NetApp

CRA IS HERE

Are you ready?

Sridhar Balasubramanian
Principal Product Security Architect
October 2026

© 2026 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

Agenda

- Three Q’s
- Product Scope and Exclusions
- Reporting Framework
- Conformance Requirements
- Recommended approach for organizations

NetApp

© 2026 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

Three Questions

Vulnerability Reporting

A vulnerability reported by an EU customer in our product with digital elements.

Our developer/SME found it to be exploitable under certain conditions.

Does this qualify to be reported to ENISA under mandatory reporting?

Answer: No. Mandatory reporting only applies to actively exploited vulnerability.
Ref: Article 14

Security Incident Reporting

We had a security incident due to unauthorized access by an adversary that resulted in an outage of our IT systems, which are separated from development.

Does this qualify to be reported to ENISA under mandatory reporting?

Answer: No. Mandatory reporting only applies to an incident that adversely impacts security of product with digital elements.
Ref: Refer Article 14

Integrated Third-party components

Our supplier reported a publicly exploited vulnerability in the component they develop for us.

Our developer/SME determined our product is not exploitable due to that vulnerability.

Does this qualify to be reported to ENISA under mandatory reporting?

Answer: No.
Ref: ENISA SRP FAQ 14, European Commission's FAQ: 5.4, EU Commission guidance, paragraph: 218

© 2026 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

Product Scope: EU CRA Articles 3 and 24

Annex III and IV: Product Classifications

Digital Elements

‘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;

Remote data processing

‘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

Open Source

Open-source software stewards will be subject **to reporting obligations, starting from 11 December 2027**, to the extent that they are involved in the deployment of products with digital elements, in accordance with Article 24(3) of CRA

Ref: FAQ #5

NetApp

© 2026 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

Product Scope Exclusions: EU CRA Article 2

Non-applicable product categories

Specific Categories

Medical devices and in-vitro diagnostics under Regulations (EU) 2017/745 and (EU) 2017/746.

Civil aviation products certified under Regulation (EU) 2018/1139.

Motor vehicles and their trailers governed by Regulation (EU) 2019/2144 and UN Regulation No. 155.

Marine equipment falling within the scope of Directive 2014/90/EU.

Spare Parts

Spare parts that are made available on the market to replace identical components in products with digital elements and that are manufactured according to the same specifications as the components that they are intended to replace.

Cyber Security/Defense

Products with digital elements developed or modified exclusively for national security or defense purposes or to products specifically designed to process classified information.

© 2026 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

Reporting Framework

Enforced from September 11, 2026

Reporting Scope

- Vulnerability reporting when there is an **actively exploited vulnerability** found in the product containing digital elements placed in EU/EEA market.
- Security incident reporting if an **incident adversely impacts** the product with digital elements placed in EU/EEA market.
- **Security updates** (releases with security fixes) must be made available for 10 years from the date of issuance of the publicly posted software releases or until the product reaches end of support period, whichever occurs earlier.

Who needs to report?

- Authorized Representative (AR) on behalf of the manufacturer of the product with digital elements must establish a user account via ENISA Single Reporting Platform (SRP), by registering with SRP.
- It it appropriate to designate the AR from the Security Incident Response group (PSIRT or CSIRT) within the manufacturer's organization.
- AR must follow the user registration process as described in ENISA SRP portal.

How to Report?

- ENISA SRP reporting/notification process is using a manual form-based submission with specific data fields to indicate 24 hours (early warning), 72 hours and Final report associated with an actively exploited vulnerability or a security incident.
- Such notifications must be linked to the manufacturer of the product with digital elements.
- If not already present, Manufacturers can be added in ENISA SRP.

NetApp

© 2026 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

Conformance Requirements (Abstract)

To be enforced from December 11, 2027

Article 13

Manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential cybersecurity requirements set out in Part I of Annex I.

Manufacturers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements.

Annex I Part I

Made available on the market without known exploitable vulnerabilities.

Made available on the market with a secure by default configuration.

Vulnerabilities can be addressed through security updates, including automatic security updates.

Protection from unauthorized access and the confidentiality of stored, transmitted or otherwise processed data.

Capability for users to securely and easily remove on a permanent basis all data and settings.

Annex I Part II

SBOM in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products.

Address and remediate vulnerabilities without delay, including by providing security updates, if feasible, separately from functional updates.

Once a security update has been made available, share and publicly disclose information about fixed vulnerabilities.

Enforce a policy on coordinated vulnerability disclosure.

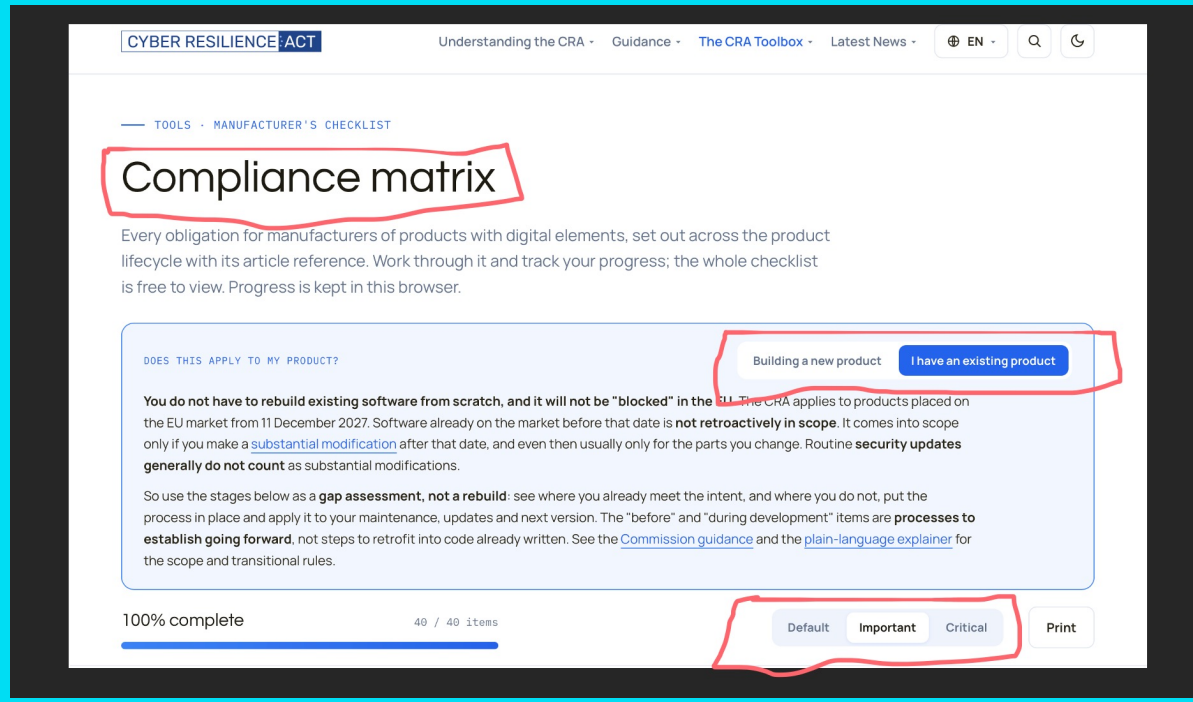
© 2026 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

CRA Compliance Checklist

Ref: EU Commission Guidance: July 27, 2026

- A compliance matrix checklist made available as part of CRA toolbox for manufacturers.
- Select product classification: Default, Important or Critical, as applicable.
- Select the checklist option applicable to your use case
  - Building a new product (or)
  - I have an existing product
- Compliance areas are divided into 5 sections
  - Company level foundations
  - Before development
  - During development
  - Before product release
  - After product release

Manufacturer's Checklist



NetApp
© 2026 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

Proposed Approach for organizations

Step by step guidance

- Reporting obligation is already in force since September 2026.
- Determine Product scope
  - Product with digital elements placed in EU/EEA market after September 11, 2026.
- Establish single point of technical contact for each product identified in scope
- Gear up the Incident Response team in your organization to:
  - Develop reporting data structure as per data fields for notifying actively exploited vulnerabilities in products with digital elements or incidents that adversely impacts the security of the products with digital elements, by following notification guidelines at SRP.
  - On behalf of the organization, Authorized Representative (AR) must establish an account in ENISA SRP through user registration per procedure.
- Conformance obligation is expected to commence by December 11, 2027.
  - This implies the enforcement applies to product with digital elements placed in the EU/EEA market after Dec 11, 2027.
  - If products with digital elements placed in the market prior to Dec 11, 2027, underwent substantial modification after Dec 11, 2027, and still offered for sale and placed in the market will also be in scope for conformance requirements per Article 69, Paragraph 2.
- Establish baseline requirements for the products in scope by reviewing Annex I Part I and Part II.
  - Develop auditing workflows as part of SDLC process for each product as part of risk assessment on per SW/HW release basis.
  - Gather evidential information and artifacts to serve towards conformance fulfillment as part of the SDLC process and maintain it throughout the lifecycle of the product.
- Introduce EU Declaration of Conformity and sign-off process upon successfully validating conformance requirements are being met for the product.
  - As described in Annex V, per terms in Article 28.

© 2026 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

References

- EU CRA:
  - https://eur-lex.europa.eu/eli/reg/2024/2847/oj
- ENISA:
  - https://www.enisa.europa.eu/
- SRP:
  - https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/cra-srp-guidance-ar-user-registration
- ENISA SRP FAQ:
  - https://www.enisa.europa.eu/topics/product-security-and-certification/single-reporting-platform-srp#
- EU Commission Guidance:
  - https://digital-strategy.ec.europa.eu/en/library/commission-publishes-new-guidance-support-timely-cyber-resilience-act-implementation
- Manufacturer's checklist:
  - https://www.cyberresilienceact.eu/compliance-matrix.html

© 2026 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

THANK YOU

NetApp

© 2026 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL