PROTECTED AGAINST CYBERATTACKS

ENSURING THE PROVISION OF SERVICES ON CRITICAL INFRASTRUCTURE OF PORTS

05. November 2025

NIS2 DIRECTIVE

- The NIS2 Directive is an EU directive designed to improve the cybersecurity and resilience of critical infrastructures and digital service providers.
- It requires relevant companies and organizations to maintain an effective risk management system and to report serious or significant cyber incidents to the competent national authorities, which can then take the necessary measures.
- To minimize potential harm to users, the environment, and public order, the directive aims to identify security vulnerabilities early and take preventive action. To ensure that all parties meet the same high standards, companies are also responsible for ensuring the security of their entire supply chain and for passing the requirements on to their business partners and suppliers.
- The NIS2 Directive is strictly enforced, including high financial penalties for non-compliance or failure to meet reporting obligations. The amount of the fines depends on the classification of each company.
- The duty of care in the area of cybersecurity is non-negotiable, and top management is responsible for leading the implementation and monitoring of these cybersecurity measures.

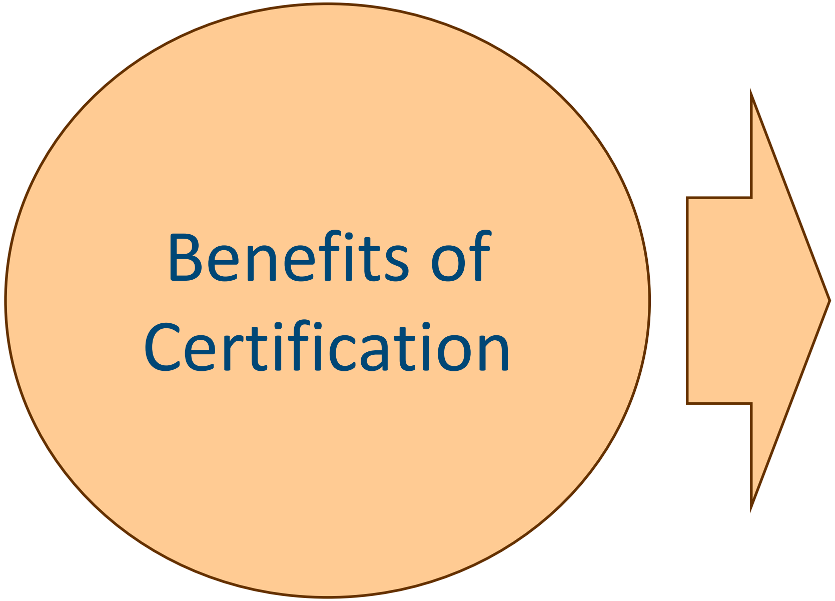
NIS2 DIRECTIVE

Further measures include, among others:

- Implementation of appropriate and proportionate security measures that comply with current standards and best practices to ensure the confidentiality, integrity, availability, and authenticity of their data and services.
- Development and regular updating of a Business Continuity Plan to enable the restoration of normal operations after a cyber incident.
- Introduction of multi-factor authentication for access to networks and information systems to prevent unauthorized access.

AUDIT ISO/IEC 27001

The certification an Information Security Management System demonstrates that you are committed to the proactive management and protection of your information and assets, while ensuring compliance with legal and regulatory requirements.



Benefits of Certification

- Confidentiality
- Heightened Awareness
- Proven Security
- Future-readiness
- Employee Awareness
- Integrity
- Technical Protection Against Fraud
- Competitive Advantage

AWARENESS TRAINING

Awareness training for employees is conducted to increase knowledge and awareness of information security, cyber risks, and organizational security policies.

Reasons for these trainings:

- Employees are often the weakest link in the security chain (e.g., phishing, social engineering).
- Increasing cyberattacks on organizations require trained personnel.
- Legal and regulatory requirements (e.g., ISO 27001, NIS2, GDPR) mandate security awareness and proof of training.

OBJECTIVES

- **Raise awareness of security risks**
  - Recognize phishing, malware, weak passwords, and social engineering attempts.
- **Promote secure behavior**
  - Correct use of passwords, devices, emails, and IT systems.
  - Proper handling of sensitive and confidential information.
- **Strengthen the organization’s security culture**
  - Employees understand their role and responsibility for information security.
- **Reduce security incidents**
  - Minimize human errors that could lead to data loss, system downtime, or compliance violations.
- **Ensure legal and regulatory compliance**
  - Provide evidence of awareness measures for auditors, regulators, or certification bodies.

BUSINESS CONTINUITY MANAGEMENT

- BCM is a systematic approach that ensures a company can maintain or quickly restore critical business process during disruption or crises.

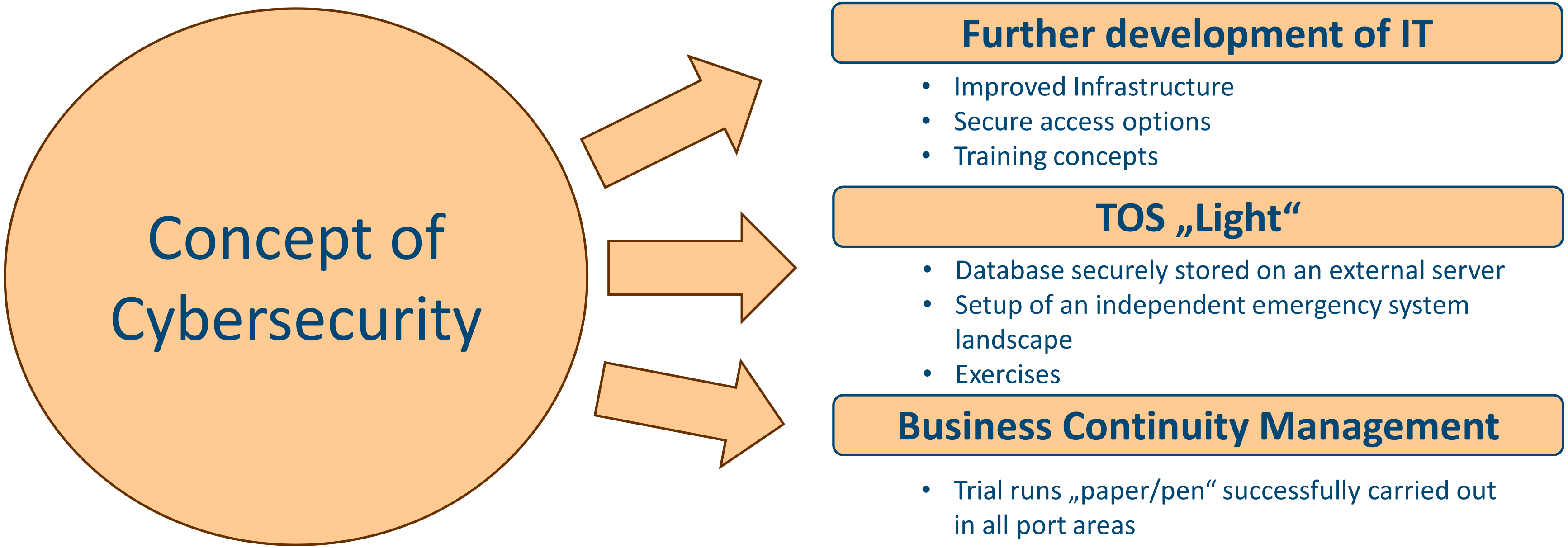
- It involves the planning, preparation, response and recovery of operations in the event of emergencies, outages or disasters - whether physical, technical or personal related.

- BCM ensures that a company remains operational during disruptions, reduces risks and can quickly recover.

OBJECTIVES OF BCM

- **Maintain critical business processes**
  - Ensure essential services and products remain available even during disruptions.
- **Minimize downtime and damage**
  - Reduce financial losses, reputational damage, and legal risks.
- **Risk awareness and management**
  - Identify and assess potential threats to the organization.
  - Develop strategies to mitigate these risks.
- **Rapid recovery after disruptions**
  - Implement emergency plans, backup systems, and recovery strategies.
- **Ensure legal and regulatory compliance**
  - Comply with standards such as ISO 22301 (BCM standard) or industry-specific regulations.

THE CHALLENGES RELATED TO CYBERSECURITY HAVE BEEN ADDRESSED AT VARIOUS LEVELS



Concept of Cybersecurity

Further development of IT

- Improved Infrastructure
- Secure access options
- Training concepts

TOS „Light“

- Database securely stored on an external server
- Setup of an independent emergency system landscape
- Exercises

Business Continuity Management

- Trial runs „paper/pen“ successfully carried out in all port areas
- Training of administrative staff

LHG
LÜBECKER
HAFEN-GESELLSCHAFT

A MEMBER OF
PORT OF LÜBECK

YOUR TRANSPORT.