

EU CRA: Survival Guide for Enterprise & Open Source

Roman Zhukov

Principal Architect - Security Communities Lead
Expert, the European Standardization Organizations (ESOs)
Security Lead, Maintainer and Contributor to Open Source

DISCLAIMER

The opinions expressed are solely my own and do not necessarily reflect the official views or opinions of my current or previous employer(s).

Nothing in this presentation is a legal advice.

Some images are generated using AI. All coincidences are random.



Meet SmartWidget – IoT Environmental Sensors



OUT OF SCOPE

Alex (libsensor)

Developer from Nebraska.
Maintains libsensor library
part of GreenCore toolkit.
MIT license. No
monetisation or support.

"Zero CRA obligations."

"Yes, but..."



OSS STEWARD

GreenCore

FOSS foundation, Brazil.
maintaining the core toolkit
SmartWidget is using. Hosts
infra, governs project,
employs 5 engineers.

***"Policy & vulnerability
facilitation."***



MANUFACTURER

WidgetWorks

Startup IoT manufacturer,
Berlin. Builds and sells
SmartWidget
under their own brand.

***"Risk assessment & CE
marking."***



MANUFACTURER

InfraGuard

Large vendor, Brussels.
Embeds SmartWidget into
building management systems
sells for thousands of EU
companies.

***" + Responsible for
integrated deps."***

Note: By December 2027, every actor is affected by the CRA, but their legal exposure is fundamentally different.

1

Who ships software that runs in the EU AND uses open-source components in their products?

2

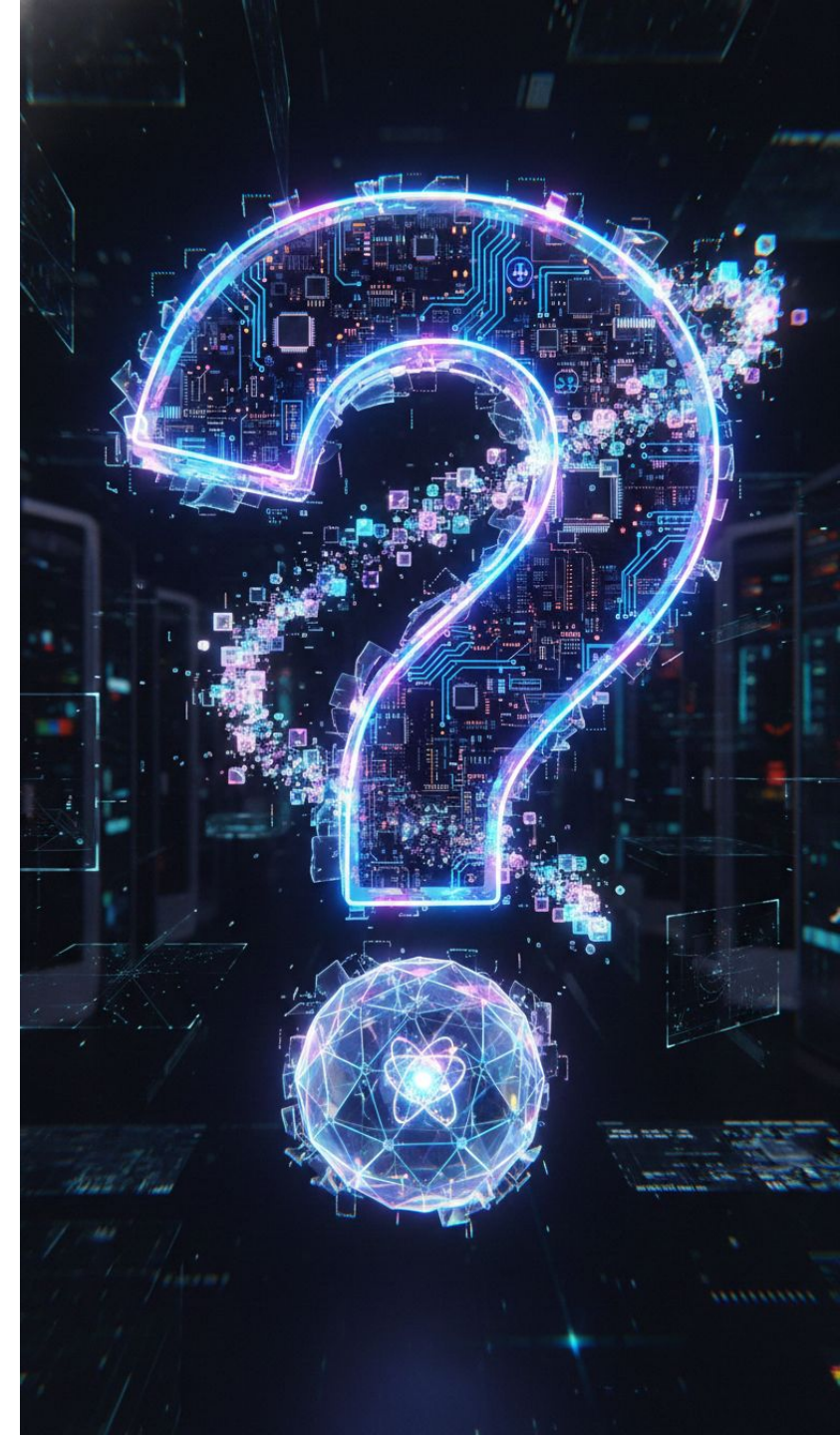
Who has a documented process for reporting a vulnerability to a government authority within 24h?

3

Who has ever inherited a codebase or dependency and thought 'I hope nobody asks me what's in this'?

4

Are you maintainer of or contributor to an open source project?



To safeguard European consumers of Products with Digital Elements (PDE)

CRA establishes essential cybersecurity requirements for companies operate in the EU.



Core Goals

- Reduce vulnerabilities
- Product lifecycle security
- Enable Informed decisions for users



Scope & Roles

- Targets mostly Manufacturers (vendors), Importers and Distributors
- Covers 3rd party dependencies
- Defines open source Stewards



Compliance

- Worldwide applicability for commercial activity within EU
- Fines up to €15M or 2.5% global turnover



September 2026




Vulnerability Reporting Obligations

December 2027

Full Force Implementation

Article 3(1): “**PDE** a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately”







✓ IN SCOPE

-  Meets the definition of a PDE (**software** or **hardware**)
-  Made available on the market (in a **commercial** activity)
-  Intended/**foreseeable use** includes a data connection to a device or network

Note: Software = “the part of an electronic information system which consists of computer code” (Art. 3(4)).

Source code, compiled, interpreted – all count.

✗ OUT OF SCOPE

-  Own use products
-  SaaS
 - If the cloud part goes down, and the product breaks – that cloud part **is in scope** as Remote Data Processing Solutions (**RDPS**)
-  Aviation, Marine, Medical, Auto
-  National Defense
-  Unfinished software (Beta)
-  Free and Open Source SW (FOSS)
 - If not monetized

PDEs are...



src: <https://knowyourmeme.com/memes/x-x-everywhere>



- ▶ Consumer devices, toys
- ▶ Simple IoT device

90%+ of SW and HW

Default Category



Self assessment
(Module A)

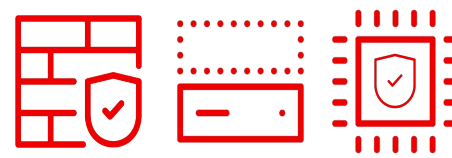


- ▶ Smart home
- ▶ Operating Systems
- ▶ Web browsers
- ▶ Password mgrs.

Important Class I (19)



Self-assessment with
harmonised
standards
(Module A)

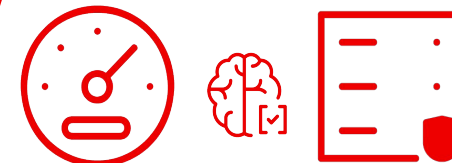


- ▶ Firewalls
- ▶ Tamper-resistant CPUs
- ▶ Hypervisors and CRS

Important Class II (4)



3rd Party
assessment
(Module B+C;
Module H)



- ▶ HW Devices w/Security Boxes
- ▶ Smart meter gateways

Critical (3)



EU Cert Scheme

Economic Operators



Manufacturer – develops places PDE on the market under their name/trademark in course of commercial activity.

Full obligations



Importer and Distributor – bringing a product into the EU market (re-sells PDEs)

Ensure compliance, Verify CE marking, check documentation, Maintain records

Other Notable CRA Actors



Notified Body (NSB) and Conformity Assessment Body (CAB) – independent organizations checks product compliance with the CRA.

Perform 3rd party assessment



Market Surveillance Authority (MSA) – EU27 National authority that ensures products meet CRA rules.

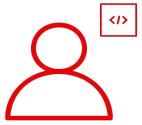
Monitor compliance



National CSIRT and ENISA – you must report actively exploited vulnerabilities and severe incidents to the SRP (Single Reporting Platform).

Incident receiving and dissemination

FOSS is out of scope. Isn't it?



OSS **Maintainer** and **Contributor** – **out of scope** if don't monetize project, as per Recital 18.

*No obligations under the CRA. *suppose to do nothing =)*



OS SW **Steward** – systematically supports FOSS projects, but not a Manufacturer.

Most OSS projects don't have a Steward. Steward obligations are triggered by development and infrastructure support.

✓ **Non-commercial -> Not a Manufacturer**

- Developing FOSS without monetisation
- Receiving donations that cover actual costs
- Being employed to contribute code to a FOSS project
- Publishing on public repositories (contributor)
- Paid support for the PDE you don't build (not a manufacturer)

⚠ **Commercial activity indicators -> Manufacturer**

- Charging a price for the software
- Monetising via a platform built around it
- Requiring personal data processing beyond security needs
- Donations exceeding costs of development
- Charging for support beyond cost recuperation

Why Red Hat Cares

Red Hat as a **Manufacturer**

- ▶ Provider of enterprise open-source software solutions for the global market, including the EU.

Red Hat as a potential **Open Source Software Steward**

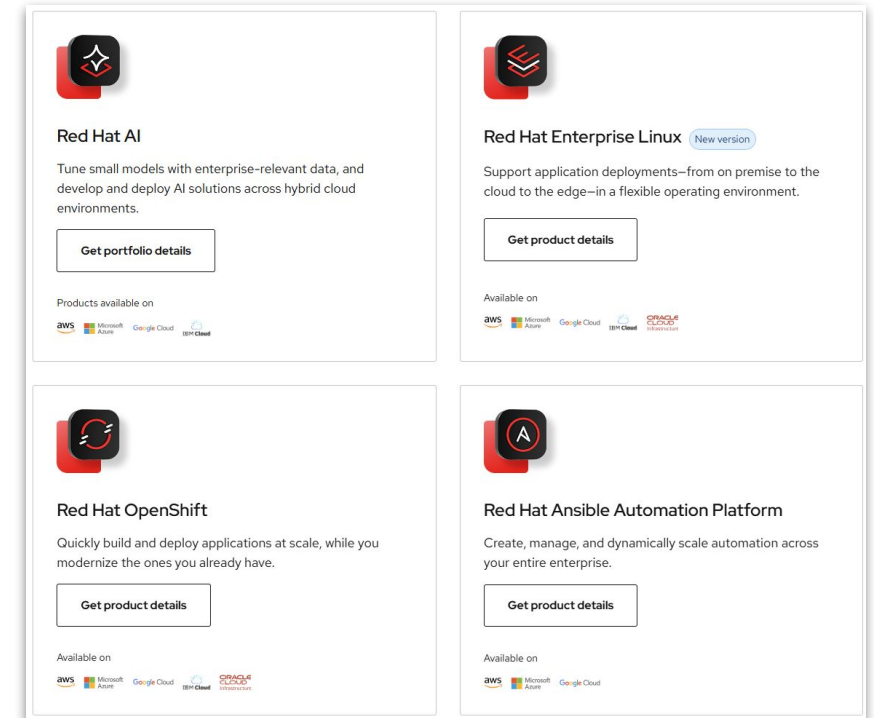
- ▶ Red Hat's relationship with open source software is foundational. The company actively supports Fedora and countless others projects.

Red Hatters are **Contributors** and **Maintainers**

- ▶ Thousands of Red Hatters contribute to open source projects everyday.



We're leading CRA efforts in Open Source Communities and EU Official Standardization bodies to make sure the open-source ecosystem is CRA-compliant and healthy.



Obligations compared – manufacturers own them

Obligation	Manufacturer	Steward
Cybersecurity risk assessment	Required (Art. 13)	Not required
Conformity assessment and CE marking	Required (Art. 32)	Not required
5 Years Support and 10 Technical documentation	Required (Rec. 60, Art.13 and Annex VII)	Not required
Secure by design and by default, incl. Data and communication protection	Required	Cybersecurity policy and Facilitation of secure development only (Art. 24)
3rd party components list and SBOMs	Required (Rec. 77)	Not required
Due diligence for 3rd party components	Required (Art. 13)	Not required. (Art. 25 is for <u>voluntary</u> FOSS attestations)
Release with no known vulnerabilities and Vulnerability handling	Required (Annex I)	Facilitate only (Art. 24)
Reporting to ENISA of actively exploited vulnerabilities and severe incidents (24-Hour initial reporting)	Mandatory (Art. 14)	Only if aware via their development or infrastructure support (Art. 24)
MSA Cooperation	Required	Required



Vulnerability Mgmt & Reporting

CRA Article 14 & Annex I, Part II



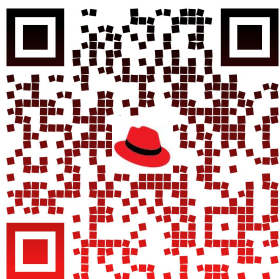
24h Early warning – Initial notification that an actively exploited vulnerability exists. 72h - Full vuln details. 14d - Final report.



Security updates – apply and ship without delay.



Proactive push – mandatory testing, CVD, sharing CVE data.



github.com/RedHatProductSecurity/aegis-ai



AI-Powered CVE analysis

- Automates CWE, CVSS Scoring, Impact
- Fetches NVD, GitHub, osv.dev, CISA KEV, Linux CVEs, Wikipedia, PyPI
- Integrates OSIDB, GUAC/Trustify, CI/CD, MCP



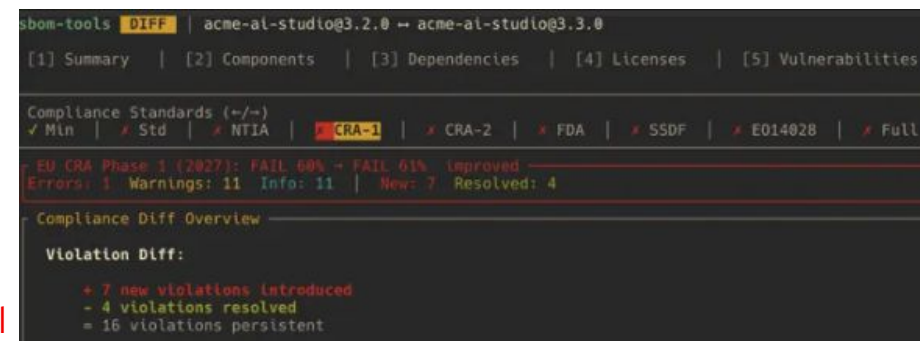
Software Bill of Materials (SBOM)

CRA Rec. 77 & Annex I, Part II

- ▶ Identify & document all components in the product – including FOSS dependencies.
- ▶ Generate SBOM in a machine-readable format (SPDX, CycloneDX expected).
- ▶ Include at minimum: top-level dependencies of the product.
- ▶ PT3 Standard may push towards full transitive dependency listing.
- ▶ Publishing SBOMs is not a requirement, but a good practice to inform downstream users.



github.com/sbom-tool



SBOMs are vital for Vulnerability Management & Reporting

Know what's inside



Match CISA KEVs and EUVD

Scope your reports

Prioritize patches with VEX

Good Security Practices are Not Invented by the CRA



Automate compliance posture

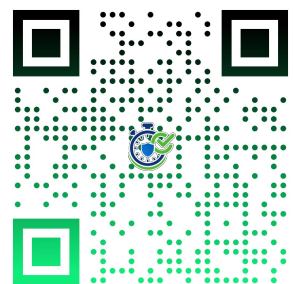
Policy-As-Code and compliance automation across any hybrid environments.

OpenSSF Gemara:

The one machine-readable standard to rule all your compliance (from NIST to PCI-DSS to OSPS to CRA) in uniform & automated manner.

ComplyTime:

Convert your policy catalogues into technical implementation for engineers. Cloud-native.



Turn on security controls

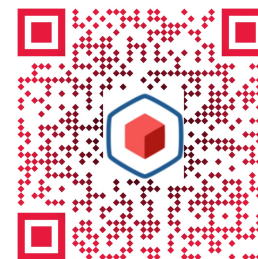
Enable "security-by-default" in a cloud-native manner.

StackRox:

Kubernetes Security Platform providing visibility, vulnerability management, threat detection, incident response, and risk profiling.

Confidential Containers:

HW-backed protection of your data and applications, even from cloud providers and Kubernetes cluster administrators.



Manage SBOM and CVE at scale

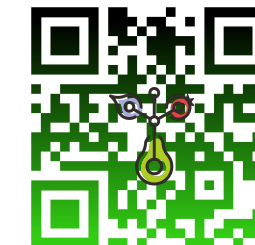
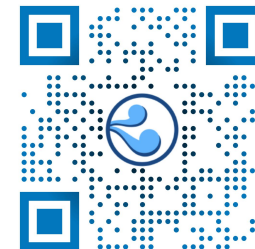
Improve evidence collection and vulnerability analysis as part of your pipelines.

Konflux:

Trusted software factory to make your builds with native verifiable security with signed SBOMs.

OpenSSF Guac & Trustify:

Brings vulnerability metadata (SBOM, CVE, VEX) within one database with actionable UI.



Due Diligence for the entire supply chain – Art. 13 & Rec. 34

Note: Manufacturers carry absolute **Product liability**; Mandatory secure integration of **all third-party** components; **No liability offload**.



Supplier Verification

- CE Marking & Declaration Audit
- Assess Security Posture and Docs
- Establish CSSA Agreements



Architecture

- Purpose Alignment
- Sandboxing & Isolation
- Security Function Mapping



Vulnerabilities

- Query CVE Registers
- Audit Update History
- Support Period Check
- SBOM Deep Review



Tech Testing

- Functional Sec Tests
- SCA, Pen & Fuzz Testing
- Binary Analysis
- Rebuild from Source



Same for FOSS!



“

Open Source
Maintainers
owe you nothing.

Mike McQuaid

”

<https://mikemcquaid.com/open-source-maintainers-owe-you-nothing/>



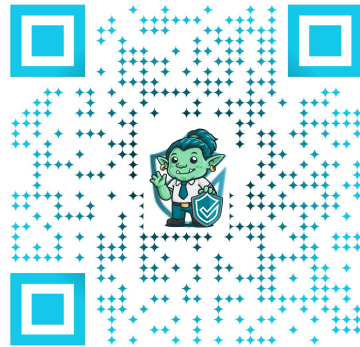
Respectful compliance for FOSS is the only path

Note: Don't send "CRA Questionnaire" to FOSS as for your supplier. Minimizing the burden on open-source projects will be the key.

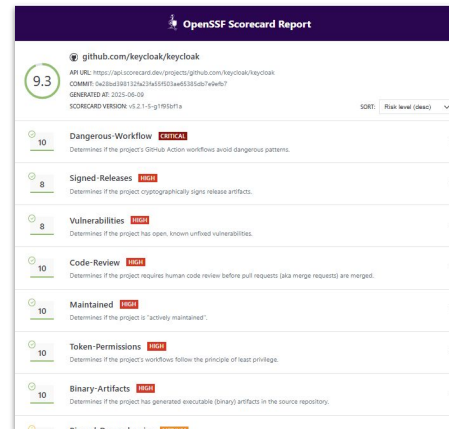
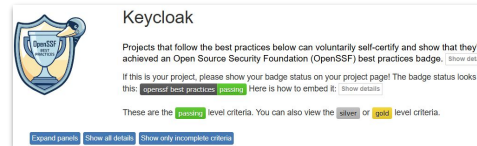


FOSS Controls

- Maintainer Vitality
- CVD Verification
- FOSS Steward ID
- Secure-by-Design Audit
- Patch Availability
- Cost Per Dependency
- Risk Per Dependency



Brainstorm together:
github.com/orcwg



Try out:
bestpractices.dev
github.com/ossf/scorecard







Tooling for Due Diligence:
github.com/ossf/orbit-launchpad



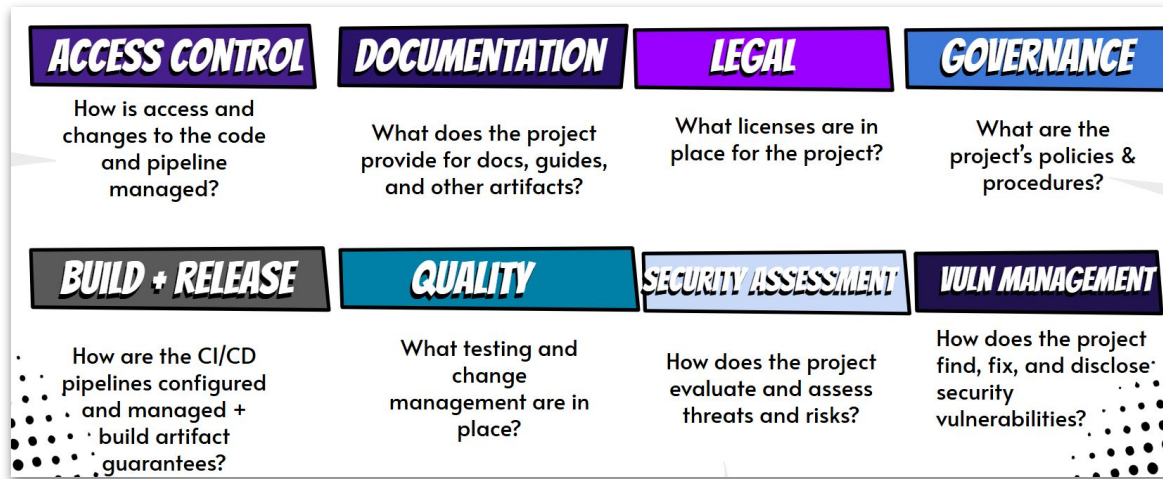
Join CRA discussions:
github.com/ossf/wg-globalcyberpolicy

Alex as a FOSS maintainer? No obligations!

*"But what I **want** my project to be useful, widely adopted (by users & **manufacturers**) and at best quality and security. I **voluntarily** implement and document good security practices.*

 OUT OF SCOPE Alex (libsensor) Developer from Nebraska. Maintains libsensor library part of GreenCore toolkit. MIT license. No monetisation or support. "Zero CRA obligations." "Yes, but..."	 OSS STEWARD GreenCore FOSS foundation, Brazil. maintaining the core toolkit SmartWidget is using. Hosts infra, governs project, employs 5 engineers. "Policy & vulnerability facilitation."	 MANUFACTURER WidgetWorks Startup manufacturer, Berlin. Builds and sells SmartWidget under their own brand. "Risk assessment & CE marking."	 MANUFACTURER InfraGuard Large vendor, Brussels. Embeds SmartWidget into building management systems sells for thousands of EU companies. "Responsible for integrated deps."
---	--	---	--

OpenSSF Baseline – 64 requirements x 3 levels of maturity.



Learn: policy.openssf.org/CRA/maintainers.html



Explore: github.com/ossf/security-baseline

- ▶ Security Policy
- ▶ [Security.md](https://security.md) vulnerability handling
- ▶ SBOMs
- ▶ MFA
- ▶ Branch Protection
- ▶ SLSA - L1
- ▶ Signing Commits
- ▶ OpenSSF Baseline (OSPS) - L1

Red Hat CRA Program Structure – 8 Workstreams



Strategic Investment. Not Just Compliance.

Red Hat views the CRA as a milestone for global cybersecurity and a shared opportunity to elevate trust in SW supply-chains. We leverage 25 years of leading security expertise to make sure our customers can rely on a compliant software supply chain that supports their own security and regulatory goals.



Vulnerability Excellence

Reporting

Working with ENISA/CSIRTs for real-world SRP needs.

SBOM & VEX

Auditable processes for scale and quality, powered by leading analysis and reporting via CSAF.



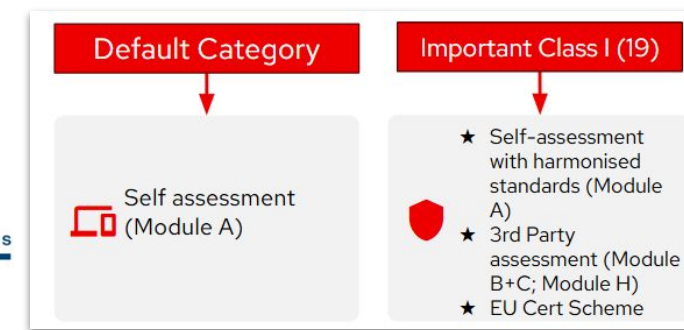
Responsible FOSS Stewardship

Active Contribution: Shaping EU Standards and implementation documents.

Open Source-First: Leadership in Eclipse ORC and OpenSSF. All we do is upstream – come join us!

Upstream Hardening: Championing security in projects like Fedora and Ansible and beyond.

41 CRA standards are under development by ESOs. 36 expected by end of 2026.



Standard	Content	Status	Expected
PT1 - Horizontal (CEN/CLC) (EN 40000-1-2) (+EN 40000-1-1 Vocabulary)	Principles for cyber resilience, product risk management and lifecycle activities	All 2500 comments during public consultation are resolved. "Good is good enough" approach - final stages. No due diligence requirements (out of scope).	Aug 2026
PT2 - Horizontal (EN 40000-1-4)	Generic security requirements: catalogue of security controls	Uses RED DA (EN 18031) as an inspiration. Deprioritized at the moment, public enquire is planned in Q3'26. Needs more contributors.	Oct 2027
PT3 - Horizontal (EN 40000-1-3)	Vulnerability handling	Only 1 horizontal <i>may</i> give "presumption of conformity". Comments resolution in progress > 2500 comments. Some architectural debates on imposing requirements. Moving towards more than 1-level SBOMs requirement.	Dec 2026
18 - Vertical (ETSI) 8 - Vertical CEN/CENELEC	Each covering Important (Class I & II) and Critical PDE category	17 mature drafts. (Ongoing open consultation: docbox.etsi.org/CYBER/EUSR/Open) Heated discussions on: PKI, OT use-cases, Routers, Boot Manager, Browsers, Operating Systems, Hypervisors.	Dec 2026

Key shifts over working on Standards

No SHALL beyond CRA



Industry practices and specs

FOSS is taken seriously

(Relatively) open to feedback

ENISA Single Reporting Platform (SRP)

FAQ and some info: enisa.europa.eu/topics/product-security-and-certification/single-reporting-platform-srp



SRP = Unified Reporting Hub

A single electronic system for manufacturers to report actively exploited vulnerabilities and severe incidents. Replaces notifying multiple national authorities individually. **NEW - 25 fields on what to report.**



Mandatory Launch Date

Operational by **September 11, 2026**. Early testing with selected manufacturers is planned for July 2026.

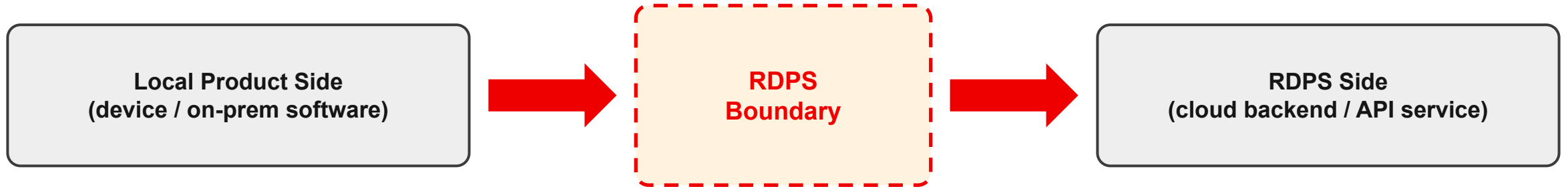


Legal & Technical Security

Managed by ENISA with strict technical security measures. All reporting is text-based to prevent malware risks from document uploads.

If the cloud part goes down, and the product breaks – cloud part is RDPS

RDPS clarifications are under active development by ETSI, CEN/CLC (Annex R) and the Commission.



Definition

Any data processing solution operated remotely and **required** by the product to perform **one or more of its functions** – including cloud dashboards, AI inference endpoints, OTA update servers, telemetry backends.



Why it matters

Under Article 3(2), **RDPS is part of the product**. The manufacturer bears **the same essential cybersecurity requirements** (Annex I) for the remote component as for the device itself. *May reference SOC 2 or ISO 27001 certs.*



Scope boundary

CRA covers the product-facing interface ("RDPS boundary") – **not the full cloud infrastructure**. Security obligations focus on what crosses **that boundary**: commands, responses, keys, updates, personal data.

- RDPS boundary - demonstrate full CRA conformance.
- The rest of cloud infra - due diligence for provider.

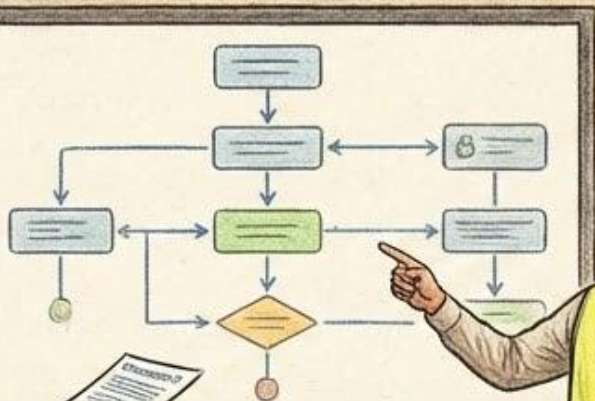
CRA: EU CYBER RESILIENCE ACT - COLLABORATION FOR A SECURE FUTURE!

Yay!

Yay!

Collaboration!

Secure Supply Chain!



OSS
MAINTAINER

OSS
MAINTAINER

OSS
MAINTAINER

OS SW
STENOGR

OS SW
STENOGR

UNIDENTIFIED
SCOPE 1
COUN

UNIDENTIFIED
SUPPLY
CHAIN

1

Explore CRA - scope is broader than you think

Assess carefully. Take into account RDPS and FOSS. Even outside the EU – the 'Brussels Effect' makes this global.

2

Understand your role and responsibilities

Manufacturer, distributor, maintainer, steward – obligations differ dramatically. Liability flows downstream and non-transferable.

3

Don't wait - build your CRA program now

Complete gap analysis. Plan quick wins. First obligations are enforceable in a few months already.

4

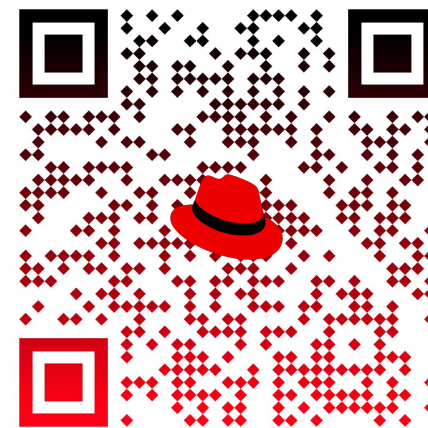
Apply security practices available

Invest in real security and compliance will follow. There are plenty of mature frameworks and open source tools.

5

Collaborate upstream - it's free

Join Red Hat and other peers at Eclipse ORC WG and OpenSSF GCP WG. We need your voice and support.



Championing CRA

red.ht/cra-ext

Building secure future
open source way.

(Find Links and Checklists in this deck)

 LINKEDIN.COM/IN/ROZHUKOV



linkedin.com/company/red-hat



youtube.com/user/RedHatVideos



facebook.com/redhatinc



twitter.com/RedHat

Your CRA Toolkit

Resource	Link
CRA Full Text	eur-lex.europa.eu/eli/reg/2024/2847/oj
CRA Implementation Portal, incl. FAQ (Commission)	digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation
Draft CRA Guidance	digital-strategy.ec.europa.eu/en/news/commission-publishes-feedback-draft-guidance-assist-companies-applying-cyber-resilience-act
ENISA Single Reporting Platform (SRP)	https://www.enisa.europa.eu/topics/product-security-and-certification/single-reporting-platform-srp
Red Hat CRA Page (links to blogs and materials)	red.ht/cra-ext
CRA Standards Educational Portal	www.stan4cra.eu
ETSI Standards Open for Consultation	docbox.etsi.org/CYBER/EUSR/Open
Free CRA Basics Class by Linux Foundation	training.linuxfoundation.org/express-learning/understanding-the-eu-cyber-resilience-act-cra-lfel1001/
OpenSSF Global Cyber Policy WG	github.com/ossf/wg-globalcyberpolicy
Eclipse Open Regulatory Compliance WG	github.com/orcwg
OpenSSF CRA Voluntary Guide for FOSS Maintainers	policy.openssf.org/CRA/maintainers.html
OpenSSF Stewards Playbook	policy.openssf.org/CRA/stewards-playbook.html
OpenSSF Maintainers Guide	policy.openssf.org/CRA/maintainers.html
OSPS Baseline	baseline.openssf.org
Kunflux - Trusted SoftwareFactory	github.com/konflux-ci
Stackrox - Kubernetes Security Platform	github.com/stackrox/stackrox
Gemara - Compliance Automation Spec	github.com/gemaraproj

Manufacturer Checklist (1/2)

#	Requirement (Annex I, Part I – Security by Design)	✓/✗
A1	Documented cybersecurity risk assessment (intended purpose + foreseeable misuse)	
A2	Risk assessment covers full product lifecycle (design → delivery → maintenance)	
A3	Risk assessment updated after significant changes or substantial modification	
A4	Risk assessment covers integrated third-party components (incl. OSS dependencies)	
A5	Threat model documented (proportionate to product risk profile)	
B1	Product delivered without known exploitable vulnerabilities	
B2	Secure by default configuration (no default passwords, debug ports closed)	
B3	Protection against unauthorised access (authentication, identity mgmt)	
B4	Confidentiality of data (at rest + in transit, encryption where appropriate)	
B5	Data integrity protection	
B6	Data minimisation (only process data necessary for intended purpose)	
B7	Availability + resilience (protection against denial-of-service)	
B8	Minimised attack surface	
B9	Secure update mechanism (authenticated, integrity-protected)	
B10	Logging and monitoring capabilities where appropriate	

Manufacturer Checklist (2/2)

#	Requirement (Annex I, Part II + Conformity + Reporting)	✓/✗
C1	Vulnerability handling policy + process documented (Annex I, Part II)	
C2	Vulnerability disclosure contact published (SECURITY.md / security.txt)	
C3	Coordinated vulnerability disclosure (CVD) process in place	
C4	Security updates provided throughout declared support period, free of charge	
C5	Security updates delivered separately from feature updates (where feasible)	
C6	Security advisories published for remediated vulnerabilities	
C7	SBOM generated and maintained (minimum: top-level deps; PT3 direction: full transitive)	
C8	Process to share security fixes with upstream OSS maintainers	
D1	Conformity assessment procedure identified (Module A / B+C / H)	
D2	Technical documentation prepared per Annex VII	
D3	EU Declaration of Conformity drafted (Annex V)	
D4	CE marking process defined	
D5	Support period defined and communicated to users	
D6	User information and instructions prepared (Annex II)	
E1	ENISA Single Reporting Platform (SRP) registration planned	
E2	Internal 24h / 72h / 14d reporting process ready	
E3	Process to detect actively exploited vulnerabilities (KEV monitoring)	
E4	Contact point designated for vulnerability + incident reporting	

OSS Steward Checklist

#	Required – Art. 24 Obligation	✓/✗
F1	Verifiable cybersecurity policy documented and published (Art. 24(1))	
F2	Policy covers: secure development, risk handling, vuln reporting, CVD, end-of-life plan	
F3	Secure development practices documented (fostering “security by design”)	
F4	Vulnerability handling process established and documented	
F5	Coordinated vulnerability disclosure (CVD) process in place	
F6	Security contact published (SECURITY.md / security.txt in each repo)	
F7	Process to facilitate CRA obligations of downstream manufacturers	
F8	Process to cooperate with market surveillance authorities on request	
F9	Reporting: actively exploited vulns / severe incidents discovered via development activities	
F10	Reporting: incidents discovered via hosting activities (CI/CD, build systems, infra)	

FOSS Maintainer Checklist (Voluntary)

#	Voluntary "CRA-Friendly" Practice (policy.openssf.org)	✓/✗
H1	Cybersecurity & Vulnerability Management Policy (SECURITY.md): reporting process, contact info, vuln handling, CVD process, end-of-life plan	
H2	Contributing Guidance (CONTRIBUTING.md) with links to secure development practices	
H3	Release Documentation (CHANGELOG / release notes) noting security fixes	
H4	Bug Reporting Guide (distinct from security vulnerability reporting)	
H5	MFA Enforcement for all contributors, especially maintainers/admins	
H6	Branch Protection enabled on main/release branches	
H7	Clear LICENSE file (OSI-approved license)	
H8	OSPS Baseline Level 1 achieved (covers most of the above)	