

Navigating EU Cybersecurity Regulations to Protect Critical Infrastructure and Ensure Compliance

NIS2, DORA & KRITIS Guide



Table of contents

1. Introduction.....	3
2. Similarities and differences between NIS2, DORA, KRITIS.....	3
2.1 Common goals.....	3
2.2 Comparison table.....	4
2.3 Overview in the EU and DACH countries.....	5
3. Challenges/opportunities.....	6
3.1 Crucial effects on security of companies & authorities.....	6
3.2 Security shortcomings for critical sectors.....	9
4. Network-specific requirements.....	10
4.1 Requirements of all regulations.....	10
4.2 Article on network security.....	10
5. Network Detection & Response (NDR) as an enabler.....	11
5.1 Advantages of NDR.....	11
5.2 How it works in practice.....	12
6. Conclusion: Enabler wanted!.....	13

1. Introduction

The EU and its member states have introduced regulations like [NIS2](#) and [DORA](#) to strengthen the cybersecurity and resilience of organizations across the region. These frameworks particularly impact **financial service providers, energy suppliers, and other critical infrastructure sectors**, where cyberattacks can cause severe economic losses and major operational disruptions.

Ransomware, data theft & targeted attacks increasing

In 2024, a ransomware attack shut down 25 hospitals in Romania, halting critical services, and Germany's CDU party was forced offline by an attack linked to state actors. Two of - unfortunately - many examples. These incidents underscore the ongoing vulnerability of critical systems. The financial sector is especially at risk.

68%

of banks reported serious cyberattacks in the past two years.

With these regulations now in force, organizations face more than just the cost of a cyberattack; they also risk significant fines for non-compliance. Now is the time for companies to reassess their security posture, align with new legal requirements, and proactively strengthen their defenses.


2. Similarities and differences

2.1 Common goals




These regulations aim to:

- strengthen cybersecurity resilience by requiring organizations to implement robust defenses and effective risk management practices,
- quickly detect and respond to threats,
- introduce mandatory incident reporting and regular security audits to ensure ongoing oversight.

2.2 A closer look

Feature	NIS2	DORA	KRITIS/SzA 
Target Group	Critical entities across sectors such as energy, transport, health, water, and public	Financial institutions, banks, insurers, IT and cloud providers and payment services	IT Security Act 2.0 expanded critical infrastructure (per BSI-KritisV) to include healthcare, media, and waste
Focus	Cybersecurity risk management Reporting and supply chain security	Operational resilience, IT risk & ICT threat management, BCM, and digital resilience	Securing critical infrastructure through mandatory IT audits, security standards, and reporting to the BSI
Incident Reporting	There will be a 24-hour initial, a 72-hour update, and a one-month final reporting to national cybersecurity authorities (e.g., BSI)	Immediate reporting required – initial incident report must be submitted within 4 hours	Under the IT Security Act, companies must report significant IT incidents to the BSI within 72 hours
Penalties	Up to EUR 10 million or 2% of global annual turnover	Up to 2% of total yearly turnover	Sanctions by BSI include fines and mandatory corrective measures

2.3 Overview: Comparison of cybersecurity regulations in the EU vs. Germany & Switzerland

Feature	EU: NIS2, DORA 	KRITIS/SzA 	Current status 
Legal Basis	NIS2 for critical enterprises, DORA for the financial sector	IT Security Act, KRITIS Regulation (KritisV), Sector-Specific Requirements (SzA)	Federal Information Security Act (ISG), Data Protection Act (DSG), and upcoming mandatory incident reporting for critical infrastructure
Target Group	Critical and essential sectors, financial institutions, IT service providers	Key infrastructure: energy, health, water, transport, government	Federal authorities and critical infrastructure operators (private sector regulation still limited)
Focus	Cybersecurity, network security, digital resilience, incident reporting	Protection of critical infrastructures, minimum IT security standards, reporting obligations	Protection of public sector data, voluntary security for businesses, with more regulation ahead
Incident Reporting	Mandatory for all affected companies (24h initial report, 72h update, 1-month final report)	Mandatory for KRITIS companies, reporting to BSI (72h deadline)	Currently voluntary, mandatory for federal authorities; mandatory reporting for KRITIS companies planned (via NCSC).
Violation Penalties	Up to EUR 10 million or 2% of global annual turnover (NIS2), up to 2% of revenue for financial institutions (DORA)	Sanctions and requirements imposed by BSI, fines for KRITIS companies	There are no specific fines for private companies or potential sanctions for federal authorities



3. Challenges/opportunities

3.1 The most important effects on the security of companies and authorities

The NIS2 Directive is expected to impact approximately **29,500 additional companies in Germany alone**, expanding its scope beyond the previously regulated operators of critical infrastructures.

DORA is applicable to a broad spectrum of financial entities throughout the EU, encompassing approximately **22,000 financial entities and ICT service providers**. Consequently, these cybersecurity regulations will significantly impact a growing number of organizations throughout Europe.

Many companies are subject to **multiple regulations** simultaneously, resulting in complex network security, incident reporting, and risk management requirements.

The following ten key areas illustrate overlapping requirements and organizational challenges.

1. Extended cybersecurity requirements and resilience obligation

Under the IT Security Act and BSI-KritisV, companies must secure networks, have emergency plans, and follow reporting rules.

DORA requires financial institutions to ensure operational resilience and manage ICT risks.

NIS2 and KRITIS demand dual authentication, business continuity planning, and a broader scope of protection.

2. Stricter incident reporting obligations

DORA: Initial notification within **4 hours for major incidents**.

NIS2: Initial report in 24 hours, update in 72 hours, final report in 30 days.

KRITIS: Report to BSI within 72 hours.

3. Secure use of cloud and third parties

DORA: enforces strict controls on ICT providers for financial entities.

NIS2: demands supply chain security—companies need hybrid cloud strategies with robust controls.

KRITIS: restricts moving critical systems to the cloud without proper safeguards.

4. High penalties for non-compliance

The regulations impose severe penalties of up to €10 million or 2% of global turnover. KRITIS adds enforcement via BSI audits and mandatory actions. Organizations need integrated compliance management to avoid fines and reputational damage.

5. Growing threats from new technologies

DORA requires detailed ICT risk assessments for mobile banking, APIs, and cloud platforms.

NIS2 emphasizes network security against ransomware, phishing, and targeted threats. Critical infrastructure in finance must align IT-security across all digital channels.

6. Responding to geopolitical risks

Rising global tensions increase the risk for banks, energy, public et al. NIS2 and KRITIS demand proactive contingency plans and strong cyber defenses. Resilient IT architectures are now essential for operational stability.

7. Securing digital assets & cryptocurrencies

DORA: boosts IT risk controls to protect crypto assets and payment systems.

NIS2: stresses integrity in digital transactions – requiring built-in, end-to-end security.



8. AI as both a risk and an opportunity

AI-driven threat detection helps meet NIS2 and DORA requirements by enabling faster, [automated responses to incidents](#). At the same time, **NIS2 and KRITIS mandate protection against AI-based cyberattacks**, particularly in fraud detection and identity protection. Hence, AI must be part of both your defense strategy and your threat model.

9. Balancing isolation and visibility

DORA: pushes for real-time monitoring and integrated IT environments.

NIS2: demands regular IT security audits to balance system isolation and operational visibility.

KRITIS: companies rely on [on-premises](#) and [air-gapped](#) systems to secure critical infrastructure.

10. Urgent need for unified cyber risk management

Many organizations fall under multiple frameworks, each with distinct but overlapping requirements.

DORA: resilience for financial operations during attacks or outages.

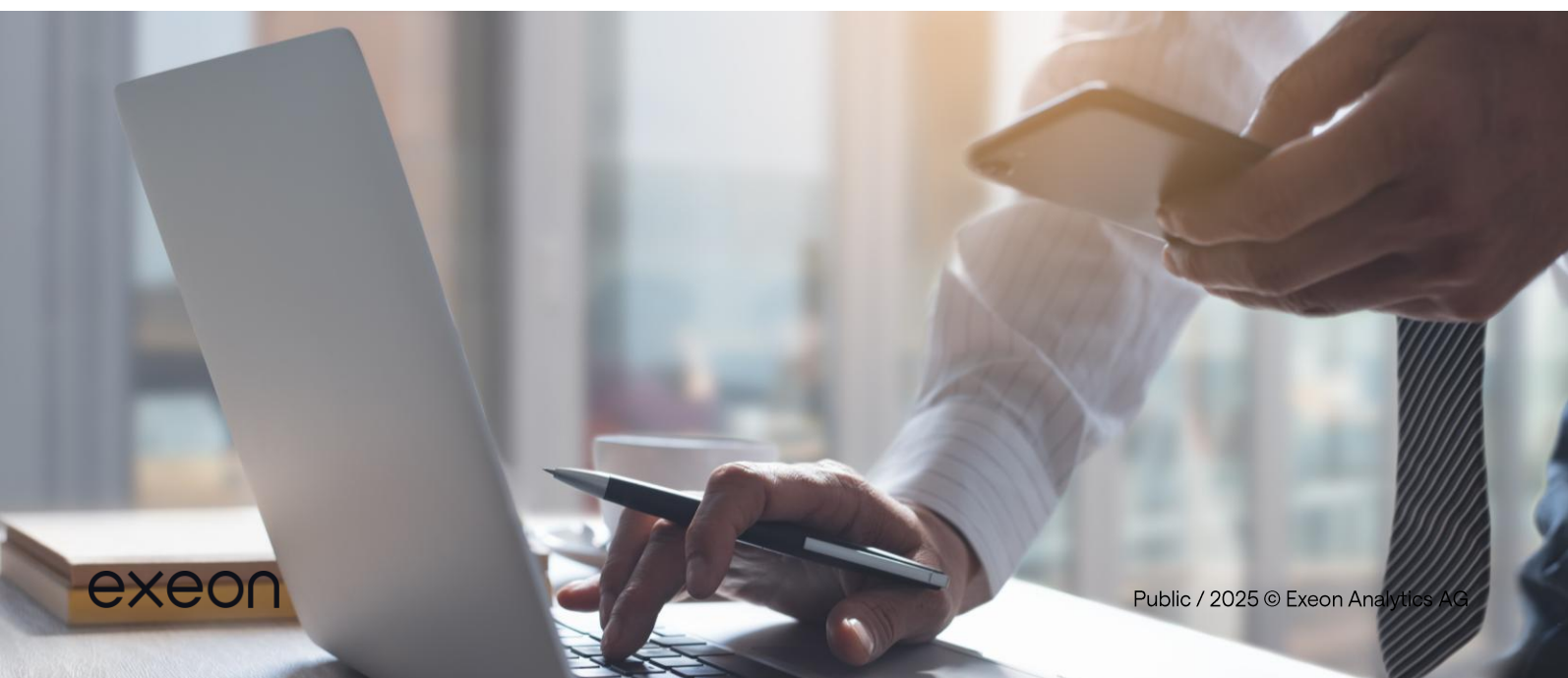
NIS2: continuous threat analysis and early detection.

KRITIS: mandatory IT audits and enforced improvements.

3.2 Cybersecurity shortcomings for critical sectors

In the area of IT and cybersecurity, shortcomings have been identified in critical sectors:

- **Incomplete risk analysis & security measures:** Missing threat models, lack of network segmentation, and inadequate protection of sensitive data.
- **Deficiencies in identity & access management:** Weak or missing multi-factor authentication, excessive user rights, and insufficient monitoring of privileged access.
- **Weak detection & reporting of security incidents:** Incomplete [SIEM](#), IDS/IPS implementation, unclear reporting channels, and missed regulatory deadlines.
- **Deficits in incident response:** Lack IR plans, employee training, and tested emergency procedures.
- **Insufficient resilience & recovery measures:** Missing redundancy concepts, untested business continuity plans, weak or unsecured backup systems.
- **Unclear asset inventories & risk classifications:** Poor documentation and prioritization of critical IT systems and services.
- **Weak physical & network security architecture:** Gaps in physical access control, insufficient segmentation of sensitive areas, and inadequate perimeter defenses.
- **Lack of cyber defense capabilities:** Outdated threat intelligence, slow patching, and weak endpoint protection.
- **Gaps in emergency & crisis management:** Unclear responsibilities, lack of coordination with authorities, and untested crisis scenarios.
- **Regulatory compliance issues:** Poor implementation of reporting obligations, documentation gaps, and missing audit trails.



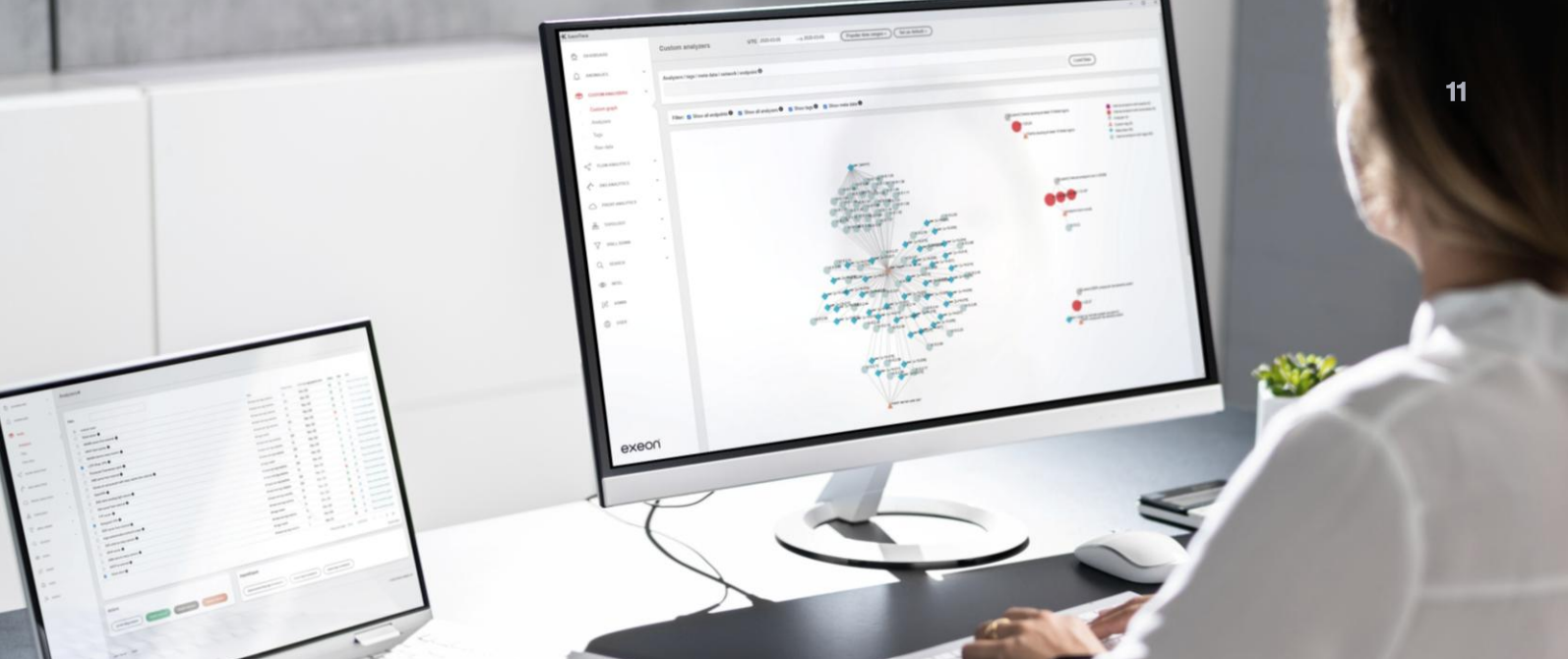
4. Network-specific requirements & challenges

4.1 NIS2, DORA, and KRITIS

- **Real-time Threat Detection & Response:** Companies must be able to identify and react to cyber threats as they happen.
 - NIS2 Art. 21
 - DORA Art. 5
 - KRITIS/BSI IT Security Act §8a
- **Zero Trust network architecture** for network security.
 - NIS2 Art. 20
 - DORA Art. 6
 - SzA according to BSI
- **Continuous monitoring & logging:** All systems must be monitored and logs maintained for transparency and traceability.
 - NIS2 Art. 22
 - DORA Art. 11
 - KRITIS-Anford.
- **Regular digital resilience testing:** Financial institutions must regularly test their defenses, including TLPT (Threat-Led Penetration Testing).
 - DORA Art. 11
- **Mandatory attack detection for KRITIS operators:** Critical infrastructure operators are legally required to have attack detection in place.
 - BSI IT-Sicherheitsgesetz §8a

4.2. Articles on network security

- **Resilient IT & risk management:** IT systems must be resilient and include strong risk management processes.
 - DORA Art.5
- **Regular resilience testing:** Includes mandatory Threat-Led Penetration Testing (TLPT) to assess digital defenses.
 - DORA Art. 11
- **Incident Detection & Reporting:** ICT-related incidents must be quickly identified and reported.
 - DORA Art. 15



- **Network cybersecurity measures:** Companies must implement robust cybersecurity protections across their networks.
 - NIS2 Art. 21
- **CSIRTs & vulnerability management:** Requirements for national CSIRTs to support threat detection and vulnerability handling.
 - NIS2 Art. 11
- **Threat intelligence sharing:** Encouragement and support for sharing threat-related information between stakeholders.
 - NIS2 Art. 29
- **Mandatory attack detection for critical infrastructure**
KRITIS operators must have systems in place to detect cyberattacks.
 - BSI IT-Sicherheitsgesetz §8a

5. Network Detection & Response (NDR) as an enabler

5.1 Advantages of NDR solutions

- Automatic anomaly detection through AI-supported algorithms.
- Lateral movement detection to stop attackers within the network early.
- Reduced false positives through [risk-based alerting](#).
- Agentless integration into existing IT and security infrastructures.

With [Exeon.NDR](#), organizations gain complete visibility into their networks, detect threats in real-time, and simultaneously meet the requirements of multiple regulations without complex and cumbersome security architectures.

5.2 And this is how it works in practice

Exeon.NDR enables the efficient implementation of most of NIS2, DORA, and KRITIS cybersecurity requirements through a combination of AI-supported analysis, continuous monitoring, and easy integration into existing IT landscapes. With a holistic approach, it not only helps companies meet regulatory requirements but also proactively strengthens their security strategy and effectively defends against cyberattacks.

- **Early detection of attacks:** Using machine learning, NDR analyzes network traffic in real-time and detects suspicious patterns to identify attacks such as ransomware, [APTs \(Advanced Persistent Threats\)](#), or insider threats at an early stage.
- **Fast incident response:** Automated correlation of threat indicators enables the security team to [respond efficiently](#) and isolate attackers before they cause damage.
- **Compliance optimization:** Organizations comply with NIS2, DORA, and KRITIS to seamlessly document all security-related network activity and report security incidents according to regulatory requirements.
- **Seamless integration and scalability:** As Exeon.NDR works agentless, so it can be easily integrated into complex, hybrid IT environments—whether [on-premise, in the cloud](#), or in critical infrastructures with an [air-gapped environment](#).
- **Optimization of resources:** [Reducing false positives](#) and prioritizing real threats ensures that security analysts can focus on the most critical incidents instead of drowning in irrelevant alarms.



6. Wanted: Enabler for NIS2, DORA et.al

NIS2, DORA and KRITIS requirements demand robust security strategies with state-of-the-art technology. Exeon enables efficient implementation of these requirements by combining network security, threat detection, and compliance needs. Organizations benefit from increased resilience, reduced false positives, and faster response to cyber threats. ([incident response](#)).

- Quick & easy implementation without additional hardware.
- Complete network visibility through metadata analysis.
- Ensure compliance with NIS2, DORA, and KRITIS through automated reporting.
- Effective threat detection for cloud, on-premises, and hybrid environments.
- Technical implementation with Exeon:
 - Machine learning & AI to detect unknown threats.
 - Network forensics & anomaly analysis for real-time threat detection.
 - Log data & flow monitoring for detailed traffic analysis.
 - API interfaces for seamless integration with SIEM, [SOAR](#), and EDR.



Christian Keller, CISO @ SWISS

“For the security of SWISS IT, we use Exeon as a central cybersecurity tool, fully managed by our long-term partner Reist Telecom AG. A perfect combination and solution to monitor our network and quickly detect any kind of anomalies.”

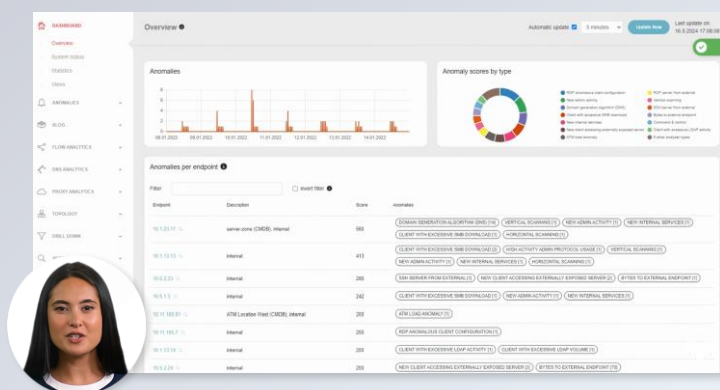
What can you do next?

We recommend the following next steps:

- Assess if you check your network as comprehensively as possible for anomalies, identify weak points, and determine the status quo.
- **Take 10 minutes to understand how anomalies and APTs can be identified, prioritized and countermeasures derived in the NDR tool by watching the video below.**

Guided video tour:

How NDR detects the most advanced threats in complex networks



[Watch the video >](#)

