CRA Reporting obligations for Manufacturers - Resource Guide

From 11 September 2026, the Cyber Resilience Act (CRA) requires manufacturers to report actively exploited vulnerabilities (AEVs) and severe incidents having an impact on the security of their products with digital elements. Once a manufacturer becomes aware of such an event, it must report it through the EU Single Reporting Platform (SRP) within the applicable 24-hour, 72-hour deadlines followed by a final report within 14 days after a corrective or mitigating measure becomes available for AEVs, and within one month of the 72-hour notification for severe incidents. This one-pager summarises the key obligations and practical considerations for manufacturers from 11 September 2026.

11 September checks for Manufacturers:

1. Confirm your reporting scope

- ☐ For each product with digital elements, confirm that it falls within the scope of the CRA and determine whether your entity meets the CRA definition of a manufacturer;
- ☐ Ensure you have a process to assess whether a reported vulnerability is an AEV and whether an incident qualifies as a severe incident under Article 14(5);
- ☐ Identify the CSIRT designated as coordinator to which you must report under Article 14(7), based on your main establishment in the Union or, where applicable, the alternative criteria in the aforementioned article;
- ☐ Remember that Article 14 applies from **11 September 2026**, including in-scope products placed on the market before **11 December 2027** and after the product's support period has ended.

2. Be ready to report

Establish a process to report AEVs and severe incidents through the SRP. Make sure you have:

- ☐ One Primary Assigned Representative, with up to 20 Secondary Representatives, able to report through the SRP and ready with their EU Login accounts;
- ☐ Internal procedures to ensure timely identification, triage, and escalation of vulnerabilities and incidents that may trigger CRA reporting obligations;
- ☐ A process capable of meeting the 24-hour, 72-hour and final report deadlines;
- ☐ The relevant CSIRT designated as coordinator identified and ready for reporting;
- ☐ Knowledge of how to submit and regularly update an AEV or severe-incident notification through the SRP to be compliant with the relevant deadlines, including the information required at each reporting stage;
- ☐ A process to inform impacted users, and where appropriate all users, of relevant vulnerabilities and severe incidents and applicable mitigation or corrective measures (Art. 14(8)).

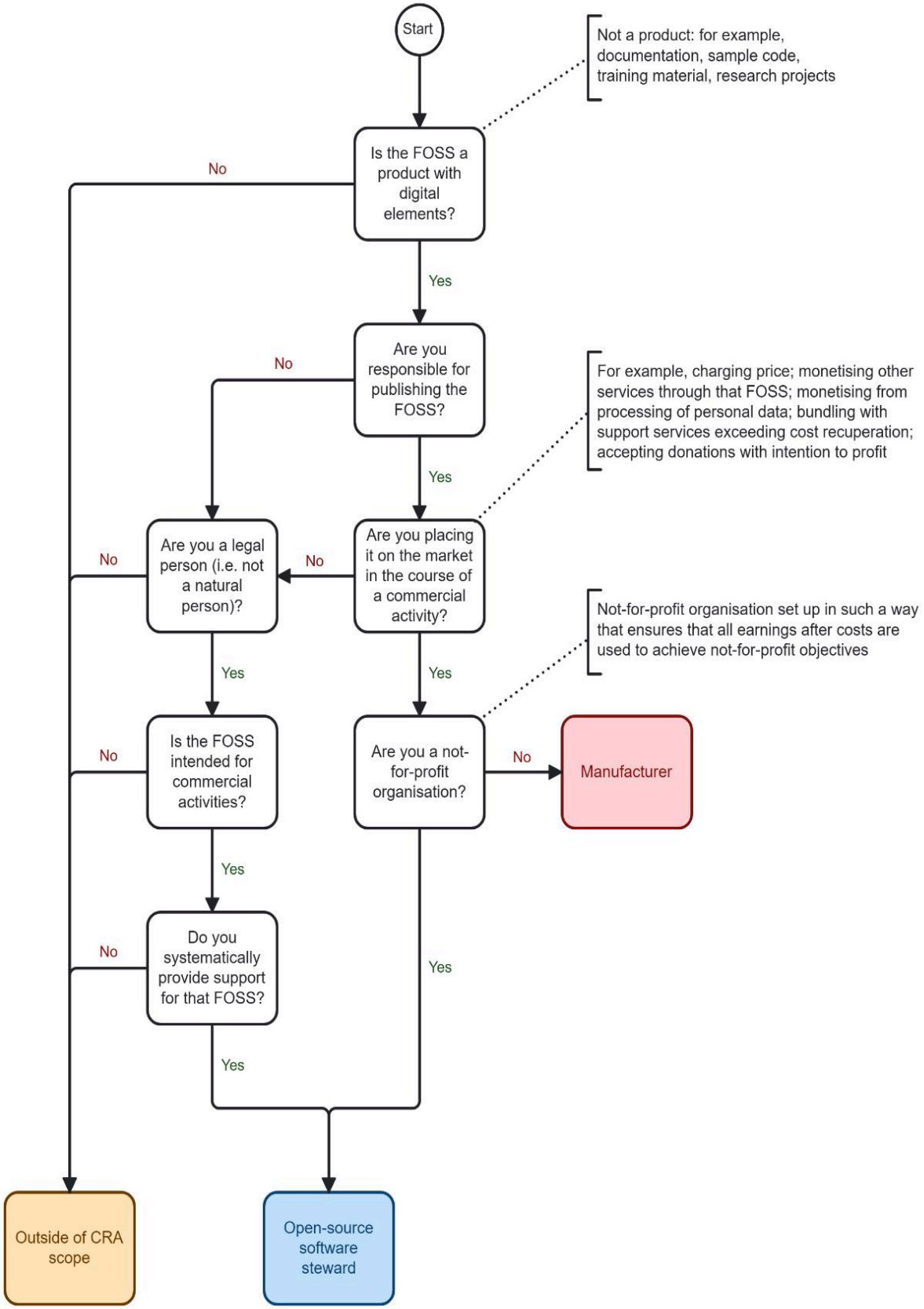
3. Recommended readiness measures (voluntary)

The measures below are recommended steps to support readiness and should not be read as additional CRA obligations applying from 11 September 2026.

- ☐ **Prepare product information**: Maintain up-to-date information on products, components, dependencies and relevant contacts to support rapid assessment and reporting;
- ☐ **Strengthen upstream collaboration**: Establish direct channels with maintainers of third-party and open source components that you leverage as part of your PDEs. Manufacturers are encouraged to apply the principles of Article 13(6) early, including sharing identified vulnerabilities and relevant fixes with upstream maintainers to support coordinated and timely remediation;
- ☐ **Test your reporting and response process**: Ensure relevant security, product, legal/compliance and communications teams understand their roles and can act quickly once an event is identified.

Appendix

Manufacturer vs steward - stylized flowchart[1]



[1] EC Guidance - https://ec.europa.eu/newsroom/dae/redirection/document/131456 - page 29

Appendix

Definitions

CRA Art. 3:

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

'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;

'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;

'support period' means the period during which a manufacturer is required to ensure that vulnerabilities of a product with digital elements are handled effectively and in accordance with the essential cybersecurity requirements set out in Part II of Annex I;

'remote data processing' means data processing at a distance for which the software is designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions;

Products within the scope of CRA:

CRA Guidance, 17: *"Article 3(1) of the CRA defines a product with digital elements as 'a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately'. Such products with digital elements fall within the scope of the CRA where their intended purpose or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network."*

CRA Guidance, 18: *"The CRA therefore can cover a range of products with digital elements, including: (i) standalone software, such as apps and computer programs, whether digitally or physically distributed; (ii) hardware with embedded software (e.g. Internet-of-Things devices, laptops, tablets); (iii) standalone hardware (e.g. integrated circuits, motherboards); and (iv) any combination of hardware and software supplied separately but intended to operate together."*

CRA Guidance, 19: *"Standalone software therefore falls in scope of the CRA where it is placed on the market as a product with digital elements. It is helpful to distinguish between software products with digital elements that are subject to the CRA and the remote provision of services that do not fall in scope of the CRA."*

Appendix

CRA Guidance, 20: *"For software to fall within the scope of the CRA, a software product with digital elements must be provided to a user, obtained by that user and operated on, or as part of, an electronic information system on the user's side. Software that is downloaded, installed or otherwise supplied to the user and that executes on the user's electronic information system meets these criteria, including for example where it takes the form of a browser extension or an application developed using web technologies but supplied for local execution."*

CRA Guidance, 21: *"By contrast, software that executes remotely and is merely accessed by the user is not, on that basis alone, a product with digital elements. Recitals 11 and 12 of the CRA, in fact, draw this distinction, by explaining that processing or storage at a distance is subject to the CRA only to the extent that it is necessary for a product with digital elements to perform its functions (i.e. through the concept of remote data processing as defined in Article 3(2)), and not themselves as products with digital elements. This is typically the case for web applications, including progressive web apps, where they are accessed exclusively through a web browser. The same applies to websites: whilst websites may, to a limited extent, technically run and execute on the user's device, it follows from recital 12 of the CRA that websites are not themselves to be considered as products with digital elements, and fall within the scope of the CRA only where they support the functionality of a product with digital elements, i.e. to the extent that they qualify as remote data processing"*

Manufacturers vs stewards:

CRA Guidance, 52:*"manufacturers of FOSS supply versions for free of that software (often called 'community' versions), whose codebase is (almost) identical to the paid version. Those products with digital elements, however, are different products: the paid version is monetised in some way (e.g. either by charging a price or via other means as discussed in this section) and therefore considered to be placed on the market, triggering the manufacturer's obligations. The version provided for free (or community version) is not monetised and therefore is not considered to be placed on the market for the purposes of the CRA."*

CRA Guidance, 56: *"The decisive factor is whether access to the FOSS itself (i.e. the provision of the product with digital elements), including its maintenance, is conditioned on remuneration, rather than the mere offering of professional services around a freely available product with digital elements, as indicated in recital 18 of the CRA ('the provision of products with digital elements qualifying as free and open-source software that are not monetised by their manufacturers should not be considered to be a commercial activity'). Where the FOSS can be downloaded and installed freely, and users can optionally choose to purchase professional services separately, that FOSS is not considered to be placed on the market."*

CRA Guidance, 57: *"By contrast, in some cases access to a specific version of the product with digital elements including certain benefits such as technical assistance or performance optimisation, is conditioned on remuneration. In such cases, that provision constitutes a*

Appendix

monetised provision of a product with digital elements supplied in the course of a commercial activity and is therefore considered placed on the market. This includes cases where a paid edition or enterprise version is made available under a commercial agreement, irrespective of whether functionally equivalent software is also available free of charge under a free and open-source licence."

Vulnerability reporting obligations

Citation	Requirement	*TL/DR*
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.	*establish an EU National CSIRT contact, report known actively exploited vulns to EU National CSIRT contact and ENISA*
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.	*AEV reporting: submit the early-warning notification without undue delay and in any event within 24 hours of becoming aware of the actively exploited vulnerability; submit the vulnerability notification without undue delay and in any event within 72 hours of becoming aware; and submit the final report no later than 14 days after a corrective or mitigating measure is available.*
Article 14	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.	*Severe security incident -> notify CSIRT + ENISA simultaneously via the single reporting platform.*
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; (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	*Manufacturers must report severe security incidents in 3 stages: Within 24h: Early warning + whether malicious/unlawful activity is suspected. Within 72h: Incident details, initial assessment, and*

Appendix

Citation	Requirement	*TL/DR*
	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.	*mitigation measures. Within 1 month after the submission of the incident notification: Final report with severity/impact, likely cause/threat, and mitigation measures.*
Article 14	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.	*Notification of impacted users*

*CRA, article 3(42): '**actively exploited vulnerability**' means a vulnerability for which there is reliable evidence that a malicious actor has exploited it in a system without permission of the system owner;*

*CRA, article 3(44): '**incident** having an impact on the security of the product with digital elements' means an incident that 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 data or functions;*

The **criteria for severity** are defined in Article 14(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.*"

EC FAQ 5.1: "How can a manufacturer become aware of an actively exploited vulnerability or a severe incident?

The CRA does not specify how a manufacturer is to become aware of an actively exploited vulnerability or a severe incident, but rather imposes the obligation to notify in accordance with Articles 14 once it does.

Appendix

The paragraphs below provide some examples on how a manufacturer may become aware of such vulnerabilities or incidents, via a variety of activities and channels. It should be noted that this does not imply that the manufacturer is required to carry out such activities or monitor such channels to comply with the reporting obligations.9

For example, a manufacturer may become aware because a customer or a partner organisation inform it of unusual activity or compromise, providing the manufacturer with reliable evidence that an actively exploited vulnerability is contained in its product (or the manufacturer gathers reliable evidence confirming its existence).

A manufacturer may also become aware via threat intelligence reports, e.g. security researchers or cybersecurity firms publish reports detailing a zero-day vulnerability (i.e. a vulnerability for which a patch or a security update is not yet available) in the manufacturer's product being used in targeted attacks. Governmental cybersecurity agencies may also notify the manufacturer, having detected exploitation of a vulnerability through their monitoring systems. Ethical hackers may also report a vulnerability that is already being exploited in the wild.

Furthermore, the manufacturer may also become aware via internal monitoring, scanning activities or telemetry. For example, the manufacturer's telemetry system or honeypot (i.e. a security mechanism used to lure cybercriminals away from legitimate targets) indicates exploitation of a previously unknown vulnerability in the manufacturer's product, or the manufacturer's security team monitors dark web forums and finds evidence that hackers have successfully exploited a vulnerability in the manufacturer's product."

EC FAQ 5.3: "*By way of derogation from paragraph 2 of this Article, the obligations laid down in Article 14 shall apply to all products with digital elements that fall within the scope of this Regulation that have been placed on the market before 11 December 2027 (Article 69(3)).*

Reporting obligations start applying as of 11 September 2026. Manufacturers are required to comply with Article 14, and particularly with the obligation to notify actively exploited vulnerabilities and severe incidents having an impact on the security of the product for all products with digital elements falling within the scope of the CRA, including products that have been placed on the market before 11 December 2027.

If the product has been placed on the market before 11 December 2027, manufacturers may not be able to investigate such vulnerabilities, for example because tooling to scan or run old software versions may no longer exist, build environments for old code may be impossible to recreate, dependencies may be unavailable or incompatible with modern systems, staff with knowledge of old codebases may have left. For such products, manufacturers are required to notify the vulnerability or incident but are not required by the CRA to comply with other obligations, e.g. in relation to vulnerability handling.

Furthermore, the obligation to notify applies upon becoming aware following the entry into application of the reporting requirements

Appendix

Nonetheless, Article 14(8) requires the manufacturer to inform the impacted users of the product with digital elements, and where appropriate all users, of those vulnerabilities or incidents. Where the manufacturer decides not to inform the users of the product with digital elements in a timely manner, the CSIRTs that receive the notification 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." The same topic is explained also in the CRA Guidance, 210 and detailed further in CRA Guidance, 219-221

CRA Guidance, 213 *"In some cases, a manufacturer will detect a suspicious event, or a third party, such as an individual, a customer, an entity, an authority, a media organisation or other source will bring a potential incident or vulnerability to its attention. In such cases, the manufacturer should assess the suspicious event immediately to determine whether it constitutes an actively exploited vulnerability or a severe incident having an impact on the security of the product with digital elements. The manufacturer is therefore to be regarded as having become aware when, after such an initial assessment, it has a reasonable degree of certainty that: (i) a vulnerability contained in its product with digital elements is being actively exploited; or (ii) a severe incident has occurred and has led to the security of its product with digital elements being compromised."*

CRA Guidance, 214 *"Therefore, the point in time at which a manufacturer can be considered to be aware will depend on the circumstances of the specific actively exploited vulnerability or severe incident. In some cases, it will be relatively clear from the outset that a vulnerability is being actively exploited or that a severe incident is impacting the security of a product with digital elements. In others, it may take some time to establish whether a product with digital elements is affected by a vulnerability and whether that vulnerability is being exploited by a malicious actor, or whether an incident is impacting the security of a product with digital elements. However, the emphasis should be on prompt action to carry out the initial assessment to determine whether such conditions are indeed met, particularly where the vulnerability may pose a significant risk, and if so, to take remedial action and notify in accordance with the CRA."*

CRA Guidance, 217*"It should also be clarified that, because the obligation to report actively exploited vulnerabilities applies when the manufacturer becomes aware of active exploitation, the manufacturer is not required to report vulnerabilities of whose active exploitation it had already become aware before 11 September 2026 (the date on which the reporting obligation starts to apply). The CRA, therefore, does not require the retroactive reporting of such vulnerabilities. By contrast, the obligation does apply where the manufacturer was aware of a vulnerability before 11 September 2026 but was not, at that time, aware of any active exploitation of it (either because none had yet occurred or because the manufacturer had not become aware of it). If, after 11 September 2026, active exploitation subsequently occurs or the manufacturer becomes aware of it, the vulnerability is deemed an actively exploited one subject to the reporting obligation."*

Appendix

EC FAQ 5.4: "'*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 [...]*

A manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of (Article 14(1))

Manufacturers should notify actively exploited vulnerabilities to ensure that the CSIRTs designated as coordinators, and ENISA, have an adequate overview of such vulnerabilities and are provided with the information necessary to fulfil their tasks as set out in Directive (EU) 2022/2555 and raise the overall level of cybersecurity of essential and important entities as referred to in Article 3 of that Directive, as well as to ensure the effective functioning of market surveillance authorities. As most products with digital elements are marketed across the entire internal market, any exploited vulnerability in a product with digital elements should be considered to be a threat to the functioning of the internal market (Recital 66).

Manufacturers are required to notify any actively exploited vulnerability contained in their product with digital elements. Where the product with digital elements contains an actively exploited vulnerability originating from an integrated component, the manufacturer of the product with digital elements is required to notify that vulnerability. The manufacturer of the integrated component is also required to notify it, if that component has been placed on the market.

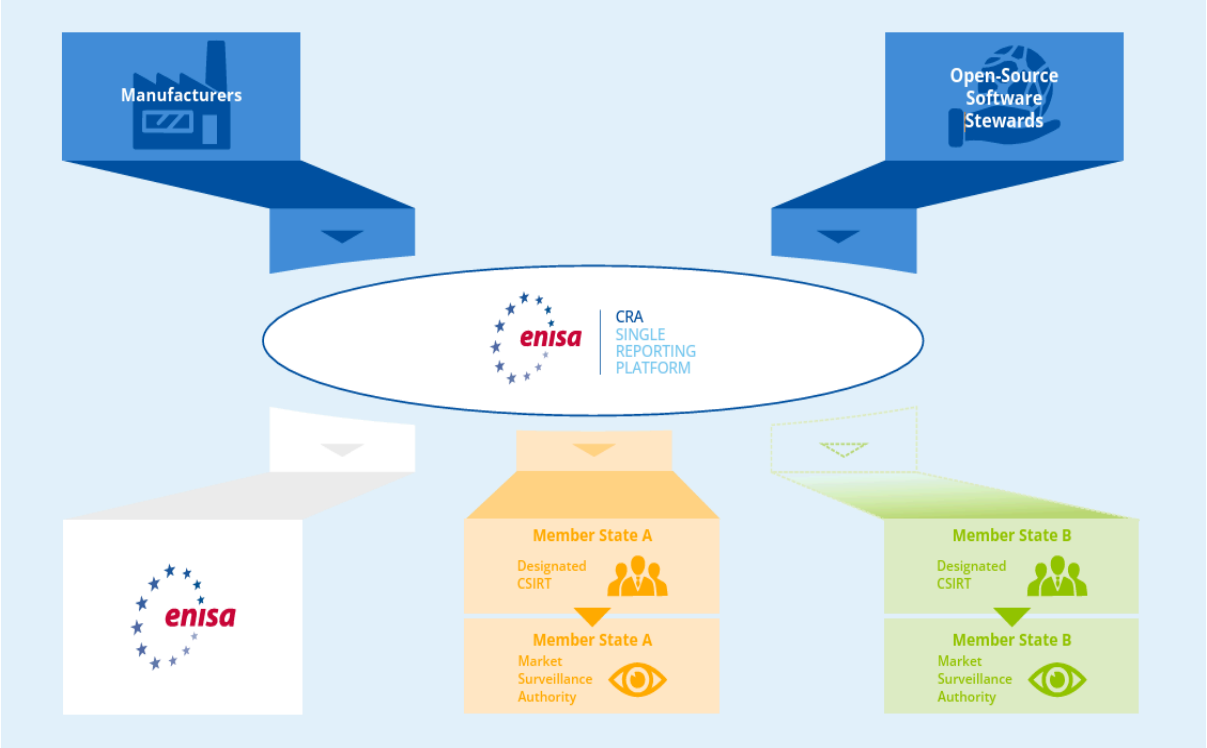
If the manufacturer of a product with digital elements is aware that an integrated component contains a vulnerability, but that vulnerability cannot be exploited in its product with digital elements, that vulnerability is not actively exploited, and therefore it is not subject to mandatory reporting. Manufacturers can still notify that vulnerability on a voluntary basis, in accordance with Article 15, and are required to report the vulnerability to the person or entity manufacturing or maintaining the component, in accordance with Article 13(6). For further information see* CRA Guidance, 218

This enables the CSIRTs receiving the notification and ENISA to have an overview of the security landscape in the internal market and to assess the level of criticality and market penetration of actively exploited vulnerabilities."

**Voluntary reporting will not be in place at 11 September 2026*

Appendix

Simple submission flow[2]:



Reporting process and timelines[3]:

[2] https://www.enisa.europa.eu/sites/default/files/2026-07/ENISA_CRA_SRP_Factsheet_v1.0_0.pdf
[3] https://www.enisa.europa.eu/sites/default/files/2026-07/ENISA_CRA_SRP_Factsheet_v1.0_0.pdf