LINK11

# WHITEPAPER

## It's a fact: NIS-2 comes

Status October 2024

www.link11.com

In Kooperation mit:

SCHALAST
LAW | TAX

## Dear readers,

The NIS2 Directive ("The Network and Information Security (NIS) Directive") presents companies in the EU with a new challenge: the comprehensive strengthening of their cybersecurity processes. While awareness of the importance of cybersecurity has grown in recent years, numerous surveys show that many companies are not yet sufficiently prepared to meet the new requirements.

NIS2 goes beyond previous regulations. It affects a larger number of companies and sectors and places higher demands on risk assessment, incident management, and supply chain security. Companies that are not compliant will face severe fines.

Unsurprisingly, the implementation of NIS2 is complex. This white paper provides you with a comprehensive overview of NIS2 and shows you how to successfully implement the new requirements. We look at the most important aspects, such as the specific measures you need to take to become NIS2 compliant and which technologies can support you in doing so.

Let's work together to make sure your organization is ready for the future of cybersecurity.
We wish you an informative read.

Best regards

**Jens-Philipp Jung**
Link11
CEO

**Janka Schwaibold**
Schalast LAW | TAX
Rechtsanwältin, Partnerin

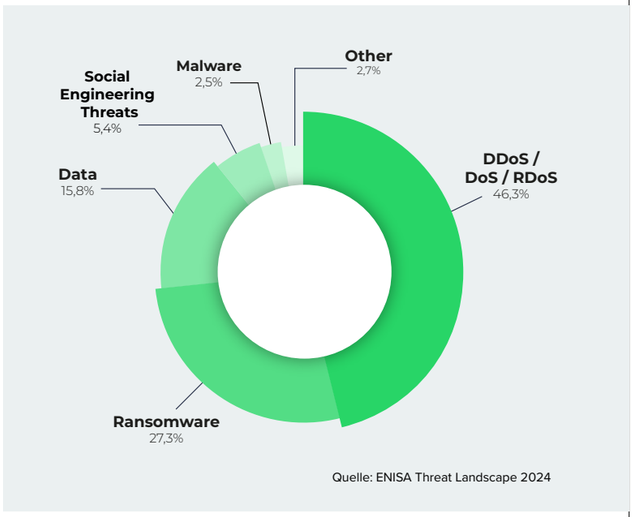
## Table of contents

# Overview of current cyber threats in Europe

The digital transformation has fundamentally changed our lives. But this impact is both positive and negative, as it has exponentially increased the attack surface for cybercriminals. The current threat situation is complex and dynamic and presents companies of all sizes with immense challenges.

According to the latest X-Force Threat Intelligence Index from IBM[1], Europe recorded the most cyberattacks in 2023, accounting for 32% of all incidents worldwide. The UK (27%), Germany (15%) and Denmark (14%) were particularly affected. The report also shows that 74% of cyberattacks in the European Union targeted critical infrastructure. This is an alarming increase that highlights the sector's vulnerability.

The threat is exacerbated by the increasing use of stolen credentials that allow easy access to networks. Abuse of valid accounts by cybercriminals increased by 66% in 2023.



Quelle: ENISA Threat Landscape 2024

**Cybercrime-as-a-Service: cybercrime for everyone**

Ransomware attacks continue to be one of the biggest threats. According to the FBI's Internet Crime Report (IC3) 2023[2], more than 2,825 ransomware incidents were reported - an increase of 18% compared to the previous year. Nevertheless, almost half of cyberattacks in the European Union are distributed denial of service (DDoS) attacks. The European Cybersecurity Agency (ENISA) has identified a "significant increase" in cybersecurity incidents in the EU. According to the current "Threat Landscape 2024"[3], the biggest threats from July 2023 to June 2024 were attacks against availability (DDoS) followed by ransomware. The development of cybercrime-as-a-service models has lowered the threshold for carrying out cyberattacks, meaning that less technically skilled attackers can now make use of these tools.

**Artificial intelligence: a blessing and a curse**

Artificial intelligence (AI) is revolutionizing many areas, but it also poses risks for cybersecurity. While AI is being used to develop innovative defense mechanisms, cybercriminals are using it to create highly personalized phishing emails and to automate attacks. Generative AI models allow attackers to create realistic deepfakes and deceptively real content.

**The gap between big and small**

The growing gap in cyber resilience is particularly problematic. While large organizations are improving their security measures, small and medium-sized enterprises (SMEs) are increasingly falling behind. According to the World Economic Forum's Global Cybersecurity Outlook 2024[4], 30% fewer organizations meet the minimum standards for cyber resilience than in the previous year. This development is worrying, as SMEs make up the majority of the economy in many countries, but are disproportionately affected by this discrepancy. More than twice as many SMEs as large companies state that they do not have sufficient cyber resilience to meet their critical business needs.

Another major problem is the lack of qualified personnel. Many small companies state that they do not have the necessary skills to achieve their cyber goals.

**The supply chain as a gateway**

Companies' digital networking across supply chains offers cybercriminals numerous opportunities to penetrate their defenses. Weak points in the supply chain can be used to infect trusted software with malicious code or gain access to sensitive data. More than half of companies state that they have some catching up to do in this area.

In addition, the Internet of Things (IoT) and the increasing use of cloud services are creating new attack vectors. The large number of networked devices and the storage of sensitive data in the cloud make companies more susceptible to cyberattacks.
State-sponsored cyberattacks also pose a growing threat. These attacks can target critical infrastructure or political opponents. In the face of these challenges, increased cooperation between government agencies and the private sector is crucial for effective countermeasures.

The cyberthreat landscape is dynamic and complex. Companies must take proactive measures to strengthen their digital resilience, including investing in modern security technologies, training employees, and working closely with external experts. In this way, companies can counter the growing cyber risks and protect their digital assets.

1 https://www.ibm.com/reports/threat-intelligence
2 https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf
3 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
4 https://www.weforum.org/publications/global-cybersecurity-outlook-2024/



# Risk analysis and assessment under the NIS2 Directive

The NIS2 Directive represents a milestone in the European cybersecurity landscape. It obligates companies that operate critical infrastructures to carry out a comprehensive risk analysis and assessment. This is essential in order to identify vulnerabilities and take targeted protective measures.

**Central role of risk analysis in NIS2**

Risk analysis is at the heart of the NIS2 directive. It obligates companies to systematically examine their IT landscape and identify potential risks. This involves not only technical aspects, but also organizational and human factors.

This comprehensive assessment of potential threats and vulnerabilities is not only a legal requirement, but also an indispensable basis for effective protective measures.

**Objectives of the risk analysis according to NIS2:**

- **Identification of weak points:** Both technical and organizational weaknesses should be uncovered.
- **Estimation of the probability of occurrence and the potential impact:** The analysis should estimate the probability of a successful attack and the resulting damage.
- **Development of protective measures:** Targeted protective measures can be taken on the basis of the risk assessment.
- **Continuous improvement:** Risk analysis is not a one-off process, but must be repeated regularly to ensure appropriate reaction to changes in the IT landscape and the threat situation.

However, the implementation of the NIS2 directive comes with numerous challenges. The complexity of modern IT landscapes, the lack of qualified personnel, and the constantly changing threat situation make comprehensive risk analysis difficult. In addition, the question of the right methodology – qualitative or quantitative approaches or a combination of both – is often controversial.

Against this background, the question arises as to how companies can successfully implement the requirements of the NIS2 Directive. What specific measures are necessary to carry out an effective risk analysis? How is a company's supply chain integrated and what impact does this have? How do corporate structures affect the implementation of NIS2? We clarified these and other questions with Sophia Zimmer, Senior Consultant at VICCON GmbH.

**Sophia Zimmer**
Senior Consultant,
VICCON GmbH

Sophia Zimmer is a consultant with extensive experience in information security management at VICCON. She has in-depth knowledge in the areas of Information Security Management System (ISMS) auditing, project management, and risk management. Sophia assists organizations to ensure compliance with current standards and has successfully established the ISMS.

**NIS2 & risk management**

**Sophia, I would like to know what specific challenges you see in the practical implementation of the NIS2 Directive with regard to risk analysis.**

*In principle, NIS2 requires the following points with regard to risk management: There must be a concept for risk identification, evaluation of risk management measures, and the assessment of critical supplier risks, taking into account the all-hazard principle (all-hazard approach).*

*GmbHs and AGs in particular are already legally obliged to continuously monitor risks (in accordance with AktG, StaRUG), i.e., risk management exists. I see the challenge in the fact that different players, along with their very different perspectives and interests, come together to assess IT and information security risks. However, I also believe that this is the decisive factor for success. Ultimately, the NIS2 directive makes it clear that IT risks must be viewed as corporate risks. The aim should be to use the methods of existing risk management so that all relevant people develop a common understanding, so risks can be reported and managed with efficiency and transparency. For me, a key challenge in risk management is to present risks transparently in order to provide decision-makers with concrete support and to get all relevant people on board.*

*Those who have already implemented an effective ISMS (Information Security Management System) will not initially encounter any new challenges. However, the risk analysis will have to be expanded to include supply chains, as NIS2 makes it very clear that networked risks and dependencies on service providers and suppliers must be specifically recorded and evaluated.*

**Companies have a lot to deal with, including some tricky situations. How does the involvement of the entire supply chain affect risk analysis in accordance with the NIS2 requirements, and why is careful documentation of decisions particularly important here?**

*The biggest challenge is that security-related aspects must be recorded between the individual providers and their direct service providers. It can also be tricky in terms of risk management measures, as redundancies are not always proportionate. The companies affected in the future are not expected to carry out a perfect risk assessment; all measures must be evaluated in terms of their proportionality, depending on the size of the company, the severity of incidents, and the social and economic consequences. NIS2 considers IT and information security risks to be regular business risks that must be dealt with appropriately. If a decision is made not to take certain measures, this should be documented and justified so as not to be accused of negligence in retrospect.*

**How can companies effectively manage the risks of their supply chains under NIS2, especially in complex global value chains?**

*The biggest challenge lies in the risk analysis of the supply chain. Critical suppliers need to be identified and evaluated in detail. Companies must identify risks in the supply chain, think through failure situations, and ensure that their suppliers guarantee cybersecurity.*

*Once I have identified all the service providers that are critical to me, I need to*
*1) Assess their information and IT security (especially if there is a network connection or if there is a large exchange of files)*
*2) Evaluate their BCM in terms of what consequences a supplier failure could have on my ability to operate (e.g. after a ransomware attack --> what impact does this have on my production/ processes/services) and how is my supplier and my own company preparing for this?*
*3) How is the reporting channel defined and are other communication channels besides email specified for reporting a cyber attack?*

**What steps should companies take to ensure information security in their supply chain, especially if they rely on numerous suppliers and service providers?**

*Companies should go through the following steps, regardless of the length of their supplier list: List suppliers and evaluate them in terms of relevant factors. Next, critical business partners must be considered and evaluated in more detail within a risk analysis. Finally, consideration should be given to which suppliers/ service providers can provide what evidence to ensure IT and information security in the supply chain. It is important to clearly define the contractual obligations, such as requirements for patch management, backup management, emergency drills and incident management.*

**NIS2 & Risk Management**

- **Required:** Concept for risk identification, evaluation of measures and analysis of critical supplier risks.
- **Objective:** Treat IT and information security risks as corporate risks, using standardized methods and create reports for management.
- **Focus:** Consideration of the entire supply chain and recording networked risks. Establish transparent risk management to support decision-makers.

**NIS2 & Group structures**

**How do groups ensure that the NIS2 requirements are implemented uniformly in all group companies? This is particularly relevant for companies that operate in different countries and may be subject to the respective national regulations.**

*In principle, if a company carries out an activity in one of the sectors listed in the annexes, it is subject to the requirements of NIS2 implementation if the defined thresholds are exceeded. Whether the entire group or only a subsidiary is affected by the requirements depends on the respective parts' independence from the wider company. If the independence of a company from the group can be proven, the figures of the subsidiary are decisive. In this case, the regulations of the EU country in which the subsidiary has its headquarters are relevant.*

*It is assumed that the decisions on cybersecurity risk management measures are made there. If the respective regulations of another EU member state apply, these must be reviewed separately, as they may be stricter than the requirements of NIS2 itself due to the minimum harmonization principle.*

*In order to ensure that the affected business units actually report to and register with the relevant competent body, it is first necessary to check whether they are affected and whether they are connected, in order to then determine the relevant responsibility in accordance with the law. Based on this, it is then possible to analyze which requirements of which EU country are relevant for which parts of the company.*

**What role do the individual company divisions (e.g., IT, legal department) play in fulfilling the NIS2 requirements in a group?**

*In general, the holistic view of the company aims to make the relevance of all areas of the company clear. The scope can no longer be limited to the IT used for a specific service or performance. Instead, all IT processes used by the company must be included in the implementation of the requirements.*

*By this, the legislator specifically means all the activities a company undertakes in order to provide its services. This is a major regulatory change. Many companies are therefore faced with the challenge of either rolling out an existing ISMS company-wide or establishing a new ISMS across the entire company.*

*Business Continuity Management (BCM) is critical, with all relevant stakeholders contributing to the Business Impact Analysis (BIA). Those responsible for BCM, IT security, ISMS, and (IT) risk management must work together to map business risks in a consistent manner. Compliance officers and the purchasing department, who must be trained for the incident management process, also play an important role.*

*In my opinion, this is precisely where the major success factor of NIS2 lies: a uniform company-wide understanding and awareness is required in order to counter current and future threats in the cyber world. The gateway for a threat can be in IT as well as in OT (Operative Technology). Where the incident occurs is not relevant from this perspective - a hit is a hit.*

**What role does the "gateway" data center play?**

*The "gateway" refers to the often forgotten fact that data centers operated in-house fall under the economic activity mentioned in Annex 1. Companies that operate their own data centers exclusively for their own IT are exempt from these regulations. However, the independence of the data center must be carefully checked.*

*This is intended to prevent companies from outsourcing their data centers to subsidiaries. If a group has a subsidiary that operates a data center for other companies in the same group, the exemption no longer applies. This is because, in this case, there is an affiliated company and the outsourced company is deemed to be the operator of a data center and is therefore affected.*

**What about NIS2 applicability and secondary employment?**

*The decisive factor for whether a company is affected is not its core business, but rather all of its economic activities. If a company division falls under the activities listed in NIS- , the entire company is considered to be affected. It is therefore better not to carry out an impact analysis using a standard form. It is important to take a really close look and follow a structured analysis.*

**NIS2 & Group structures**

- **Jurisdiction: Depends on the independence of the parts of the company; regulations of the EU country in which the head office or decision-making body is located.**
- **Holistic approach: Involvement of all areas of the company (IT, legal department, management) in the implementation of the requirements.**
- **Important: Independence of subsidiaries must be proven in order to comply with various regulatory requirements.**

**NIS2 & Outsourcing**

**How does outsourcing affect compliance with NIS2 requirements?**

*Outsourcing in the sense of "I set up my own company and thus have smaller values and figures that I have to use for evaluation and can thus bypass parts of the company from fulfilling the requirements" will not work. NIS2 is aimed precisely at preventing this. In actual outsourcing, differentiated supply chain security comes into play. Companies must analyze which activities are outsourced, how relevant and critical these are to their operational capability, and carry out an appropriate risk analysis. The results should be translated into requirements that are regularly reviewed and set out in contracts.*

**NIS2 & Outsourcing**

- **Avoidance of circumvention: Outsourcing to circumvent the NIS2 requirements is not permitted.**
- **Supply chain security: Detailed analysis of outsourced activities and their criticality for operational capability.**
- **Measures: Formulate and regularly review results-based requirements to ensure compliance.**

**VICCON has been supporting companies, public institutions and KRITIS operators in the implementation of information and cybersecurity for 25 years. Through tailor-made solutions, VICCON optimizes business processes, strengthens resilience, and enables compliance with regulatory requirements. More information at www.viccon.de**

VICCON
CONSULTING

# What is behind the NIS2 directive?

The NIS2 Directive, short for "Network and Information System Security", is an important step by the European Union to strengthen cybersecurity in its member states. It replaces its predecessor, the NIS Directive, and introduces a series of new, stricter requirements.

**Background and objectives:**
Increasing digitalization and growing dependence on digital technologies have significantly increased the threat of cyberattacks. Critical infrastructures, such as energy supply, transport, healthcare and financial services, are particularly at risk. The NIS2 Directive was developed to:

- **Ensure a higher level of cybersecurity:** By introducing stricter requirements, companies and organizations should be better protected against cyberattacks.
- **Create a uniform level of security in the EU:** The directive is intended to help ensure that all EU member states implement comparable cybersecurity standards.
- **Improve cooperation between the member states:** Member states are to take joint action against cyber threats through an increased exchange of information and better coordination.

**Key points of the NIS2 Directive:**

- **Extended scope of application:** The NIS2 Directive covers a larger number of sectors and companies than its predecessor.
- **Stricter requirements:** Companies must carry out comprehensive risk analyses, create incident management plans, and regularly review their IT systems.
- **Obligation to report:** Companies are obliged to report certain cyberattacks to the competent authorities.
- **Cooperation with authorities:** Companies must work closely with the relevant authorities to combat cyberattacks.
- **Stricter sanctions:** Companies that violate the NIS2 Directive will face heavy fines.

**Why is the NIS2 Directive important?**

- **Critical infrastructure protection:** The NIS2 Directive will better protect critical infrastructure and increase the EU's resilience to cyberattacks.
- **Strengthening the economy:** A secure digital infrastructure is a prerequisite for a functioning economy.
- **Protection of citizens:** The NIS2 Directive provides better protection for citizens' personal data.

The NIS2 Directive is an important step towards strengthening cybersecurity in Europe. It presents companies and organizations with new challenges and at the same time offers them the opportunity to increase their resilience to cyberattacks.

## Strategic importance for corporate security

The NIS2 Directive represents an important strategic milestone in cybersecurity for companies. It requires companies to fundamentally rethink their cybersecurity strategies and take proactive measures. In addition, NIS2 brings decisive benefits for corporate security that go far beyond regulatory compliance.

The strategic importance of NIS2 lies in reputation management. A successful cyberattack can cause massive damage to a company's reputation and destroy customer trust. NIS2 requires companies to take proactive measures to minimize such risks and protect their image. The directive promotes a comprehensive risk analysis and a robust incident management plan, which are crucial for protecting corporate reputation.

The NIS2 Directive also has far-reaching implications for business continuity. By implementing the directive, companies can significantly increase their resilience to cyberattacks and protect their business processes from potential disruption. This is particularly important at a time when cyber threats are becoming increasingly complex and dangerous. Regular updates, backups and a structured emergency plan are therefore essential components of the cybersecurity strategy.

In addition, NIS2 can serve as a catalyst for innovation in the field of cybersecurity. Companies that look closely at the directive's requirements can use new technologies and security solutions to strengthen their systems. This proactive attitude not only gives them a competitive advantage, but also contributes to the continuous improvement of security standards. Compliance with NIS2 thus becomes a strategic advantage that not only protects companies, but also strengthens their market position.

*"Critical infrastructure is in the spotlight because the threat is real. Organizations that are not managing their risk today are not only putting their data at risk, they are putting their ability to do business at risk. It's not just about compliance - it's about protecting our economy and our citizens."*

**Florian Frisse, Partner and Lawyer, Schalast**

# Important innovations compared to the previous NIS Directive

The NIS2 Directive is a development of the original NIS Directive that introduces significant changes and new requirements. Both directives have the clear aim of strengthening cybersecurity in the European Union and protecting companies and organizations from cyberattacks.

Digital transformation is progressing rapidly and with it the complexity of cyber threats. We must act to protect our systems and data. The NIS Directive was introduced to counter these risks and protect critical services, sensitive information, and the well-being of people and the economy.

However, since its introduction in 2018, it has become clear that the NIS Directive has not been implemented uniformly in member states. This led to an inefficient, fragmented system. The resulting inadequacies necessitated a revision to take into account current market requirements and create a more detailed, improved piece of legislation.

The new NIS2 Directive extends the scope of application and contains stricter reporting obligations and increased sanctions. It calls for more comprehensive cybersecurity measures and strengthens the personal liability of management. It also establishes new mechanisms for coordination and cooperation at a European level. The implementation of the NIS2 Directive will not be carried out exclusively in the BSIG. For example, the TKG will also be amended; the catalog of measures to be taken will be included in Section 165 TKG-E and the notification procedure in Section 168 TKG-E.



The following table contains a detailed comparison of the most important new features of the NIS2 Directive compared to the original NIS Directive:

| | NIS Directive | NIS2-Directive |
|---|---|---|
| **Area of application** | Operators of essential services, providers of digital services | Extension to additional sectors such as the chemical industry, medical devices, food processing, social networks. New terms: "essential facilities" and "important facilities" |
| **Cybersecurity measures** | Basic measures to ensure cybersecurity | Advanced measures including risk management, business continuity, supply chain security, cyber hygiene, cryptography and more |
| **Reporting obligations** | Report significant incidents, time limits not specified | Stricter reporting obligations: Initial notification within 24 hours, detailed notification within 72 hours, final notification within one month |
| **Sanctions** | National sanctions, no uniform requirements | Higher fines: up to €10 million or 2% of global turnover for significant facilities; up to €7 million or 1.4% of global turnover for significant facilities |
| **Liability** | No specific regulations on the liability of management | Personal liability of management for the implementation of cybersecurity measures |
| **Certifications** | No explicit requirements, some national regulations | Increasing importance of audits and certifications, obligation for operators of critical infrastructures and essential facilities to provide evidence to the BSI every three years |
| **Security of the supply chain** | No specific requirements | Comprehensive requirements for supply chain security, including the security aspects of relationships with suppliers and service providers |
| **EU-CyCLONe** | Not available | Establishment of the European Cyber Crisis Coordination Network (EU-CyCLONe), support for countries in managing large-scale cybersecurity incidents |
| **Peer Reviews** | Not available | Introduction of voluntary peer reviews to improve cybersecurity and exchange best practices between member states |
| **Cyberhygiene** | No specific regulations | Introduction of cyber hygiene measures, including regular software updates, password changes, network segmentation and training for employees. |

The NIS2 Directive is an important step towards strengthening cybersecurity in the EU. It sets new standards and at the same time promotes cooperation and the exchange of information between member states. Companies, especially SMEs, must be prepared for higher requirements and possible adaptation needs in order to meet the new requirements.

## Transposition into national law

On May 7, 2024, the draft bill for a law to implement the NIS2 Directive and to strengthen IT security in the federal administration was published in Germany. On July 24, 2024, the Federal Cabinet passed a draft law to strengthen IT security in Germany. The draft law was forwarded to the Bundesrat by the Federal Government on August 16, 2024. The NIS2 Directive is to be implemented by amending the existing BSIG. It is unclear whether the legislative process will be completed by the deadline in October 2024. The BMI timetable envisages entry into force in March 2025. .

**The debates in Germany make it clear that the transposition of the NIS2 Directive into national law is a complex and time-consuming process.** Some EU member states are already much further along than Germany.

The Federal Government's draft law to implement the NIS-2 Directive and to regulate the main features of information security management in the Federal Administration (NIS-2 Implementation and Cybersecurity Strengthening Act; Drs. 380/24) contains an amendment to the Federal Office for Information Security Act (BSI Act - BSIG) as well as amendments to a number of other federal laws (including the BND Act, the Telecommunications Act, the Whistleblower Protection Act, the Energy Industry Act, parts of the Social Security Code, the Foreign Trade and Payments Ordinance, and many others).

The following explanations contain only the regulations (most relevant for companies) contained in the BSI draft law (BSIG-E) (from Part 3, Chapters 1 and 2):

**Competent authority and central reporting office**

§ Section 3 BSIG-E comprehensively regulates the tasks of the Federal Office for Information Security (BSI), which, according to Section 4 BSIG-E, is the central reporting office for the cooperation of federal administration institutions in information technology security matters and, according to Section 5 BSIG-E, receives information on security risks in information technology and evaluates this information as the central office for reports from third parties.

According to Section 40 (1) BSIG-E, the BSI is also the national liaison office and central reporting and contact point for the supervision of particularly important and important institutions.

**Sectors of particularly important and significant facilities**

Annexes 1 and 2 to the BSIG-E regulate the sectors of particularly important and important facilities (Annex 1) and (only) important facilities (Annex 2), subdividing them into sectors and facility types, whereby the draft partially consolidates the sector terms mentioned in the NIS2 Directive. Annex 1 contains the sectors of energy, transport and traffic, finance, health, water, digital infrastructure and space, while Annex 2 contains the sectors of transport and traffic, waste management, production, manufacture and trade in chemical substances, production, processing and distribution of foodstuffs, manufacturing/production of goods, providers of digital services and research.

*"NIS2 is more than just an obligation. It's an opportunity for organizations to strengthen their cyber resilience and secure the trust of their customers and partners for the long term."*

**Micheal Scheffler, VP Sales, Link11**



**Important and particularly important facilities**

The so-called **"size cap rule"** required by the NIS2 Directive, according to which uniform identification criteria based on company size are defined for all EU Member States, i***s to be implemented as follows***:

**Section 28 BSIG-E defines important and particularly important facilities as follows**

Pursuant to Section 28 (1) sentence 1 BSIG-E, the following are considered particularly important facilities:

1. Operators of critical facilities,
2. qualified trust service providers, top level domain name registries or DNS service providers,
3. providers of publicly accessible telecommunications services or operators of public telecommunications networks which a) employ at least 50 employees or b) have an annual turnover and an annual balance sheet total of more than 10 million euros each,
4. other natural or legal persons or legally dependent organizational units of a local authority that offer goods or services to other natural or legal persons in return for payment, which are assigned to one of the types of facilities specified in Annex 1 and which a) employ at least 250 employees or b) have an annual turnover of more than 50 million euros and also an annual balance sheet total of more than 43 million euros.

**Pursuant to Section 28 (1) sentence 1 BSIG-E, the following are considered important institutions**

1. Trust service providers,
2. providers of publicly accessible telecommunications services or operators of public telecommunications networks which a) employ fewer than 50 employees and b) have an annual turnover and an annual balance sheet total of EUR 10 million or less in each case,
3. natural or legal persons or legally dependent organizational units of a local authority that offer goods or services to other natural or legal persons in return for payment, which are assigned to one of the types of facilities specified in Annexes 1 and 2 and which a) employ at least 50 employees or b) have an annual turnover and an annual balance sheet total of more than 10 million euros each


13

**The following graphic shows you at a glance which groups are affected and which criteria apply:**


**Mandatory risk management**
The BSIG draft provides for comprehensive, mandatory risk management, whereby the systems must generally comply with the state of the act.

According to Section 30 (1) sentence 1 BSIG-E, particularly important institutions and important institutions are obliged to take suitable, proportionate and effective technical and organizational measures to prevent disruptions to the availability, integrity and confidentiality of the information technology systems, components and processes that they use to provide their services and to minimize the impact of security incidents. § Section 30 (2) BSIG-E specifies minimum standards, including concepts relating to risk analysis and security in information technology (No. 1), the management of security incidents (No. 2), and supply chain security (No. 4).

According to Section 31 (1) BSIG-E, operators of critical systems are subject to special requirements for risk management measures. For example, the information technology systems, components and processes that are decisive for the functionality of the critical facilities they operate are to be subject to an even higher level of protection compared to other information technology systems, components and processes of particularly important facilities, the cost of which will also have to be assessed more strictly in terms of proportionality.

Operators of critical installations are also obligated under Section 31 (2) BSIG-E to use systems to detect attacks, which must continuously and automatically record and evaluate suitable parameters and characteristics from ongoing operations. The systems should be able to continuously identify and prevent threats and provide suitable remedial measures for any faults that occur.

**Operators of critical facilities must provide the Federal Office with evidence of the implementation of the measures in accordance with Section 30 (1) sentence 1 in conjunction with Section 31 (1) and (2) sentence 1:**

- At a time determined by the Federal Office in consultation with the Federal Office of Civil Protection and Disaster Assistance, at the earliest three years after they are first considered to be an operator of a critical facility or at the latest three years after they are again considered to be an operator of a critical facility,
- And then every three years
- Through safety audits, inspections or certifications in accordance with Section 39 (1) sentence 1 BSIG-E.

**Time-critical notification and reporting obligations as well as information obligations**

**Particularly important and important facilities pursuant to Section 32 BSIG-E are obliged in particular,**

- to submit an early initial report immediately, but at the latest within 24 hours of becoming aware of a significant security incident, providing a suspicion assessment,
- immediately, but at the latest within 72 hours of becoming aware of it, a report relating to the suspicious activity report for further assessment of the significant security incident, and
- submit a final report no later than one month after the transmission of the security incident report.
- In addition, an interim report on relevant status updates must be submitted at the request of the Federal Office.

§ Section 35 BSIG-E regulates the obligation of particularly important and important institutions to inform the Federal Office in the event of a significant security incident.

**Self-classification obligation and registration obligation**
Pursuant to Section 33 BSIG-E, particularly important and important institutions as well as domain name registry service providers are obligated to register with the Federal Office via a registration option set up for this purpose, self-classifying in the relevant categories, no later than three months after they first or again qualify as one of the aforementioned institutions or offer domain name registry services.

**Certain types of entities** (DNS service providers, top level domain name registries, domain name registry service providers, providers of cloud computing services, providers of data center services, operators of content delivery networks, managed service providers, managed security service providers and providers of online marketplaces, online search engines or platforms for social network services) **are subject to a special registration obligation pursuant to Section 34 BSIG-E.**

**Possible exceptions**
Pursuant to Section 37 (1) BSIG-E, a particularly important institution or an important institution may be partially exempted from obligations under this Act in accordance with the requirements set out in paragraph 2 (simple exemption notice) or be exempted in full in accordance with paragraph 3 (extended exemption notice), provided that the institution complies with requirements that are equivalent to the obligations under this Act.

**Comprehensive obligations and liability for management boards**
According to Section 38 (1) BSIG-E, management boards of particularly important and significant institutions are personally obligated to implement the risk management measures to be taken by these institutions in accordance with Section 30 and to monitor their implementation.

According to Section 38 (2) BSIG-E, management boards that violate these obligations are liable to their institution for culpably caused damage in accordance with the rules of company law applicable to the legal form of the institution.

According to Section 38 (3) BSIG-E, management boards are also obligated to take part in regular training courses.

**Regulations on fines**
Section 65 BSIG-E provides for fines of up to €10 million or 2% of global turnover for major facilities and up to €7 million or 1.4% of global turnover for significant facilities.

**Determination of critical installations by statutory order**
Pursuant to Section 56 (4) in conjunction with Section 2 No. 22 BSIG-E, an ordinance shall determine which installations are considered critical installations.

### Liability risks and legal consequences of non-compliance

**Non-compliance with obligations arising from the implementation of NIS2 has far-reaching consequences.**

**Increase in fines:** Significant entities face fines of up to €10 million or 2% of annual global turnover for breaches, whichever is higher. For significant entities, fines can be up to 7 million euros or 1.4% of annual global turnover, whichever is higher.

**Liability of management:** The explicit obligations for management in Section 38 BSIG-E should, according to the intention of the legislator, also lead to corresponding liability in the event of non-compliance. The BSIG-E refers to the rules of company law applicable to the corresponding legal form of the institution. Liability with private assets towards the company can be particularly relevant here (e.g., pursuant to Section 43 GmbHG or Section 93 AktG).

If the management refuses to participate in training courses despite a deadline having been set, Section 61 (9) BSIG-E even provides for a temporary ban on the exercise of activities by the authorities.

**New compliance requirements and their significance**

The NIS2 Directive sets new standards for the compliance requirements of the companies affected by it. Many SMEs in particular will be confronted with compliance requirements for the first time. In order to avoid possible fines, supervisory measures or the private liability of the management, it is essential to implement an adequately equipped compliance department. For example, the reporting process stipulated by the legislator in accordance with Section 32 BSIG-E must be strictly adhered to. Precise planning and implementation of the measures to be taken is necessary to ensure proper reporting, especially in the stressful situation of a (successful) cyberattack.

**Best practice - a 5-step plan for implementation**

The necessary action steps can generally be summarized into 5 stages for most of those affected:

1. Early clarification of the roles and responsibilities of the individual stakeholders in the audit and implementation process with early involvement of those responsible for information, IT and cybersecurity within the company.
2. Identification of relevant regulations and thresholds for self-classification of the company and activities, as well as implementation of registration.
3. Setting up and regularly updating the necessary cybersecurity protection measures.
4. Carrying out fire tests for practical verification of the cybersecurity protection measures taken (remember the human factor).
5. Continuous monitoring and advancement of the process by the management.

When implementing the new legal framework, the selection of suitable legal advisors and external support is of particular importance. Once a suitable team of consultants has been found, the requested documents and data should be made available to them as quickly as possible.

## DORA and NIS2: What are the differences?

At first glance, the DORA regulation (Digital Operational Resilience Act) and NIS2 have similar objectives - namely to protect against cyber risks and increase resilience to IT disruptions. However, they differ significantly in their scope of application and requirements. While NIS2 targets a wide range of economic sectors and deals with the cybersecurity of network and information systems, DORA focuses exclusively on the financial sector and emphasizes operational resilience.

DORA's range of instruments includes IT stress tests and the management of third-party providers. The regulated financial sector includes, for example, banks, insurance companies, investment companies, payment service providers, and financial infrastructures such as stock exchanges, clearing houses and financial market infrastructures. The DORA Regulation also applies to IT service providers working for financial institutions, including cloud providers and IT security service providers. A key difference is that DORA, as a regulation, has direct legal effect in the individual EU member states, as opposed to NIS2, which requires a national transposition act that often leads to delays in the individual member states.



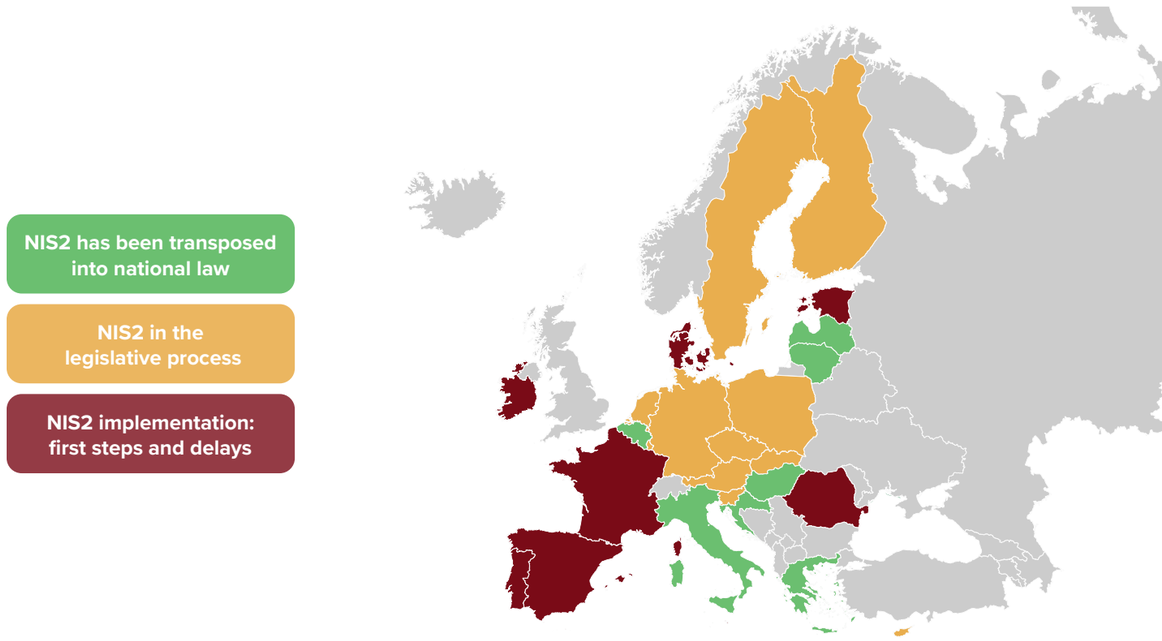
## Side view of other EU countries

Click on the fields for more information

NIS2 has been transposed into national law

NIS2 in the legislative process

NIS2 implementation: first steps and delays




Note: This information is based on the data available at the time of printing and may have changed in the meantime.

# Technical measures and safety strategies

A successful cybersecurity strategy must start with a thorough risk assessment. Companies must identify their critical assets, processes and systems and assess the potential risks to which they are exposed. Companies must develop attack scenarios in order to be able to adapt their defensive measures in a targeted manner.

- **Technical control measures for comprehensive protection** Technical control measures are essential to minimize the risks.
- **Access control:** Sensitive data and systems may only be made accessible to authorized persons. Strong multi-factor authentication and regular checks of access rights are essential.
- **Network security is a top priority:** DDoS protection, firewalls, intrusion detection and prevention systems (IDS) and strict network segmentation protect against unauthorized access and data loss.
- **End device security:** Through regular patching, the use of virus protection software and mobile device management (MDM), it is possible to ensure the security of end devices.
- **Cloud security:** Migration to the cloud requires special attention. Companies must select trustworthy cloud providers and implement strict security measures for their data in the cloud.
- **Security awareness:** An important factor for cybersecurity is trained staff. Employees must receive regular training and be made aware of the most common threats through phishing simulations.

**Incident response: react quickly and effectively**
A comprehensive incident response plan is essential in the event of an emergency. It enables a company to respond quickly and effectively to cyberattacks. This plan must define clear responsibilities, escalation paths and recovery processes. Regular simulations are essential to check the plan's effectiveness.

**Companies need to think beyond their own borders: supply chains and employees are key factors.**
In addition to implementing security controls such as network segmentation, multi-factor authentication and endpoint detection and response, organizations must also secure their supply chains. Companies need to identify and minimize potential vulnerabilities in their supply chains by incorporating stringent security requirements into contracts with third-party vendors and conducting regular risk assessments. In this context, the inclusion of an undetailed clause obliging the contractual partner to comply with defined standards is unlikely to be sufficient to avoid liability. The same is likely to apply to contractual provisions under which the contractual partner is only obliged to provide evidence of certificates or to issue declarations of compliance without any testing or monitoring.

**Compliance management:** Effective compliance management is required to ensure compliance with the NIS2 directive. Companies must fully document their security measures, carry out regular audits, and continuously work on improving their security processes. Compliance with the General Data Protection Regulation (GDPR) is crucial as it is closely intertwined with the NIS2 Directive. Companies can meet the requirements of both NIS2 and the GDPR by implementing technical measures to ensure data protection.

*"By viewing the NIS2 directive as an opportunity to strengthen their cybersecurity, companies can not only meet legal requirements, but also secure their competitive advantage."*

**Jens-Philipp Jung, CEO, Link11**



**Cybersecurity 4.0**
The role of AI and automation: Companies should invest in technologies such as artificial intelligence (AI) and machine learning (ML) to increase their resilience to cyberattacks. These technologies detect anomalies and automate security tasks. AI and ML offer new opportunities to significantly improve cybersecurity, as AI-based systems can detect anomalies in network traffic and report suspicious activity automatically.

The cybersecurity landscape is evolving rapidly. It is therefore imperative that companies continuously review and adapt their security measures. Implementing the NIS2 directive requires a holistic security strategy - no ifs, ands, or buts. Companies can significantly increase their resilience to cyberattacks and ensure the confidentiality, integrity and availability of their data and systems through a combination of technology, organization and strong security awareness. This gives them a decisive competitive advantage.

**Recommendations for decision-makers:**

**Investing in cybersecurity:** Companies must not hesitate to invest in cybersecurity. They should allocate sufficient resources to building and maintaining robust cybersecurity.

**Cooperation:** Close cooperation between the IT department, management and other relevant departments is crucial to the success of cybersecurity initiatives.

**External expertise:** If necessary, companies should call in external experts to evaluate and optimize their security measures.

**Focus on risk awareness:** Promote risk awareness and strive for continuous improvement in the areas of cybersecurity.

# Long-term effects of the NIS2 Directive

The NIS2 Directive will have a lasting impact on European cybersecurity. It will lead to a harmonization of security standards across industries and promote a risk-based approach, forcing companies to better target their security measures to their specific threats. By promoting information sharing and strengthening cooperation between companies and authorities, NIS2 will lead to a better joint assessment of the situation and a more efficient defense against cyber threats. In the long term, it will not only increase the security of critical infrastructures, but also strengthen citizens' trust in digital services.

However, the implementation of NIS2 also presents companies with challenges. Implementing an effective security strategy requires companies to plan for the long term and be willing to invest in appropriate measures. The shortage of skilled workers and the need to adapt to a constantly changing threat landscape also play a decisive role here. Companies will face new challenges in the future, such as the growing importance of cloud computing and the development of quantum technologies. In order to meet these challenges, investments in innovative security solutions and continuous employee training are required.

The NIS2 Directive represents a milestone in the European cybersecurity landscape. Due to emerging changes in the field, this directive will also have to be adapted to the constantly changing threat situation. Future adaptations could include the following aspects:

- **Extension of the scope:** The directive could be extended to other sectors that are particularly relevant for critical infrastructures.
- **Tightening supply chain requirements:** Supply chain security requirements could be tightened to minimize risks from third parties.
- **Greater focus on cloud security:** In view of the increasing importance of cloud services, the requirements for cloud security could be increased.
- **Integration of new technologies:** The directive should be regularly adapted to take appropriate account of new technologies such as AI and quantum technologies.

Cybersecurity will become increasingly complex and dynamic in the future. Companies must be prepared to adapt their security concepts on an ongoing basis. The NIS2 Directive provides an important framework for this, which is likely to become more dynamic in the future. However, it will also have to be adapted to the new challenges.

*"Decision-makers should view cybersecurity as a strategic investment and not just a cost factor. By making targeted investments in modern technologies, training and promoting a strong security culture, companies can significantly increase their resilience to cyberattacks. Sustainable cybersecurity requires a long-term commitment at all levels of the organization."*

**Janka Schwaibold, Partner & Lawyer,**
**Schalast LAW | TAX**



# Conclusion

The NIS2 Directive presents companies with a complex challenge, but also offers new opportunities. If they have not already done so, companies should immediately check whether they are affected by the NIS2 Directive by reviewing their affiliation with essential or critical KRITIS sectors. Both the specific sector classifications and the thresholds for company size must be taken into account. In addition, companies should evaluate their supply chains and customer relationships, as the security of the entire supply chain must be guaranteed in accordance with NIS2.

**Unsure whether your company is affected by NIS2?**
With the BSI's NIS2 impact assessment, you can quickly obtain an initial assessment. In just a few steps, you can find out whether your company falls under NIS2.

To the test

In order to meet the directive's requirements, companies must fundamentally rethink and adapt their security measures. The first step is a comprehensive risk analysis. This involves identifying and eliminating weak points in the IT infrastructure, processes and supply chain. The implementation of an information security management system (ISMS) in accordance with ISO 27001 can serve as a guide.

The implementation of NIS2 requires the active involvement of the entire company, especially management. Clear communication of the importance of cybersecurity and the provision of the necessary resources are crucial. Employees must be trained regularly to increase security awareness and minimize human error. Modern technologies, such as artificial intelligence and machine learning, can support companies in implementing NIS2. They enable more efficient threat detection and an automated response to security incidents. However, companies should also keep an eye on the risks associated with new technologies.

Cooperation with external experts can support companies in the implementation of NIS2. IT security service providers and law firms often have a broad range of expertise and experience that companies cannot always maintain internally.

**To meet the requirements of NIS2, companies should take the following steps:**

- **Risk assessment:** Comprehensive analysis of your own IT landscape and business processes.
- **Introduce an ISMS:** Introduce an ISMS in accordance with ISO 27001 or adapt it to the requirements of NIS2.
- **Train employees:** Conduct regular cybersecurity training.
- **Use technology:** Use modern technologies such as AI and ML.
- Consult external experts: Seek support from IT security service providers and consultants.
- **Continuous improvement:** Regular review and adjustment of safety measures.

The NIS2 directive is dynamic. Companies should be prepared for the requirements to evolve over time. A proactive and holistic approach is therefore essential to ensure the company's cybersecurity in the long term and to stand out from the competition.

## Strong together against cyber threats!

Benefit from our many years of experience in the areas of IT security and law.
Our experts will be happy to assist you.

# Contact

**Michael Scheffler**
Link11

m.scheffler@link11.com

**Janka Schwaibold**
Schalast LAW | TAX

janka.schwaibold@schalast.com

**Florian Frisse**
Schalast LAW | TAX

Florian.Frisse@schalast.com

**Lorenz Haase**
Schalast LAW | TAX

Lorenz.Haase@schalast.com

**Sophia Zimmer**
VICCON GmbH

s.zimmer@viccon.de

## Head office

Link11
Lindleystr. 12
60314 Frankfurt