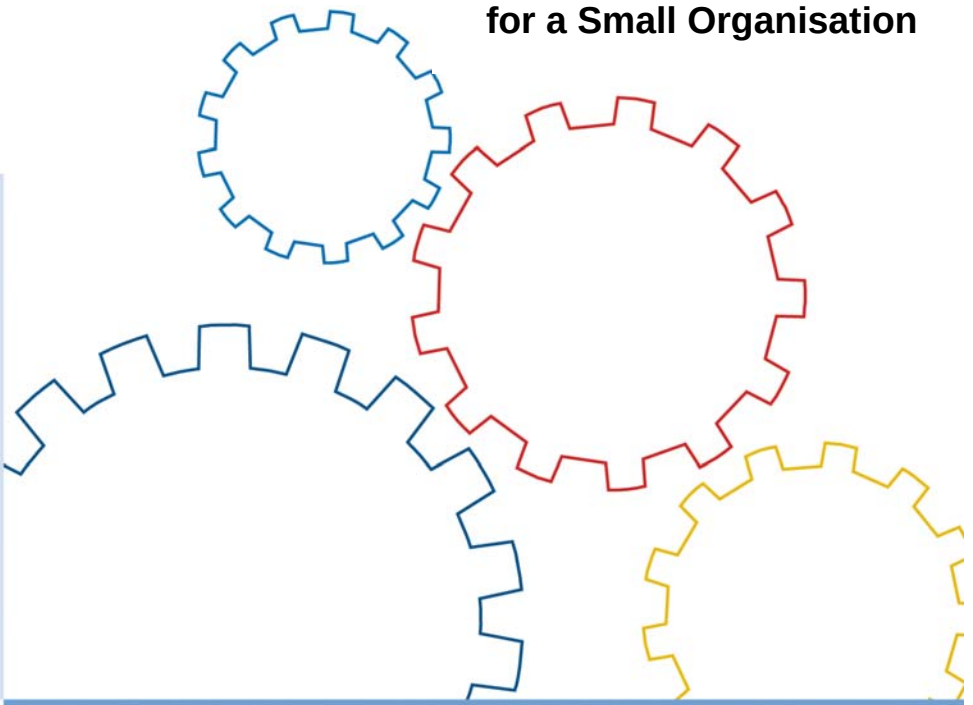
Bundesamt
für Sicherheit in der
Informationstechnik

IT-Grundschutz-Profile

An IT-Grundschutz-Profile for a Small Organisation



www.bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik
Referat 114 IT-Sicherheitsmanagement, Grundschutz
Postfach 20 03 63
53133 Bonn
Tel: +49 (0) 228 99 9582-0
E-mail: gshb@bsi.bund.de
Internet: www.bsi.bund.de

Contents

1 Introduction

Have you ever had problems with computer viruses?

Do you store confidential or personal customer, client or patient data on your PCs?

Have you ever lost data for good? Do you or your employees have Internet access in the office?

If you answered one of these questions with "Yes", we strongly advise you to concern yourself with the subject of Information Security. In today`s information society, computers are used in nearly every work environment. Craftsmen, doctors, solicitors and tax advisors alike use PCs and additional information technology (IT) in their offices. Often, highly sensitive company data are processed that have to be protected.

The IT Security Guidelines [SECGUIDE] provide an introduction into the 50 most important standard security safeguards. A summary of legal provisions relating to IT security, a comprehensive glossary containing the most important technical terms and a description of typical mistakes should help you to tackle the subject of IT security systematically.

This document provides you with an example of how to develop an IT security concept in your company or public authority systematically. You will learn about concrete security aspects to be taken into account when using information technology in a small organisation. Based on a sample organisation with only a few employees, we show you how to apply the corresponding work steps of the IT-Grundschutz methodology appropriately.

Examples for typical small organisations are doctors' practices, lawyers' offices, tax advisors' offices, small workshops, small public agencies, travel agencies or hotels. Without information and communications technology, work in these professions is almost inconceivable.

1.1 The BSI series of Standards for IT Security Management

An organisation needs to pay attention to many different aspects to fulfil all security requirements. To help you to establish appropriate processes for this, the BSI has outlined an efficient and tested methodology in BSI-Standard 100-2. The key security safeguards are listed in the BSI IT-Grundschutz Catalogues as Best Practices to support you.

The German Federal Agency for IT Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) outlines a systematic methodology for setting up IT security concepts. The series of publications and standards for various areas of information security includes the following BSI-Standards for IT security management:

- BSI-Standard 100-1: Information Security Management Systems (ISMS)
- BSI-Standard 100-2: IT-Grundschutz Methodology
- BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz

The current versions of the BSI-Standards and IT-Grundschutz Catalogues are available on the Internet for review and download at http://www.bsi.bund.de/english/gshb/index.htm.

1.2 The IT-Grundschutz Catalogues

One of the most challenging tasks of IT security officers is to keep an overview of the business processes to be protected and the related information technology. Adequate security measures must be identified and implemented. For this purpose, BSI offers IT-Grundschutz as a simple method. BSI-Standard 100-2 describes the IT-Grundschutz Methodology, i.e. how to set up and pursue information security management in practice.

The IT-Grundschutz Catalogues are more comprehensive and include collections of threat and safeguard descriptions for various topics. They are categorised according to modules.

One of the main aims of IT-Grundschutz is to reduce the efforts within the IT security process by combining and disseminating known procedures for enhancing information security. Therefore the IT-Grundschutz Catalogues contain standard threats and safeguards for typical business processes and IT systems which can be applied to the own institution as needed. The main focus of Grundschutz is to achieve adequate security for all information of an institution.

The IT-Grundschutz Catalogues not only explain *what* should be done; they also provide very specific information on *how* this can be implemented. Proceeding in accordance with IT-Grundschutz is therefore a proven and efficient way to fulfil all the requirements of the ISO-Standards.

In the course of this document we will illustrate various risks in handling information security and outline any countermeasures using the example of Mr. Adams.

The examples in this document are highlighted with a grey background and a border.

Mr. Adams has a small family business with 3 employees, Miss Burke (a secretary) who works half-time, and two field workers who spend their days working onsite at customers of the family business. Mr. Adams himself is responsible for the acquisition of new customers. He attends to his customers and takes care of smaller details as well as special requests made by the customers at short notice.

The customers appreciate this service and readily recommend the small business to family and friends. A good reputation is therefore very important for this business and in the long term secures the customer base.

Mr. Adams admits that he doesn't have a clue about computers, although he uses PCs and a laptop for various purposes in the company to maintain the customer database, to set up quotes, to write invoices and for online banking via the Internet, to name only a few tasks which are handled using computers.

Mrs. Adams has made herself somewhat familiar with how to work with PCs and networks and has attended an evening course on the subject. Every now and then she helps out in the business and is in particular responsible for PC maintenance.

This document contains mnemonics and instructions. These are highlighted by a double border.

References to other documents are provided in abbreviated form in square brackets (e.g. [GSK]). The detailed references to the relevant literature can be found in Appendix B using these abbreviations.

2 General Conditions of the IT-Grundschutz-Profile for a Small Set of IT Assets

2.1 Definition of protection requirements

What are the key business processes in your organisation?

Do you know which data within your organisation are so important that loss or disclosure could entail the violation of a law, a contract or a regulation?

What importance do you attribute to your customer data?

How long will you be able to work without problems in the event of a computer or hard disk failure or if you have no Internet access or cannot use your telephone?

You first need to answer these important questions for yourself if you wish to base the security of your information technology on IT-Grundschutz.

The customer file on Mr. Adams's PC not only stores all transactions relating to completed orders but also confidential information which might be useful in the preparation of new quotes.

Mr. Connelly, a competitor who is not quite as successful as Mr. Adams, would love to know his secrets. For this reason he asks a friend, a computer science student, to develop malicious software - so-called malware - which he appends to a harmless small computer game. He then sends this modified computer game to Miss Burke. The malware takes advantage of vulnerabilities in PC operating systems in order to gain access to these computers' hard disks via the Internet.

Once Miss Burke starts the game, the malware is released. It opens a backdoor in the computers so that Mr. Connelly can access Mr. Adams's computers via the Internet.

Since Mrs. Adams has not updated the operating systems and the various programs installed to keep the computers free from malicious programs (virus scanner, firewall, etc.) for quite some time, the malware can spread and Mr.Connelly is then free to access the hard disks and thus Mr. Adams's data.

Among the data, Mr. Connelly also finds documents that were set up in preparation for a call for tenders in which he also wants to participate. The data found here provides Mr. Connelly with enough information to understand Mr. Adams's calculation thus allowing him to make a comparable quote for a lower price.

In this example, the fundamental value of "confidentiality" was violated because Mr. Connelly was able to gain access to Mr. Adams's internal information.

Confidentiality means that data and information may exclusively be **read** by authorised persons.

In addition to confidentiality, the fundamental values of "integrity" and "availability" play an important role.

Integrity refers to the fact that the correctness (intactness) of data is ensured and that data may only be modified by authorised persons.
Availability means that data, information and systems are available to users as required.

Imagine the consequences if unauthorised persons accessed your data or the systems you need to work with during the day were not available. Or if data you need to edit were modified or deleted.

Each managing director should be aware of the serious consequences for an organisation if unauthorised persons gained access to confidential data. The methodology of standard security safeguards recommended by the BSI-Standard enables you to select measures from the IT-Grundschutz Catalogues to improve IT security in your organisation.

2.2 Responsibility

Do you know who is responsible for security incidents in your organisation?

Which tasks need to be performed by the head of a small organisation him/herself and in which activities is he/she intensively involved in order to protect the organisation?

The head of an organisation has the following responsibilities:

- to set up a security policy (see Section 4.1 and the sample security policy in Section 11.1);
- to perform a risk analysis based on the assessment of protection requirements (see Chapter 6 and Section 11.4);
- to complete a PC passport (or have one completed) for each individual system (see Section 11.2); if this is done by an employee the passport must be checked for correctness and completeness afterwards by the head of the organisation;
- to implement relevant security safeguards in the organisation (in Chapter 8 we provide examples relevant for a small set of IT assets), and
- to document all transactions and measures (see also the checklists in Section 11.6).

In small organisations it is the head of the company or public authority him/herself who is responsible for all relevant issues. Especially when it comes to the issue of IT security, the head of a small organisation hardly has a possibility to delegate responsibility to employees. For this reason he/she needs to deal with the issue of security of the business processes implemented in the organisation.

3 Defining the IT Assets

As a managing director, how do you describe your IT assets?

What relevant business processes exist in your organisation?

What IT systems exist in your organisation?

At the weekend Mr. Adams has time to relax. He then often comes up with improvements for his company which he would like to put into practice immediately. He is still frustrated about the fact that Mr. Connelly managed to offer a lower price than his in the call for tenders. To be better protected in the future he has asked his wife to check and update the operating systems of all computers installed in the company. Unfortunately, Mrs. Adams became ill last week and therefore was not able to perform the scheduled operating system updates. Since only Mrs. Adams knows exactly which systems exist at all, where these are located and how they are configured and interconnected, nobody can step in for her and perform the planned modifications.

After her recovery, Mr. Adams asks her to prepare a summary of all relevant systems and how they are interconnected. This way, he can fall back on this list and have the modifications performed by a service provider if Mrs. Adams is not available.

This section describes the organisation's IT assets from the point of view of the head of the company or public authority. The IT assets from the point of view of the BSI-Standards are described in Chapter 5 (Structure Analysis).

In accordance with BSI-Standard 100-2 the term "IT assets" covers all infrastructural, organisational, personnel and technical components which assist with the performance of tasks in a particular area in which information processing is applied.

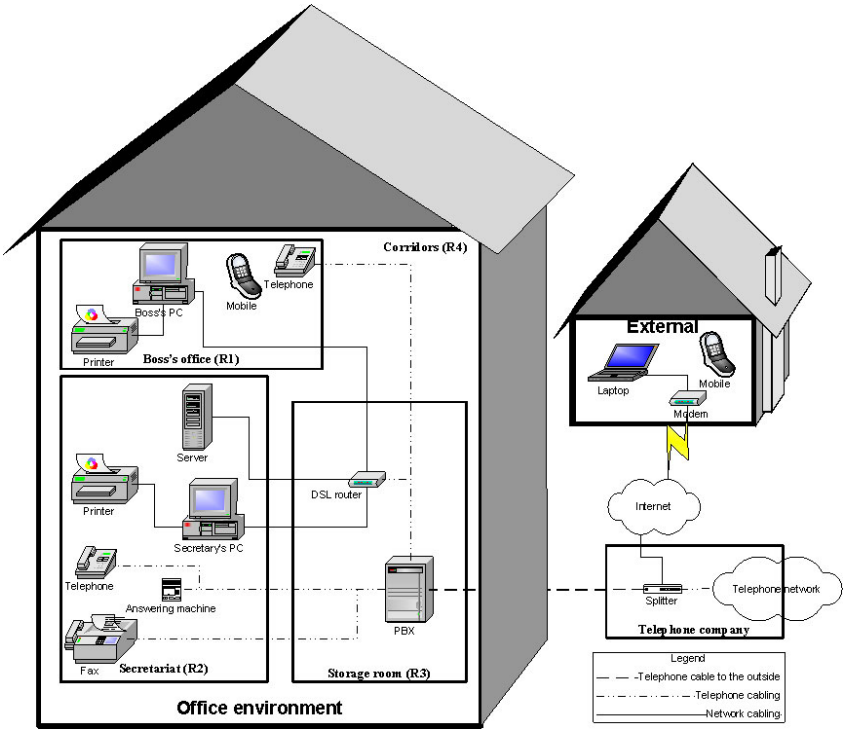


Figure 1: Small set of IT assets

Figure 1 shows the set of IT assets on which this document is based. The office environment of the organisation shown here consists of various offices, rooms and areas (R1-R4). When the laptop is in the office environment it is in the boss's office (R1).

In which rooms are the individual devices and systems located?

- **Boss's office (R1):** Boss's PC, printer, telephone, laptop, mobile phone.
- **Secretariat (R2):** Secretary's PC, printer, telephone, fax machine, answering machine, server.
- **Storage room (R3):** Telephone system, DSL router including firewall.

- **Connecting rooms (R4, e.g. corridors):** Parts of the cabling

  These rooms are not public and only accessible via the corridor.

What IT systems are installed?

The head of the organisation's workstation PC (**Boss's PC**) runs under Windows 2003 and the **secretary's PC** under Windows 2000, with a similar configuration and identical applications. The **server** runs under Windows 2000 and is used for centralized data storage for various applications. All **telephones**, the **fax,** , the **answering machine** and the **DSL router** are connected to the **telephone system** (PBX). The **laptop** runs under Windows 2000 and is equipped with a modem. The **DSL router'**s firewall uses a manufacturer-specific operating system. The **mobile phone** is a mobile IT system which the head of the organisation carries around with him.

What computer programs are used?

In addition to a special program to support the organisation's business process, Microsoft Office 2000 is used.

Each employee can access all hard disks and print on each printer.

What (communication) lines are used for data transfer?

The communication lines (IT connections) consist of the internal cabling and the external connection to the Internet and the telephone network.

Application of the IT-Grundschutz-Profile

What parallels to your own office can you see?

How can you benefit from the IT-Grundschutz measures described in this document (see Chapter 8) in your specific environment?

Having recovered, Mrs. Adams has produced the requested systems summary and now compares the list provided in this document with the sample set of IT assets provided by the BSI. She notices that they still use an old PC running under Windows 95 and not a single one with Windows XP.

A comprehensive IT security design is set up based on the organisation described in this document. This example need not necessarily correspond completely with the situation in your company or public authority. It is rather meant to serve as a template to which you can make minor changes without much effort.

Examine the extent to which the described set of IT assets corresponds with the situation in your organisation. Should there be major differences between your IT structure and the one described here we recommend that you use a different IT-Grundschutz-Profile, for example the company profiles for medium-sized or large set of IT assets (see [GSPROF1] or [GSPROF2]).

4 Security Policy and IT Security Concept

Do you know what the term 'security policy' refers to and what an IT security concept includes? Why do you need the security policy and the IT security concept?

A security policy defines the IT security objectives an organisation wants to achieve. The IT security concept describes how these objectives are to be achieved.

The development of a security policy and an IT security concept are two critical aspects for implementation of the IT-Grundschutz methodology. Simply document the steps explained in the following chapters and you have then already dealt with these aspects!

4.1 Security policy

The security policy defines the desired IT security level. It includes the security objectives to be fulfilled and the security strategy to be pursued and is thus both a requirement and a statement. It is used to define the "target" (= security level) for the organisation.

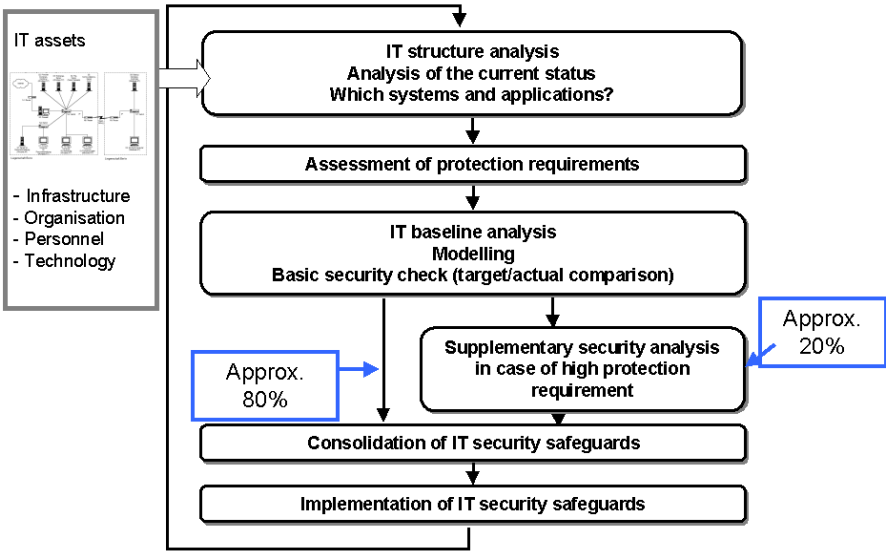
You can find a description of how to set up a security policy in the [BSISIPOL] document. In Section 11.1 we provide you with a security policy which is based on this document and adapted to the requirements of a small organisation.

Define and document your security policy on the basis of the example in Section 11.1 and adapt it to the specific requirements of your organisation, if necessary.

4.2

IT security concept

What exactly do I need to protect? What do I need to protect it from? How can I achieve effective protection?



If you wish to improve your IT security you will soon be confronted with these questions. An IT security concept answers the above questions and is divided into several sub-tasks.

Once you have defined the security objectives in the security policy you need to determine, as part of the IT security concept, the protection requirements for the IT applications and systems and to implement appropriate security safeguards.

In the following chapters we provide you with information on how to set up an IT security concept with a simple approach. Examples and checklists help you to document the processes in your organisation and to select appropriate security safeguards.

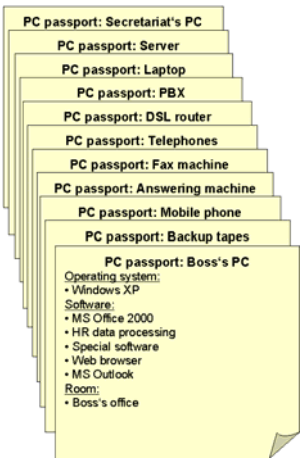
Set up a paper file for the IT security concept. Complete the checklist and file it in the paper file. This way, you document that the security safeguards have been implemented. When the paper file is complete you have reached your target: You have created an IT security concept!

Once Mrs. Adams has set up the IT systems summary and updated the operating systems, she adapts the sample security policy to the situation in her company. She once more discusses the security policy with her husband. After signing it, Mr. Adams informs all employees about it and explains the reasons for it. Mr. Adams wants all employees to be aware that the IT systems are a critical factor for the company's success. He asks his wife to develop an IT security concept.

5 Structure Analysis

What IT systems and data exist in my organisation?

What IT systems are used for critical business processes?



The first step when developing the IT security concept is to perform a structure analysis which serves to answer exactly the above questions. To this end you first have to record the following information for each IT system to have all relevant data and information at hand quickly (in the case of an incident involving damage).

- *Name of the IT system*
- *Operating system of the IT system*
- *Applications/programs on the IT system*
- *Are personal data processed by the applications?*
- *In which room is the system located?*

Completion of a PC passport has proved useful to document the data. The PC passport contains all relevant information related to an IT system.

Simply copy the PC passport from Section 11.2 of this profile and complete one PC passport for each of your IT systems. For the time being ignore the fields provided for entries related to protection requirements; these are filled in at a later date.

A critical step when developing the IT security concept is to obtain an overview of one's own systems, applications and data. This step is complete once you have filled out a PC passport for each individual PC in your organisation.

Note: Printers connected directly to the PCs are not entered as standalone components but as a part of the corresponding PC.

Note: Although telephone systems, mobile phones and answering machines are not PCs we recommend that you complete a PC passport for them as well. Just leave the fields in the PC passport which are not applicable to these devices empty (e.g. the operating system of the fax machine). A sample PC passport completed for the Boss's PC from the example is provided in Section 11.3.

Mrs. Adams fills out the PC passports for all the systems and files them in a separate paper file. She was able to do this in no time since she had obtained an overview of the existing systems only recently and had updated the operating systems of some of the PCs and installed new application software.

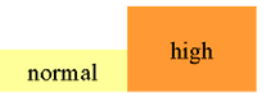
6 Assessment of Protection Requirements

The assessment of protection requirements answers questions as to which data are to be protected and where these are located and processed. When assessing protection requirements you therefore try to answer the following questions:

What needs to be protected? On which systems are sensitive data processed?

Which systems are critical for maintaining your business processes?

With the assessment of protection requirements you clearly document your organisation's comprehension of security.



The objective of determining the protection requirements is to decide for each recorded IT application including its data which damage could result if the fundamental IT security values of confidentiality, integrity and availability were violated. Since it is hardly ever possible to assess the potential damage precisely in terms of exact figures, you should define two categories, distinguishing between "normal" and "high" protection requirements.

This facilitates the selection of measures from the IT-Grundschutz Catalogues and helps to answer the question as to which components require additional measures. For "normal" protection requirements, the standard IT-Grundschutz security safeguards are sufficient and appropriate. For components with "high" protection requirements it may be necessary to take additional measures.

A potential customer asks Mr. Adams to make an offer as soon as possible for a contract which is considerable from Mr. Adams's point of view. To this end Mr. Adams had a lengthy conversation with the customer, taking notes of the most important points with his laptop. Mr. Adams is very keen on making a bid for this job since the work to be performed will amount to 25,000 €. While talking with the potential customer he had already developed an idea for the offer and the work to be performed based on services his company had rendered a couple of

years ago. On this basis he should be able to prepare a well-founded, sound and attractive offer during the weekend.

It is very important for him to get this major contract.

When sitting in his office in the evening, Mr. Adams notices that the documents from earlier years are not available on the server. He remembers that the hard disk was exchanged some time ago. He calls his wife and tells her that he urgently needs these documents, otherwise he would lose a major contract.

The protection requirement categories are defined using damage scenarios matched to your organisation's specific requirements. Potential damage is not only of a purely financial nature; damage to the image of the organisation as well as violations of laws and regulations and infringements of contractual obligations also need to be considered.

In all scenarios you need to decide on how important your data are to you and you also have to consider the specific situation in your organisation. Assuming damage of 200,000 €: in terms of turnover this sum is rather small for a bank but could lead to bankruptcy in the case of a travel agency. The IT-Grundschutz Catalogues provide additional examples and questions to define the protection requirement category.

For Mr. Adams a contract worth 25,000 € is very important. For this reason he assigns availability of the data he requires to instantly set up the offer to the category 'high'.

To define the protection requirement categories for your organisation, simply adapt the entries in the tables provided in Section 11.4 to your company or public authority. Please add any additional damage scenarios which are relevant to you.

6.1 IT applications

For each IT application, including its data, you need to define the protection requirements with regard to confidentiality, integrity and availability.

In the PC passport, for each application installed on the IT system you record whether personal data are processed there. You then determine – differentiated by the fundamental IT security values confidentiality, integrity and availability – the protection requirement in the categories normal and high.

For the boss's PC in our sample set of IT assets the entry in the PC passport would look as follows:

PC passport: Boss's PC

Applications/programs/data	Hotline	person-rel. data	Protection requirement: Availability	Protection requirement: Confidentiality	Protection requirement: Integrity
MS Office		✓	☒ normal ☐ high	☒ normal ☐ high	☒ normal ☐ high
Special software		✓	☒ normal ☐ high	☒ normal ☐ high	☒ normal ☐ high
			☐ normal ☐ high	☐ normal ☐ high	☐ normal ☐ high

Figure 2: Sample assessment of the protection requirement for the boss's PC

The information on the protection requirement for each IT application provides you with an overview of how important the individual IT applications are for your organisation and the extent to which your organisation relies on the security of the individual applications.

Mrs. Adams assesses the protection requirements for the IT applications used in the family business. When doing this she notices that the entire customer file including all entries is only stored on her husband's laptop. She remembers that they had agreed on this procedure to ensure that no unauthorised person can access these data, the main reason being the entries on special requests from Mr. Adams's customers which he fulfils flexibly and quickly. This file is very important for Mr. Adams. For this reason Mr Adams never leaves his laptop unattended.

Mrs. Adams assesses the protection requirement for the customer file. She categorizes the protection requirement for availability as "normal", since the unavailability of the customer data has indeed a strong impact on the business, but for a limited period this can be bridged by using other documents. She categorizes the protection requirement for confidentiality as "normal" as the information in the customer file could enable unauthorised persons to draw conclusions and gain insight into the business model. This way, competitors could e.g., be able to make the customer a more favourable offer. The loss of confidentiality, however, does not threaten the survival of the company. She assesses the protection requirement for integrity as "normal" since mistakes in the customer file can be identified easily and it is possible to subsequently correct the data.

Assess - as Mrs. Adams did in our example - the protection requirement for all IT applications installed on the IT systems in your organisation and enter the results into the corresponding PC passports.

6.2 IT systems

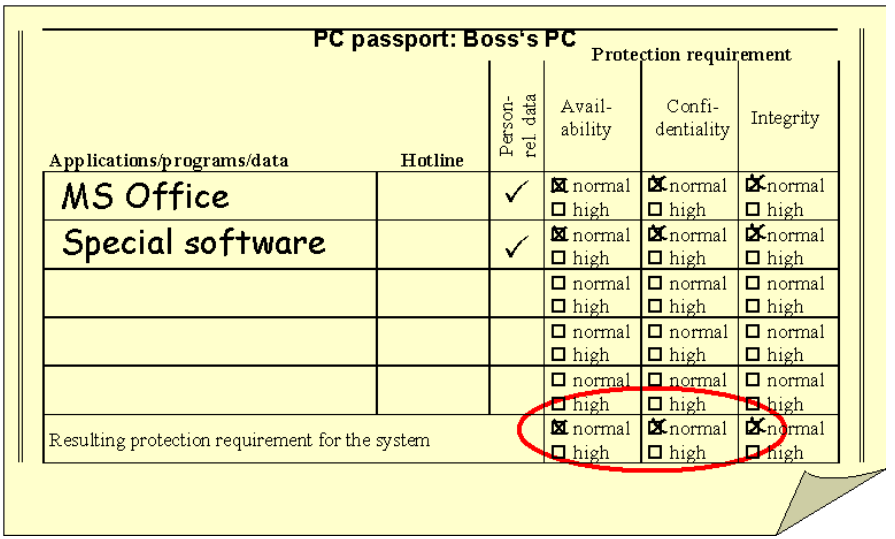
IT systems are used to support applications. For this reason the IT systems' protection requirements are determined by the applications running on these systems. The term "IT system" not only refers to PCs and laptops but also to photocopying and fax machines, telephones and mobile phones.

To be able to determine an IT system's protection requirement, you first need to consider all the IT applications installed on this system. The

completed PC passports provide you with an overview of the relevant IT applications and their protection requirements. The IT systems "inherit" the protection requirements determined for the IT applications.

In order to define the protection requirements for the IT system, you need to consider the potential damage to the relevant IT applications in its entirety. An IT system's protection requirements are determined by the damage or total damage with the most serious effects (maximum principle).

The entry in the PC passport for the boss's PC in a small set of IT assets in accordance with Chapter 3 is therefore as follows:



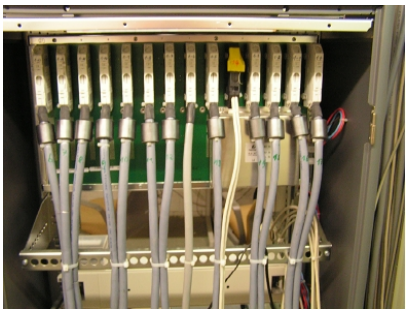
PC passport: Boss's PC

Applications/programs/data	Hotline	Person-rel. data	Protection requirement: Availability	Confidentiality	Integrity
MS Office		✓	☒ normal ☐ high	☒ normal ☐ high	☒ normal ☐ high
Special software		✓	☒ normal ☐ high	☒ normal ☐ high	☒ normal ☐ high
			☐ normal ☐ high	☐ normal ☐ high	☐ normal ☐ high
			☐ normal ☐ high	☐ normal ☐ high	☐ normal ☐ high
			☐ normal ☐ high	☐ normal ☐ high	☐ normal ☐ high
Resulting protection requirement for the system			☒ normal ☐ high	☒ normal ☐ high	☒ normal ☐ high

Figure 3: Assessment of an IT system's protection requirement using the boss's PC as an example

Now complete the PC passport for each IT system in your organisation by "inheriting" the protection requirements determined for the applications to the IT system.

6.3 Communication links



Which of the communication links in the organisation need to be protected?

When it comes to defining protection requirements, the importance of communication links as part of the set of IT assets should not be underestimated. Communication links play an important role for business operations, e.g. when sensitive data are transmitted. The IT-Grundschutz Catalogues only consider critical communication links

- which represent communication links to the outside world, i.e. which lead into or through uncontrolled areas (e.g. to the Internet or over areas to which the public have access),
- which are used to transmit data with a high protection requirement in terms of confidentiality, integrity or availability, or
- which may not be used to transmit data with a very high protection requirement.

In the set of IT assets described in Chapter 3 the Internet connection is a critical communication link as it leads to an uncontrolled area. In the example in Section 2.1 we saw how the malware transmitted data to an unauthorised person.

6.4 Rooms

In this small and clearly structured set of IT assets, the actual inheritance of the systems' protection requirements to rooms can be neglected. As many small public authorities are open to the public it is generally assumed that the rooms have higher protection requirements.

6.5 Interpretation of the results of the protection requirement assessment

In the previous chapters you have seen that all aspects need to be equally considered.

The examples provided so far have made it clear that you have to consider all fundamental IT security values (confidentiality, availability and integrity) when setting up an IT security concept. Neglecting just one fundamental IT security value can have significant consequences on security in your organisation.

Once the assessment of protection requirements is complete you have achieved the following:

- You have an up-to-date overview of the information technology in your organisation and a good understanding of the significance of your IT for handling the business processes.
- Also, you have already developed a feeling for potential dangers in your organisation and their consequences with respect to your IT.

In the following chapters this assessment of protection requirements which you now have at hand will be used to derive actual measures for the set of IT assets in your organisation to counteract the threats and thus help to minimize the impact of any loss or damage.

7 Modelling

The IT-Grundschutz Catalogues cover the threat scenarios and the recommended security safeguards for many areas and are therefore very comprehensive.

But don’t worry; you don’t need to deal with each and every threat and security safeguard and assess every single one individually for your organisation.

Each module of the IT-Grundschutz Catalogues covers a specific subject area and refers to the relevant threats and standard security safeguards. To provide a structure each module is assigned to one of the following layers depending on the respective subject area:

1. Organisation-wide applicable IT security aspects: Concepts and regulations applicable to the entire organisation, e.g. data backup policy, contingency planning concept, outsourcing
2. Infrastructure: Architectural and structural security aspects, e.g. protection against fire, burglary, the power supply within the building, cabling etc.
3. IT systems: Security aspects of IT systems, e.g. servers, clients, PBXs, firewalls
4. Networks: Network connections of IT systems (e.g. modem, WLAN)
5. IT applications: Security of typical IT applications, e.g. email, databases, Apache Web server, Outlook

In Section 2.2 “Assignment on the basis of the layer model“ the IT-Grundschutz Catalogues provide you with information to help you to decide on how to map (model) your IT environment. They especially deal with the question as to when the individual modules should be used and what they should be applied to (instructions for modelling).

Link the individual modules of the IT-Grundschutz Catalogues to your actual information technology by systematically working through the modules with the instructions for modelling. To this end, set up a table where you make a note of which module is assigned to which application area (for the example under review, you find a completed table in Appendix 11.5).

No.	Module	Applicable to
Organisation-wide applicable IT security aspects		
B 1.0	IT Security Management	Entire set of IT assets
B 1.1	Organisation	Entire set of IT assets
B 1.2	Personnel	Entire set of IT assets
B 1.4	Data Backup Policy	Entire set of IT assets
B 1.6	Computer Virus Protection Concept	Entire set of IT assets
B 1.9	Hard- and Software-Management	Entire set of IT assets
B 1.10	Standard Software	Entire set of IT assets
Infrastructure		
B 2.1	Building	Office environment
B 2.2	Cabling	Office environment

Figure 4: Extract from the IT asset modelling process in accordance with the IT-Grundschutz Catalogues including the specific modules to be applied in each case

When Mr. Adams recently required data which was stored on an exchanged hard disk to quickly prepare an offer, his wife was able to help him instantly. Before the hard disk was exchanged, she had backed up all data to tape and could restore the requested data within fifteen minutes. This way her husband had all the necessary information at hand to produce the offer for the potential customer. This was possible because Mrs. Adams had followed the instructions of Module B 1.4 of the IT-Grundschutz Catalogues referring, among other things, to regular data backup.

The result of the modelling process forms part of the IT security concept since each module of the IT-Grundschutz Catalogues refers to the security safeguards to be implemented in each case.

8 Self-assessment

We now come to the final step in the process of defining an IT security concept which will answer the following question:

What standard security safeguards have already been implemented and in what areas does something still need to be done?

This chapter will help you to identify deficits within your organisation which can put your IT systems and data at risk and to determine concrete countermeasures. The modules of the IT-Grundschutz Catalogues identified for the set of IT assets are used for this. You can find a description of the measures and threats related to the individual modules under the corresponding module number in the IT-Grundschutz Catalogues. Based on concrete examples for individual modules, you will learn how you can apply the IT-Grundschutz Catalogues and how the requirements can be effectively applied to your set of IT assets.

8.1 Implementation examples

Q11
Q12
Q18

The following sections deal with examples for some modules of the IT-Grundschutz Catalogues. In the left-hand margin you will find references to the measures described in detail in the IT-Grundschutz Catalogues (identified by Mx.y, where x and y refer to the corresponding numbers in the IT-Grundschutz Catalogues) and to the questions formulated in the checklists (identified by Qn, where n refers to the sequential number of the question in Section 11.6). To learn more about the individual measures just read the information provided under the corresponding security safeguard numbers in the IT-Grundschutz Catalogues.

8.2 Module B 1.4 Data Backup Policy

Computer systems and data storage media (e.g. hard disks) may fail and thus cause serious damage as work processes might be based on the stored data. For this reason you need to ensure that the damage caused by a failure of data storage media is minimized.

You should consider the following:

S 6.22
S 6.32
S 6.36
S 6.37
S 2.41
S 2.137

- Acquire a storage medium suitable for regular (at least weekly, better daily) data backup (e.g. a tape drive). Make sure that the storage capacity is sufficient and label the data media clearly.

  It makes sense to have the data backup performed automatically so that the medium only needs to be exchanged once a week (name a person responsible for backup).

  Create a PC emergency repair disk for each IT system.

  Note: Store the backup data media (e.g. CD-Rs, tapes) outside your office environment (e.g. in a safe-deposit box in a bank). This way your data is always available, even if a fire breaks out in your organisation.

S 6.41

- Check on a regular basis whether the data on the backup media (e.g. CD-Rs) can still be read and used.

We demonstrated already how useful the data backup was which Mrs. Adams made of the exchanged hard disk. In addition Mrs. Adams makes a backup to tape from all PCs, usually on Saturday afternoons. For this she uses a total of three tapes alternately. She stores these tapes in a safe in the basement of her house. Each month, she makes an additional backup which she stores in the vault of the local bank. It goes without saying that she has also created emergency repair disks for all PCs.

8.3 Module B 5.3 E-mail

E-mails (electronic mail) are used to send digital data from one computer to another. When using e-mails you need to pay special attention to the problem of viruses and should handle attachments to incoming e-mails with special care. It is also important to determine which data may not be sent via e-mail.

Q10
Q32
Q33
Q34

You can also find more useful information on e-mails on the BSI's Internet site.

Remember the following:

- Certain rules should apply when using e-mails. Instruct your staff to delete e-mails on a regular basis. Inform them when e-mails have to be encrypted.

S 2.118
S 2.119
S 2.121

- Attachments to e-mails may contain harmful functions and, like spam, can have adverse effects. Instruct your staff to handle e-mails carefully and not to open any suspicious attachments or unsolicited e-mails as these often contain viruses. If in doubt contact the originator of the e-mail by telephone.

S 5.53
S 5.54
S 5.55

- Tell your staff which data may not be sent via e-mail at all or only encrypted. Customer and patient data are examples of data that should definitely be encrypted if sent via e-mail.

S 2.118

- If you exchange sensitive data with a business partner via e-mail, use a specific e-mail encryption product (see for example [GNUPG]).

S 5.108

- When setting up deputisation arrangements, consider that e-mails addressed to employees who are on vacation or on sick leave are answered by the previously appointed deputy.

S 2.274

Mrs. Adams has installed virus scanners on all PCs in the office rooms and on the laptop PC. She updates these virus scanners along with the weekly data backup. Whenever she gets information on new dangerous viruses, for example in the news, she updates the virus scanners as soon as possible rather than waiting until the weekend.

Some of her husband's customers prefer to exchange information via e-mail, even for the submission of bids. For these cases Mrs. Adams has installed a user-friendly encryption tool on the PCs in the company which is also made available to the customers. This way it is possible to exchange confidential data via the Internet.

8.4 Module B 3.201 General Client and Module B 3.207 Windows 2000 Client

Module B 3.201 summarizes important safeguards to secure a client whereas system-specific safeguards for the individual operating systems are summed up in the specific modules such as Windows 2000 Client.

Q6 Q11 Q14 Q13 Q23 Q24 Q38 Q39 Q40 Q41 Q42 Q43 Q44 Q45 Q46 Q50 Q51

The Windows 2000 operating system is widely used, with a multitude of options and also risks. The different security safeguards can be used to prevent unauthorized persons from using the system or accessing data on the system. If the PC under review is a portable PC (laptop, notebook), additional aspects must be considered. With a portable PC the risk of theft is higher than with a desktop PC in the office since a portable PC is operated in an unprotected environment (e.g. a train station) where many people have access. Sensitive data that need to be protected appropriately are nonetheless stored on portable PCs.

For a Windows 2000 PC implement the following security safeguards:

- It should not be possible to boot a Windows 2000 PC using a removable data carrier (e. g. CD-ROM, floppy disk). Deactivate this function in the system's BIOS. If you don't know how to do this, contact a service provider or the supplier of the IT system.	**S 4.49**
- In the case of Windows systems, applications are started immediately from CD-ROM as soon as the CD-ROM is inserted in the drive (Autostart). Deactivate this function. For details refer to security safeguard S 4.57 in the IT-Grundschutz Catalogues.	**S 4.57**
- When installing Windows 2000 you need to pay attention to the following: Make sure that the instructions provided by Microsoft ([MSSEC]) and the recommendations in the IT-Grundschutz Catalogues are followed (see S 4.136).	**S 4.136** **S 4.149** **S 4.150**
- Note down the operating system name and version in all relevant PC passports and take a note of the manufacturer's telephone hotline.	**S 2.10**
- Regularly (at least weekly) install the patches published by Microsoft on your systems. This helps to reduce the risk of security gaps resulting from errors in the software.	**S 2.273**
- Train your staff in handling the operating system. In this context, make sure that comprehensible manuals are available.	**S 3.4** **S 3.5** **S 3.28**
- Activate the screen saver on all systems running under Windows with password protection. The screen saver should activate after 15 minutes at the latest. *Note:* The BSI offers a screen saver with security instructions. This screen saver and instructions for installation can be accessed under [BSIBS].	**S 4.2**
- Document in detail how Windows is installed on your computers. In particular record the options selected during the installation process.	**S 2.25**

If Windows 2000 is installed on a portable PC you also need to pay attention to the following (included in Module B 3.203 Laptop):

S 1.33

- Never leave the device unattended. Unauthorized persons may access the system or steal the device.

  Note: If a portable PC is kept in a vehicle make sure that it is not visible from the outside. It is advisable to cover the device or lock it in the boot. A portable PC is a high-value object attracting potential thieves, all the more as portable PCs can be re-sold easily. If the portable PC is used on-site in a third party's offices, the room should where possible be locked by key even when left only for a short time. If you leave the room for a longer period the portable PC should also be switched off (or switched to stand-by mode) to prevent unauthorized persons using it using the boot password.

  Some newer devices additionally provide a capability of chaining the device to a solid object (e.g. a desk). In this case tools are required to steal the device.

  Encrypt sensitive data on the computer.

S 4.2

- Activate the screen lock on your portable PC such that deactivation is possible only after entering a password.

S 4.3

- Use a virus scanner and update this scanner on a regular basis.

S 6.71

- Regularly copy the data from your portable PC to CD-ROM or a workstation PC in your office environment. This way you can still access the data even if the portable PC is stolen or becomes defective. And don't forget to also perform a data backup after using the portable PC for longer periods.

Note: Most portable PCs have permanently installed modems, WLAN components and network cards. When travelling a WLAN interface can for example setup a connection to the internet using a so-called Hotspot. In this respect remember the following:

- Using a wireless LAN you need to pay attention to the Module B 4.6. Especially portable PCs have to be protected against unauthorized access via the wireless LAN. Make sure to configure and use the security settings of WLAN components. The trustability of public access points (Hotspots) has to be considered.
- Do not store passwords for access to online services on the computer. It is often possible to store the access password on the computer for convenience. Refrain from using this capability as it allows unauthorized persons to use your access to online services.

For Mr. Adams the laptop has become a very important element in his work since, among other things, his customer file is stored on it. For this reason he never leaves his laptop unattended and secures his data in two ways: Firstly Mrs. Adams regularly makes backup copies and secondly she installed a program to encrypt the files on the laptop's hard disk. Even if the laptop was stolen the data could be restored immediately and would be of no use to the thief. The laptop's hardware itself is insured against theft.

8.5 Module B 3.101 General Server

Q6 Q11 Q12 Q13 Q23 Q24 Q46 Q47 Q48 Q49

The term server-based network refers to a local network with at least one server which, e.g., runs under Windows 2000. Consistent documentation of all systems, changing of any factory-set passwords and regular data backups as well as compliance with security notices with regard to the server's operating system are critical (see for example [MSSEC] for Microsoft operating systems).

In this respect pay attention to the following:

S 1.32

- The server in your organisation is a central component of your IT. When selecting the location for the server make sure that it can only be accessed by authorized persons.

S 3.10

- Define who is responsible for maintaining the IT systems and enter the telephone number of the person in charge and his/her deputy in the PC passport.

  Note: Make sure that your systems are only managed by competent staff. For example, have a requirement included in the contract that the external service provider's staff responsible for managing your systems is sufficiently qualified. Alternatively, simply ask the member of staff him/herself! A suitable reference could be, e.g., an MCSE (Microsoft Certified Systems Engineer) certification.

You should also make sure that the installation of the systems is documented in detail.

S 4.7

- Change the standard passwords of all systems. This way you prevent unauthorized persons who know these standard passwords from accessing the systems.

  Note: Don't forget to keep the passwords in a safe place!

For a Windows 2000 server (Module B 3.106), the following should be remembered:

- Highly sensitive files may be stored on the server. It may be possible to restore deleted files. To prevent this you should use a tool that overwrites these files before they are actually deleted. **S 4.56**
- When operating a Windows 2000 server you need to pay attention to various security aspects. Follow the directions in S 4.146 in the IT-Grundschutz Catalogues. **S 4.146**

Mrs. Adams has located the server in a storage room in her husband's company. This room has no windows and is also used as an archive for documents. The room is not used on a regular basis and is therefore mostly locked. Keys are held by Mr. and Mrs. Adams and Miss Burke. Only Mr. and Mrs. Adams know the administrator password for the server.

8.6 Security status

Which security requirements have been implemented to date? Where are there still security gaps? What is my company`s current security level?

A list of questions querying basic security requirements for each individual module helps you gain an initial overview of your own security status.

From the answers to these questions which are included in a checklist in Section 11.6 an initial estimate of the security level can be derived for our example of a small set of IT assets.

Supplement the questionnaire with your own questions and delete any questions that do not apply to you. This way, you can develop a customized tool to perform a self-assessment for your organisation.

9 Basic Security Check

You need to determine for each individual module whether all measures have been implemented.

In the course of the basic security check you determine for each individual module whether the measure has been “implemented“, ”partially“ implemented or ”not implemented“. A security measure may however be “dispensable“ if other safeguards counteract the corresponding threats (e.g. when infrastructural safeguards are not required since technical safeguards are implemented on a higher level) or if the function to be protected by the respective measure is not available (e.g. when the service reviewed in connection with the threat is not available on the computers).

In Section 11.7 you will find a form for a small set of IT assets which will help you document the implementation status of all security safeguards.

Now perform a target/actual comparison for your organisation by adding or deleting any measures in the sample form.

Implementation of the IT security safeguards and maintenance of the IT security level

In most cases there will be some security safeguards that have not been implemented yet or only partially. The next step is to eradicate these deficits to the largest possible extent.

Mrs. Adams has learnt that a new update is available for the operating system on Miss Burke’s PC. The update removes some security gaps that may occur when accessing the Internet with the PC. As Miss Burke can access the Internet with the company PC, Mrs. Adams gets the update and installs it.

To achieve a permanently secure status it is not sufficient to perform the IT-Grundschutz methodology only once. For this reason update your PC passports on a regular basis and go through the questionnaire again.

10 Summary

The procedure described here introduced you, step-by-step, to setting up the IT security concept for the set of IT assets in your organisation.

You have now documented

- that security is an important issue for you and
- the measures which you have implemented to achieve it.

The effort you invested will definitely pay off. For example: Banks consider a company's IT risks when assessing their credit risks. But also when concluding an insurance contract for your IT systems the existing IT security concept may have a positive impact on the premiums to be paid. It helps you, e.g., to easily prove that it is no problem for you to recover data in the event of a hard disk failure because you perform backups on a daily basis. When assessing the risk the insurance company could limit the cover and premiums to the mere cost of the hardware.

In the afternoon Mr. Adams visited a customer to check the quality of the work performed. The customer was very satisfied. When talking to each other the customer mentioned that hackers had tried to penetrate the network of the company he worked with as a development engineer. The customer reported that the entire documentation on the development of current and newly developed products was stored on the computers of the medium-sized company. Fortunately the administrator, who only performs this task as a secondary job, noticed this attack on the network. However, the only way the administrator could find at first was to disconnect the company's internet access entirely for several hours. The analysis of the situation in the company showed that basic protective measures had been disregarded. In particular the default password provided when the firewall was installed had never been changed. This is what the hackers took advantage of.

Mr. Adams then mentioned that he and his wife had only recently implemented a pragmatic procedure for setting up an IT security concept.

Mr. Adams is sure that the kind of attacks his customer described would not be successful in his own company.

You have learnt that IT security is not a complicated subject and that use of a standard methodology helped you to achieve your target quickly.

IT security safeguards are not introduced for their own sake. All safeguards are aimed at **safeguarding your core business.**

11 Forms and Sample Applications

On the following pages we provide you with forms and sample applications to help you set up your IT security concept. In addition to a *sample security policy* you will find a two-page PC passport which you should copy, complete for each of your systems and file, together with the customized security policy, in your dedicated IT security concept paper file. You will also find a completed PC passport for the boss's PC in our sample set of IT assets.

Following the PC passports we provide you with a sample definition of protection requirement classes which you can use as a basis for your categorization of protection requirement classes and which you should also file in your dedicated IT security concept paper file.

This is followed by the complete modelling process for the sample set of IT assets. You should set up a similar table and model your own set of IT assets. You should then also file this result in your dedicated IT security concept paper file.

Finally we provide you with a checklist to perform your self-assessment. After editing and completing this checklist you file it in your dedicated IT security concept paper file. Do not forget to go through and update the checklist on a regular basis to reflect changes to your set of IT assets and any new measures resulting from these changes.

11.1 Sample Security Policy

The "sample security policy" below is provided to help you set up a security policy for your organisation. Check the text passages in *<italics>* and adapt them to your specific requirements if necessary.

Security policy for <organisation>

We, the <management>, hereby adopt the following IT security policy as part of our <company policy>:

The IT supports our business purpose, especially as regards <here, enter areas where IT is used in your organisation>.

It should be possible to compensate for a failure at short notice; at the same time business operation may not be significantly affected by security deficiencies. The measures undertaken to guarantee IT security are based on minimizing the costs incurred by damaging incidents, including costs incurred for avoiding and preventing damage.

Our data, our <customers'/clients'> data and our IT systems in all areas are secured for availability such that the downtimes to be expected are tolerable. Malfunctions and irregularities with respect to data and IT systems are acceptable to a small extent only and only in exceptional cases (integrity). Ensuring confidentiality of company data is a foremost requirement in our company.

To this end, responsibilities for IT security have been defined. The <head of organisation> and an administrator have been nominated as responsible for IT security and deputisation arrangements have been put in place. The staff have been and will continue to be trained in using the IT services and the corresponding security safeguards and have also been and will continue to be made aware of the threats to IT security.

We shall comply with the requirements of the data protection legislation and aim to achieve a data protection level appropriate for the business purpose and the importance of the person-related data and data processing. The organisational requirements are based on securing compliance with data protection legislation.

To ensure the striven-for IT security and data protection level the regulations and their compliance shall be reviewed continuously. Deviations shall be analyzed to improve the IT security situation <in the organisation> and to constantly keep it up-to-date with the current state of IT security technology.

---------- ----------

Date *Signature*

11.2 PC passport

The PC passport is intended to provide the person responsible for IT with an overview of the existing computers and to allow this person to react instantly and effectively if problems occur. This way the person responsible for IT can gain an overview of the existing systems and the level of protection they require. When making any changes to an IT system do not forget to amend the entries in the PC passport accordingly.

PC passport

Page 1

System

Service telephone numbers

Serial/inventary number

Operating system incl. installed service packages and patches

Virus scanner; settings, update interval

Last update

Room (number)		**Protection requirement** Availability	Confidentiality	Integrity
	Protection requirement for the room	☐ normal ☐ high	☐ normal ☐ high	☐ normal ☐ high

Notes

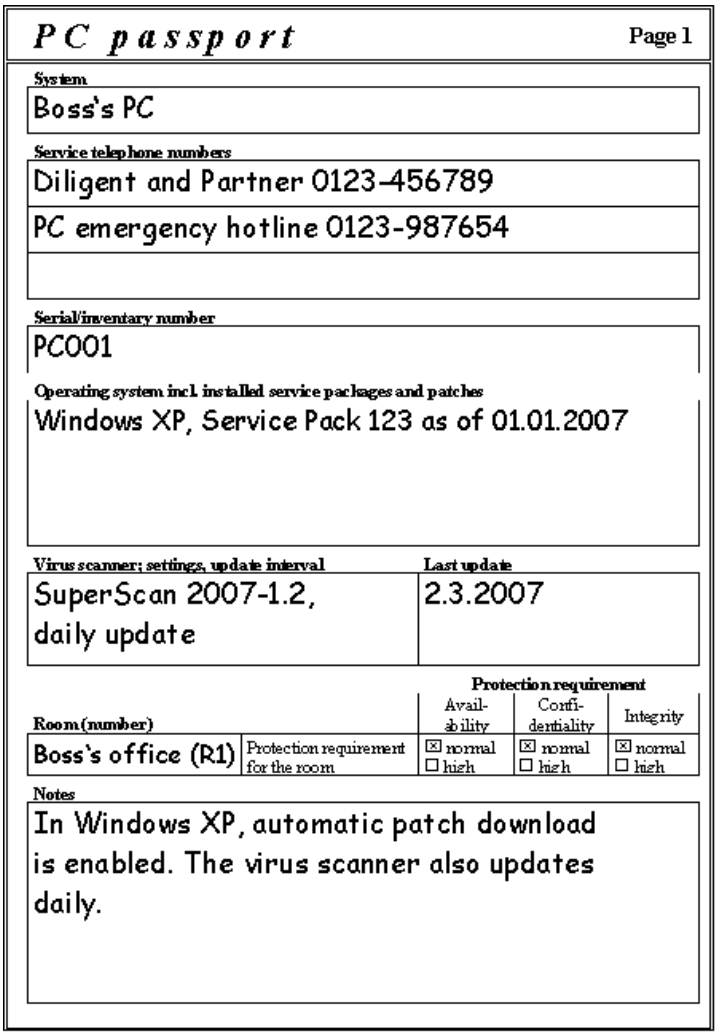
PC passport

Page 2

Applications/programs/data	Hotline	Personal data	Protection requirement: Availability	Protection requirement: Confidentiality	Protection requirement: Integrity
			☐ normal ☐ high	☐ normal ☐ high	☐ normal ☐ high
			☐ normal ☐ high	☐ normal ☐ high	☐ normal ☐ high
			☐ normal ☐ high	☐ normal ☐ high	☐ normal ☐ high
			☐ normal ☐ high ☐ normal ☐ high	☐ normal ☐ high ☐ normal ☐ high	☐ normal ☐ high ☐ normal ☐ high
Resulting protection requirement for the system			☐ normal ☐ high	☐ normal ☐ high	☐ normal ☐ high

System installation/configuration/notes

11.3 Sample PC passport for the boss's PC



PC passport Page 1

System

Boss's PC

Service telephone numbers

Diligent and Partner 0123-456789

PC emergency hotline 0123-987654

Serial/inventary number

PC001

Operating system incl. installed service packages and patches

Windows XP, Service Pack 123 as of 01.01.2007

Virus scanner; settings, update interval	Last update
SuperScan 2007-1.2, daily update	2.3.2007

Room (number)		Protection requirement: Availability	Protection requirement: Confidentiality	Protection requirement: Integrity
Boss's office (R1)	Protection requirement for the room	☒ normal ☐ high	☒ normal ☐ high	☒ normal ☐ high

Notes

In Windows XP, automatic patch download is enabled. The virus scanner also updates daily.

PC passport

Page 2

Applications/programs/data	Hotline	Personal data	Protection requirement: Availability	Confidentiality	Integrity
MS Office		✓	☒ normal ☐ high	☒ normal ☐ high	☒ normal ☐ high
Special software		✓	☒ normal ☐ high	☒ normal ☐ high	☒ normal ☐ high
			☐ normal ☐ high	☐ normal ☐ high	☐ normal ☐ high
			☐ normal ☐ high ☐ normal ☐ high	☐ normal ☐ high ☐ normal ☐ high	☐ normal ☐ high ☐ normal ☐ high
Resulting protection requirement for the system			☒ normal ☐ high	☒ normal ☐ high	☒ normal ☐ high

System installation/configuration/notes

The PC's installation has been documented in writing. The document ("Installation of the boss's PC") can be found in the Appendix of the dedicated IT security concept paper file. A list of the individual hardware components is also provided there.

11.4 Definition of protection requirement categories

The following table is intended to assist you in defining the protection requirement categories in your organisation. To do this you need to adapt text passages in <*italics*> to the situation in your organisation. The wording applicable to *normal/high* protection requirements is always separated by "/".

Impairment of the right to informational self-determination	
Normal/ high	- Impairment of the right to informational self determination would be assessed as *acceptable/considerable* by the individual. - Possible misuse of person-related data would have *moderate/considerable* effects on the social or financial standing of those concerned.
Impaired performance of duties	
Normal/ high	- Impairment of the performance of duties would be assessed as *acceptable/unacceptable* by all individuals concerned. - The maximum acceptable downtime is e.g. *24/1 to 24 hours*.
Violation of laws, regulations or contracts	
Normal/ high	- Violations of regulations and laws have *minor/considerable* consequences - Violations of contracts lead to *minor/high* penalties.
Physical injury	
Normal/ high	- Physical injury to an individual can *probably/not absolutely* be ruled out.
Negative effects on external relationships	
Normal/ high	- *Minimal or only internal/severe* impairment of reputation or trust is to be expected.
Financial consequences	
Normal/ high	- The financial loss to the organisation amounts to *50 to 250/250 to 5000 EUR*.

Note: The protection requirement categories merely serve as examples and differ depending on an organisation's specific requirements (e.g. banks or computer centres). The assessment of protection requirements provides a basis for a risk analysis in your organisation.

11.5 Modelling the sample set of IT assets

The following table demonstrates the modelling process for the sample set of IT assets from Chapter 3. The number in the first column refers to the number of the module in the IT-Grundschutz Catalogues. The questions refer to the checklist in Section 11.6.

No.	Module	Applicable to	Questions
Organisation-wide applicable IT security aspects			
B 1.0	IT Security Management	Entire set of IT assets	Q1,Q2,Q3
B 1.1	Organisation	Entire set of IT assets	Q4,Q5,Q6,Q7
B 1.2	Personnel	Entire set of IT assets	Q8,Q9,Q10,Q14
B 1.4	Data Backup Policy	Entire set of IT assets	Q11,Q12,Q18
B 1.6	Concept of Computer Virus Protection	Entire set of IT assets	Q13,Q14,Q15,Q16
B 1.9	Hardware- and Software-Management	Entire set of IT assets	Q18,Q19,Q20
B 1.10	Standard Software	Entire set of IT assets	Q22,Q23,Q24
B 1.13	IT Security Awareness and Training	Entire set of IT assets	Q13,Q32,Q33

No.	Module	Applicable to	Questions
Infrastructure			
B 2.1	Building	Office environment	Q25,Q26,Q27
B 2.2	Cabling	Office environment	Q28,Q29
B 2.3	Office	Boss's office, secretariat, corridor, storage room	Q20,Q30,Q31
IT systems			
B 3.101	General Server	Server	Q6,Q11,Q12,Q13, Q23,Q24,Q47,Q48
B 3.106	Windows 2000 Server	Server	Q46,Q48,Q49
B 3.201	General Client	Laptop, secretary's PC boss's PC	
B 3.203	Laptops	Portable PC	Q6,Q13,Q14,Q38 Q39,Q40,Q41,Q42 Q43,Q44,Q50,Q51
B 3.207	Windows 2000 Client	Laptop, secretary's PC	Q6,Q11,Q14,Q13 Q23,Q24,Q45,Q46
B 3.209	Windows XP Client	Boss's PC	Q6,Q11,Q14,Q13 Q23,Q24,Q45,Q46
B 3.301	Security Gateway (Firewall)	DSL router	Q13,Q14,Q23,Q47, Q48,Q52,Q53,Q54
B 3.401	Telecommunicat-ions System	Private branch exchange (PBX)	Q13,Q20,Q27,Q48, Q55

No.	Module	Applicable to	Questions
B 3.402	Fax machine	Fax machine	Q7,Q13,Q48,Q56, Q57,Q58
B 3.403	Answering machine	Answering machine	Q13,Q48,Q59
B 3.404	Mobile telephones	Mobile phone	Q60,Q61,Q62
Networks			
B 4.3	Modem	Laptop	Q23,Q47, Q48,Q52,Q53,Q54
B 4.5	LAN connection of an IT system via ISDN	DSL router	Q13,Q14,Q23,Q47, Q48,Q52,Q53,Q54
IT applications			
B 5.3	E-mail	Outlook	Q10, Q32, Q33, Q34
B 5.7	Databases	Database for the special software	Q6, Q11, Q13, Q19, Q24, Q37

Table 1: Modules in the IT-Grundschutz Catalogues applicable to the sample set of IT assets.

Should you not find a module in the IT-Grundschutz Catalogues that suits exactly, orient yourself to similar modules and apply them accordingly!

11.6 Checklist

No.	Question
Q1.	Have the following issues been defined in your IT security policy?
□	- Importance of IT security and relevance of the IT to your company
□	- Definition of IT security objectives
Q2	Have your employees been made sufficiently aware as regards IT
□	security?
Q3	In the past 12 months have you updated the security policy, the protection requirement assessment and the PC passports or are you
□	just about to do it?
Q4	In the PC passport have you already entered the contact and the
□	hotline telephone numbers for all IT systems?
Q5	Do you have a specific contact to turn to when problems occur with the computers, programs/applications, and have you entered his/her telephone number (hotline telephone number) in the PC
□	passport?
Q6	Have you informed your employees that a password
□	- needs to be changed on a regular basis,
□	- must include at least 8 characters,
□	- should not be easy to guess (like husband's first name, own car ID etc.) and
□	- must be recorded and stored in a closed envelope?
Q7	Do you have a shredder in your organisation?
□	
Q8	Do you tell new employees about the security policy and its
□	contents?
Q9	Do you have a checklist you work through when an employee
□	joins and
□	leaves the organisation?
Q10	Does a deputisation arrangement (for vacation/sick leave) exist for
□	employees responsible for the IT?
□	Does it ensure that the e-mails of an absent employee are answered?

No.	Question
Q11	Have you determined which data are to be backed up regularly and which person is responsible for data backup (change of media)? Do you check regularly whether data backup functions properly?
Q12	Are the backup media (tapes, CD-ROMs) kept in a safe place (e.g. in a safe-deposit box in a bank; safe)?
Q13	When new programs and equipment are introduced, are your employees instructed and trained how to use them? Virus protection Database Use of laptops Operating system (Windows 2000/XP etc.) PBX / telecommunications system Fax machine Answering machine
Q14	Have you prohibited your employees from installing their own software on the computers?
Q15	Do you use virus scanners and are they automatically updated on a regular basis?
Q16	Do you and your employees know how to operate the virus scanners and what to do if a virus is reported? Do you inform yourself of new viruses regularly?
Q17	Are data carriers (e.g. C-ROMs, floppy disks) checked for viruses before they are passed on?
Q18	Are the data carriers (floppy disks, CD-ROMs, etc.) in your organisation labelled clearly?
Q19	Do you and your employees know where to find the manuals for the programs you use on a daily basis? Especially those for the databases/special software!
Q20	Are visitors to your organisation accompanied and supervised continuously by one of your employees during their stay?
Q21	Do you know where your secretary files important documents and would you be able to find them without her assistance (e.g. when she suddenly falls ill)?

No.	Question
Q22	Did you note in the PC passport which software is installed on each of the existing computers and which version? Did you also note the hotline telephone number and whether the software was complete upon delivery?
Q23	In the last four weeks, have you checked whether updates or patches are available for the software used in your organisation?
Q24	Have the installation and de-installation of software and operating system been documented in writing and filed in the dedicated IT security concept paper file?
Q25	Have smoke alarms been fitted in your organisation?
Q26	Do you and your staff know where the emergency exits are located, where escape routes lead to and where fire extinguishers are located? Do you and your staff know how to handle a fire extinguisher and that inflammable equipment is a fire hazard?
Q27	Have you instructed your staff to close windows and doors at the end of their working day and to switch off inflammable equipment?
Q28	Has it been ensured that visitors have no chance to manipulate cables in your office environment?
Q29	Have all electric cables been fitted by a specialist company and have they been protected against short-circuits?
Q30	Have you determined the hours when staff may enter the organisation?
Q31	Do your employees lock sensitive data at the end of their working day and do they keep their workplace tidy?
Q32	Do you inform your staff about the risk of e-mail attachments (viruses, worms) on a regular basis ?
Q33	Have you defined which information must **NOT** be sent by e-mail?
Q34	Do you use an encryption product when sending sensitive data by e-mail?

No.	Question
Q35	Has the configuration of your special office software been documented in writing and is this documentation updated when modifications are made?
Q36	Has it been ensured that, e.g. your secretary cannot access data she does not necessarily need to access?
Q37	Does the database you use provide for the definition of different access rights for the data contained in the database?
Q38	When using the laptop outside the office do you always keep an eye on it?
Q39	Have you installed a screen saver with password protection on your laptop?
Q40	Have you installed a virus scanner on the laptop which is updated on a regular basis?
Q41	Is the laptop's operating system updated regularly?
Q42	Are the data on the hard disk encrypted?
Q43	Are you able to restore the data on your laptop if the hard disk fails?
Q44	Do you regularly copy the data on your laptop to the server, or do you burn these data to a CD-ROM?
Q45	When starting the system using removable media (e.g. CD-ROM, floppy disk etc.), is it ensured that the system is password-protected or cannot be started at all?
Q46	Was your Windows 2000 system installed securely?
Q47	Have you included in your contract with your service provider that your systems may only be administered by qualified staff (e.g. MCSE-certified staff)?
Q48	Have you positioned your server and telecommunications equipment such that they cannot be accessed by unauthorized persons (e.g. visitors)?
Q49	When deleting files containing confidential information do you use a special program which prevents data from being restored?
Q50	Have you deactivated the password storage option in the communications software?
Q51	Have you checked the number dialled by the modem?

No.	Question
Q52	Has Internet access been secured by a firewall?
Q53	Have you documented the configuration of the firewall (in particular its filter lists) in writing and is it ensured that your systems cannot be accessed via the Internet?
Q54	Has the use of active contents (in particular ActiveX) been deactivated in your browsers?
Q55	Is the telecommunications equipment maintained by qualified staff and have the provider and telephone number been documented?
Q56	Have you defined which information may not be sent by fax?
Q57	Do you use a fax cover sheet which contains at least the number of the fax machine, the name of the originator, a contact telephone number, the recipient's name and the number of pages including the cover sheet?
Q58	Do you regularly check the transmission reports for incoming faxes and called numbers for plausibility?
Q59	Has the remote query function of your answering machine been deactivated or secured with a specific code?
Q60	Have you recorded your mobile phone provider's hotline telephone number so that you can have your mobile disabled if is stolen?
Q61	Have you selected a PIN which is not easy to guess?
Q62	Do you keep your mobile's PIN and PUK codes and the SIM card in a safe place, together with the passwords?
Q63	Have your systems been protected and insured against theft? Special attention should be given to laptops and mobile phones!
Q64	...

11.7 Safeguards

The following tables provide a selection of safeguards related to the modules of the IT-Grundschutz Catalogues dealt with in Chapter 8. The left-hand table column refers to the corresponding numbering in the IT-

Grundschutz Catalogues where you can find more detailed information on the respective safeguards if required. When working through this table you can indicate in the columns at the right whether you have implemented the safeguard completely (Y), partially (P) or not at all (N). If you think the safeguard is dispensable, indicate this in column (D).

	Data Backup Policy B 1.4	Y	D	P	N
S 2.41	Employees' commitment to data backup				
S 2.137	Procurement of a suitable data backup system				
S 6.20	Appropriate storage of backup data media				
S 6.21	Backup copy of the software used				
S 6.22	Sporadic checks of the restorability of backups				
S 6.32	Regular data backup				
S 6.33	Development of a data backup policy				
S 6.34	Determining the factors influencing data backup				
S 6.35	Stipulating data backup procedures				
S 6.36	Stipulating a minimal data backup policy				
S 6.37	Documenting data backup procedures				
S 6.41	Training data reconstruction				

	General Server B 3.101	Y	D	P	N
S 1.28	Local Uninterruptible Power Supply (UPS)				
S 2.22	Escrow of passwords				
S 2.32	Establishment of a restricted user environment				
S 2.35	Obtaining information on security weaknesses of the				

	General Server B 3.101	Y	D	P	N
	system				
S 2.138	Structured data storage				
S 2.204	Prevention of Insecure Network Access				
S 2.273	Prompt installation of security-relevant patches and updates				
S 2.314	Use of high-availability architectures for servers				
S 2.315	Planning the use of a server				
S 2.316	Defining a security policy for a general server				
S 2.317	Procurement criteria for a server				
S 2.318	Secure installation of a server				
S 2.319	Migration of a server				
S 2.320	Well-ordered disposal of a server				
S 4.7	Change of preset passwords				
S 4.15	Secure log-in				
S 4.16	Restrictions on access to accounts and/or terminals				
S 4.17	Blocking and erasure of unneeded accounts and terminals				
S 4.24	Ensuring consistent system management				
S 4.40	Preventing unauthorised use of computer microphones				
S 4.93	Regular integrity checking				
S 4.237	Secure basic configuration of an IT system				
S 4.238	Use of a local packet filter				
S 4.239	Secure operation of a server				
S 4.240	Setting up a testing environment for a server				

	General Server B 3.101	Y	D	P	N
S 5.8	Regular security checks of the network				
S 5.9	Logging at the server				
S 5.10	Restrictive granting of access rights				
S 5.37	Restriction of Peer-to-Peer Functions in a Server-Supported Network				
S 6.24	PC emergency floppy disk				
S 6.96	Contingency planning for a server				

	General Client B 3.201	Y	D	P	N
S 2.23	Issue of PC Use Guidelines				
S 2.25	Documentation of the system configuration				
S 2.273	Prompt installation of security-relevant patches and updates				
S 2.321	Planning the use of client-server networks				
S 2.322	Defining a security policy for a client-server network				
S 2.323	Well-ordered disposal of a client				
S 3.18	Log-out obligation for PC users				
S 4.2	Screen lock				
S 4.3	Periodic runs of a virus detection program				
S 4.4	Correct handling of drives for removable media and external data storage				
S 4.40	Preventing unauthorised use of computer microphones				
S 4.41	Use of a appropriate security products for IT systems				
S 4.93	Regular integrity checking				
S 4.200	Handling of USB storage media				
S 4.237	Secure basic configuration of an IT system				
S 4.238	Use of a local packet filter				
S 4.241	Secure operation of clients				
S 4.242	Setting up a reference installation for clients				
S 5.37	Restricting Peer-to-Peer functions in a server-supported netork				
S 5.45	Security of Web browsers				

	General Client B 3.201	Y	D	P	N
S 6.24	PC emergency floppy disk				
S 6.32	Regular data backup				

	E-mail B 5.3	Y	D	P	N
S 2.30	Provisions governing the configuration of users and of user groups				
S 2.42	Determination of potential communications partners				
S 2.46	Appropriate key management				
S 2.118	Determination of a security policy for the use of e-mail				
S 2.119	Regulations concerning the use of e-mail services				
S 2.120	Configuration of a mail centre				
S 2.121	Regular deletion of e-mails				
S 2.122	Standard e-mail addresses				
S 2.123	Selection of a mail provider				
S 2.274	Deputisation arrangements for e-mail				
S 2.275	Setting up function-specific e-mail addresses				
S 4.33	Use of a virus scanning programm on exchange of data media and during data transfer				
S 4.34	Using encryption, checksums or digital signatures				
S 4.64	Verification of data before transmission / elimination of residual information				
S 4.199	Avoiding dangerous file formats				
S 5.22	Compatibility check of the transmission and reception				

	E-mail B 5.3	Y	D	P	N
	systems				
S 5.32	Secure use of communications software				
S 5.53	Protection against mail bombs				
S 5.54	Protection against mail overload and spam				
S 5.55	Checking of alias files and distribution lists				
S 5.56	Secure operation of a mail server				
S 5.57	Secure configuration of mail clients				
S 5.63	Use of GnuPG or PGP				
S 5.67	Use a time stamp service				
S 5.108	Cryptographic protection of e-mail				
S 5.109	Use of an e-mail scanner on the mail server				
S 5.110	Protection of e-mail with SPHINX (S/MIME)				
S 6.38	Back-up copies of transferred data				
S 6.90	Data backup and archiving of e-mails				

Appendix A Glossary of Terms

BIOS	Basic Input/Output System. The BIOS is a permanent basic operating system responsible for data input and output in a PC. The BIOS controls the exchange of data between hard disk, graphics card, keyboard and mouse.
BSI	German Federal Office for Information Security.
Computer worm	A self-contained reproductive program spreading through a system (usually networks).
IT-Grundschutz	The aim of the IT-Grundschutz is to establish an information security management system and to achieve a security level for IT systems that is reasonable and adequate to satisfy normal protection requirements.
Intranet	A company-internal network, usually with connections to the Internet.
IT	Information Technology.
IT application	Software used for a specific purpose, i.e. application. An application program may be, e.g., a word processing or image processing program.
IT assets	IT assets refer to all infrastructural, organisational, personnel and technical components which serve to perform tasks in a particular field of information processing. A set of IT assets can refer to the entire information technology of an organisation or to individual areas defined in terms of organisational structures (e.g. a departmental network) or shared IT applications (e.g. a personnel information system).
IT security concept	The IT security concept is the central document in the IT security process of an organisation. It must be possible to trace each concrete security safeguard back to this security

	concept. First of all the IT security concept must include the description of the current status of a set of IT assets and the data to be processed with it. In addition to a description of the technical components, the IT applications operated on them and the data to be processed with them, the current status of a set of IT assets includes a list of the existing vulnerabilities, potential threats, if any, and security safeguards that have already been implemented.
IT system	The term IT system is generally used for devices and equipment used to process information/data. This includes not just PCs but also devives such as copiers, fax machines and telephones.
LAN	Local Area Network.
Maximum principle	The IT application with the highest damage potential in respect of violation of the fundamental IT security values. The protection requirement for the IT system on which this application is running is determined by the damage with the most serious effects (maximum principle).
Patch	A patch is a program, usually created at short notice, which eliminates errors in already released software. In most cases the patch is offered for download on the software producer's website and enables users to eradicate the shortcomings of the software.
ISO	International Organization for Standardization
Trojan horse	A program named after the model from Greek mythology with a damaging function which at first sight appears completely harmless.
WLAN	Wireless Local Area Network.

Appendix B References

[GSK] IT-Grundschutz Catalogues, http://www.bsi.bund.de/english/gshb/index.htm

[GSPROF1] Company profiles medium-sized set of IT assets, BSI http://www.bsi.bund.de/gshb/deutsch/download/index.htm (in German)

[GSPROF2] Company profiles large set of IT assets, BSI http://www.bsi.bund.de/gshb/deutsch/download/index.htm (in German)

[SECGUIDE] IT Security Guidelines, BSI http://www.bsi.bund.de/english/gshb/guidelines/index.htm

[BSISIPOL] Sample policy and sample concepts, BSI http://www.bsi.bund.de/gshb/deutsch/hilfmi/musterrichtlinien/index.htm (in German)

[DSIN] Germany secure in the internet, https://www.sicher-im-netz.de/ (in German)

[GNUPG] The GNU Privacy Guard (GnuPG) http://www.gnupg.org/

[MSSEC] Microsoft Security http://www.microsoft.com/security/default.mspx

[BSIBS] http://www.bsi-fuer-buerger.de/Bildschirmschoner/liesmich.htm (in German)

[DIALER] http://www.bsi.de/av/dialer.htm (in German)