From Regulation to Implementation

Managing Risk under CRA

Adrian Anghel
Cybersecurity Consultant
at Enersec Technology

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.
The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

CRA's Risk-Based Approach: Why Risk Sits at the Core

- CRA places **cybersecurity risk at the center** of product compliance
- Manufacturers must ensure a level of cybersecurity **appropriate to the risks** the product faces
- Risk is **not optional** — it shapes *how* the essential requirements apply to the product
- The approach is **lifecycle-wide**:

  planning → design → development → production → delivery → maintenance

- Two complementary pillars in **Annex I**:
  - product security properties
  - vulnerability handling

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.
The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Risk Assessment: A Mandatory Process Under CRA

- A cybersecurity risk assessment is an **explicit legal obligation** for manufacturers (Art. 13)
- The analysis must be **product-specific** and consider:
  - **Intended purpose** and reasonably foreseeable use
  - **Conditions of use** — operational environment, assets to protect
  - **Expected duration** the product will remain in service
- It must determine **which essential security requirements apply** and **how they are implemented**
- It must also address how **vulnerability handling** will be performed
- It must be **written down** and included in the **technical documentation**
- Where a requirement does not apply, the manufacturer must provide a **clear justification** — silence is not an option
- **Proportionality applies**: where a requirement is genuinely incompatible with the product's intended purpose or context, this can be justified — but it must be argued, not assumed

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.
The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

A Living Document: Risk Assessment Across the Lifecycle

- The risk assessment must be **maintained and updated** throughout the entire support period
- Typical update triggers: **new vulnerabilities**, threat landscape shifts, product changes, evolving use cases
- It should drive decisions in **every lifecycle phase** — not only at market release
- It enables **traceability**: risk → applicable requirement → implemented control → evidence
- This same chain underpins everything that follows — SBOM, vulnerability handling, risk treatment, audits

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.
The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

SBOM: The Foundation of Vulnerability Awareness

- CRA explicitly requires manufacturers to **identify and document the components** contained in the product (*Annex I, Part II*)
- The **Software Bill of Materials (SBOM)** is the mandated mechanism — a structured inventory of all software components, including third-party and open-source dependencies
- Must be in a **commonly used, machine-readable format** — in practice **SPDX** or **CycloneDX**
- Must cover **at least the top-level dependencies**
- Maintained at **product-version level** — different versions ship with different components, and so with different risk profiles

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.
The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

From Components to Vulnerabilities to Risk

- Each component in the SBOM is **continuously checked** against vulnerability databases (CVE, NVD, GHSA, vendor advisories)
- Detected vulnerabilities feed a **structured handling process** — receipt → verification → remediation → release — required by Annex I, Part II and Article 14
- A vulnerability detected by a scanner is **not yet a risk** — it must be evaluated in product context: exploitability, exposure, impact on users (including health & safety)
- Risk evaluation is what **prioritizes** which vulnerabilities deserve urgent action vs. monitoring vs. acceptance
- The result is a continuous loop: **SBOM → Scan → Vulnerability → Risk → Treatment → Evidence** — sustained for the entire support period

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.
The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Documentation: The Audit Trail CRA Demands

- CRA requires manufacturers to draw up **technical documentation** before placing the product on the market (*Article 31, Annex VII*)
- Must demonstrate **how** the product meets the essential cybersecurity requirements — not just *that* it does
- Required content includes: product description, design and development processes, **risk assessment, SBOM and vulnerability handling**, applied standards, test results, declaration of conformity
- Must be kept current for the support period and **retained for at least 10 years** after market placement
- **Proportionality for SMEs**: a simplified technical documentation form is being established by the Commission for microenterprises and small enterprises (*Recital 93*)

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.
The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Auditability: Traceability from Risk to Evidence

- A market surveillance authority can ask, at any moment, "*why did you decide this?*" — your documentation must answer
- Each compliance claim should be backed by a **chain of evidence**: identified risk → applicable requirement → implemented control → test or artefact proving it works
- Practical implications: version everything, link decisions to artefacts, log changes, keep a clear **risk register** and **vulnerability log**
- The chain breaks if any link is missing — at audit, "we did it but did not record it" equals "we did not do it"
- This is precisely the chain that **OSCRAT** is designed to maintain

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.
The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Risk Treatment under CRA

- Four standard treatment options: **Accept, Reduce, Avoid, Transfer**
- CRA judges adequacy against a **regulatory standard** — based on intended purpose and foreseeable use, not internal cost or risk tolerance
- "Accept" is allowed, but **significant risks must be addressed before market** — residual risk that remains is the manufacturer's responsibility
- Where relevant, residual risks must be **communicated to users** in the product information (*Annex II*)
- Every treatment decision must be **documented and traceable** back to the risk that triggered it

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.
The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

OSCRAT: Identifying & Registering Risks

- Risk Assessment is a **dedicated task type** in OSCRAT, attached to a specific Product Version
- Structured capture: **Asset · Threat · CIA category · Likelihood · Impact · Owner**
- **Exposure auto-calculated** from a 3×3 matrix (Low / Medium / High)

Likelihood x Impact	Low	Medium	High
Low	Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	High

- Built-in treatment workflow: **Accept / Reduce / Avoid / Transfer**, with residual exposure and responsible person
- Result: a **product-level risk register** that is auditable, traceable, and always linked to its product version

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.
The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

OSCRAT: Traceability — Tasks + Evidence

- Every artefact — **risks, vulnerabilities, SBOMs, configuration scans, documents** — lives under one Product Version
- Tasks are **auto-generated** from compliance gaps, failed scans, and detected vulnerabilities
- Each task carries a backlink to its source: requirement, CVE, scan finding, or risk
- **Evidence uploads** are attached at the level where they prove something
- One unbroken chain: *risk* → *requirement* → *control* → *task* → *evidence* — exportable as an audit package

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.
The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

From Regulation to Implementation: Conclusions

- CRA makes risk management a **mandatory, documented, lifecycle process** — not a one-off exercise
- Compliance is judged on the **chain of evidence**: risk → requirement → control → task → evidence
- The hard part is not understanding what CRA requires — it is **keeping the chain consistent** across teams and across the entire support period
- **OSCRAT** is being built to close exactly this gap — bringing risks, SBOMs, vulnerabilities, configurations, tasks and evidence into one auditable workspace
- The earlier risk thinking is embedded into the development lifecycle, the lighter the compliance burden becomes at the end

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.
The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

OSCRAT

Open-Source Cyber Resilience Act Tools

Follow us on social media

Co-funded by the European Union

ECCC

EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180