Cyber Resilience Act Requirements Checklist

1 Identify what's in scope

Understanding whether the CRA applies to your products is the first and most crucial step.

- [ ] Create a complete inventory of all products with digital components like hardware, software, IoT, firmware, or any device connected to a network
- [ ] Determine your company's role: manufacturer, importer, distributor, or software developer. Each has specific legal obligations under the CRA
- [ ] Identify indirect exposure, like your suppliers, third-party vendors, or customers, that might bring CRA responsibilities into your ecosystem
- [ ] Map your product dependencies, including open-source libraries, third-party APIs, and embedded firmware, to ensure you can trace security accountability end to end

2 Build security into design

The CRA emphasizes prevention over reaction. Products must be built securely from day one.

- [ ] Integrate cybersecurity risk analysis into your design phase rather than as a final-stage CRA compliance checklist

- [ ] Define clear security objectives per product, covering confidentiality, integrity, availability, and resilience
- [ ] Adopt and enforce secure coding practices, regular peer reviews, and static code analysis
- [ ] Remove unnecessary features, default passwords, and excessive permissions before product release
- [ ] Ensure your update mechanisms are protected from tampering and can be applied automatically or easily by users

3 Risk & vulnerability handling requirements

Continuous risk management is at the heart of CRA compliance.

- [ ] Establish a structured, ongoing process to identify, assess, and mitigate vulnerabilities
- [ ] Conduct threat modeling to understand how your product could be targeted and what impact exploitation might have
- [ ] Perform scheduled penetration tests and security scans across all versions
- [ ] Manage supply chain risk by assessing and monitoring your third-party software and hardware components
- [ ] Maintain a documented vulnerability disclosure process, both internal (for staff) and external (for customers and researchers)
- [ ] Keep detailed logs of identified risks, mitigations, and patch history for CRA audit readiness

- [ ] Define clear security objectives per product, covering confidentiality, integrity, availability, and resilience
- [ ] Adopt and enforce secure coding practices, regular peer reviews, and static code analysis
- [ ] Remove unnecessary features, default passwords, and excessive permissions before product release
- [ ] Ensure your update mechanisms are protected from tampering and can be applied automatically or easily by users

4 CRA technical documentation & transparency

If it's not documented, it doesn't exist. Especially in compliance.

- [ ] Maintain a technical security file for every product. Include architectural diagrams, security testing results, and patch management records
- [ ] Prepare clear, user-facing documentation that explains how to configure, maintain, and update products securely
- [ ] Define standardized procedures for vulnerability reporting and incident escalation
- [ ] Ensure all records, be it technical, procedural, or communication, are version-controlled, time-stamped, and accessible to compliance reviewers

5 Incident & reporting readiness

The CRA introduces strict timelines for reporting cybersecurity issues. Preparation is key.

- [ ] Develop a comprehensive incident response plan covering detection, containment, and reporting workflows
- [ ] Assign clear ownership: who investigates, who communicates, and who reports to authorities
- [ ] Be ready to notify the EU's cybersecurity agency (ENISA) within the legally required timeline (currently 24 hours for initial notification) if an exploited vulnerability or active incident is discovered
- [ ] Test your response process through tabletop simulations or red-team exercises at least annually
- [ ] Integrate your response process with your communication plan to ensure customers and partners are informed responsibly

6 Lifecycle security

Cyber resilience doesn't end at product launch. It extends through the entire lifespan of your product.

- [ ] Plan long-term security maintenance for each product, including patch delivery mechanisms and update frequency
- [ ] Define and communicate end-of-life (EOL) policies on how long users will receive updates and what happens after support ends
- [ ] Regularly review your lifecycle policies in response to emerging threats or updated EU guidance

- [ ] Use telemetry and feedback loops to learn from field data and improve future versions.

7 CRA Compliance Governance

Compliance is not a single team's responsibility. It's a company-wide mindset.

- [ ] Appoint a CRA compliance lead or cross-functional working group to oversee implementation
- [ ] Align internal policies such as data protection, incident management, and product development with CRA requirements
- [ ] Monitor EU updates, harmonized standards, and technical guidance as they evolve
- [ ] Schedule periodic internal audits and, when appropriate, collaborate with independent security assessors to verify compliance posture
- [ ] Train all relevant employees, namely developers, product managers, and customer support, on their CRA-related roles.

How to Adopt a Continuous CRA-Ready Workflow?

The EU CRA is built on a clear expectation: security must be continuous, measurable, and embedded across the entire product lifecycle. Meeting that bar means adopting tools and processes that provide continuous visibility, ongoing testing, and defensible CRA audit evidence of security decisions... not just annual reports.

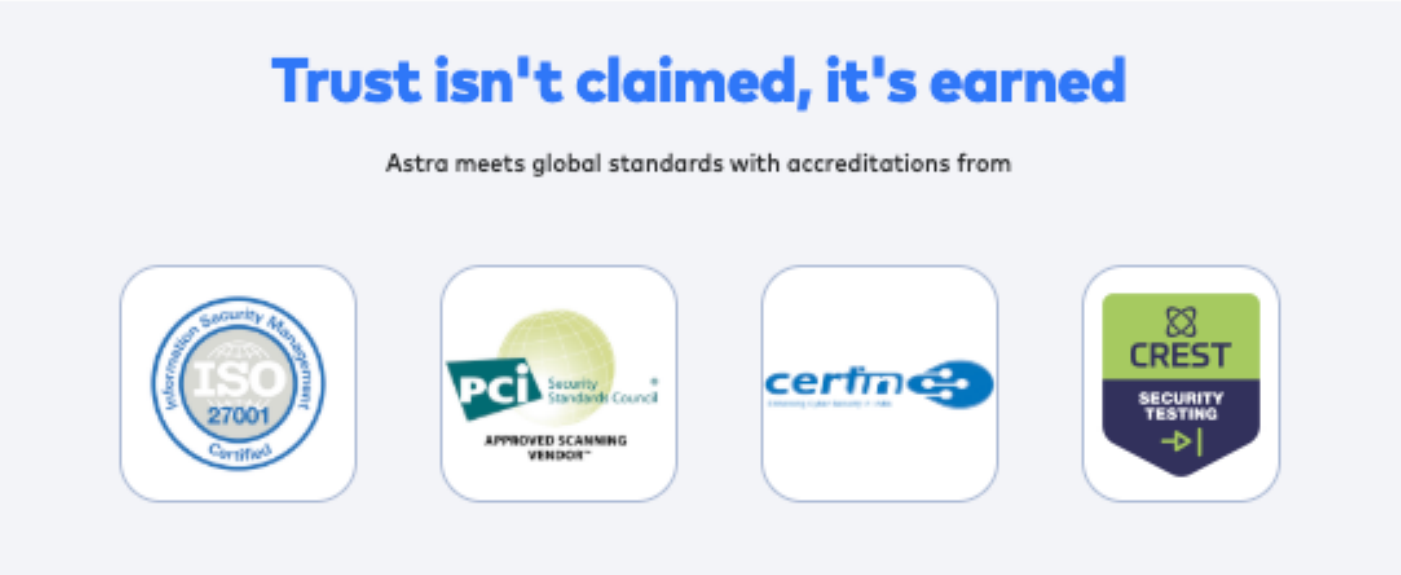
Platforms built around continuous security make this shift far more practical. They centralize testing, validation, and compliance evidence so teams can align with CRA expectations without adding unnecessary overhead. Astra Security is designed with that exact workflow in mind, helping you operationalize CRA requirements across development, testing, and audits. We help you achieve that level of assurance and clearly show it.

Continuous Vulnerability Scanning

From APIs and web apps to cloud infrastructure, Astra Security gives you one place to see and secure everything. In just 30 minutes, you will have a live inventory of your digital assets and vulnerabilities, verified by our in-house experts to ensure no false positives.

Compliance mapping

Every pentest mixes AI-driven automation with manual testing by certified experts (OSCP, CEH, eWPTXv2) with 90+ CVEs to their name and counting. Each finding is linked to compliance frameworks such as ISO 27001, SOC 2, PCI DSS, and GDPR, helping you demonstrate your due diligence rather than just assert it.

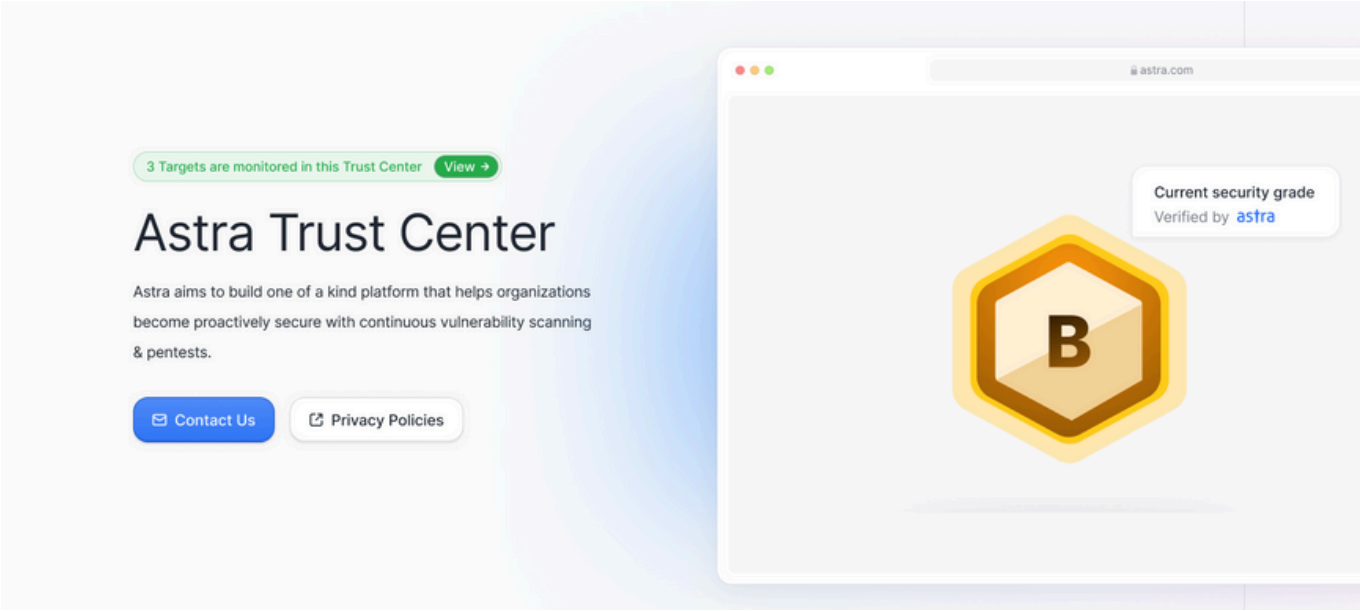


DevOps readiness

Astra Security's PTaaS platform plugs directly into your CI/CD pipelines (GitHub, GitLab, Jenkins, Bitbucket, Azure, and more) to make vulnerability checks part of your build process, not an afterthought. Every code push can trigger a new scan, giving teams a chance to pinpoint & fix issues before they go live.

Proof of trust

Our Trust Center turns your continuous testing data into living documentation. It surfaces your security status, fix history, and CRA-style traceability at any time, ensuring you are ready for audits (by disciplinarian auditors and cautious customers) without scrambling for reports.



AI that thinks like an attacker

At the core of Astra Security is the Attack AI engine, a system designed to mimic real adversaries, connect risks across APIs, apps, and cloud environments, and find vulnerabilities that static scanners overlook. It adapts with your environment, helping you stay ahead of both human and AI-driven threats.

In short, Astra gives you what the CRA expects: secure-by-design foundations, continuous validation, and proof of resilience over time. Turn security from an annual task into a steady practice your team can maintain.

Meet EU CRA Compliance with Astra Security

The EU Cyber Resilience Act (CRA), in the simplest words, is a response to an entire digital ecosystem built on the assumption that “we’ll fix it later” is a sustainable security strategy. All it achieved was far too many digital products shipped with security holes you could drive a mid-size compliance audit through, and in too many cases, products that ultimately had to be pulled from the market for flaws that never should have shipped in the first place.

The National Vulnerability Database recorded 28,831 new vulnerabilities in 2023, which is more than 25,081 recorded the year before. The sheer volume shows how many more potential weak points are out there.

As of 2025, the CRA has been adopted and is in its implementation phase, giving companies a transition window before the bulk of requirements become enforceable in 2027. Its scope is intentionally broad: software, hardware, and anything that connects to and exchanges data online. If your product touches a network, the CRA almost certainly applies to you.

At its core, the Cyber Resilience Act requirements give manufacturers clear responsibilities: design with security built in, test after release, respond to issues, and keep supporting the product through its lifecycle.