

Information Security Management

Everyone talks about information security. What is this exactly? With the world-wide networking of companies, locations, countries and even continents not only do opportunities arise, but also risks. With increasing complexity and the abstraction of the structures, the electronic business world has become very susceptible to external as well as internal threats. The countermeasures are usually badly coordinated isolated solutions which fight the symptoms but not their causes. This is where we come in. Through our holistic approach, we create a clear increase in value, particularly for smaller and medium-size enterprises. With "holistic", we mean that not only is the enterprise IT examined, but also the physical environment as well as the organizational imbedding and the documentation as a whole.

In our practice-oriented philosophy we recognized that a profit-oriented enterprise can afford only a very limited measure of bureaucracy these days. Accordingly, our terminology such as: cost optimization, high security posture, individual security needs, ease-of-use, flexibility and expandability are at the forefront. This makes the management of information security not only simple, but also "livable" – Quality, not quantity!

Examples:

"The executive committee has to establish suitable measures; in particular, implement a monitoring system, whereas the enterprise can detect endangering developments early to ensure business continuity (§91 Abs.2 AktG)".

Operating a business without risks is not possible. The law as a check and transparency in publicly traded enterprises (KonTraG) has, due to the change of the §91 AktG (which is also applied to private corporations), the obligation of the executive committee to provide for an appropriate risk management and for an appropriate internal revision – explicitly formulated and accordingly described two important attributes of an Information Security Management System. Usually, the information security function is delegated to qualified coworkers. However, the responsibility remains strictly with the management.



The measurable benefits

- ✓ Sensibilization for Security Deficits
- ✓ Risk Analysis of the Business Processes
- ✓ Increase of the Security Posture
- ✓ Cost Savings through Centralization of Security Protection Measures

The Steps to Information Security

Security Checks

With our "Security Checks", security relevant areas are analyzed for weaknesses and vulnerabilities and if necessary, possible solutions provided. Since we view information security with a holistic approach, topics that are only indirectly related to IT such as building design and the organizational aspect are also considered. Accordingly, relevant topics that not only deal with computers and networks, but also the facility security or emergency plans are addressed.

Security Certification

With quality management today, it is common practice that enterprises certify their processes according to ISO Standards. There are also standardized certification possibilities for security management, for example the ISO standard 27001 with the introduction of a systematic management of information security in enterprises. With the implementation our introduction seminars assist whereas the structures and procedures of the ISO standard 27001 are described. This is especially recommended for those enterprises striving to certify to ISO Standard 27001.

Security Training

With "Security Training" we offer training and further development in the area of information security. Among the attendants are security officers and security managers or interested newcomers in this field. Hence, the development and maintenance of a comprehensive information security program is an enterprise-wide process.

Upon request, general security topics can be addressed to assist in the understanding thereof. Upon completion of these seminars, the participants will have the ability to develop an information security management system, prepare for a future certification and to maintain it. Additional "Security Training" main topics are from employee coaching for enterprises that do not wish to attain this security know-how in their own company up to moderation of security workshops where risk analyses or security concepts are developed.

