ensure corrective measures are prioritised, fully traceable and supported by the evidence needed to demonstrate effective post-market compliance under the CRA.

TYPICAL OUTPUTS

Maintain continuous oversight of your post-market cyber security obligations. Our monitoring services provide ongoing visibility of vulnerabilities, emerging threats, regulatory reporting activities and remediation progress, helping you sustain CRA compliance through auditable operational evidence and effective corrective measures throughout the product lifecycle.

WHY RESILLION

Strategy and hands-on delivery, from one partner

It's uncommon to find a partner that combines strategic advisory and governance capability with deep technical implementation and assurance expertise. Resillion brings these together through a Total Quality approach, helping manufacturers meet both business and compliance needs in highly regulated industries.

We support customers from CRA interpretation and governance design through to practical implementation, independent assurance and ongoing operational support, combining GRC expertise with hands-on cyber security, software quality and testing capability.

- Advisory and governance
- Technical implementation
- Independent assurance

GLOBAL PRESENCE

EU · UK · US · India · China

READY TO START?

Get in touch with our GRC experts today

Contact us →

resillion

www.resillion.com