
Angelika Jaschob • Lydia Tsintsifa

Bundesamt für Sicherheit in der Informationstechnik
{angelika.jaschob | lydia.tsintsifa}@bsi.bund.de

Abstract

Using the pragmatic two-tier risk assessment and management approach of IT-Grundschutz helps organisations to optimise the efforts for the IT security management process as well as to achieve the requirements of ISO/IEC 27001.

1 Need for an Information Security Management Method

Along with the increasing importance of compliance, the use and implementation of recognised and well-structured methods for IT security has now become more important than ever in business. The decision of ISO/IEC to develop an entire series of information security standards – the ISO/IEC 27000 family – reflects the increasing importance of information security. The ISO/IEC 27001 standard specifies requirements for the design and implementation of an appropriate Information Security Management System (ISMS) in an organisation, ensuring that adequate and proportionate controls are selected to protect information assets and to give confidence to interested parties.

Complementary to the controls defined in ISO/IEC 17799:2005, ISO/IEC 27001 gives the specification for the certification of an ISMS. However, both standards contain generic controls, described on a high abstraction level and do not include a specific method for risk assessment. The Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) in Germany provides via IT-Grundschutz ([BSI1], [BSI2], [BSI3], [BSI6]) a method to implement these high level controls in a practical and efficient way. Furthermore, the IT-Grundschutz Methodology can be applied to establish, maintain and monitor an ISMS. Part of this is the performance of a risk analysis for the IT assets in focus.

2 Optimising resources

One of the primary objectives of IT-Grundschutz is to increase the efficiency within the IT security process. Examining the cost-benefit trade-off of IT security one conclusion is, that the higher the IT security level is, the more hard and expensive it becomes to increase it respectively. Figure 1 illustrates this effect and demonstrates why it is not possible to achieve perfect IT security.
Figure 1: Cost-benefit trade-off for IT security

IT-Grundschutz takes into account this cost-benefit relation of IT security and first provides the means to reach a standard IT security level by using the framework concept.

2.1 The IT-Grundschutz concept

The main idea here of IT-Grundschutz is to break an information security management system down into reusable components, representing the basic elements in information security management. On this basis, an easily extensible standard system, that is adaptable to a particular case, can be created. The IT-Grundschutz Catalogues ([BSIC], [BSIM]) build thus a repository of characteristic threat scenarios and standard security measures for typical IT environments. Threats and countermeasures concerning one specific aspect of information security are grouped in "modules". Some IT-Grundschutz modules address higher level issues in information security, like "organisational aspects", "contingency planning" or "outsourcing" whereas other modules deal with technical topics like "Windows 2000 Server", "WWW-Server", "Mobile Telephones" or "Databases".

The modules also reflect typical areas in which IT assets are employed, for example client/server networks, buildings, communications and application components. Every module begins with a description of the typical threats which may be expected in the given area together with their assumed probability of occurrence.

The IT-Grundschutz modules build the fundament for developing an IT security concept based on the IT-Grundschutz methodology. They can be used in their original form or can be appropriately adapted. There is here some commonality between such a concept for IT secu-