MYRA

Implementing NIS-2 requirements with Myra

NIS-2 is the next stage in the evolution of the European cyber security strategy. The directive significantly expands the scope of application and sets stricter requirements for companies and organizations in critical sectors. The focus is on risk management, the reporting of security incidents and information security along the supply chain. Implementing the requirements is an enormous challenge for many affected organizations.

Myra itself is a critical infrastructure operator and as such fulfils all the requirements associated with NIS-2. In addition, Myra has more than 10 years of experience in securing digital business processes against cyber attacks at the infrastructure and application level in highly regulated sectors and critical infrastructure industries. Companies can rely on this expertise. Our customers benefit from comprehensively certified and audited solutions and processes – these contribute significantly to the fulfilment of the NIS-2 compliance requirements.

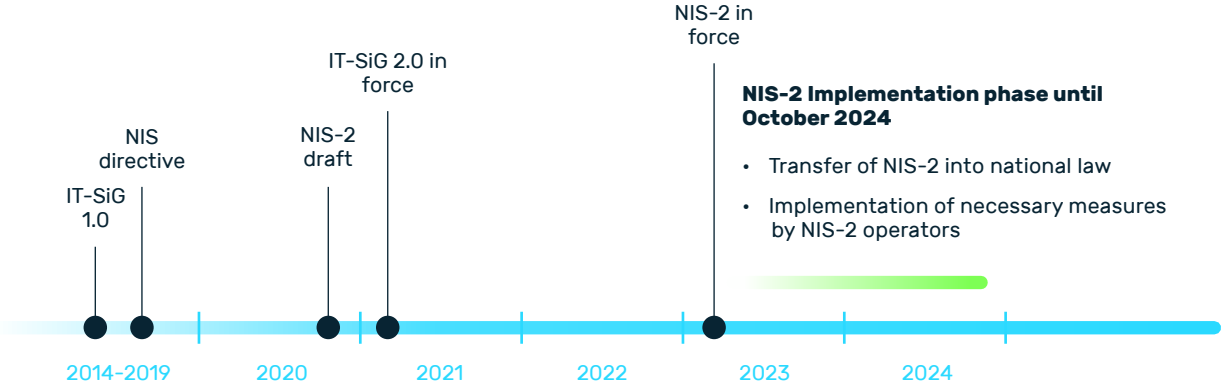
In this compliance fact sheet, you can find out in which areas Myra can support your company in implementing the NIS-2 requirements.

Disclaimer:

Please note that the information provided has been compiled to the best of our knowledge and with legal support. Nevertheless, it is for information purposes only and is not to be construed as legal advice. A general assessment of regulatory requirements is not possible due to the individual requirements of each organization.

We assume no liability for the accuracy, completeness or timeliness of the following information. Any liability or responsibility for actions taken on the basis of the information provided is hereby excluded. The basis for the fact sheet is the draft bill of the German NIS-2 Implementation and Cybersecurity Strengthening Act (NIS2UmsuCG) of June 24, 2024.

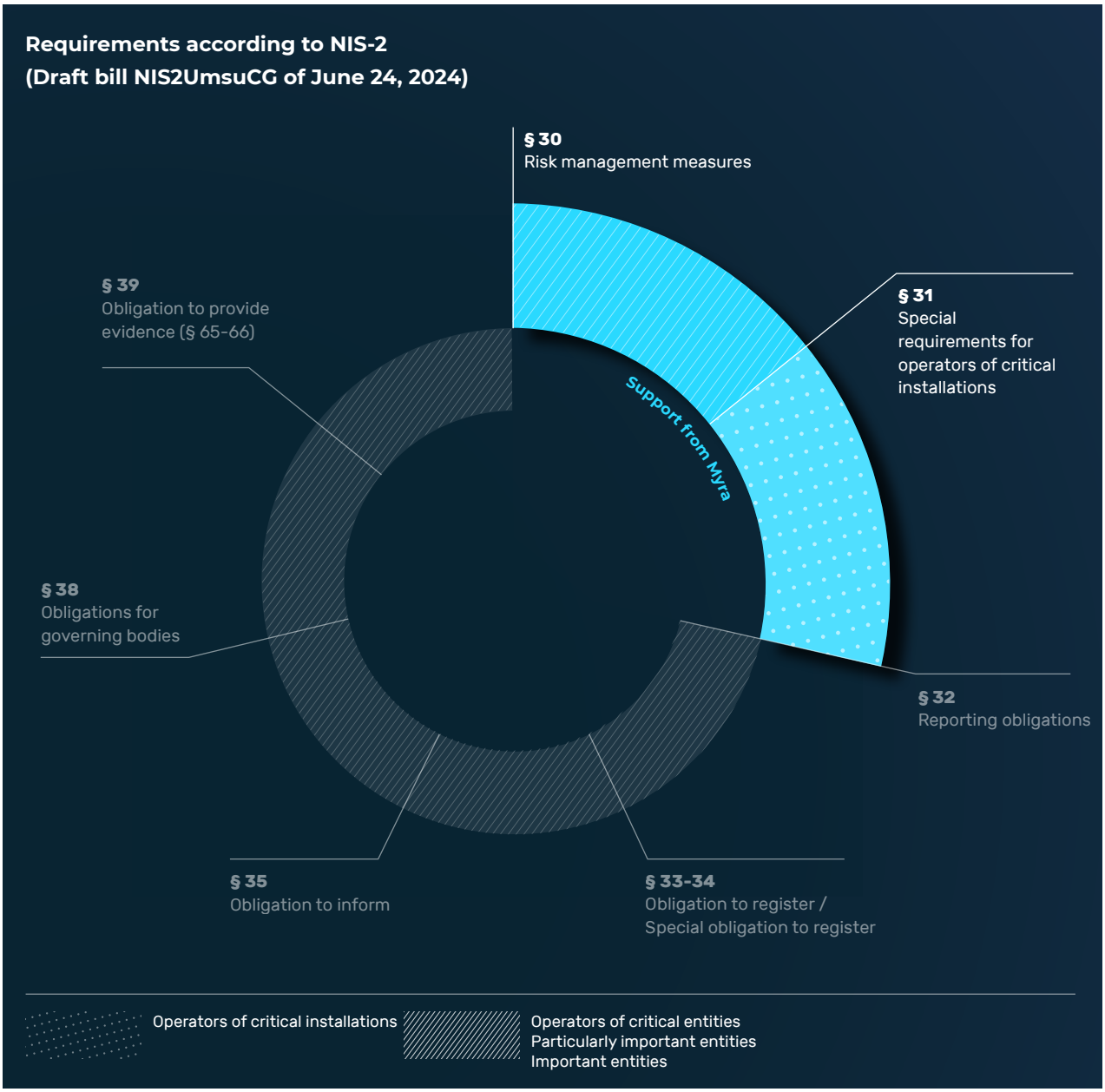
NIS timeline



Cybersecurity requirements in NIS-2

NIS-2 breaks down cybersecurity requirements into seven key areas to strengthen the resilience of operators and entities. Risk management can be emphasized as a central component of the requirements. The specific requirements for the individual areas are defined in paragraphs 30 to 35, 38 and 39, as you can see in the following diagram.

With its security solutions against cyberattacks at the infrastructure and application level, Myra can make a significant contribution to fulfilling the compliance requirements, particularly in the areas of risk management (section 30) and special requirements for operators of critical installations (Section 31).



Requirements for risk management under NIS-2

Particularly important and important entities must take technical and organizational measures to adequately prevent IT disruptions and minimize the impact of security incidents. Compliance with the measures must be documented. These should correspond to the state of the art, relevant standards and be based on a cross-risk approach.

In view of the short time until the implementation deadline and the complexity of fulfilling all requirements it is advisable to outsource individual protective measures to qualified service providers. The following table shows in detail how you can implement key NIS-2 requirements with Myra's solutions and processes.

NIS-2 requirement according to § 30 (2)	Implementation approach from Myra	
1. Risk analysis and security for information systems	By means of **individual risk analyses and ongoing security optimizations** in cooperation with customers, external auditors, supervisory authorities and our partners, Myra supports the **development and maintenance of efficient security concepts.**	✓
2. Management of security incidents	With its security solutions for the infrastructure and application level, **Myra protects websites, online platforms, web APIs and web infrastructure comprehensively and automatically** against cyber risks such as DDoS attacks, bot networks and attacks on databases. (An overview of the scope of protection of Myra solutions based on the Gartner taxonomy for DDoS mitigation solutions can be found on page 5)	✓
3. Maintenance of operations, recovery, backup management, crisis management	Myra's solutions ensure error-free operation of processes and thus ensure business continuity - even in the event of an ongoing attack. The **multiple geo-redundant server infrastructure** ensures fail-safe high availability using **policy-based routing and IP Anycast.** In addition, Myra allows redundancies to be **secured across multiple data centers and cloud instances** in order to ensure consistent protection functionality and quality.	✓
4. Security in the supply chain, security between facilities, service provider security	The **AI-based bot and threat detection with automated defense against attacks** prevents attackers from accessing web processes in real time and thus protects against the compromise of systems and the spread of malware to connected organizations.	✓
5. Security in the acquisition, development and maintenance of information technology systems	Myra's technology and the protection services operated on it are **comprehensively tested, audited and certified** to guarantee our customers the highest level of integrity, confidentiality and availability. • BSI ISO 27001 on the basis of IT-Grundschutz • KRITIS certificate according to § 8a para. 3 BSIG • BSI C5 Type 2 • PCI DSS • DIN EN 50600 • IDW PS 951 Type 2 (ISAE 3402) • Trusted Cloud • VS-NfD	✓
6. Evaluation of the effectiveness of risk management measures	Myra's **real-time monitoring** allows the **granular identification, classification and logging of anomalies and security incidents at traffic level.** All logged events are based on server events for fully transparent **traffic visibility.** Freely definable threshold initiate **automatic responses to attacks** and trigger **escalation paths for notifying and warning** of affected organizations.	✓

7. Cyber hygiene and training in the area of cyber security	Myra's security services are continuously updated and optimized to defend against new and acute threats. In addition, Myra offers a wide range of **functions to maintain cyber hygiene,** such as **granular rights management** for users of the platform, **mandatory strong passwords as well as 2-factor authentication or support for client certificates (mTLS) for zero trust concepts.** ✓
8. Use of cryptography and encryption	Myra's services offer the highest level of security. The **SSL/TLS certificates** of our customers are stored in a secure area of our infrastructure. It is not possible to download or display existing SSL/TLS certificates from the Myra platform. Decoding only takes place to check the packets **(deep package inspection).** The entire communication in our network to the outside world, to the user and to your origin server, is **fully encrypted.** SSL/TLS termination at Myra takes place exclusively in Germany at the customer's request - **legally GDPR-compliant.** As a German company, Myra is not affected by the US surveillance laws FISA Section 702 and CLOUD Act. ✓
9. Security of personnel, access controls and system management	Myra's **user management** allows granular **management of access and administration rights** for the security services, including **guidelines for password strength** and **mandatory 2-factor authentication.** In addition, Myra supports the **use of client certificates (mTLS) for the implementation of zero trust concepts.** ✓
10. Multi-factor authentication or continuous authentication, secure communication (voice, video, text), emergency communication systems	

Special requirements for operators of critical installations according to § 31	**Implementation approach of Myra**
1. Higher standards and more extensive measures for risk management according to § 30	Myra has **more than 10 years of experience in securing critical infrastructure** – the implementation of comprehensive security requirements is our daily business. As one of the leading providers Myra fulfills all 37 criteria of the BSI for qualified **DDoS mitigation service providers in accordance with § 8 BSI Act (BSIG).** In addition, Myra itself has a **certificate in accordance with § 8a para. 3 BSIG for critical infrastructures** and thus fulfills the BSI's requirements for „KRITIS" operators. Furthermore, Myra's security services comply with the **BSI C5 Type 2** and are certified in accordance with **ISO 27001 on the basis of IT-Grundschutz.** ✓
2. Use of state-of-the-art technology for attack detection	Thanks to **real-time monitoring**, Myra allows the granular **identification, classification and logging of anomalies and security incidents at traffic level.** All logged events are based on server events for fully transparent **traffic visibility.** Freely definable threshold initiate **automatic reactions to attacks** and trigger escalation paths to notify and warn affected organizations. ✓

Scope of protection of Myra according to Gartner taxonomy for DDoS mitigation services

To ensure sufficient cyber resilience and safeguard business continuity, it is essential to implement a comprehensive protection system. In the area of application and infrastructure protection, Myra delivers all functionalities defined by Gartner – from DDoS protection across all relevant layers to Secure CDN, Web Application and API Protection (WAAP) as well as DNS Security.

Core capabilities	
Detection and mitigation of Layer 3 volumetric attacks	✓
Amplification/reflection attacks (via DNS, NTP, SSDP, CLDAP, Memcached etc.)	✓
Carpet bombing	✓
ICMP flood attacks etc.	✓
Detection and mitigation of Layer 4 protocol attacks, causing resource exhaustion	✓
Flood attacks (UDP, TCP SYN, ACK, SYN/ACK, RST, UDP fragmentation etc.)	✓
Detection and mitigation of Layer 7 application layer attacks	✓
HTTP flood attacks (GET, POST, HEAD, Recursive GET Flood etc.)	✓
Low-and-slow attacks (Slowloris etc.), ReDoS, Denial of Wallet attacks	✓
Detection and mitigation of multivector attacks	✓

Optional capabilities	
Real-time logging and reporting interface	✓
Security Operations Center (SOC) and Managed Security Services (MSS)	✓
CDN	✓
Web Application and API Protection (WAAP)	✓
Bot mitigation	✓
Domain Name System (DNS) security	✓

Made in Germany

Myra Security is the new benchmark for global IT security.

Would you like to find out more about how you can use our solutions to increase your revenue, minimize your costs and protect your applications from malicious attacks? Our team of experts will be happy to advise you individually and develop a customized solution for your company. Why not arrange a no-obligation consultation today?

Request free protection advice →

Myra Security GmbH

+49 89 414141 - 345
www.myrasecurity.com
info@myrasecurity.com