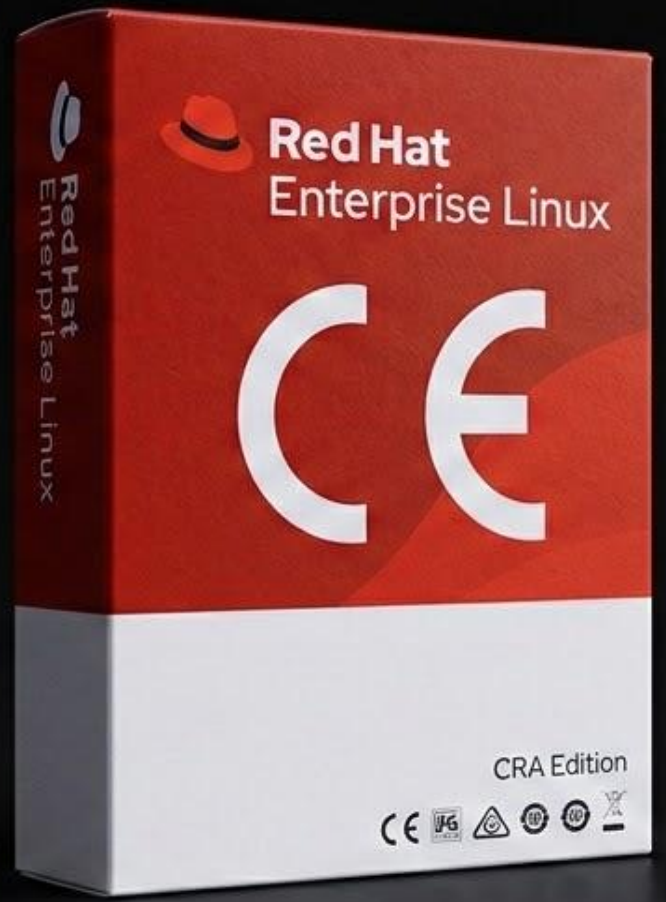
EU CRA and the cybersecurity harmonised standards

Jaroslav Řezník
Red Hat, Product Security
Compliance, Governance and Risk

Red Hat


Red Hat
Enterprise Linux
CE
Red Hat
Enterprise Linux
CRA Edition

Cyber Resilience Act (CRA) EU Regulation 2024/2847

Products with Digital Elements (PDE) - all software or hardware with software placed on the EU market

- **Unless other regulations/directives are already in place (SaaS, automotive, health...) but RDPS**
- **PDEs in development (alpha, beta, etc...)**
- **And Free and Open Source software (FOSS)**



Core Goals

- Reduce vulnerabilities
- Product lifecycle security
- Enable Informed decisions for users
- **Risk Assessment driven**
- Essential Requirements



Scope & Roles

- Targets mostly Manufacturers (Red Hat), Importers and Distributors
- Covers 3rd party dependencies
- Defines open source Stewards



Compliance

- Worldwide applicability for commercial activity within EU
- Fines up to €15M or 2.5% global turnover



Red Hat Product Categorization and Compliance to CRA Standards



Default Category

- All products not listed in other categories, expectation is 90 percents of all products belongs to this category.
  - Consumer devices, toys, games etc.
- Self-assessment, compliance to **Essential Requirements** and harmonised vulnerability handling standard (prEN 40000-1-3)



Important Class I and II

- Class I (self-assessment against vertical harmonised standards)
  - Operating systems (*RHEL*)
  - PKI (*RHCS*)
  - Browsers, password managers etc.
- Class II (3rd party assessment)
  - Hypervisors and containers (*OpenShift Virtualization*)
  - Firewalls etc.



Critical

- Smart Cards
- Secure Elements
- Smart meter gateways

- EUCC Delegated Act Draft

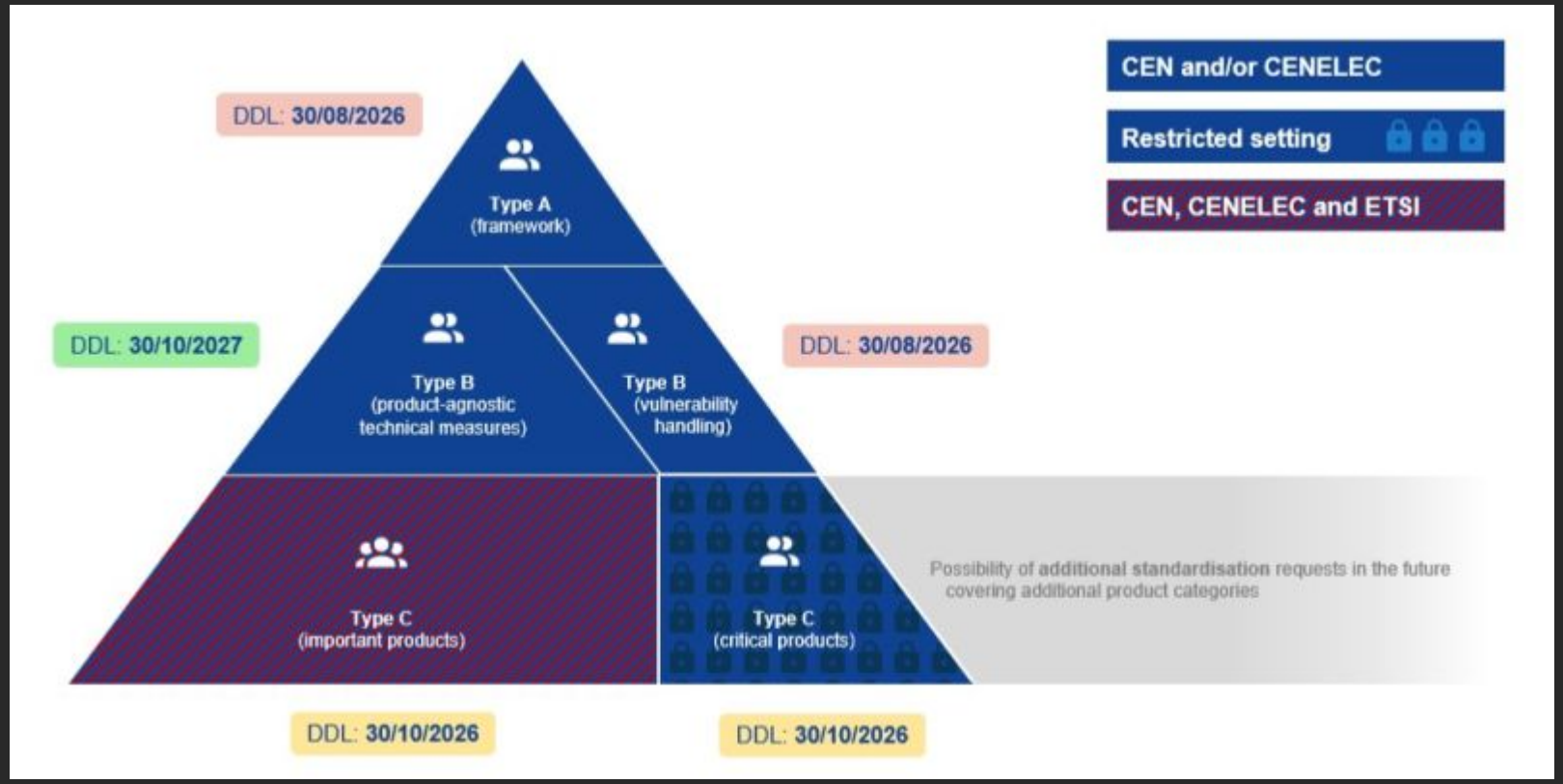
Harmonised Standards and Standardisation Request

- Prepared by European Standardisation Organisations (ESO)
  - CEN/CENELEC for Horizontal standards
  - ETSI for Vertical standards
- Standardisation Request M/606
- Harmonisation - all standards needs to be referenced in the Official Journal of the European Union (OJEU)
  - **Optional but part of the EU law!**
  - The Court of Justice of the European Union (CJEU) is the ultimate CRA arbiter.

Source:
https://single-market-economy.ec.europa.eu/single-market/goods/european-standards/key-players-european-standardisation_en
https://ec.europa.eu/transparency/documents-register/detail?ref=C(2025)618&lang=en
https://single-market-economy.ec.europa.eu/single-market/goods/european-standards/harmonised-standards_en



Harmonised Standards and Standardisation Request



Source:
https://digital-strategy.ec.europa.eu/en/policies/cra-standardisation

Horizontal Standards

- Horizontal standards are across all product categories
- Developed under CEN/CENELEC JTC13 WG9
- Vocabulary (prEN 40000-1-1) - **approved**
- Principles (prEN 40000-1-2) - **approved**
- Vulnerability Handling (prEN 40000-1-3) - **final draft**
- Generic Security Requirements (prEN 40000-1-4) - **public enq**



Horizontal Standards

Vulnerability Handling

- Cybersecurity requirements for products with digital elements, Part 1-3: Vulnerability handling (prEN 40000-1-3)
  - This standard brings **Presumption of Conformity** to all products including the Default CRA category
  - Everyone needs to be fully compliant, otherwise every product would need to go through the Notified Body evaluation (or Module H)
- Red Hat participated during the development, shared comments, etc.
- Free of charge updates were removed from the Assessment Criteria as it is not a technical requirement but business relationship



Horizontal Standards

Other 40000 series standards

- The remaining standards in the 40000 series do not give the Presumption of Conformity
- Are fully optional; however for example prEN 40000-1-2 talks about risk assessment, prEN 40000-1-4 transposes CRA into controls, etc.
- Likely won't be harmonised at all



Horizontal Standards

Timeline

Overall planning JTC 13/WG 9

UPDATED!
2026-08-28

MMM YYYY	F2F	40000-1-1 JT013095	40000-1-2 JT013089	40000-1-3 JT013090	40000-1-4 JT013091	Location	Dates	Focus
Feb 2026	*	CR	CR	ENQ	Drafting	Frankfurt, DE	Mon 9 – Fri 13 Feb	**PT1,PT2,PT3 HAS cmnts**
Mar 2026	*	CR	CR	CR preparation	Drafting + EC	Paris, FR	Thu 26 Mar	**1 Day only: PT1,PT2,PT3**
Apr 2026	*	CR + Prep-FV	CR + Prep-FV	CR	Drafting	Oslo, NO	Mon 20- Tue 21 Apr	**PT1 CR ONLY**
May 2026	*	EC	Submit to EC	CR	Drafting	Stockholm, SE Berlin, DE	Tue 5- Fri 8 May Wed 27-Thu 28 May	**PT1,PT2,PT3** **PT2 Editing ONLY**
Jun 2026	*	CR EC + Drafting	EC	CR	Drafting	Linköping, SE	Mon 29 Jun- Fri 3 Jul	**PT1 CR,PT2,PT3 (Priority)**
July 2026		CR EC + Drafting	CR EC	CR + submit EC	EC (1st week)	Eindhoven, NL	Thu 16 – Fri 17 Jul	**PT3 Editing ONLY**
request Aug 2026		FV	FV	EC	CR EC			
Sep 2026	*	FV	FV	CR EC	CR EC / Prep ENQ	Cyprus, CY	Tue 22- Fri 25 Sep	(PT1,) **PT2, PT3**
new Oct 2026		CR	CR	CR EC / Prep-FV	CR EC / Prep ENQ			
Nov 2026		PUB	PUB	FV	ENQ			
Dec 2026		2nd edition	-	FV	ENQ			
Jan 2027		↓	-	CR	ENQ			
Feb 2027		↓	-	PUB	CR→PUB | CR→FV			
Mar 2027		↓	-	-	PUB | CR			
Apr 2027		↓	-	-	2nd ed | Submit EC			
Jun 2027		↓	-	-	↓ | ↓ 30/10			

CR = Comment resolution; ENQ = Enquiry; FV = Formal Vote; PUB = Publication
Note: TR/40000-1-5 JT013097 discontinued

CEN CENELEC

CEN-CLC JTC 13 / WG 9 - Meeting slides 17

Vertical Standards

- Vertical standards are applicable to product categories based on a technology for Important Class I and Class II (Annex III) PDEs
- 17 standards
- Intended purpose
- For example
  - Operating systems - Red Hat Enterprise Linux
- Auxiliary standards
  - Password managers, antivirus, etc...

Source:
https://docbox.etsi.org/CYBER/EUSR/Open



Vertical Standards

- EN 304-617 Browsers
- EN 304-618 Password Managers
- EN 304-619 Antivirus
- EN 304-620 Virtual Private Networks
- EN 304-621 Network Management Systems
- EN 304-622 Security Information Event Management
- EN 304-623 Boot Managers
- EN 304-624 PKI Certificate Issuance Software
- EN 304-625 Network Interfaces
- EN 304-626 Operating Systems
- EN 304-627 Routers, Modems, Switches
- EN 304-631 Smart Home Virtual Assistants
- EN 304-632 Smart Home Security Products
- EN 304-633 Internet Connected Toys
- EN 304-634 Personal Wearables
- EN 304-635 Virtualization Container
- EN 304-636 Firewalls

Source:
https://docbox.etsi.org/CYBER/EUSR/Open

Vertical Standards

Operating Systems

- Cybersecurity requirements for operating systems (ETSI prEN 304 626)
  - Red Hat is involved in the development of the standard together with Debian/OSI, SUSE, Google and Microsoft
- Public enq draft, HAS (Harmonised Standards) Consultant comments resolution, more NSO comments to come

Source:
https://docbox.etsi.org/CYBER/EUSR/Open/EN_304-626_V1.0.1_2026-08-12_Operating-Systems_Enquiry-draft.pdf



Vertical Standards

VES/CES

- Cybersecurity requirements for Virtualisation Execution Stack (VES)

  and Container Execution Stack (CES), including hypervisors and container runtime systems (ETSI prEN 304 635)
- Red Hat is involved in the development of the standard
- Public enq draft, HAS (Harmonised Standards) Consultant comments resolution, more NSO comments to come
- Comment on VES/CES split, now formal comment by Irish NSO

Source:
https://docbox.etsi.org/CYBER/EUSR/Open/EN_304-635_V1.0.1_2026-06-24_Virtualization_Container_Enquiry-draft.pdf



Machine-readable access to standards

To allow automation

- Standards are not available in machine-readable form
- Mostly PDFs, development versions in docx... (same ver, different content)
  - OS was initially Markdown on GitHub but moved to docx
  - Horizontals - OSD tool
  - Intellectual Property
- It is not possible to share standards in machine-readable form even some manufacturers already do it (in OSCAL)
- Vibe-coded extraction tool to Gemara and OSCAL. Each standard is different, they do not follow the same structure etc.
- Standards are not redistribuable, the tool is (will be)

Source:
https://docbox.etsi.org/CYBER/EUSR/Open/EN_304-635_V1.0.1_2026-06-24_Virtualization_Container_Enquiry-draft.pdf

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.



linkedin.com/company/red-hat



youtube.com/@redhat



facebook.com/redhat



x.com/RedHat

Red Hat