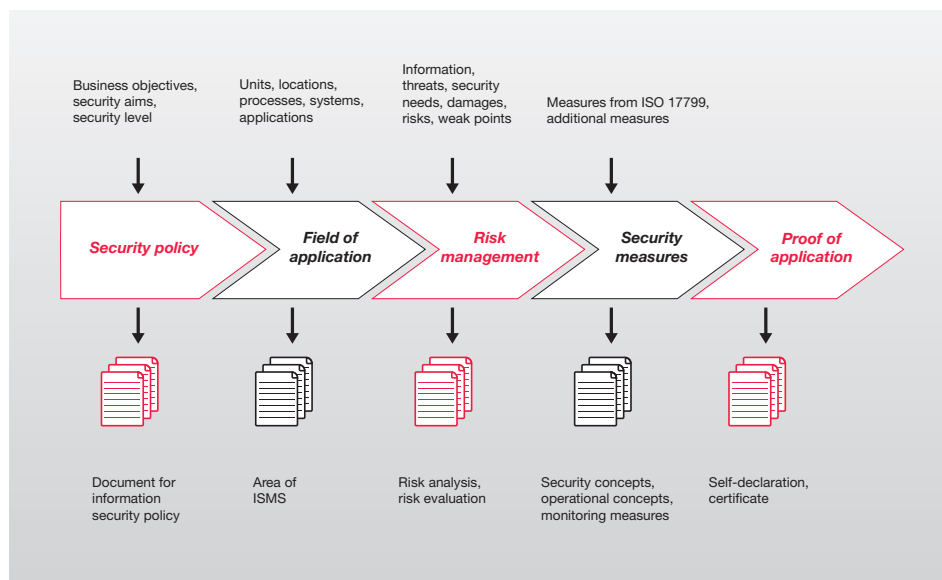


Holistic Security Concepts According to ISO 27001



Benefits:

- » Target-orientated measures resulting from expert knowledge
- » Excellent cost-benefit ratio
- » Holistic concept for comprehensive security

Information is a critical resource in companies. Protecting it from unauthorised disclosure, modification or loss has become more important than ever. A company's security measures can only be effective if they are part of an overall information security concept. At the same time, it must be ensured that legal requirements are met, e.g. in terms of data protection or corporate risk management. **secunet has extensive experience in setting up holistic information security management systems according to ISO 27001.** The consulting we provide takes your individual needs and specific requirements into consideration.

Do you know your requirements?

Identifying a company's requirements and demands is a key factor in developing a company-specific security strategy. What are the requirements in terms of confidentiality, integrity and availability of information? How can the information available in the company be classified in terms of sensitivity? Which processes and IT systems are mission-critical? Which IT security measures have you implemented so far and how can your security situation be rated in comparison with best practices in other companies?

On the basis of an analysis of your current situation, we define your security requirements together with you and devise your IT security strategy.

Defining corporate standards

Attempts to ensure IT security by means of one-off measures often results in a collection of different, possibly redundant, security mechanisms. This is inefficient and even leads to security problems since an isolated view of individual aspects prevents the development of the big picture of fundamental issues that apply on a corporate-wide basis.

Therefore, it is advisable to define uniform standards at a higher level which are binding for all individual projects and which ensure an end-to-end, holistic security level. One internationally recognised way to fulfil these requirements is to set up an information security management system (ISMS) which is certified according to the ISO 27001 standard.

Assessing the risks

For IT security to be cost-effective, the measures must be geared towards those risks which actually threaten your company. Our experts identify possible threat and damage scenarios by means of a risk analysis and assess them in terms of their effects and the likelihood of their occurrence. We use proven methodologies and tools in such assessments.

Defining measures

The choice of measures for raising the IT security level is especially critical. They must

- be cost-efficient and future-proof,
- comply with the higher-level security strategy,
- reinforce security awareness and
- fit into the corporate context.

Further measures are necessary as a result of modern working practices, e.g. the need for mobility, permanent availability and dynamic data interchange. Our experts are familiar with all of today's security solutions and products from numerous projects and are ready for any challenge which may arise.

Meeting industry-specific requirements

IT security management does not only have to prevent financial damage. Compliance with pertinent legislation is an important objective for which management is personally responsible.

Backed by our comprehensive industry-specific know-how, we can outline the requirements relevant for your organisation and how to ensure compliance in an efficient way. Our security documentation helps you to provide proof of compliance vis-à-vis third parties (e.g. authorities).

Certifying security

After an ISMS has been established, it is possible to apply for certification according to the ISO 27001 standard. Once all prerequisites have been met, we offer you certification of your IT system through one of our ISO 27001 auditors. This internationally recognised certificate allows you to prove that you have an operational ISMS at your disposal, furnishing you with one of the most valuable security seals available today. This shows that the issue of IT security is a top priority for you.

If you are not sure whether you meet all the prerequisites for certification, we additionally offer the opportunity to conduct a preliminary audit. The procedure is comparable to that of a live audit, however without the direct involvement of the certification.

Getting the security process underway

Security concepts must be adapted, extended and updated on an on-going basis as a result of the further development of an organisation and its IT, but also as a result of external influences such as new attack patterns, technological progress or new legislation. This only works if security is implemented in the company as a clearly defined process with responsibilities and process models.

We support you at every stage of this process:

- Selection and specification of scope of the IT system under consideration
- Determination of protection requirements
- Risk analysis
- Definition of measures
- Implementation
- Certification



It is our guiding principle to pursue an appropriate, purpose-orientated course of action; and to do so in a way that achieves the optimum level of protection for you through continuously improved IT security.

More information:
www.secunet.com/en/isms