GRUNDIG

GRUNDIG Security NIS2 Compliance Guide

Revision: 05/2026

Foreword

The European Union's NIS2 Directive[1] drastically tightens cybersecurity requirements for critical infrastructure and their supply chains. As an ISO 9001 and ISO 27001 certified manufacturer, **GRUNDIG** Security offers tailored, legally compliant video technology solutions to efficiently meet these strict regulatory requirements.

Background of Regulation

The NIS2 Directive has been in force at the EU level since January 2023 to consistently harmonize the general security level of network and information systems. National implementation expands the scope of affected companies in Germany from 4,500 to approximately 29,500 organizations. This massive expansion is forcing entire sectors of the economy to fundamentally realign their IT strategies.

The years 2025 and 2026 will require European companies to drastically increase their cyber resilience due to a volatile geopolitical security situation. The new NIS2 Directive addresses market failures in IT security through far-reaching and strict regulatory requirements. As a manufacturer of video technology, **GRUNDIG** Security actively supports affected planners, installers, and operators in ensuring the required security throughout the supply chain.

Key objectives of the directive

NIS2 aims to massively strengthen the resilience of the entire European economy against digital and physical threats. To this end, the law sets stricter standards for cyber risk management, business continuity, and vulnerability management. In addition, the concept of protection is extended beyond company boundaries to include suppliers and service providers.

Implications for video technology in general

Modern video surveillance systems are highly networked and deeply integrated into operators' complex IT and OT environments. As a result, they are considered security-relevant and represent a potential entry point for serious cyberattacks.

Classification of facilities

The NIS2 Directive classifies affected organizations into two main categories based on their criticality. The differences primarily manifest in company size, regulatory oversight, and the legal framework for sanctions.

Classification: Essential facilities

Essential facilities include large companies in highly critical sectors such as energy, transportation, banking, healthcare, and digital infrastructure. Operators of traditional critical infrastructure (KRITIS) automatically fall into this highest regulatory class. These organizations are subject to the strictest regulatory oversight and must demonstrate the highest standards of resilience.

[1] Source: https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/raising-awareness-campaigns/network-and-information-systems-directive-2-nis2

Classification: Important Facilities

The category of important facilities includes medium-sized and large companies from sectors such as waste management, food production, manufacturing, and the chemical industry. Companies are considered medium-sized if they employ more than 50 people or generate over 10 million euros in revenue. Although oversight here is reactive, the fundamental security requirements for these operations are identical.

Characteristic	Essential facilities	Critical facilities
Sector affiliation	Highly critical (e.g., KRITIS, energy sector)	Other critical (e.g., food sector)
Company size	Large enterprises (>250 employees)	Medium and large enterprises (>50 employees)
Type of oversight	Strict and proactive	Reactive (case-by-case)
Maximum fine	€10 million or 2% of global revenue	€7 million or 1.4% of global revenue

Identification and registration

Companies are required to independently assess their compliance with the NIS2 Directive and identify their obligations in accordance with the law. Affected organizations must register with the competent national authority, such as the BSI in Germany. A central point of contact for information security management must be designated to the authority.

Installers and planners must work together to ensure compliance.

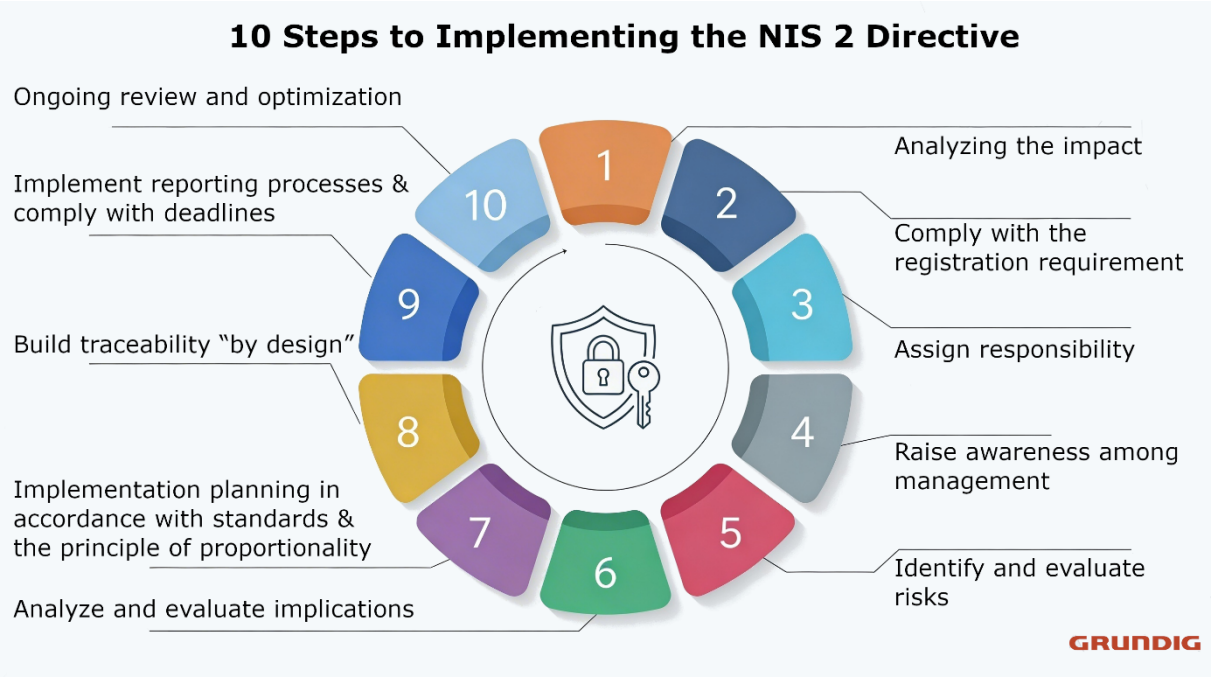
Strict reporting requirements

In the event of significant security incidents, organizations must submit an official early warning to the supervisory authority within 24 hours. The law requires a detailed and comprehensive report of the incident within 72 hours at the latest. Within one month, the authority may also request a detailed final report on the causes and countermeasures taken.

Regulated companies must always demonstrate a high level of cooperation with government inspection agencies. This includes the smooth provision of information and temporary access to IT systems for regulatory investigations. Proactive cooperation is crucial here to quickly avert systemic risks to the public.

Documentation Requirements

All implemented security measures and operational processes must be documented comprehensively and in a traceable manner. The effectiveness of this documentation must be verified through regular, independent audits. Upon request by the authorities, these structured records must be available for submission at any time and within the specified deadlines.



Cybersecurity measures

The law requires appropriate technical, operational, and organizational measures to minimize far-reaching cyber risks. These include comprehensive backup strategies, disaster recovery procedures, and systematic incident response management. The use of secure voice, video, and text communication is also explicitly mandated in sensitive areas.

Required cybersecurity hygiene

Organizations must rigorously enforce basic cybersecurity hygiene practices to minimize attack surfaces. This includes mandatory employee training, strict access controls, and consistently maintained asset management. Additionally, multi-factor authentication must be mandatorily established for all critical system processes.

Impending sanctions and liability of the end customer's management

In cases of non-compliance, critical infrastructure operators face hefty fines of up to 10 million euros or 2 percent of their global annual turnover. For important infrastructure operators, the upper limit is 7 million euros or 1.4 percent of global turnover. These enormous penalties are intended to serve as a deterrent and force companies to prioritize IT security.

Through NIS2, cybersecurity is strategically elevated to the top management level and is definitively declared a top priority. In the future, managing directors and board members will be personally liable for non-compliance with legal obligations in the event of violations or omissions. In addition, the law mandates regular security training for the entire executive management team.

Risks of Non-Compliance

Manufacturers without verifiable cybersecurity processes will be systematically excluded from the supply chains of regulated NIS2 entities. Furthermore, in the event of security incidents, they may face financial penalties due to product liability and substantial recourse claims. Geopolitical risks and the absence from international trusted lists also lead to direct market exclusion.

GRUNDIG Security as a Partner

As a reliable European partner, **GRUNDIG** Security offers tailored support for NIS2 compliance to its professional clients. We combine high-performance hardware with the flexible video management software C-WERK to create a highly secure end-to-end system. This integrated approach significantly reduces the burden on facility operators when fulfilling their supply chain obligations.

State of the Art

The NIS2 Directive requires IT devices to comply with the current state of the art. This naturally includes the use of cameras, recorders, and servers.

Cameras, recorders, and servers are popular targets of cyberattacks. Whether for spying on behavior or building a so-called botnet - access to the firmware and software of security technology is highly valuable from an attacker's perspective.

In terms of cybersecurity, our product lines are hardened, tested against various attack vectors, and undergo continuous internal audits.

AI and Video Analysis

The state-of-the-art required in video technology increasingly necessitates the use of artificial intelligence for automated threat detection. The SMART line from **GRUNDIG** Security processes analyses such as facial recognition, perimeter monitoring, and virtual tripwire directly on the camera, recorder, or server in compliance with data protection regulations.

Security by Design

According to Article 21 of the NIS2 Directive, IT products must be designed in accordance with strict security principles as early as the first phase of development. **GRUNDIG** Security consistently integrates this Security by Design philosophy into the C-WERK video management system and all network cameras offered. The surveillance systems are delivered to end customers by default with secure presets (Security by Default) and minimized attack surfaces.

Innovative SMART Line features such as "One-Click-Disable" block all internet communication when required - even if devices receive a valid gateway to connect to.

Cloud and Encryption

Consistently secure data transmission is a fundamental core requirement of NIS2 risk management obligations. **GRUNDIG** Security enables seamless and highly encrypted communication between local hardware and the connected C-WERK Cloud. This architecture reliably protects sensitive metadata from unauthorized third-party access and ensures legal compliance for cross-location surveillance projects.

Focus on Supply Chain Security

A central element of the NIS2 Directive is the consistent securing of the entire supply chain in accordance with Article 21. Affected entities must strictly monitor and audit the cybersecurity of their upstream suppliers and service providers. Ultimately, an organization's security chain is only as resilient as its weakest third-party provider.

Certified security processes

The most reliable response to NIS2 compliance requirements in the supply chain is independent and international certification. **GRUNDIG** Security holds the demanding ISO 9001 certification for quality management and ISO 27001 for its own information security management. These official seals of approval guarantee customers that all development and business processes are subject to the highest security standards and are systematically audited by third parties.

Compliance and Trust

Absolute geopolitical independence is a decisive criterion for selecting trustworthy technology suppliers under the NIS2 regime. All cameras and recorders in the SMART line from **GRUNDIG** Security therefore fully comply with the strict NDAA standards. This excludes critical components from high-risk suppliers and safeguards the digital sovereignty of critical European infrastructure.

Our SMART Line cameras and recorders also comply with NDAA guidelines. This prohibits U.S. government agencies and their contractors from using telecommunications and video surveillance technology from certain Chinese manufacturers in order to minimize security risks.

Vulnerability Management

Agile and proactive vulnerability management is legally required for critical infrastructure. **GRUNDIG** Security supports its end customers in this regard through continuous firmware updates and the extremely rapid deployment of security patches. Strict compatibility with open standards such as ONVIF also ensures that the systems remain compatible with third-party manufacturers in the long term.

GRUNDIG Security participates in the MITRE Corporation's "Common Vulnerabilities and Exposures (CVE)" program alongside its technology partner Axxonsoft. This standardized system for identifying and cataloging publicly known cybersecurity vulnerabilities in software and hardware facilitates the publication and tracking of attack vectors.

More information is available at the following link:
https://www.cve.org/PartnerInformation/ListofPartners/partner/AxxonSoft

Network Authentication

European law requires strict access controls and the use of robust cryptographic methods to protect plant networks. **GRUNDIG** Security recorders and IP cameras support complex alarm inputs as well as state-of-the-art authentication mechanisms in accordance with IEEE standards. Thus, all products in the SMART Line series support port-based network access control (PNAC) in accordance with IEEE 802.1X.

The C-WERK VMS also offers forensically secure rights management that completely prevents unauthorized data manipulation.

Conclusion

Operators of video systems must ensure that their IT infrastructure can easily withstand future regulations. The seamless integration of IP and HD-TVI technologies in the **GRUNDIG** Security portfolio enables a scalable and investment-secure migration of existing systems. This guarantees a cost-effective yet fully compliant implementation of the required technical measures.

By partnering exclusively with an ISO 27001-certified manufacturer such as **GRUNDIG** Security, critical enterprises significantly reduce their own compliance risk. Comprehensive documentation and proof of demonstrably secure products reliably protect organizations from government sanctions amounting to millions of dollars. At the same time, this approach substantially relieves management of personal liability risks that could threaten the company's existence.

www.grundig-security.com

Abetechs GmbH (**GRUNDIG** Security)

info@grundig-security.com

Subject to changes and errors.