29 January

2026

{code & compliance}

FOSDEM EDITION

Open
Regulatory
Compliance

Manufacturer Open Source Due Diligence

Gergely Csatari, Timo Perälä
Code & Compliance
Brussels Jan 29th 2026

The starting point

Requirements from CRA

- Due diligence **should be done** by manufacturers when integrating third party components or open source (Article 13(5)).
- Due diligence **results should be recorded** and presented to the authorities on request (an indirect reference, Article 13(22))
- Tying together **open source voluntary attestation** and **manufacturer open source due diligence** (Article 25)

Current state of ORC Due Diligence white paper:

- Included to the WG work program since early 2025
- Late 2025 a proposal for the structure of the white paper
- Need to ramp-up community activity, call for action

https://github.com/orcwg/orcwg/blob/main/cyber-resilience-sig/whitepapers/due-diligence.md

Some additional sources, from OpenSSF, food for thought

- ”Manufaturers’ checklist” started;
- a proposal for SIG on practices and tooling for manufacturers https://docs.google.com/document/d/1H_P4x7BgAD-6SGhFcPtKD3iJcmXmnlnRBu2RNpJ0KAU/edit?tab=t.0
- Scorecard https://github.com/ossf/scorecard?tab=readme-ov-file#public-data
- Open Source Summit EU 2025: Beyond the Scorecard: Managing Open Source Operability Risk in Telecoms - Gergely Csatari, Nokia
- Worth to follow, ORBIT WG: https://github.com/ossf/wg-orbit/tree/main

But what exactly is due diligence under CRA?

CRA is fairly silent about it. The most we can find is in Resital 34.

CEN/CENELEC ”Princliples for cyber resilience” (a.k.a. PT1) draft attempts to provide further guidance:

7.4 Cybersecurity architecture and design, 7.4.3 Requirement:

> The cybersecurity architecture and design shall ensure that third-party component **integration is performed with due diligence**,
>
> In case the product contains third-party components or RDPS as identified in the product context, **due diligence shall be applied** to all components, whether third-party or not, and to their integration.

7.5 Secure implementation, 7.5.1 General:

> Managing dependencies and third-party libraries by selecting secure libraries and keeping them up to date. **Follow the due diligence** in 7.11 when selecting secure libraries;

7.11 Third-Party Component Cybersecurity Management

> It is important to **take due diligence** when selecting and incorporating third-party components.

PT1: 7.11 Third-Party Component Cybersecurity Management

[This section] specifies the requirements and activities to ensure that cybersecurity risks relevant to third-party components integrated into the product are handled with due diligence and other relevant activities

Assessing that the **intended purpose and reasonably foreseeable use** of the third-party component aligns with the use/integration within the product;

Evaluating that the third-party component is **compliant with applicable legal and contractual requirements** and the **cybersecurity requirements** in particular for the product. This can be done by, amongst others, checking for:

- a CE marking, if available;
- verification that there are no vulnerabilities registered in the European **vulnerability database** established pursuant to Article 12(2) of Directive (EU) 2022/25550 or other publicly available vulnerability databases;
- indicators of **cybersecurity by design**;
- availability of **regular cybersecurity patches**;
- **vulnerability disclosure** and handling;
- a risk assessment;
- checking if additional cybersecurity testing is required.

PT1: 7.11 Third-Party Component Cybersecurity Management, cont.

Considering the **support period** of components when selecting them for integrating these into the product. This anticipates the risks arising from **deprecated third-party component and obsolete technologies**;

Assessing the risk of the third-party component and its integration in the risk assessment of 6.4;

Securely incorporating the third-party component according to 7.5;

Monitoring for vulnerabilities in the third-party component **over the product lifecycle** according to 7.9;

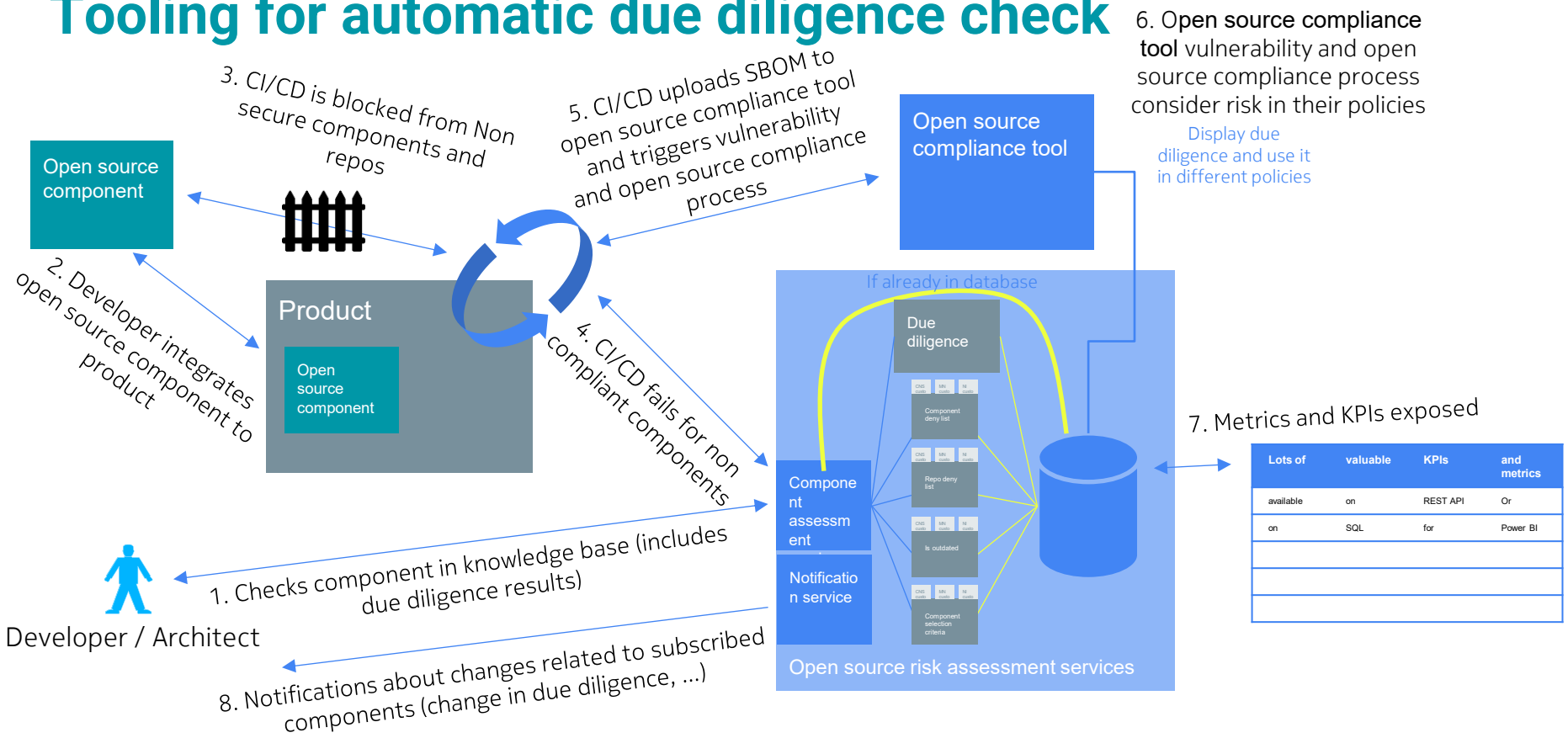
Communicate newly found vulnerabilities in the third-party component as well as **sharing potential solutions** if available.

However, these are not mandatory, they are “can be done, among other things”

To be considered by the manufacturer

- Which products are included into due diligence; all products or only those sold in EU?
- When will manufacturer plan to put due diligence in place?
- Does manufacturer do due diligence for transitive dependencies?
- Tooling for due diligence? (Automation is must)
- **What are the actual criteria / parameters for due diligence?**

Tooling for automatic due diligence check



Possible risk scenarios and mitigation plan 1/2

#	Risk	Consequences	Mitigation
1	Not fully sure about the requirements for criteria of due diligence (what to check on each open source component)	Manufacturer's due diligence implementation does not make them CRA compliant	Establish industry best practices for due diligence with clear requirements.
2	Not fully sure what are the requirements for the scope of due diligence (which open source components to check)	Manufacturer's due diligence implementation does not make them CRA compliant	Establish industry best practices for due diligence with clear requirements.
3	It is difficult to automate due diligence checks.	Manufacturers are not able to do due diligence for everything.	Work on attestation guidance with the communities. Implement attestation in open source projects our companies hosts or supports
4	Not able to do due diligence consistently.	Manufacturers are not CRA compliant and/or they can not prove that we are.	Built open source tools together to automate the due diligence check and documentation in compliance tooling.

Possible risk scenarios and mitigation plan 2/2

#	Risk	Consequences	Mitigation plan
5	Some open source components used in a product do not pass due diligence	Manufacturers have to replace or re-implement open source components in products	Work with the communities of critical open source components to match due diligence requirements.
6	Product teams do not push for fulfilling the due diligence requirements.	Manufacturers are not CRA compliant.	Manufacturers need to change their software implementation practices and processes.

Topics for Open Forum/Workshop/Snack time

What should the due diligence white paper contain for it to be useful for manufacturers?

- Is the PT1 view of due diligence requirements adequate, or should it be amended? Or shall create our own from clean slate?
- Tooling to support due diligence
- …

Flesh out the white paper table of contents

Commitment to contribute to white paper

Agree on logistics. Proposal: to start with

- use Vulnerability Handling Task Force call every other Thursday 15:00 CET and
- #tf-vulnerability-handling

Thank you!