Allianz für Cyber-Sicherheit

VDMA

ZVEI: Die Elektroindustrie

INTERNATIONAL DATA SPACES ASSOCIATION

industrial internet CONSORTIUM

Guide
Cyber Security Check

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

Version 2

ISACA Germany Chapter

dpunkt.verlag

Publisher:
ISACA Germany Chapter e. V.
Storkower Straße 158
D-10407 Berlin

www.isaca.de
info@isaca.de

Team of authors:
- Dr. Peter Ebinger
- Martin Ennenbach
- Sebastian Fritsch
- Tobias Glemser
- Arne Günther
- Markus Lörsch
- Markus J Neuhaus
- Armin Nilles
- Jan Oetting
- Holger Pfeiffer
- Peter Reiner
- Jan Rozek
- Dr. Tim Sattler
- Dirk Schugardt
- Christian Schwartz
- Andreas Teuscher
- Dr. Karl-Friedrich Thier
- Dr. Jens Vykoukal
- Gregor Wittkowski

The latest version of this guide is available free of charge on the ISACA chapter Germany website: *https://www.isaca.de/de/veroeffentlichungen/cyber_security*.

Edition: February 2020

Guide
Cyber Security Check

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

Version 2

ISACA®
Germany Chapter

Alliance for Cyber Security

The Alliance for Cyber Security 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 enhancing cyber security in Germany and strengthening the resilience of Germany against cyber attacks. The Alliance for Cyber Security supports the exchange of information and experiences between the different players from industry, administration, associations, such as ISACA Germany Chapter e. V., 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. As an example, by reporting to the BSI, which new threats or IT security incidents their organization are confronted with, they contribute to the development of a greatly improved 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.

Preface

German Electrical and Electronic Manufacturers Association (ZVEI)

Hundreds of thousands of new malware variants are registered daily; botnets execute denial-of-service attacks with up to 300 Gbit/s, and ransomware attacks cause increasingly often computer and network failures at companies, government agencies and private users. In an increasingly networked world, cyber security has never played a more important role.

For this reason, ZVEI supports the revised guide "Cyber Security Check' as a co-publisher. The publication provides essential knowledge in an accessible format: The cyber security check facilitates a quick assessment of risks and provides a basis for defining specific security controls in a detailed manner. Small companies in particular can thus identify risks in the cyberspace more easily.

As a cross-cutting topic, cyber security permeates all leading markets of ZVEI – from Industry 4.0, mobility and health to energy and buildings. The association wishes to raise due awareness at enterprises, their employees, in politics and among the citizens. The aim is to strengthen the security culture within the electronics industry and thus to build trust.

ZVEI's political work includes the support of cyber security-related legislative initiatives in Germany and Europe and practical regulations, which ideally should be harmonized on a European level.

The exchange of information and experiences – between ZVEI and its members, with government agencies such as the Federal Office for Information Security (BSI) or in networks such as the Alliance for Cyber Security (ACS) – is essential. Small- and medium-sized enterprises in particular benefit greatly from the expert knowledge.

The cyber security check meets strong demand: In recent years, over 450 persons have been trained and certified to perform these checks. In addition, many companies without an explicit certification have autonomously performed internal cyber security checks based on this guide. Each successful and efficient check raises the level of protection:

"Cyber security is essential to the protection of the state, economy and society. Only together can we master the challenge of networked data and systems."

Dr. Klaus Mittelbach
Chief Executive Officer
ZVEI – German Electrical and Electronic Manufacturers' Association

Mechanical Engineering Industry Association (VDMA)

The mechanical and plant engineering industry is in the middle of a digital transformation. Digital business models and the global networking of machines must be developed and operated in a cyber-secure manner. One third of the VDMA members have been affected by production downtime due to security incidents, so far. The business value of security is now firmly on the radar of the management boards of our 3,200 members.

The mostly medium-sized companies need practical support in the assessment of security risks and protection against these. The cyber security check provides a suitable solution to the industry's demand and has been developed with the objective of quickly assessing cyber security risks. The present guide will help the German mechanical and plant engineering industry to operate globally in a secure manner also in the future. With over 450 trained persons, the cyber security check is a good example of successful cooperation between government agencies, companies and the security industry.

Last but not least, the Alliance for Cyber Security, sponsored by VDMA, provides an excellent information network to VDMA members. Together with our partner associations from the industrial and crafts sectors, we are working in the Alliance and the VDMA Competence Center Industrial Security on our contribution to cyber-secure machinery and services.

"We need a lot more cyber resilience. Absolute security does not exist. However, preparing for an emergency builds trust among employees and business partners."

Thilo Brodtmann
Managing Director
Mechanical Engineering Industry Association

Federal Office for Information Security (BSI)

Digitization affects us day after day: While numerous processes at our institutions have been automated and networked, new potentials for the IT projects and business models of tomorrow have been opening up at the same time, for example, in connection with the subject of the future "artificial intelligence". Technological development knows no rest and demands a great deal of decision-makers, administrators but also developers. Driven by this fast-paced change, we must not neglect security considerations. After all, IT governs today not only the daily operations of companies and government agencies but also our very lives if we look at critical infrastructures. This dependency will further increase with self-driving vehicles and other developments. The IT failures at hospitals in September 2019, for example, showed the scope that cyber attacks could have. The BSI situation report has established a high risk potential for private users, companies and government agencies. These threats are produced by increasingly professional perpetrators developing sophisticated malware, such as Emotet. There is a long victims list; in many cases, there has been massive damage, in some cases, there have even been business closures.

In view of this situation, sound risk management must not only be a standard feature of corporate governance today but also include cyber threats and cyber security controls. ISACA und BSI have been cooperating closely since 2014 to raise the awareness for cyber security among the relevant stakeholders and to develop practical guidelines to determine the status quo. The fact that this document is the second edition of the guide is only one of the numerous indicators of the successful cooperation. More than 450 certified Cyber Security Practitioners prove that the demand for cyber security experts including at companies and government agencies is continuously increasing.

With this new edition, ISACA and BSI take account of the rapid change in the cyber world. Topics such as cloud computing have gained major importance in recent years and have therefore received particular attention in this guide. At the same time, the basic IT controls have been substantially revised. The new possibilities of this proven methodology have also been included in the new edition.

"I am pleased that you are addressing this topic and I wish for this guide to assist you in the optimization of your cyber security controls as best as possible."

Arne Schönbohm
President
Federal Office for Information Security (BSI)

International Data Spaces Association (IDSA)

Data is the raw material for innovation – especially for artificial intelligence, the Internet of Things and Big Data. For data to reach its full potential, it must be made available in business ecosystems across companies and industries and linked to form data value chains.

The International Data Spaces Association (IDSA), as a non-profit organisation with over 100 member companies from 20 countries, defines a reference architecture in cross-industry working groups and industry-specific communities and a formal standard for data sovereignty in virtual data spaces.

Data sovereignty is based on the premise that the data at every level of the data value chain have been assigned clearly defined usage rights. This requires technical infrastructure and includes contractual regulations: Data linkage or data analysis may be prohibited or permitted; third parties may be forbidden or authorized to access data.

In order to adequately protect data spaces against attacks from cyberspace, we need technical and organisational measures (TOMs). The so-called IDS Connector, the endpoint at which a company makes data available to the ecosystem according to its terms, makes this technically and semantically possible. The technical requirements have been defined in the DIN SPEC 27070 standard. As for the organisational requirements, the Cyber Security Check guide can provide an introduction especially for usage of data spaces by medium-sized businesses. This down-to-earth approach combined with the risk assessment and recommendation of controls supports the security commitment of IDSA.

"We need standards and inspiration for secure and trustworthy cleanrooms for data to take the next step in data management towards more innovation and economic success."

Lars Nagel
CEO
International Data Spaces Association

ISACA Germany Chapter e.V.

ISACA Germany Chapter e.V. is the German branch of the world's leading professional association of IT auditors, IT security managers and IT governance officers. The association was founded in 1986 and, with about 3,000 members, is part of the global ISACA association, to which more than 140,000 experts in more than 180 countries worldwide belong.

The aim and purpose of the association is to promote the training of the members and interested parties to develop their auditing and consulting skills in the fields of IT governance, IT auditing, cyber security and internal control systems, to impart this expertise to all members and interested parties through publications and seminars as well as to promote the exchange in these fields between the members, companies and organisations. In addition to this, the association contributes to the promotion of the job profile and the young generation of IT auditors, IT security managers and IT governance officers.

The working groups pool the expertise and knowledge of the ISACA Germany Chapter members and enable the expert community to leverage it. In particular, I would like to thank the members of the Working Group Cyber Security and our partners, without whom this guide would not exist.

"The threats from cyberspace are more real than ever. 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 existing knowledge to be prepared when faced with new attack scenarios."

Andreas Teuscher
ISACA Germany Chapter e.V.
Head of Working Group Cyber Security

Industrial Internet Consortium (IIC)

The IIC is the world's leading organization transforming business and society by accelerating the Industrial Internet of Things (IIoT). By studying in situ industrial settings with respect to the use of IoT in smart cities, healthcare, agriculture, energy systems, smart buildings, manufacturing and other vertical markets we learn best how to build these systems, and then apply those learnings to technology challenges solving real end-user problems with Industrial IoT. We have developed essential guidance for Digital Transformation, and our Industry Connect Services apply that guidance to real-world problems with our members. Besides developing market-leading studies in architecture, artificial intelligence and trustworthiness, we offer a Resource Hub with our guidance packaged into a Project Explorer and other features to help make the digital leap.

Our mission is to deliver a trustworthy IIoT in which the world's systems and devices are securely connected and controlled to deliver transformational outcomes. Knowing the value of data delivered by such a system (and trusting the outcomes) is central to quality implementations and we are proud to present trustworthy solutions like this guide.

"Cyber security is a key component of industrial internet solutions, which might feature thousands or even millions of Internet-connected nodes."

Dr. Richard Mark Soley
Executive Director
Industrial Internet Consortium

Cooperation BSI / ISACA

This guide was jointly developed by the Working Group Cyber Security of ISACA Germany Chapter e.V. and BSI experts.

In order to teach the correct application of the guide, ISACA Germany Chapter e. V. has created the certificate course "Cyber Security Practitioner" *(www.cyber-security-practitioner.de)* within the framework of the Alliance for Cyber Security *(www.allianz-für-cybersicherheit.de)*. The course includes an introduction to the main aspects of cyber security and the current threat situation and an instruction on the practical implementation of the six steps of the cyber security check described in this guide with specific application cases.

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. Based on these and other activities of the expert groups, ISACA Germany Chapter 2019 has been named key member (multiplier) in the Alliance for Cyber Security.

Table of Contents

1 Introduction

Today, business processes depend on the reliable and proper functioning of information and communication technologies. Therefore, many rating agencies already evaluate IT security as part of a company's operational risks. However, the actual threats as well as the impact resulting from successful cyber attacks are not always immediately obvious: For example, know-how theft through unauthorized access to and copying of data does not lead to immediate business interruption and might only be recognized 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 business activities of modern companies with a high degree of dependency on IT can be brought to a complete halt (see, for example, the cyber attacks with WannaCry in May 2017 and with NotPetya in June 2017) – with all the consequences related to this. Recent studies show that advanced persistent threats (APTs) target increasingly ever smaller companies. The opinion that is nevertheless still widespread in many companies "Well, nothing has happened so far" might thus result in serious problems if the existing security concepts are not regularly and adequately adjusted to the changed threat situation.

"Cyber security should be given top priority."

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 risk assessment (see chapter 4.2, step 2) and thus to respond to current threats from cyberspace effectively.

Given the relevance and importance of this topic, all levels, i.e. from the executive/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 guide describes the structured implementation

of a cyber security check at companies and government agencies and can be used by different roles:

- Accountable Managers who have no security expertise can use this document as an orientation aid and as directions for action if they want to initiate or implement a cyber security check.
- 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.
- Auditors and consultants are provided with a practical guide containing specific guidelines and instructions for the implementation of a cyber security check and for the preparation of the report. The standardization 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 basis of each cyber security check are the "Basic Controls for Cyber Security" published by the BSI within the framework of the Alliance for Cyber Security (see chapter 7). As a particularly interesting added value, BSI and ISACA also provide an assignment of the control objectives to be assessed to known standards of information security (IT-Grundschutz, ISO 27001, COBIT, PCI DSS). A sample template for a final report, presenting in compact form both the deficiencies found and the recommendations given for resolving these deficiencies, completes the tools provided for the implementation of a cyber security check.

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". 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.

The Federal Office for Information Security and ISACA Germany Chapter e.V. would like to thank the authors of the ISACA Working Group Information Security for drawing up version 1.0 of this guide: Matthias Becker, Olaf Bormann, Ingrid Dubois, Gerhard Funk, Nikolai Jeliazkov, Oliver Knörle, Andrea Rupprich, Dr. Tim Sattler and Andreas Teuscher.

The revision of version 2.0 of the guide was performed by the ISACA Working Group Cyber Security: Dr. Peter Ebinger, Martin Ennenbach, Sebastian Fritsch, Tobias Glemser, Arne Günther, Markus Lörsch, Markus J Neuhaus, Armin Nilles, Jan Oetting, Holger Pfeiffer, Peter Reiner, Jan Rozek, Dr. Tim Sattler, Dirk Schugardt, Christian Schwartz, Andreas Teuscher, Dr. Karl-Friedrich Thier, Dr. Jens Vykoukal und Gregor Wittkowski.

1.1 The Cyber Security Check Version 2.0

Cyber security has been generally accepted in the digital world of today as the basis for secure services. Organisations and multinational companies are putting a lot of effort into making their networked systems and applications more resilient against cyber attacks. The implementation of all controls seems to be only possible with a lot of resources. How are small and medium-sized organisations and companies supposed to tackle this issue? Answering this question was the objective of the cyber security check of version 1.0. BSI and ISACA worked together to create a guide which would serve as an introduction to cyber security for this target group and help them gradually increase their level of security. The positive response, the continued interest and the success resulting from the application of the guide have motivated the authors to adapt the guide to the new reality. In addition, the large amount of helpful feedback and suggestions for improvement have also been included in this version 2.0.

During the revision of this guide, the authors received many requests to prepare a similar guide for operation technology (OT). We have taken up this idea and will develop a guide on this topic with the support of our partners.

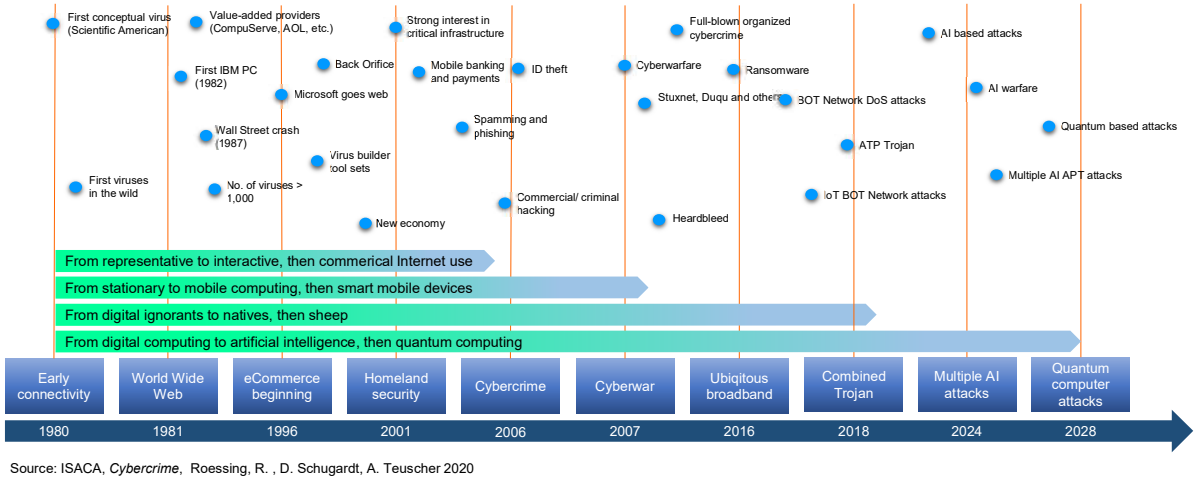
2 Introduction to cyber security

2.1 What is cyber security?

Cyber security, cyber attack, cyber crime and cyber espionage are long known buzzwords in the press and public discussions. This is partly due to technical development, but is mainly due to the continuously growing number of security incidents, criminal acts and new information-based attack methods. The myth that hackers are people with proven specialist knowledge has now given way to the realization that it is mostly well-organised and profit-oriented organisations and groups that are behind the attacks. Consequently, cyber security is becoming an increasingly important facet of information security and must be taken into account by the executive/senior management of an organisation. It requires the use of suitable resources and should be an integral part of enterprise risk management. Checking the existing controls within the framework of a cyber security check to ensure their adequacy can protect organisations and individuals from falling victim to a cyber attack, cyber crime or cyber espionage.

In the context of information security, however, the term "cyber" requires an additional explanation, since it is often misunderstood or generalized. It refers to "cyberspace" as an open space, where information-processing systems are present and connected. With respect to this guide, cyber security covers the protection of interfaces to the information-processing systems of an organisation against threats from cyberspace and, in particular, "the interface" between public cyberspace and controlled business environments.

In practice, cyber security tends to focus on advanced and targeted attacks that are difficult to detect and to defend against (see next section on Advanced Persistent Threats (APTs)). Cyber security is thus also an important part of the general fight against crime, with the perpetrators using information technology deliberately and specifically as a weapon for carrying out their attacks.



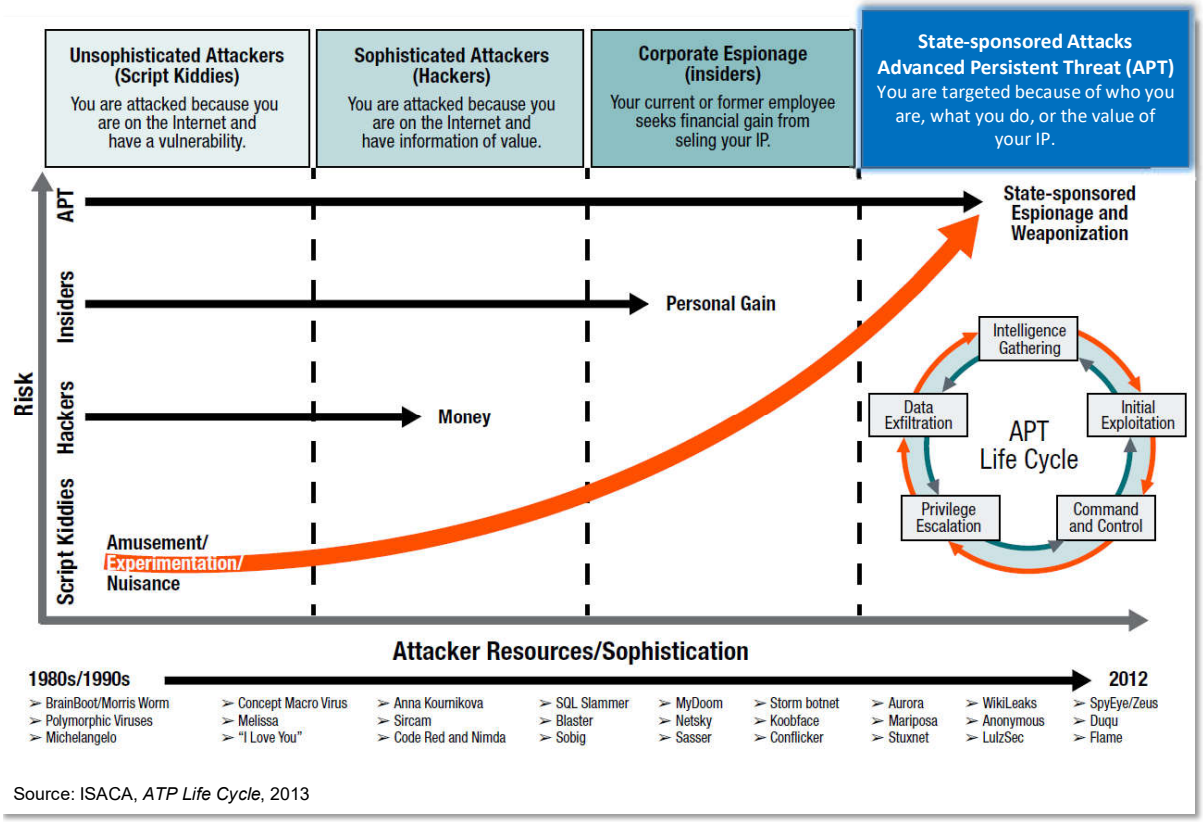
Source: ISACA, *Cybercrime*, Roessing, R. , D. Schugardt, A. Teuscher 2020

Figure 2–1: Developments in cyberspace (based on ISACA)

As shown in Figure 2-1, cyber security has a history dating back to the early 1980s, when criminals started to use technical attacks targeting IT systems in the form of hacking, cracking and malware (e.g. viruses, worms and Trojan horses) for their purposes.

2.2 Cyber attacks and Advanced Persistent Threats (APTs)

Organisations must deal with IT-related threats, risk scenarios and vulnerabilities on a daily basis. Targeted cyber attacks by advanced, well organized and professionally equipped attackers represent the highest threat for companies and government agencies as well as for their partners. This type of attack is often summarized under the term APT (Advanced Persistent Threat) (see [ISACA7]). APTs are often very complex both in preparation and in execution 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. Figure 2-2 shows how threats have developed over time and the motivation behind them.



Source: ISACA, *ATP Life Cycle*, 2013

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

This guide and the underlying control objectives for the assessment have been designed to make APT-based cyber attacks fundamentally more difficult and to strengthen the ability to discover an attack and respond adequately. The risk of falling victim to an APT-based cyber attack cannot be completely excluded, but it can be greatly minimized by regularly implementing a cyber security check. If an organisation has already been victim of an APT attack and/or if an APT attack is suspected, further controls should be implemented beyond those of the cyber security check.

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 organized 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 misuse of identities
- Sabotage of business processes through destructive cyber attacks and Denial-of-Service attacks

Cyber crime, as the entire field of information technology, is highly dynamic. While crime figures in many areas have improved, cyber crime in the narrow sense of the term is continuously increasing. The crime statistics of the Federal Criminal Police Office (BKA), for example, of 2017 recorded a total of 85,960 crimes. This represented an increase of 4.0% year-on-year (2016: 82,649). When evaluating such case figures, it must be taken into account that each illegal act, irrespective of the number of victims, is recorded as only one case. For example, the software manipulation of approximately 1.3 million DSL routers of a German internet provider by malware (Mirai) in November 2016 – despite the seven-digit number of victims – was recorded as only one instance of computer sabotage in the statistics report of the Federal Criminal Police Office (see [BKA17]).

Furthermore, it is assumed that there is a high number of unreported cases, which never appear in statistics: According to a poll[1] of the BSI, 70 percent of the interviewed German enterprises were affected by cyber attacks in 2017. The majority of these attacks (57%) was executed by means of malware. This assessment of the threat situation is supported by the report on the state of IT security[2] of the BSI for 2019.

The effects on society, organisations and person concerned are immense and "non-participation in cyberspace" no longer seems to be a realistic option in the digital age. Rather it must become generally accepted that every organization that operates in cyberspace is inevitably

1. *https://www.bsi.bund.de/DE/Pressemitteilungen/Presse2018/Allianz_digitalundsicher_15022018.html*
2. *https://www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html*

exposed to such attacks. The management of an organisation should bear this in mind when assessing its risks and provide resources to implement adequate controls.

2.4 Cyber security strategy of the German Federal Government

Cyberspace comprises all information infrastructures that can be reached worldwide across territorial borders through the Internet. In Germany, all areas of social and economic life make use of the possibilities provided 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 functioning of information and communication technologies and the Internet.

As part 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 (see [BMI2]), which was adopted by the Federal Government in February 2011 and updated in 2016, 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 established as part of the national security precautions by predominantly civil approaches and controls. For 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

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 provide substantiated statements. This guide and the underlying control objectives for the assessment are based on the proven concept of the three lines of defence but focus entirely on cyber security aspects. Figure 3-1 exemplifies such cyber security-relevant aspects for the respective lines of defense.

Figure 3–1: The concept of three lines of defense

The first line of defense – the executive/senior management of an organisation – must first understand the necessity of cyber security controls, the protection requirements of the business processes as well as their dependencies and threats.

The second line of risk and security management should then analyse the extent to which cyber security risks affect the organisation and its processes and what controls could be implemented to prevent this. The

organisation's risk management function is the first independent body to review and evaluate the decisions of the executive/senior management, albeit without decision-making authority of its own. The final decision on the implementation of security controls remains with the executive/senior management.

The third line of defense is internal or external audit, for example, by IT audit. This is where the cyber security check comes into play, with which an independent and objective assessment of the existing level of security can be made. The assessor supports the organisation in achieving its goals by using a systematic and focused approach to assess cyber-security in the organization and by promoting the optimisation of security controls through their activities.

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 mandate for the cyber security check by the organisation (see ISACA Standard for IS Audit and Assurance 1001 – Audit Charter [ISACA6])
- Independence (see ISACA Standards for IS Audit and Assurance 1002 – Organisational Independence and 1003 – Professional Independence [ISACA6])
- Integrity and confidentiality (see ISACA Standard for IS Audit and Assurance 1005 – Due Professional Care [ISACA6])
- Professional expertise (see ISACA Standard 1006 for IS Audit and Assurance – Proficiency [ISACA6])
- Evidence and traceability (see ISACA Standard for IS Audit and Assurance 1205 – Evidence [ISACA6])
- Objectivity and diligence (see ISACA Standards for IS Audit and Assurance 1207 – Irregularity and Illegal Acts and 1204 – Materiality [ISACA6])
- Objective and factual presentation (see ISACA Standard for IS Auditand Assurance 1401 – Reporting [ISACA6])

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 a corresponding legitimate interest. In the latter case, the assessor must be security cleared and authorized in accordance with the "Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen" (in English: General Administrative Regulation 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 security clearance depends on the degree of confidentiality of the information concerned.

In addition to this guide, the basis for the cyber security check is provided by the two BSI recommendations on cyber security "Basismaßnahmen der Cyber-Sicherheit" (in English: Basic Controls for Cyber Security) (see chapter 7) and "Cyber-Sicherheits-Risikoeinschätzung" (in English: Cyber Security Risk Assessment) (see chapter 4.2, step 2). If there are no statements on specific parts of the subject of the assessment in these publications, other relevant regulations, laws, standards or specifications by manufacturers or professional associations must be used. 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 or 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 significantly by the assessment. The assessor never actively interferes with systems and does not give any instructions for changes to IT systems, infrastructures, documents or organisational procedures. In each case, the assessor only requires read access.

4 Implementation of a Cyber Security Check

4.1 Subject of the assessment

The subject of a cyber security check (CSC) is generally the entire organisation including its connections to the Internet, the connections to the Internet via other organisational units, except for operational technology, as well as all connections to other networks, such as networks of partners, service providers and customers. Control systems, such as fire detection, access control and video monitoring systems, even if they are not directly accessible via the Internet, are also affected by indirect attacks. Manipulated USB flash drives and QR codes are used to prompt these systems to initiate external communication. Physical security (environmental hazards, building security, etc.) is not part of cyberspace and thus plays only a minor role in the cyber security check.

If essential logical IT systems or IT services are excluded from the assessment, this must be documented and justified in the assessment report as assessed delimitation of the subject of the assessment.

4.2 Approach

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

Step 1 – "Assignment"

In order to ensure a comprehensive and effective assessment, the mandate to perform a cyber security check should be given by the executive/senior management of the respective organisation.

Furthermore, to implement a cyber security check, it is not necessary for mandatory documents regarding the security process to exist or for a defined implementation status of specific security controls 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.

Step 2 – "Determining the cyber security risk"

In order to carry out a risk assessment for the organisation to be assessed, the cyber security risk is determined prior to the on-site assessment. This determination includes the calculation of a risk level indicator based on the impact and likelihood of incident occurrence. Based on this, the expected time expenditure, the assessment depth as well as the selection of samples can be determined in a risk-oriented manner.

If the cyber security risk has already been determined by the organisation, the assessor adopt it without carrying out any further activities of their own (provided that the impact and likelihood of incident occurrence have been determined) if they consider it to be understandable and adequate.

If the determination of the cyber security risk for the organisation concerned has not been carried out yet, this should be performed by the organisation or by the assessor in cooperation with the organisation according to the following scheme.

The starting point of the determination of cyber security risk is the determination of impact for each protection target (confidentiality, availability and integrity) according to the following table 4-1.

	Confidentiality		**Availability**		**Integrity**	
Value of data and processes	low normal high very high	0 1 2 3	low normal high very high	0 1 2 3	low normal high very high	0 1 2 3
Impact = value per protection target						

Table 4–1: Determination of the impact

The next step is the determination of the likelihood of incident occurrence according to Table 4-2.

	Confidentiality		Availability		Integrity	
1) Dependency on IT and level of networking (attractiveness for attackers)	local[3] partially networked[4] fully networked[5]	1 2 3	local partially networked fully networked	1 2 3	local partially networked fully networked	1 2 3
2) Expertise (knowledge) of the attackers	general[6] moderate[7] specific[8]	1 2 3	general moderate specific	1 2 3	general moderate specific	1 2 3
3) Attacks in the past	blocked undetected/ successful	1 3	blocked undetected/ successful	1 3	blocked undetected/ successful	1 3
Likelihood of incident occurrence = total of the values for each protection target						

Table 4–2: Determination of the likelihood of incident occurrence

Now, the risk level indicator is calculated for each protection target by multiplying the impact with the likelihood of occurrence (total of the individual values for each protection target).

3. IT-supported processes, which can also be performed manually, in a verifiably closed network without any Internet connection.
4. IT-supported processes, which can be performed manually for a limited period, separate networks with monitored data exchange (remote maintenance) and limited Internet use (e.g. web shop).
5. Completely IT-supported processes, separate networks with controlled data exchange (remote maintenance) and Internet use (e.g. e-mail, Internet search, use of cloud services, mobile applications).
6. The attacker has basic knowledge, resources and tools to access data and processes in an unauthorized manner and to modify or delete them.
7. The attacker has knowledge about the organization and suitable resources and tools to access data and processes in an unauthorized manner and to modify or delete them.
8. The attacker has specific knowledge about the organization, substantial resources and targeted tools to access data and processes in an unauthorized manner and to modify or delete them.

Formula for each protection target (CIA):
(Dependency + Expertise + past Attacks) × Impact = Risk Level Indicator

The highest value of the three risk level indicators is used to determine the cyber security risk and in the subsequent steps of the cyber security check.

This results in the following risk assessments:

normal = 0 – 9

high = 10 – 18

very high = 19 – 27

The cyber security risk assessments (normal, high, very high) is used in the cyber security check to determine the appropriateness of the controls to be assessed within the on-site assessment (step 5) and the report (step 6).

Step 3 – "Document review"

The document review serves to gain an overview of the organisation's tasks, structure and IT infrastructure. The document review merely consists of a rough inspection of the documents provided. In particular, the IT framework, the list of critical business processes, the security policy and the security concept including network plan (if available) are assessed.

If no sufficiently informative documents are available, the document review is supplemented by interviews during which the assessor can gain the required overview. Based on the knowledge gained, the assessor determines the samples and focal points of the assessment in a risk-oriented manner.

Step 4 – "Preparing the on-site assessment"

In preparation for the on-site assessment, a schedule should be drawn up taking the cyber security risk assessment 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 sent 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 an exit meeting. During the opening meeting, the approach and objective 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 process.

As part of the on-site assessment, interviews are conducted, IT systems are inspected and, if necessary, additional documents are reviewed. During the on-site assessment, the contact persons to be interviewed for 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 sufficient detail in order to be able to adequately use this information later for the preparation of the report.

During the exit meeting, in which the organisation's management level should also participate, a first general evaluation of the cyber security level in the organisation is provided. In addition to this, the assessor discloses any serious security deficiencies that pose an immediate and significant threat to the organisation's cyber security and should therefore be addressed promptly.

Step 6 – "Follow-up evaluation / preparing the report"

The cyber security check is concluded with an assessment report. The report provides an overview of the cyber security in the organisation and, in addition to the cyber security risk assessment, contains a list of the deficiencies found. For each control objective (see chapter 7), the respective assessment result should be documented. In the report, general recommendations for dealing with the deficiencies identified are given. These recommendations allow the organisation to determine in which areas additional activities are required to increase the level of cyber security.

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

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 (minimum requirement: Cyber Security Practitioner or equivalent qualification, e.g. CISA or ISO 27001 Lead Auditor native or based on IT-Grundschutz).

In both cases, however, it must be ensured that the approach specified in this guide is used.

4.3 Assessment methods

The term "assessment methods" refers to all actions taken to examine a situation. During a cyber security check, the following assessment methods can be used by the assessor:

- Interview,
- (Visual) inspection of IT systems, sites, premises and objects,
- Observation (perceptions as part of the on-site assessment),
- File analysis (this also includes the analysis of electronic data or statistical evaluations),
- Data analysis (e. g. configuration files, log files, analysis of databases etc.) and
- Survey in writing (e. g. questionnaire).

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

4.4 Mandatory control objectives

The establishment of mandatory control objectives (see chapter 7) is intended to ensure both a consistent high quality of the cyber security check and comparability of the activities of different assessors.

The mandatory control objectives for a cyber security check are based on the "Basismaßnahmen der Cyber-Sicherheit" (in English: Basic Controls for Cyber Security) (see [ACS3]). A detailed description of the mandatory control objectives can be found on the website 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 cyber security risk assessment.

4.5 Assessment scheme

If security deficiencies are identified during a cyber security check, the assessor must determine, when preparing the report at the latest, how the criticality of the deficiencies concerned is to be assessed.

Security deficiencies must be classified as follows:

- **"No security deficiency"**

  At the time of the assessment, no security deficiency could be identified. There is no supplementary information.

- **"Security recommendation"**

  By implementing the control recommendations described in the established facts, the security can be increased. Improvement suggestions for the implementation of controls, additional controls that have been successful in practice or comments regarding the appropriateness of controls can also be listed as security recommendations. Even a fully implemented IT security control can be supplemented by a security recommendation.

- **"Security deficiency"**

  In the event of a „security deficiency", there is a vulnerability which should be resolved in the medium term. The confidentiality, integrity and/or the availability of information may be impaired.

- **"Serious security deficiency"**

  A "serious security deficiency" is a vulnerability which should be resolved immediately, since the confidentiality, integrity and/or the availability of information is exposed to a high risk and substantial 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 assessment report of a cyber security check must be communicated to the executive/senior management of the organisation and/or the client in writing. A draft version of the report should be sent to the organisation assessed in advance in order to verify whether the facts established (only identified facts – without assessments and recommendations) have been recorded correctly and objectively.

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

- the outline data, including the detailed description of the subject of the assessment,
- a summary (Management Summary, including cyber security risk assessment), and
- the detailed assessment (detailed description of the deficiencies identified, their evaluation and recommendations to correct the deficiencies).

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

Part I – Outline Data

This part contains organisational information:

- Subject of the assessment
- The scope of the assessment
- Assessors
- Contact persons of the organisation assessed
- Basis for assessment
- Time schedule
- Distribution list for the assessment report
- Metadata 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 summarized in a brief and understandable manner.

- Summary
- Cyber security risk assessment
- Overview of the assessment results (for all control objectives)

Part III – Detailed Assessment for each control objective

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

- Control objective (see chapter 7)
- Result including evaluation
- Sample(s)
- Description of any deficiencies identified including recommended corrective action(s)

Formal aspects of 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 as well as version number, title and date of the report).
- Any terminology or abbreviations used which are not in general use must be summarized in a glossary and/or index of abbreviations.
- The report must clearly be specifying both the organisational units 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 [ACS4]).

5 Glossary and Definition of Terms

The following terms are used in this document:

APT (Advanced Persistent Threat) refers to a very complex, targeted, elaborately prepared and executed cyber attack (see also chapter 2.2).

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

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

CIA is an abbreviation of the protection objectives confidentiality, integrity and availability

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

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

CSP (Cyber Security Practitioner) is a certificate issued by ISACA Germany Chapter. ISACA offers interested persons a one-day cyber security training course, enabling them to document their knowledge of the main principles of cyber security and the implementation of cyber security checks to the public. After successfully passing an examination, the participant can obtain a certificate as a "Cyber Security Practitioner". The certificate is valid for 3 years and can be renewed by providing proof of completed assessments (confirmation of employer or customer of 6 completed assessments or 3 assessments and 24 CPE points) during this period.

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

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

Cyber security risk is determined based on the impact and likelihood of incident occurrence. The risk level indicator can be used to determine the risk for the enterprise and thus the expected time expenditure, the assessment depth and the selection of samples for the cyber security check.

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

DoS refers to Denial of Service, i.e. the malicious disruption of an internet service that should normally be available.

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

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

IT is the information technology that is used for office communication, administration but also for company-wide resource management, etc.

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.

NIST is the National Institute of Standard and Technology based in the US.

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

OT refers to "operational technology". This is hard- and software used for the controlling and monitoring of production processes (based on NIST).

Whistleblower (also "informant") is someone who discloses information important to the general public 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

[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-Risikoeinschätzung" (in English: Cyber Security Risk Assessment) (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 Controls for Cyber Security) (in German only), *www.allianz-fuer-cybersicherheit.de*

[ACS4] Allianz für Cyber-Sicherheit (in English: Alliance for Cyber Security), Report template for the cyber security check, *www.allianz-fuer-cybersicherheit.de*

[BKA17] Bundeskriminalamt (in English: Federal Criminal Police Office), Bundeslagebericht Cybercrime 2017 (in English: Federal Situation Report on Cyber Crime of 2017), *www.bka.de*

[BMI1] Bundesministerium des Innern (in English: Federal Ministry of the Interior), Nationaler Plan zum Schutz der Informationsinfrastrukturen in Deutschland (in English: National 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), November 2016, *www.bmi.bund.de/cybersicherheitsstrategie*

[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*

[BMWi] Bundesministerium für Wirtschaft und Technologie (in English: Federal Ministry for Economic Affairs and Technology, 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*

[BSI1] Bundesamt für Sicherheit in der Informationstechnik (in English: Federal Office for Information Security), Informationssicherheitsrevision – Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz (in English: Information Security Audit – A Guideline for IS Audits Based on IT-Grundschutz), March 2010, *www.bsi.bund.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/cobit5*

[ISACA3] ISACA, Code of Professional Ethics) 2013, *www.isaca.org*

[ISACA4] ISACA, COBIT® 5 for Information Security, *www.isaca.org/cobit5*

[ISACA5] ISACA, Responding to Targeted Cyberattacks, *www.isaca.org*

[ISACA6] ISACA, IS Auditing and Assurance Standards available as a free download at *www.isaca.org/bookstore/audit-control-and-security-essentials/itaf*

[ISACA7] ISACA, Advanced Persistent Threats: How to Manage the Risk to Your Business, 2013, *www.isaca.org/apt-book*

7 Control Objectives

Assessing the control objectives A to N listed below is mandatory when implementing a cyber security check. In doing so, the order of the control objectives is not to be considered as prioritization or mandatory order to be complied with during the assessment, but solely serves structuring purposes.

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

The samples for the on-site assessment must be examined according to a risk-oriented approach. Detailed information on the implementation of a cyber security check can be found in chapter 4.

Control objectives		Basic controls	References
A	**Securing Network Transitions** Securing network transitions is a decisive factor for efficiently defending against attacks from the Internet. Based on the network architecture, protective measures for all internal and external network transitions and the corresponding processes (such as change management) must be planned and implemented.	- All network transitions are identified and documented. - The network is divided into segments and the number of network transitions is kept to a minimum. - All network transitions are secured by suitable security gateways and are checked at regular intervals. - A technical interface control is implemented on client and server systems, which monitors permissible use and prevents unauthorised use. - Access of mobile IT devices is adequately secured and limited to the minimum necessary. - Access for remote administration and monitoring is adequately secured. - Only up-to-date encryption and authentication methods are used.	**BSI IT-Grundschutz-Kompendium 2/2020:** OPS.1.2.4, OPS.1.2.5, OPS.2.1, OPS.2.2, OPS.3.1, SYS.3.2.1, SYS.3.2.2, SYS.3.2.3, SYS.3.2.4, SYS.4.3, SYS.4.4, NET.1.1, NET.1.2, NET.2.1, NET.2.2, NET.3.1, NET.3.2, NET.3.3, IND.1.A16 **COBIT 2019:** DSS05.02, DSS05.03, DSS06.06 **ISO/IEC 27001:2013:** A.6.2.1, A.6.2.2, A.9.1.2, A.13.1.1, A.13.1.2, A.13.1.3 **PCI DSS 3.2.1 :** 1.1.1, 1.1.2, 1.1.4, 1.1.6, 1.1.7, 1.2.1, 1.2.3, 1.3.1, 1.3.3, 1.4, 2.2.2, 2.2.4, 2.3

Control objectives		Basic controls	References
B	**Protection against malware** For the purposes of a staggered defense 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 users's workplace system, the client forms the last line of defense.	- Protection software against malware is used consistently and kept up to date on a continuous basis. - Distributed across different IT systems, multiple solutions supplied by different providers are used (staggered defense). - IT systems without appropriate protection against malware are isolated in dedicated network segments.	**BSI IT-Grundschutz-Kompendium 2/2020:** OPS.1.1.2, OPS.1.1.3, OPS.1.1.4, SYS.1, SYS.2, SYS.3, IND.1.A12 **COBIT 2019:** DSS05.01 **ISO/IEC 27001:2013:** A.12.2.1 **PCI DSS 3.2.1:** 5.1, 5.2

Control objectives		Basic controls	References
C	**Inventory of IT systems** In order to plan and subsequently implement protective measures on the IT systems used, a complete inventory of the IT systems and software used is necessary. With the help of this inventory, it is particularly important to determine which different types of systems are in use in the organisation.	- The stock of hard- and software has been completely inventoried and is updated continuously. - Versions and patch levels of operating systems and applications are recorded regularly. - Automated procedures exist to detect unauthorized IT systems and applications.	**BSI IT-Grundschutz-Kompendium 2/2020:** ORP.1, SYS.1.5.A10, IND.1.A4, IND.1.A5, CON.4, CON.5, OPS.1.1.6, ORP.1.A7, ORP.1.A8 **COBIT 2019:** APO01.07, BAI03.04, BAI09.01, BAI09.03, BAI09.05 **ISO/IEC 27001:2013:** A.8.1.1, A.8.1.2, A.8.1.3, A.8.1.4 **PCI DSS 3.2.1:** 2.4, 9.7, 11.1, 12.3.3, 12.3.4

Control objectives		Basic controls	References
D	**Prevention of open security vulnerabilities** To minimize the risk of successful cyber attacks, open security vulnerabilities must be consistently avoided. Existing security mechanisms of operating systems should therefore be used. In addition, available security updates of software must be tested and installed promptly. An effective change management process should be established.	- An efficient vulnerability and patch management process is established. - In the context of software planning, the use of stronger defense mechanisms in more current software is advocated. - Known security vulnerabilities are closed promptly by means of workarounds and provided security updates. - Operating systems, server services and applications are hardened prior to commissioning. - A process for secure software development is established. - When purchasing new hardware and software, security requirements are taken into account.	**BSI IT-Grundschutz-Kompendium 2/2020:** ISMS.1, OPS.1.1.2, OPS.1.1.3, OPS.1.1.4, OPS.1.1.6, SYS.1, SYS.2, SYS.3, APP.1, APP.2 APP.3, APP.4, APP.5, IND.1.A17, NET.3.2.A11, **COBIT 2019:** APO12.01, BAI02.01, BAI10.02, BAI10.03, BAI10.05, DSS05.03, DSS05.07 **ISO/IEC 27001:2013:** A.9.4.4, A.12.1.2, A.12.5.1, A.12.6.1, A.14.1.1, A.14.2.2, A.14.2.3, A.14.2.4 **PCI DSS 3.2.1:** 2.2, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7

Control objectives		Basic controls	References
E	**Secure interaction with the Internet** All processes in which data and services from the Internet are retrieved and processed must be secured with suitable controls. The respective strength of the protective mechanisms used must meet the protection requirements of the data processed on the respective IT system, as well as the potential transfer mechanisms available to an attacker.	- The browser including all extensions (Flash, Java, ActiveX etc.) is equipped with strong security features and is particularly isolated (e. g. sandbox) when the cyber security exposure is high. - Incoming e-mail traffic is centrally scanned for threats, such as malware and phishing attacks. - Secure display options are used to display documents from external sources. - Unwanted active content is filtered centrally. - Apps and other Internet applications are secured by suitable protective mechanisms. - There are mandatory provisions for the secure use of cloud services and other services on the Internet	**BSI IT-Grundschutz-Kompendium 2/2020:** CON.7.A8, CON.7.A14, OPS.1.2.4.A7, NET.1.2.A13, ORP.4.A22, ORP.4.A23 **COBIT 2019:** BAI10.02, BAI10.03, BAI10.05, DSS05.01 **ISO/IEC 27001:2013:** A.13.2.1, A.13.2.2, A.13.2.3, A.13.2.4 **PCI DSS 3.2.1:** 1.1, 1.4, 4.1, 6.6, A1

Control objectives		Basic controls	References
F	**Log data recording and analysis** Security incidents often go undetected, since no visible or obvious damage occurs 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 non-obvious security incidents and long-term attacks.	- For the purpose of attack detection, relevant log data is recorded in accordance with applicable statutory, regulatory and organizational requirements and evaluated regularly. - The use of privileged accounts and administrative access is continuously monitored. - Log data is adequately protected against manipulation and destruction, e. g. through offloading to central log management servers.	**BSI IT-Grundschutz-Kompendium 2/2020:** OPS.1.1.5, DER.1.A6, DER.1.A7, DER.1.A8, DER.1.A9, DER.1.A10, DER.1.A11, DER.1.A12, DER.1.A13, DER.1.A14, DER.1.A15, DER.1.A16, DER.1.A17, DER.1.A18, IND.1.A10, IND.1.A15 **COBIT 2019:** APO11.04, DSS05.04, DSS05.07 **ISO/IEC 27001:2013:** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4 **PCI DSS 3.2.1:** 10.1, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.4, 10.5, 10.6

Control objectives		Basic controls	References
G	**Ensuring an up-to-date level of information** The ability to plan effective cyber security controls is predominantly determined by the quality and the scope of your own level of information. Therefore, the provision of up-to-date and reliable information about cyber security must be ensured.	- Current information on cyber security is continuously obtained from reliable sources and evaluated. - Based on the information available, the effectiveness of cyber security controls is regularly reviewed and adjusted.	**BSI IT-Grundschutz-Kompendium 2/2020:** ISMS.1 IND.1.A1, ORP.4.A4 **COBIT 2019:** APO12.01, APO13.02, DSS04.02, DSS05.01 **ISO/IEC 27001:2013:** A.6.1.1, A.6.1.2, A.6.1.4, A.16.1.3 **PCI DSS 3.2.1:** 6.1, 6.2

Control objectives		Basic controls	References
H	**Management of security incidents/ emergencies** 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 handling 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 authorities for criminal prosecution and situational awareness.	**BSI IT-Grundschutz-Kompendium 2/2020:** IND.1.A13, IND.2.7.A5, NET.2.1.A8, NET.2.2.A4, NET.3.2.A12, ORP.1.A10, OPS.1.1.2.A2, OPS.2.1.A14, DER.2.1.A1, DER.2.1.A2, DER.2.1.A3, DER.2.1.A4, DER.2.1.A5, DER.2.1.A6, DER.2.1.A7, DER.2.1.A8, DER.2.1.A9, DER.2.1.A10, DER.2.1.A11, DER.2.1.A13, DER.2.1.A14 **COBIT 2019:** APO12.06, DSS02.02, DSS02.04, DSS04.03 **ISO/IEC 27001:2013:** A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.17.1.1, A.17.1.2, A17.1.3, A.17.2.1 **PCI DSS 3.2.1:** 11.1.2, 12.5.3, 12.10, A1.4

Control objectives		Basic controls	References
I	**Secure authentication** For the secure authentication of users, complex passwords and/or multifactor authentication should be used. Authentication data for areas with different protection requirements should be separated from each other.	- Access to critical resources is secured by using multi-factor authentication. - 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, such as password hashes or private keys, are protected adequately.	**BSI IT-Grundschutz-Kompendium 2/2020:** ORP.4.A9, ORP.4.A10, ORP.4.A12, ORP.4.A13, ORP.4.A21 **COBIT 2019:** DSS05.04, DSS06.03 **ISO/IEC 27001:2013:** A.9.1.1, A.9.1.2, A.9.2.4, A9.3.1, A.9.4.2, A.9.4.3, A.9.4.4 **PCI DSS 3.2.1:** 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.8

Control objectives		Basic controls	References
J	**Ensuring the availability of necessary resources** To counter cyber security threats effectively, the organisation should supply sufficient financial and human resources and, if required, fall back on qualified external service providers.	- Sufficient financial and human resources to counter cyber security threats are available. - If required, qualified and reliable external service providers are involved. - Data backups and recovery tests must be performed regularly.	**BSI IT-Grundschutz-Kompendium 2/2020:** ISMS.1.A1, ISMS.1.A2, ISMS.1.A3, ISMS.1.A4, ISMS.1.A5, ISMS.1.A6, ISMS.1.A8, ISMS.1.A15, OPS.1.1.2.A9, OPS.1.1.2.A10 **COBIT 2019:** APO07.01, APO10.02, APO14.01, APO14.10, DSS4.07 **ISO/IEC 27001:2013:** A.6.1.1, A.2.1.2, A.7.2.1 **PCI DSS 3.2.1:** 6.4.5.4, 12.10.1
Control objectives		**Basic controls**	**References**
K	**Awareness raising and training of employees** The organisation's personnel must also shift into the focus of a cyber security strategy. All technical controls can become ineffective due to human error or deliberate acts.	- Users and IT staff are regularly made aware of the hazards of a cyber attack in a target group-oriented manner and instructed on the correct behaviour. - IT staff and management are familiar with their roles and responsibilities. - There is a clear separation of roles. The concentration of too many responsibilities in one role is avoided.	**BSI IT-Grundschutz-Kompendium 2/2020:** ISMS.1.A8, ISMS.1.A9, ISMS.1.A14, ORP.1.A1, ORP.1.A2, ORP.1.A6, OPS.1.1.2.A10 **COBIT 2019:** APO07.02, APO07.03, APO13.02, DSS05.01, DSS05.04, DSS06.03 **ISO/IEC 27001:2013:** A.6.1.1, A.7.2.2, A8.1.2 **PCI DSS 3.2.1:** 6.4.2, 7.1, 7.2, 12.6

Control objectives		Basic controls	References
L	**Secure use of social networks** The awareness-raising programme for employees must in particular include the behavior in social networks in the form of mandatory provisions (Social Media Guidelines) and educational measures.	- There are mandatory provisions (Social Media Guidelines) governing the secure and reputable appearance of the organisation as well as the professional profiles of employees in social networks. - Employees are regularly made aware of the risks and correct behavior when using social networks. - Direct interfaces between social networks and the organisation's own infrastructure, if any, are adequately secured.	**BSI IT-Grundschutz-Kompendium 2/2020:** APP.1.4.A2, CON.9.A1, CON.9.A2, CON.9.A3, CON.9.A4 **COBIT 2019:** APO07.03 **ISO/IEC 27001:2013:** A.7.2.2, A.8.1.3, A.8.2.3, A.13.2.1, A.13.2.2, A.13.2.3 **PCI DSS 3.2.1:** n/a

Control objectives		Basic controls	References
M	**Performing penetration tests** Regular penetration tests should be carried out by qualified and experienced personnel who have not been involved in the planning or implementation of the IT systems under assessment.	- In order to verify and confirm the effectiveness of technical controls, penetration tests are regularly carried out by qualified personnel. - The scope and intensity of penetration tests correspond to the cyber security risk assessment. - The results of penetration tests are used consistently in order to reduce risks.	**BSI IT-Grundschutz-Kompendium 2/2020:** OPS.1.1.6.A14 **COBIT 2019:** APO12.01, APO13.02, DSS05.02 **ISO/IEC 27001:2013:** A.14.2.8, A.18.2.1, A.18.2.3 **PCI DSS 3.2.1:** 11.3, A3.2.4

Control objectives		Basic controls	References
N	**Secure handling of cloud applications** The cloud applications used should be regularly reviewed and subject to a release process. Inadmissible cloud applications should be blocked; admissible applications should be protected by suitable security controls.	- Mandatory requirements exist regarding the storage, use and processing of data in cloud applications. - Applicable security standards and contractual specifications are enforced against the cloud service provider. - Cloud services are professionally provisioned, managed and monitored. - Employees are regularly made aware of the risks and proper use of cloud applications. - Direct interfaces between cloud applications and the organisation's own infrastructure, if any, are adequately secured.	**BSI-Standard 200-2 V1.0:** Kapitel 10.1.1, insbesondere 10.1.3 **BSI IT-Grundschutz-Kompendium 2/2020:** OPS.2.1.A1, OPS.2.1.A3, OPS.2.1.A4, OPS.2.1.A5, OPS.2.1.A6, OPS.2.1.A7, OPS.2.1.A8, OPS.2.1.A9, OPS.2.1.A10, OPS.2.1.A11, OPS.2.1.A12, OPS.2.1.A13, OPS.2.1.A15 **COBIT 2019:** APO07.03, APO09.01, APO09.02, APO09.03, DSS01.02, DSS01.03, DSS05.02, DSS06.03 **ISO/IEC 27001:2013:** A.15.1.1, A15.1.2, A15.1.3, A15.2.1, A15.2.2, A.18.2.1, A.18.2.2, A.18.2.3 **PCI DSS 3.2.1:** 2.6, 12.8, A1

ISACA Germany Chapter e. V.
Storkower Straße 158
D-10407 Berlin

www.isaca.de
info@isaca.de