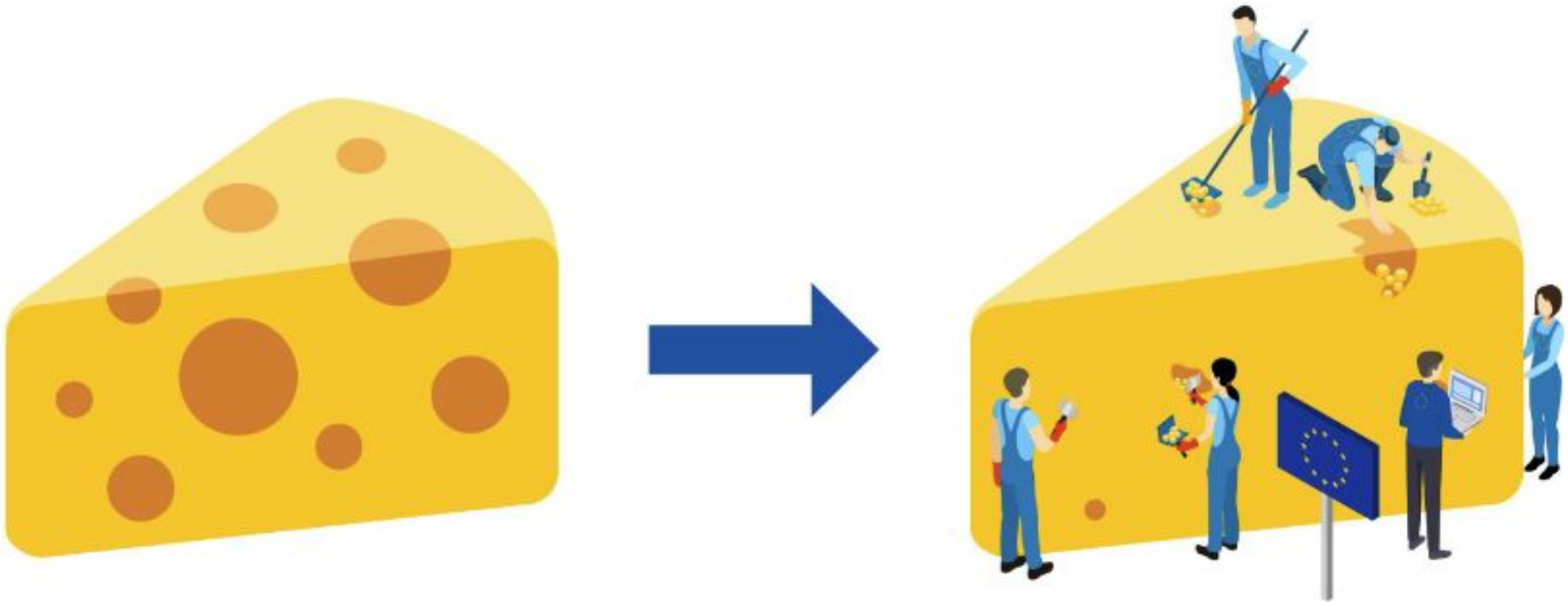


European Commission

EU CRA: Survival Workshop for Enterprise & Open Source

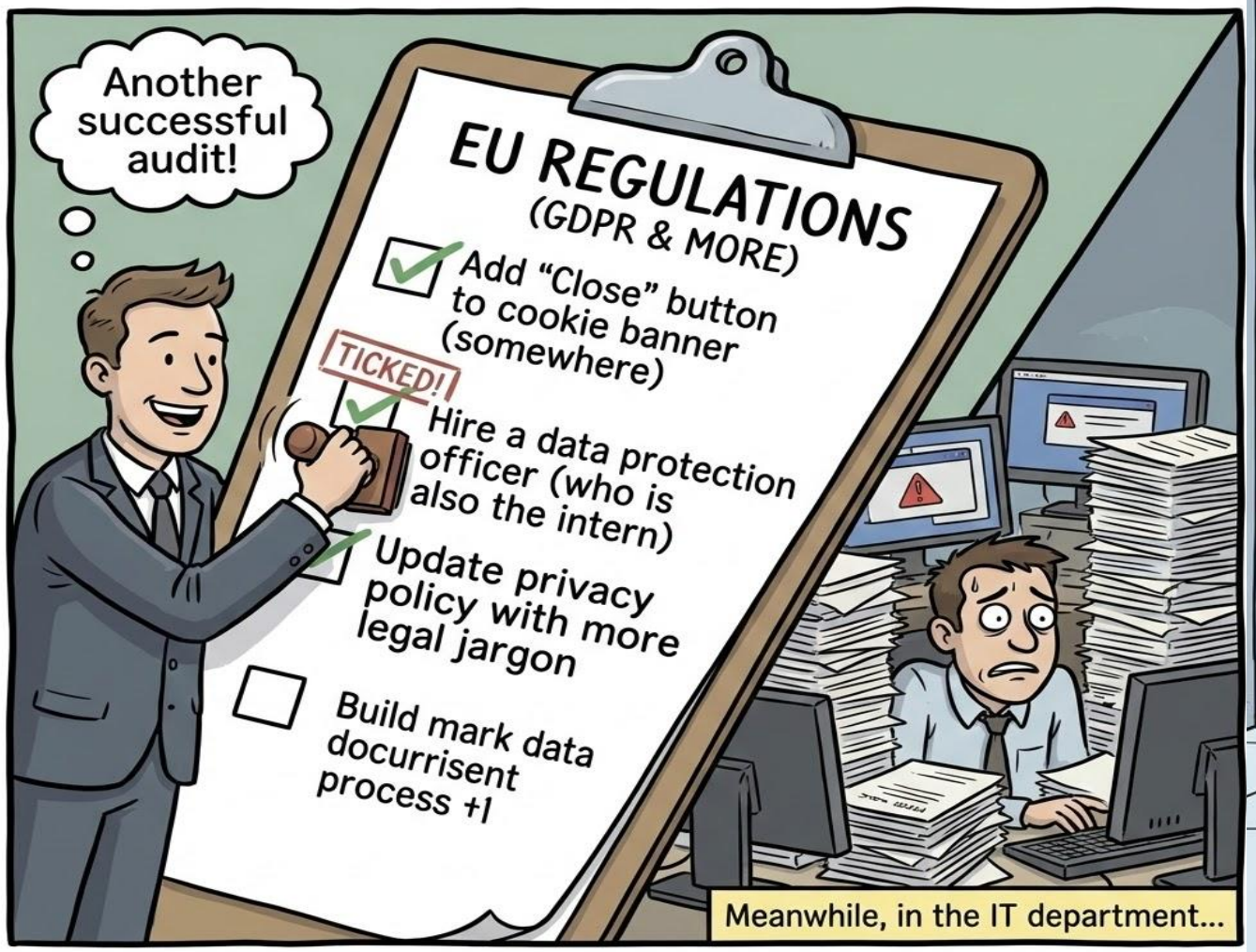
Roman Zhukov

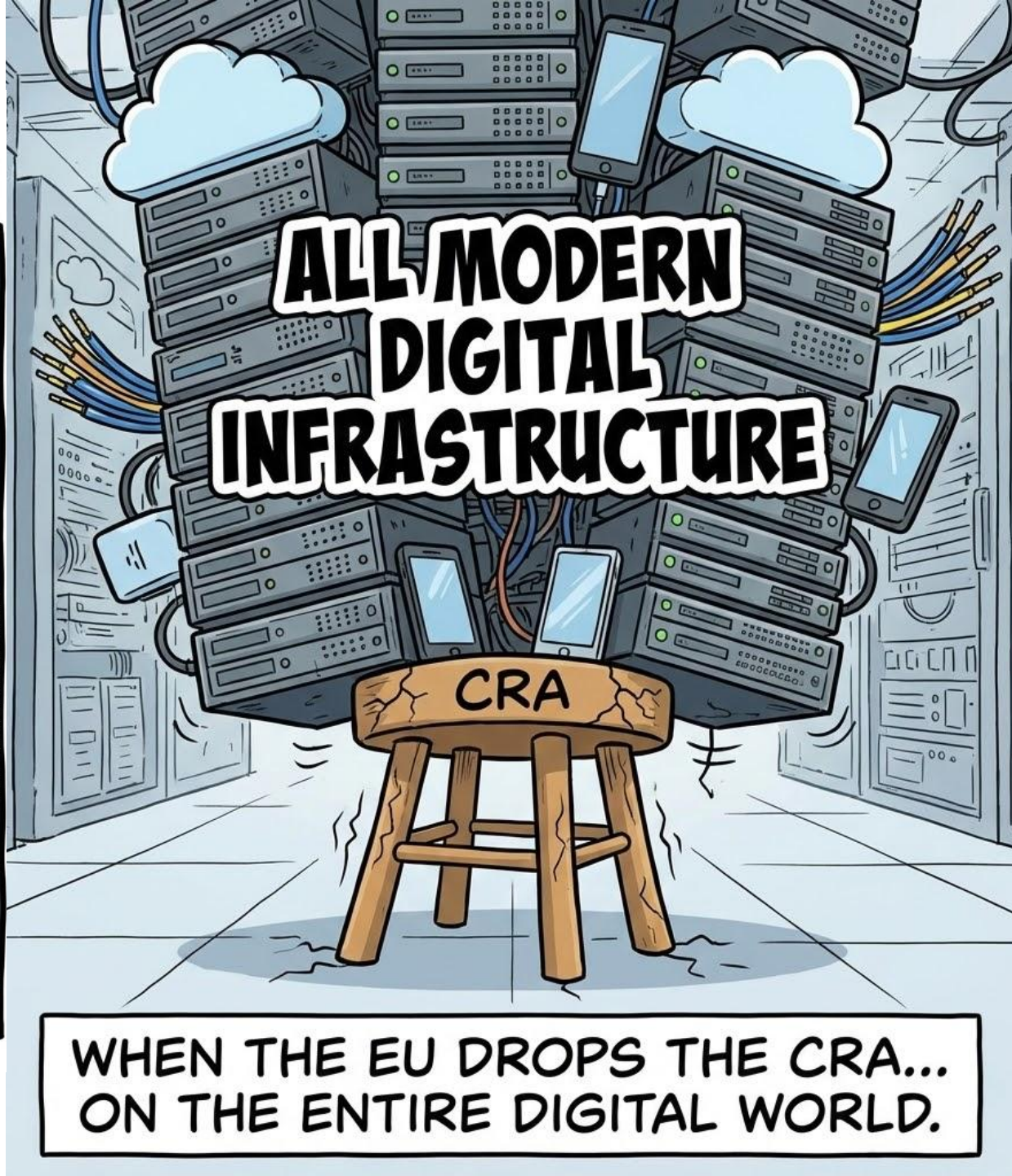
Principal Architect - Security Communities Lead
Expert, the European Standardization Organizations (ESOs)
Security Lead, Maintainer and Contributor to Open Source

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.

THE ART OF CORPORATE COMPLIANCE





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?

Part 1

CRA Basics & Nuances

What is it, who does it affect, and when?

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

CRA is not yet another GDPR, NIS2 or DORA

Outcome-Based

Focuses on results rather than rigid obligations.

NLF* Framework

Uses CE marking and harmonized standards for compliance.

PLD** Linkage

If poor security leads to defective product, it triggers liability.

Massive Scope

Horizontal and vertical coverage of all digital products - everything from SW to HW and devices.

Open Source Recognition

First regulation to acknowledge the criticality of Open Source ecosystems.

*NLF - the EU New Legislative Framework

**PLD - the EU Product Liability Directive

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

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

- Firewalls
- Tamper-resistant CPUs
- Hypervisors and CRS

- HW Devices w/Security Boxes
- Smart meter gateways

Default Category	Important Class I (19)	Important Class II (4)	Critical (3)
Self assessment (Module A)	Self-assessment with harmonised standards (Module A)	3rd Party assessment (Module B+C; Module H)	EU Cert Scheme

Exercise 1:
"In Scope or Out of Scope?"

- I will read out scenarios describing real-world products or situations
- For each one, vote:
  - **IN SCOPE** (raise right hand / green card)
  - **OUT OF SCOPE** (raise left hand / red card)
- After voting, I reveal the correct answer with the CRA reference
- Keep score – winner gets bragging rights!

#1 The Offline Calculator App

A French developer publishes a calculator app on an app store.

The app performs arithmetic entirely offline — no network calls, no analytics, no data sync. It works on a smartphone but never initiates any connection itself.

IN SCOPE or OUT OF SCOPE

#1 The Offline Calculator App

IN SCOPE

Even though the calculator itself doesn’t initiate connections, it runs on a smartphone OS that is connected to a network. This constitutes an indirect logical connection (Art. 3(8), 3(10)).

The app is placed on the market via an app store (commercial distribution channel). It qualifies as a PDE with an indirect data connection.

CRA Art. 2(1); FAQ 1.3; Draft Guidance Section 2.4

#2 A Standalone SaaS Platform

A Danish startup offers a project management tool delivered entirely as a web application. No downloadable client, no plugin, no on-premises component. Users access it via a browser.

IN SCOPE or OUT OF SCOPE

#2 A Standalone SaaS Platform

OUT OF SCOPE

Standalone SaaS that is not designed and developed by a manufacturer as part of a specific PDE does not itself constitute a product with digital elements.

The CRA applies to products placed on the market, not to cloud services.

However, if this SaaS were the remote data processing solution (RDPS) for a specific PDE, it would be in scope as part of that product.

CRA Recital 12; FAQ 1.2; Draft Guidance Section 8

#3 Firmware for a Dishwasher

A manufacturer produces dishwashers with embedded firmware that controls wash cycles. No Wi-Fi, no Bluetooth, no app, no USB data port.

No capability to connect to any network, device, or external system.

IN SCOPE or **OUT OF SCOPE**

#3 Firmware for a Dishwasher

OUT OF SCOPE

While the dishwasher contains software (firmware), its intended purpose does not include any data connection to a device or network.

The third cumulative test (data connection) is NOT met.

The FAQ explicitly lists “a dishwasher with embedded firmware controlling dishwashing cycles, but with no capability to connect” as out of scope.

CRA Art. 2(1); FAQ 1.3

#4 A Python Library

A Dutch company develops a Python data-processing library available for free. It also provides a version with security updates and other optimizations (exact the same name and trademark) to enterprise customers. Source code is delivered as .py files. Customers compile/integrate it into their own products.

IN SCOPE or **OUT OF SCOPE**

#4 A Python Library

IN SCOPE

“Whether computer code is uncompiled, compiled or interpreted is not relevant” to the PDE definition (Draft Guidance Section 2.3).

Source code is available for free (FOSS). However, users must pay to receive the version with security updates (as opposed to get them for free as per CRA requirements).

‘manufacturer’ means a natural or legal person…markets them under its name or trademark, whether for payment, monetisation or free of charge” (Art.3 (13))

The company is the manufacturer; it places source code on the market in a commercial activity. Customer is responsible for their own adaptations.

Draft Guidance Section 3.2, Example 15

#5 A Company Contributing to FOSS

MegaCorp employs 20 engineers contributing full-time to an open-source database project. MegaCorp doesn’t govern it, doesn’t host its infra, and doesn’t sell the DB. It sells a separate commercial product built on top.

IN SCOPE or **OUT OF SCOPE**

#5 A Company Contributing to FOSS

Contributions: OUT (Product: IN)

Contributing source code to FOSS not under MegaCorp's responsibility does NOT make them a manufacturer of that project (Recital 18).

"Manufacturers contributing source code to an open source component do not become responsible for that component's compliance solely by virtue of their contribution."

BUT: MegaCorp's own commercial product IS a PDE placed on the market. MegaCorp has a due diligence obligation when integrating the OSS database.

CRA Recital 18; Draft Guidance Section 3.4; FAQ 4.4.4

Exercise 1: Debrief

CRA scope depends on three cumulative conditions:

- Product with digital elements?
- Placed on the market (commercial activity)?
- Has a data connection?

Most common mistakes:

- Assuming all open source is exempt
- Forgetting that source code sold or supported (notably, security updates) commercially is in scope
- Forgetting that integrators are manufacturers too if they modify and sell a PDE
- Confusing SaaS with RDPS

Part 2

CRA Roles, Obligations and Toolkit

Who does what and how under the CRA?

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.

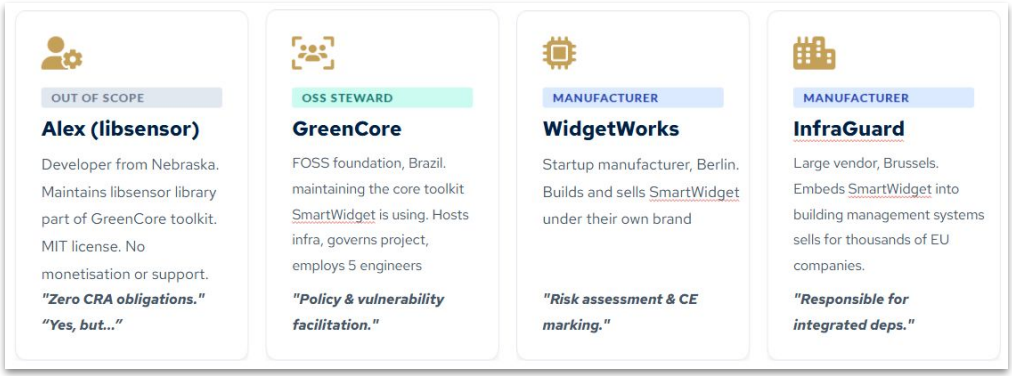
✅ Non-commercial -> Not a Manufacturer

- 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

WidgetWorks: Who is who?



Actor	CRA Role	Why?
Alex (solo maintainer)	Out of scope	Volunteers code to libsensor. No monetisation. Zero CRA obligations even though libsensor is embedded in millions of devices.
GreenCore Foundation	OSS Steward	Hosts and governs the core firmware toolkit. Doesn't sell it. Has some obligations, light-touch regulatory regime.
WidgetWorks	Manufacturer	Develops SmartWidget. Sells it in the EU under their brand. Full CRA obligations for SmartWidget as a manufacturer, including due diligence for libsensor.
InfraGuard	Manufacturer	Integrates SmartWidget into building management systems (BMS), sells it under their brand. Full CRA obligations for BMS as a manufacturer, including due diligence for SmartWidget.

Note: Responsibility always flows **downstream**, never upstream.

Why Red Hat Cares

Red Hat as a Manufacturer

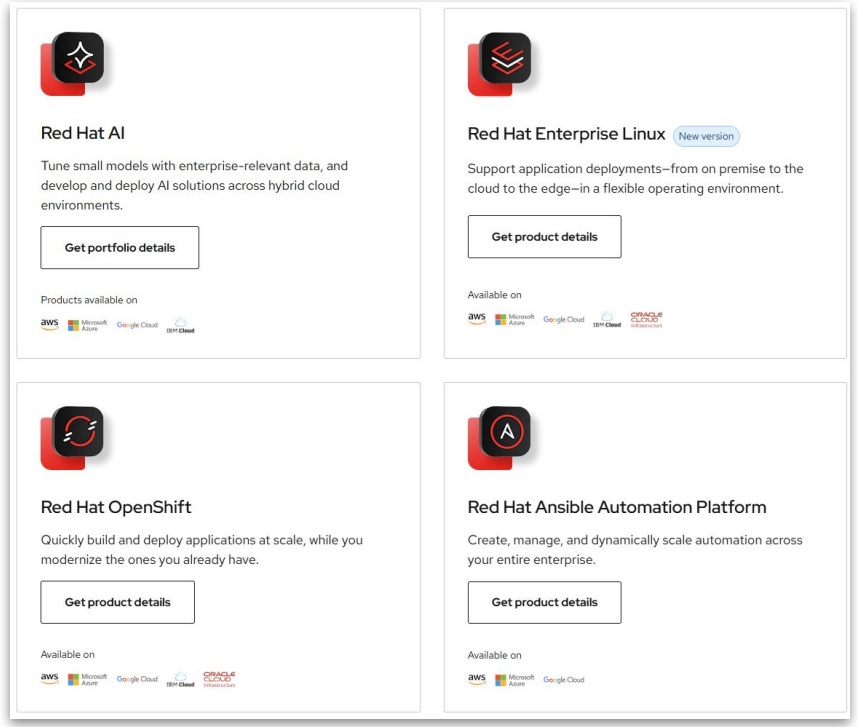
- Provider of enterprise open-source software solutions for the global market, including the EU.

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.



fedora KONFLUX ramalama

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.

THE LINUX FOUNDATION ECLIPSE FOUNDATION CEN CENELEC ETSI EUROPEAN STANDARDIZATION ORGANIZATIONS

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 voluntary 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.

📋 Software Bill of Materials (SBOM)

CRA Rec. 77 & Annex I, Part II

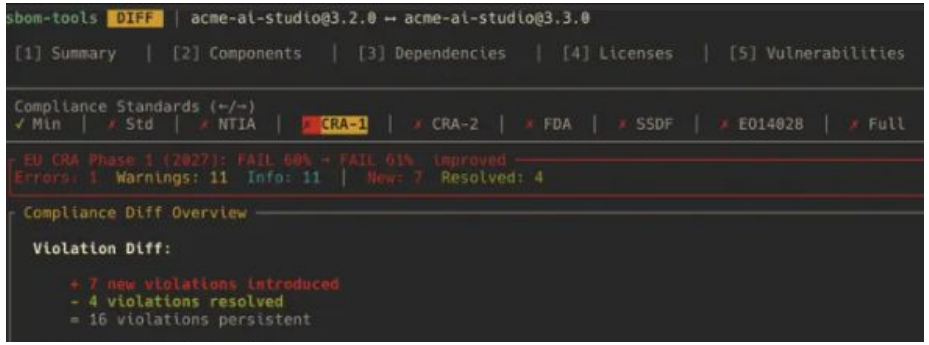
- Identify & document all components in the product – including FOSS dependencies.
- Generate SBOM in a machine-readable format (SPDX, CycloneDX expected).
- Include at minimum: top-level dependencies of the product.
- PT3 Standard may push towards full transitive dependency listing.
- Publishing SBOMs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

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

github.com/RedHatProductSecurity/aegis-ai

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

CRA Annex I, Part I – "Security by design and by default" is not optional

🛡️ **Security by Default** = Ship with the most secure configuration out of the box. No exposed debug ports, default passwords, or unnecessary open services. The user should not need to *harden* the product – the manufacturer already did (to the extent possible).

🏗️ **Security by Design** = Build security into every phase – not as an afterthought. CRA requires documented evidence of this lifecycle.

📋 PLAN	💻 DEVELOP	🔍 VERIFY	📦 RELEASE	🔄 MAINTAIN
Threat modelling	Secure coding standards	Penetration testing	SBOM generation	Security updates (support period)
Security requirements	Peer review & static analysis	Fuzz testing	CE marking & documentation	Incident response & ENISA reporting
Risk-based design decisions	Dependency scanning	Conformity assessment prep	Vulnerability coordination plan	Patch within awareness timeline

Good security practices are not invented by the CRA

Automate compliance posture

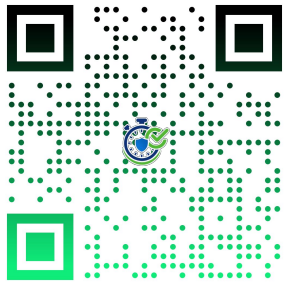
Policy-As-Code and compliance automation across any hybrid inverements.

OpenSSF Gemara:

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

ComplyTime:

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



Turn on security controls

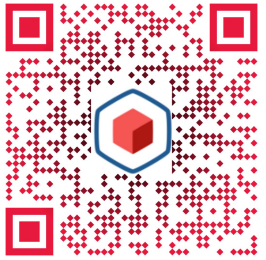
Enable “security-by-default” in an cloud-native manner.

StackRox:

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

Confidential Containers:

HW-baked 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

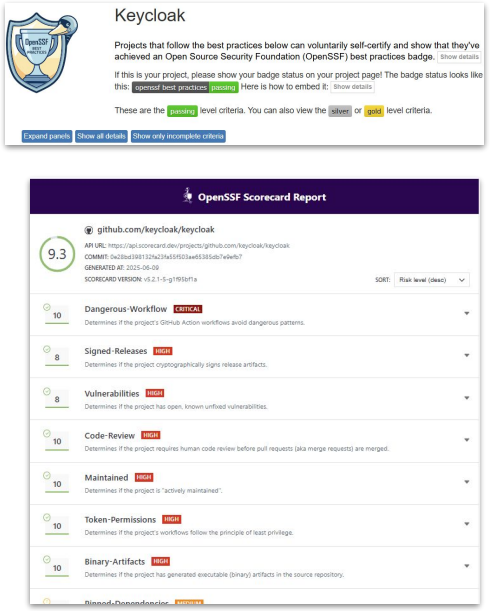
> **Note:** Don't send "CRA Questionnaire" to FOSS as for your supplier. Minimizing the burden on open-source projects will be the key.

FOSS Controls

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

ECLIPSE FOUNDATION — Open Regulatory Compliance

Brainstorm together:
github.com/orcwg



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

THE LINUX FOUNDATION — OpenSSF

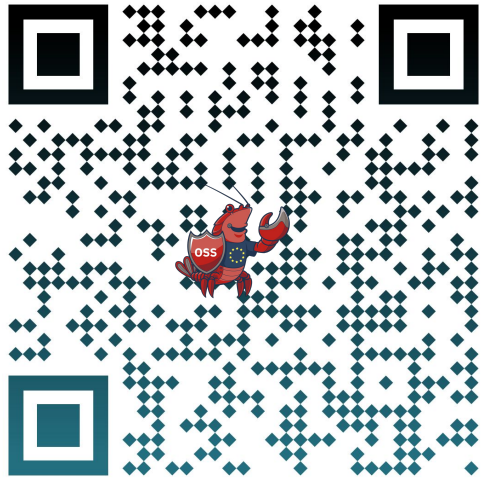
Tooling for Due Diligence:
github.com/ossf/orbit-launchpad

THE LINUX FOUNDATION — OpenSSF

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

Red Hat is Proud To Be a Steward and Committed to Provide a Sustained Support

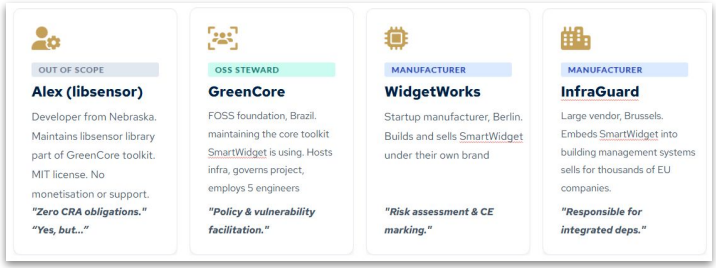
pulp
fedora
KONFLUX
CentOS
okd
ramalama
ANSIBLE
Project QUAY
StackRox
sssd
osbuild
containers
hermeto
iib
maistra



policy.openssf.org/CRA/stewards-playbook.html

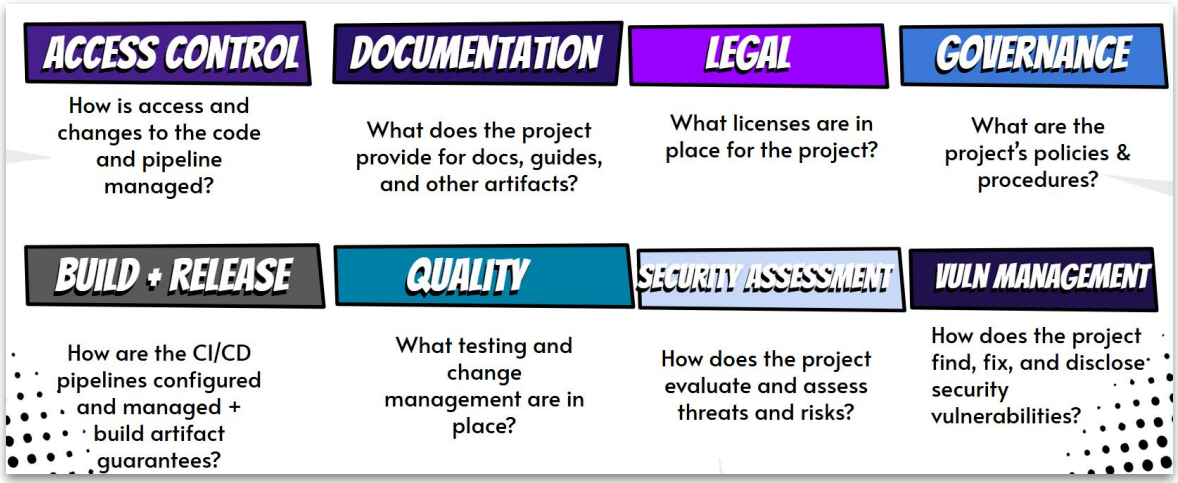
Red Hat constantly evaluates FOSS projects we are a potential Open Source SW Steward for. This list might change in future.

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.*

OpenSSF Baseline – 64 requirements x 3 levels of maturity.



Explore: github.com/ossf/security-baseline

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

- Security Policy
- Security.md vulnerability handling
- SBOMs
- MFA
- Branch Protection
- SLSA - L1
- Signing Commits
- OpenSSF Baseline (OSPS) - L1

Exercise 2:
“Who Am I?”

- Each role card describes a person/entity with a specific situation
- For each card, answer two standard questions plus one card-specific question:
  - **What is my CRA role?**
  - **What are my top 3 obligations?**
  - **A tailored third question (shown on each card)**
- Cards cover: Manufacturer, Distributor, Importer, OSS Steward, Out of Scope, RDPS, incidents, gray zones
- After all we will debrief together

Card 1

“I’m Clara, CTO of SecureNet GmbH”

SecureNet GmbH is an Austrian cybersecurity company. We develop and sell a network firewall appliance to enterprise customers across Europe. The product includes custom hardware and our proprietary firmware. We sell directly and through channel partners. We’re ISO 27001 certified with an in-house security team.

1. What is my CRA role?

2. Top 3 obligations?

3. What am I NOT responsible for?

Card 1

Clara — SecureNet GmbH

MANUFACTURER

Obligations:

- Cybersecurity risk assessment + implement essential requirements (Annex I, Part I)
- Vulnerability handling: SBOM, security updates, coordinated disclosure throughout support period
- Third-party conformity assessment (Module B+C or H) — firewalls are Important Class II
- Report actively exploited vulnerabilities to ENISA: 24h / 72h / 14d

Q3 Answer

Clara is NOT responsible for:

- How her customers configure the firewall after purchase
- Vulnerabilities in third-party products that happen to sit next to hers on the same network
- Guaranteeing zero vulnerabilities (CRA requires process and no known affected CVEs at the placement)

Key point

Firewalls are Important Class II — Clara cannot self-assess. She needs a notified body for conformity assessment. Her ISO 27001 certification helps but does not replace CRA conformity.

Card 2

“I’m Alex, Solo Maintainer of libsensor”

I’m a developer from Ogallala, Nebraska, USA. I created libsensor five years ago as a weekend project. It reads data from environmental sensors. Published on GitHub under MIT license. Used by thousands of projects, including commercial IoT products. No charges, tiny donations (under €500/yr), no commercial support, no formal organisation.

1. What is my CRA role?

2. Top 3 obligations?

3. Do I have to fill out a questionnaire a huge company (manufacturer) sent me?

Card 2 Alex — Solo Maintainer

OUT OF SCOPE

Obligations:

- None.
- Zero.
- The CRA does not apply to Alex.

Q3 Answer

No. Alex cannot be forced to accept CRA obligations via:

- Supplier questionnaires or onboarding forms
- Contractual clauses from downstream companies
- “Responsible disclosure” demands with legal threats

Manufacturers have due diligence duties, but those are THEIR responsibility, not Alex’s.

Key point

Alex does not monetise the project (Recital 18). Donations do not exceed costs. Alex is not placing software on the market in a commercial activity.

Voluntary best practices (SECURITY.md, MFA, OSPS Level 1) are good engineering — NOT legal requirements. No one can compel Alex to adopt them.

Card 3

“I’m Fatima, VP Engineering at HomeSmart”

HomeSmart makes smart thermostats. The device runs our firmware, but the companion app talks to a cloud API hosted entirely by a third-party SaaS provider, ThermoCloud. We have a service agreement with ThermoCloud but no visibility into their security posture. ThermoCloud processes user schedules, temperature data, and firmware update delivery.

1. What is my CRA role?

2. Top 3 obligations?

3. Can I delegate or outsource this obligation?

Card 3

Fatima — HomeSmart

MANUFACTURER (with RDPS)

Obligations:

- The cloud API is an RDPS (Remote Data Processing Solution) — it is part of the product under CRA
- HomeSmart must ensure CRA Annex I requirements are met at the RDPS boundary (data authenticity, integrity, confidentiality, availability)
- Must include the RDPS interface in the cybersecurity risk assessment and conformity assessment

Q3 Answer

You can outsource the operations, but you CANNOT outsource the legal obligation.
You need from ThermoCloud:

- Contractual security commitments mapped to CRA Annex I
- Evidence for conformity assessment (SOC 2, ISO 27001, penetration test results)
- Incident notification SLA aligned with your 24h ENISA obligation

Key point

If ThermoCloud gets breached and user data is exposed, HomeSmart is on the hook — not ThermoCloud. The manufacturer bears the RDPS obligation. Daniil should renegotiate the SLA before Dec 2027, or find a provider willing to give contractual CRA-aligned commitments.

Card 4

“It’s Tuesday morning. A critical CVE just dropped.”

You’re the security lead at WidgetWorks (SmartWidget manufacturer). A critical CVE has been published in log4sensor, a library that libsensor depends on. Your product SmartWidget uses libsensor. You found out through a social media post 6 hours ago. No evidence of active exploitation yet. Your CEO is panicking. What do you do?

1. What is my CRA role?

2. Top 3 obligations?

3. What is the first thing I should do right now?

Card 4

WidgetWorks — CVE Incident

MANUFACTURER (INCIDENT)

Obligations:

- A published CVE alone does NOT trigger the 24h ENISA reporting obligation
- Reporting is triggered by: (a) an actively exploited vulnerability you're aware of, or (b) a severe incident impacting PDE security
- You DO have an obligation to assess impact, remediate, and monitor for exploitation

Q3 Answer

Right now:

- Verify whether log4sensor is actually in your dependency tree (check SBOM)
- Assess exploitability in SmartWidget's context
- Monitor threat intel for active exploitation (CISA KEV, ENISA advisories)
- If NOT actively exploited: patch on your normal cycle, no ENISA report required yet
- If exploitation confirmed: 24h clock starts from the moment you become aware

Key point

Key distinction: CVE ≠ KEV. You don't report every CVE to ENISA. You report actively exploited vulnerabilities (KEVs) that you're aware of. "Becoming aware" means credible evidence of exploitation, not just a CVE publication. But you DO have an ongoing obligation to monitor.

Tell to the company leaders: "We're assessing. No report required yet. We have a process."

Card 5

“I’m Ava, Founder of PixelGuard”

PixelGuard makes an image-processing SDK. The ‘Community’ version is open-source, free, no telemetry, no tracking — but it has a watermark on output images. The ‘Pro’ version removes the watermark and adds GPU acceleration for EUR 99/year. Same codebase, same repo. 80% of our users are on Community. Some EU companies use Community in production.

1. What is my CRA role?

2. Top 3 obligations?

3. Where exactly is the line between in-scope and out-of-scope for my products?

Card 5

Ava — PixelGuard (Freemium)

MANUFACTURER (PRO) + GRAY ZONE (COMMUNITY)

Obligations:

- PixelGuard Pro: clearly a PDE placed on the market — full CRA obligations (conformity, CE, SBOM, reporting)
- PixelGuard Community: the watermark is a feature limitation designed to drive upgrades — this could be interpreted as commercial activity
- FAQ and Draft Guidance indicators: functional limitation to incentivize paid version, same codebase, same brand — all point toward “commercial activity”

Q3 Answer

The line is blurry here. Arguments for in-scope:

- Watermark is a deliberate commercial incentive
- Same codebase under same trademark
- Community edition drives the conversion funnel

Arguments for out-of-scope:

- No telemetry, no payment, truly free
- Watermark could be seen as a feature, not a limitation

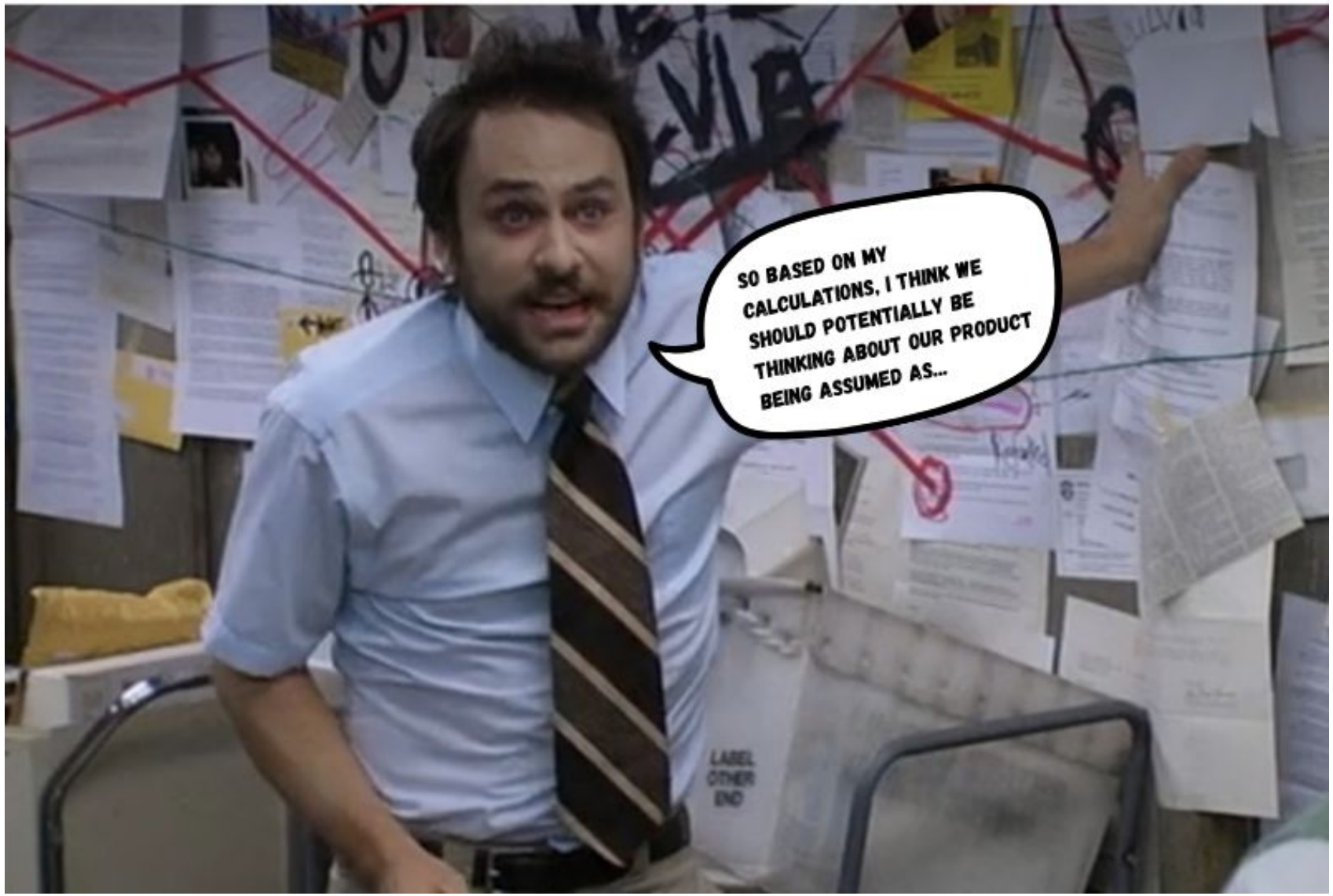
Be prepared to everything.

Key point

This is exactly the “gray zone” the upcoming guidance tries to clarify. The indicators for “commercial activity” include: software published under a trademark associated with a commercial entity, functional limitations designed to push paid upgrades, and integration into a commercial business model. Ava should get legal advice and likely treat Community as in scope to be safe.

Exercise 2: Debrief

CRA Product Classification Flowchart Be Like:



src: https://www.periphery.security/blog/part-2-product-classification---the-hidden-complexity

Exercise 1: Debrief

4 Notable Principles

Downstream Responsibility
Flows downstream, never upstream to OSS maintainers.

Independent Ownership
Each manufacturer in the chain owns their product. No liability outsource.

CVE vs. KEV Focus
Report exploited vulns, not every advisory.

Role Can Evolve
New version, rebranding or acquisition can lead to roles changing..

Watch These “Gray” Zones

Freemium OSS
Features like watermarks or gates may bring "free" software into scope.

App Stores
Distributor or co-manufacturer? Depends on ecosystem control.

Platform + RDPS
Toolkits with cloud consoles create dual manufacturer scenarios.

Forks
A fork is a new product. Cherry-picking is a due diligence decision.

Supplier Failure
Bankruptcy doesn’t end your support period obligations.

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.

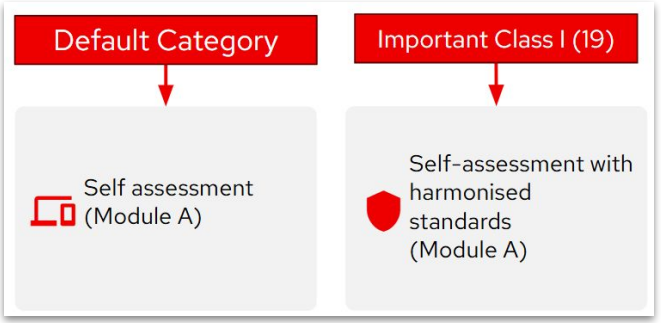
Part 3

CRA Standardization and Implementing Acts Latest Updates

What's happening today and what to expect?

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

CEN CENELEC ETSI
EUROPEAN STANDARDIZATION ORGANIZATIONS



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 *may 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

(Draft) CRA Guidance by the EU Commission

digital-strategy.ec.europa.eu/en/news/commission-publishes-feedback-draft-guidance-assist-companies-applying-cyber-resilience-act

71 amazing pages of practical clarifications for the industry.

Finalized version will be adopted by the Commission by Summer 2026.

Scope Clarification

RDPS & FOSS in scope; Standards boundaries for multi-function products; Physical repairs vs software updates.

Lifecycle Predictability

Support Periods (incl. Recital 60 & commercial FOSS realities); Substantial modifications; EOL; Resetting the clock.

Vulnerability Handling

Standardized Risk Assessments & "Nearly-Zero-CVE" posture tracking.

Along with CRA FAQ it impacts the entire ecosystem

Manufacturers

Clear role identification flow & 3rd-party component handling.

Importers

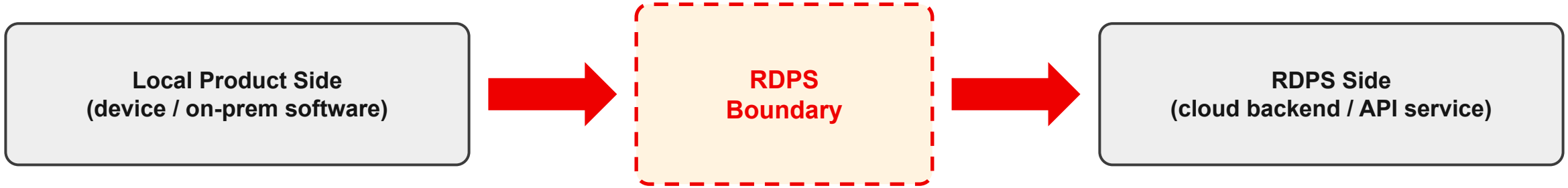
Guidance on avoiding "accidental manufacturer" status via repairs.

FOSS Maintainers and Stewards

Boundaries for community vs. commercial placement.

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.

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.

Exercise 3:
"Live Gap Analysis"

1. **IDENTIFY THE CRA ROLES**
2. **RUN THE CHECKLIST**
3. **IDENTIFY TOP 3 GAPS AND 1 ACTION ITEM FOR THIS MONTH**

Alex

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

GreenCore

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

WidgetWorks

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

InfraGuard

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

Checklist — WidgetWorks

#	Item	✅/❌	Comment
A1	Does WidgetWorks have a documented risk assessment for SmartWidget?	❌	*Startup — probably informal only*
A4	Does the risk assessment cover libsensor and the cloud backend?	❌	*Likely unaware of transitive deps*
B2	Is SmartWidget shipped without known exploitable vulnerabilities?	?	*Ask: do they scan before release?*
B9	Is there a secure update mechanism for firmware in the field?	?	*Critical for IoT — OTA updates?*
C1	Is there a vulnerability handling policy documented?	❌	*Startup may lack formal process*
C3	Is there a CVD process? Can researchers report securely?	❌	*No SECURITY.md yet?*
C7	Is there an SBOM for SmartWidget?	❌	*Key gap for most orgs*
D1	Has WidgetWorks identified its conformity module? (A for default PDE)	❌	*May not even know about this*
D5	Is the support period defined and communicated?	❌	*Common omission*
E1	Is WidgetWorks registered on ENISA SRP? (needed by Sep 2026)	❌	*Probably not yet*

WidgetWorks – Top 3 Gaps & Action

1

Gap: No SBOM

Impact: Can't trace what's inside SmartWidget. Can't do due diligence on libsensor. Can't meet Annex I Part II.

Quick win: Integrate CycloneDX/SPDX into CI pipeline

2

Gap: No vulnerability handling process

Impact: No SECURITY.md, no CVD policy, no way for researchers to report. If a vuln is found, no defined response.

Quick win: Create SECURITY.md from template; define triage + response workflow

3

Gap: No Risk Assessment

Impact: Risk assessment is not only one of the essential requirements, but is instrumental to identify other actions (like other requirements applicability and reporting).

Quick win: Introduce Threat Modelling (OWASP Threat Dragon / STRIDE) to your processes (documenting is key)

WidgetWorks' ONE ACTION this month:

"Generate our first SBOM using one of the popular SBOM tools, integrate it into CI, and review what's actually inside SmartWidget."
By when: end of this month

Takeaways

SmartWidget's Happy End

OUT OF SCOPE

Alex (libsensor)

Action: Voluntary SECURITY.md, MFA, branch protection, OSPS L1

Result: *More attractive project, less downstream harassment.*

OSS STEWARD

GreenCore

Action: Cybersecurity policy, coordinated vulnerability disclosure.

Result: *Trusted and covered upstream, easier adoption.*

MANUFACTURER

WidgetWorks

Action: Risk assessment, Vulnerability process, SBOM.

Result: *Clear CRA conformity path with achievable deadline.*

MANUFACTURER

InfraGuard

Action: Due diligence on SmartWidget, own CRA Program, invest money into GreenCore and libsensor.

Result: *CE-marked building system, trusted enterprise supplier, FOSS supporter.*


CRA: EU CYBER RESILIENCE ACT -
COLLABORATION FOR A SECURE FUTURE!
Yay!
Yay!
Collaboration!
Secure Supply Chain!
OSS MAINTAINER
OS SW STEWARD
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

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)	

Building secure future for all.

Open source way.

LINKEDIN.COM/IN/ROZHUKOV

linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

facebook.com/redhatinc

twitter.com/RedHat