FORTiT
SECURE DIGITAL BUSINESS

NIS 2 Directive:
Are your cybersecurity measures EU-compliant?

The EU's NIS 2 Directive (Network and Information Security Directive 2) entered into force in October 2024. It defines new cybersecurity requirements for essential and important entities. Swiss companies with business relationships in the EU or subsidiaries based there may be directly or indirectly affected.

We support you in analysing your **NIS 2 compliance** and act as a reliable partner for **implementing the required technical and organisational measures.**

For Swiss companies

Direct impact:

- Companies with operations in the EU that provide essential or important services must ensure compliance with NIS 2.

Indirect impact:

- Swiss suppliers providing essential services to the EU economy are subject to increased cybersecurity requirements.

Comparison with Swiss legislation:

- Switzerland is pursuing similar objectives through the revised Information Security Act (ISG) and the ICT Minimum Standard for critical infrastructures. However, there are differences, particularly regarding incident reporting obligations and sanctions.

Key requirements of the directive

Security measures and risk management

- Implementation of a risk-based security approach
- Regular penetration testing and vulnerability assessments
- Introduction of Zero Trust architectures[1]

Incident reporting obligations for serious security incidents

- Initial notification to the competent authorities within 24 hours
- Detailed report within 72 hours
- Final report including root-cause analysis within one month

Governance and responsibilities

- Executive management is directly responsible for cybersecurity; the board of directors has oversight
- Mandatory cybersecurity training for executives
- Stricter liability rules and fines

[1] NIS 2 does not explicitly mandate Zero Trust but includes several provisions that align with or support Zero Trust principles .

Act now to avoid regulatory risks

FortIT services – your added value

Compliance assessment: Holistic evaluation of your security posture across governance, risk management, security analysis and incident response planning.

Your added value: A prioritised action plan to close compliance gaps and strengthen your overall security level.

Risk management: Design and implementation of cyber risk and threat management, including modern SIEM and SOAR solutions for attack detection.

Your added value: Identify and reduce cyber risks. Detect and defend against attacks at an early stage.

Incident response & business continuity: Assessment of existing security measures against legal and regulatory requirements as well as leading standards.

Your added value: Improved resilience of your products and services, effective security controls and reliable implementation.

Supply chain security: Contractual definition of security requirements for third-party providers and implementation of third-party risk management (TPRM).

Your added value: Cyber-resilient supply chains and reduced external attack surfaces.

NIS 2 checklist

- Conduct a compliance analysis
- Implement risk management
- Introduce Zero Trust principles
- Establish an incident response plan
- Strengthen supply chain security
- Provide regular executive training

Rely on our expertise and experience for your NIS 2 compliance

- ✓ Extensive experience with regulatory requirements and internationally recognised standards
- ✓ Deep expertise in managing cyber and supply-chain risks
- ✓ Cross-industry experience in designing and implementing technical security measures

Contact us today!

FortIT AG
Badenerstrasse 281
8003 Zürich
fort-it.ch

Saner Çelebi
Partner
saner.celebi@fort-it.ch

Rolf Wagner
Partner
rolf.wagner@fort-it.ch