txOne networks

Side-by-Side Comparison of EU Regulations:

Cyber Resilience Act (CRA), Machinery Regulation (EU) 2023/1230, and NIS2 Directive

1. Scope & Objective

Aspect	Cyber Resilience Act (CRA)	Machinery Regulation (EU) 2023/1230	NIS2 Directive
Primary Focus	Cybersecurity for digital products (hardware & software)	Safety and security of machinery with digital elements	Cybersecurity of essential and important services
Objective	Ensure digital products are secure-by-design and resilient	Ensure machinery is safe, including from cyber threats	Improve overall cybersecurity resilience in critical sectors
Scope	Digital products across all sectors (IoT, software, hardware)	Machinery, including AI, robotics, and software components	Operators of essential and important infrastructure sectors
Entities Affected	Manufacturers, importers, distributors of digital products	Machinery manufacturers, importers, distributors	Operators of essential and important services (e.g., energy, healthcare)

2. Cybersecurity Requirements

Aspect	CRA	Machinery Regulation (EU) 2023/1230	NIS2 Directive
Security-by-Design	Mandatory for all products with digital components	Required for machinery with digital or AI components	Encouraged for critical infrastructure systems
Vulnerability Management	Continuous monitoring, reporting, and patching required	Cyber risks assessed during design and throughout lifecycle	Risk-based approach for ongoing cyber risk monitoring
Data Protection	Encryption, access control, and data integrity checks	Safety measures must consider unauthorized data access	Requires appropriate security measures to protect data integrity
Incident Reporting	Obligatory within 24 hours of detection for critical incidents	Report safety-related cybersecurity incidents	Mandatory reporting to national authorities for significant incidents

3. Risk Management Requirements

Aspect	CRA	Machinery Regulation (EU) 2023/1230	NIS2 Directive
Risk Assessment	Identify, analyze, and mitigate cyber risks in digital products	Assess cybersecurity risks impacting machinery safety	Identify and manage risks across critical systems and services
Supply Chain Security	Required, especially for software supply chains	Required for machinery components sourced externally	Essential to ensure third-party suppliers meet security standards
Technical & Organizational Measures	Technical focus: secure coding, encryption, and monitoring	Safety focus: ensuring machinery control systems cannot be compromised	Organizational focus: policies, procedures, and employee training

4. Compliance, Enforcement & Penalties

Aspect	CRA	Machinery Regulation (EU) 2023/1230	NIS2 Directive
Certification/ Marking	CE marking with cybersecurity compliance	CE marking including cybersecurity as part of product safety	No CE marking but requires sectoral compliance verification
Audits/ Inspections	Conformity assessment before product placement	Risk assessment during design, manufacturing, and use	National supervisory authorities can conduct audits
Penalties	Up to 15 million EUR or 2.5% of annual turnover	Penalties based on general EU product safety rules	Fines up to 10 million EUR or 2% of global turnover

5. Commonalities & Differences

Commonalities:

- All three regulations emphasize risk-based cybersecurity approaches.
- Incident reporting and vulnerability management are essential across all.
- Secure-by-design principles are applied to varying degrees.
- Supply chain security is a shared concern.

Differences:

- **CRA** focuses on product-related cybersecurity; **Machinery Regulation** integrates cyber risks into machinery safety; **NIS2** targets organizational cybersecurity for essential and important services.
- **CRA** and **Machinery Regulation** require CE marking for compliance, while **NIS2** does not.
- **CRA** applies broadly to digital products across industries, **Machinery Regulation** focuses on industrial machinery, and **NIS2** addresses critical infrastructure sectors.

6. TXOne Networks Solutions and Their Role in Achieving Compliance

TXOne Networks offers cybersecurity solutions specifically designed to protect OT (Operational Technology) environments, supporting compliance with these EU regulations. Key offerings include:

TXOne Solution	CRA Compliance	Machinery Regulation Compliance	NIS2 Directive Compliance
EdgeFire (Industrial Firewall)	Network segmentation and access control for digital product protection	Prevents unauthorized access to machine control systems	Supports segmentation and monitoring of critical infrastructure networks
EdgeIPS (Intrusion Prevention System)	Protects against cyber threats via network traffic monitoring	Ensures machine communication remains secure	Helps detect and respond to network-based attacks
StellarProtect (Endpoint Protection)	Ensures secure endpoints by preventing unauthorized software	Safeguards machinery endpoints against malware	Provides endpoint protection for critical infrastructure systems
Portable Inspector (OT Asset Visibility)	Identifies vulnerabilities and ensures compliance	Helps monitor and secure machinery assets	Assists in asset discovery and risk assessment for NIS2 compliance
Safeport (Data Sanitization & Scanning Station)	Provides a secure scanning station to prevent malware from entering through portable media	Ensures safe data transfer in operational environments	Protects critical systems from malicious files introduced via external media
SageOne (Centralized Security Management)	Centralized management for OT security solutions	Facilitates centralized control and monitoring of machinery cybersecurity	Enhances oversight and reporting for NIS2 compliance requirements

Conclusion

These three regulations reflect the EU's holistic approach to cybersecurity, each addressing security concerns from different angles. While the CRA ensures digital product security, the Machinery Regulation ensures that machinery with digital elements remains safe. The NIS2 Directive, on the other hand, ensures the resilience of critical services. Companies operating in more than one of these domains must harmonize their compliance efforts to meet all applicable requirements simultaneously.

TXOne Networks' solutions provide critical support in achieving compliance across these regulations by offering protection for OT environments, ensuring secure communication, and providing comprehensive visibility into assets and potential threats.

txOne networks