



CyberWehr

RISK MANAGEMENT SOLUTIONS GMBH

Monika Wehr ▪ +41 79 348 55 63 ▪ 8803 Rüschlikon, Alte Landstrasse 109

---

## The risk analysis ISO 27001/2, 31000 - the most important step to avoid risks

### Initial situation

Both laws, the revised Swiss Data Protection Act as well as the EU GDPR, must not only be implemented in a compliant manner, but also appropriately, i.e., with a **risk-based approach tailored to the individual framework conditions** of the company.

With the progress of electronic data processing technologies and the emergence of ever greater volumes of personal data, the question arises as to how the **consequences of technologization on the personal rights of the data subjects** can be systematically analyzed and appropriate action measures taken.

Data protection sees only those risks in the risk analysis that have an influence on natural persons. A risk is also defined in data privacy as the multiplication of the damage by the probability of occurrence. In the case of data privacy risks, the damage relates to the person.

A vulnerability in your IT infrastructure is only a problem if it can be exploited by hackers. It allows data protection security objectives to be violated if, for example, security measures are missing, or a threat is not fully covered. Vulnerabilities can also occur in security measures themselves, e.g., through faulty software updates. They represent a deficit in the principles of data protection implementation.

We conduct an independent risk analysis that protects all your data and holistically covers your data protection strategy, IT infrastructure, organization, and legal compliance. This is the only way to uncover potential dangers: it includes the identification and correlation of risks, the analysis of their causes, their probability of occurrence, their frequency, the evaluation of risks and suitable measures for risk mitigation. In this way, risks become controllable and manageable.

### Privacy Impact Assessment (PIA)

With the PIA, projects that "appear" to be particularly risky are subjected to a special risk assessment and only approved for data processing if the result of the assessment is positive. In addition, measures to reduce and avoid risks are also taken and implemented.

When is a risk relevant for a PIA at all?

- **processing of data that is particularly worthy of protection**, especially in the **health sector** with a high risk to the rights and freedoms of natural persons"
- **Profiling**: the usable creation of the overall image of a personality for specific purposes, e.g. for job placement or in the search for offenders
- **automated individual decisions in data processing**
- **Video surveillance**

Please note that in the above cases the risk analysis is mandatory by law!