Information risk management

AEC

Information risk management services include an assessment of the current state of IS security, form an important basis for ensuring information and cyber security and serve as a basis for making decisions on security investments.

Another important part of this is ensuring compliance with shareholder, regulatory and client requirements.

In this area we can offer you:

- An analysis of the current state - rapid identification of weaknesses and security deficiencies, a proposal of recommendations to remove them.
- An IS risk analysis – a comprehensive identification of assets, threats and weak spots, a quantification of the risks the system is exposed to, support when making decisions on risk management.
- The proposal of a risk management plan – proposed security measures/recommendations.
- Specialised audits/analyses focused on a specific area.

AEC implements IS analyses and audits based on the bountiful experience gained during its long-term work in the ICT security market and in line with recognised standards:

- ISO 31000 Risk Management,
- The ISO/IEC 27000 series of standards focused on security management,
- Our methodology can be tailor-made to the requirements of the client or the legislation (e.g. the Act on Cyber Security).

aec-security.eu

Information risk management

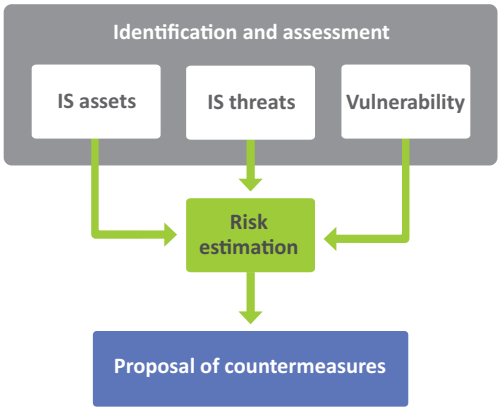
When to do a risk analysis?

Information system risk analysis is typically made in the following situations:

- There is a need to determine the current state of IS security.
- It is necessary to quantify the risks your information system is exposed to.
- A decision has been taken about the need to manage information security according to clearly defined rules.
- You want to set up an information security management system (ISMS).
- There is a requirement by auditing firms, shareholders, etc.
- You need a basis for making decisions about implementing costly security measures.
- It concerns a legislative requirement (e.g., the Act on Cyber Security).
- In the event of serious doubts about the security of information (lack of trust in the third party that manages your IS, your company has been the target of an attack, etc.).

Among the main benefits of information risk management services are:

- Determining the priorities for further security investments and projects;
- ascertaining the optimum balance between investment and the level of security achieved;
- obtaining information on the level of IS security achieved from an independent party;
- identifying risks and weak spots that pose an immediate threat to the organisation's key functions and assets;
- creating the basis for compiling the organisation's ICT security documentation;
- identifying threats such as data leakage, abuse of privileges, human error, etc., including possible abuse scenarios;
- a significant increase in IS security by implementing the proposed measures;
- attaining arguments for management decisions on the allocation of investments into IS security.



Simplified model of IS Risk Analysis

Our strengths

AEC uses its long-term experience in building information security management systems and carrying out the tasks associated with them.

Our solutions are characterised by:

- a strong team of analysts and technical consultants;
- a close tie to technical security - we are able to include technical tests in our risk analysis;
- the use of both qualitative and quantitative approaches to risk assessment;
- support for the analysis process by using our own software tool;
- a great deal of flexibility and openness to customer requirements - we can adapt the methodology to the client's requirements or use their internal procedures.

Prague – AEC a.s., Voctářova 20a, 180 00 Praha 8, tel: +420 226 229 133
Brno – AEC a.s., Veveří 102, 616 00 Brno, tel: +420 541 235 466
Bratislava – AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283