OpenSSF Tech Talk

CRA-Ready: How to Prepare Your Open Source Project for EU Cybersecurity Regulations

June 12, 1-2PM ET

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Welcome!

- Thank you for joining us today! We will begin at 10:02am PT.
- While we wait for everyone to join, please take a moment to do one (or more) of the following:
  - Please add questions using the Zoom Q&A feature
  - Follow us on Twitter: @openssf, Mastodon: social.lfx.dev/@openssf, & LinkedIn: OpenSSF
  - Visit our website: https://openssf.org
  - Sign up for training: https://openssf.org/training/courses/
- This Tech Talk is being recorded

Education

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Agenda

- Housekeeping
- Speaker Introductions
- Understanding CRA
- Unaware & Uncertain
- How Organizations Are Preparing?
- How the LFEL1001 Course Supports Readiness?
- Panel Discussion & Audience Q&A
- Important announcements

Help us improve! Tech Talk Survey

Education

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Antitrust Policy Notice

Linux Foundation meetings **involve participation by industry competitors**, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at **http://www.linuxfoundation.org/antitrust-policy**. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

Code of Conduct

- The Linux Foundation and its project communities are **dedicated to providing a harassment-free experience** for participants at all of our events, whether they are held in person or virtually.
- All event participants, whether they are attending an in-person event or a virtual event, **are expected to behave in accordance with professional standards**, with both this Code of Conduct as well as their respective employer's policies governing appropriate workplace behavior and applicable laws.
- https://openssf.org/community/code-of-conduct/

Disclaimer

The information provided in this webinar is for general informational purposes only and does not constitute legal advice.

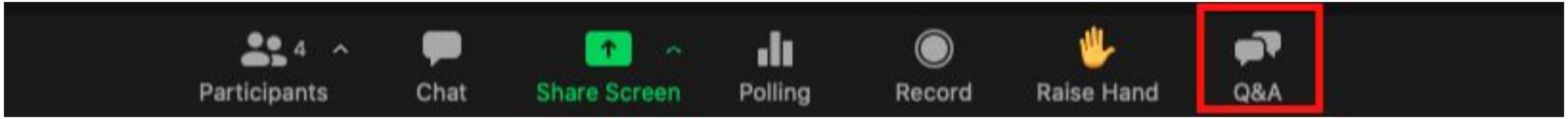
We are not your lawyers.

For advice tailored to your specific situation, please consult with a qualified legal professional.

Generated by Microsoft Image Designer "In the style of pixar, show a fun-loving lawyer weasel"

Q&A

Please submit your questions during the meeting by using the Q&A feature on Zoom.



Thank you!

Introductions

Christopher “CRob” Robinson

Christopher “CRob” Robinson - Security Lorax, Chief Architect of OpenSSF, Linux Foundation

Christopher Robinson (aka CRob) is the Chief Security Architect for the Open Source Software Foundation (OpenSSF). With over 27 years of experience in engineering and leadership, he has worked with Fortune 500 companies in industries like finance, healthcare, and manufacturing, and spent six years as Program Architect for Red Hat’s Product Security team.

CRob has spoken at major events such as RSA, BlackHat, and DefCon, and was recognized as a top presenter at Red Hat Summits in 2017 and 2018. He holds certifications like CISSP and CSSLP. He leads several OpenSSF working groups, chaired its Technical Advisory Committee, and contributes to the FIRST PSIRT SIG.

CRob enjoys hats, herding cats, and moonlit beach walks.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Adrienn Lawson, Director of Quantitative Research, Linux Foundation

Adrienn serves as Director of Quantitative Research at the Linux Foundation, where she leads data-driven initiatives to understand open source ecosystems. With expertise in social data science from the University of Oxford and a background spanning academic and governmental research, she brings methodological rigor to analyzing distributed collaboration networks. At the Linux Foundation, Adrienn leads a team conducting cross-sectional research across industry verticals and geographic regions to provide comprehensive insights into open source dynamics. Her work encompasses empirical investigations into regulatory compliance, the implications of AI, and sustainable funding models. She produces evidence-based recommendations that inform strategic decision-making within the open source community.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Dave Russo, Product Security Governance Portfolio Manager, Red Hat

Dave Russo has over 30 years of IT experience in Development, Security, Enterprise Operations, Architecture, and Support. He holds a Certified Secure Software Lifecycle Professional (CSSLP) certification, and is a member of multiple Open Source Security Foundation (OpenSSF) working groups. Dave is the Product Security Governance Portfolio Manager at Red Hat, where he focuses on Secure SDLC practices and herding cats.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

David A. Wheeler, Director of Open Source Supply Chain Security at OpenSSF, Linux Foundation

Dr. David A. Wheeler is an expert on open source software (OSS) and on developing secure software. His works include the courses Open Source Security Foundation (OpenSSF) Developing Secure Software (LFD121) and Understanding the EU Cyber Resilience Act (CRA) (LFEL1001). He is the Director of Open Source Supply Chain Security at the Linux Foundation and teaches a graduate course in developing secure software at George Mason University (GMU). Dr. Wheeler has a PhD in Information Technology, a Master's in Computer Science, is a Certified Information Systems Security Professional (CISSP), and is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE).

Understanding the CRA

David A. Wheeler

Director of Open Source Supply Chain Security
The Linux Foundation

Understanding CRA

1. What the CRA is and why it matters
2. When CRA applies to OSS
3. Key obligations for OSS maintainers and vendors
4. Debunking common misconceptions
5. What's changing—and what's still evolving

What the CRA is and why it matters

- Cyber Resilience Act (CRA) is European Union (EU) regulation 2024/2847
  - Law entered into force on 2024-12-10
  - Some reporting required 2026-09-11, full requirements 2027-12-11
- Applies to “products with digital elements (PDEs) made available on EU market”
- Aims for the development of secure PDEs
- First broad law applying to *lots* of software *globally*
  - Applies ***even if*** developer(s) are not located in the EU
  - Penalties up to €15M or 2.5% worldwide annual turnover (whichever is greater)

When CRA applies to OSS

Often does *not* apply to OSS. Don’t need to *worry* about CRA if you are only:

1. Contributing to others’ Open Source Software (OSS) projects
2. Publishing OSS code in your own repository & not trying to monetize it
3. Providing web sites/services not part of remote data processing of a product

Applies to PDEs “supplied for distribution or use in course of a commercial activity” e.g.:

1. Charging a fee for a PDE
2. Charging for technical support services beyond their actual costs
3. Providing a software platform through which the manufacturer monetizes other services
4. Requiring personal data (other than very narrow reasons)

These make you a “Manufacturer”; an org other than a manufacturer who routinely supports OSS may be an “OSS steward”

Coming soon: *Cyber Resilience Act (CRA) Brief Guide for Open Source Software (OSS) Developers*

Key obligations for OSS maintainers and vendors

- Manufacturer = “a natural or legal person who develops or manufactures PDEs or has PDEs designed, developed or manufactured, and markets them [in EU] under its name or trademark, whether for payment, monetisation or free of charge”
  - Risk management, design, development, and production of PDEs for cybersecurity
  - Vulnerability reporting, severe incident reporting, & vulnerability handling
- An OSS project that’s a manufacturer has a number of obligations
- All manufacturers have requirements that affect their relationship with OSS:
  - Must exercise due diligence when integrating components sourced from third parties [13(5)]
  - If component vulnerability found, must report to maintainer, including fix if created [13(6)]

Manufacturers have many requirements under CRA

Highlights:

1. Design, develop & produce per *essential cybersecurity requirements* in I Part I [13(1)]
2. *Assess cybersecurity risks*, apply throughout lifecycle, min. cybersecurity risks [13(2)]
3. *Document/update* cybersecurity risk assessment [13(3-4)]
4. Exercise *due diligence* when integrating 3rd party components including OSS [13(5)]
5. If component vulnerability found, *report* to component maintainer [13(6)]
6. Various *vulnerability reporting* & handling (usually 5+ year), see Annex I Part II [13(8)]
7. Create *technical documentation* per article 31 & annex VII [13(12)]
8. Designate vulnerability single *point-of-contact* [13(17)]
9. *Info* for user per Annex II [13(18)]
10. *Assess conformity* per article 32 & Annex VIII
11. Must *report* vulnerabilities & incidents per article 14

Debunking common misconceptions

- Myth: CRA directly applies to all OSS
- Myth: CRA never applies to OSS
- Myth: CRA won’t impact OSS
  - Widely affects many users of OSS & will require reporting to OSS projects
  - Manufacturers “shall exercise due diligence… from third parties” [13(5)]
  - If component vulnerability found, manufacturer reports to maintainer [13(6)]
- Myth: CRA requires software to be perfect
  - Requires effort for security by design AND process in place to report/address vulnerabilities

What’s changing—and what’s still evolving

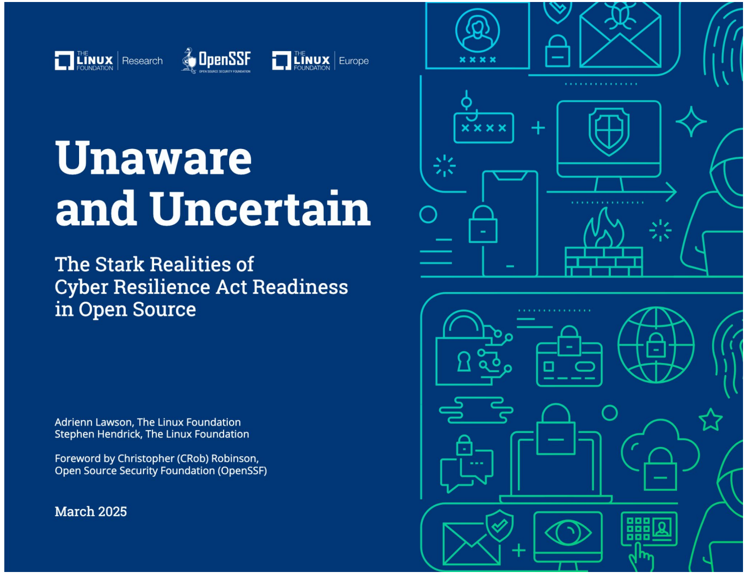
- CRA imposes a number of high-level requirements on manufacturers
  - Intentionally high level (vague)
- EU in process of developing standards to provide more detail
  - Standards are *optional* but provide more legal certainty
  - In some cases standards will provide a *presumption of conformity* (but not all will!)

Unaware and Uncertain

Adrienn Lawson

Director of Quantitative Research, Linux Foundation

Methodology



THE LINUX FOUNDATION | Research OpenSSF THE LINUX FOUNDATION | Europe

Unaware and Uncertain

The Stark Realities of Cyber Resilience Act Readiness in Open Source

Adrienn Lawson, The Linux Foundation
Stephen Hendrick, The Linux Foundation

Foreword by Christopher (CRob) Robinson,
Open Source Security Foundation (OpenSSF)

March 2025

The study is based on a web survey conducted by LF Research and OpenSSF in January 2025.

A total of 685 respondents completed the awareness section of the survey. The sample size for manufacturers is 180. For stewards, it is 34, and for non-commercial OSS contributors, it is 126.

CRA overall awareness is low

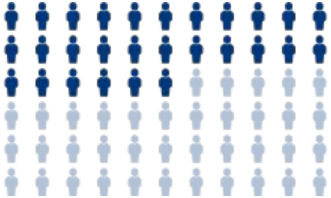
62%

Overall awareness is low, with 62% being "not familiar at all" or only "slightly familiar" with the CRA

2025 CRA Survey, Q18. Sample size = 685

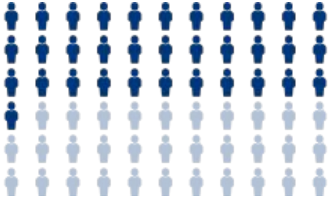
Specific knowledge gaps: findings from CRA-aware respondents

42%



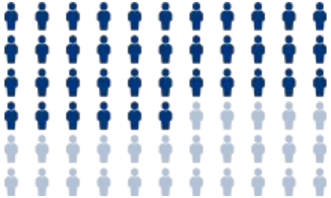
haven't determined whether the CRA applies to them at all

51%



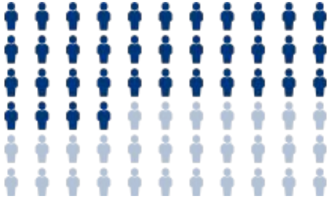
uncertain about compliance deadlines – with only 28% correctly identifying 2027 as the target year for full compliance

59%



are unaware of the penalties of CRA non-compliance

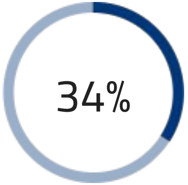
56%



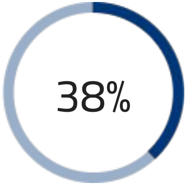
do not understand the crucial distinction between manufacturers and stewards under the CRA

2025 CRA Survey, Q24, Q22, Q25. Sample size = 384, shown to CRA-aware respondents)

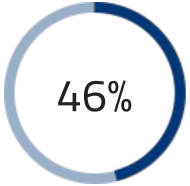
Current interaction patterns between manufacturers and their OSS components in use



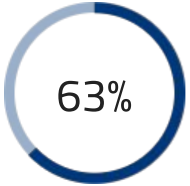
One out of three manufacturers produce SBOMs for all of their products.



Security assessment of OSS components remains low at 38% for manufacturers.



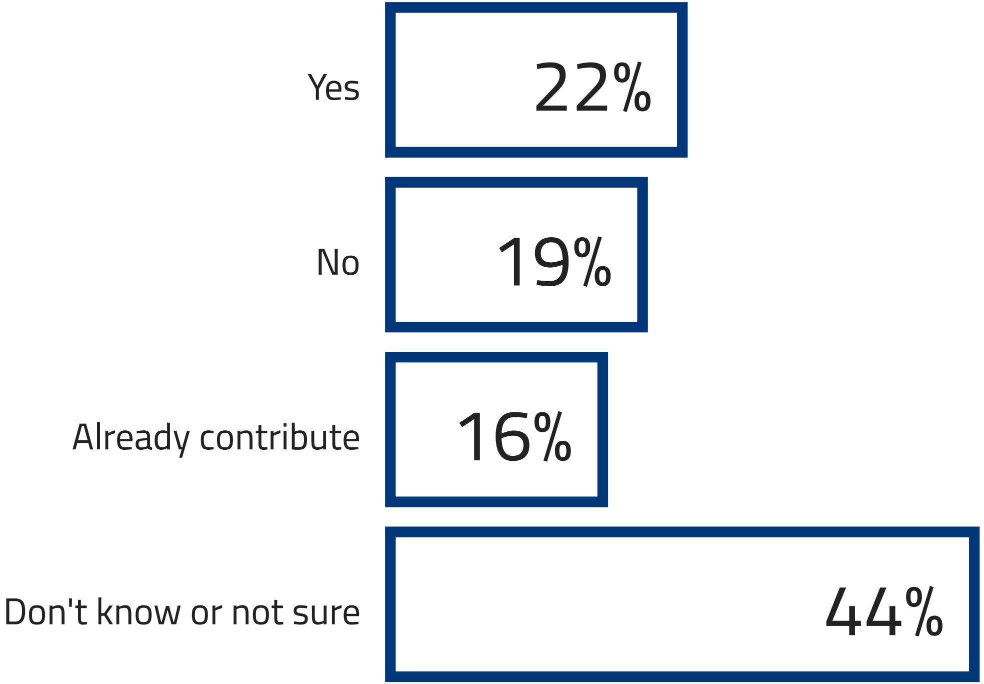
Nearly half (46%) passively rely on upstream projects for security fixes.



63% of manufacturers do not yet plan to contribute security fixes once CRA goes into effect *(full chart on next slide)*

2025 CRA Survey, Q28, Q30, Q29, Q34. Sample size = 180–205 (shown to manufacturers)

Manufacturer contribution plans under the CRA

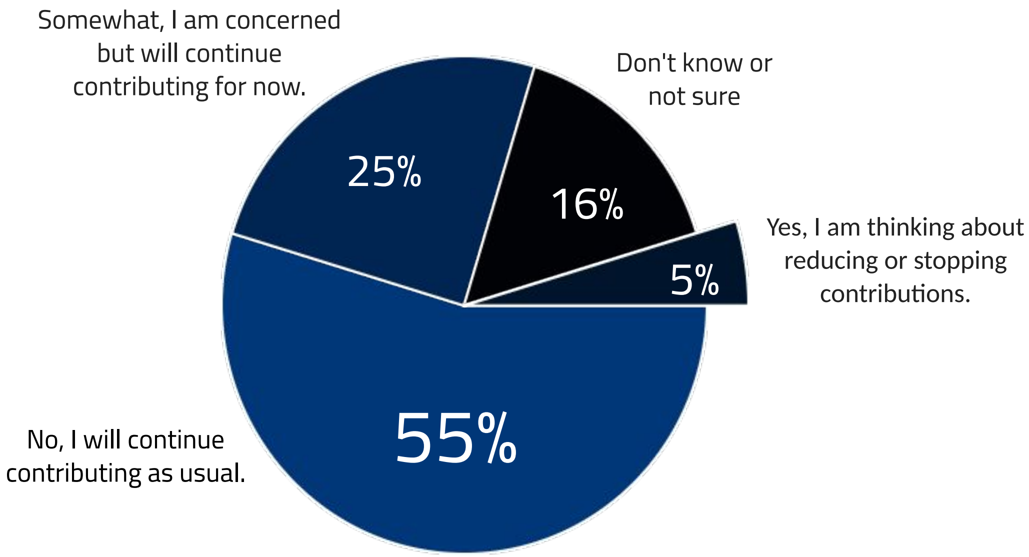


Does your organization have a plan to contribute cybersecurity fixes upstream once the CRA goes into effect? (select one)

2025 CRA Survey, Q34. Sample size = 180, shown to manufacturers

CRA's potential impact on non-commercial OSS contributions

Does the potential impact of the CRA make you reconsider contributing to OSS? (select one)



2025 CRA Survey, Q54. Sample size = 126, (shown to non-commercial OSS developers)

How Organizations Are Preparing for the CRA?

Dave Russo

Product Security Governance Portfolio Manager, Red Hat

Disclaimer

This presentation is not legal advice. The intent of this presentation it to inform interested parties about the considerations Red Hat has taken when developing and executing its internal CRA Program. This information may or may not be relevant to other businesses or organizations. Everyone is strongly encouraged to consult their own legal advisors to determine how the CRA legislation affects them.

How does the CRA affect Red Hat?

Red Hat is a leading provider of enterprise open-source software solutions. Its core strategy revolves around AI and hybrid cloud enablement, offering a comprehensive portfolio of technologies built on open standards and community collaboration. Red Hat's business model is primarily subscription-based, providing enterprise-grade support, integration services, security patches, and strategic guidance for its open-source products. This ensures continuous value for customers beyond just the software itself.

Red Hat's business reach is global, serving a vast array of industries and organizations, including a significant portion of Fortune 500 companies. Red Hat also has a broad partner ecosystem, working with cloud providers, hardware manufacturers, software vendors, and systems integrators to extend its solutions and support its customers' diverse IT needs.

Red Hat's identity and business strategy are fundamentally rooted in open source principles of freedom, community, and sustainability. It actively develops, contributes to, and maintains open source projects, ensuring users can freely inspect, modify, and distribute the code. Red Hat champions community collaboration for innovation and security, while also ensuring the sustainability of open source by providing enterprise-grade support and security hardening for its offerings, with contributions continually flowing back to the broader ecosystem.

How does the CRA affect Red Hat?

Red Hat as a Manufacturer

- “provider of enterprise open-source software solutions”
- “business model is primarily subscription-based, providing enterprise-grade support, integration services, security patches, and strategic guidance for its open-source products”
- “Red Hat's business reach is global”

Red Hat as an Open Source Steward

- Red Hat's relationship with open source software is foundational to its entire existence and business model. The company actively develops, curates, and contributes to numerous open source projects, including the Linux kernel, Kubernetes, Fedora, and countless others.
- Interpreting this as fulfilling a stewardship role for certain projects we do not manufacture, and actively working with other potential stewards (such as the Linux Foundation, Eclipse, Apache, etc.) to ensure open source projects are being supported.

Additional Information:
EUR-LEX Regulation (EU) 2024/2847: https://eur-lex.europa.eu/eli/reg/2024/2847/oj

Red Hat CRA Program Structure

Red Hat CRA Program

Awareness & Communications	Participation in EU Standards Bodies	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 standards 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

Workstream Responsibilities & Outcomes

Manufacturer & Steward Obligations

Align the CRA with Red Hat's SDLC practices to ensure all requirements are understood

- Analyze the CRA, its implementing acts, and horizontal and vertical standards to ensure that these requirements are aligned 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.
- Determine Stewardship scope and obligations, coordinate gap analysis and facilitate guidance to upstream projects.

Vuln Mgmt / Incident Response

Ensure VM/IR policies and processes met CRA requirements and reporting obligations

- Ensure that Red Hat's Vulnerability Mgmt / Incident Response capabilities can meet the CRA requirements, additional acts, and horizontal and vertical standards.
- Ensure SBOMs are generated and made available as outlined in the CRA.
- Ensure processes are in place to monitor and report on exploited vulnerabilities and severe incidents as specified in the CRA. (reported to ENISA and national CSIRTs)
- Provide VM/IR guidance to upstream projects.

Workstream Responsibilities & Outcomes

Participation in EU Standards Bodies

Coordinate interactions with stds bodies to provide Red Hat's expertise and advocate for OSS

- Engage with EU standards bodies on behalf of Red Hat to advocate for software requirements that are practical, align with open source principles, and consider the capabilities of open source projects.
- Monitor standardization work within the EU so Red Hat understands the directions the standards are moving in and can proactively plan for them.
- Align and engage with open source foundations and communities to advocate for the open source principles Red Hat represents.

Upstream Engagement & Contributions

Coordinate interactions with foundations and upstream communities regarding CRA

- Engage with open source foundations and other entities on behalf of Red Hat to spread awareness of the CRA requirements to the open source community.
- Share Red Hat's knowledge and expertise with the open source community to enable OSS projects to plan for and meet the CRA requirements.
- Determine Red Hat Stewardship scope and obligations, support gap analysis and guidance to upstream projects.

Workstream Responsibilities & Outcomes

Conformity & Certification

Define the processes for Red Hat software to attest it has met the CRA requirements

- Responsible for Red Hat software assessments and producing Declarations of Conformity.
- Ensure Red Hat meets all CRA conformity and certification requirements for Critical and Important (Class I & II) products with digital elements (PDE).
- Coordinate work with Third-Party Assessment Organizations (3PAO) as needed, such as Notified Bodies (NB) and Conformity Assessment Body (CAB).

Awareness & Communications

Prepare internal and external CRA comms and training

Data Collection

Gather metrics to evaluate resourcing & investments for CRA

Legal

Support for other workstreams, develop internal CRA guidance, review deliverables

- 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.

Challenges

- **Ambiguity:** the law mentions a lot of different obligations and practices without details that can be used to create requirements.
  - Examples include "risk assessments," "effective and regular tests and reviews," "severe incidents," "commercial activity/monetization," and SBOM content and format details.
- **Unknowns:** there is a large amount of information forthcoming over the next ~18 months.
  - Horizontal & vertical standards are currently being developed, VM/IR reporting content details are unknown, and the ENISA Single Reporting Platform is not yet available.
  - Implementing acts are also currently being developed (including Technical Descriptions of Product Categories).
- **Widespread standards work:** there are MANY standards being actively worked on across the EU, and just maintaining awareness of them is very challenging, not to mention trying to participate.
- **Tight timelines:** the due dates for standards are very close to obligation deadlines.
  - Reporting obligations for actively exploited vulnerabilities and severe incidents begin on 11 Sept 2026, but vulnerability management standards are not due until 30 Aug 2026.
  - Other standards and implementing acts are not due until October 2026 or 2027.
- **Red Hat's role(s):** how extensive should our Stewardship be and what are the expectations?
  - Specifically, what is the degree of required upstream VM/IR support.

Key Takeaways

- Understand what the CRA means to your business, project, and/or community.
- What role(s) defined in the CRA apply?
  - Manufacturer and Open Source Steward are the primary ones, but there are others.
- Understand the deadlines and the associated expectations and deliverables.
  - 11 Sept 2026: reporting obligations begin for actively exploited vulnerabilities and severe incidents
  - 11 Dec 2027: the CRA fully enters into force
- Prioritize the tasks and think both short-term and long-term.
  - What must be done? What is currently being done? When must it be done? How must it be done?
  - Assess, prioritize, start small, scale up.
- Be prepared to adapt to forthcoming implementing acts, standards, and guidance.
- Get engaged with foundations and other entities involved with the CRA.
  - Work with your partners and 3rd party suppliers to ensure alignment and meet CRA requirements.
  - There is a lot of good information available and knowledgeable people to work with.

Additional Information:
EU Cyber Resiliency Act - 2026 Obligations Presentation: https://docs.google.com/presentation/d/1RSXEk-iTkuQZS5TbN6FQUCIEFlxvn8p5j-yXVdS_uXg/edit?usp=sharing
OSSF Global Cyber Policy Working Group: https://github.com/ossf/wg-globalcyberpolicy

How LFEL 1001 Supports Readiness?

David A. Wheeler

Director of Open Source Supply Chain Security at OpenSSF,
Linux Foundation

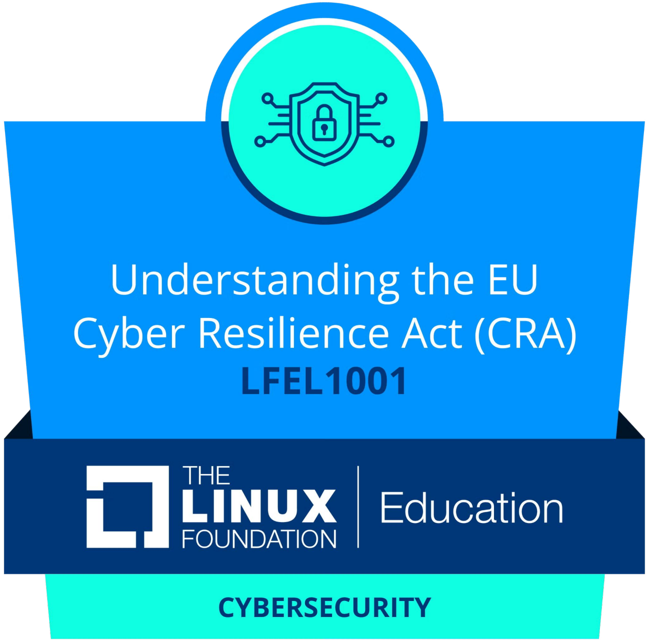
Quick tour of the LFEL1001 course content

Real-world, not theoretical

How OSS contributors and project leads can use it

Available resources for getting started now

Quick tour of the LFEL1001 course content



- Introduction, roles, and product categories
  - ○ Basics of the CRA
  - ○ CRA in context
  - ○ Roles & product categories
- Requirements and Conformity Assessments
  - ○ Open Source Software
  - ○ Manufacturers - Overall, vulnerabilities and reporting, conformity
  - ○ Importers & Distributors
  - ○ Penalties, beyond compliance, & alpha software
- Adapting to the CRA & Wrap-up
  - ○ Addressing changes to your organization

Real-world, not theoretical

We explain how you could *implement* CRA. Examples:

- “Paragraph 2b says that PDEs must have a secure-by-default configuration… For example, [instead of] a system with a known username and password like ‘admin’. [you could require] setting a password when the system first boots.”
- “Paragraph 2k says PDEs must be ‘designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;’ Examples of such mechanisms include compiler option hardening flags, operating system configurations, and the Content Security Policy aka CSP.“

How OSS contributors and project leads can use it

- Take the course!
  - If you’re a “manufacturer” under CRA, CRA directly applies
  - If you’re a “steward” under CRA, CRA has a few requirements
  - It will affect the *users* of your software, indirectly affecting you
    - They’ll be asking for info, hardening, etc., & providing more vulnerability reports
- Let others know about course (it’s free)

Available resources for getting started now

- *Understanding the EU Cyber Resilience Act (CRA) (LFEL1001)*
  - https://training.linuxfoundation.org/express-learning/understanding-the-eu-cyber-resilience-act-cra-lfel1001/
- *Cyber Resilience Act (CRA) Brief Guide for Open Source Software (OSS) Developers*
  - Coming soon
  - https://best.openssf.org/CRA-Brief-Guide-for-OSS-Developers

Panel Discussion & Audience Q&A

Call to Actions & Resources

Learn more about LFEL 1001 & enroll today:

Download the Linux Foundation Unaware and Uncertain report:

Download EU Cyber Resiliency Act 2026 Obligations

OpenSSF Global Cyber Policy Working Group

- Slack Channel
- GitHub
- Mailing List

Official Publication: Cyber Resilience Act

European Commission Public Consultations

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Upcoming Events

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

OpenSSF Hosted Events:

- Community Day NA: June 26 Colorado Convention Center, Denver, CO
  - OSS NA: David's Tip Talk at LF Education Learning Lounge: June 24 4:00-4:45PM Local Time
- Community Day Japan: June 18, Tokyo, Japan.
- Community Day India: Aug 4 Hyderbad
- Community Day Europe: August 28, Amsterdam, Netherlands
  - Sponsorship Opportunities Available
- Community Day Korea: November 4, Seoul, South Korea
  - CFP closes on August 3rd.

Ways to Participate

- Join a Working Group/Project
- Come to a Meeting (see Public Calendar)
- Collaborate on Slack
- Contribute on GitHub
- Become an Organizational Member
- Keep up to date by subscribing to the OpenSSF Mailing List

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Engage with us on social media

X
@openssf

LinkedIn
OpenSSF

Mastodon
social.lfx.dev/@openssf

YouTube
OpenSSF

Facebook
OpenSSF

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

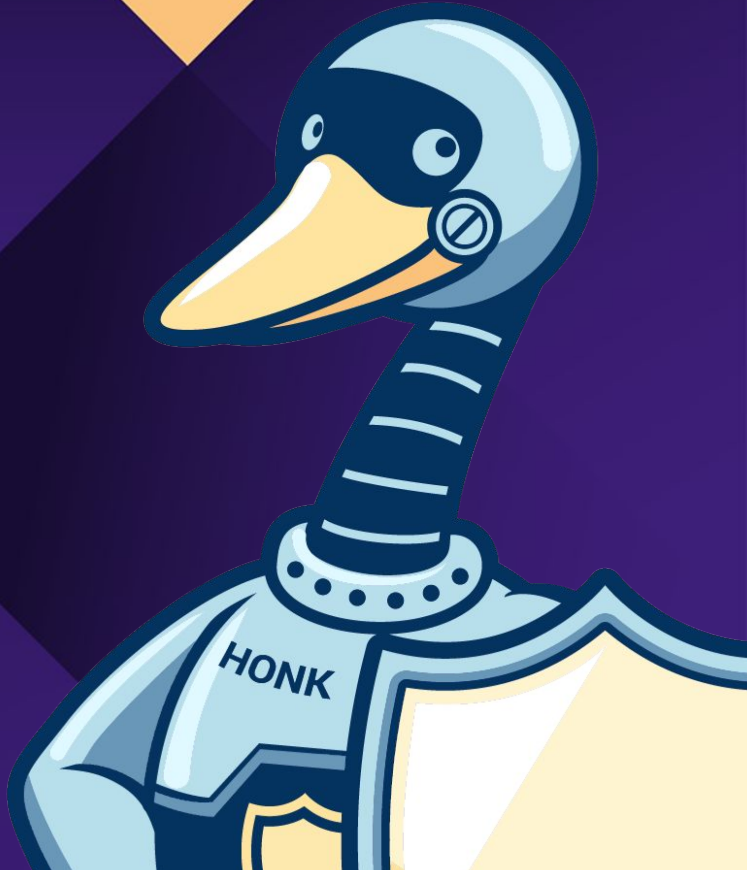
Subscribe to our mailing list

openssf.org/sign-up

Is your organization a member?

Questions? Contact membership@openssf.org

openssf.org/join



Thank You

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Take our quick Tech Talk Survey

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Help us improve!

Legal Notice