

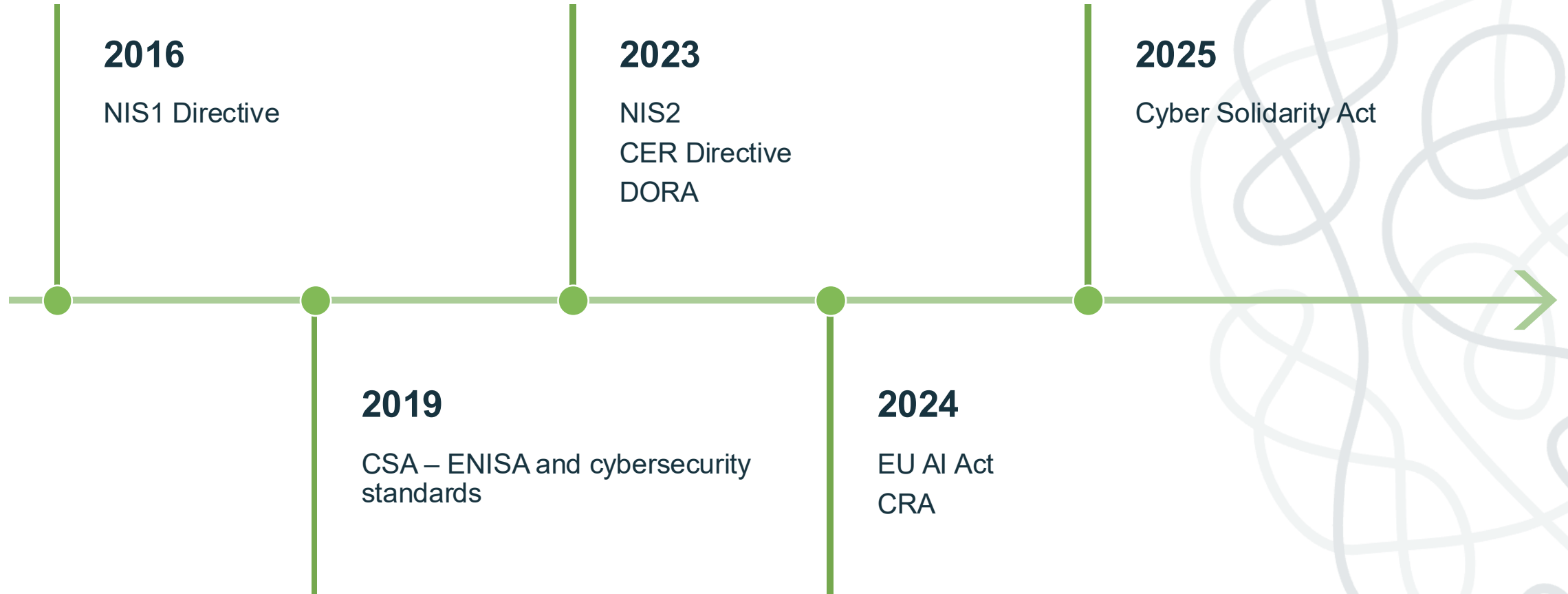
Beyond NIS2: Software Supply Chains, and the Cyber Resilience Act (CRA)

Barry O'Donovan, INEX

45th Euro-IX Forum, Utrecht, October 12th, 2026

Regulatory Tsunami

Legislative Milestones



Political Backlash & Competitive Alarms

- French President Emmanuel Macron explicitly called for a European **regulatory pause**, arguing that Europe must digest existing legislation rather than imposing new burdens...
- Mario Draghi's landmark 2024 report on EU Competitiveness delivered a **scathing critique** of the digital regulatory regime.
 - the EU has generated over 100 tech-related laws
 - And over 270 digital networks regulatory bodies



Subscriber Only Politics

Irish civil servants criticised in private missive for delays in transposing EU rules

Department of Taoiseach secretary general privately chastised colleagues for delays in transposing European legislation



NIS2 & the CRA

NIS2 and the CRA

- NIS2 now applies to most of us as operators of IXPs.
- This creates a legal obligation to manage operational cyber risk and supply chain vulnerabilities.
- What about the software manufacturers and open-source projects supplying us?
- Enter the Cyber Resilience Act (CRA):
 - Imposing direct cybersecurity and vulnerability reporting obligations on software made available on the EU market.

NIS2 and the CRA

NIS2 governs
how you run
your exchange.

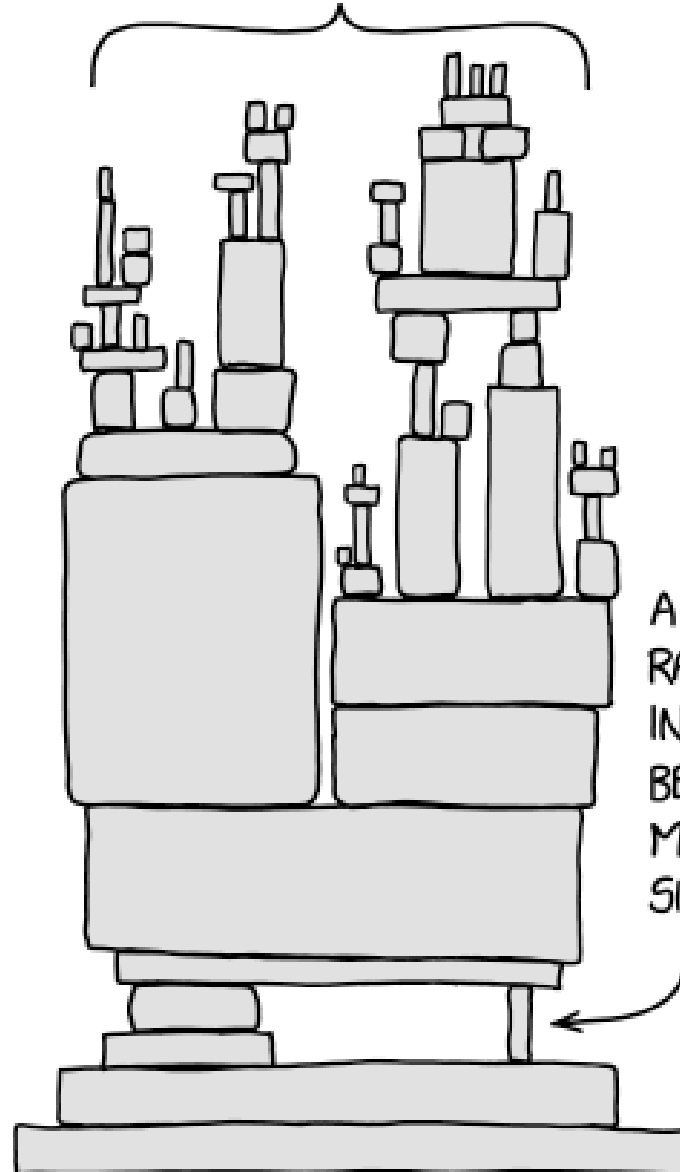
The CRA
governs the
software you
run it with.

NIS2/CRA – Understanding the Interconnection

	NIS2 Directive	The CRA
Who is regulated?	Operators (IXPs, telcos, utilities, cloud)	Makers (Software developers, vendors, OSS Stewards)
Primary Focus	Operational resilience, incident management	‘secure-by-design’ and ‘secure-by-default’ baselines, whole-lifecycle vulnerability management & support
Vulnerability Mandate	Duty to discover, patch and maintain supply chain hygiene	Duty to report active exploits to ENISA, deliver free fixes
Reporting Trigger	<i>Significant incidents</i> disrupting your IXP	<i>Actively exploited vulnerabilities</i> in software products

Open Source Under the CRA

ALL MODERN DIGITAL
INFRASTRUCTURE



A PROJECT SOME
RANDOM PERSON
IN NEBRASKA HAS
BEEN THANKLESSLY
MAINTAINING
SINCE 2003

Open-Source Software Stewards

The CRA recognises that non-profit foundations are different from commercial vendors.

‘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

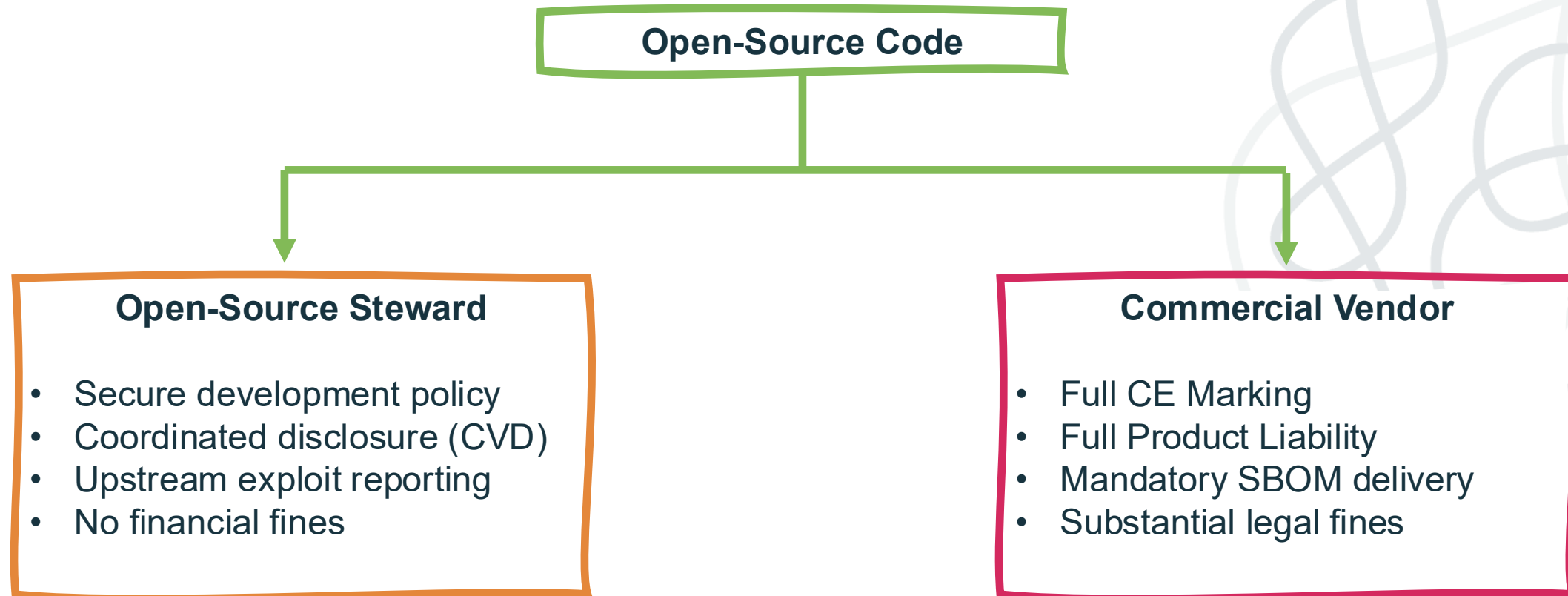
Individual FOSS Developers Not In Scope

- Software is only regulated if it is supplied "in the course of a commercial activity."
- The CRA explicitly states that the mere act of hosting software on open repositories, collaboration platforms (like GitHub or GitLab), or distributing it through package registries (like PyPI or npm) does not constitute making software available on the commercial market.
- None of the following activities push an ad-hoc project into CRA scope:
 - Accepting voluntary donations or tips, provided they are intended to offset hosting or development costs rather than generate commercial profit.
 - Tagging regular software releases or setting up automated CI/CD pipelines.
 - Receiving bug fixes or pull requests from engineers employed by commercial corporations.
 - Receiving non-commercial public research grants or academic funding.

The CRA: Stewards vs. Commercial

	Open-Source Software Steward	Commercial Open-Source Vendor
Legal & Financial Nature	Non-profit foundation, industry association, or public-benefit entity. Operates on donations, grants, or membership dues.	For-profit company or commercial venture charging for software, subscriptions, or proprietary add-ons.
Monetisation Model	Code is freely distributed without charging license fees or selling enterprise "paywalled" tiers.	"Open Core" (free basic / paid enterprise), commercial support contracts tied directly to product delivery, or paid dual-licensing.
Examples in our Ecosystem	INEX (IXP Manager), CZ.NIC (BIRD), Nlnet Labs (Unbound, Routinator, ...) ...	Enterprise Linux Vendors (e.g., Red Hat RHEL, Canonical Ubuntu Pro), Commercial Appliance Vendors (packaging FRR/Linux into proprietary network boxes)

The CRA: Stewards vs. Commercial



CRA Timelines

CRA Timelines

- Enacted as Regulation (EU) 2024/2847 in Oct 2024.
 - Regulation vs. Directive - applies without national transposition acts.
- Application follows a staggered timeline under Article 71.
- Early Reporting Obligations: September 11, 2026
- Full Market Entry: December 11, 2027
 - Mandatory CE Marking
 - Essential Cybersecurity Requirements
 - Vulnerability Handling Obligations – SBOM, CVD, ≥ 5 years of updates
 - Market Surveillance and Fines - fines reach up to €15 million or 2.5% of total worldwide annual turnover

CRA Timelines - Early Reporting Obligations

- What must be reported:
 - Any **actively exploited vulnerability** in a product with digital elements.
 - Any **severe incident having an impact on the security** of the product.
- Applies to all products currently in use or on the market.
- A manufacturer cannot ignore actively exploited flaws in older software/hardware that they still actively support.

CRA Timelines - Early Reporting Obligations

- The 3-stage notification clock (Article 14):
 - **Within 24 hours:** “Early warning notification” to the national CSIRT and ENISA via a dedicated Single Reporting Platform.
 - **Within 72 hours:** Detailed notification with sensitivity and initial assessment (unless provided in the early warning).
 - **Final report:** within 14 days after a corrective patch/remediation or within 1 month after the 72-hour notification (for severe incidents).

Other Obligations of Open-Source Software Stewards

- Establish a Cybersecurity Policy which documents a formal cybersecurity policy.
 - Must cover secure development practices, vulnerability intake, patching workflows, and the remediation of discovered flaws.
 - “tailored to the steward's organizational setup”
- Foster coordinated vulnerability handling
 - Promote the responsible, transparent sharing of vulnerability data across the wider open-source community.
- Establish discoverable channels to encourage and facilitate voluntary vulnerability disclosures from community contributors and security researchers.
- Cooperate with the market surveillance authorities, at their request

Consuming Open-Source Under NIS2 (Art 21)

Consuming Open Source Under NIS2 (Art. 21)

“It’s free software” is no longer an excuse for unmanaged supply chain risk.

Consuming Open Source Under NIS2 (Art. 21)

- **Mandatory Supply Chain Due Diligence:**
 - NIS2 requires entities to assess the security posture of third-party software, including open-source routing daemons, automation scripts, and management platforms.
- **What IXPs Must Implement:**
 - **Software Asset Inventory:** Clear mapping of all open-source packages in the production path.
 - **Vulnerability Tracking:** A structured process to ingest advisories and evaluate reachability/exploitability.
 - **Timely Patch Management:** Defined change-management procedures to deploy security patches without undue delay.

What IXPs Can Expect from Upstream Open-Source

- **From Open-Source Stewards (like INEX):**
 - Clear, published security policies and private vulnerability intake.
 - Rapid public alerts if an exploit is active in the wild.
 - Upstream collaboration if issues stem from underlying libraries.
- **From Commercial Open-Source Vendors:**
 - Machine-readable Software Bill of Materials (SBOMs) on request.
 - Guaranteed free security updates for a minimum defined lifecycle.
 - Direct customer notifications within 24 hours of critical active exploit discoveries.

Case Study: How IXP Manager Aligns as an OSS Steward

- **Secure Application Development Policy** (docs.ixpmanager.org)
- **Formal CVD Policy:** Clear intake via PGP/Signal/GHSA, 48-hour response target, and explicit support lifecycle tables. ([SECURITY.md](#))
- **GitHub Security Advisories (GHSA):** Generates standardised CVEs and machine-readable data (OSV format) that feeds directly into IXP automated scanners.
- **Proactive Code Hardening:** Using third-party pen tests and responsible disclosures as catalysts for broader internal code audits (6 consecutive security-focused releases).
- **CRA Escalation Playbook:** Documented procedures to alert the ENISA Single Reporting Platform and national CSIRTs within 24–72 hours if active exploitation is confirmed. (*WIP*)

Publishing Software? Your Responsibilities as an IXP

- **Scenario A: Internal Scripts & Code Dumps (Exempt)**
 - Sharing an open-source automation script or BGP filter generator without commercial monetisation? CRA out of scope.
- **Scenario B: Sustained Infrastructure Tooling (Steward)**
 - Maintaining an industry tool used across multiple exchanges? You fall into the Steward bracket: publish a security policy, provide an encrypted reporting channel, and coordinate disclosures.
- **Scenario C: Monetised / Packaged Software (Manufacturer)**
 - Selling a software solution or managed appliance to other networks? You are a Manufacturer and must comply with full CE-marking, conformity assessments, and SBOM requirements.

Action Items for Euro-IX Members

- 1. Audit Your Open-Source Dependencies:** Map out critical open-source software running in your core and control plane (IXP Manager, BIRD, RPKI, Looking Glass).
- 2. Automate Advisory Ingestion:** Configure your vulnerability scanners to consume machine-readable advisories (like GHSA/OSV) from your critical upstream maintainers.
- 3. Upgrade Maintained Platforms:** Ensure platforms like IXP Manager are on active, supported release branches (e.g., v7.4.1+).
- 4. Establish Your Own Disclosure Channel:** Ensure your IXP has a clear security@ or CVD contact point published for your peering portal and route servers.

The background is an aerial photograph of a harbor area. In the foreground, there's a paved walkway with trees and a small bridge. The water is calm, reflecting the sky. In the background, there are various buildings, including a large modern one with a curved roof, and a bridge with a tall, white, curved structure. A large green circle is superimposed over the center of the image, containing the text "Thank You." in white.

Thank You.