Management Statement of the SBF AG on KRITIS and NIS-2

Sustainable and responsible conduct – including with regard to IT security and physical security – is a core element of our corporate strategy. As a medium-sized company in the manufacturing sector, we consider it our responsibility to reconcile economic success with environmental and social responsibility as well as sound corporate governance.

Brief Description of the Company

- The SBF Group comprises specialists for innovative solutions in the areas of rolling stock, lighting, electromechanics and sensor technology. Within the corporate group, highly specialized and leading hidden champions in their respective fields combine their expertise. With a high-quality and forward-looking product and service portfolio, SBF benefits from megatrends such as mobility, climate protection, automation and digitalization, as well as from security solutions for critical infrastructures and defense applications. In addition, we have qualified capacities in development and engineering as well as in production for the local manufacturing of critical components, particularly in the context of increasingly fragile global supply chains.

- In the “Rolling Stock” business segment, the tier-1 system supplier and development partner supplies the world’s leading rolling stock manufacturers with complex interior, ceiling and lighting systems “Made in Germany”.

- The “Public and Industrial Lighting” business segment includes intelligent and customized LED systems for the efficient lighting of industrial, municipal and infrastructure projects.

- In the “Sensor Technology and Electromechanics” business segment, forward-looking components and software for electromechanical products such as circuit boards, sensors and communication technologies are developed and manufactured.

Further information is available at: https://www.sbf-ag.com.

KRITIS-related aspects, to the extent relevant to our company, are integrated into our Quality Management Manual (QM Manual). Measures and updates are reviewed and updated on a regular basis.

As the topic of KRITIS is also relevant to our contractual partners, we have summarized the key aspects in order to reduce potential risks for our partners.

Requirements under the KRITIS Umbrella Act

The law follows an **all-hazards approach**. It does not focus on a specific scenario but requires resilience against natural hazards (such as climate change), technical failures, and human threats (such as sabotage or terrorism). The addressees of the law are the operators of critical facilities.

The key obligations can be grouped into four pillars:

1. **Registration and Identification (§ 16 KRITIS-DachG-E)**
   Operators must independently identify their facilities and register them with the Federal Office of Civil Protection and Disaster Assistance (BBK). This will, for the first time, establish a comprehensive register of critical facilities in Germany.

2. **Risk Analysis (§ 12 KRITIS-DachG-E)**
   A comprehensive risk analysis must be conducted every four years. This analysis must be based on the Federal Government’s National Risk Analysis and must assess local threats. Dependencies on other sectors (e.g., electricity or water supply) must be explicitly taken into account.

3. **Resilience Measures and Resilience Plan (§ 13 KRITIS-DachG-E)**
   A central element of the law is the obligation to implement “appropriate and proportionate” resilience measures, which must be documented in a resilience plan. The catalogue of measures includes, among others:
   - **Structural / Technical measures:** Security fencing, access control and separation systems, hardening of building structures, emergency power supply, detection and monitoring technologies.
   - **Organizational measures:** Crisis management structures, business continuity management (BCM), personnel vetting and review procedures.

4. **Incident Reporting (§ 18 KRITIS-DachG-E)**
   Incidents that could significantly impair the provision of a critical service must be reported immediately (within 24 hours) to the joint reporting office of BBK and BSI.

KRITIS regulation in Germany is fragmented and comprises numerous different legal provisions at both statutory and subordinate regulatory levels (see also the explanations regarding the structure of the NIS-2 Implementation Act). The following section provides an overview of the most important regulations, legal justifications and interpretative guidance for the utilities and supply sectors.

All versions of the **NIS-2 Implementation Act** and the **KRITIS Umbrella Act (KRITIS-DachG)** can be found in the section on draft legislation and explanatory memoranda below.

Standards

German Legislation

- NIS-2 Implementation Act
  - BSIG (Federal Office for Information Security Act)
  - EnWG (German Energy Industry Act), in particular §§ 5c - 5e EnWG)
  - TKG (German Telecommunications Act, in particular §§ 165 - 168 TKG)
- KRITIS Umbrella Act (see current status below)
- General Laws
  - AktG (German Stock Corporation Act, in particular § 93 AktG)
  - GmbHG (German Limited Liability Companies Act, in particular § 43 GmbhG)

German Subordinate Regulations

- BSI Critical Infrastructure Regulation
- IT Security Catalogues
  - Operators of energy networks
  - Operators of energy facilities
  - Operators of telecommunications infrastructures

European Laws and Regulations

- NIS2 Directive (Directive (EU) 2022/2555 of 14 December 2022)
- CER Directive (Directive (EU) 2022/2557 of 14 December 2022)
- Delegated Regulation (EU) 2023/2450 supplementing the CER Directive by establishing a list of essential services
- Delegated Regulation (EU) 2024/1366 – Network Code containing sector-specific rules for cybersecurity aspects of cross-border electricity flows
- Implementing Regulation (EU) 2024/2690 (specific requirements for ICT operators)
- Cyber Resilience Act (cybersecurity obligations primarily for manufacturers of products with digital elements)

Draft Standards / Legislative Explanations

NIS-2 Implementation Act (2025)

- Recommendation for a decision and report of the Committee on Internal Affairs of the German Bundestag (amendments made by the Bundestag to the Federal Government's draft law; status: 12 November 2025)

NIS-2

1. Objective of NIS-2

The primary objective is to ensure a high common level of cybersecurity across the European Union, particularly for critical and important organizations. In light of the increasing number of cyberattacks, the resilience of both the economy and the public sector is to be strengthened.

2. Expanded Scope of Application

NIS-2 applies to significantly more organizations than before. It distinguishes between two categories:

- **Essential Entities**
  e.g. energy, transport, healthcare, drinking water, digital infrastructure, public administration
- **Important Entities**
  e.g. postal and courier services, waste management, chemical industry, food production, IT service providers

The determining factors are generally sector and company size, rather than only whether an organization qualifies as "critical infrastructure".

3. Mandatory Security Measures

Affected organizations must implement specific technical and organizational measures, including:

- Risk management and security concepts
- Incident handling (detection, response and recovery)
- Backup and crisis management

What must companies implement under NIS-2?

The introduction of the Network and Information Security 2 (NIS-2) Directive introduces a wide range of new obligations and requirements for companies.

First, a company must classify itself within the relevant categories (e.g. "essential entity" or "important entity") and register with the Federal Office for Information Security (BSI) within three months after identification. Entities classified as "essential" must participate in the information exchange via the BSI's central exchange platform (BISP).

In addition to registration with the competent authority in the respective member state and the mandatory reporting of security incidents, companies must in particular address the new and stringent security requirements introduced by NIS-2.

1. Establish risk management as a cornerstone of NIS-2 compliance

A key element is NIS-2-compliant risk management for information security.

Companies classified as essential or important entities are required to implement appropriate and proportionate technical, operational and organizational measures to manage risks to the security of their network and information systems and to prevent or minimize the impact of security incidents. The NIS-2 Directive therefore also requires technical and organizational measures (TOM) in accordance with the so-called “state of the art”.

Through structured risk management, companies can identify potential threats and vulnerabilities in their network and information systems at an early stage. This includes both internal and external threats, such as cyberattacks, data breaches, system failures or human error.

Systematic risk management overall leads to increased resilience against threats and attacks.

By systematically analyzing and evaluating their risks, companies can implement targeted measures to reduce identified vulnerabilities. As a result, they are better prepared for potential attacks and are able to respond more quickly and effectively to security incidents. The outcome is reduced susceptibility to cyberattacks and an improved capability for defense and damage mitigation.

If this practice were implemented consistently across the board, it would create a coherent level of security capable of sustainably protecting and strengthening European infrastructure.

2. Ensuring information security standards in supply chains

Security within the supply chain is an important aspect of the NIS-2 requirements. Companies must ensure that their business partners and service providers also implement appropriate information security measures. This may be achieved, for example, through contractual agreements defining specific security requirements. Certifications also play an important role in demonstrating compliance with defined standards.

The TISAX® label has been a key requirement for suppliers in the automotive industry for several years. One of the objectives of this standard is to prevent malicious actors from gaining access to sensitive information – such as prototypes or customer data – of major automotive manufacturers through so-called supply chain attacks by targeting the information systems of suppliers.

Such attacks can cause significant economic and reputational damage. A standardized information security management system helps to systematically reduce such risks.

3. Reporting and properly handling security incidents

Companies that fall within the scope of NIS-2 as operators of critical infrastructure are required to promptly inform their national cybersecurity authority of significant disruptions, security incidents or threats affecting their critical services.

As part of the implementation of NIS-2, an effective security program with clearly defined policies and procedures for handling security incidents must also be implemented.

Information security management systems based on the ISO 27001 standard typically contain corresponding requirements. These include, in particular, processes for the rapid identification and handling of security incidents, for maintaining business operations during an incident, and for restoring systems after an emergency.

Companies must establish clear communication channels, escalation mechanisms and emergency plans in order to respond appropriately to security incidents. In addition, they are required – where necessary and possible – to inform the recipients of their services, i.e. their customers, about relevant incidents.

Further important obligations under the NIS-2 Directive

In accordance with the NIS-2 Directive, companies must comply with numerous additional obligations. The management of affected entities is required to oversee compliance with these requirements in accordance with the respective national implementing legislation. It should be noted that, in the event of violations, personal liability of the management may be considered under certain circumstances.

- **Policies**
  Companies must develop and implement binding policies for risk management and information security. These serve as a framework for handling cybersecurity risks and ensure that appropriate protective measures are implemented systematically.

- **Business Continuity Management**
  Operators must take appropriate measures within the framework of Business Continuity Management (BCM) to ensure the continuity of critical services even in the event of a cyber incident. This includes in particular backup strategies, crisis management structures, as well as restart and recovery plans.

- **Procurement and Purchasing**
  Security aspects must also be considered in the procurement of information and network systems. Companies must assess the security features and standards of purchased products and services to ensure that they comply with applicable security requirements.

- **Effectiveness and performance monitoring**
  Companies must implement measures to assess the effectiveness of their cybersecurity and risk management activities. This enables them to evaluate the impact of their security measures and make adjustments where necessary.

- **Training and awareness (“cybersecurity hygiene”)**
  NIS-2 requires employees to receive regular cybersecurity training. The term “cybersecurity hygiene” refers to basic behavioral practices that help minimize cyber risks. These include, for example, secure password management, the ability to recognize phishing emails, and the responsible handling of sensitive data and IT systems.

- **Cryptography**
  Companies must define policies for the use of encryption technologies and implement them wherever technically and organizationally feasible. Cryptographic measures serve to protect the confidentiality and integrity of information.

- **Human Resources**
  Appropriate measures must be taken to ensure personnel security. This includes, in particular, access controls, authorization concepts, and ensuring that only authorized personnel have access to sensitive systems and data.

- **Authentication**
  Appropriate authentication mechanisms should be used to ensure the confidentiality of information. These include in particular multi-factor authentication and, where appropriate, single sign-on solutions to secure access.

- **Communication**
  Encryption of voice, video and text communication represents an essential measure to ensure the confidentiality and integrity of communication content.

- **Emergency communication**
  Companies should also implement secured emergency communication systems to ensure reliable internal and external communication in crisis situations.

NIS-2 and European cooperation

A central element of NIS-2 is the strengthened cooperation among Member States in the field of cybersecurity. In doing so, the directive acknowledges the cross-border nature of cyber threats and calls for a coordinated European response to such risks.

The importance of NIS-2 is considerable in light of increasing cyber threats. Companies and organizations are expected to take appropriate measures to sustainably protect their networks and information.

Compliance with the NIS-2 Directive will become a priority for companies throughout Europe, as they must ensure that their security measures meet the strict requirements.

Implementation and outlook

The NIS-2 Directive was adopted on 14 December 2022 and must be transposed into national law by the member states. Once the national implementing provisions enter into force, the requirements will become binding.

The implementation and monitoring of NIS-2 standards represent a complex organizational and technical challenge for many companies and may require significant human and financial resources.

Our quality management system, including ESG and KRITIS elements, is audited annually by a qualified auditor from the accredited certification body Bureau Veritas. In addition, we have confirmed compliance with the Codes of Conduct of VDB, VDMA and ZVEI.

According to Section 289b (1) of the German Commercial Code (HGB), the SBF Group is not required to publish an ESG statement. Neither do the companies of the SBF Group qualify as large corporations within the meaning of Section 267 (3) HGB, nor does the SBF Group employ more than 500 employees.

Leipzig, 30.01.2026

Robert Stöcklinger
CEO
SBF AG
Zaucheweg 4, 04316 Leipzig, Germany
www.sbf-ag.com