



8 SEPTEMBER 2025

# Feedback on CRA risk assessment guidance

## Introduction

Risk assessment is foundational within the Cyber Resilience Act (CRA), both as a practice and a deliverable.<sup>1</sup> Risk assessment forms the basis of compliant products and informs the technical information supplied to users. Manufacturers need clear guidance, maintaining proportionality and allowing freedom in their risk assessment practices. In this paper, DIGITALEUROPE outlines suggestions for more clarity in the final guidelines.

## Table of contents

<b>Introduction</b>	<b>1</b>
<b>Table of contents</b>	<b>1</b>
<b>Manufacturer risk assessment</b>	<b>2</b>
<b>Exemptions from essential requirements</b>	<b>2</b>
<b>Applicability</b>	<b>2</b>
<b>Mitigation-based implementation</b>	<b>3</b>
<b>Intended purpose, reasonably foreseeable use and reasonably foreseeable misuse</b>	<b>3</b>
<b>Expected length of time the product will be in use</b>	<b>4</b>
<b>Interplay with risk assessment required by other Union acts</b>	<b>4</b>
<b>Technical documentation</b>	<b>5</b>
<b>Remote data processing solutions</b>	<b>5</b>

---

<sup>1</sup> Regulation (EU) 2024/2847.



## Manufacturer risk assessment

A more precise delineation of the required sections described in Art. 13(2) and an overview of the risk assessment requirements would assist manufacturers in their compliance efforts.

We suggest the following edits in **bold**:

---

“ According to the CRA (article 13) manufacturers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, preventing incidents and minimising their impact, including in relation to the health and safety of users. **The risk assessment shall describe the risk context (including the intended purpose and foreseeable use) and assets to be analysed, threat and risk identification, risk evaluation and risk treatment. The risk assessment must be documented and kept up to date throughout the product’s support period.**

---

**Additionally**, the cybersecurity risk assessment shall indicate whether and, if so in what manner, the security requirements relating to the properties of products (set out in Part I, point (2), of Annex I) are applicable to the relevant product with digital elements, and how those requirements are implemented as informed by the cybersecurity risk assessment.

The risk assessment shall also indicate how the manufacturer has designed, developed and produced the product with digital elements in such a way that they ensure an appropriate level of cybersecurity based on the risks (Part I, point (1), of Annex I) and the vulnerability handling requirements (set out in Part II of Annex I).

---

## Exemptions from essential requirements

As per Art. 13(3) CRA, the cybersecurity risk assessment must indicate: 1) the **applicability** of the security requirements;<sup>2</sup> and 2) how those requirements are to be **implemented**.

Two avenues allow manufacturers an exemption from implementing an essential requirement.

### Applicability

An essential requirement does not apply if the product does not include a function or technical property applicable to the security control. An essential requirement should also not apply where it is incompatible with the product’s nature, its intended use, reasonably foreseeable use or conditions of use, as well as in cases where some requirements are fulfilled by complying with sector-specific legislation.

For example, the guidance states that ‘a product might not need to incorporate any specific mitigation measures related to the protection of personal data if the product does not process this kind of data.’ Conversely, where a product requires a user account to be fully operational and the processing of personal

---

<sup>2</sup> Part I, point (2) of Annex I.



data is undertaken through the product's remote data processing solution, non-personal data minimisation on the hardware might not be applicable.

## Mitigation-based implementation

An exemption on a risk and mitigation basis is less clear. Typically, in the cybersecurity field, achieving a single security objective requires a suite of mechanisms and measures. These must be selected and implemented as informed by the cybersecurity risk assessment, depending on the operational environment and the assets to be protected, and in the most coherent manner.

A product's intended purpose can constrain the risk in the intended operating environment. Hence, the intended operating environment can justify an exemption from implementing certain security requirements.

For example, an Ethernet-connected product expressly intended to operate on a specifically secured internal network may alleviate the need for data encryption in transit on the basis of the risk, because the assessment of the magnitude of a potential loss or disruption and the likelihood of occurrence are acceptable, and therefore encryption is not required.<sup>3</sup> Whilst the stated intended purpose and related risks are clear, the reasonable foreseeable use may envision that certain users may be operating the product on a non-secured network, in the absence of a technical control preventing this use. This foreseeable use could expose the user to adverse effects. Consequently, the mitigation-based approach should exclude prohibited use cases by the manufacturer (misuse).

The guidance should include language consistent with Recital 55, stating that intended purpose constraints take precedence over reasonably foreseeable but prohibited uses, i.e. by the stated intended purpose in the information and instructions to the user. It is necessary to provide greater clarity to manufacturers on how to coherently implement the security requirements relating to the properties of products.


Additionally, the guidance should clarify that when a manufacturer proves that the likelihood or impact of the risk is negligible, as demonstrated in the risk assessment, the product may be exempted from the essential requirement.

Lastly, it is important that the guide on risk assessment explicitly acknowledges the principle of proportionality when interpreting the essential requirements of the CRA. This would be in line with existing guidance from other Union regulatory frameworks (e.g. § 161 of the Guide to the Machinery Regulation). Specifically, we refer to situations where a technical requirement is not per se irrelevant to a product, but where the technical implementation of that requirement would be disproportionate in view of the limited cybersecurity risk identified during the risk assessment. Referencing Recital 55 of the CRA, it is clear that essential requirements apply only when the relevant functionality is present in a product. However, further clarification is needed for cases where a product does include such functionality, but implementing certain mitigation measures would involve excessive costs or complexity relative to the assessed risk.

## Intended purpose, reasonably foreseeable use and reasonably foreseeable misuse

---

<sup>3</sup> Part I, point (2e) of Annex I.



Similar to the previous section, language stating that reasonable intended purpose constraints take precedence over reasonably foreseeable but prohibited use (by the intended use statement) is required.

In addition, ‘technical operations,’ as part of the definition of ‘reasonably foreseeable use,’ can be interpreted in various ways. For instance, it could mean a series of events that would happen independent of human behaviour as a result of reasonably foreseeable usage, stemming from the very nature of how the product was designed by its manufacturer.

The guidance states that ‘[t]his means manufacturers have to look beyond what they consider the intended use of a product and place themselves in the position of the average user of a particular product and envisage in what way they would reasonably consider using the product.’

In the above, ‘average user’ could mean a consumer or professional user depending on the type of product. A tool designed to be used by a professional requires a tech-savvy user or a professional user with technical knowledge, including third parties requesting access pursuant to the Data Act.<sup>4</sup>

This interpretation blurs the boundaries between products that will be used by end users as opposed to those used by technical users. Designing products in this way is not feasible, and this obligation is too broad.

Furthermore, the guidance states that ‘a product can only qualify as of professional nature when only professional users can use it.’ The professional use of a product with digital elements is established through instructions in the materials accompanying the product.<sup>5</sup> Accordingly, if the manufacturer states that a product is for professional use, it should deploy the appropriate risk assessment for this use case, irrespective of whether the product may end up being used as a consumer device, if the product documentation specifies the professional use.

## Expected length of time the product will be in use

The guidance about the life-span exceeding five years should be removed. The CRA requires manufacturers to update the risk assessment during the support period, and any changes in the product’s security environment would be covered in these incremental updates.

Moreover, this is likely to create overly speculative results. Manufacturers cannot fully foresee what technology and risks will exist in five years or beyond. Instead, manufacturers will be simply updating the risk assessment when the risk changes, which the CRA already requires companies to do.

## Interplay with risk assessment required by other Union acts


In addition to the examples given in the draft guidance, complications could arise where sector-specific legislation requires risk assessments. DORA, for instance, requires entities in scope to conduct risk assessments at the level of individual ICT assets.<sup>6</sup> Consequently, a product such as an online banking application might be subject to a number of risk assessments. This is aggravated if remote data processing

---

<sup>4</sup> Regulation (EU) 2023/2854.

<sup>5</sup> By contrast, a sales restriction to ensure only professional users can purchase a product could create antitrust concerns.

<sup>6</sup> Regulation (EU) 2022/2554.



solutions, as defined in the CRA, require mandatory risk assessments for each IT asset in a bank's IT infrastructure.

Manufacturers should therefore retain flexibility in how they structure their risk assessments, provided the CRA's objectives are met.

## Technical documentation

The CRA requires manufacturers to prepare technical documentation and make it available when the product is placed on the market.

The draft guidance adds the phrase 'whatever its geographical origin or location,' which is unnecessary and potentially confusing. The product's origin or geographical location is not material. If this location/origin is material, it should be explained or, preferably, the modifier removed.

## Remote data processing solutions

The CRA does not provide guidance on how manufacturers should conduct risk assessments for remote data processing solutions. Clear and detailed guidance is essential in this area, given the potential complexity and overlaps generated by the CRA rules. We recommend that the Commission develop specific provisions on this point, drawing on DIGITALEUROPE's recent recommendations.<sup>7</sup>

FOR MORE INFORMATION, PLEASE CONTACT:

Sid Hollman

**Policy Manager for Cybersecurity, Digital Infrastructure & Mobility**

[sid.hollman@digitaleurope.org](mailto:sid.hollman@digitaleurope.org) / +32 491 37 28 73

---

Milda Basiulyte

**Senior Executive Director for Digital Policy**

[milda.basiulyte@digitaleurope.org](mailto:milda.basiulyte@digitaleurope.org) / +32 493 89 20 59

---

Alberto Di Felice

**Policy and Legal Counsel**

[alberto.difelice@digitaleurope.org](mailto:alberto.difelice@digitaleurope.org) / +32 471 99 34 25

---

<sup>7</sup> See DIGITALEUROPE, Towards clear guidance for remote data processing solutions under the CRA, available at [https://cdn.digitaleurope.org/uploads/2025/07/Towards-clear-guidance-for-remote-data-processing-under-the-CRA\\_DIGITALEUROPE.pdf](https://cdn.digitaleurope.org/uploads/2025/07/Towards-clear-guidance-for-remote-data-processing-under-the-CRA_DIGITALEUROPE.pdf).





## About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes corporations which are global leaders in their field of activity, as well as national trade associations from across Europe.

### DIGITALEUROPE

Rue de la Science, 37, B-1040 Brussels  
+32 2 609 53 10 ► [Info@digitaleurope.org](mailto:Info@digitaleurope.org)  
► [www.digitaleurope.org](http://www.digitaleurope.org)

EU Transparency Register: 64270747023-20

