Bundesamt
für Sicherheit in der
Informationstechnik

ISACA®
Trust in, and value from, information systems
Germany Chapter

Guide
Cyber Security Check

A Guide for the Implementation of Cyber Security Checks
in Companies and Government Agencies

Table of Contents

Alliance for Cyber Security

The Alliance for Cyber Security, started at the CeBIT 2012 trade fair, is an initiative of the Federal Office for Information Security (BSI), which was founded in collaboration with the Federal Association for Information Technology, Telecommunications and New Media (BITKOM).

As an association of important players in the field of cyber security in Germany, the Alliance aims at increasing cyber security in Germany and strengthening the resistance of Germany against cyber attacks. The Alliance for Cyber Security supports the exchange of information and experiences between the different players from industry, administration and science and, based on this, is continuously expanding a substantial knowledge base.

Enterprises are encouraged to actively play a part in the Alliance for Cyber Security and to boost the exchange of experiences. By reporting to the BSI which new threats or IT security incidents the companies are confronted with, they contribute to the development of a complete overview of the situation and help to be able to act against cyber attacks in an even more purposeful manner. At the same time, the companies also benefit from jointly gained knowledge and experiences.

Federal Office for Information Security

With its headquarters in Bonn, the Federal Office for Information Security was founded on 1 January 1991 and is part of the Federal Ministry of the Interior.

With currently around 600 employees and a total budget of 88 million euro, the BSI is an independent and neutral body dealing with matters of IT security in Germany's information society.

In this respect, the services offered by the government agency are aimed both at the public administration of federal, state and local governments and at enterprises and citizens. The BSI examines and assesses existing IT security risks and evaluates the effects of new developments. The BSI increasingly observes a large number of targeted and untargeted cyber attacks. Based on this, the BSI draws conclusions with respect to the improvement of IT security in Germany. The BSI develops for example, minimum standards and recommendations for action regarding IT and Internet security for different target groups in order to ensure that risks are prevented from arising in the future.

„Today, no industry and no company can consider themselves safe from cyber attacks. This is shown by the numerous incidents in the recent past."

Dr. Hartmut Isselhorst,
President of the Cyber Security Department,
BSI

ISACA Germany Chapter e.V.

ISACA Germany Chapter e.V. is the German branch of the worldwide leading professional association of IT auditors, IT security managers and IT governance officers. The association was founded in 1986 and, with more than 2,300 members, is part of the international ISACA association, to which more than 100,000 experts in more than 180 countries worldwide belong. The aim and purpose of the association is to promote the better understanding of the problems in the field of IT auditing, IT security and IT governance through discussions and the exchange of information between the members and interested parties and to inform all members and interested parties of these experiences through publications and seminars as well as to support and supplement the contacts between the members and interested parties through social events. In addition to this, the association is intended to contribute to the promotion of the job profile of IT auditors, IT security managers and IT governance officers.

„In the light of the current developments, it is more important than ever to be the master of one's own data. Only if organisations are able to protect their knowledge, will they maintain their competitive edge."

Andreas Teuscher,
Vice-President,
ISACA Germany Chapter e.V.

Cooperation BSI / ISACA

This guide was jointly developed by ISACA Germany Chapter Working Group Information Security and BSI experts. By means of this active partner contribution, ISACA Germany Chapter e.V. documents that it supports the objectives pursued by the Alliance for Cyber Security with its good reputation, the resources available and the expert knowledge of its members.

1 Introduction

1 Introduction

Today, most business processes depend on the reliable and proper functioning of information and communication technologies. Therefore, many rating agencies already evaluate information security as part of a company's operational risks. The actual threats as well as the amount of damage resulting from successful cyber attacks are not always obvious: For example, the consequences of a know-how theft might only be recognised at a much later point in time.

According to surveys, more than 70 percent of larger companies in Germany have already been affected by cyber attacks. In this context, the number, complexity and professionalism of the attacks are increasing. The opinion that is nevertheless still widespread in many companies „Well, nothing has happened so far" might thus quickly result in serious problems if the existing security concepts are not adjusted continuously and adequately to the changed threat situation. Irrespective of this, the number of threats is growing continuously, which is also rapidly increasing the likelihood of a company or a government agency being affected by a cyber attack. Depending on the degree of dependency on IT, the business activities of an organisation can be brought to a complete halt – with all the consequences related to this. Thus, cyber security should be given top priority.

The threats from cyberspace are real. In order to respond to cyber attacks effectively, an intensive cooperation between the state, economy and associations is required. The challenge now is to pool the existing knowledge in order to be prepared when faced with new attack scenarios.

For this reason, the Federal Office for Information Security and ISACA Germany Chapter e.V. decided to jointly develop a practical approach for the assessment of cyber security in companies and government agencies. The „Cyber Security Check" helps to determine the cyber security status based on the cyber security exposure (see [ACS2]) and thus to respond to current threats from cyberspace effectively. The basis of each

cyber security check are the basic safeguards for cyber security published by the BSI (see [ACS3]).

The duration of a cyber security check can be modified from one day up to several days by adjusting the assessment depth to the organisation to be assessed and the respective prevailing conditions. A cyber security check can be implemented both by qualified, internal personnel and by external service providers who have shown their skills in the implementation of cyber security checks by means of a personal certification as „Cyber Security Practitioner". In addition, the BSI and ISACA make an assignment of the safeguard objectives to be assessed to known standards of information security available (IT-Grundschutz, ISO 27001, COBIT, PCI DSS) as a particularly interesting added value. A sample template for a final report, describing both the detected deficiencies and the recommendations given on how to eliminate these deficiencies in a compact form, completes the aids provided for the implementation of a cyber security check.

This guide is addressed to all interested parties who deal directly or indirectly with cyber security. Given the relevance and importance of this issue, all levels, i.e. from the middle/ senior management of an organisation, information security managers / IT security officers, corporate security managers, IT administrators and IT auditors through to the end users should be concerned with cyber security. This document is intended as an orientation aid for beginners and as directions for action for the parties responsible who want to initiate or implement a cyber security check.

This guide provides specific guidelines for the implementation of a cyber security check, which can be found in chapter 4 „Implementation of a Cyber Security Check" in particular. IT security officers and other parties responsible for information security should use this guide in particular to gain an overview of the issue, to look at the security aspects to be assessed and to make themselves familiar with the procedure to be followed when implementing a cyber security check.

This guide forms the basis for the implementation of cyber

security checks in companies and government agencies.

Auditors and consultants are provided with practical action guidelines containing specific guidelines and information for the implementation of a cyber security check and for the preparation of the report. The standardisation of the approach ensures consistent high quality. In addition, it should increase the transparency for companies and government agencies when comparing different offers in the tendering and contracting process of the „Cyber Security Check“ service.

The Federal Office for Information Security and ISACA Germany Chapter e.V. would like to thank the authors of the ISACA Technical Group Information Security: Matthias Becker, Olaf Bormann, Ingrid Dubois, Gerhard Funk, Oliver Knörle, Andrea Rupprich, Dr. Tim Sattler, Nikolai Jeliazkov and Andreas Teuscher.

2 Introduction to cyber security

2 Introduction to cyber security

2.1 What is cyber security?

Cyber security, cyber attack, cyber crime and cyber espionage have long since become catchwords in security discussions. This is partly attributable to the technical development, but it is mainly due to the continuously growing number of security incidents, criminal activities and new information-based attack methods. The myth that these attacks are activities carried out by individuals with an exceptional knowledge has given way to the experience that cyber security is an important facet of security and that it must be taken into account by the middle/senior management of an organisation. It requires the use of suitable resources and should be an integral part of entrepreneurial risk management.

In the context of information security, however, the term „cyber“ requires an additional explanation, since it is often misunderstood or generalised. With respect to this guide, cyber security covers the examination of the security safeguards taken by implementing cyber security checks which are intended to protect organisations and individuals against becoming

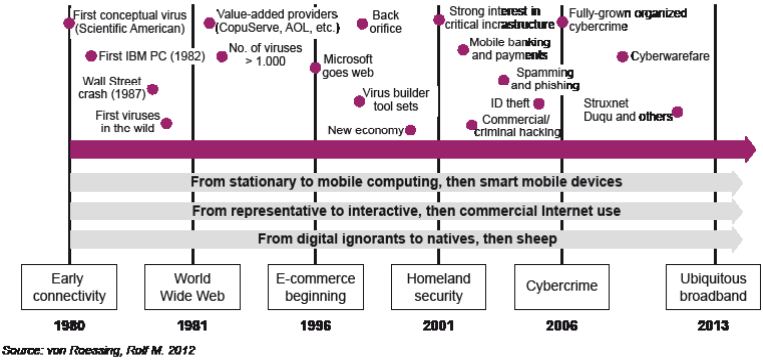


Figure 1: Developments in cyberspace (from [ISACA2])

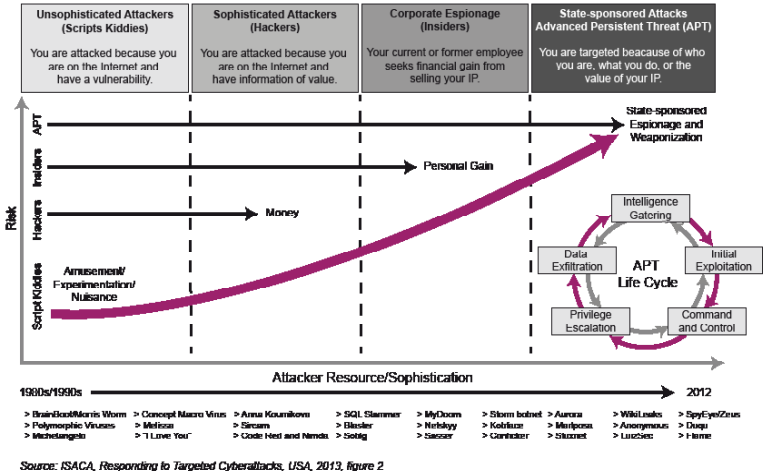
the victim of a cyber attack, cyber crimes or cyber espionage. In practice, however, cyber security is limited to advanced and targeted attacks that are difficult to detect and to defend against (see Advanced Persistent Threats (APTs)). Cyber security is thus part of the general fight against crime, with the perpetrators using information technology deliberately and specifically as a weapon for carrying out their attacks.

As shown in Figure 1, cyber security has a history dating back to the early 1980s, when criminals started to use technical attacks in the form of hacking, cracking and malware (e.g. viruses, worms and Trojan horses) for their purposes. Only in the past few years, however, have cyber crime and widespread cyber attacks become a social and economic problem.

2.2 Cyber attacks and Advanced Persistent Threats (APTs)

Organisations must deal with threats, risk scenarios and vulnerabilities on a daily basis. The highest threat for companies and government agencies as well as for their partners is currently targeted cyber attacks by advanced, well organised and professionally equipped attackers. This type of attack is often summarised under the term APT (Advanced Persistent Threat) (see [ISACA7]). APTs are often very complex both in preparation and in implementation and are usually carried out in several phases. The aim of an APT is to remain undetected for as long as possible in order to spy on sensitive information or cause other damage over a longer period of time. This type of cyber attack often has a professional background (e.g. cyber crime or industrial espionage), is difficult to detect and the attackers are only identified with considerable effort. The following figure shows how threats have developed over time and what the underlying motivation might be.

This guide and the underlying safeguard objectives for the assessment were designed in such a manner that APT-based cyber attacks are basically made difficult and the capabilities to discover an attack and to adequately respond to it are strengthened. The risk of falling victim to an APT-based cyber attack can thus be minimised by regularly implementing a cyber security check.



Source: ISACA, Responding to Targeted Cyberattacks, USA, 2013, figure 2

Figure 2: Developments of the threat landscape (from [ISACA7])

If an organisation has already become the victim of an APT attack or if an APT attack is suspected, specific reactive safeguards can be found in the BSI document „Erste-Hilfe bei einem APT-Angriff (in English: First Aid in the event of an APT Attack)“ (see [ACS5]).

2.3 Effects of cyber crime on organisations and society

Today, the threats posed by cyber crime and cyber espionage have numerous effects on society, organisations and individuals concerned. Since 2006, it can be observed that both organised crime and government agencies have been dealing with what possible targets of cyber attacks might look like. The results included:

» Theft of confidential information, product data and developments up to systematic espionage

» Theft of intellectual property, manipulation of commercial transactions, misappropriation of funds

» Financial fraud, misuse of credit cards, falsification and misu-

se of identities

What is interesting in this respect is that the development of cyber crime in its current form has reached a speed and dimension which were not even predicted by critics.

As compared to crime in general, cyber crime rose from approx. 1% in 2009 to 23% in 2011 and has thus overtaken several other types of crime within an extremely short period of time.

In both cases, the effects on society, organisations and individual concerned are immense and „non-participation in cyberspace“ no longer seems to be a realistic option. Rather, it must be recognised that each organisation moving in cyberspace is also inevitably exposed to such attacks. The middle/senior management of an organisation should integrate this awareness into its risk analysis and provide suitable resources in order to implement adequate protective precautions.

2.4 Cyber security strategy pursued by the Federal Government

Cyberspace comprises all information infrastructures that can be reached through the Internet worldwide across territorial borders. In Germany, all areas of social and economic life make use of the possibilities made available by cyberspace. As part of an increasingly networked world, the state, critical infrastructures, the economy and the population in Germany are dependent on the reliable and proper functioning of information and communication technologies as well as of the Internet.

Within the framework of the Critical Infrastructure Implementation Plan [UP KRITIS], the BSI has already been collaborating intensively with operators of critical infrastructures since 2007. The „Cyber Security Strategy for Germany“, which was adopted by the Federal Government in February 2011, allows the state, economy and private users to respond to current and future threats from cyberspace within their respective responsibilities and courses of action. Here, cyber security is included by the civil approaches and safeguards, which are to the fore, as part of

the national security precautions. For the critical information structures, the focus is on the closer interaction of state and economy on the basis of an intensive exchange of information.

3 Basic Principles of the Cyber Security Check

3 Basic Principles of the Cyber Security Check

By means of implementing a cyber security check, companies and government agencies can determine the current cyber security level of their organisation. As known from information security, such an assessment must be carried out based on a comprehensive framework in order to be able to make sound and reliable statements. This guide and the underlying safeguard objectives for the assessment were designed in such a manner that the risk of falling victim to a cyber attack can be minimised by regularly implementing a cyber security check. In this respect, the approach focuses on cyber security issues and aspects. It is drafted based on three lines of defence.

Figure 3 shows that the middle/senior management of an organisation must first understand the necessity of cyber security safeguards, the protection requirements of the business processes as well as their dependencies and threats. Via the risk management, representing the second line, an analysis as to what

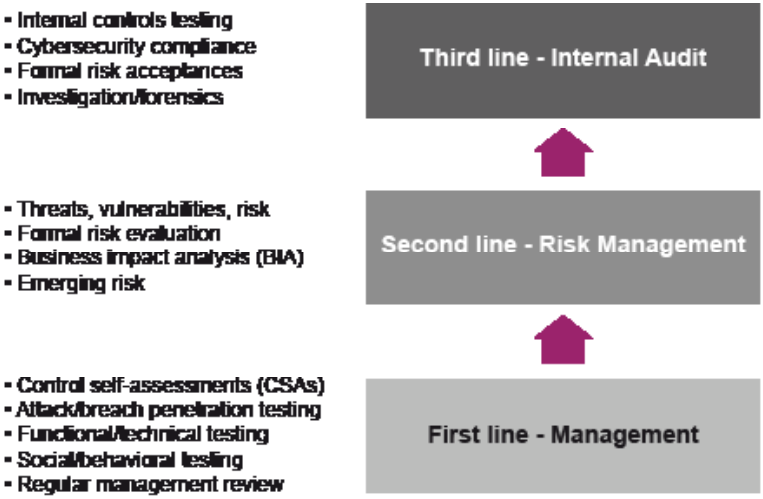


Figure 3: Three lines of defence

extent cyber security risks affect the organisation and their processes should then be carried out. Here, the organisation‘s risk management examines the decisions of the middle/senior management and assesses them as first independent body, without, however, reversing the decisions taken. The final decision on the implementation of security safeguards still remains with the middle/senior management.

As third line of defence, the cyber security check, with which an independent and objective assessment of the existing level of security is carried out, is used. The assessor supports the organisation in achieving their objectives and targets, assessing the organisation‘s cyber security based on a systematic and specific approach and promotes the optimisation of the security safeguards by means of their work.

In order to create trust in an objective assessment, the following prerequisites must be complied with both by individuals and by companies providing services in the field of cyber security:

» Formal contracting of the cyber security check by the organisation (see ISACA Standard for IS Audit and Assurance 1001 – Audit Charter) [ISACA8]

» Independence (see ISACA Standards for IS Audit and Assurance 1002 – Organisational Independence and 1003 – Professional Independence) [ISACA8]

» Integrity and confidentiality (see ISACA Standard for IS Audit and Assurance 1005 – Due Professional Care) [ISACA8]

» Professional expertise (see ISACA Standard for IS Audit and Assurance 1006 – Proficiency) [ISACA8]

» Evidence and traceability (see ISACA Standard for IS Audit and Assurance 1205 – Evidence) [ISACA8]

» Objectivity and diligence (see ISACA Standards for IS Audit and Assurance 1207 – Irregularities and Illegal Acts and 1204 – Materiality) [ISACA8]

» Objective and factual presentation (see ISACA Standard for IS Audit and Assurance 1401 – Reporting) [ISACA8]

The basic prerequisite for each assessment within the framework of the cyber security check is an unrestricted right to information and inspection. This means that no information may be withheld from the assessor. This also includes the inspection of sensitive or officially confidential information relating to the information security management and/or IT operations if the assessor can substantiate corresponding legitimate interest. In the latter case, the assessor must be security cleared and authorised in accordance with the „Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (in English: General Administrative Regulations of the Federal Ministry of the Interior for the Physical and Organisational Protection of Classified Information)“ (VSA – see [BMI3]) and/or the „Handbuch für den Geheimschutz in der Wirtschaft“ (in English: Manual for the Protection of Classified Information in the Economy (see [BMWI]). In this respect, the level of the security check depends on the degree of confidentiality of the information concerned.

In addition to this guide, the basis for the cyber security check is the two BSI recommendations for cyber security „Basismaßnahmen der Cyber-Sicherheit (in English: Basic Safeguards for Cyber Security)“ (see [ACS3]) and „Cyber-Sicherheits-Exposition (in English: Cyber Security Exposure)“ (see [ACS2]). If there are no statements on individual parts of the object to be assessed in these publications, other relevant regulations, laws, standards or specifications by manufacturers or professional associations must be applied. The application of these sets of rules must be documented and justified in the assessment report.

The on-site assessment can be carried out both by a single assessor and by a team consisting of several individuals.

As a matter of principle, it should already be taken into account when initiating a cyber security check that the ongoing operations in the organisation will not be impaired considerably by the assessment. The assessor never actively interferes in the

systems and does not give any instructions to make changes to IT systems, infrastructures, documents or organisational procedures either. In each case, the assessor only requires read access.

4 Implementation of a Cyber Security Check

4 Implementation of a Cyber Security Check

4.1 Object to be assessed

The object of a cyber security check is generally the entire organisation including its connections to the Internet, the connections to the Internet via other organisational units as well as all connections to other networks, such as networks of partners, service providers and customers.

All aspects relating to the physical access to IT systems and/or aspects dealing with physical security (fire protection, protection against entering and breaking etc.) are not relevant.

If essential logical IT systems or IT services are excluded from the assessment, they must be documented and justified in the assessment report as boundaries of the scope of the object to be assessed.

4.2 Approach

Below, the approach to the implementation of a cyber security check is explained step by step:

Step 1 - „Awarding the contract“:

In order to implement a cyber security check, it is not necessary for the mandatory documents regarding the security process to be available or for a defined implementation status of specific security safeguards to have been reached. Thus, it is possible to initiate a cyber security check in any environment and at any stage of the security process.

In order to ensure a comprehensive and effective assessment, the contract for the implementation of a cyber security check

should be awarded by the middle/senior management of the respective organisation.

Step 2 - „Determining the cyber security exposure“:

In order to carry out an initial risk assessment for the organisation to be assessed, the cyber security exposure is determined prior to the on-site assessment. Based on this, the required time to be expected, the assessment depth as well as the selection of samples can be determined in a risk-oriented manner.

If the determination of the cyber security exposure for the organisation concerned was not carried out based on a management decision, this should be adequately performed by the assessor in cooperation with the organisation. In this context, the approaches presented in (see [ACS2]), brief interviews conducted by the assessor or existing empirical values, for instance, serve as orientation. If the cyber security exposure had already been determined by the organisation, the assessor can take it over without carrying out any further activities of their own if they consider it to be understandable and adequate. In any case, the cyber security exposure results must be documented in the report in a suitable manner.

Detailed information on the determination of the cyber security exposure can be found in the BSI recommendation for cyber security BSI-CS_013 „Cyber-Sicherheits-Exposition (in English: Cyber Security Exposure)“ (see [ACS2]).

Step 3 - „Document review“:

The document review serves to gain an overview of the tasks, the organisation itself and the organisation‘s IT infrastructures. The document review merely consists of a rough inspection of the documents provided. Here, the IT framework concept, the list of the critical business processes, the security guideline and the security concept including network plan (if available) are assessed in particular.

If there are no adequately informative documents available, the document review is supplemented by meetings during

which the assessor can gain the required overview. Based on the knowledge gained, the assessor determines the samples and focuses of the assessment in a risk-oriented manner.

Step 4 - „Preparing the on-site assessment“:

In order to prepare the on-site assessment, a schedule should be prepared taking the cyber security exposure into consideration. This schedule describes which contents are to be assessed at what time/date and which contact persons (roles/functions) are required for this purpose. The schedule must be forwarded to the organisation concerned in advance.

Step 5 - „On-site assessment“:

The on-site assessment itself always starts with a short opening meeting and ends with a final meeting. During the opening meeting, the approach and target course of the cyber security check is explained to the organisation. In addition, organisational issues are clarified, such as access control, meeting room or changes to the approach if any.

As part of the on-site assessment, interviews are conducted, IT systems given a close inspection and, if necessary, additional documents reviewed. When carrying out the on-site assessment, the contact persons to be interviewed with respect to the respective topics should be available. The samples to be assessed (e.g. documents, IT systems) and the facts established should be documented by the assessor in a sufficiently detailed manner in order to be able to adequately use this information later for the preparation of the report.

During the final meeting, in which the organisation‘s management level should also participate, a first general estimate of the cyber security level in the organisation is provided. In addition to this, the assessor discloses any serious security deficiencies which put the organisation‘s cyber security at an immediate high risk and should thus be dealt with and handled promptly.

Step 6 - „Follow-up evaluation / preparing the report“:

The cyber security check is concluded by means of an assessment report. The report provides an overview of the cyber security in the organisation and, in addition to the cyber security exposure, contains a list of the deficiencies detected. For each safeguard objective (see [ACS4]), the respective assessment result should be documented.

In the report, general recommendations for how to deal with the deficiencies detected are given. These recommendations show the organisation assessed in which areas additional activities are required in order to increase the cyber security level.

More detailed information on the preparation of the report can be found in chapter 4.6 „Preparing the assessment report".

4.2.1 Implementation quality / personal certificate

An organisation can have a cyber security check implemented both by its own qualified personnel and by a qualified service provider. In both cases, however, it must be ensured that the approach specified in this guide is used.

In order to document the essential principles of cyber security and the implementation of cyber security checks to the outside, the Alliance for Cyber Security and ISACA provide interested participants with a one-day further education course on the subject of cyber security with the opportunity to obtain a certificate as „Cyber Security Practitioner" after they have successfully passed a multiple-choice test. The certificate is valid for three years and must then be renewed through corresponding further education events. The one-day event is recognised by the BSI and ISACA as a further education course for the certificate holders of the two organisations within the CPE (Continuing Professional Education) framework.

4.3 Assessment methods

The term „assessment methods" refers to all actions taken to examine a situation. During a cyber security check, the fol-

lowing assessment methods can be used by the assessor:

» Oral questioning (interview),

» (Visual) inspection of IT systems, sites, premises and objects,

» Monitoring (perceptions as part of the on-site assessment),

» File analysis (this also includes the analysis of electronic data or statistical analyses),

» Data analysis (e.g. configuration files, log files, analysis of databases etc.) and

» Written questioning (e.g. questionnaire).

Which of these methods are to be applied depends on the specific situation and must be determined by the assessor. The assessor must also take into account that the principle of proportionality is complied with in all cases. In order to examine a situation, a combination of several assessment methods can also be used.

4.4 Binding safeguard objectives

Due to the establishment of binding safeguard objectives, both the consistent high quality of the cyber security check and the comparability of the activities of different assessors is to be ensured.

The binding safeguard objectives for a cyber security check are based on the „Basismaßnahmen der Cyber-Sicherheit (in English: Basic Safeguards for Cyber Security]“ (see [ACS3]). A detailed description of the binding safeguard objectives can be found on the websites of the Alliance for Cyber Security (see [ACS4]).

The assessment depth (intensity) is adjusted in a risk-oriented manner by the assessor depending on the level of cyber security exposure.

4.5 Assessment scheme

If any security deficiencies are detected within the framework of a cyber security check, the assessor must thus determine, when preparing the report at the latest, how the deficiencies concerned are to be assessed in terms of their criticality.

Security deficiencies must be classified as follows:

„No security deficiency“
At the time of the assessment, no security deficiency could be detected. There is no supplementary information.

„Security recommendation“
Even a fully implemented IT security safeguard can be supplemented by a security recommendation.

By implementing the safeguard recommendations described in the situation, the security can be increased. Improvement suggestions for the implementation of safeguards, additional safeguards that have been successful in practice or comments regarding the appropriateness of safeguards can also be listed as security recommendations.

„Security deficiency“
In the event of a „security deficiency“, there is a security gap which should be closed in the medium term. The confidentiality, integrity and/or the availability of information might be impaired.

„Serious security deficiency“
A „serious security deficiency“ is a security gap which should be closed immediately, since the confidentiality, integrity and/or the availability of information are exposed to a high risk and considerable damage can be expected.

Security deficiencies and recommendations must be documented in the final report in such a manner that the assessment can be understood by a qualified third party (expert).

4.6 Preparing the assessment report

The middle/senior management of the organisation and/or the client must be informed of the assessment report of a cyber security check in writing. A draft version of the report should be forwarded to the organisation audited and assessed in advance in order to verify whether the situations detected (only the situations detected– without assessments and recommendations) were recorded correctly and objectively.

The assessment report consists at least of the following three parts:

» the framework data, including the detailed description of the object to be assessed

» a summary (Management Summary, including cyber security exposure)

» the detailed assessment (detailed description of the deficiencies detected, their assessment and recommendations to correct the deficiencies)

The assessment report must be prepared as deficiency report without appreciating any positive aspects.

Part I - Framework Data

This part contains organisational information:

» Object to be assessed

» Boundaries of the scope of the object to be assessed

» Assessors

» Contact persons of the organisation assessed

» Bases for assessment

» Time schedule

» Distributor for the assessment report

» Framework data of the assessment document and/or document control

  • File name

  • Print date

  • Document status

Part II - Management Summary

This part includes a summary for the management. The main deficiencies and any recommendations resulting from them should be summarised in a brief and understandable manner.

» Summary

» Cyber security exposure

» Overview of the assessment results
(for all safeguard objectives (see [ACS4]))

Part III - Detailed Assessment for each Safeguard Objective

This part of the report contains the detailed description of the topics assessed, the deficiencies detected, their assessment as well as recommendations to correct the criticised situations. For the assessment of the deficiencies detected, the scheme shown in chapter 4.5 must be used.

» Safeguard objective (see [ACS4])

» Result including assessment

» Sample(s)

» Description of any deficiencies detected including safeguard recommendation(s)

Formal aspects regarding the final report:

When preparing the assessment report, the following formal aspects must be taken into account:

» The pages must be marked in such a way that each page can be clearly identified (e.g. including page number and version number, title and date of the report).

» Any terminology or abbreviations used which are not in general use must be summarised in a glossary and/or index of abbreviations.

» The report must be clearly specify the organisational units audited and assessed and the recipients of the report as well as state any restrictions of use.

» The report must be signed by the assessor.

» The form and contents of a report might vary depending on the type of the contracted assessment work; however, the minimum requirements for the assessment report (see this chapter) and the ISACA IS Audit and Assurance Standard 1401 (see [ISACA6]) must be complied with when implementing the cyber security check.

A sample report of a cyber security check can be found on the website of the Alliance for Cyber Security (see [ACS6]).

5 Glossary and Definition of Terms

5 Glossary and Definition of Terms

The following terms are used in this document:

APT (Advanced Persistent Threat) refers to a very complex, specific, intensively prepared and performed cyber attack (see also chapter 2.2).

BSI (Federal Office for Information Security) is the central IT security service provider of the Federal Administration.

Assessor is someone who implements a cyber security check on the basis of this guide.

CPE (Continuing Professional Education) is a measure for the performance of continuing professional education.

Cyber crime refers to criminal activities using cyberspace as source, target and/or tool.

Cyberspace comprises all information infrastructures that can be reached through the Internet worldwide across territorial borders.

Cyber security pursues the protection of confidentiality, integrity and availability of information against threats from cyberspace.

Organisation is used as generic term for government agencies, companies and other public or private organisations.

ISACA (Information Systems Audit and Control Association) is the international professional association of IT auditors, IT security managers and IT governance officers.

KRITIS (critical infrastructures) are organisations and facilities of major importance for society whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order or other dramatic consequences.

Middle/senior management is used to refer to the management boards, managing directors and the management of government agencies.

Safeguard objectives are cyber security aspects and questions relevant for the assessment. They include security management issues and topics as well as technical aspects.

Whistle-blower (also ‚informant') is someone who makes information important for the general public interest from a secret or protected context public.

All personal pronouns used in this document refer equally to men and women. If the male form of a term is used in the text, this is only for the sake of readability.

6 References

6 References

[ACS1] Allianz für Cyber-Sicherheit (in English: Alliance for Cyber Security), website (in German only), www.allianz-fuer-cybersicherheit.de

[ACS2] Allianz für Cyber-Sicherheit (in English: Alliance for Cyber Security, BSI-CS_013 „Cyber-Sicherheits-Exposition (in English: Cyber Security Exposure)“ (in German only), www.allianz-fuer-cybersicherheit.de

[ACS3] Allianz für Cyber-Sicherheit (in English: Alliance for Cyber Security, BSI-CS_006 „Basismaßnahmen der Cyber-Sicherheit (in English: Basic Safeguards for Cyber Security)“ (in German only), www.allianz-fuer-cybersicherheit.de

[ACS4] Allianz für Cyber-Sicherheit (in English: Alliance for Cyber Security, Verbindliche Maßnahmenziele für den Cyber-Sicherheits-Check (in English: Binding Safeguard Objectives for a Cyber Security Check) (in German only), www.allianz-fuer-cybersicherheit.de

[ACS5] Allianz für Cyber-Sicherheit (in English: Alliance for Cyber Security, BSI-CS_072 „Erste-Hilfe bei einem APT-Angriff (in English: First Aid in the event of an APT Attack)“ (in German only), www.allianz-fuer-cybersicherheit.de

[ACS6] Allianz für Cyber-Sicherheit (in English: Alliance for Cyber Security, Muster-Bericht für den Cyber-Sicherheits-Check (in English: Sample Report for the Cyber Security Check), www.allianz-fuer-cybersicherheit.de

[BMI1] Bundesministerium des Innern (in English: Federal Ministry of the Interior), Nationaler Plan zum Schutz der Informationsinfrastrukturen in Deutschland (Na-

tional Plan for Information Infrastructure Protection in Germany), Umsetzungsplan KRITIS (UP-KRITIS) (in English: CIP Implementation Plan), September 2007, www.bmi.bund.de

[BMI2] Bundesministerium des Innern (in English: Federal Ministry of the Interior), Cyber-Sicherheitsstrategie für Deutschland (in English: Cyber Security Strategy for Germany), February 2011, www.bmi.bund.de

[BMI3] Bundesministerium des Innern (in English: Federal Ministry of the Interior), Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (in English: General Administrative Regulations of the Federal Ministry of the Interior for the Physical and Organisational Protection of Classified Information), June 2006, www.verwaltungsvorschriften-im-internet.de (in German only)

[BMWI] Bundesministerium für Wirtschaft und Energie (in English: Federal Ministry for Economic Affairs and Energy), Handbuch für den Geheimschutz in der Wirtschaft (in English: Manual for the Protection of Classified Information in the Economy) (in German only), November 2004, www.bmwi.de

[ISACA1] ISACA Germany Chapter e.V., website (in German only), www.isaca.de

[ISACA2] ISACA, Transforming Cybersecurity Using COBIT® 5, 2013, www.isaca.org/cybersecurity-cobit

[ISACA3] ISACA, Berufs-Ehrenkodex (in English: Code of Professional Ethics), 2013, www.isaca.org

[ISACA4] ISACA, COBIT® 5 for Information Security, 2012, http://www.isaca.org/cobit5security

7 Safeguard Objectives

Explanation

Assessing the safeguard objectives A to M listed below is mandatory when implementing a cyber security check. The order of the safeguard objectives is thus not be considered as prioritisation or mandatory order to be complied with during the assessment, but solely serves structuring purposes.

In order to assess a safeguard objective, at least the basic safeguards associated with the respective safeguard objective must be used.

The samples for the on-site assessment must be checked according to a risk-oriented approach.

Detailed information on the implementation of a cyber security check can be found in chapter 4 of the „Cyber Security Check“ guide (www.allianz-fuer-cybersicherheit.de).

	Safeguards	Basic safeguards	References
A	**Protection of network gateways** Protecting network gateways is one of the decisive factors for efficiently defending against attacks from the Internet. Based on the network architecture, countermeasures for all internal and external network gateways and the corresponding processes (such as change management) must be planned and implemented.	» All network gateways are identified and documented. » The network is divided into segments and the number of network gateways is kept to a minimum. » All network gateways are secured by suitable security gateways and are checked at regular intervals. » On client and server systems, technical interface control monitoring and controlling admissible use and preventing inadmissible use is carried out. » Accesses of mobile IT devices are adequately secured and limited to the minimum necessary. » Accesses for remote administration and monitoring are adequately secured. » Only up-to-date encryption and authentication procedures are used.	**BSI IT-GSC 13th version:** M 3.301, M 3.302, M 4.1, M 5.14, S 2.204 **COBIT 5:** DSS05.02, DSS05.03, DSS06.06 **ISO/IEC 27001:2005:** A.10.6, A.10.7.1, A.11.4, A.11.6.2, A11.7, A.12.5.4 **ISO/IEC 27001:2013:** A.6.2, A.8.3.1, A.9.1.2, A.13.1 **PCI DSS 3.0:** 1.1, 1.1.2, 1.1.4, 1.1.6, 1.2, 1.2.3, 1.3, 1.3.1-1.3.8, 1.4, 2.2.3, 2.2.4, 4.1, 4.1.1, 8.3, 11.4, 12.3.8, 12.3.9

	Safeguards	Basic safeguards	References
B	**Protection against malware** For the purposes of a staggered defence against attacks by malware (viruses, worms and Trojan horses), the protection must be distributed across a large number of IT systems including the security gateways. As the workstation system, the actual client forms the last line of defence.	» Protection software against malware is used consistently and kept up to date on a continuous basis. » Distributed across different IT systems, several solutions supplied by different providers are used (staggered defence). » IT systems without appropriate protection against malware are isolated in special network segments.	**BSI IT-GSC 13th version:** M 1.6 **COBIT 5:** DSS05.01 **ISO/IEC 27001:2005:** A.10.4 **ISO/IEC 27001:2013:** A.12.2.1 **PCI DSS 3.0:** 5.1, 5.1.1, 5.1.2, 5.2, 5.3, 5.4
C	**Inventory of the IT systems** In order to plan and subsequently implement countermeasures on the IT systems used, a complete inventory of the IT systems and software used must first be performed. Using the resulting inventory list, it must be clarified in particular which different types of systems are used in the organisation.	» The stock of hard- and software has been completely inventoried and is updated continuously. » Versions and patch statuses of operating systems and applications are documented at regular intervals. » There are automated procedures in order to detect unauthorised IT systems and applications.	**BSI IT-GSC 13th version:** S 2.10 **COBIT 5:** APO01.06, BAI03.04, BAI09.01, BAI09.05 **ISO/IEC 27001:2005:** A7.1.1, A.7.1.2 **ISO/IEC 27001:2013:** A.8.1.1, A.8.1.2 **PCI DSS 3.0:** 2.4, 9.7, 9.7.1, 11.1, 11.1.1, 12.3.3, 12.3.4

	Safeguards	Basic safeguards	References
D	**Prevention of open security gaps** In order to minimise the risk of successful cyber attacks, open security gaps must be consistently avoided. Existing security mechanisms of operating systems should therefore be used. In addition, security updates of software used should be tested promptly and subsequently installed. An effective change management process should have been established.	» An efficient vulnerability and patch management process has been established. » Within the software planning framework, the use of stronger defence mechanisms in later software is supported. » Known security gaps are closed quickly by means of workarounds and security updates provided. » Operating systems, server services and applications are hardened prior to commissioning. » A process ensuring secure software development has been established. » When purchasing new hard- and software, security requirements are taken into account.	**BSI IT-GSC 13th version:** M 1.14, S 2.337 **COBIT 5:** APO12.01, BAI02.01, BAI10.02, BAI10.03, BAI10.05, DSS05.03 **ISO/IEC 27001:2005:** A.10.1.2, A.11.5.4, A.12.1.1, A.12.4.1, A.12.5.1, A.12.5.2, A.12.5.3, A.12.6 **ISO/IEC 27001:2013:** A.9.4.4, A.12.1.2, A.12.5, A.12.6, A.14.1.1, A.14.2.2, A.14.2.3, A.14.2.4 **PCI DSS 3.0:** 6.1, 6.2, 6.3, 6.3.1, 6.3.2, 6.4, 6.4.1, 6.4.2, 6.4.4, 6.4.5, 6.5, 6.5.1–6.5.10

	Safeguards	Basic safeguards	References
E	**Secure interaction with the Internet** All processes involving the detection and processing of data and services from the Internet must be protected using suitable safeguards. The respective strength of the protection mechanisms used must take into account the protection requirements of the data processed on the respective IT system, as well as the potential forwarding mechanisms available to an attacker.	» The browser including all extensions (Flash, Java, ActiveX etc.) is equipped with strong security features and is particularly isolated in the event of high cyber security exposure (e.g. Sandbox). » Incoming e-mail traffic is examined centrally for threats, such as malware and phishing attacks. » In order to display documents from external sources, secure display options are used. » Undesired active contents are filtered centrally. » Apps and other Internet applications are secured by means of appropriate protection mechanisms. » There are binding specifications on the secure use of cloud services and other services on the Internet.	**BSI IT-GSC 13th version:** M 5.3, M 5.4, M 5.12, M 5.18, M 5.19, M 5.21, S 2.162, S 2.164, S 2.166, S 5.67, S 2.46, S 3.78, S 5.158 **COBIT 5:** BAI10.02, BAI10.03, BAI10.05, DSS05.01 **ISO/IEC 27001:2005:** A.6.2.3, A.10.4.2, A.10.8.4 **ISO/IEC 27001:2013:** A.13.2.3, A.15.1.2 **PCI DSS 3.0:** 1.4, 6.6, 12.3

	Safeguards	Basic safeguards	References
F	**Logged data recording and analysis** Security incidents often go undetected, since they cause no visible or obvious damage in the short term. However, a well concealed and sufficiently careful approach may enable attackers to control the target systems for extended periods of time without these attacks being detected immediately due to singular events. Therefore, it is necessary to also develop procedures for detecting inconspicuous security incidents and attacks planned for the long term.	» Relevant logged data is recorded completely according to the relevant statutory, regulatory and organisational requirements and evaluated at regular intervals. » The use of privileged accounts and administrative accesses is monitored continuously. » Logged data are adequately protected against manipulation and destruction.	**BSI IT-GSC 13th version:** M 5.22, S 2.64 **COBIT 5:** APO11.04, DSS05.07 **ISO/IEC 27001:2005:** A.10.10 **ISO/IEC 27001:2013:** A.12.4 **PCI DSS 3.0:** 10.1, 10.2, 10.2.2-10.2.7, 10.3, 10.3.1-10.3.6, 10.5, 10.5.1-10.5.5, 10.6, 10.6.1-10.6.3, 11.4
G	**Securing an up-to-date level of information** The ability to plan efficient cyber security safeguards is predominantly determined by the quality and the scope of your own level of information. Therefore, the provision of up-to-date and technically reliable information about cyber security must be ensured.	» Current information on cyber security is continuously obtained from reliable sources and analysed. » Based on the information available, cyber security safeguards are checked and adjusted with respect to their effectiveness at regular intervals.	**BSI IT-GSC 13th version:** M 1.13, S 3.5, S 3.11, S 3.38, S 3.43, S 3.59, S 3.62, S 3.71, S 3.73 **COBIT 5:** APO12.01 **ISO/IEC 27001:2005:** A.6.1.7, A.13.1.2 **ISO/IEC 27001:2013:** A.6.1.4, A.16.1.3 **PCI DSS 3.0:** 6.1

	Safeguards	Basic safeguards	References
H	**Management of security incidents** Suitable processes and procedures governing the management of security incidents must be established and drilled in order to ensure the fast and adequate management of security incidents, thus maintaining continuous business operations.	» There are established processes and procedures governing the fast and adequate handling of security incidents. » The management of security incidents is drilled at regular intervals. » Completed security incidents are evaluated regarding their causes and possible consequences. » Security incidents are reported to responsible government agencies for criminal prosecution purposes and in order to assess the situation.	**BSI IT-GSC 13th version:** M 1.8 **COBIT 5:** DSS02.02, DSS02.02, DSS04.03, DSS05.01 **ISO/IEC 27001:2005:** A.13.1, A.13.2 **ISO/IEC 27001:2013:** A.16.1 **PCI DSS 3.0:** 12.10, 12.10.1-12.10.6
I	**Secure authentication** For the secure authentication of users, complex passwords and/or multi-factor authentication procedures should be used. Authentication data for areas with different protection requirements should be separated from each other.	» The access to critical resources is secured by using multi-factor authentication procedures. » Authentication data for areas with different protection requirements are separated from each other, e.g. accounts of administrators from accounts of other users. » Only secure authentication protocols are used. » Authentication data is protected adequately.	**BSI IT-GSC 13th version:** M 5.15, S 2.6, S 2.7, S 2.8, S 4.133, S 4.176, S 4.250, S 4.392, S 5.59, S 5.160 **COBIT 5:** DSS05.04, DSS06.03 **ISO/IEC 27001:2005:** A.11.1.1, A.11.5.1, A.11.5.2 **ISO/IEC 27001:2013:** A.9.1.1, A.9.4.2 **PCI DSS 3.0:** 8.2, 8.2.1-8.2.6, 8.3, 8.4, 8.5, 8.5.1, 8.6

	Safeguards	Basic safeguards	References
J	**Guarantee of the availability of the required resources** To counter threats of cyber security effectively, the organisation should supply sufficient financial and personnel resources and, if required, fall back on qualified external service providers.	» Sufficient financial and personnel resources to counter the threats of cyber security are available. » If required, qualified and reliable external service providers are involved.	**BSI IT-GSC 13th version:** S 2.1, S 2.2, S 2.193, S 2.226, S 2.337, S 2.339, S 3.3, S 3.51, S 4.392, S 5.59, S 5.160 **COBIT 5:** APO07.01, APO10.02 **ISO/IEC 27001:2005:** A.6.1.3 **ISO/IEC 27001:2013:** A.6.1.1 **PCI-DSS:** 12.4
K	**Performance of user-oriented safeguards** The organisation's own personnel must also be taken into consideration in a cyber security strategy. All technical precautions could become ineffective due to human errors or deliberate improper handling.	» Users and IT personnel are sensitised at regular intervals to the risks of a cyber attack in a way tailored to specific target groups and trained regarding the correct behaviour. » IT personnel and management are familiar with their roles and responsibilities. » There is a clear division of roles. The concentration of too many responsibilities in on role is avoided.	**BSI IT-GSC 13th version:** M 1.13, S 2.1, S 2.225, S 3.51 **COBIT 5:** APO07.02, APO07.03, DSS05.04, DSS06.03 **ISO/IEC 27001:2005:** A.8.2.2, A.10.1.3, A.15.1.5 **ISO/IEC 27001:2013:** A.6.1.2, A.7.2.2 **PCI DSS 3.0:** 6.4.2, 7.1, 7.1.1-7.1.4, 12.4.1, 12.6, 12.6.1, 12.6.2

	Safeguards	Basic safeguards	References
L	**Secure use of social networks** The awareness-raising programme for employees must in particular include their behaviour in social networks in the form of binding specifications (Social Media Guidelines) and educational measures.	» There are binding specifications (Social Media Guidelines) governing the secure and reputable presences of the organisation as well as the professional profiles of the employees in social networks. » Employees are sensitised at regular intervals regarding the risks and the correct behaviour when using social networks. » Direct interfaces between social networks and the organisation's own infrastructure, if any, are adequately secured.	**BSI IT-GSC 13th version:** S 3.5, S 5.157 **COBIT 5:** APO07.03 **ISO/IEC 27001:2005:** A.7.1.3, A.8.2.2,A.10.8.1 **ISO/IEC 27001:2013:** A.7.2.2, A.8.1.3, A.13.2.1, A.13.2.3 **PCI DSS 3.0:** n/a
M	**Performing penetration tests** Regular penetration tests of qualified and experienced people, who were not involved in the planning or implementation of the IT systems to be assessed, are performed.	» Penetration tests are performed by qualified personnel at regular intervals. » The scope and intensity of the penetration tests correspond to the cyber security exposure. » The results of the penetration tests are used consistently in order to reduce risks.	**BSI IT-GSC 13th version:** S 5.150 **COBIT 5:** APO12.01 **ISO/IEC 27001:2005:** A.6.1.8, A.15.2.2 **ISO/IEC 27001:2013:** A.14.2.8, A.18.2.1, A.18.2.3 **PCI DSS 3.0:** 11.3, 11.3.1-11.3.3

Imprint

Published by
Federal Office for Information Security – BSI
Godesberger Allee 185-189
D-53175 Bonn (Germany)
E-mail: bsi@bsi.bund.de
Internet: www.bsi.bund.de
www.bsi-fuer-buerger.de · www.facebook.com/bsi.fuer.buerger
www.allianz-fuer-cybersicherheit.de

Source of supply
Federal Office for Information Security – BSI
Godesberger Allee 185-189
D-53175 Bonn (Germany)
E-mail: info@cyber-allianz.de
Internet: www.bsi.bund.de
Phone: +49 (0) 22899 9582 - 0
Fax: +49 (0) 22899 9582 - 5400

As per
March 2014

Printed by
WM Druck + Verlag
D-53359 Rheinbach (Germany)

Texts and editing
Federal Office for Information Security – BSI

Article number
BSI-BroAfCS14/002

www.bsi.bund.de