Risk Analysis

Information security assessment services are used to assess the current state of security and identify the risks to which your system is exposed. It is an important source of information for decision-making on security investments.

In this area we offer:

Analysis of the current state
Evaluation of compliance with the selected information security standard (e.g. ISO 27001) and identification of weaknesses and security gaps, including their prioritization in the given environment, suggestions and recommendations for eliminating the identified gaps.

IS Risk Analysis
Preparation of a methodology for an information security risk analysis or use of an existing one. Subsequently, according to the chosen methodology, comprehensive identification and evaluation of information security-related assets, identification and evaluation of information security threats, identification and evaluation of information security vulnerabilities. Assessment of the level of information security risks according to the methodology and support in risk management-related decision-making. Preparation of proposals for measures that can reduce risks to acceptable levels.

Draft Risk Management Plan
Design of safety measures/ recommendations including their timing in line with the company's capabilities.

Analyses are performed in accordance with ISO/IEC 27005, the Cybersecurity Act, or other methodologies chosen by the client.

When to perform a risk analysis?

An information system risk analysis is usually performed in the following cases:

- When there is the need to assess the current level of IS security.
- When there is the need to quantify the risks to which your information system is exposed.
- Following the decision to implement clearly defined rules for information security management.
- During implementation of the Information System Risk Analysis (ISMS).
- When required by auditors, shareholders or others.
- If the client requires evidence of the quality of your security.
- When there is a need to provide documentation for strategic decisions concerning the implementation of costly security measures.
- In accordance with the legislative requirements, such as the Cybersecurity Act.
- If you have serious doubts about the security of your information, for example, if you do not trust the third party managing your IS or if your company is targeted by an attack.

Solution Characteristics

- Backed by a strong team of analysts and technical consultants.
- Closely linked to technical security - we are able to include technical tests in the risk analysis.
- Use of a qualitative and quantitative approach to risk assessment.
- A wide range of software tools can be used.
- High degree of flexibility and openness to client requirements - we are able to adapt the methodology to the client's requirements or use their internal procedures.
- High degree of flexibility and openness to client requirements - we are able to adapt the methodology to the client's requirements or use their internal procedures.

Benefits

- Identifying priorities for further security investments and projects.
- Determining the optimal ratio between investment and the level of security achieved.
- Obtaining information on the level of IS security achieved from an independent party.
- Identifying risks and vulnerabilities that pose an immediate threat to the organization's core functions and assets.
- Preparation of documents for the creation of ICT security documentation in the organization.
- Identification of threats such as data leakage, abuse of privileges, human error, etc., including possible abuse scenarios.
- Implementing the proposed measures significantly boosts IS security.
- Obtaining the arguments to enforce the necessary security measures.

Simplified IS Risk Analysis Model