TOSIBOX

Mikko Peltola

Board Member, Tosibox Inc.

Mikko currently serves as a board member at Tosibox and co-founder and COO of A-CX, a Dallas-based boutique software development company. With extensive leadership experience from Nokia, Microsoft, and F-Secure, Mikko is known for creating award-winning products and services. Throughout his distinguished career, he has leveraged his strong business acumen and passion for technology to drive innovation and accelerate growth.

New Regulatory Standards for OT Security

Cyber threats are increasingly targeting the heart of industrial operations, prompting regulators to implement new standards. In 2025, OT security regulations will reshape cybersecurity for energy grids, manufacturing, and critical infrastructure. Organizations must navigate the complexities of US & EU cybersecurity standards, from Zero Trust for operational technology to the Cyber Resilience Act. This guide provides actionable insights and industrial cybersecurity best practices to help organizations safeguard their assets and achieve compliance.

1 The Shift in OT Security Regulations

As cyber threats targeting industrial environments grow, 2025 marks a pivotal year for OT security regulations. Governments and regulatory bodies are enforcing stricter cybersecurity mandates to protect critical infrastructure, energy grids, and manufacturing systems from cyberattacks.

OT systems have traditionally operated outside the scope of IT security regulations, prioritizing uptime and operational stability over cybersecurity. However, with the increasing interconnectivity of IT and OT systems, threats that once targeted IT networks are moving laterally into industrial environments.

New regulations—including NIS2 in the EU, NIST 800-82 updates in the US, and the Cyber Resilience Act—are expanding compliance obligations for industrial and critical infrastructure operators. Organizations must now adopt Zero Trust for operational technology, secure remote access solutions, and improve monitoring frameworks.

This blog will explore the key OT security regulations for 2025, their impact on compliance, IT-OT convergence, risk management, and how Tosibox helps businesses meet these new security mandates.

OT Security and Cyber-Physical Systems (CPS)

Traditionally, Operational Technology (OT) – the hardware and software that controls industrial operations – existed separately from IT. Think of it as the machinery managing physical processes, distinct from information systems. However, this is changing. OT is evolving into Cyber-Physical Systems (CPS), a term Gartner popularized. This isn't just a name change; it reflects growing connectivity and intelligence within industrial environments.

Why does this shift matter? As OT becomes CPS, the attack surface expands. Once isolated systems, like power grids or manufacturing lines, are interconnected, they bring benefits like real-time monitoring and expose them to new cyber threats. The consequences are tangible: disrupted production, power outages, and potential physical accidents.

This evolution is driving the need for stricter OT security regulations. Unlike IT, which manages data, OT manages physical processes. This difference and the increasing convergence of the two bring unique challenges. Regulations are now addressing this, forcing organizations to adapt. The terminology change signifies a fundamental shift, demanding a new approach to securing industrial infrastructure."

What is IT/OT Convergence?

Gartner defines IT/OT integration as "the end state sought by organizations (most commonly, asset-intensive organizations) where instead of separating IT and OT as technology areas with different areas of authority and responsibility, there is integrated process and information flow."

Distiction	Characteristics
Focus	IT prioritizes data storage, processing, and transmission, while OT prioritizes real-time monitoring and control of physical devices.
Data type	IT handles diverse data like transactional, voice, and video, whereas OT deals with specific process data for immediate action.
System design	IT systems are typically more flexible and adaptable to changing needs, while OT systems are often designed for stability and long lifecycles with less frequent updates due to safety concerns.
Security concerns	In IT, data confidentiality is paramount, while in OT, operational safety and system availability are the primary concerns.
Network structure	IT networks are often more open and interconnected, while OT networks are often isolated and segmented to prevent disruptions to critical processes.
Typical applications	IT systems include email, databases, and enterprise applications, while OT systems include industrial control systems (ICS), SCADA systems, and sensor networks.
IT example scenario	A company's IT department manages employee email systems, data backups, and network access controls.
OT example scenario	In a manufacturing plant, the OT system monitors and controls machinery like conveyor belts, temperature sensors, and production lines in real-time to ensure smooth operation.

2 Why New OT Security Regulations Matter in 2025

As cyber threats against critical infrastructure and industrial systems continue to escalate, 2025 marks a turning point for OT security regulations. Governments and regulatory bodies are enforcing stricter cybersecurity mandates to protect energy grids, manufacturing plants, and essential services from cyberattacks.

High-profile incidents like Colonial Pipeline, Norsk Hydro, and Oldsmar Water Facility have exposed gaps in OT security, prompting new legislation in both the US and EU. The expansion of NIS2, NIST 800-82, and the Cyber Resilience Act ensures that OT environments are no longer exempt from compliance standards that have long been applied to IT networks.

Key reasons these regulations matter:

- Industrial control systems (ICS) are prime targets – Nation-state and ransomware attacks on OT are increasing.
- IT and OT are more connected than ever – The risk of lateral cyberattacks across networks is growing.
- Governments are mandating stricter reporting & security measures – Organizations must now implement real-time monitoring, Zero Trust models, and enhanced vendor security.

With compliance deadlines approaching, companies must adapt quickly to avoid penalties and secure their OT infrastructure. Now that we understand why new OT regulations matter let's take a deeper look at how the US will shape its regulatory landscape in 2025.

3 US Regulatory Updates for OT Security

The 2025 regulatory landscape is bringing significant shifts in how U.S. industrial and critical infrastructure organizations must secure their OT environments. Several key frameworks shape compliance requirements, particularly in energy, manufacturing, and other industries reliant on industrial control systems (ICS).

CISA's Cyber Performance Goals (CPGs 2025) – Strengthening OT Defenses

CISA's latest Cyber Performance Goals (CPGs) focus on enhancing OT network segmentation, enforcing Zero Trust principles, and strengthening supply chain security. Organizations must adopt risk-based cybersecurity strategies to comply with these guidelines.

NIST 800-82 Updates – Best Practices for Industrial Security

With evolving cyber threats, NIST 800-82 now includes:

- Zero Trust for OT networks, shifting security beyond perimeter-based models
- Risk assessment frameworks tailored for ICS environments
- Guidelines for IT-OT security integration to reduce vulnerabilities

FERC & NERC-CIP – Cybersecurity Compliance in the Energy Sector

For energy and utility providers, updates to NERC-CIP (Critical Infrastructure Protection)—mandated by FERC (Federal Energy Regulatory Commission)—increase requirements for:

- Enhanced continuous monitoring
- Stronger incident response measures
- Expanded third-party security controls

SEC Cybersecurity Disclosure Rules – Impact on Industrial Firms

The SEC's new cybersecurity disclosure rules now require publicly traded industrial companies to:

- Report cybersecurity risks and breaches
- Strengthen governance and risk management for OT security
- Increase transparency in security incidents and response measures

As OT security regulations tighten, businesses must ensure their industrial networks align with compliance requirements. The following section explores how EU regulations set similar security mandates for OT environments.

4 EU OT Security Compliance & Cyber Resilience Act

As cyber threats against critical infrastructure and industrial systems continue to rise, the EU has introduced stricter OT security regulations. Key frameworks such as NIS2, the Cyber Resilience Act (CRA), and ISO/IEC 62443 are setting new compliance standards for industrial cybersecurity across Europe.

NIS2 Compliance for OT Security – Expanding Regulatory Scope

The NIS2 Directive, which replaces NIS1, significantly expands cybersecurity obligations for OT-dependent industries. Key changes include:

- Broader industry coverage, now including energy, transport, manufacturing, and digital services
- More substantial incident reporting requirements with 24-hour breach notifications
- Mandatory risk assessments for OT networks to prevent supply chain attacks

Cyber Resilience Act (CRA) – New Vendor Responsibilities for OT Security

The Cyber Resilience Act sets stricter security requirements for OT hardware and software manufacturers. Key compliance mandates include:

- Built-in cybersecurity by design, ensuring OT devices meet security standards before deployment
- Continuous software updates and security patches for the lifespan of industrial products
- Accountability for supply chain security, requiring vendors to assess third-party risks

ISO/IEC 62443 Alignment – Strengthening OT Security Frameworks

Many EU regulations align with ISO/IEC 62443, a globally recognized industrial cybersecurity standard. Compliance with this framework helps companies:

- Implement risk-based security controls for ICS and OT networks
- Secure remote access solutions in industrial environments
- Improve incident detection and response strategies

With the EU's enhanced regulations mandating rigorous OT security, businesses must adapt their industrial networks for compliance. However, achieving this is further complicated by the growing convergence of IT and OT systems, which introduces new risks and challenges.

5 IT-OT Convergence: Risks & Compliance Challenges

The convergence of IT and OT is reshaping industrial cybersecurity, bringing opportunities and new risks. While regulatory frameworks now mandate stricter security for OT environments, organizational and technological challenges remain.

Legacy Systems and Interoperability in IT-OT Convergence

Historically, OT has been managed separately from IT, using different tools, teams, and security priorities. Now, as OT falls under CIxO leadership and aligns with IT compliance standards, two perspectives emerge:

- IT sees OT as another legacy system that needs modernization.
- OT considers this shift a chance to gain investment, visibility, and a new dependency on IT teams and tools.

This transition creates compliance challenges, as aging OT infrastructure must now meet modern security standards without disrupting critical operations.

Cybersecurity Risks Unique to OT Systems

Unlike IT, OT networks prioritize uptime over security, making them vulnerable to:

- **Unpatched legacy systems** – OT updates are rare due to operational risks.
- **Expanded attack surfaces** – OT devices connect to IoT and physical infrastructure.
- **Lack of segmentation** – Poor IT-OT network separation allows lateral cyberattacks.
- **Nation-state threats** – Attacks like Stuxnet target OT to disrupt critical industries.

Regulatory Frameworks Driving IT-OT Security Alignment

Regulations now mandate:

- Unified security policies for IT and OT.
- Stronger monitoring and incident response in OT environments.
- Supply chain security measures to reduce vendor-related vulnerabilities.

As businesses navigate IT-OT security compliance, Tosibox simplifies secure access, segmentation, and compliance enforcement—ensuring operational continuity without compromising security. The following section explores how Tosibox helps organizations align with OT security regulations.

6 How to Achieve OT Security Compliance in 2025 with Tosibox

This year, Tosibox will offer solutions solutions that prioritize asset management and network flow monitoring, foundational elements for securing OT environments.

Fundamental Steps to Enhance OT Security

1. Asset Management

- Comprehensive Inventory: Tosibox enables organizations to maintain a detailed inventory of all devices, including legacy and undocumented ("shadow OT") assets, ensuring no device is overlooked.
- Patch and Update Prioritization: By identifying and categorizing devices, Tosibox assists in prioritizing critical updates, especially for legacy systems susceptible to exploitation.
- Incident Response Preparation: By clearly understanding assets, their configurations, and roles, organizations can accelerate response times during security incidents.

2. Network Flow Monitoring

- Detecting Anomalies: Tosibox's solutions monitor communication patterns between OT devices and IT systems, identifying unusual activities that could signal potential threats.
- Protocol-Specific Monitoring: By focusing on OT-specific protocols (e.g., Modbus, DNP3), Tosibox ensures that unauthorized or abnormal commands are promptly detected.
- Command & Control (C2) Detection: Tosibox detects unauthorized outbound communications or lateral movements within the OT network, preventing potential breaches.

Continuous Improvement and Compliance

Tosibox is committed to helping clients continually enhance their security posture and maintain compliance. Its solutions are designed to adapt to evolving cybersecurity standards, ensuring that organizations remain protected against emerging threats. By leveraging Tosibox's automated and secure networking solutions, clients can stay ahead of regulatory requirements and industry best practices.

Collaborative Partnerships for Enhanced Security

Tosibox recognizes that achieving comprehensive OT security requires collaboration. Tosibox actively seeks to partner with technology innovators and distribution experts to deliver integrated, cutting-edge solutions. By working together, we aim to provide our clients with the tools and support necessary to secure their critical infrastructures effectively.

By focusing on these fundamental aspects and fostering strategic partnerships, Tosibox empowers organizations to navigate the complexities of OT security compliance in 2025 and beyond.

7 Why Proactive OT Security Compliance is Critical

The 2025 OT security regulations mark a shift from reactive compliance to proactive cybersecurity strategies. With frameworks like NIS2, NIST 800-82, and the Cyber Resilience Act enforcing stricter standards, organizations must secure OT environments before threats arise rather than responding after incidents occur.

Compliance is no longer just about avoiding fines—it is about protecting critical infrastructure, ensuring operational continuity, and mitigating cyber risks. Companies that adopt Zero Trust, secure remote access, and automated monitoring will stay ahead of evolving threats.

Tosibox empowers businesses with scalable, compliant OT security solutions, ensuring resilience in an increasingly regulated landscape.