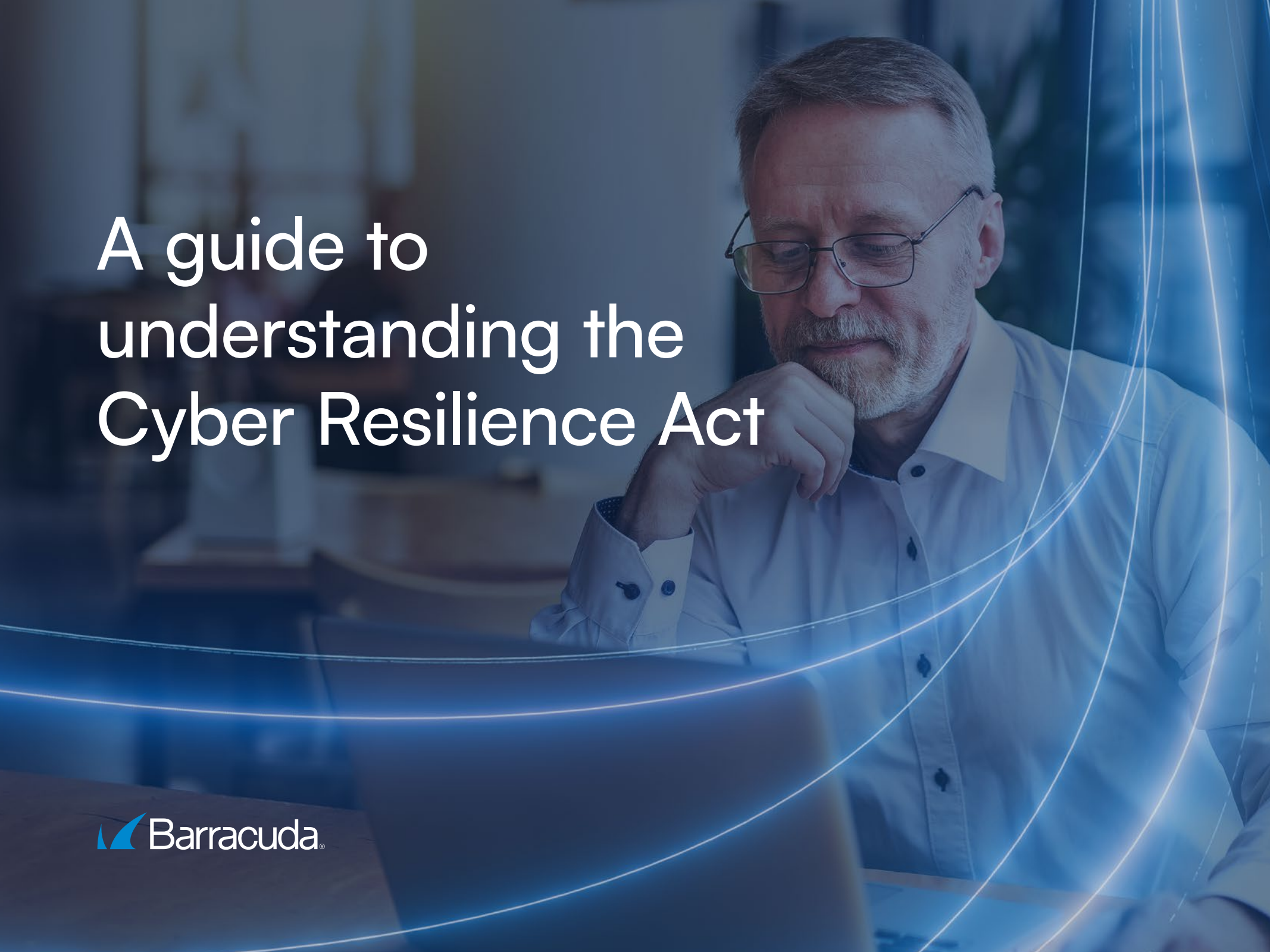

A guide to understanding the Cyber Resilience Act

Barracuda

Understanding the European Union's (EU) Cyber Resilience Act (CRA) is essential for organisations that do business in the EU. Manufacturers of digital products offered for sale in the EU and the importers and distributors of those products are subject to the CRA. This e-book provides some CRA highlights for manufacturers but is not a substitute for and is not intended to be legal advice for your company.

The CRA went into force in December of 2024, allowing organisations some time to achieve compliance. Here are some key dates to know:

- 11 September 2026 — Manufacturers must begin reporting severe cybersecurity incidents and actively exploited vulnerabilities.
- 11 December 2027 — All net-new products and any "substantially modified" existing products placed on the market on or after this date must comply with the CRA.

The law is intended to provide a more uniform set of security requirements across all products with digital elements sold in the EU and to provide consumers and businesses buying these products with more information about their security before they buy them. The act hopes to rectify what the EU describes as the "inadequate level" of cybersecurity found in many products, including a lack of security updates.

The CRA complements the Digital Operational Resilience Act (DORA) and the Network Information Security 2 Directive (NIS2):

- DORA is focused on improving the cyber resilience of the financial industry, and NIS2 applies to a broader set of entities that provide essential services in key sectors.
- Both DORA and NIS2 specify cybersecurity requirements, including supply chain security measures, with a view to increasing the resilience of the regulated companies, due to the impact their offerings have for other people.
- The CRA applies at the product level, providing the mandatory framework for secure products with digital elements. Where the customer of such products is regulated by DORA or NIS2, using CRA-compliant hardware and software can help these entities comply with their obligations.

NIS2 and DORA are outside the scope of this e-book. Please see Understanding DORA: A Guide to Digital Operational Resilience Act and Navigating NIS2: A guide to the upcoming European cybersecurity regulations for more details.

Why is the CRA important?

The CRA covers all products containing "digital elements," meaning that this regulation covers both hardware and software that is connected to a device or network, plus such products' integrated remote data processing solutions (i.e., cloud services). The European Commission says, "The regulation applies to all products connected directly or indirectly to another device or network except for specified exclusions such as certain open-source software or services products that are already covered by existing rules, which is the case for medical devices, aviation, and cars."[1] Non-compliant products will not be allowed to be sold in the EU. Organisations caught doing so will be subject to fines. Just as the General Data Protection Regulation (GDPR) fundamentally changed how companies handle personal information, the CRA has the potential to have a similar effect on how manufacturers make, sell and support their products with digital elements offered on the market in the EU.

The CRA addresses a growing issue with modern technology products that collect, process, share and store user data — often with either no security or weak security — putting that data at risk. As these products age, available security solutions can become outdated. There is little oversight on how, when or if security updates are provided to users. The CRA seeks to increase the security of products with digital elements and ensure that those products remain secure throughout their lifecycle. The act will also provide greater transparency to users, who will have a better understanding of the security of products with digital elements and how that could affect their data.

[1] Cyber Resilience Act | Shaping Europe's digital future

CRA obligations for manufacturers

The CRA introduces mandatory cybersecurity requirements for manufacturers that govern the planning, design, development, production, delivery, documentation and maintenance of such products. These obligations must be met at every stage of the value chain.

Under the CRA, products can be classified as standard (lowest level), “Important” (with more obligations) — which is divided into two subcategories, Important Class I and Important Class II — and “Critical” (with highest level of risk and thus obligations).

For standard items, manufacturers are required to design, manufacture and test goods and services for compliance with the “essential security requirements” specified in Annex I of the CRA, document the assessment and keep the technical documentation available for market surveillance authorities. At this level, manufacturers may rely on an internal conformity assessment (self-assessment).

Generally speaking, about 90% of hardware and software products are expected to fall into this standard category, allowing manufacturers to self-test and create a declaration of conformity before affixing the CE mark that compliant products will receive.

Certain products with digital elements — such as web browsers, firewalls and operating systems — fall into the “Important” category, others even in the “Critical” category. They must still comply with the Annex I technical requirements but may be subject to a more stringent conformity assessment process, including third-party assessment/certification before they are sold in the EU.

In addition to obligations at the time of sale, the CRA also requires manufacturers to provide vulnerability management and security patching as described below.

Barracuda

Security reporting obligations

Actively exploited security vulnerabilities and severe incident reporting under the CRA goes into force on 11 September 2026.

The reporting obligations are stringent. Manufacturers will need to provide an “early warning” notice to regulators within 24 hours of becoming aware of the matter. Within 72 hours of becoming aware of an exploited vulnerability, manufacturers will need to provide general information about the affected product, a general description of the exploited vulnerability and any mitigation action that the manufacturer has taken and that users can take, as well as indicate the sensitivity of the issue. Within 14 days after the mitigating steps are available, the manufacturer has further disclosure obligations in the sense of a final report.

Reporting obligations also include informing affected users and advising them on ways to mitigate exposure.

Manufacturers should become familiar with these reporting requirements and develop processes to comply by the September 2026 start date.

Barracuda

Technical support obligations

Cybersecurity support in the sense of providing security updates is also an important topic in the CRA and must be planned to address the entire product lifecycle. Manufacturers must specify the support period upfront for products with digital elements. In general, companies that place products with digital elements on the market in the EU must support them for at least five years unless the expected lifetime of the product is less than five years, and in that case, the support must last for the expected life of the product. For products that generally have a life longer than five years (examples: motherboards, network routers, modems, switches and operating systems), the support period should be longer. Security updates made available during the support period must be available to users for the longer of the support periods or 10 years.

How will compliance be enforced?

Non-compliance can result in penalties, both financial — fines of up to €15 million or 2.5% of total global turnover — and non-financial. Regulators could force a company to recall non-compliant products.

Barracuda

Six steps to compliance for manufacturers

Below are basic steps for manufacturers to begin their compliance process to be ready for the CRA when it is fully in effect. The multiple annexes of the CRA provide details on what is expected at each step.

1. Classify products and conduct a cyber risk assessment. Organisations can have products in multiple categories. Therefore, it is important to assess each product to determine which category it falls into — standard, Important or Critical.
2. Prepare technical documentation. Review CRA Annex I and supply chain requirements for all products and identify any gaps. Conduct and document a risk assessment for each product against the applicable criteria and identified suitable standards, common specifications or certification schemes.
3. Determine each product's conformity assessment approach. If necessary, engage a third party for this exercise.
4. Prepare a declaration of conformity in line with Annex V/VI and complete the technical documentation covering the content of Annex VII. Then the manufacturer must apply the CE mark to a compliant product, its packaging or documentation. The CE marking will indicate the conformity of products with digital elements with the CRA, so that they can move freely within the EU.
5. Prepare and provide user information/instructions as per Annex II. Documentation is a crucial part of compliance and its goal of providing transparency to the user.
6. Monitor and handle vulnerabilities. The CRA demands active and ongoing participation from manufacturers during the support coverage period, which includes providing cybersecurity support, monitoring for any vulnerabilities, and reporting and remediation, such as software updates addressing security issues.

Barracuda is actively engaged in confirming its product categories and addressing the next steps. We will provide information on the Trust Center when available.

Barracuda

Important Class I and Important Class II

Important Class I products pose a lower cybersecurity risk than Important Class II products. Manufacturers may choose to self-declare compliance if they comply with certain qualified EU standards/common specifications/certification schemes, provided they are available and applicable to the product. Otherwise, they may require a third-party verification.

Important Class II products are considered to pose a higher level of cybersecurity risk, and certification by an authorised third party is required.

The CRA, DORA and NIS2 together comprise a complex set of cybersecurity regulations for companies doing business in the EU. Your company may be subject to more than one of these regulations. Barracuda's Trust Center contains multiple assets to help customers understand DORA, including our e-book Understanding DORA: A Guide to Digital Operational Resilience Act, and NIS2, including our e-book Navigating NIS2: A guide to the upcoming European cybersecurity regulations, to help companies with their compliance obligations.

About Barracuda

Barracuda is a leading global cybersecurity company providing complete protection against complex threats for all sized businesses. Our AI-powered BarracudaONE platform secures email, data, applications and networks with innovative solutions, managed XDR and a centralized dashboard to maximize protection and strengthen cyber resilience. Trusted by hundreds of thousands of IT professionals and managed service providers worldwide, Barracuda delivers powerful defenses that are easy to buy, deploy and use. For more information, visit barracuda.com.

Barracuda