NIS 2

High Cyber Security Requirements

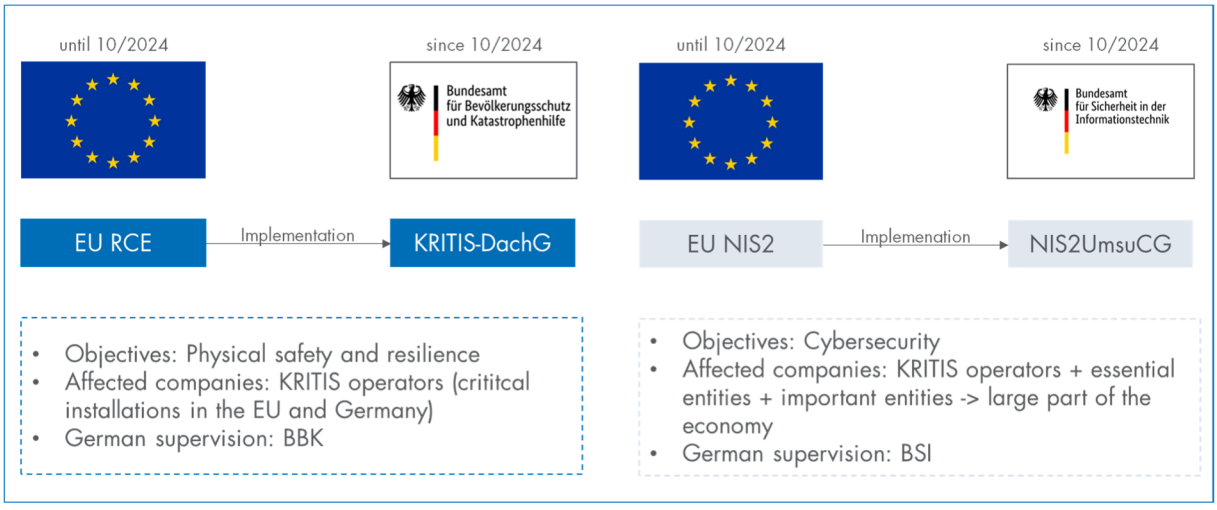
Since the entry into force of the Directive on measures for a high common level of cybersecurity across the Union – NIS 2 (EU 2022/2555), cybersecurity should be a top priority for companies. NIS 2 has once again significantly expanded the catalogue of measures and obligations for companies with regard to cybersecurity. It now applies not only to 'critical infrastructures' in the narrow sense, but instead places comprehensive, high cybersecurity requirements on companies. NIS 2 is generally applicable to both public and private institutions. In certain sectors, companies are affected regardless of their size.

Fact Sheet on the Implementation of NIS 2

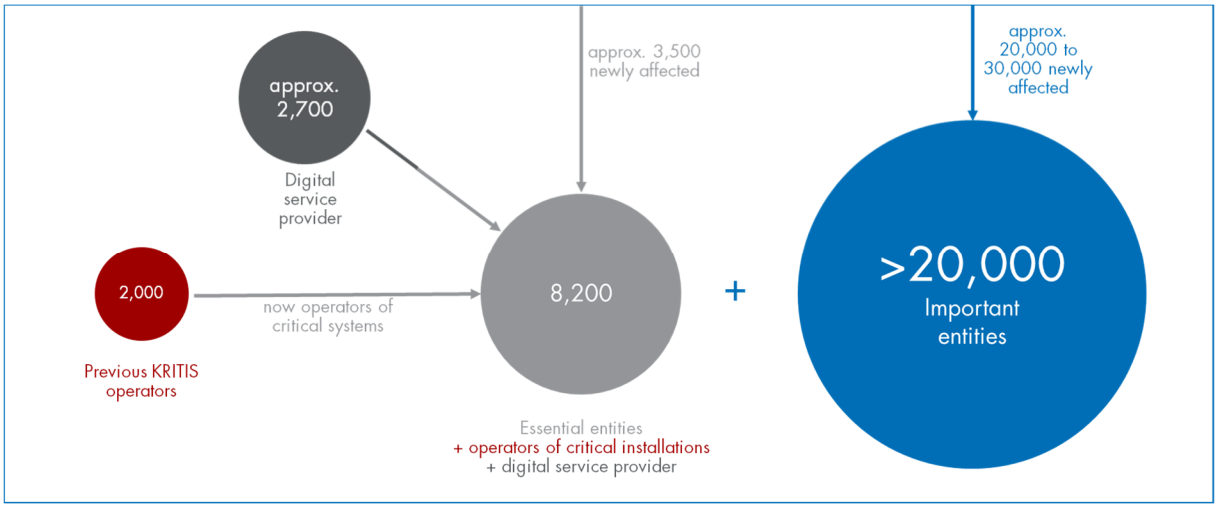
Background and Principles of NIS 2

The implementation of the NIS 2 (Network and Information Security) Directive is part of the EU cybersecurity strategy to strengthen and standardise the level of IT security within the EU. In Germany, the NIS 2 Implementation and Cybersecurity Strengthening Act (NIS2UmsuCG) is implementing the directive, which significantly reforms the Act on the Federal Office for Information Security (BSI Act – BSIG).

In light of a 'hybrid threat situation', the EU cyber security strategy with the 'CER' (Critical Entities Resilience) Directive also focuses on the physical protection of critical installations (sabotage, natural disasters, etc.). The CER Directive is implemented through the KRITIS-Dachgesetz (KRITIS-DachG – German Critical Infrastructure Act).



NIS 2 implementation will no longer only affect operators of 'critical infrastructures' ('KRITIS'), but will affect the broader economy. The legislator estimates that around 30,000 additional companies and institutions will be affected.



When Do NIS 2 Regulations Apply?

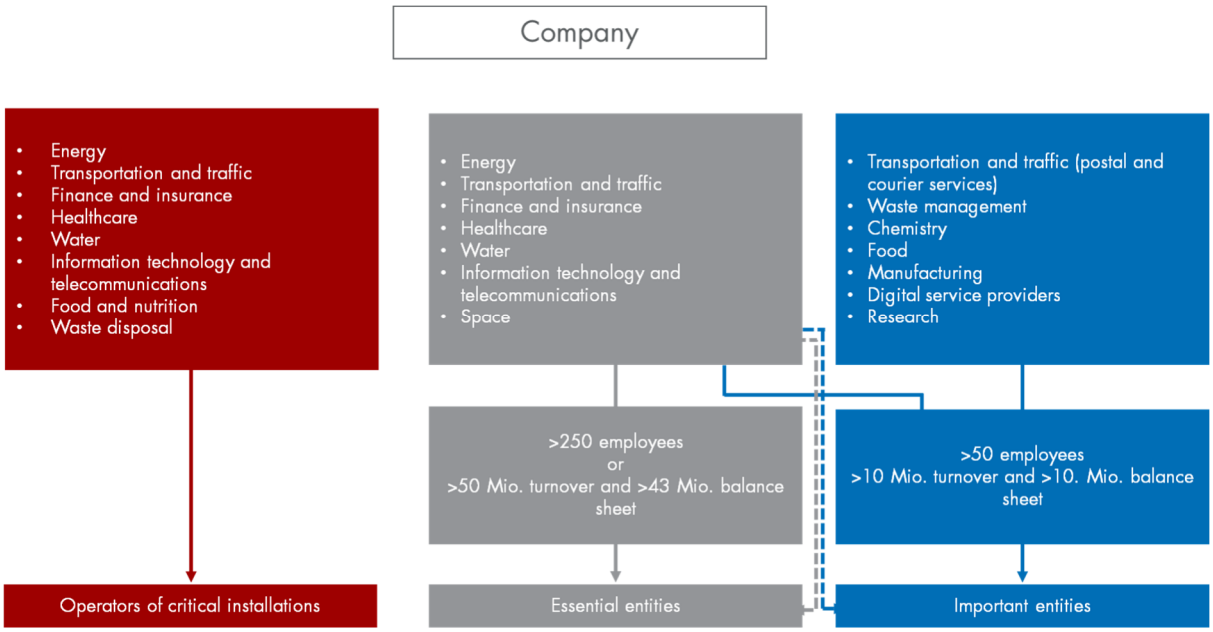
The NIS 2 Directive must be implemented by the EU member states. The implementation period expires on 17 October 2024. It is currently assumed that NIS2UmsV CG will not come into force before autumn 2025. However, it will apply immediately to the companies affected as soon as it comes into force.

Scope

To determine whether a company or organisation falls within the scope of the NIS2UmsvG, the following key questions must be answered:

- Does the business activity fall within one of the sectors?
- Are the thresholds from Sec. 28 BSIG-E (the draft version of the Federal Office for Information Security Act) or the (new) BSI KRITIS (Critical Infrastructure) Regulation reached?

A distinction is made between 'important entities' and 'essential entities', as well as 'operators of critical installations' (as a category of 'essential entities').



The graphic provides an overview. For a precise classification, an individual case assessment is required, which also involves clarifying specific questions regarding the calculation, the treatment of group companies, secondary activities of a company and also the assignment of a company to multiple sectors. We are available for any further questions and happy to assist you with this!

NIS 2 Obligations for Affected Companies

Companies that fall within the scope of NIS 2 must comply with several obligations, including:

Risk management measures (Sec. 30, 31 BSIG-E):

- Policies on risk analysis and information system security;
- Incident handling (management of security incidents);
- Business continuity, such as backup management and disaster recovery, and crisis management;
- Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
- Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
- Policies and procedures for the assessment of the effectiveness of cybersecurity risk-management measures;
- Basic practices for cyber hygiene and cybersecurity training;
- Policies and procedures for the use of cryptography and encryption;
- Human resources security, access control policies and asset management;
- Use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Reporting obligations (Sec. 32 BSIG-E): 24h/72h/30 days, if applicable, interim reports to the BSI.

Registration obligations (Sec. 33, 34 BSIG-E): Deadline: 3 months.

Notification obligations (Sec. 35 BSIG-E).

Implementation, monitoring and training obligations for management bodies (Sec. 38 BSIG-E). Management bodies that violate these obligations are liable to the company for any damage culpably caused as a result.

Proof obligation for operators of critical installations (Sec. 39 BSIG-E): Audits, inspections, certifications. Every three years, random checks by the BSI.

If applicable, appointment of a representative (Sec. 60 (3) BSIG-E).

Sanctions

In the event of non-compliance with the obligations, essential entities may be fined up to €10 million (or 2% of global turnover); important entities may be fined up to €7 million (or 1.4% of global turnover).

If essential entities fail to comply with the BSI's orders under this law in the event of cybersecurity deficits, despite a set deadline, their operating licence may be temporarily suspended in whole or in part, or unreliable management bodies may be temporarily prohibited from performing their duties.

Our Approach

Our lawyers provide comprehensive legal and strategic advice on the implementation of NIS 2. We take an integrated approach, covering IT security law, data protection, compliance and risk management, insurance law (including cyber insurance issues), defamation and media law (reputation protection) and, where appropriate, criminal law.

When it comes to more technical issues, such as the specific implementation and appropriateness of the required risk management measures, including a technical gap analysis, we rely on close cooperation with specialised partners.

Michael Herold

Partner
m.herold@gvw.com

Arnd Böken

Partner
a.boeken@gvw.com