
CRA PSIRT TL/DR
Or…
How I learned to love the CRA, but for PSIRTs

Who is this guy?

CRob, n, adj, and v

Pronunciation: U.S. (K-rowb)

```
# chmod 666 crob.md
```

43rd level Dungeon Master

26th level Securityologist

Pirate-enthusiast & hat-owner

Former Governing Board member and Chairman of the OpenSSF Technical Advisory Council

Chief Security Architect, OpenSSF - Linux Foundation

FIRST PSIRT SIG leader & VulnCon program committee

Disclaimer/ Weasel Words

CRob is not a lawyer.

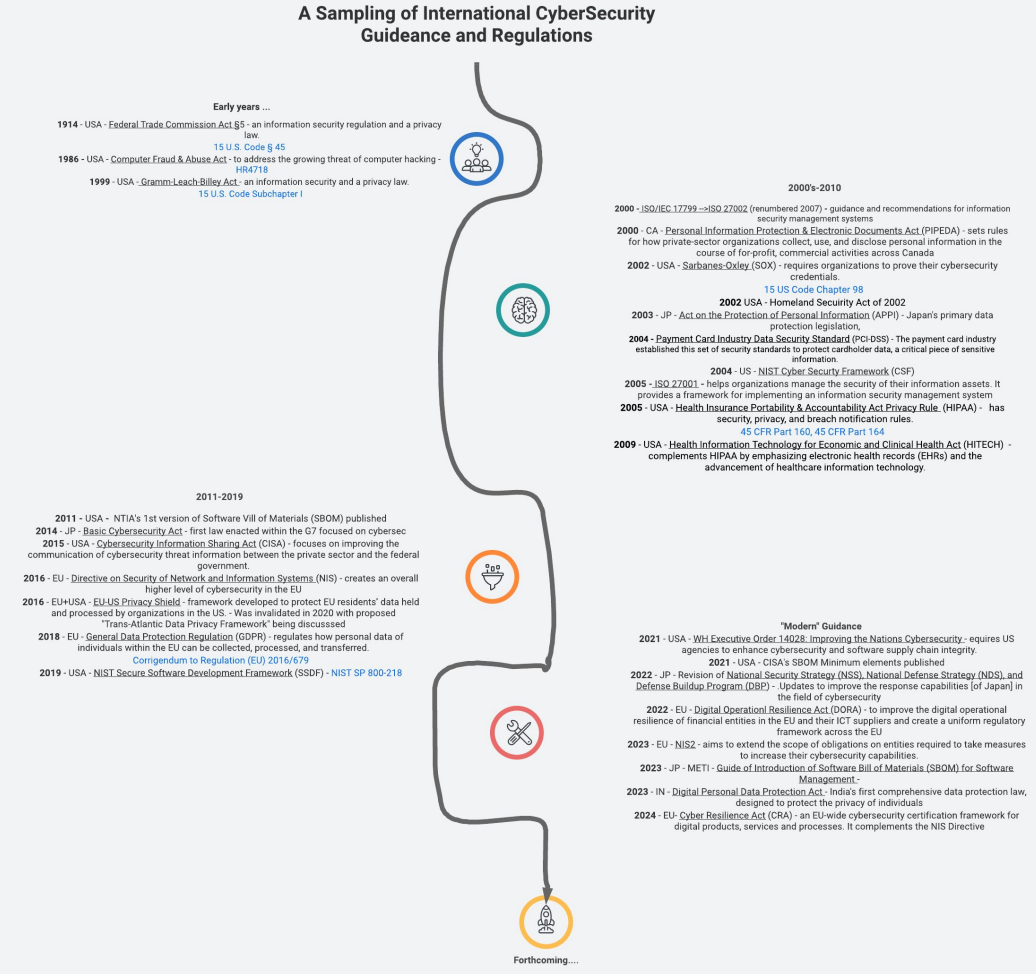
CRob is certainly not YOUR lawyer.

These are thoughts, feelings, and insights from CRob's career; consult YOUR attorney to understand what YOU and YOUR Org needs to be doing

Follow the bouncing CRob-head for "CRob Pro-Tips", insights, advice, and commentary

Welcome to the awesome World of Global CyberSecurity Compliance

Just ~100 years of applicable laws and frameworks that apply to “the cybers”



TL/DR - CRA WAT

So… you “get to” do some CRA, eh?

Regulation (EU) 2024/2847 (Cyber Resilience Act, CRA)

The **EU Cyber Resilience Act** sets new regulatory requirements for hardware & software security, placing a significant emphasis on the safety and security of digital products sold within the European market.

This is designed to protect EU citizens from damages resulting from cybersecurity incidents related to products they have purchased or that support those offerings.

This is a LAW, compliance is mandatory for anything sold within the European Common Market.

The 1st components of the law will become in effect Q4 2026, with the final law going into effect in 2027

For more information, checkout the OpenSSF’s Global Cyber Policy Working Group 2024 Stewards & Manufacturers Workshop

Why is the CRA important?

The EU acts to strengthen the approach to cybersecurity regulation at union level. The CRA aims to achieve 3 policy goals:

- To reduce vulnerabilities in digital products,
- To ensure cybersecurity is maintained throughout a product's life cycle and
- To enable users to make informed decisions when selecting and operating digital products

The CRA establishes horizontal mandatory cyber-security requirements for all digital products, software and/or hardware.

It imposes objective-oriented and technology-neutral requirements in order to make products available in the EU.

The EU intends to play a leading international role in cybersecurity regulation.

Consequences on non-compliance

Article 64 lays out the framework for Penalties of non-compliance….

***Emphasis** added*

2. Non-compliance with the **essential cybersecurity requirements** set out in Annex I and the obligations set out in Articles 13 and 14 *shall be subject to administrative fines of up to EUR 15 000 000 or, if the offender is an undertaking, up to 2,5 % of the its total worldwide annual turnover for the preceding financial year, whichever is higher.*

3. Non-compliance with the obligations set out in Articles 18 to 23, Article 28, Article 30(1) to (4), Article 31(1) to (4), Article 32(1), (2) and (3), Article 33(5), and Articles 39, 41, 47, 49 and 53 *shall be subject to administrative fines of up to EUR 10 000 000 or, if the offender is an undertaking, up to 2 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.*

4. **The supply of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities** in reply to a request *shall be subject to administrative fines of up to EUR 5 000 000 or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.*

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847#cpt_IV

Key CRA terms/phrases

‘product with digital elements’ means a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately;

‘placing on the market’ means the first making available of a product with digital elements on the Union market;

‘making available on the market’ means the supply of a product with digital elements for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge;

The language of the law is dense, extremely verbose, and very nuanced. The above two actions are NOT identical, and are used throughout the text of the law

3ish roles (these two have the bulk of the compliance obligations)

Manufacturer - **‘manufacturer’** means a natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under its name or trademark, whether for payment, monetisation or free of charge; - Article 13

If you sell hardware or software, for money, to an EU citizen or entities within the EU Common Market

…this is YOU!

OSS Steward - **‘open-source software steward’** means a legal person, other than a manufacturer, that has the purpose or objective of systematically providing support on a sustained basis for the development of specific products with digital elements, qualifying as free and open-source software and intended for commercial activities, and that ensures the viability of those products; - Article 24

This is CRob - the LF, Apache Foundation, Eclipse Foundation, non-profits, etc. – the fun upstream folks!

This is probably not you.

Others……

OSS Developer - not officially defined, but Article 25 talks about voluntary things upstream *could* do (self-attestation) ← we'll talk more about this later on

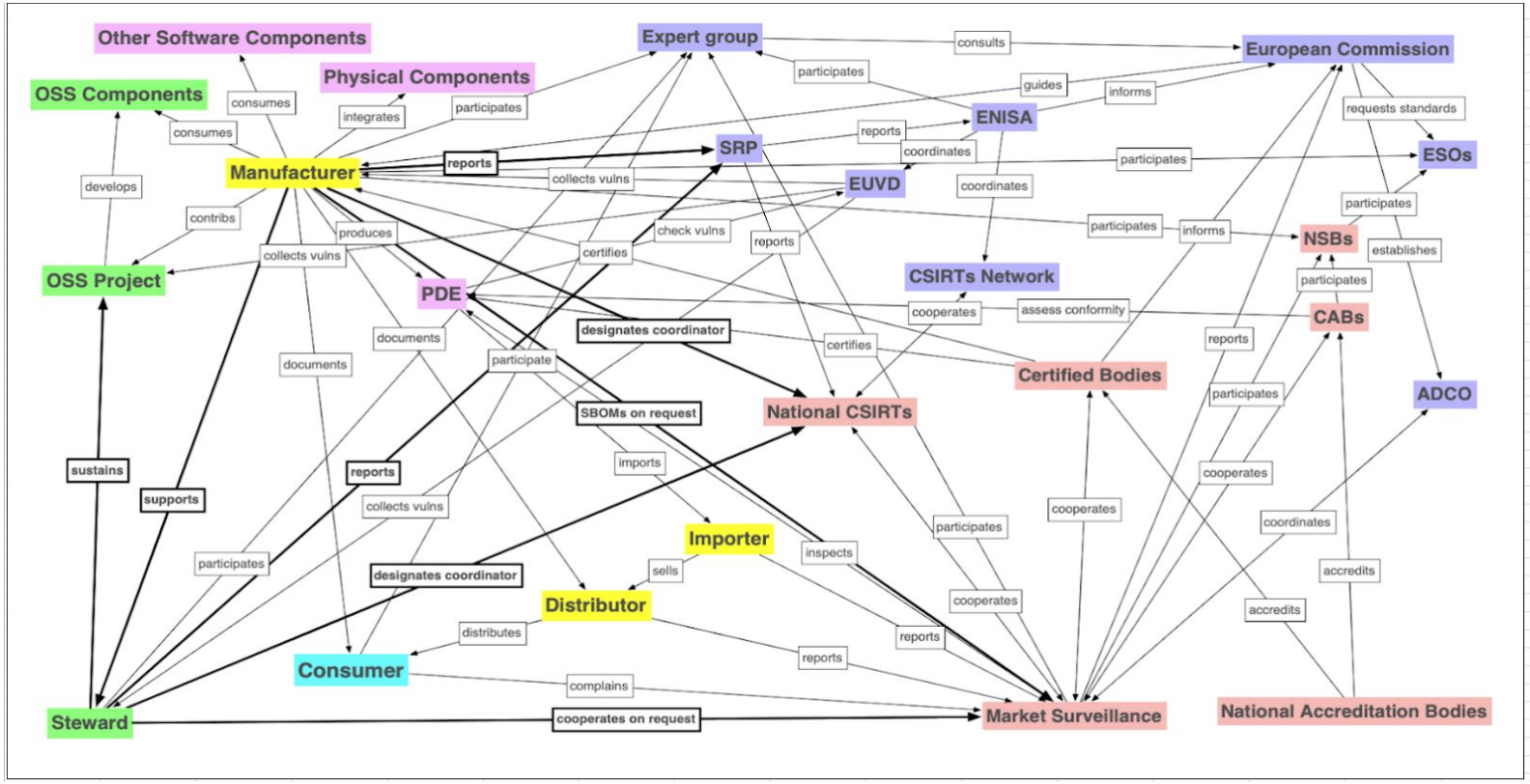
Consumer - **'consumer'** means a natural person who acts for purposes which are outside that person's trade, business, craft or profession;

Distributor/Importer - folks that help get your product into the EU

Market Surveillance Authority - 'market surveillance authority' means a market surveillance authority as defined in Article 3, point (4), of Regulation (EU) 2019/1020;

CERTs - **'CSIRT designated as coordinator'** means a CSIRT designated as coordinator pursuant to Article 12(1) of Directive (EU) 2022/2555.

CRA Roles - Nothing confusing about this....



Created by Fukami - https://github.com/ossf/wg-globalcyberpolicy/blob/main/documents/CRA/CRA_Roles.png

Sections to look at - https://data.consilium.europa.eu/doc/document/PE-100-2023-INIT/en/pdf

Article 3 - definitions

Article 6,7,8 - requirements for (important, critical) “products with digital elements made available on the market”

Article 13 - obligations of manufacturers

Article 14 - reporting obligations of manufacturers (oh boy, this’ll be “fun”!)

Article 22 - “substantial modifications” clause

Article 24 - obligations of open source stewards

Article 25 - security attestations of free and open-source software

Article 64 - Penalties

Annex I

Annex III & IV - Important & critical products with digital elements

Depending on what you make and how “critical” it is in the commission’s eyes, you have stricter requirements (Annex III + IV)

Other interesting things…

Article 16 - establishment of single reporting platform

Chapter III - Conformity of the product with digital elements

Chapter V - Market surveillance and enforcement

But wait, there's **MOAR**!

PLD - The Product Liability Directive - "common rules on liability for defective products with the aim of removing divergences between the legal systems of Member States that may distort competition and affect the movement of goods within the internal market."
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402853

Blue Guide - Canonical definitions for terms used throughout EU Regulations, Directives, and Decisions
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C:2022:247:FULL

…other regs (....so many new regs….) =====>

Related Dossiers

EU Legislation	In CRA?	Common name of legislation
Regulation (EU) No 168/2013	Amended by CRA	Approval and market surveillance of two- or three-wheel vehicles and quadricycles
Regulation (EU) 2019/1020	Amended by CRA	Market surveillance and compliance of products
Directive (EU) 2020/1828	Amended by CRA	Representative actions for the protection of the collective interests of consumers
Regulation (EU) 2019/881	Deeply integrated: voluntary and mandatory certification	Cybersecurity Act
Directive (EU) 2022/2555	Deeply integrated: single reporting, ENISA/CSIRTs Network involvement	NIS2 Directive
Regulation (EU) No 910/2014	EUDI provider to follow CRA	eIDAS
Directive (EU) 2018/1972	Amended by NIS2	EECC (European Electronic Communications Code)
Commission Recommendation 2003/361/EC	Used as definition for SMEs	Definition of micro, small and medium-sized enterprises
JOIN(2020) 18 final	Political Reference	Joint communication 'The EU's Cybersecurity Strategy for the Digital Decade'
2020/C 427/04	Political Reference	Council Conclusion on cybersecurity of connected devices
9364/22	Political Reference	Council Conclusions on the development of the European Union's cyber posture
Directive 2014/24/EU	Ensure CRA compliance	Public procurement
Directive 2014/25/EU	Ensure CRA compliance	Procurement by entities operating in the water, energy, transport and postal services sectors
Regulation (EU) 2025/327	Amends the CRA	European Health Data Space (EHDS): manufacturer of EHR systems need to show conformity
Regulation (EU) 2017/745	Out of scope of CRA	Medical devices
Regulation (EU) 2017/746	Out of scope of CRA	In vitro diagnostic medical devices
Regulation (EU) 2019/2144	Out of scope of CRA	Type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users
Directive 2014/90/EU	Out of scope of CRA	Marine equipment
Regulation (EU) 2018/1139	Out of scope of CRA	Common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency
Commission Delegated Regulation (EU) 2022/30	Out of scope of CRA	Application of the essential requirements (RED)
Commission Implementing Decision C(2022) 5637	Standardisation request RED	Draft Standardisation request RED
Directive (EU) 2024/2853	Complementary to CRA	Liability for defective products (PLD)
Regulation (EU) 2016/679	Also using data protection measures to demonstrate compliance	GDPR (General Data Protection Regulation)
Regulation (EU) 2024/1781	Right to repair	Framework for the setting of ecodesign requirements for sustainable products
Commission Implementing Regulation (EU) 2024/482	Possible mandatory certification	European Common Criteria-based cybersecurity certification scheme (EUCC)
Regulation (EU) 2023/988	Refers to GPSR as baseline	General Product Safety Regulation
Regulation (EU) No 1025/2012	Harmonised/European standards	European standardisation
Regulation (EU) 2024/1689	Implement High-risk AI essential cybersecurity requirements	Artificial Intelligence Act
Commission Recommendation (EU) 2019/534	Refers fo resilience in 5G	Cybersecurity of 5G networks
Regulation (EU) 2023/1230	Needs CRA compliance	Machinery Regulation
Regulation (EU) 2022/2554	National level single entry points for reporting requirements	Digital operational resilience for the financial sector (DORA)
Directive 2002/58/EC	National level single entry points for reporting requirements, also with GDPR	Processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
Regulation (EC) No 765/2008	CE Marking	Requirements for accreditation and market surveillance relating to the marketing of products
Decision No 768/2008/EC	Conformity assessment	Common framework for the marketing of products (CE)
Regulation (EU) No 182/2011	Comitology Procedure	Rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers
Regulation (EU) 2018/1725	Data Protection Framework for EU Institutions	Protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data,
Directive (EU) 2016/943	Protection of Trade Secrets	Protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition
Directive 2009/48/EC	Needs CRA compliance	Safety of toys
Directive (EU) 2019/944	Smartmeters	Internal market for electricity

Bookmark these links RIGHT NOW!

"Fukami's spreadsheet" - https://docs.google.com/spreadsheets/d/1z8WxHRCw8kPKehTsKJn2bWmrJI9BWos5ofbjuwbEGzU/edit?gid=1008270796#gid=1008270796

PSIRT (Manufacturer) Requirements

Using the lens of Annex I, we'll walk through programs, processes, and artifacts/attestations you will need to have prepared and ready when requested by the Commission or the Market Surveillance Authorities for MANUFACTURERS…

Annex I covers ~21 requirements, divided between "cybersecurity" (think SDLC/Sec-By-Design/default + risk management) and "vulnerability handling"

We'll explore Annex I and the affiliated Articles more in depth…..

Annex 1 - ESSENTIAL CYBERSECURITY REQUIREMENTS

1. SECURITY REQUIREMENTS RELATING TO THE PROPERTIES OF PRODUCTS WITH DIGITAL ELEMENTS

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;

The expectation that unlike the CISA Sec-by-Design Promise, Manufacturers will now be legally obligated to create, sell, and support their PDE using Security-by-Default and Security-by-Design principles…. And have the receipts to prove it. You WILL be asked to provide many SDLC/design artifacts to the Commission, the MSA, and others.

(2) Products with digital elements shall be delivered **without any known exploitable vulnerabilities**;

You will need to provide evidence that just prior to release that a product was checked for known exploited vulnerabilities

Annex I continued

3.) On the basis of the **risk assessment** referred to in Article 10(2) and where applicable, products with digital elements shall:

(a) be delivered with a secure by default configuration, including the possibility to reset the product to its original state;

(b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;

(c) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms;

(d) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;

(e) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data');

(f) protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;

(g) minimise their own negative impact on the availability of services provided by other devices or networks;

(h) be designed, developed and produced to limit attack surfaces, including external interfaces;

(i) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

More about managing your risks…..

From Article 13.4

When placing a product with digital elements on the market, the manufacturer shall include the cybersecurity risk assessment referred to in paragraph 3 of this Article in the technical documentation required pursuant to Article 31 and Annex VII. For products with digital elements as referred to in Article 12, which are also subject to other Union legal acts, the cybersecurity risk assessment may be part of the risk assessment required by those Union legal acts. Where certain essential cybersecurity requirements are not applicable to the product with digital elements, the manufacturer shall include a clear justification to that effect in that technical documentation.

You should be doing this today, but you might not have a formal process or artifacts that meet the desired

EU risk assessment standard, and you most likely are not publishing this info today to external folks.

Risk Assessments

Find a repeatable, well-known RM framework to follow and start documenting!

https://www.enisa.europa.eu/topics/risk-management

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.pdf?__blob=publicationFile&v=2

The OpenSSF is developing a class based on the ENISA RMF to illustrate how to conduct assessments per their desired standard.

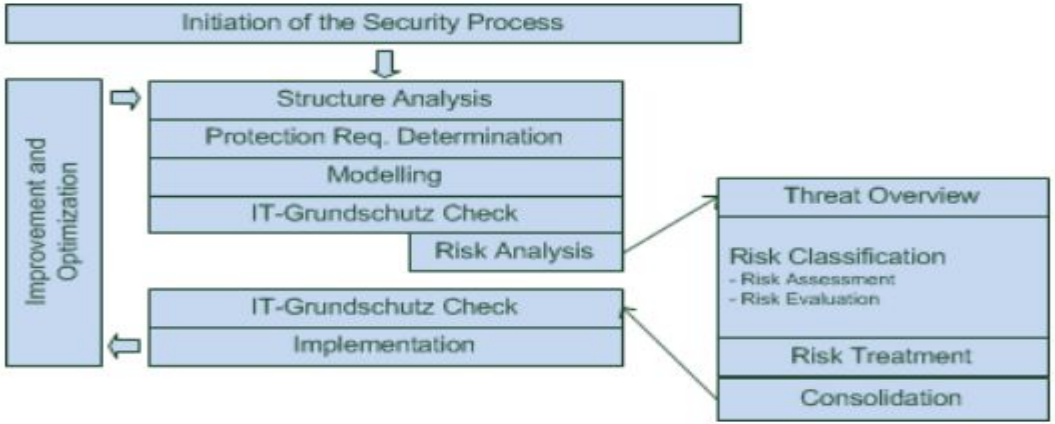


Figure 1: Integration of the risk analysis into the security process

Annex I continued

2. VULNERABILITY HANDLING REQUIREMENT

Manufacturers of the products with digital elements shall:

(1) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;

*You WILL be required to provide SBOMS at the request of authorities in either CycloneDX or SPDX format.**

(2) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates;

*A few points here…. "Providing updates" and "**Without delay**"*

* SBOM is one of the topics of the standardization efforts, and new criteria/minimum elements may be developed over the coming months stay tuned!

Encouraging better upstream engagement….

From Article 13.6

Manufacturers shall, upon identifying a vulnerability in a component, including in an open source-component, which is integrated in the product with digital elements report the vulnerability to the person or entity manufacturing or maintaining the component, and address and remediate the vulnerability in accordance with the vulnerability handling requirements set out in Part II of Annex I. Where manufacturers have developed a software or hardware modification to address the vulnerability in that component, they shall share the relevant code or documentation with the person or entity manufacturing or maintaining the component, where appropriate in a machine-readable format.

This is how YOU can help make YOUR upstream sources better, but giving the fixes back. That way you, your customers, and the whole ecosystem benefit

Support Periods

From Article 13.8

Manufacturers shall ensure, when placing a product with digital elements on the market, and for the support period, that vulnerabilities of that product, including its components, are handled effectively and in accordance with the essential cybersecurity requirements set out in Part II of Annex I.

Manufacturers shall determine the support period so that it reflects the length of time during which the product is expected to be in use, taking into account, in particular, reasonable user expectations, the nature of the product, including its intended purpose, as well as relevant Union law determining the lifetime of products with digital elements.

Without prejudice to the second subparagraph, **the support period shall be at least five years**. Where the product with digital elements is expected to be in use for less than five years, the support period shall correspond to the expected use time.

Depending on your core business, you may already be doing this, or doing in as an enhanced offering.

It is now mandatory

More support dates

From Article 13.9

Manufacturers shall ensure that each security update, as referred to in Part II, point (8), of Annex I, which has been made available to users during the support period, remains available after it has been issued for a minimum of 10 years or for the remainder of the support period, whichever is longer.

13.10. Where a manufacturer has placed subsequent **substantially modified** versions of a software product on the market, that manufacturer may ensure compliance with the essential cybersecurity requirement set out in Part II, point (2), of Annex I only for the version that it has last placed on the market, provided that the users of the versions that were previously placed on the market have access to the version last placed on the market free of charge and do not incur additional costs to adjust the hardware and software environment in which they use the original version of that product.

13.19. Manufacturers shall ensure that the end date of the support period referred to in paragraph 8, including at least the month and the year, is clearly and understandably specified at the time of purchase in an easily accessible manner and, where applicable, on the product with digital elements, its packaging or by digital means.

Where technically feasible in light of the nature of the product with digital elements, manufacturers shall display a notification to users informing them that their product with digital elements has reached the end of its support period.

This part is pretty “cool” too….

From Article 13.21

From the placing on the market and for the support period, manufacturers who know or have reason to believe that the product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential cybersecurity requirements set out in Annex I shall immediately take the corrective measures necessary to bring that product with digital elements or the manufacturer’s processes into conformity, or to withdraw or recall the product, as appropriate.

See what they did here? The law is RETROACTIVE, so not only applies to new/in-flight products, but also your “back catalog”

Annex I continued

(3) apply effective and regular tests and reviews of the security of the product with digital elements;

(4) once a security update has been made available, publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and information helping users to remediate the vulnerabilities;

(5) put in place and enforce a policy on coordinated vulnerability disclosure;

(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

So about reporting…..

From Article 13.17.

For the purposes of this Regulation, manufacturers shall designate a single point of contact to enable users to communicate directly and rapidly with them, including in order to facilitate reporting on vulnerabilities of the product with digital elements.

Manufacturers shall ensure that the single point of contact is easily identifiable by the users. They shall also include the single point of contact in the information and instructions to the user set out in Annex II.

The single point of contact shall allow users to choose their preferred means of communication and shall not limit such means to automated tools.

So far, so good. This is all "Mom & Apple Pie" for a mature PSIRT….

Meet your “pal” Article 14….

1. A manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. **The manufacturer shall notify that actively exploited vulnerability via the single reporting platform** established pursuant to Article 16.

MOAR Article 14

2. For the purposes of the notification referred to in paragraph 1, the manufacturer shall submit:

(a) an **early warning notification** of an **actively exploited** vulnerability, without undue delay and in any event **within 24 hours** of the manufacturer becoming aware of it, indicating, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available;

(b) unless the relevant information has already been provided, **a vulnerability notification,** without undue delay and in any event **within 72 hours** of the manufacturer becoming aware of the actively exploited vulnerability, which shall provide general information, as available, about the product with digital elements concerned, the general nature of the exploit and of the vulnerability concerned as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take, and which shall also indicate, where applicable, how sensitive the manufacturer considers the notified information to be;

(c) unless the relevant information has already been provided, **a final report,** no later than 14 days after a corrective or mitigating measure is available, including at least the following:

(i) a description of the vulnerability, including its severity and impact;

(ii) where available, information concerning any malicious actor that has exploited or that is exploiting the vulnerability;

(iii) details about the security update or other corrective measures that have been made available to remedy the vulnerability.

This is new and focuses on "exploited vulns". You probably aren't doing a lot around this proactively today (but maybe you are)

Article 14, redux

3. A manufacturer shall notify any **severe incident** having an impact on the security of the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. The manufacturer shall notify that incident via the single reporting platform established pursuant to Article 16.

MOAR MOAR Article 14

4. For the purposes of the notification referred to in paragraph 3, the manufacturer shall submit:

(a) an **early warning notification** of a severe incident having an impact on the security of the product with digital elements, without undue delay and in any event within 24 hours of the manufacturer becoming aware of it, including at least whether the incident is suspected of being caused by unlawful or malicious acts, which shall also indicate, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available;

*VEX *may* be a solution here*

(b) unless the relevant information has already been provided, **an incident notification**, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the incident, which shall provide general information, where available, about the nature of the incident, an initial assessment of the incident, as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take, and which shall also indicate, where applicable, how sensitive the manufacturer considers the notified information to be;

(c) unless the relevant information has already been provided, **a final report**, within one month after the submission of the incident notification under point (b), including at least the following:

(i) a detailed description of the incident, including its severity and impact;

(ii) the type of threat or root cause that is likely to have triggered the incident;

(iii) applied and ongoing mitigation measures.

This basically is your current process, with some new timelines and targets of notification with the addition of this “final report”

Article 14 cont.

5. For the purposes of paragraph 3, an incident having an impact on the security of the product with digital elements shall be considered to be severe where:

(a) it negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions; or

(b) it has led or is capable of leading to the introduction or execution of malicious code in a product with digital elements or in the network and information systems of a user of the product with digital elements.

6. Where necessary, the CSIRT designated as coordinator initially receiving the notification may request manufacturers to provide an intermediate report on relevant status updates about the actively exploited vulnerability or severe incident having an impact on the security of the product with digital elements.

Article 14 keeps on rolling…

7. The notifications referred to in paragraphs 1 and 3 of this Article shall be submitted via the single reporting platform referred to in Article 16 using one of the electronic notification end-points referred to in Article 16(1). The notification shall be submitted using the electronic notification end-point of the CSIRT designated as coordinator of the Member State where the manufacturers have their main establishment in the Union and shall be simultaneously accessible to ENISA.

For the purposes of this Regulation, a manufacturer shall be considered to have its main establishment in the Union in the Member State where the decisions related to the cybersecurity of its products with digital elements are predominantly taken. If such a Member State cannot be determined, the main establishment shall be considered to be in the Member State where the manufacturer concerned has the establishment with the highest number of employees in the Union.

Where a manufacturer has no main establishment in the Union, it shall submit the notifications referred to in paragraphs 1 and 3 using the electronic notification end-point of the CSIRT designated as coordinator in the Member State determined pursuant to the following order and based on the information available to the manufacturer:

(a) the Member State in which the authorised representative acting on behalf of the manufacturer for the highest number of products with digital elements of that manufacturer is established;

(b) the Member State in which the importer placing on the market the highest number of products with digital elements of that manufacturer is established;

(c) the Member State in which the distributor making available on the market the highest number of products with digital elements of that manufacturer is established;

(d) the Member State in which the highest number of users of products with digital elements of that manufacturer are located.

You might not know this today, but you're going to have to figure this out before Dec 2027

Article 14 keeps on going….

8. After becoming aware of an actively exploited vulnerability or a severe incident having an impact on the security of the product with digital elements, the manufacturer shall inform the impacted users of the product with digital elements, and where appropriate all users, of that vulnerability or incident and, where necessary, of any risk mitigation and corrective measures that the users can deploy to mitigate the impact of that vulnerability or incident, where appropriate in a structured, machine-readable format that is easily automatically processable.

Where the manufacturer fails to inform the users of the product with digital elements in a timely manner, the notified CSIRTs designated as coordinators may provide such information to the users when considered to be proportionate and necessary for preventing or mitigating the impact of that vulnerability or incident.

9. By 11 December 2025, the Commission shall adopt delegated acts in accordance with Article 61 of this Regulation to supplement this Regulation by specifying the terms and conditions for applying the cybersecurity-related grounds in relation to delaying the dissemination of notifications as referred to in Article 16(2) of this Regulation. The Commission shall cooperate with the CSIRTs network established pursuant to Article 15 of Directive (EU) 2022/2555 and ENISA in preparing the draft delegated acts.

*You probably have *something* for high-profile incidents/exploits…. Double check you're ready to supply this info publicly more quickly than you may currently*

Annex I cont.

(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;

“In a timely manner” shows up constantly. BSI has provided implementation guidance for German companies on their expectations, be sure to check with YOUR designated CSIRT for their expectations

(8) ensure that, where security patches or updates are available to address identified security issues, they are disseminated **without delay** and **free of charge**, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

It is commonly accepted that security updates are freely available, but not universally…. CRA changes that

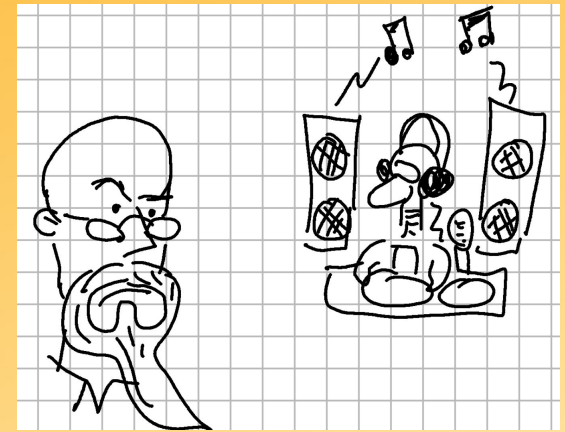
And that’s it

….for now

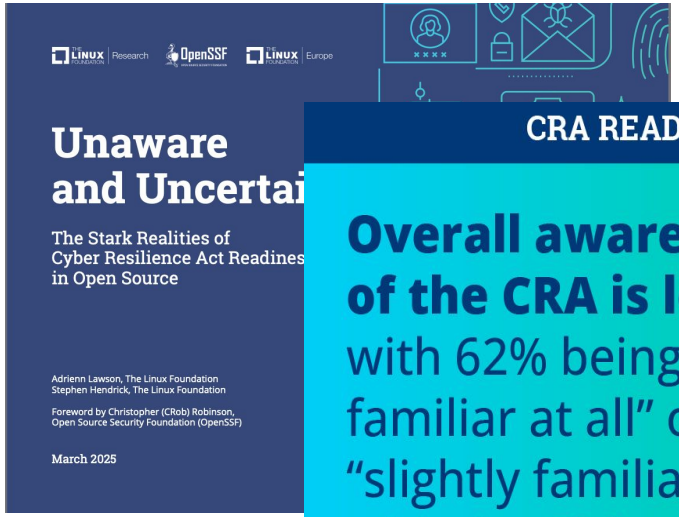
The legislation is being actively updated with amendments/clarifications and implementation guidelines (notable horizontal standards)

Anyone interested in sitting in 41+ different standards meetings for all of this spread across multiple groups?

Hi. My name is CRob. I’m from the Open Source, and I’m here to help.



LF Research around the CRA



An honest assessmen
upstream developers, open source stewards, and manufacturers for the CRA

https://www.linuxfoundation.org/hubfs/LF%20Research/lfr_cra_readiness_031725a.pdf?hsLang=en

open source projects are
demonstrating good cybersecurity practices (and how your projects could too!)

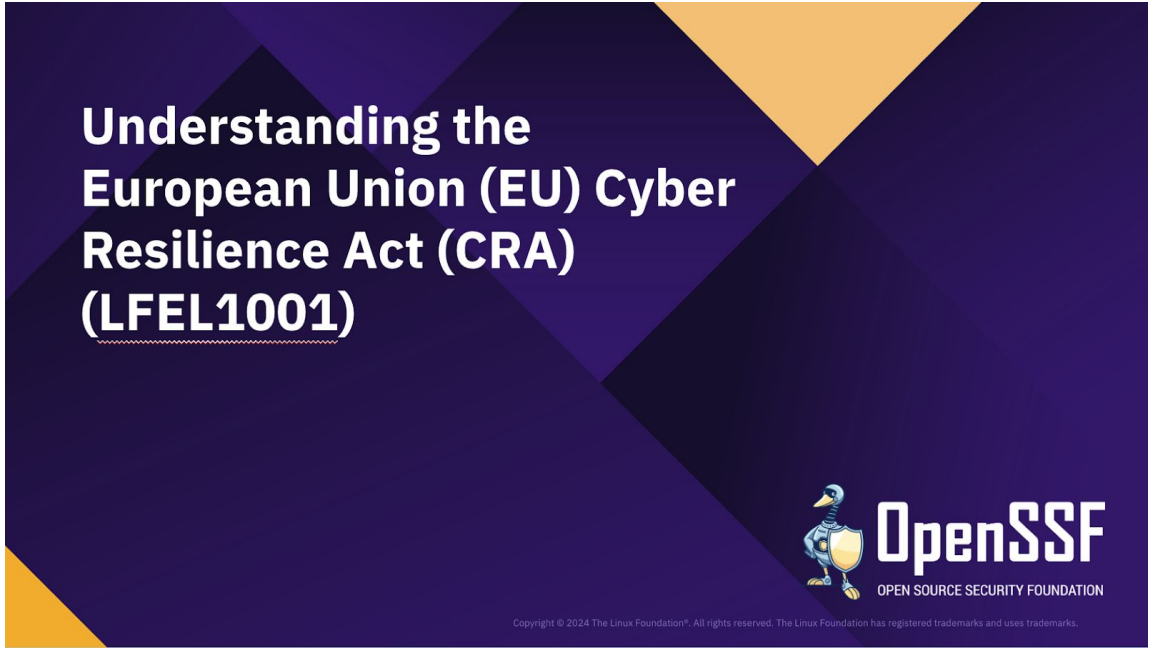
https://www.linuxfoundation.org/hubfs/LF%20Research/lfr_cra_031725a.pdf?hsLang=en

“CRA 101”

One of the 1st deliverables of the CRA Awareness SIG will be a free educational course covering the CRA

Will be available Q2 2025

Additional courses are planned, including how to conduct Risk Assessments throughout the development and productization lifecycle



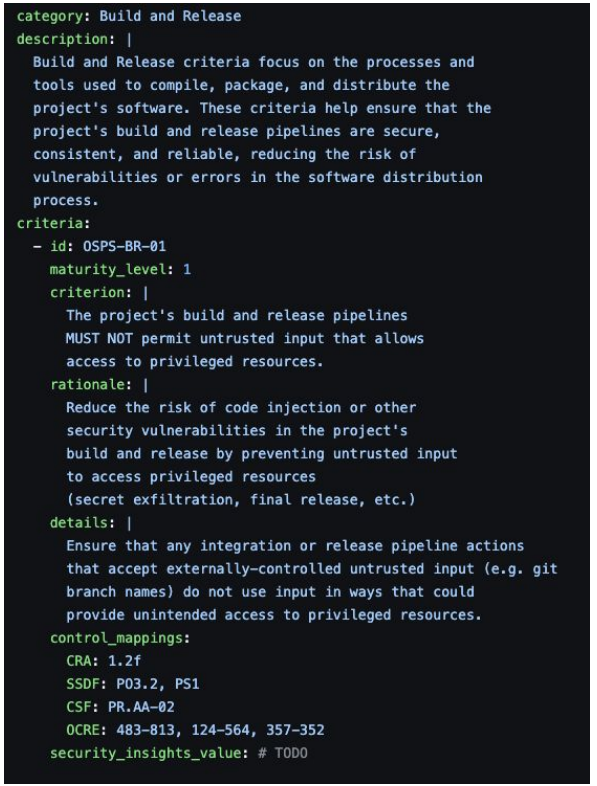
OpenSSF Security Baseline

Global cybersec frameworks+regulations-based minimum criteria to improve project security and empower downstream consumer understanding/review of security controls and artifacts.

8 Categories with 3 levels of maturity:

- Access Control
- Build+Release
- Documentation
- Governance
- Legal
- Quality Assurance
- Security Assessment
- Vulnerability Management

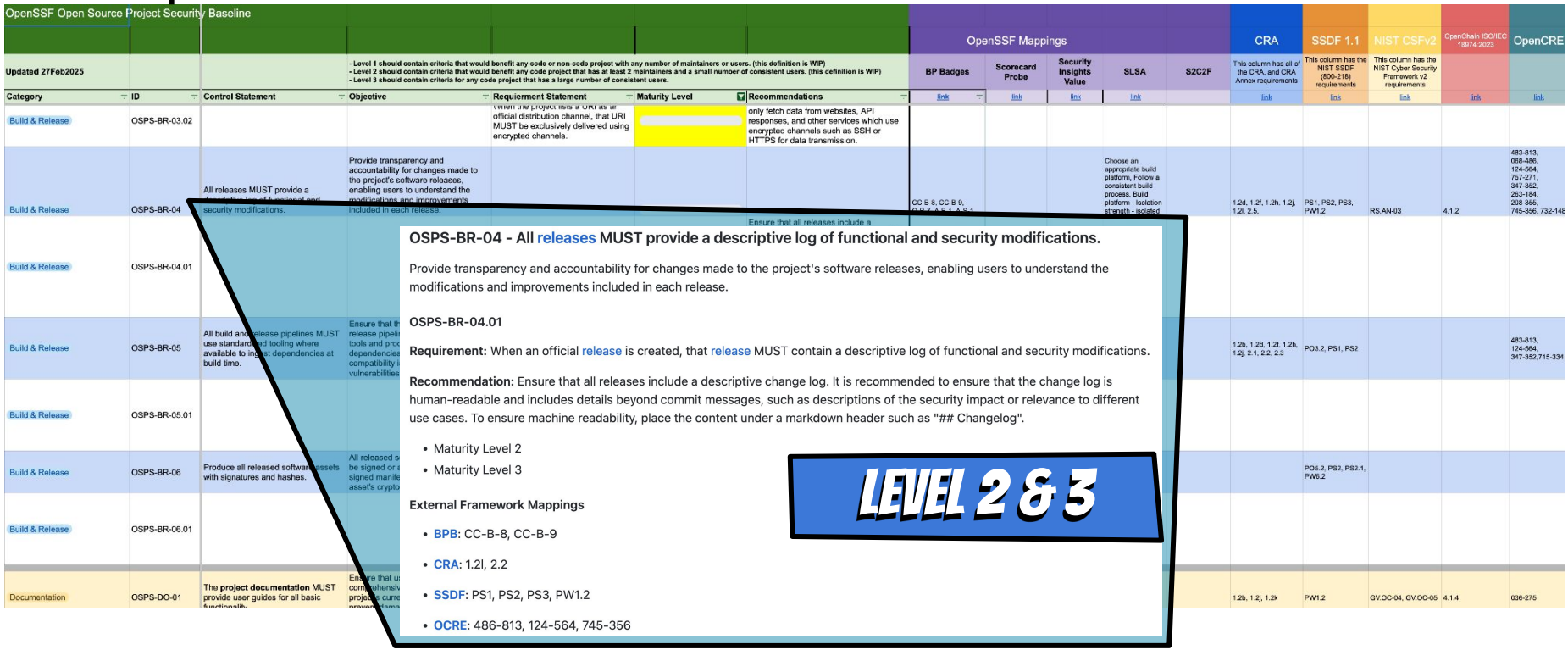
https://github.com/ossf/security-baseline
https://github.com/SecurityCRob/presentations/blob/main/LFMS24-%20Super%20BEST%20Friends-1.pdf



```yaml
category: Build and Release
description: |
  Build and Release criteria focus on the processes and
  tools used to compile, package, and distribute the
  project's software. These criteria help ensure that the
  project's build and release pipelines are secure,
  consistent, and reliable, reducing the risk of
  vulnerabilities or errors in the software distribution
  process.
criteria:
  - id: OSPS-BR-01
    maturity_level: 1
    criterion: |
      The project's build and release pipelines
      MUST NOT permit untrusted input that allows
      access to privileged resources.
    rationale: |
      Reduce the risk of code injection or other
      security vulnerabilities in the project's
      build and release by preventing untrusted input
      to access privileged resources
      (secret exfiltration, final release, etc.)
    details: |
      Ensure that any integration or release pipeline actions
      that accept externally-controlled untrusted input (e.g. git
      branch names) do not use input in ways that could
      provide unintended access to privileged resources.
    control_mappings:
      CRA: 1.2f
      SSDF: PO3.2, PS1
      CSF: PR.AA-02
      OCRE: 483-813, 124-564, 357-352
    security_insights_value: # TODO
```

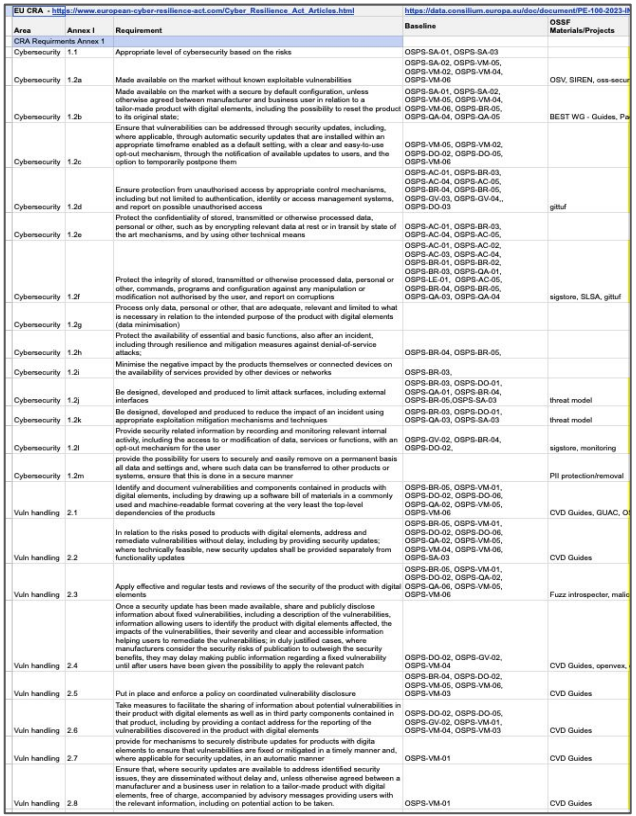
https://github.com/ossf/security-baseline/blob/main/baseline/OSPS-BR.yaml

Compliance Crosswalk



https://docs.google.com/spreadsheets/d/1an5mx3rayoz3JRFUepD56zgprpwXBXBG70fVZvIMCpA/

Upstream helping Downstream to help upstream help more



EU CRA - https://www.european-cyber-resilience-act.com/Cyber_Resilience_Act_Articles.html			https://data.consilium.europa.eu/doc/document/PE-100-2023-IN	
Area	**Annex I**	**Requirement**	**Baseline**	**OSSF Materials/Projects**
CRA Requirments	Annex 1			
Cybersecurity	1.1	Appropriate level of cybersecurity based on the risks	OSPS-SA-01, OSPS-SA-03	
Cybersecurity	1.2a	Made available on the market without known exploitable vulnerabilities	OSPS-SA-02, OSPS-VM-05, OSPS-VM-02, OSPS-VM-04, OSPS-VM-06	OSV, SIREN, oss-secur
Cybersecurity	1.2b	Made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;	OSPS-SA-01, OSPS-SA-02, OSPS-VM-05, OSPS-VM-04, OSPS-VM-06, OSPS-BR-05, OSPS-QA-04, OSPS-QA-05	BEST WG - Guides, Pa
Cybersecurity	1.2c	Ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them	OSPS-VM-05, OSPS-VM-02, OSPS-DO-02, OSPS-DO-05, OSPS-VM-06	
Cybersecurity	1.2d	Ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access	OSPS-AC-01, OSPS-BR-03, OSPS-AC-04, OSPS-AC-05, OSPS-BR-04, OSPS-BR-05, OSPS-GV-03, OSPS-GV-04,, OSPS-DO-03	gittuf
Cybersecurity	1.2e	Protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means	OSPS-AC-01, OSPS-BR-03, OSPS-AC-04, OSPS-AC-05,	
Cybersecurity	1.2f	Protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions	OSPS-AC-01, OSPS-AC-02, OSPS-AC-03, OSPS-AC-04, OSPS-BR-01, OSPS-BR-02, OSPS-BR-03, OSPS-QA-01, OSPS-LE-01, OSPS-AC-05, OSPS-BR-04, OSPS-BR-05, OSPS-QA-03, OSPS-QA-04	sigstore, SLSA, gittuf
Cybersecurity	1.2g	Process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation)		
Cybersecurity	1.2h	Protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;	OSPS-BR-04, OSPS-BR-05,	
Cybersecurity	1.2i	Minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks	OSPS-BR-03,	
Cybersecurity	1.2j	Be designed, developed and produced to limit attack surfaces, including external interfaces	OSPS-BR-03, OSPS-DO-01, OSPS-QA-01, OSPS-BR-04, OSPS-BR-05,OSPS-SA-03	threat model
Cybersecurity	1.2k	Be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques	OSPS-BR-03, OSPS-DO-01, OSPS-QA-03, OSPS-SA-03	threat model
Cybersecurity	1.2l	Provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user	OSPS-GV-02, OSPS-BR-04, OSPS-DO-02,	sigstore, monitoring
Cybersecurity	1.2m	provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner		PII protection/removal
Vuln handling	2.1	Identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products	OSPS-BR-05, OSPS-VM-01, OSPS-DO-02, OSPS-DO-06, OSPS-QA-02, OSPS-VM-05, OSPS-VM-06	CVD Guides, GUAC, O
Vuln handling	2.2	In relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates	OSPS-BR-05, OSPS-VM-01, OSPS-DO-02, OSPS-DO-06, OSPS-QA-02, OSPS-VM-05, OSPS-VM-04, OSPS-VM-06, OSPS-SA-03	CVD Guides
Vuln handling	2.3	Apply effective and regular tests and reviews of the security of the product with digital elements	OSPS-BR-05, OSPS-VM-01, OSPS-DO-02, OSPS-QA-02, OSPS-QA-06, OSPS-VM-05, OSPS-VM-06	Fuzz introspector, malic
Vuln handling	2.4	Once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch	OSPS-DO-02, OSPS-GV-02, OSPS-VM-04	CVD Guides, openvex,
Vuln handling	2.5	Put in place and enforce a policy on coordinated vulnerability disclosure	OSPS-BR-04, OSPS-DO-02, OSPS-VM-05, OSPS-VM-06, OSPS-VM-03	CVD Guides
Vuln handling	2.6	Take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements	OSPS-DO-02, OSPS-DO-05, OSPS-GV-02, OSPS-VM-01, OSPS-VM-04, OSPS-VM-03	CVD Guides
Vuln handling	2.7	provide for mechanisms to securely distribute updates for products with digita elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner	OSPS-VM-01	CVD Guides
Vuln handling	2.8	Ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.	OSPS-VM-01	CVD Guides

While not 100% coverage* (CRob has VERY FEW obligations under the CRA), we feel that if upstream projects follow the Baseline and if downstream uses the Baseline as a means to evaluate third-party components and work with your upstream providers to implement, that Manufacturers will have a VERY good start in providing evidence for THEIR compliance and attestation obligations!

**ONLY 19 out of 21 Annex I requirements….so sad*

Where to learn more/get engaged

EU CRA portal - https://www.european-cyber-resilience-act.com/

EU Expert Group - https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3967

ENISA - https://www.enisa.europa.eu/search?keys=cra#contentList

BSI (proactive National CERT, lots of useful implementation guides) - https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html

OpenSSF Global Cybersecurity Policy Working Group - Open, public forum where anyone can attend and participate https://github.com/ossf/wg-globalcyberpolicy/tree/main

OpenSSF Public Policy website + CRA microsite + other resources - https://openssf.org/?s=cra

LF Research “Unaware and Uncertain - The Stark Realities of Cyber Resilience Act Readiness in Open Source” - https://www.linuxfoundation.org/research/cra-readiness?hsLang=en

Eclipse ORC Working Group - https://orcwg.org/

Thanks!

The CRAfish →

Do you have any questions?

@~~SecurityCRob~~

@SecurityCRob@infosec.exchange

https://github.com/SecurityCRob

The Security Unhappy Hour,
Chips & Salsa
What's in the SOSS?

https://www.linkedin.com/in/darthcrob/