Eight questions for your suppliers

Send these to every supplier of connected devices or software you resell or import, before the EU's Cyber Resilience Act applies in full. Send it as it stands. The order is the one that reveals readiness fastest.

The regulatory facts behind this checklist are printed at the end, each with its source: `cra.full_application`, `cra.importers_distributors`, `cra.importer_distributor_as_manufacturer`, `cra.declaration_of_conformity`, `cra.technical_documentation`, `cra.sbom`, `cra.support_period`, `cra.report_clocks`. No date or reference is typed into this document by hand.

How to use it

1. Send the eight questions to each supplier, with a date for the reply.
2. Score each answer: evidence received, promised with a date, or nothing.
3. Suppliers with nothing and no date on questions 1, 3 and 5 are the ones who will block your sales first. Start there.
4. If you sell a supplier's product under your own name, or you modify it, you count as the maker. Answer the questions yourself.

The eight questions

1. The signed declaration

Ask for: a draft EU declaration of conformity for each product, or the date one will exist, and who will sign it.

Good answer: a draft naming the product, the versions, the requirements it addresses and who checks the work, with a named signatory.

Warning sign: "we will look into it", or a company certificate such as ISO 27001 offered instead of a declaration for the product.

2. The paperwork

Ask for: confirmation that the technical documentation exists for the product, follows the structure the law requires, and can be produced for you or for an authority on request.

Good answer: a contents page with the state of each section and when it was last updated.

Warning sign: a marketing datasheet offered as the documentation.

3. The list of what is inside the product

Ask for: a machine-readable list of the software components in the current release of each product — the trade calls it a software bill of materials — and confirmation that one is produced for every release.

Good answer: a file produced by their build system, with component versions, sent within days.

Warning sign: a spreadsheet, a delay of weeks, or the question "what is that?".

4. How long the product is supported

Ask for: the support period the maker has set for each product, in writing, and how buyers are told about it.

Good answer: a dated statement per product with an end date or a clear rule, and where users can find it.

Warning sign: "as long as we sell it", or no answer.

5. Where security problems get reported

Ask for: the maker's published policy for reporting a security problem, and one address that reaches a person.

Good answer: a public policy page, a security address that actually answers, and the standard file on their website that points to it.

Warning sign: "send it to your account manager".

6. How updates reach the product

Ask for: how security updates get to a product already in the field, whether they are verified and can be undone, and how users learn one is available.

Good answer: a documented, tested update channel with signed updates and a way to notify users.

Warning sign: updates need a site visit, or a manual flash with nothing verifying it.

7. What happens when something is attacked

Ask for: confirmation that the maker has a process for telling the authorities about attacks and serious incidents within the legal deadlines, and a contact who will tell you when one of your products is affected.

Good answer: a named owner, a written plan, a rehearsal date, and an undertaking to inform you within a stated time.

Warning sign: no owner, or an assumption that you will do the reporting.

8. The plan for the CE mark

Ask for: the plan and the date for CE marking each product under this law, and which group they have put it in — ordinary, important class I or II, or critical — with their reasoning.

Good answer: a group with reasoning, a route to checking the work, and a target date comfortably before the law applies in full.

Warning sign: no group assigned, or a group with no reasoning.

Scoring sheet

#	Question	Evidence	Promised, date	Nothing
1	Signed declaration			
2	Paperwork			
3	List of components			
4	Support period			
5	Where problems get reported			
6	Update mechanism			
7	Attack reporting			
8	CE marking plan			

If a supplier has gaps

Send them to us through the "send us a supplier" form on our website. We contact their general or security mailbox, offer the free check and a call, and — with their agreement — tell you where they stand against this list. We never send scan results to anyone who did not ask.

DASKALOS APPS SAS, Péronnas, France. This checklist is an engineering aid, not legal advice. Your own duties as an importer or distributor are yours to confirm. Copy it and pass it on freely.

Regulatory facts referenced

`cra.full_application`

The main obligations of the Cyber Resilience Act (essential requirements, technical documentation, conformity assessment, CE marking, importer and distributor duties) apply from 11 December 2027.

Source: Art. 71(2) https://eur-lex.europa.eu/eli/reg/2024/2847/oj

`cra.importers_distributors`

Importers may place only compliant products on the market and must verify that the manufacturer has carried out conformity assessment, drawn up the technical documentation and affixed the CE marking; distributors must verify the CE marking, the declaration of conformity and that the manufacturer and importer have met their duties.

Source: Arts. 19, 20 https://eur-lex.europa.eu/eli/reg/2024/2847/oj

`cra.importer_distributor_as_manufacturer`

An importer or distributor that markets a product under its own name or trademark, or substantially modifies it, is treated as the manufacturer.

Source: Art. 21 https://eur-lex.europa.eu/eli/reg/2024/2847/oj

`cra.declaration_of_conformity`

The manufacturer draws up and signs the EU declaration of conformity, with the content set out in Annex V, and keeps it up to date; a simplified form is set out in Annex VI.

Source: Art. 28; Annexes V, VI https://eur-lex.europa.eu/eli/reg/2024/2847/oj

`cra.technical_documentation`

The manufacturer draws up the technical documentation with the content set out in Annex VII before placing the product on the market and keeps it up to date during the support period.

Source: Art. 31; Annex VII https://eur-lex.europa.eu/eli/reg/2024/2847/oj

`cra.sbom`

Manufacturers must identify and document the components of the product, including a software bill of materials in a commonly used machine-readable format covering at least the top-level dependencies.

Source: Annex I, Part II, point 1 https://eur-lex.europa.eu/eli/reg/2024/2847/oj

`cra.support_period`

The manufacturer determines the support period so that it reflects the expected time in use; it must be at least five years unless the product is expected to be used for a shorter time.

Source: Art. 13(8) https://eur-lex.europa.eu/eli/reg/2024/2847/oj

`cra.report_clocks`

For an actively exploited vulnerability: an early warning within 24 hours of becoming aware, a vulnerability notification within 72 hours, and a final report no later than 14 days after a corrective or mitigating measure is available.

Source: Art. 14(2) https://eur-lex.europa.eu/eli/reg/2024/2847/oj