Risk Analysis According to NIS2

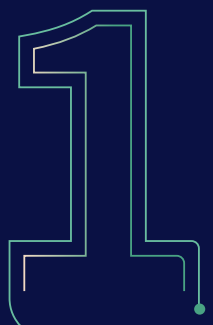
Athereon GRC

Athereon GRC

Risk Analysis According to **NIS2**

Step by step

The NIS2 Directive requires companies and organizations to implement appropriate and proportionate measures for information security risk management (Art. 21). The foundation is a systematic risk analysis. It enables you to identify threats and vulnerabilities, assess impact, and take appropriate protection measures.



Define context and scope

Before you can assess risks, it must be determined which systems, processes, and information are being considered. This includes defining the scope of the investigation: What IT systems, services, and data are relevant for performing business-critical tasks or legal obligations? NIS2 calls for all essential and important institutions to systematically record their critical dependencies.

Identify threats and vulnerabilities

Second step is to identify potential sources of danger: from cyber-attacks to technical failures to organizational flaws. It is equally important to document existing vulnerabilities that could facilitate attacks or disruptions. This step creates transparency across the entire risk environment.

Assess risks

The identified risks must be assessed according to their probability of occurrence and impact. The aim is to prioritize: What are the most significant risks to availability, integrity, confidentiality, or authenticity? NIS2 requires organizations to assess risks based on their potential operational and societal consequences.

Derive and implement measures

Technical and organizational measures (TOMs) are derived from the assessment. These include, for example, access controls, backup strategies, emergency plans, and employee awareness training. NIS2 requires these measures to be designed appropriately and in proportion to the risk situation.

Documentation and continuous review

All results of the risk analysis must be documented in a comprehensible manner. These include assumptions, evaluation criteria, decisions and measures taken. Because the threat situation and business environment are constantly changing, risk analysis is to be reviewed and updated regularly. NIS2 emphasizes the obligation to continuously adapt.

Conclusion

Risk analysis is at the heart of NIS2 risk management. It helps organizations to systematically address information security and demonstrably comply with legal requirements. Starting early creates a solid foundation for further security measures and, at the same time, increases the resilience of your own company.

Athereon GRC

Athereon GRC GmbH
Innovationsring 7-9
66115 Saarbrücken, Germany

grc@athereon.de

+49 681 9697 297

www.athereon.de/en