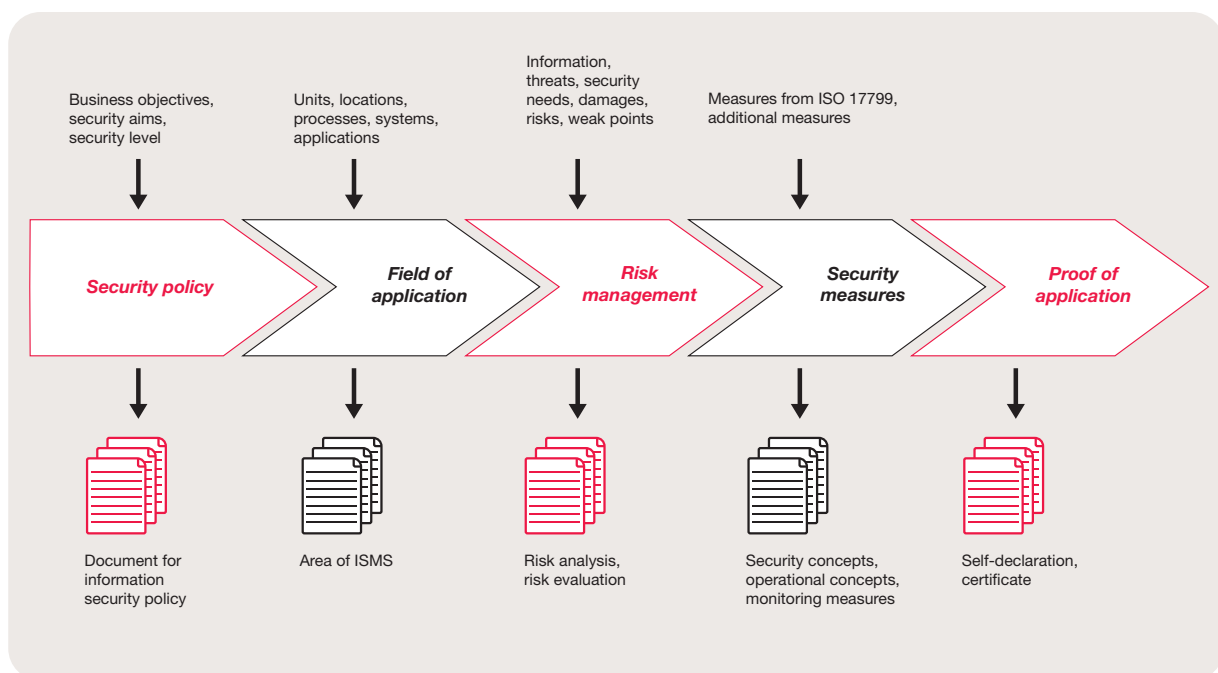


secunet

Security Management

End-to-end security concept for holistic protection



Information is a critical resource in companies. Therefore, protecting information from unauthorised disclosure, modification or loss has become crucial. Security measures can only be effective if they are part of a corporate information security concept that implements legal requirements concerning corporate risk management.

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.

Your advantages:

- High level of security due to end-to-end, holistic concept
- Effective measures due to expert know-how
- Excellent cost/performance ratio

Defining corporate standards

If security issues are defined individually for each project, this often results in uncontrolled growth of non-homogeneous and sometimes 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 corporate level which are binding for all individual projects and which implement an end-to-end, holistic security level.

Standards such as ISO 17799 or the "IT-Grundschutz" manual of the German Federal Office for Information Security which has been used in the development of standard ISO 27001 together with the comprehensive experience of our consultants in hands-on projects can provide valuable assistance in such a definition.

Assessing the risks

For IT security to be cost-effective, the measures must be geared towards those risks which actually threaten your company. Threat and damage scenarios must be identified by means of a risk analysis and assessed in terms of their effects and the likelihood of their occurrence. secunet uses proven methodologies and tools in such assessments.

Defining measures

We provide our customers with comprehensive support in defining suitable security measures and selecting the appropriate technologies and architectures. Our experts are familiar with all current security solutions and products from numerous projects. However, the implementation is not just a matter of technology. Organisational rules and the development of a security awareness of your staff are just as important.

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).

Getting the security process underway

Security concepts must be adapted, extended and updated on an ongoing 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.

secunet supports you all along the way from the concept to the implementation in your organisation and a possible certification according to ISO 27001.

Benefit from our hands-on experience

Each organisation has its own security culture, but the challenges are comparable for many companies. secunet has provided effective support and consultancy for medium-sized companies and global players such as the Allianz Group and BMW alike. Our security consultants are backed by comprehensive industry-specific experience, e.g. in the financial, telecommunication and automotive sectors.

And not only are we familiar with the requirements of the private sector, but also with those of the public sector. In this field, we closely cooperate with the German Federal Office for Information Security where we provided major support for the Centre of Competence for Data Security for the BundOnline2005 Initiative.

secunet Security Networks AG

IT security and its trend-setting usage is the core competence of secunet Security Networks AG. The development and implementation of IT security solutions for sensitive data turn secunet into a specialist in great demand. Excellent technological understanding is reflected in our consulting services and modulated products. Progressive digitalization of processes and communication channels of all kind pose new challenges for secunet day-to-day. Due to our large know-how we set standards in the IT security market. Our extensive clientele comprises national and international companies and affiliated groups as well as the public sector. About 230 highly qualified and experienced employees at seven branch offices in Germany as well as at further offices in subsidiaries in Switzerland and the Czech Republic are engaged in the creation of innovations, the optimal settlement of projects and our twenty-four-seven support.

Editor:

secunet

secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen, Germany
Phone: +49 - 201 - 54 54 - 0
Fax: +49 - 201 - 54 54 - 123
E-mail: info@secunet.com
www.secunet.com