From Manufacturer to Steward: Red Hat's Approach to CRA Readiness

Roman Zhukov

Principal Architect - Security Communities Lead

DISCLAIMER

Nothing in this presentation is a legal advise.

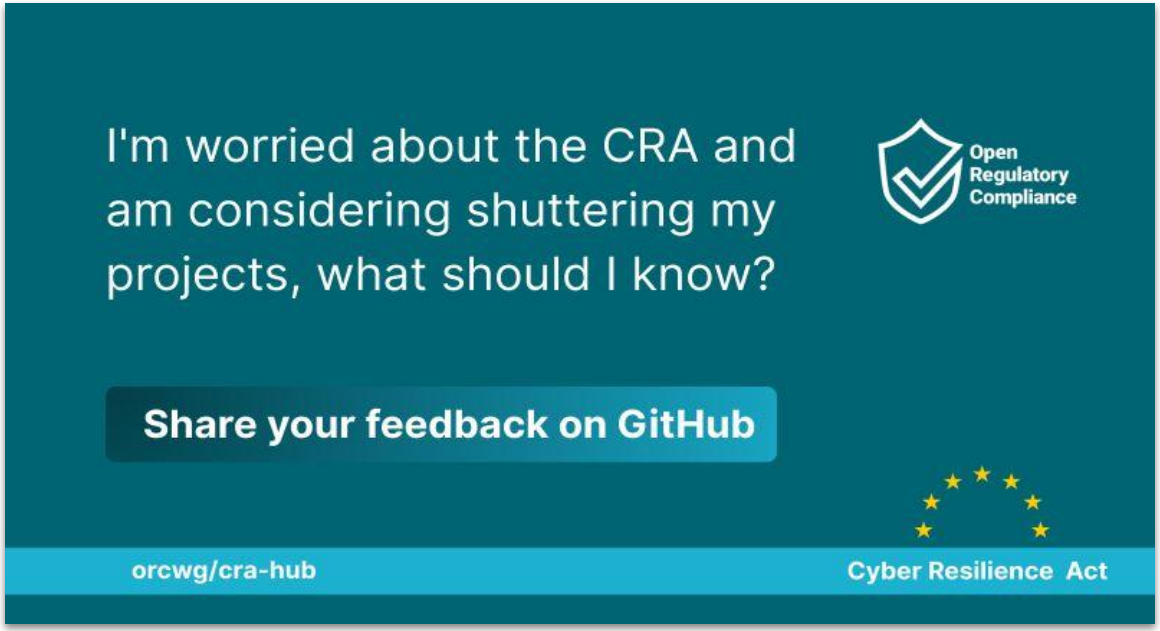
EU CRA is one of the most complex tech legislations which is still under implementation development.

Don't consider this material as a finalized position or an official statement.

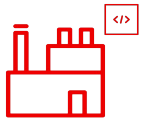
Red Hat

> CRA has a potential to make **more for supply-chain security** and OSS ecosystem health at scale **in just a few years** than
>
> we, as a minority of security experts in the engineering community, have been trying to make in decades.

OSS Security Community


I'm worried about the CRA and am considering shuttering my projects, what should I know?
Open Regulatory Compliance
Share your feedback on GitHub
orcwg/cra-hub
Cyber Resilience Act

Important OSS Roles in CRA



Manufacturer - natural or legal person who develops PDEs.

Importer and **Distributor** - re-sells PDEs.

OSS **Contributor** (**Developer**) - entirely out of scope as per Recital 18.

OSS **Maintainer** - out of scope if doesn't monetize project.

OSS **Steward** - systematically supports OSS projects.

Important OSS Roles in CRA

Manufacturer - natural or legal person who develops PDEs.

Most of obligations

Importer and **Distributor** - re-sells PDEs.

Ensures Manufacturer's done a good job

OSS **Contributor** (**Developer**) - entirely out of scope as per Recital 18.

OSS **Maintainer** - out of scope if doesn't monetize project.

Most of the OSS projects will not have a Steward

New

OSS **Steward** - systematically supports OSS projects.

Red Hat roles in CRA

Red Hat as a Manufacturer

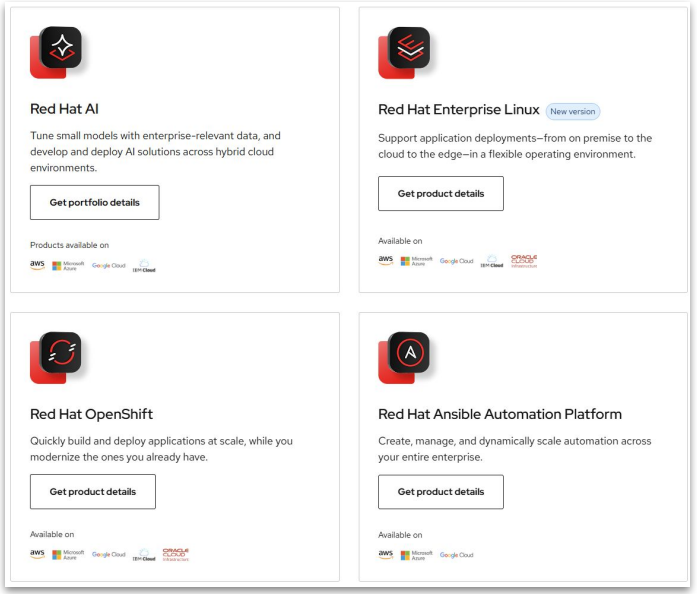
- Provider of enterprise open-source software solutions for the global market, including the EU.

Red Hat as a potential Open Source Software Steward

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

Red Hatters are Contributors and Maintainers

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



Red Hat roles in CRA

Red Hat as a Manufacturer

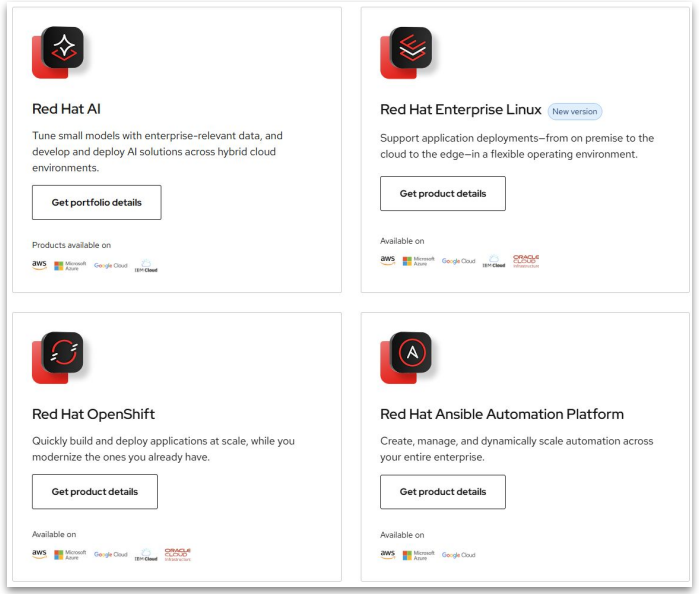
- Provider of enterprise open-source software solutions for the global market, including the EU.

Red Hat as a potential Open Source Software Steward

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

Red Hatters are Contributors and Maintainers

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

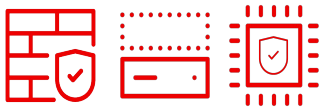


Yes, we do care about open-source ecosystem and are committed to support it.

What we manufacture*

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

Important Class I (19)



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

Important Class II (4)

- HW Devices w/Security Boxes
- Smart meter gateways

Critical (3)

- Consumer devices and everything else
- **All SW (incl. FOSS)**

Default Category

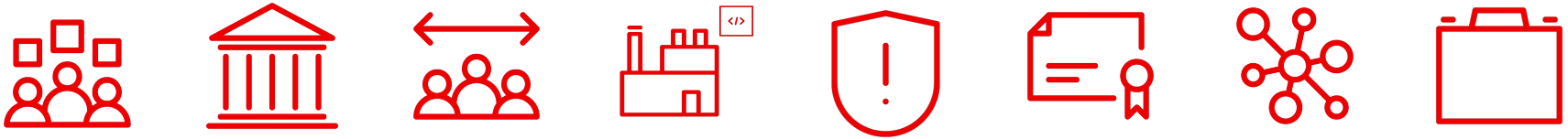
The rest 90%

* Based on current interpretation of the Draft Technical Descriptions of Important and Critical PDEs.

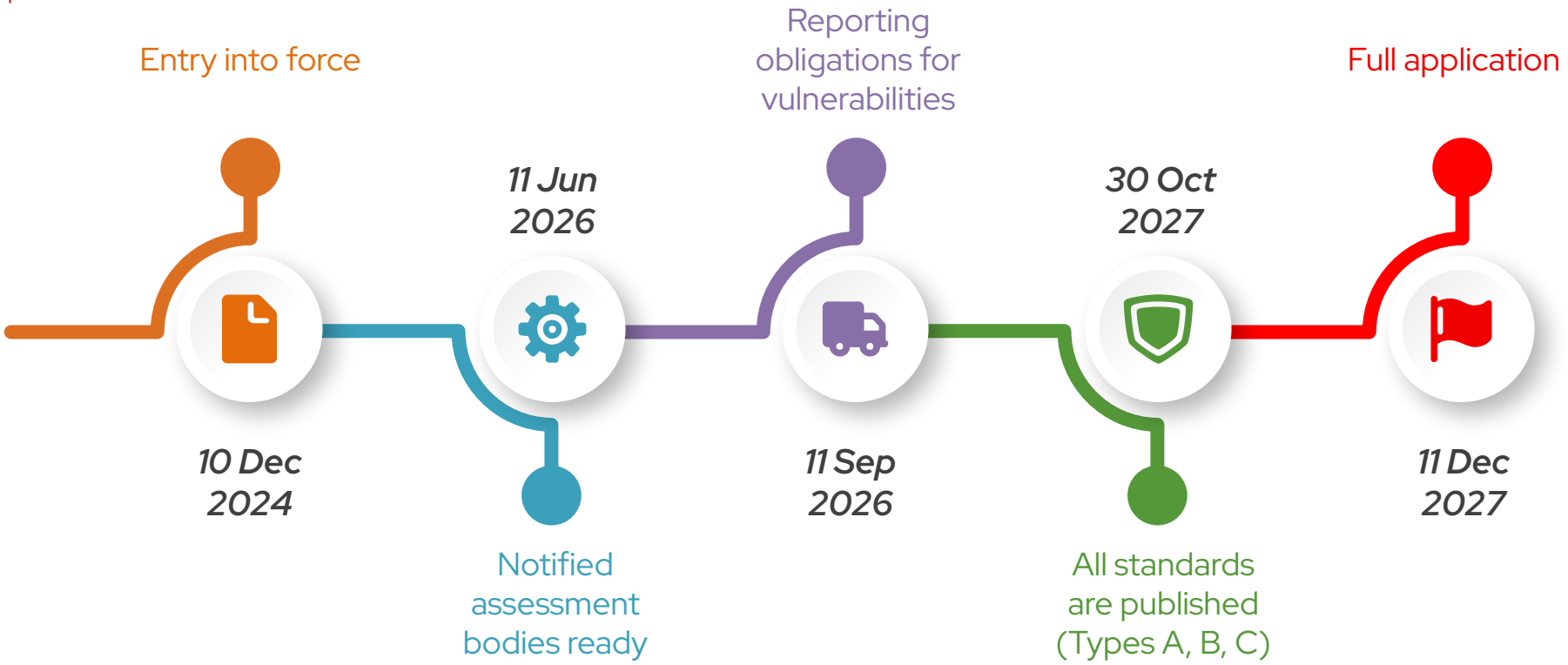
Red Hat CRA Program

Red Hat CRA Program Structure - 8 Workstreams

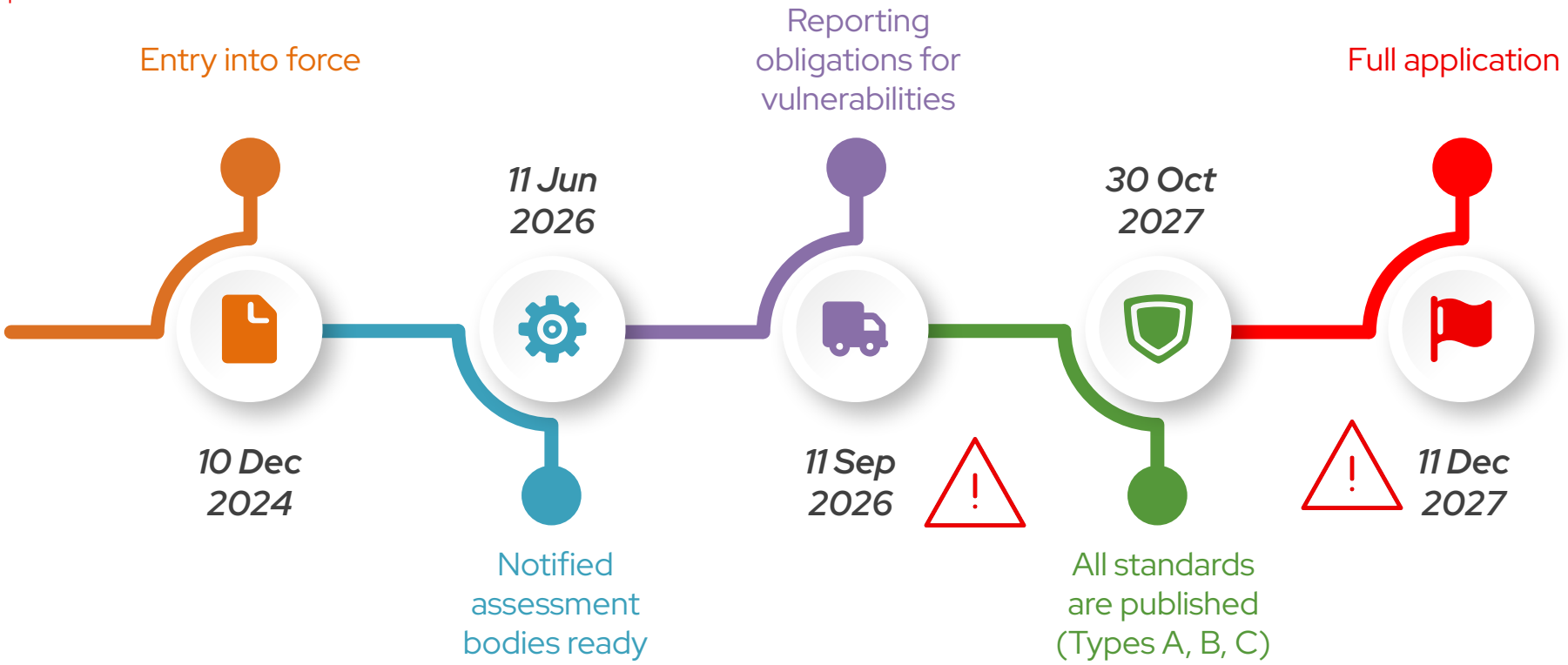
Awareness & Communications	Participation in EU Standards Development	Upstream Engagement & Contributions	Manufacturer & Steward Obligations	Vuln Mgmt / Incident Response Obligations	Conformity & Certification	Data Collection	Legal
Prepare internal and external CRA comms and training	Coordinate interactions with standardization bodies to provide Red Hat's expertise and advocate for open source	Coordinate interactions with foundations and upstream communities regarding CRA	Align the CRA with Red Hat's SDLC practices to ensure all requirements are understood	Ensure VM/IR policies and processes met CRA requirements and reporting obligations	Define the processes for Red Hat software to attest it has met the CRA requirements	Gather metrics to evaluate resourcing & investments for CRA	Support for other workstreams, develop internal CRA guidance, review deliverables



CRA timeline



CRA timeline

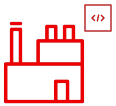


Red Hat CRA Program

- Develop communications and training around Red Hat's approach to the CRA and how our expertise will guide both internal efforts and external engagement.
- Evaluate and report on CRA activities and ensure all business areas have the necessary support.
- Ensure we are correctly interpreting the legalese and that all necessary legal requirements, obligations, and protections are being addressed.

Red Hat CRA Program

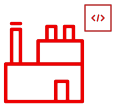
Manufac-turer Obligations



- Analyze the CRA and upcoming standards to ensure alignment with Red Hat's secure software development and delivery policies, standards, guidance, and practices.
- Analyze reporting and documentation requirements related to all the CRA obligations and ensure mechanisms are in place to meet them.
- Plan how to exercise due diligence as FOSS ecosystem is inconsistent.

Red Hat CRA Program

Manufac-turer Obligations



- Analyze the CRA and upcoming standards to ensure alignment with Red Hat's secure software development and delivery policies, standards, guidance, and practices.
- Analyze reporting and documentation requirements related to all the CRA obligations and ensure mechanisms are in place to meet them.
- Plan how to exercise due diligence as FOSS ecosystem is inconsistent.

Vuln Mgmt / Incident Response Obligations

- Ensure that Red Hat's Vulnerability Mgmt / Incident Response capabilities can meet the CRA requirements and upcoming standards.
- Ensure SBOMs are generated and made available.
- Ensure processes are in place to monitor and report on exploited vulnerabilities and severe incidents (reporting mechanisms to ENISA and national CSIRTs are work-in-progress).

Red Hat CRA Program

Steward Obligations

- Open Source projects inventory.
- Determine Stewardship scope and obligations, coordinate gap analysis and facilitate guidance to upstream projects.
- Collaboration with other FOSS Stewards (e.g. foundations).

Red Hat CRA Program

Steward Obligations

- Open Source projects inventory.
- Determine Stewardship scope and obligations, coordinate gap analysis and facilitate guidance to upstream projects.
- Collaboration with other FOSS Stewards (e.g. foundations).

Upstream Engagement & Contributions

- Engage with open source communities to spread awareness of the CRA requirements.
- Share Red Hat's knowledge and expertise to enable OSS ecosystem to plan for and meet the CRA requirements.
- Provide VM/IR guidance to upstream projects.

Red Hat CRA Program

Participation in EU Standards Bodies

- Engage with standardization bodies to advocate for requirements that are practical, align with open source principles, and consider the capabilities of FOSS projects.
- Monitor standardization work so we can proactively plan.
- Support interoperability with existing industry standards and practices.

Red Hat CRA Program

Participation in EU Standards Bodies

- Engage with standardization bodies to advocate for requirements that are practical, align with open source principles, and consider the capabilities of FOSS projects.
- Monitor standardization work so we can proactively plan.
- Support interoperability with existing industry standards and practices.

Conformity & Certification

- Assessments and producing Declarations of Conformity.
- Ensure Red Hat meets all CRA conformity and certification requirements, specifically for Critical and Important PDEs.
- Coordinate work with Third-Party Assessment Organizations (3PAO) as needed, such as Notified Bodies (NB) and Conformity Assessment Body (CAB).

Challenges and Lessons Learned

Ambiguity – “commercial activity”, “actively exploited vulnerabilities”.

Unknowns – standards and implementing documents are work in progress.

41 standards (!) – just to maintain awareness is challenging.

Timeline – no gap between standards are completed and enforcement.

Roles extension – how far will we go in support of the FOSS ecosystem?

Takeaways

Start making your PDE (product and project) **inventory now**.

Understand all **CRA roles** applicability to you and do gap analysis.

To **be CRA compliant** – continue to follow **industry best practices.**

Timeline is tight – start planning CRA now, be prepared to adjust.

Get engaged – industry needs more voices to make CRA actionable.

LET'S MAKE OUR FUTURE OPEN AND SECURE. FOR ALL.

LINKEDIN.COM/IN/ROZHUKOV

linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

facebook.com/redhatinc

twitter.com/RedHat

Red Hat