NIS2

With the advent of the NIS Directive2 , the planned revision of cybersecurity legislation focuses on the implementation of mandatory measures and strengthening mechanisms for responding to cybersecurity incidents, with the aim of improving the overall protection of digital infrastructure.

These changes will have an impact not only on organizations that already have to comply with the requirements of Act No. 181/2014 Coll. on Cyber Security and the related Decree No. 82/2018 Coll., but also many other entities that have not yet been included in the regulation and have not had to fulfil any obligations in this area.

The new Cybersecurity Act should come into force in October 2024. The Act will grant a one-year transition period to enable organizations to adapt to and gradually implement the new requirements.

We can help you implement NIS2 in three steps.
The NIS2 Directive brings significant changes to the field of cybersecurity. Following the decision to enshrine the Directive in national law, the framework of obligations set out in the document is being transposed into the national legislation through the new Cybersecurity Act and its decrees.

In particular, we can help you with the following areas:

Analysis of the current state of information security

We will analyse the current state of your organization with regard to cybersecurity. The analysis will include, in particular, an assessment of the information security management system, security documentation, asset management, risk management, vendor management, human resource management, change management and access management. As part of the analysis, we also assess the management of cybersecurity events and incidents and business continuity management.

Risk Analysis

We offer risk analysis to identify and assess potential threats and vulnerabilities associated with your organization's assets. This gives you a clear overview of the risks that could compromise your safety.

Drafting or revising security documentation

We will draft or revise documents with respect to your existing internal policies. Specifically, we can help you create an incident management plan, recovery plan, impact analysis, security guide for users, etc.

Training

To increase the security awareness of your employees (from regular users, security administrators to senior management), we offer training tailored to the needs of your organization. In addition to face-to-face sessions, the training can also be provided as e-learning using entertaining video courses, which end with a knowledge test.

Penetration testing

We will test your systems' ability to withstand cyber attacks. We will draw up a report describing any vulnerabilities and will suggest appropriate remediation measures to prevent real-world attacks.

Strengthening IT infrastructure security

We can help you identify weaknesses in the technical security of your internal network, and implement security technologies such as firewalls or EDR solutions that can identify, monitor and respond to suspicious activity on endpoint devices.

How can we help you with NIS2?

1

We define the requirements

Initial meetings with our consultant include identifying all the legal requirements that need to be met.

2

We assess the situation

We will conduct a thorough analysis of the current information security in place in your organization. We will assess the impact of the NIS2 Directive and recommend specific steps and measures to ensure full compliance with with all the requirements of the Directive or the Cybersecurity Act and related decrees.

3

We realize and implement

We will proactively help you to implement the proposed steps, including preparing the necessary documents and setting up a training plan for employees. We will work closely with you through the entire process.