NIS-2 Transposition in Germany: Who is affected, obligations, fines for companies

www.massandra-eBusiness.com

👉 Operators of critical facilities

The sectors for operators of critical facilities are defined separately from the NIS-2 entities and both in the NIS-2 Directive and in the KRITIS framwork law. Critical facilities are those whose failure or impairment could have significant effects on the security of supply or public safety. Some of the critical services and facilities still have to be defined in an ordinance. The KRITIS framework law is still being drafted. Thresholds for critical facilities are set out in the "Ordinance on the Determination of Critical Infrastructure under the BSI Act" BSI-KritisV.

👉 **KRITIS thresholds:** They belong to an operator of critical facilities according to the installation categories if a threshold value is exceeded.

👉 Operators of critical facilities must comply with both the KRITIS framework law and the NIS-2 directive. Operators of critical facilities, regardless of the size of the company, are always regulated as an essential entity and as an operator of a critical facility.

Essential entities

👉 Operators of critical facilities;

👉 Qualified trust service providers, top-level domain name registries or DNS service providers;

👉 Providers of publicly available telecommunications services or of public telecommunications networks that
(a) employ at least 50 employees or
(b) have an annual turnover and an annual balance sheet total of more than 10 million euros;

👉 Natural or legal persons who offer other natural or legal persons goods or services for a fee t that can be assigned to one of the types of facility specified in **Appendix 1** and which
a) employs at least 250 employees or
b) has an annual turnover of more than 50 million euros and an annual balance sheet total of more than 43 million euros.

Important entities

👉 Trust service providers

👉 Providers of publicly available telecommunications services or of public telecommunications networks that
(a) have fewer than 50 employees and
(b) have an annual turnover and an annual balance sheet total of 10 million euros or less.

👉 Natural or legal persons who offer other natural or legal persons goods or services for a fee that can be assigned to one of the types of establishment specified in **Appendices 1 and 2** and who
a) employ at least 50 people or
b) have an annual turnover and an annual balance sheet total of more than 10 million euros each.

NIS-2 Transposition Germany

NIS-2 government draft of October 2, 2024

Sectors critis: Operators of critical facilities

1. Energy,
2. Transportation and Traffic,
3. Financial and Insurance services,
4. Health,
5. Nutrition,
6. Information technology and Telecommunications,
7. Residential and Waste disposal,
8. Water.

NIS-2 Sectors Appendix 1

1. Energy,
2. Transportation and Traffic,
3. Finance
4. Health
5. Water
6. Digital Infrastructure
7. Space

NIS-2 Sectors Appendix 2

1. Transportation and Traffic: Postal and courier services,
2. Waste management,
3. Production,
4. Manufacturing and trade in chemical substances,
5. Production, processing and distribution of food,
6. Processing industry/manufacturing of goods,
7. Digital service providers,
8. Research.

Special cases and extended obligations

1. DORA, TKG, EnWG regulated companies,
2. Operators of Internet Exchange Points,
3. DNS service providers,
4. Top Level Domain Name Registry,
5. Cloud computing service providers,
6. Data center service providers,
7. Content Delivery Network operators,
8. Managed services providers,
9. Managed security services providers,
10. Online marketplace providers,
11. Online search engines,
12. Social networking service platforms,
13. Providers of publicly available electronic communications services.

👉 Additional obligations for operators of critical facilities

§ 31 Special requirements for risk management measures
§ 32 Reporting requirements
§ 33 Registration requirement
§ 34 Special registration requirement for certain types of facilities
§ 35 Information requirements
§ 39 Verification requirements for operators of critical systems
§ 41 Prohibition of the use of critical components

👉 § 65 Administrative fine regulations

- Important entities: Fines of between EUR 100,000 and EUR 7 million (or up to 1.4 percent of annual revenue) depending on the infringement.
- Essential entities: Fines of between EUR 100,000 and EUR 10 million (or up to 2 percent of annual revenue) depending on the infringement.

👉 §§ 61,62 Enforcement measures

- Ordering audits, inspections or certifications
- Defining technical and organizational requirements
- Verifying compliance with requirements
- Ordering measures to prevent or resolve a security incident
- Providing information about cyber threats
- Publicly disclosing violations
- Reporting to the relevant regulatory authority
- Suspending the license and prohibiting the activity

👉 § 30 Risk management measures for particularly important facilities and important facilities

- Concepts relating to risk analysis and information technology security.
- Security incident management.
- Business continuity, such as backup management and disaster recovery, and crisis management.
- Security of the supply chain, including security-related aspects of the relationships between the individual facilities and their immediate providers or service providers.
- Security measures for the acquisition, development and maintenance of information technology systems, components and processes, including management and disclosure of vulnerabilities.
- Concepts and procedures for evaluating the effectiveness of risk management measures in the area of information technology security.
- Basic procedures in the area of cyber hygiene and training in the area of information technology security.
- Concepts and procedures for the use of cryptography and encryption.
- Security of personnel, concepts for access control and for the management of facilities.
- Use of multi-factor authentication or continuous authentication solutions, secure voice, video and text communications, and, where appropriate, secure emergency communications systems within the facility.

👉 §§ 32, 35 Reporting requirements, duties to provide information

Essential entities and important entities are required by the NIS2 regulation to report significant security incidents without undue delay and to inform recipients of their services about such incidents. The German Federal Office for Information Security (BSI) offers feedback and support in managing the incidents:
Within 24 hours of becoming aware of the incident, within 72 hours of becoming aware of the incident, an update to the report.
At the request of the Federal Office, an interim report, a final report no later than one month after submission of the report of the security incident.

👉 § 33 Registration obligation

Essential entities and important entities must register with the Federal Office no later than three months after they are first or again considered as such. Registration is carried out via a registration option set up jointly by the Federal Office (BSI) and the Federal Office for Civil Protection and Disaster Assistance. This registration includes basic information such as name, contact details and the sector of the entity.

👉 § 38 Duties of the management of essential entities and important entities

- Executive boards are obliged to implement the risk management measures to be taken by these institutions in accordance with § 30 and to monitor their implementation.
- Executive boards that violate their obligations shall be liable to their institution for any culpably caused damage in accordance with the rules of company law applicable to the legal form of the institution. Under this Act, they shall only be liable if the company law provisions applicable to the institution do not contain any liability provision.
- The management boards must regularly attend training sessions in order to gain sufficient knowledge and skills to recognize and assess risks and risk management practices in the area of security in information technology, as well as to be able to assess the effects of risks and risk management practices on the services provided by the institution.