IT Security Association Germany

TeleTrusT
Pioneers in IT security.

IT Security Act (Germany) and EU General Data Protection Regulation:

Guideline "State of the art"

Technical and organisational measures

2020

English version

In co-operation with

enisa
European Network
and Information
Security Agency

Acknowledgement

TeleTrusT would like to thank the following individuals for their participation in the TeleTrusT Task Force "State of the art" as well as for their active contribution in this guideline.

Project management

RA Karsten U. Bartels LL.M. - HK2 Rechtsanwälte
Tomasz Lawicki - m3 management consulting GmbH

Authors and participating experts

Alsbih, Amir
Bartels, Karsten U. - HK2 Rechtsanwälte
Barth, Michael - Genua GmbH
Dehning, Oliver - Hornetsecurity GmbH
Dominkovic, Dennis - SEC Consult Unternehmensberatung GmbH
Dubbel, Sascha - CrowdStrike GmbH
Falkenthal, Oliver - CCVOSSEL GmbH
Fischer, Marco - procilon IT-Solutions GmbH
Gehrmann, Mareike - Taylor Wessing Partnergesellschaft mbB
Gora, Stefan - Secorvo Security Consulting GmbH
Heyde, Steffen - secunet Security Networks AG
Jäger, Hubert - Digital Trust Innovations
Kerbl, Thomas - SEC Consult Unternehmensberatung GmbH
Kippert, Tobias - TÜV Informationstechnik GmbH
Kolmhofer, Robert - FH Oberösterreich Studienbetriebs GmbH
Lawicki, Tomasz - m3 management consulting GmbH
Liedke-Deutscher, Bernd - TÜV Informationstechnik GmbH
Maier, Janosch - Crashtest Security GmbH
Menge, Stefan - AchtWerk GmbH & Co. KG
Mühlbauer, Holger - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Müller, Siegfried - MB connect line GmbH
Paulsen, Christian
Robin, Markus - SEC Consult Unternehmensberatung GmbH
Rost, Peter - secunet Security Networks AG
Schlensog, Alexander - secunet Security Networks AG
Wüpper, Werner - Wüpper Management Consulting GmbH

Imprint

Publisher:

IT Security Association Germany (TeleTrusT)
Chausseestrasse 17
10115 Berlin
Tel.: +49 30 4005 4306
Fax: +49 30 4005 4311
E-Mail: info@teletrust.de
https://www.teletrust.de

V 1.7_2020-10 EN

Contents

Principles of the guideline 6

1 Introduction 7
1.1 IT Security Act 7
1.2 German BSI security standards for CI operators in specific sectors 8
1.3 European implications 8
1.4 General Data Protection Regulation 9
1.5 Appropriateness of measures 10

2 Determining the state of technology 11
2.1 Definition 11
2.2 Method for determining the state of technology 12
2.3 Quality assurance process for the guide 13
2.4 Required protection objectives 14

3 Technical and organisational measures (TOMs) 15
3.1 General information 15
3.2 Technical measures 18
3.2.1 Password strength assessment 18
3.2.2 Enforcing strong passwords 20
3.2.3 Multi-factor authentication 21
3.2.4 Cryptographic procedures 24
3.2.5 Disk encryption 25
3.2.6 Encryption of files and folders 25
3.2.7 E-mail encryption 28
3.2.8 Securing electronic data communication with PKI 30
3.2.9 Use of VPNs (layer 3) 32
3.2.10 Layer 2 encryption 34
3.2.11 Cloud-based data exchange 37
3.2.12 Data storage in the cloud 38
3.2.13 Use of mobile voice and data services 39
3.2.14 Communication through instant messenger 41
3.2.15 Mobile Device Management 42
3.2.16 Router security 43
3.2.17 Network monitoring using Intrusion Detection System 45
3.2.18 Web traffic protection 47
3.2.19 Web application protection 48
3.2.20 Remote network access/ remote maintenance 50
3.2.21 Server hardening 52
3.2.22 Endpoint Detection & Response Plattform 54
3.2.23 Using internet with web isolation 56
3.2.24 Attack detection and analysis (SIEM) 58
3.2.25 Confidential computing 60
3.2.26 Sandboxing for malicious code analysis 61
3.2.27 Cyber threat intelligence 63
3.3 Organisational measures 65
3.3.1 Standards and norms 65
3.3.2 Processes 68
3.3.3 Secure software development 76
3.3.4 Process certification 80
3.3.5 Vulnerability and patch management 83
3.3.6 Management of information security risks 85

List of figures

Figure 1: Three-step theory according to the Kalkar decision
Figure 2: Evaluation criteria
Figure 3: Example of state of technology classification
Figure 4: Process outline for evaluating technical measures in chapter 3.2
Figure 5: Structure levels of standards relevant to information security
Figure 6: PDCA model

List of tables

Table 1: Overview of ISO/IEC 27000 series
Table 2: Differentiation of ISO 27001 vs. BSI’s IT basic protection

Principles of the guideline

When the German IT Security Act came into effect in July 2015, the IT Security Association Germany (TeleTrusT) launched the Task Force “State of the art" to provide interested parties with recommended actions and guidelines on the “state of the art" required for technical and organisational measures. To meet this difficult challenge, the Task Force established the following principles for developing, evaluating and updating the guidelines:

1. **Basic understanding of the document**
   These guidelines are intended to provide companies using it and providers (manufacturers, service providers) alike with assistance in determining the “state of the art" within the meaning of the IT Security Act (ITSiG) and the General Data Protection Regulation (GDPR). The document can serve as a reference for contractual agreements, procurement procedures or the classification of security measures implemented.

   These guidelines are considered a starting point for identifying statutory IT security measures. They are not a replacement for technical, organisational or legal advice or assessment in individual cases.

2. **Responsibility for development, evaluation and updating**
   The Task Force “state of the art" and the TeleTrusT working group “Law" are dedicated to answering the question of how to determine the state of the art within the meaning of the law in relation to technical and organisational measures and how to implement statutory requirements.

3. **Understanding the approach**
   The Task Force achieves its results in a transparent process and puts the recommended actions and guidance up for public discussion in a regular updating procedure.

4. **Evaluation procedure**
   The Task Force bases its evaluation on a standardised method that is filled out and published for the individual measures under consideration. The method for evaluating the technology level of technical measures is described in chapter 2.2.

5. **Updating**
   In order to keep pace with technological progress, regular updates and issues of these guidelines are scheduled. Currently the goal is to publish a new version of the guidelines every two years.
   Small adjustments and additions to the guidelines (such as new contributions to technical measures) during the year will appear in the form of revisions to the guidelines.

Instructions for use

These guidelines are considered a starting point for determining statutory IT security measures that correspond to the state of the art. They are not a replacement for technical, organisational or legal advice or assessment in individual cases.

1 Introduction

1.1 IT Security Act

The IT Security Act (ITSiG) has been in effect since 25/07/2015 and is intended to contribute to improvement of the security of information systems in Germany. The regulations of this act serve to protect these systems in terms of current and future threats to the availability, integrity, confidentiality and authenticity of protected goods. According to the explanatory memorandum, the objective of the act is to improve the IT security of companies, increased protection for citizens on the internet and also to strengthen the German Federal Office for Information Security (BSI) and the German Federal Criminal Police Office (BKA) in this context.

The IT Security Act is an omnibus bill, meaning that the law itself was merely an adaptation of various laws for specific sectors. The ITSiG created regulations for critical infrastructures (CI) in the Act on the Federal Office for Information Security (BSI Act) and made statutory changes in the Atomic Energy Act (AtomG), the Energy Industry Act (EnWG), the Telemedia Act (TMG) and the Telecommunications Act (TKG), among others.

The IT Security Law and its explanatory memorandum can be found at the following link: https://www.teletrust.de/it-sicherheitsgesetz.

The ITSiG stipulates the most extensive changes for CI operators and companies that provide telemedia services. Operators of critical infrastructures, pursuant to Section 8a(1) of the BSI Act, shall keep a minimum level of IT security corresponding to the “state of the art". They are also obligated to report certain IT security incidents to the BSI. Classifying a company as a critical infrastructure takes place on two levels. One is to assess whether it can be assigned to a sector inherently classified as critical (sector affiliation) and the other is to assess whether there is a particular relationship to security (significance of consequential errors). The service providers and suppliers of CI operators are also affected indirectly by statutory regulations where the CI operators contractually impose the relevant obligations on them.

Pursuant to Section 10(1) of the BSI Act, the German Federal Ministry of the Interior, Building and Community (BMI) is authorised to issue a regulation specifying which equipment, systems or parts thereof are considered critical infrastructures within the meaning of this law. The significance of the services and their coverage level is taken into account for this process. The German Federal Government approved the adoption of the ministerial regulation put forth by the German Federal Minister of the Interior to determine critical infrastructures based on the BSI Act (BSI-KritisV) on 13/04/2016. The first part of the CI regulation for implementing the IT Security Act subsequently came into effect on 03/05/2016. The second part of the CI regulation was further enacted on 31/05/2017, and finally came into effect on 01/06/2017. The regulation governs the classification of companies as critical infrastructures in the energy, water, food, information technology and telecommunications sectors (basket 1) and the health, finance and transportation and traffic sectors (basket 2).

Pursuant to Section 8a(1) of the BSI Act, operators of critical infrastructures have a period of two years after the decree comes into effect to take adequate technical and organisational measures (TOMs) to prevent disruptions in availability, integrity, confidentiality and authenticity of their IT systems, components or processes that are essential to the functionality of the critical infrastructures that they operate.

Providers of telemedia services shall guarantee, pursuant to § 13(7) of the TMG that their technical equipment is protected by TOMs within their technical and economic means. The “state of the art" must be taken into consideration when choosing these TOMs. Incidents are not required to be reported. This affects any company that operates a telemedia service. The provisions of the Telemedia Act do not stipulate any transitional periods or exemptions for micro-entrepreneurs, in comparison with the CI regulations.

1.2 German BSI security standards for CI operators in specific sectors

The ITSiG requires CI operators to comply with or at least consider the “state of the art" of IT security measures. However, this level of security is not specified further in the law. It is permitted, however, for CI sectors to propose security standards for specific sectors (“B3S" hereafter). It is up to the BSI to approve the security standards for specific sectors proposed by representatives of the sectors.

The first indications for developing the B3S can be found by the CI operators and associations in question in the draft published by the BSI for a “Guide to the contents and requirements of B3S as per Section 8a(2) of the BSI Act"[1]. The draft provides the following methodology:

1. Definition of the scope and protection objectives of the B3S.
2. Assessment of the vulnerabilities in the specific sector.
3. Performance of a risk analysis for the vulnerabilities in the specific sector.
4. Derivation of suitable and adequate measures for the specific sector.

According to this, the B3S should be helpful in choosing adequate measures by indicating provisions and measures based on “best practice" typical for the sector. The B3S should also demonstrate its boundaries where needed, e.g. if “more" protection and thus additional measures are needed and recommend these additional provisions and measures.

Regarding the question of adequacy, the economic expense required for the CI operator must be taken into account first and foremost, especially the costs of implementation that would be required to spend. Finally, the “expense required" for implementation “should not be disproportionate to the consequences of a failure or damage to the critical infrastructure in question[2]." Whether a measure is adequate or economical, however, can only be determined on an individual basis in consideration of their unique protection needs and implementation costs for any measures required.

The guide then cites a list of topics (such as asset management, suppliers, service providers and third parties) that the B3S must cover. The CI operators and associations in question subsequently receive further information about the level of detail at which proposals in the B3S must be described. Finally, the guide mentions other options for verifying implementation.

The guide once again clarifies that establishing a minimum standard for a certain sector depends on a number of individual factors. An exact determination of the minimum standard must therefore be made based on individual conditions. This especially applies to regulated sectors that are subject to special statutory regulations, such as the Telecommunications Act.

A sector-specific standard (B3S WA) in the water and sanitation sector was defined and approved by the BSI for the first time on 01/08/2017. The B3S WA is comprised of a information sheet and an IT security manual that are updated on a yearly basis. The B3S WA is based on the BSI’s Basic protection catalogue (IT Grundschutz) and security requirements for the specific sector.

However, it remains unclear which criteria were used to select the proposed security standards for the water sector and which criteria were then used by the BSI to approve it as the “B3S WA" within the meaning of “state of the art."

1.3 European implications

Other European guidelines are being added to the BSI Act. For this purpose, the European Commission has adopted the directive concerning measures for a high common level of security of network and

[1] "Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG"; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/b3s_Orientierungshilfe.html.

[2] § 8a(1)(3) BSIG

information systems across the European Union (NIS Directive), which is to be implemented in domestic law. This does not result in any fundamental changes, as national legislature have already anticipated a majority of the requirements intended by European lawmakers in adopting the ITSiG. The corresponding NIS Directive Implementation Act adopted on 27/04/2017 thus merely results in an expansion of the BSI Act.

Section 8c of the BSI Act was created based on the Directive, among other things, to create additional obligation on the part of providers of "digital services." Digital services are subsequently online marketplaces, online search engines and cloud computing services of a normalised value. These services must also implement technical and organisational measures (TOMs) to ensure IT security that take the state of the art into consideration. The measures are intended to guarantee an adequate level of protection commensurate with the risk and, in doing so, take into consideration the security of systems and plants, the handling of security incidents and business continuity management.

1.4 General Data Protection Regulation

The European General Data Protection Regulation (GDPR) was adopted in 2016 and came into effect permanently on 25/05/2018. The primary goal of the GDPR is to protect the personal data of European citizens. At the same time, the Regulation is based on a risk-based approach in terms of its protection objectives. Appropriate technical and organisational measures must be taken to protect the rights and freedoms of natural persons in the area of technical data protection. These must also take the "state of the art" criterion into account. In particular, Article 32 of the GDPR, which governs the security of processing and supersedes Section 9 of the German Federal Data Protection Act (BDSG) along with its appendix 1, stipulates that the "state of the art" must be taken into consideration as part of data processing security. To this end, controllers and processors must take appropriate technical and organisational measures. As well as the ITSiG, the GDPR does not provide a definition for the "state of the art" criterion. The same is also true of the EU Data Protection Adaptation and Implementation Act (DSAnpUG-EU) and the revised version of the BDSG resulting therefrom (BDSG-new).

Furthermore, pursuant to Article 25 of the GDPR, the principles of data protection must be observed through data protection by design (privacy by design) as well as through data protection by default (privacy by default). These principles must also be implemented through appropriate technical and organisational measures.

However, the "state of the art" should not only be taken into consideration when implementing the guidelines, but also be fully documented. Comprehensive and far-reaching documentation requirements, especially the requirement to perform a data protection impact assessment and the principle of accountability, were created for this purpose. The Regulation sets out documentation requirements regarding this matter as its own legal obligations. Thus, technical and organisational measures must be individually established as well as described in detail and documented.

1.5 Appropriateness of measures

The “state of the art" described in this guide (or “STOA" hereafter) focuses on the content demanded by the ITSiG and the GDPR. However, it is permissible within the context of IT security and data protection legislation to take economic factors into account as well, among other things, when choosing protective measures[3]. Whether a measure is economic, though, can only be determined by individual examination of the unique protection needs and the implementation costs required by the measures. Therefore, the performance audit has been left out of this guide.

[3] See Bartels/Backer, Die Berücksichtigung des Standes der Technik in der DSGVO, DuD 4-2018, 214, for the requirements of legal "consideration”

2 Determining the state of technology

2.1 Definition

The “state of the art" of technology[4] must be defined in terms of content separately from similar terms regarding state of technology, such as the “generally accepted rules of technology" (“GART" hereafter) and “existing scientific knowledge and research" (“ESKaR" hereafter)[5] and must be independently measurable. This distinction is the essential basis for defining the required state of technology. As many examples from practice show, these three terms are mixed up or even confused in equal measure in case law and in the public.[6]

These three terms were introduced with the Federal Constitutional Court’s Kalkar decision[7] in 1978, as was the “three-step theory" as a consequence thereof. Based on this decision, the three states of technology can be graphically depicted something like this:

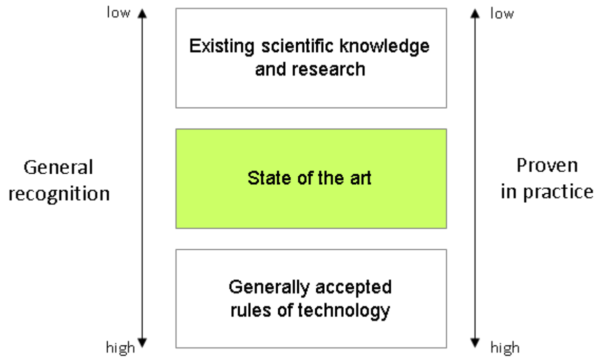

low
Existing scientific knowledge and research
low
General recognition
State of the art
Proven in practice
Generally accepted rules of technology
high
high

Figure 1: Three-step theory according to the Kalkar decision

The “state of the art" technology level is situated between the more innovative “existing scientific knowledge and research" technology level and the more established “generally accepted rules of technology" level. These three states of technology are flanked by the categories “general recognition" and “proven in practice."

The classification of the laws requires a clear distinction between subjective and objective criteria. The “state of the art" criterion is purely objective. The subjective aspects take into account the laws in the event of an offence; however, they do not concern the definition of the “state of the art" itself.

As a result, the “state of the art" can be described as the procedures, equipment or operating methods available in the trade in goods and services for which the application thereof is most effective in achieving the respective legal protection objectives.[8]

In short it can be said that the “state of the art" describes a subject’s best performance available on the market to achieve an object. The subject is the IT security measure; the object is the statutory IT security objective.

[4] The term "level of technology” is used as a substitute for "state of technology.”
[5] "Existing scientific knowledge and technology” can be used alternatively. "Existing scientific knowledge and research” will subsequently be used in this guide so that a distinction can be made between this and "state of the art.”
[6] Dr Mark Seibel, Higher Regional Court Judge, https://www.dthg.de/resources/Definition-Stand-der-Technik.pdf
[7] BVerfGE, 49, 89 (135 f)
[8] Bartels/Backer, Die Berücksichtigung des Stands der Technik in der DSGVO, DuD 4-2018, 214; Bartels/Backer/ Schramm, Der "Stand der Technik" im IT-Sicherheitsrecht, Tagungsband zum 15. Deutschen IT-Sicherheitskongress 2017, Bundesamt für Sicherheit in der Informationstechnik, 503.

Technical measures at the “existing scientific knowledge and research" stage are highly dynamic in their development and pass into the “state of the art" stage when they reach market maturity (or at least are launched on the market). The dynamics dwindle there, e.g. due to process standardisation. Technical measures at the “generally accepted rules of technology" stage are also available on the market. Their degree of innovation is diminishing, though they have been proven in practice and are often described in corresponding standards.

A shift across the individual states of technology can be observed due to progress (“innovative shift").

1. A measure will initially reach the “existing scientific knowledge and research" stage at its origin.
2. When introduced on the market, it will pass to the “state of the art" stage,
3. and as it is distributed and recognised more widely on the market, it will at some point be as signed to “generally accepted rules of technology."

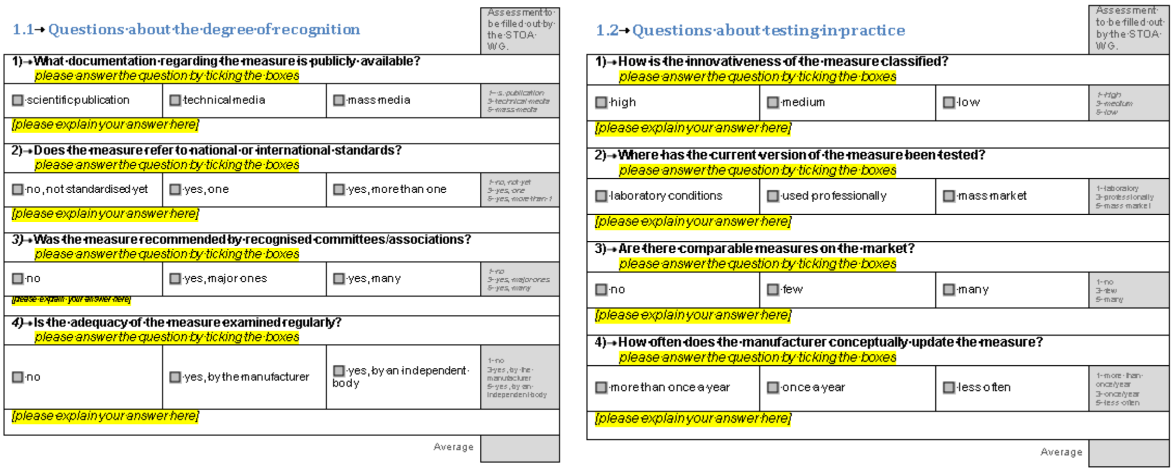
In order to provide the required evidence based on the orientation of their own measures at the “state of the art" level, it is not sufficient to evaluate the measures implemented once and update by installing patches. This sort of evidence can only be successful by comparing the measure implemented with the alternatives available on the market at regular intervals by means of transparent methods.

2.2 Method for determining the state of technology

The technical measures described in chapter 3.2 of this guide were evaluated using a practicable method based on a simple principle of answering central questions about the “degree of recognition" and “degree of proof in practice." The central questions used were deliberately worded simply and allow for a more detailed view of the two dimensions of the examination.

There are three possible answers for each of the central questions. The answers were chosen to allow classification into one of the three levels of technology. Each answer must also be justified. Although the individual questions allow classification into one of the three levels of technology, each of them only covers partial aspects, which means a measure’s state of technology is first determined by answering all the questions for both dimensions.

The following figure shows the template used by the Task Force “state of the art" for all central questions to evaluate the state of technology for a technical measure:



1.1 → Questions about the degree of recognition

			Assessment to be filled out by the STOA WG.
1) → What documentation regarding the measure is publicly available? *please answer the question by ticking the boxes*			
□ scientific publication	□ technical media	□ mass media	*1 - s. publication 3 - technical media 5 - mass media*
[please explain your answer here]			
2) → Does the measure refer to national or international standards? *please answer the question by ticking the boxes*			
□ no, not standardised yet	□ yes, one	□ yes, more than one	*1 - no, not yet 3 - yes, one 5 - yes, more than 1*
[please explain your answer here]			
3) → Was the measure recommended by recognised committees/associations? *please answer the question by ticking the boxes*			
□ no	□ yes, major ones	□ yes, many	*1 - no 3 - yes, major ones 5 - yes, many*
[please explain your answer here]			
4) → Is the adequacy of the measure examined regularly? *please answer the question by ticking the boxes*			
□ no	□ yes, by the manufacturer	□ yes, by an independent body	1 - no 3 - yes, by the manufacturer 5 - yes, by an independent body
[please explain your answer here]			
		Average	

1.2 → Questions about testing in practice

			Assessment to be filled out by the STOA WG.
1) → How is the innovativeness of the measure classified? *please answer the question by ticking the boxes*			
□ high	□ medium	□ low	*1 - high 3 - medium 5 - low*
[please explain your answer here]			
2) → Where has the current version of the measure been tested? *please answer the question by ticking the boxes*			
□ laboratory conditions	□ used professionally	□ mass market	1 - laboratory 3 - professionally 5 - mass market
[please explain your answer here]			
3) → Are there comparable measures on the market? *please answer the question by ticking the boxes*			
□ no	□ few	□ many	1 - no 3 - few 5 - many
[please explain your answer here]			
4) → How often does the manufacturer conceptually update the measure? *please answer the question by ticking the boxes*			
□ more than once a year	□ once a year	□ less often	1 - more than once/year 3 - once/year 5 - less often
[please explain your answer here]			
		Average	

Figure 2: Evaluation criteria

An average score is generated using a point system based on the answers given. The values obtained allow the measures to be displayed in the diagram.

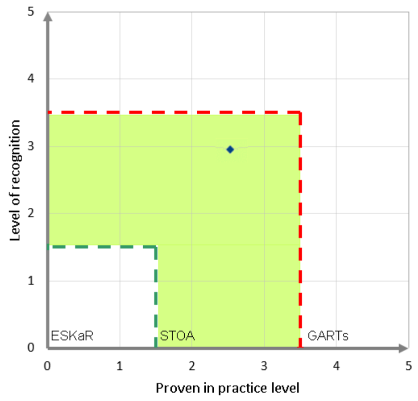


Figure 3: Example of state of technology classification

As can be seen in the diagramm, a measure is assigned to the "state of the art" state of technology if it is within the green field based on the methods used.

In this guide, technologies and methods are described and evaluated, but no particular security products. Therefore, the suitability of the measures described here is deemed to be fulfilled for the respective purpose, for example.

In business practice, a suitable method (e.g. similar to those outlined here) should be adapted to the existing circumstances in the company in order to evaluate the measures implemented objectively, compare them to alternatives and document them for evidence.[9]

2.3 Quality assurance process for the guide

The Task Force “state of the art" is striving to ensure a high quality of the contents in the guide. To succeed at this, a process was established in the STOA WG in which contributions must be successful in several stages:

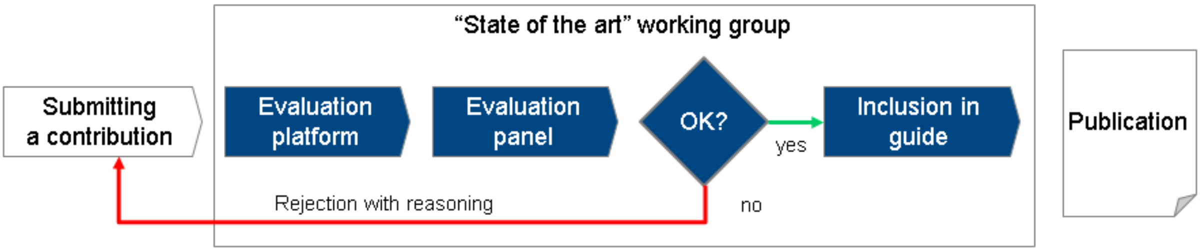


Figure 4: Process outline for evaluating technical measures in chapter 3.2

After a new or modified contribution is submitted in a standardised template (see figure 3), the contribution is evaluated anonymously by IT security experts through an evaluation platform.

The results of this are discussed and agreed upon by the Task Force “state of the art" regular evaluation panel[10]. The central questions defined in the template and their answers serve as evaluation criteria, among others, along with technical correctness and the currency of the contents.

[9] Lawicki, "Was bedeutet "Stand der Technik?", published in the TeleTrusT special supplement "Sicherheit & Datenschutz" in the magazine iX 6/2018

[10] A list of the members active in the Task Force (evaluation panel) is published on TeleTrusT’s webpage: https://www.teletrust.de/arbeitsgremien/recht/stand-der-technik/
(English version: https://www.teletrust.de/en/arbeitsgremien/recht/task-force-state-of-the-art-in-it-security/)

If the evaluation panel comes to the conclusion that a contribution does not meet the required quality, it will be rejected for inclusion in the guide with justification and the author will be informed. The author then has the option to update or add to their contribution and prepare it for a new round of examination.

Contributions that pass this comprehensive procedure will be included in the guide.

2.4 Required protection objectives

The legislative amendments introduced by ITSiG focus on the availability, integrity, confidentiality and authenticity of protection objectives.

- **Availability**
  IT systems and components are considered available when these can always be used for their intended purpose and within their scope of functionality.
- **Integrity**
  Integrity refers in particular to the data. Integrity is considered to be present when it is assured that sent data reaches its recipients complete and unchanged.
- **Confidentiality**
  Confidentiality is deemed to exist when sensitive data is only made available to authorised persons in the manner permitted.
- **Authenticity**
  Authenticity exists when the unique identity of the communication partners (and that of the communicating components) is ensured.

In addition to these IT security protection objectives focused on by the ITSiG, there are other protection objectives, which are mentioned here in particular because of the aforementioned General Data Protection Regulation:[11]

- **Unlinkability (+ data minimisation)**
- **Transparency**
- **Intervention capability**

Some of these additional objectives are in competition with the IT security protection objectives mentioned above. Because the legal requirements of the ITSiG and the GDPR apply concurrently, the objective in the company is to achieve a common, sustainable solution for a high level of IT security and data protection. This can only be done through cooperation between the officers for IT security and data protection.

Whereas from the perspective of IT security the main goal is the protection of data and infrastructure, the main objective from the perspective of the data protection is to protect human rights. It is important to understand these different viewpoints in order to establish protective measures and implement them accordingly.

[11] Inspired by the Independent Centre for Privacy Protection Schleswig-Holstein (ICPP), https://www.datenschutzzentrum.de/

3 Technical and organisational measures (TOMs)

The ITSiG and the GDPR require technical and organisational measures to comply with or at least consider the “state of the art". The legislator did not further specify the relevant systems and components. Compliance with the state of the art must therefore be based on all relevant components of data processing, including all options for data portability and storage.

Because IT infrastructures depend greatly on application and sector, it is not possible to fully list the individual components in this guide. The authors have therefore focused on describing the essential components and processes.

3.1 General information

Applications regarding use within the context of the IT Security Law are sometimes very specific. This ranges from common standards, such as secure email communication, up to demanding requirements, e.g. as needed for safe control functionality in a power plant.

As a result, it is very difficult to draw up a full list of applications in this study and also describe this application. IT security can likewise be implemented differently, as there are many ways to achieve a goal and thus there is no ONE implementation of secure architecture. It is therefore intended to identify essential elements that can be understood as “state of the art" within the meaning of today’s IT security usability.

Protection needs depend on the application in each case. According to the IT Security Law, the IT security objectives of integrity, authenticity, availability and confidentiality must be adhered even if they are evaluated for the individual figure with different protection needs as applicable. This means that the following protection objectives in particular must be taken into account:

- Protection from attack for the purpose of unauthorized reading, modifying or deleting transmitted and stored data
- Protection from attacking the availability of the services and data in question to the operator or user
- Protection from unauthorised manipulation of operating and application systems, etc.

In addition to implementing adequate protective measures, the detection of attacks on IT systems, services and data must be guaranteed according to the state of the art.

Functionality that realizes the desired IT security application must be fully and correctly implemented at all times. This should have been verified by an independent auditor. Implementation must always incorporate “state of the art" methods. These include:

- Two-factor authentication
- Mutual authentication
- Encryption of communication during transport
- Data encryption (e.g. during storage)
- Protection of the private key against unauthorised copying
- Use of secure boot processes
- Secure software administration including patch management
- Secure user administration with active locking option
- Secure mapping of network zones for additional protection at the network level
- Secure data communication between different network areas
- Secure internet browsing
- Realization of the need-to-know principle
- Realization of the minimal approach (including hardening)
- Realization of logging, monitoring, reporting and response management systems
- Realization of malware protection
- Use of secure backup systems for preventing loss of data

- Multiple system layouts for implementing high availability, etc.

In addition to the individual technical application functionalities, the security architecture as a whole must also be considered. The following points must be evaluated under the conditions for this purpose (the German Federal Network Agency (BNetzA) requires a risk assessment for implementation with regard to the IT security catalogue as per German Energy Industry Act (EnWG), Section 11, as high as standard or critical for critical processes and applications):

■ It must be apparent to the user under which conditions they can use and apply the respective system in the respective secure configuration. If different operational scenarios are possible on one device (e.g. access to office IT via session 1 and access to the process IT via session 2), this must be clearly displayed to the user in each case.

■ A holistic security architecture for the product or service and corresponding documentation for evaluation by independent third parties must exist and be implemented.

■ The cryptography used must be able to be mapped in a secure and modern way up to the end of the product life cycle. For this, the BSI recommends up to date algorithms in a catalogue for cryptography standards.

■ The product or respective service must not contain any back doors that can be read along or even allow for manipulation of data and applications.

■ The manufacturer must not have access interfaces that can be used independently of the operator.

■ It would be advisable to have the implementation of the security function verified by trusted third parties.

■ The processes implemented in the application (e.g. user authorisation, key management, etc.) must be mapped securely.

There are other criteria that must be met in order to evaluate a product in terms of "state of the art." They are as follows:

■ The product or service must take international standards into account and should be interoperable with standard protocols.

■ If there are standards for the specific sector, they should be taken into consideration for the implementation.

■ The product or service must facilitate a reliable operation of the components (market maturity).

■ The product or service must have been tested successfully in practice.

■ Evaluation must consider the solution as a unit where hardware and software are linked.

■The product must be able to be safely updated in terms of security and application functionality.

The manufacturer of the solution is also subject to criteria for evaluation of the solution that must be considered when choosing "state of the art" implementations. The manufacturer can guarantee investment security for the implementation in question. This means that the following tests should be performed:

■ The manufacturer's financial background guarantees further life cycles for the product.

■ There is an established product management for the respective product and a road map for further development for the user's period of use exists.

■ The product is not marked as a discontinued product during the period of use.

- The manufacturer reacts proactively to vulnerabilities that come to their attention and affect their product, fixes them at short notice and makes necessary software updates available quickly.

- The manufacturer produces the respective solution in a environment with trusted personnel.

- The manufacturer has independent control of all security functions and does not rely on other suppliers regarding the security functions.

If third party products are used that are less reliable, the security architecture for the product and manufacturer measures in the production process must ensure that the entire security architecture remains in place in terms of the defined protection needs.

3.2 Technical measures

3.2.1 Password strength assessment

The measure simulates practical attacks on securely stored/hashed login information and measures the objective resilience based on mathematical methods, personal behaviour, etc. The measure takes a thorough inventory and evaluates all passwords, even those that are unknown. The measure determines the level of compliance with internal guidelines within the company and supports or facilitates the implementation of measures related to security, such as notifying employees if unsafe passwords are used in compliance with the GDPR.

Which IT security threat(s) is the measure used against?

The measure should prevent the risk of misuse of account information (login data).

80% of IT security incidents that lead to the disclosure of account information - private, personal data and business data, can be attributed to weak and/or stolen passwords (Verizon Report, 2017).

Compliance with static password policies for user accounts is therefore proven to be not an adequate measure for implementing strong, secure passwords. The password policies deceives a false level of security.

Which measure (procedure, equipment or operating mode) is described in this section?

Company networks generally use a central storage for user login information that is used to authenticate users who access services and/or workstations (e.g. Microsoft Active Directory).

All modern login information storage systems use hashing functions for passwords that are intended to prevent attackers with access to the central database from being able to retrieve plaintext passwords.

While this hashing function represents crucial protection of passwords from unauthorised access, it also prevents a company from being able to evaluate passwords. However, this is necessary in order to implement measures against potential attacks - such as trying words from the dictionary as passwords, using passwords known to be compromised or guessing passwords using personal information about the target.

The password security assessment defines a password's resilience by simulating an actual attack that uses and exploits various potential weak points, such as predictable/weak passwords, passwords used by multiple users, faulty cryptographic implementations, etc.

In this way, retrieved passwords are processed according to national, regional and internal data protection rules without disclosing or storing any information about specific users or passwords.

Retrieved passwords are then assessed based on objective mathematical and structural entropy - and subjective - password guideline compliance - criteria. As soon as the assessment is complete, the plaintext passwords are discarded and a meaningful report is generated.

The results of the password security assessment - the audit report - allow the company to gauge the exact security risks of the passwords used in various multiple and heterogeneous systems. Thus, the best awareness and training measures can be defined for users and central enforcement methods can be identified for strong passwords. This also allows the effectiveness of measures already in place to be reviewed and improved.

What protection objectives are covered by the measure?

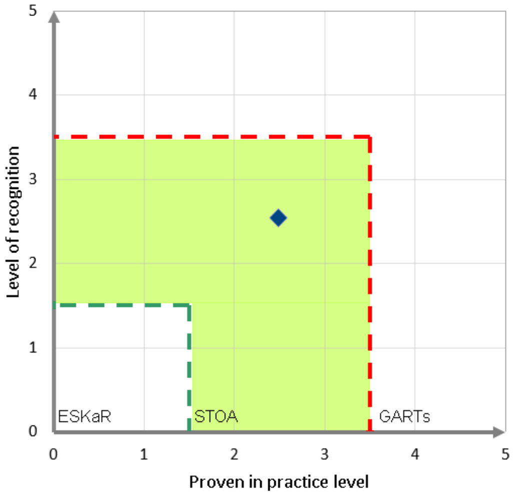
☐ Availability

☒ Integrity

☒ Confidentiality

☒ Authenticity

State of technology classification



3.2.2 *Enforcing strong passwords*

The measure enforces the use of strong, secure passwords for all technical and organisational measures put in place by a company.

The strength of the password is scaled to the respective user account's security level by a regulatory framework. The defined security level is based on the potential impact of the security of this account being compromised.

Which IT security threat(s) is the measure used against?

80% of IT security incidents that lead to the disclosure of account information - private, personal data and business data - can be attributed to weak and/or stolen passwords (Verizon Report 2017).

Therefore, compliance with static password policies for user accounts has proven not to be an adequate measure for the enforcement of strong, secure passwords - The password guideline simulates a false level of security.

The measure described will increase the security level of the passwords used to one that corresponds to the security risk (control and detection).

Which measure (procedure, equipment or operating mode) is described in this section?

Newly set passwords will be checked against a set of rules assigned to each account and parametrised individually for different categories.

The rules include measures for: Composition (length, character set, symbols, character sequences and repetitions), mathematical and structural entropy values, uniqueness (the password must not be in use by another account on the same system within the organisation), the use of known standard passwords and reused passwords (historical). The rules are not limited to blacklisting, but can be parametrised individually.

The solution will be used and managed centrally by a single interface for all systems within the organisation. This allows for coherent, system-wide policies to be effective. It also prevents multiple use of passwords in different systems and makes it possible to keep a central record of the password history.

Plaintext data will never be stored or displayed. The end user will receive a clear message if their new password is rejected, explaining the reason. This relieves the burden on the call centre and protects the user's privacy.

All communication between servers and systems for enforcing strong passwords is secured with the use of encryption.

The measure described will result in central enforcement of the adequate password strength in each case and give the organisation complete supervision, control and documentation of the passwords used in the company. It can also achieve an adequate level of security in authentication with the use of passwords.

Enforcement must be evaluated by means of a measure for assessing and evaluating passwords. The resilience of the passwords used to actual attacks must be gauged and determined and whether the rules are effective as expected or if they need to be corrected to prevent the use of weak passwords, as circumstances may require.

What protection objectives are covered by the measure?

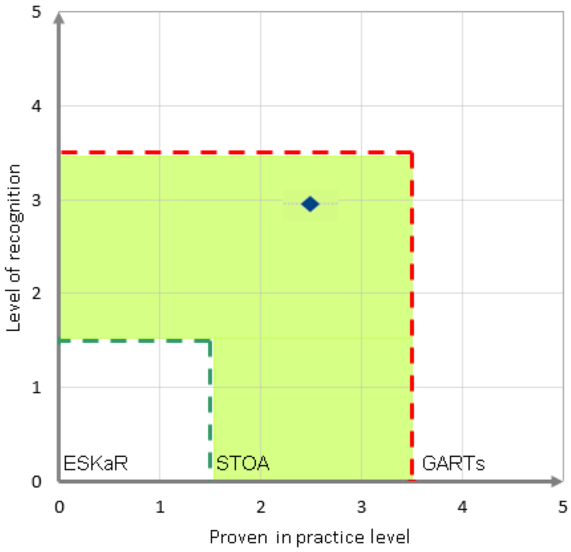
☐ Availability

☒ Integrity

☒ Confidentiality

☒ Authenticity

State of technology classification



3.2.3 Multi-factor authentication

Multi-factor authentication (MFA) and two-factor authentication (2FA) describe authentication processes in which more than one factor, such as a password, is used to securely authenticate subjects on objects. An MFA or 2FA solution ensures that the subject really is the subject itself. This measure is becoming increasingly important in a fully interconnected world as the significance and opportunities for access to digital identities grow as well. The possibilities of modern MFA systems and securing of digital transactions also play an interesting role in growing digitalisation and stricter regulations, such as the EU Payment Services Directive 2 (Payment Service Directive 2, PSD2).

Which IT security threat(s) is the measure used against?

81% of compromising situations are due to weak and stolen passwords, according to the Verizon 2017 Data Breach Investigations Report[12].

Stolen and weak passwords are the cause of compromised security in over 80% of all cases today. This is because passwords empirically do not constitute protection for digital identities. The reasons for this are as follows:

1. Attackers can already take over one percent[13] of all user accounts with 10 guess attempts per account - which is within the typical guess limit.
2. The inclusion of public information, such as that from social media (targeted guessing) allows attacks to take over digital identities with a probability of 32% (security-savvy users) to 73% (normal users)[14].

[12] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017
[13] http://www.jbonneau.com/doc/B12-IEEESP-analyzing_70M_anonymized_passwords.pdf
[14] http://www.comp.lancs.ac.uk/~yanj2/ccs16.pdf

3. In addition, users generally use the same pattern for creating their passwords, which significantly reduces the actual password space in comparison with the potential theoretical password space[15]. Examples include:

    a. Upper case letter lower case letter lower case letter lower case letter lower case letter number number
    b. Upper case letter lower case letter lower case letter lower case letter lower case letter lower case letter number number
    c. Upper case letter lower case letter lower case letter lower case letter number number number number
    d. Previous combinations with an “!" at the end.

Many users also reuse their passwords for different applications (five passwords for an average of 26 accounts per user). Thus, a compromised account on one service means a compromised account on all services. Attackers systematically and automatically try the captured data on various different services. The longer the attacker remains undetected, the more data they can collect and thus they can cause more damage or generate results.

Using an MFA or 2FA system considerably lowers the risk that an attacker can abuse a digital identity with a password or access the data accessible with it.

Which measure (procedure, equipment or operating mode) is described in this section?

Two-factor or multi-factor authentication makes identity theft much more difficult. These procedures traditionally require that at least one other authentication factor besides the password be met before allowing access to a site, application or certain data. A simple two-factor authentication therefore requires two of three features:

- Something to identify the user knows (such as a password)
- Something the user carries with himself (a bank card or authentication token - whether hardware or digital)
- Something specific to the user with biometric identifiers (such as fingerprint or iris recognition)
- Something the system knows about the user. (Geolocation, device ID, time periods, previous transactions)

Modern multi-factor systems offer a wide range of applications:

1. Support various types of tokens (software, hardware, SMS, voice, mOTP) that can be configured based on the intended purpose and risk for different target groups.
2. Support for third-party scenarios with the ability to limit the validity of any token type in terms of number of uses or time period.
3. Token support connected to transactions. These tokens are only used with modern MFA/2FA solutions and allow processes to be secured by generating a one-time password (OTP) based on transaction details such as are required for PSD2. This guarantees non-repudiation along with confidentiality and integrity.

Modern 2FA and MFA systems can be easily integrated. Using standard links to an active directory, LDAP, SQL or JSON, applications can quickly be enhanced by an MFA or 2FA component and the users managed within will be secured. Modern APIs can be used to secure internal developments, custom software or portals very quickly and with just a few lines of code.

Modern transaction tokens allow a high degree of user-friendliness to be implemented while also guaranteeing non-repudiation. In this process, the user receives a message on their smartphone which prompts them to approve their login or their “critical action" in the system a second time by pressing OK

[15] https://www.youtube.com/watch?v=5i_Im6JntPQ and https://youtu.be/zUM7i8fsf0g

on their smartphone. By combining the use of public key mechanisms with QR codes, these procedures can also be used to remove devices or for offline authentication.

What protection objectives are covered by the measure?

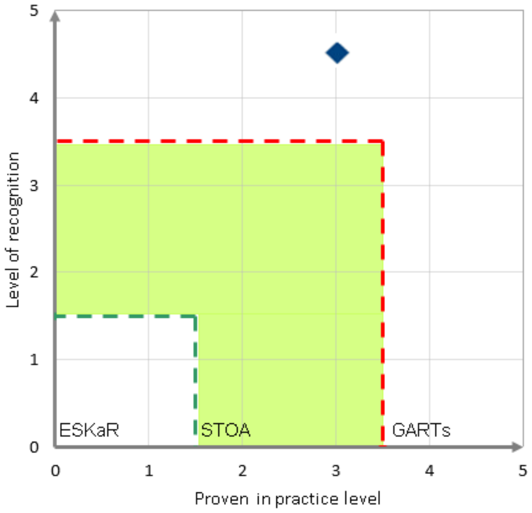
☐ Availability

☒ Integrity

☒ Confidentiality

☒ Authenticity

State of technology classification



Note: In particular, this ongoing innovation and the measure’s high level of effectiveness in preventing the loss of digital identities result in the evaluation made here of proof in practice.

3.2.4 Cryptographic procedures

Cryptographic procedures, such as methods to encrypt and sign data, essentially depending on the configuration, the procedure used and the key lengths. The protection objectives can only be implemented in terms of confidentiality, integrity and authenticity through an appropriate combination of all three factors. This chapter provides recommendations for using and choosing cryptographic procedures.

Cryptographic procedures are used for a variety of purposes and form the basis for many IT security measures. Modern cryptography is used in

- Authentication procedures
- To guarantee authenticity
- Access control
- To implement repudiation and non-repudiation
- Secret sharing
- To implement anonymisation procedures
- Elections and votes (Commitment procedures)
- Cryptocurrencies
- Digital rights management (DRM)

and many other scenarios.

A common feature of these procedures is that they primarily serve to guarantee confidentiality and authenticity. This means, for example, preventing the theft of confidential data or undetected manipulation of data.

Cryptographic procedures are meant to fulfil Kerckhoff’s principle. Open algorithms can be systematically evaluated for weak points and optimised by a large, global community of experts. This is roughly how today’s standard for symmetric encryption, AES, was created in a public competition. It is considered to be extremely secure.

The level of security of an encryption method indicates the effort to which an attacker would have to go to produce plaintext. Simply put, it grows with the number of options available for choosing the key (the bit length).

Due to advancing computing power, analytical progress and technical possibilities, there is a risk that an attack on a procedure will become known which lowers the level of security to practically feasible. It is also possible that someone will succeed in building a quantum computer that can perform a “brute force" key search in a much shorter amount of time, which would cut the level of security for the symmetric procedure in half. Many asymmetric procedures would be broken down altogether using available quantum computers.

For these reasons, cryptographic methods used must be checked about once a year to make sure they are effective.

The current version of the recommendations is published by the BSI as Technical Guidelines TR-02102.[16] Further recommendations can be found in documents by the American NIST, ENISA, and other organisations.[17,18,19,20,21,22]

[16] See https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html (English version: https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/tr02102/tr02102_node.html)

[17] BSI TR-02102-1 "Cryptographic Mechanisms: Recommendations and Key Lengths” version: 2018-02

[18] NIST Special Publication 800-57 Part 1 Revision 4: Recommendation for Key Management Part 1: General

[19] NIST Special Publication 800-175B: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms

[20] European Union Agency for Network and Information Security: Algorithms, key size and parameters report – 2014

[21] https://eprint.iacr.org/2015/1018.pdf

[22] https://safecurves.cr.yp.to/

At this time, the following recommendations can be made in particular:

- Symmetric encryption methods: AES-128, AES-192, AES-256 ideally with GCM as operating mode. EAX mode is recommended as well if a stream cipher is required for resource reasons and a slightly higher delay due to encryption is acceptable. In modern systems, Authenticated Encryption with Associated Data (AEAD) should be used as the operating mode. Operating modes without additional Message Authentication Code (MAC) are generally considered insecure without further integrity protection and should not be used.
- Asymmetric encryption methods: at least ECIES-250, DLIES-2000, RSA 2000, curve25519, curve448 or ECC Brainpool. ECIES should be used with 384 or more bits. If DLIES or RSA is in use, 3072 bits or more should be used.
- Hash functions: Pay attention to SHA-256, SHA-384, SHA-512, SHA3-256, SHA3-384 and SHA3-512. The SHA1 and MD5 algorithms are no longer “state of the art."
- Key derivation functions (KDF) and password hashes: Current appropriate algorithms are:[23] Argon2, PBKDF2, scrypt and bcrypt. New systems should use the Argon2 algorithm.
- Random number generators:
    - physical random number generators, functionality class PTG.2 or PTG.3[24]
    - Deterministic random number generators, functionality class DRG.3 and DRG.4
- TLS[25], [26]: TLS 1.3 combined with forward secrecy using secure algorithms as per BSI TR-02102-2, table 1[27]. The use of tools such as: https://www.owasp.org/index.php/O-Saft and https://www.ssllabs.com/ssltest/ helps inspect TLS configuration.

Note:

Side-channel attackers are a relevant problem for cryptography. Choosing “recommended" algorithms does protect against analytical attacks, but not against side-channel attacks. These attacks are generally made by measuring physical parameters such as run times, power consumption, heat and vibrations.

Potential side channels depend especially on the implementation of the algorithm and the platform used. The side-channel resistance of IT security products varies based on the provider. If you are uncertain in this case, work with specialised service providers.

3.2.5 Disk encryption

Full disk encryption protects data storage devices installed in a system, such as magnetic hard drives or flash memory-based SSDs, from unauthorised access (reading, modifying) by third parties. The information stored there is not accessible as plaintext unless the user is authenticated before booting up the PC or smartphone operating system.

Which IT security threat(s) is the measure used against?

This measure protects data on the hard drives of unattended, switched-off end devices such as PCs, laptops, tablets or smartphones (data at rest). In the event of loss through inattention or theft, or temporary availability for unauthorized third parties (hotel rooms), attackers cannot evaluate the content or

[23] https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet

[24] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_for_random_number_generators_e.pdf

[25] Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths
Part 2 – Use of Transport Layer Security (TLS)

[26] NIST Special Publication 800-52 Revision 1 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

[27] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf (Englisch version: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-2.pdf)

manipulate the stored information. Copying the read-only memories of devices protected in this way then only delivers useless data because it is encrypted.

Which measure (procedure, equipment or operating mode) is described in this section?

The data carrier(s) installed in a system, such as magnetic hard disks or flash memory-based SSDs on which the operating system and company confidential data are stored, are encrypted by the measure in such a way that their unauthorized reading does not provide any plain text. This applies both to the case of readout with the system switched off or the hard disk removed, as well as during operation for the tapping of the data at the hard disk internal interface (eSATA etc.).

At least AES-256 in XTS mode should be selected as symmetric encryption. A central management tool facilitates the use on all PCs of an organization considerably. The cryptographic keys should never be stored in the cloud, not even for backup purposes.

When choosing the authentication features, great importance should be attached to hard-to-crack passwords and 2-factor authentication, ideally by means of "knowledge and possession", for example with an additional token. This also enables the use of hardware-supported delay mechanisms for multiple incorrect password entries. An expansion of the data carrier for analysis in an attacker system becomes pointless.

As far as the device allows, for example with Windows 10 systems, the so-called "Secure Boot" should also be supported. This protects the entire boot process, including 2-factor authentication, against manipulation and preserves the integrity of the system and the encryption mechanisms.

Some available solutions also support full or folder-based encryption of removable media. Within organizations, automatic, user-transparent encryption for company data is preferable in order to prevent plaintext storage due to operating errors.

Solutions for Windows 7, 8 and 10 are available that have been approved by the BSI for use by public authorities but can also be used in critical infrastructures and companies.

What protection objectives are covered by the measure?

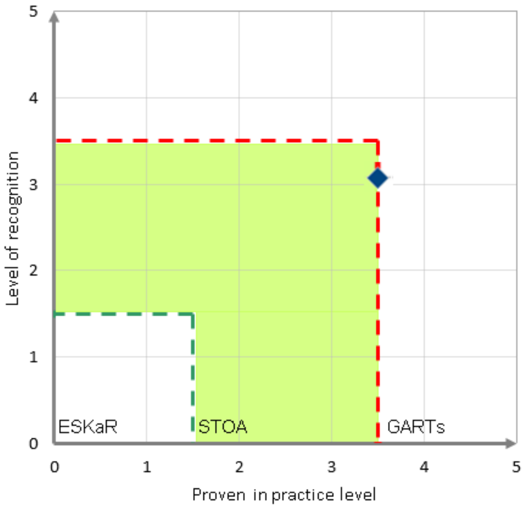
☐ Availability

☒ Integrity

☒ Confidentiality

☐ Authenticity

State of technology classification



3.2.6 Encryption of files and folders

File and folder encryption encompasses the encryption of individual objects, such as containers, folders or individual files, which is why this type of encryption is also known as object encryption. The programs available for this often work transparently, meaning users can work with the objects as if they were unencrypted.

Object encryption offers the ability to securely transport files and folders from one location to another and prevent unauthorised users from accessing them. It is therefore necessary to ensure that no one other than the authorised persons have access to the protected information. This can jeopardise personal data in individual cases or, in the worst cases, a company's livelihood.

Furthermore, object encryption is useful when using cloud services because it effectively prevents data from being accessed by the operator.

Which IT security threat(s) is the measure used against?

1. Interception and misuse of data during transport, e.g. through e-mail
2. Loss and theft of removable media with subsequent unauthorised access to sensitive data
3. Misuse of data stored in the cloud

Which measure (procedure, equipment or operating mode) is described in this section?

File and folder encryption encompasses the encryption of individual objects, such as containers, folders or individual files, which is why this type of encryption is also known as object encryption. The programs available for this often work transparently, meaning users can work with the objects as if they were unencrypted.

Object encryption offers the ability to securely transport files and folders from one location to another and prevent unauthorised persons from accessing them.

What protection objectives are covered by the measure?

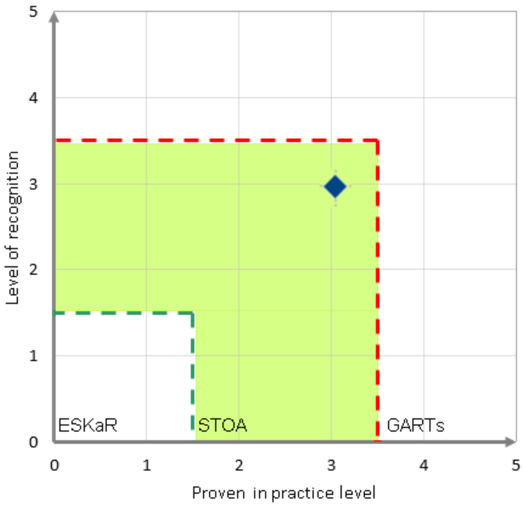
☐ Availability

☐ Integrity

☒ Confidentiality

□ Authenticity

State of technology classification



3.2.7 E-mail encryption

Business e-mails often contain important and sensitive data, and e-mail addresses are often personalised as well, and therefore generally contain personal data that must be protected from unauthorised access or modification. The protection objectives can generally be achieved by encrypting the transmission of e-mails and/or e-mail contents.

Which IT security threat(s) is the measure used against?

- *Spying on or manipulating e-mails in transport*
- *Spying on or manipulating stored e-mails*

Which measure (procedure, equipment or operating mode) is described in this section?

Encrypted e-mail transmission (transport encryption); TLS

Encryption of e-mail contents; S/MIME or PGP

The security requirements for e-mail are based on the type of data transmitted and stored in the mail system, among other things. In the case of business transactions, it can generally be assumed that e-mails for the company contain important information at least. E-mail addresses, if personalised, continue to be regarded as personal data; it can therefore be assumed that personal data will be transmitted and stored by e-mail. In individual cases and depending on the use of e-mail, data with special protection needs, such as data concerning health or client data from lawyers, for example, or particularly valuable company secrets such as design data, may also be transmitted.

This results in the following security requirements for e-mail:

- Protection against unauthorised access or modification of e-mails in transport and in storage (protection objective: confidentiality),
- Protection against subsequent modification of e-mails that are archived long-term (protection objective: integrity).

These protection objectives can generally be achieved with encryption. For e-mail encryption, a distinction must be made between encrypting the transmission (transport encryption) and encrypting the e-mail itself (or “end-to-end encryption"). The protection objectives necessitate the use of transport encryption, at least, when transmitting e-mails through public networks. The protocols used when transmitting e-mails over the internet, namely SMTP, POP3 and IMAP, however, provide unencrypted data transmission in their basic form. Large parts of e-mail traffic are therefore still transmitted unencrypted, even though plenty of tools have been available for e-mail encryption for a long time.

The current version of TLS (Transport Layer Security), (defined in RFC 5246), should be used for transport encryption in e-mail traffic. Secure encryption methods (e.g. AES-256, currently) must be used; insecure encryption methods (e.g. RC4) must not be used. Forward secrecy should be activated as a general rule. It is also sensible to inspect the certificates used for TLS by the respective other side for authenticity and validity, e.g. using DANE (RFC 7671). The BSI’s Technical Guidelines TR-02102-02, part 2, provides an extensive list of recommendations for TLS.

End-to-end encryption is recommended to protect particularly sensitive data. Two standards have been established for this: S/MIME (Secure/Multipurpose Internet Mail Extensions, defined in RFC 5751) and OpenPGP (Pretty Good Privacy, defined in RFC 4880). Both essentially use the same cryptographic mechanisms. However, they differ in the certification of public keys and thus in confidentiality models, and are not compatible with each other.

When using end-to-end encryption, no system in the transmission path can access the contents of the e-mail. However, this means eschewing the use of content filters, antivirus programs, anti-spam, data loss prevention and archiving entirely. Therefore, content encryption can only be used meaningfully between organisations; meaning e-mail messages are encrypted and unencrypted in transmission from the public internet to the organisation’s private network (gateway) (organisation end-to-end encryption), or combined as necessary with internal company content encryption.

What protection objectives are covered by the measure?

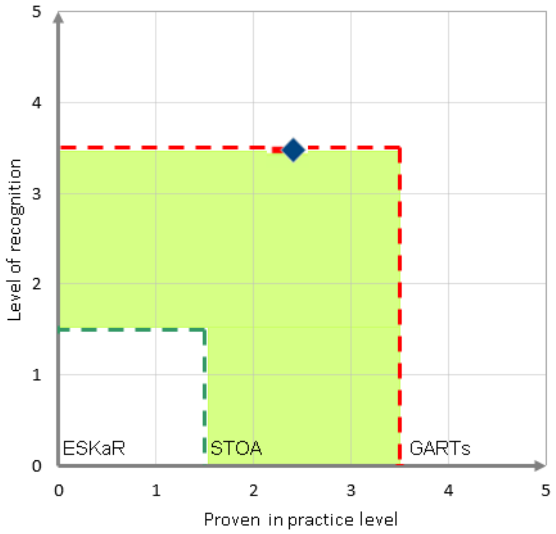
☐ Availability

☒ Integrity

☒ Confidentiality

☒ Authenticity

State of technology classification



3.2.8 Securing electronic data communication with PKI

In electronic data communication, it is important that the identity of the communication partners and the authenticity of the transmitted contents is ensured. Proof of electronic identities for persons, organisations or devices can be ensured by the use of electronic certificates. Electronic signatures are suitable for proving the authenticity of transmitted documents and messages. Certificate-based solutions are also used for secure encryption of data transport. All of these scenarios require a component for generating, managing and inspecting electronic certificates that reliably ensures proof of electronic identities: a Public Key Infrastructure (PKI).

The eIDAS regulation that has been in effect since summer 2016 also provides for the use of a PKI.

Which IT security threat(s) is the measure used against?

- Identity theft/pretence of a false identity
- Manipulation of the contents of digital messages or files
- Manipulation of the timing of messages or files

Which measure (procedure, equipment or operating mode) is described in this section?

The following measures are sensible against the threats described above:

- Creating an internal PKI or using an external one
- Using digital signatures (signatures, certificates, stamps) from an accredited trust centre
- Using qualified time stamps to prove authenticity and timing of messages and documents

The digital certificates are issued by the certificate authority of a PKI organisation. The term “certificate authority", or CA, is used here. The validity of public keys is confirmed by the CA’s digital signatures here. Along with the key itself, the digital certificate also contains other information, such as the period of validity, etc. The CA is responsible for being the central component in the Public Key Infrastructure. In order to maintain the CA’s trustworthiness, the identity of the applicant, whether a person or organisation, must be subjected to an unequivocal inspection before the electronic certificate is issued. This is done by the Registration Authority (RA).

A Validation Authority (VA) is required to inspect the validity of digital certificates. In general, a distinction is made between the check against a published certificate revocation list (CRL) or real-time validation through an online certificate status protocol service (OCSP). The choice of the type of inspection is usually based on the application scenario in each case.

Depending on the PKI’s legal status, the legally admissible logging of all transactions in a PKI is sensible or even necessary in most cases. Certified CA products are also required for some areas of application.

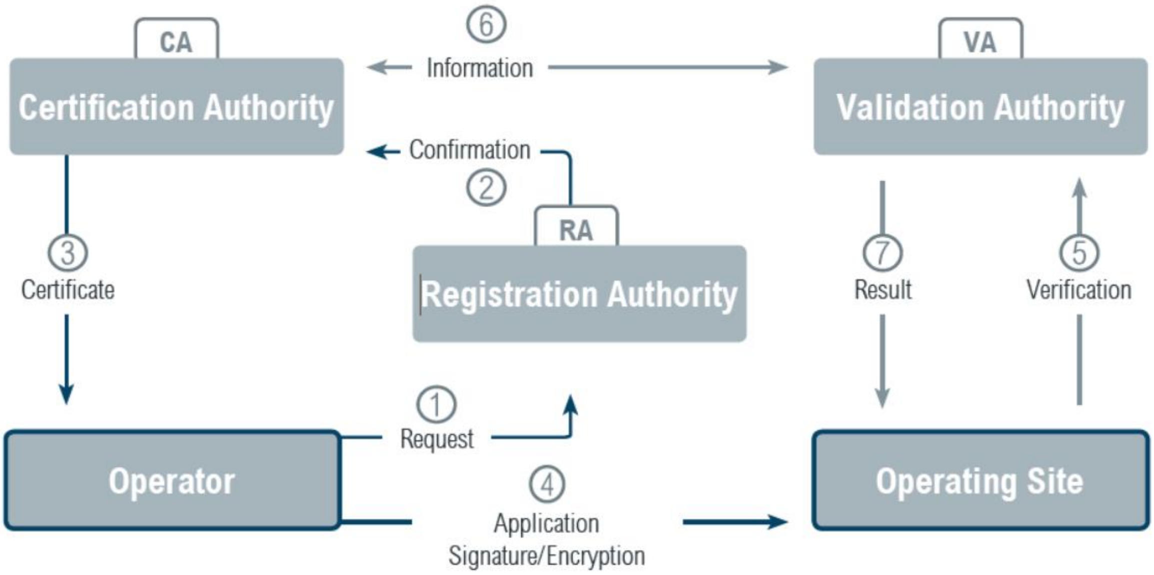
The applications of PKI-based methods are diverse. The following application procedures are cited as examples:

- Signature and encryption of e-mails (S/MIME)
- Authentication and encryption in the “Internet of Things"
- Authentication and encryption on the web (HTTPS)
- Authentication and encryption for VPN services
- Authentication and integrity security for executable code (code signing)
- Authentication and integrity security for documents (digital signature)

- Authentication of clients/users on the internet

Depending on the operator and the security standard of the dedicated computer centre, a wide variety of solutions can be arranged. This ranges from a root CA as a “trust anchor" to a strictly hierarchical PKI with several sub-CAs. Cross certification can also be implemented with other PKIs.

The following chart shows the overall structure and interaction of PKI components in a workflow.



The use of certificates is meaningful and useful in almost all areas. In addition to application areas in the public sector, they are also found in energy and gas supply, e-justice (with beA, beN, beBPO), healthcare and the industrial and non-profit sector (e.g. associations, societies).

The eIDAS regulation in particular provides for an extensive array of usage scenarios. For example, proof of identity and trust services are supported by PKIs (see table below).

eIDAS regulations/applications	
Identities	Certificates
	Electronic ID
Trust services	Electronic stamps
	Electronic time stamps
	Website authentication
	Electronic delivery services
	Preservation services

An example of use in the public sector is: www.cio.bund.de/Web/DE/IT-Angebot/IT-Beratungsdienstleistungen/Public-Key-Infrastruktur-der-Verwaltung/public_key_node.html and www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/PKI/pki_node.html in the energy supply sector

or even at TeleTrusT: https://www.ebca.de.

What protection objectives are covered by the measure?

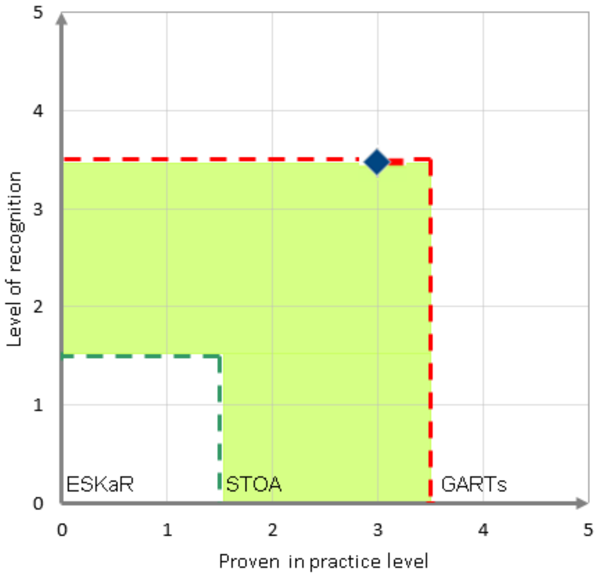
☐ Availability

☒ Integrity

☒ Confidentiality

☒ Authenticity

State of technology classification



3.2.9 Use of VPNs (layer 3)

A layer 3 VPN describes the connection of two or more networks on layer 3 of the OSI model. The data transmitted is encrypted. This allows, for example, company branch offices in different countries to be connected to each other securely and confidentially over the internet.

Which IT security threat(s) is the measure used against?

Using VPNs protects against:

- Loss of confidentiality due to unencrypted/poorly encrypted connections
- External attackers
- Connection manipulation

The VPNs used are themselves subject to other threats:

- Outflow of key material
- Weak cryptography
- Denial of service: The VPN’s availability is threatened due to error or attacks

Which measure (procedure, equipment or operating mode) is described in this section?

A layer 3 VPN describes the connection of two or more networks or the linking of a client to a network on layer 3 of the OSI model. The data transported in this process is encrypted and the VPN endpoints authenticate and authorise the other respective VPN endpoint. This allows, for example, company branch offices in different countries to be connected to each other securely and confidentially over insecure third-party lines, such as the internet or services hired by a telecommunication services provider. Less data is transported in comparison with a layer 2 VPN because layer 2 data, like broadcasts, is not transmitted. Conversely, a layer 3 VPN cannot be used transparently for all applications because of this. Complex topologies, such as on-demand VPN connections, can sometimes only be implemented with a layer 3 VPN or it is considerably easier to do so. The same is true of VPN configurations with a large number of endpoints. A layer 3 VPN requires VPN access for each participant. Often when a hub-and-spoke VPN architecture is used, the central node is referred to as a VPN concentrator. It is recommended to source a layer 3 VPN as a solution from the manufacturer.

As a key component of an IT infrastructure, the configuration and operation of a layer 3 VPN must have the benefit of special attention. A layer 3 VPN solution should only be provided by authorised and trusted suppliers. Manufacturers of secure VPN solutions can be expected to provide active patch management and respond quickly to security issues so that you have the best possible protection at all times. A manufacturer without any corresponding patch management cannot be considered a professional and should be ruled out of the selection process.

A layer 3 VPN must ensure the confidentiality of the data directed through it. For this purpose, the device must perform encryption and authentication with algorithms and parameters that are considered secure. The manufacturer must be able to prove that they are actively working on the security of the cryptography used, whether by replacing algorithms that have become insecure or by choosing appropriate parameters. Secure mechanisms for authentication must be used wherever technically feasible. A variety of measures must be put in place to provide extra protection for access to administration of the layer 3 VPN. This includes encrypted access with secure authentication (e.g. HTTPS for a WebGUI, SSH for console access, protected authentication information in hardware), but also the manufacturer's special attention on the security of the platform for the VPN device itself so as to rule out unauthorised access due to technical shortcomings. Sensitive information is generally transported over a VPN.

A layer 3 VPN with devices that include back doors or allows software bugs to run so that the devices themselves can be taken over is an unacceptable risk. Therefore, products should be favoured that are able to demonstrate high platform security and a high level of self-protection, such as through independent inspections (certifications or even accreditation). The requirements for the operational environment must continue to ensure that physical access to VPN devices is only possible for authorised persons.

Like the confidentiality protection objective, the platform's integrity is crucial to maintaining the integrity and authenticity of the data passed through it. It is also important here that the VPN devices are set up on an extra hardened platform, have excellent self-protection and do not have any back doors. The security protocols that use a layer 3 VPN also guarantee the integrity and authenticity of the transported data. Management and the secure use of key materials also play a crucial role. Preference should be given to manufacturers who can demonstrate that they facilitate secure random number generation, secure key management for private authentication keys (such as on chip cards) and track the age of used encryption keys.

Appropriate measures are required to ensure the availability of layer 3 VPNs for VPN endpoint hardware and software (such as VPN concentrators). Regarding hardware, the manufacturer must be able to demonstrate that the platform has been designed and implemented for high availability according to the requirements. This includes, for example, redundant power supplies, execution of processing power and fan configuration in which the failure of one fan does not cause the entire system to fail. Because these measures are not yet sufficient in practice to prevent hardware failure, there must be the option of redundant operation (high availability configuration). Monitoring also plays a key role here so that faulty hardware can be detected in a timely manner. In this case, the manufacturer must support appropriate monitoring, such as through SNMP. On the software side, it is crucial to pay special attention to correct implementation so as to avoid malfunctions. Preference should be given to manufacturers who make special efforts in development in the form of code reviews. It is still important to focus on protecting against Denial of Service attacks. A particularly secure platform is an important requirement here as well, of course, in addition to controlled access to the areas where the VPN endpoints (VPN concentrators) are operated in the LAN.

Log data accrues on the devices of a layer 3 VPN. This is extremely important for being able to detect attacks on the network. However, this data has to be mandatory for this purpose. Similarly, it is important to be able to track administrative changes and that this log data is mandatory and allocable accordingly. This means that there must be options for filing such log data so that it is secure against manipulation. This can be guaranteed by local append-only logs, for example, or by using an interface to external log servers or SIEM systems.

What protection objectives are covered by the measure?

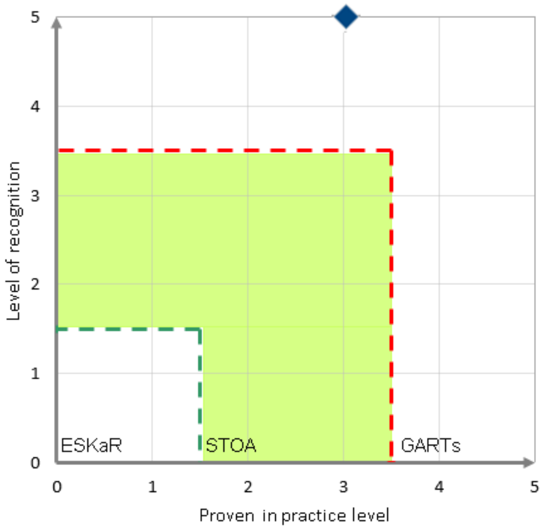
☒ Availability

☒ Integrity

☒ Confidentiality

☒ Authenticity

State of technology classification



Note: While there is no doubt about the fundamental need to use VPNs, manufacturers are regularly delivering innovations to increase their level of security, user-friendliness and operability. Thus, the state of the art for VPNs is defined not only by their existence, but also by the form of these qualities.

3.2.10 Layer 2 encryption

Layer 2 encryption is a security solution alternative to layer 3 VPNs, which are utilised on the payload of Ethernet frames instead of on IP packets. IP headers do not need to be processed (which saves time) and the load on the line capacity is much lower than encryption through layer 3 or higher due to the encryption overhead.

Which IT security threat(s) is the measure used against?

Recording and evaluating massive amounts of data from traffic-linking locations across the corporate network backbone or the cloud connection through security gaps in network hardware, with network providers and underground or underwater cables not subject to monitoring and wireless or satellite connections, as well as DDoS attacks on encrypted layer 3 connections.

Which measure (procedure, equipment or operating mode) is described in this section?

Using encryption to secure WAN communication between company locations and data centres. Using bandwidth-neutral cryptography solutions with very little delay for layer 2 WAN backbones and direct links (such as dark fibre or Satcom).

Layer 2 encryption is a security solution that works as a suitable alternative to layer 3 VPNs in certain applications. It is applied to the payload of Ethernet frames instead of IP packets. IP headers do not need to be processed (which saves time) and there is no encryption overhead (line bandwidth is fully available). An Ethernet-based network (point-to-point, hub-spoke or fully meshed) via dedicated cables (copper/fibreglass) or a layer 2 service provided by network providers (e.g. Carrier Ethernet services) is required for use.

Typical applications for layer 2 encryption include protecting WAN backbone lines (even internationally) and data centre connections within the corporate network or to trusted clouds and collocation providers, as well as protecting campus backbone lines that run outside buildings and over property owned by third parties.

The performance benefits are worth it, especially for adopting central IT services, massive desktop virtualisation, data centre consolidation and distributed and redundant storage systems that have a high proportion of IP packets that are small or relevant to real time (such as VoIP, IoT or Smart Grid),

and for which IPsec overhead and delay are unacceptable.

Using this network encryption technology does not require changing existing IP routing configurations. This type of encryption is transparent for virtually all network services and applications of OSI layers 3 and higher and does not have any measurable impact on network performance.

Remote encryption stations and periodic changes of cryptographic keys are synchronised and authenticated automatically. Key generation and distribution in layer 2 encryption devices is decentralised, avoiding key servers as single points of failure and thus increasing network availability. BSI-approved solutions are available.

What protection objectives are covered by the measure?

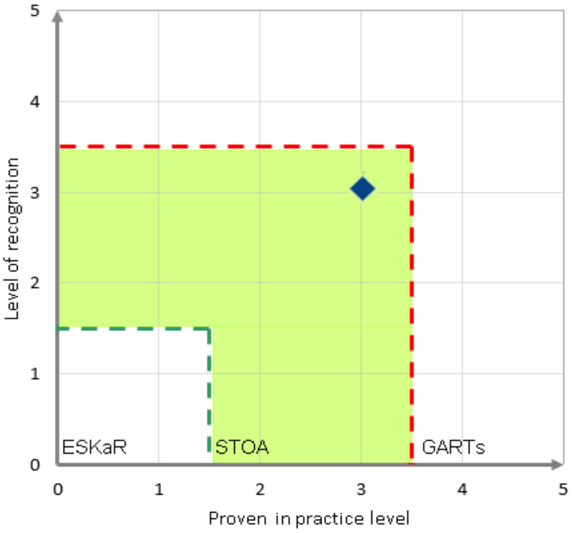
☒ Availability

☒ Integrity

☒ Confidentiality

☒ Authenticity

State of technology classification


5
4
3
2
1
0
Level of recognition
0
1
2
3
4
5
Proven in practice level
ESKaR
STOA
GARTs

3.2.11 Cloud-based data exchange

As digitalisation progresses and working methods become more widely geographically distributed, cloud-based data exchange services, as they are called, are used more frequently in the IT environment (e.g. Dropbox, OneDrive, Google Drive). Adequate measures must be put in place in order to use these services securely and protect against known threats.

Which IT security threat(s) is the measure used against?

The data stored in a cloud-based data exchange service is susceptible to the following threats:

- *Unauthorised access and inspection by the operator of the service*
- *Hacking by third parties while the data is transported through the internet*
- Theft or unauthorised use of the identity that was agreed on with the cloud service

Which measure (procedure, equipment or operating mode) is described in this section?

The following measures are appropriate for protecting the data stored:

1. *Encrypted transmission of files to and from the data exchange service*
2. *Client-side, end-to-end encryption of data for the recipient prior to transfer to the cloud*
   - *Through encryption integrated into the data exchange service in the client software that is part of the cloud*
   - *Through separate client end-to-end encryption software*

The following questions should be regarded in particular:

1. *Who operates the service and does the operator have access to the data when necessary?*
2. *How is data protected during transport to and from the operator?*

If the service is operated by a trusted body, then end-to-end encryption of the data itself is unnecessary in some circumstances, though is generally useful even with trusted operators.

There are data exchange services in which data is encrypted transparently before uploading, meaning without any special action by the user, and decrypted again after downloading. In these cases, the operator only sees encrypted data. Alternatively, client-side encryption software can be used that provides end-to-end encryption of data before uploading and after downloading. However, these solutions generally require additional expense for the user. Encryption should focus on the use of secure methods for encryption, key generation and key management.

Under no circumstances should data not be encrypted during transport to and from the operator (transport encryption, generally TLS).

What protection objectives are covered by the measure?

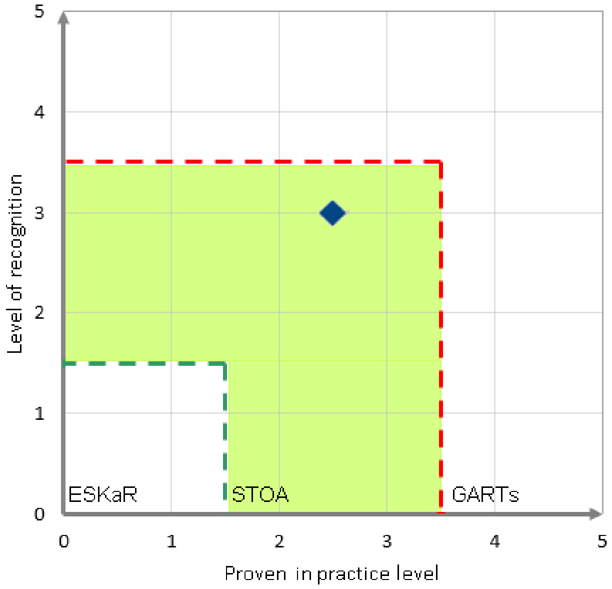
☐ Availability

☒ Integrity

☒ Confidentiality

☒ Authenticity

State of technology classification



3.2.12 Data storage in the cloud

Protection strategies that only protect the IT structure by itself are no longer sufficient in decentralised cloud structures. In the arms race against attackers, the most fundamental measure is the most secure: encrypting sensitive data as soon as it leaves a secure internal environment to be processed or stored in the cloud. The cryptographic keys should remain exclusively in the possession of the user organisation in order to prevent unauthorised access by external administrators. A state-of-the-art solution must therefore allow appropriate key management to be fully internal. Internal distribution of administrative key management functions to multiple people also makes it more difficult to compromise sensitive data. State-of-the-art solutions are those that do not limit important functions such as searching or filtering data, reporting or automated processing of encrypted data in cloud applications.

Which IT security threat(s) is the measure used against?

Sensitive data stored or processed in the cloud is susceptible to many forms of compromise, including:

1. unauthorised access to the cloud (by both external and internal users),
2. access by external cloud administrators or data centres,
3. interception during transmission between the organisation and the cloud, and
4. theft from cloud storage.

Which measure (procedure, equipment or operating mode) is described in this section?

An encryption gateway is a proxy-based solution that transmits between the end-user application and the cloud. It encrypts all data that leaves a previously defined, secure internal environment and decrypts information requested from the cloud by authorised end users. With this type of solution, cryptographic keys must remain exclusively in the possession of the user organisation in order to guarantee data sovereignty and centralise control of reading access authorisation. This state-of-the-art solution should therefore allow fully internal key management. Key management functions should be distributed internally to multiple controllers. This ensures that key data cannot be compromised by individuals.

Internal key management makes this solution more secure than native encryption solutions from third-party cloud providers (bring your own key, etc.). In the latter case, there is no way to eliminate the possibility of third-party (such as database administrators) reading access to sensitive information. With an encryption gateway, third-party data processors can still perform administrative tasks, but not read any sensitive data in plaintext form. The solution also provides protection in the event of data theft: Without cryptographic keys, attackers are unable to use encrypted data.

The central factor in using an encryption gateway should be maintaining the protected data's ability to be processed. This can be achieved by using partial encryption methods.

Looking ahead, it is advisable to choose an encryption gateway that allows the user organisation to change the encryption algorithms they use as they wish. With the ongoing development of extremely powerful quantum computers, methods that are classified as secure today may become obsolete in the near feature. Therefore, the ideal solution is one that is already compatible with post-quantum cryptographic algorithms (PQC).

What protection objectives are covered by the measure?

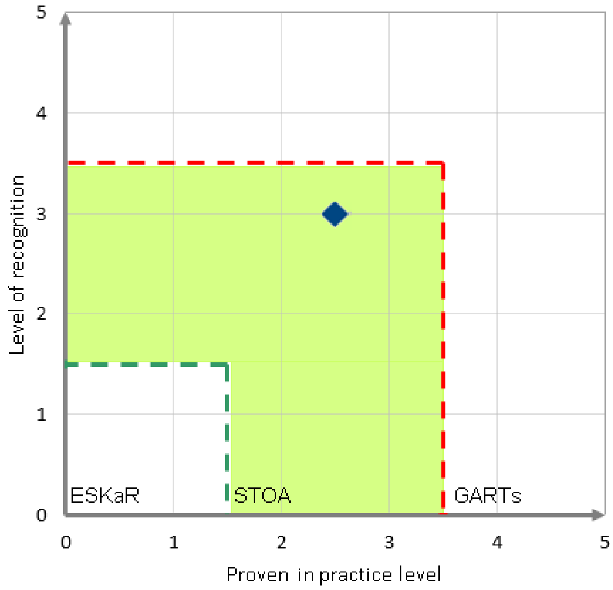
☐ Availability

☒ Integrity

☒ Confidentiality

☒ Authenticity

State of technology classification



3.2.13 *Use of mobile voice and data services*

Mobile conversations and data transfers are easier to intercept than landline telephony. Encryption of mobile voice and data transfer protect against this, as do device hardening and configuration.

Which IT security threat(s) is the measure used against?

Classic landline and mobile telephony today is also one of the most direct and personal forms of communication in spite of chat and web-conference applications. However, it presents several risks and offers potential attack vectors. The vast majority of phone calls made from landlines also involve the participation of a mobile phone.

- *Hacking mobile conversations and data traffic from landlines run by mobile and telephone network operators, and for which the base stations are connected to each other and to the landline connections and are based on internet technology, etc.*
- *Hacking mobile conversations and data traffic as well as their transfer to command & control - attacker servers through malware installed on the mobile phone that exploits vulnerabilities in the operating system and apps in order to gain direct access to the microphone, speakers and touchscreen keyboard and screen, and remove the encryption app that way*
- *Unencrypted mobile conversations and data traffic can be intercepted using cheap hardware on the air interface. Attackers do not have to infect the mobile phone or break into the communication network to do this. However, they do need to be located in the reception area of the mobile phone in question. Attackers may pretend, for example, to be part of the mobile network in order to register the mobile phone on their listening device and then directly record and analyse conversations and data traffic.*

Which measure (procedure, equipment or operating mode) is described in this section?

The confidentiality of conversations can be assured by using voice and data encryption on OSI layer 7 (in the Communication apps). Spoken word and chat data, along with any file transfers, are encrypted on the device in real time and then decrypted and displayed when they reach the recipient.

The following counter-measures are recommended:

- Encryption of voice and data communication through suitable and trusted apps or hardware that meet current encryption standards and applicable data protection rules for end-to-end encryption
- Additionally, central configuration of terminals by the issuing organisation or one that supports BYOD through mobile device management (MDM/EMM) systems to avoid unwanted user actions and app activities that lead to mobile phone infection
- For higher levels of reliability, the use of mobile phones with hardened operation systems that ensure microphone and speaker are only used by the encryption app and prevent any existing malware from hacking the encryption key.

What protection objectives are covered by the measure?

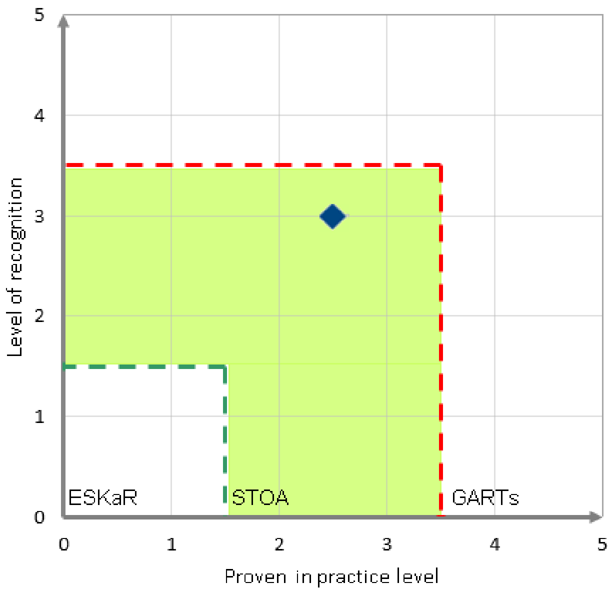
☐ Availability

☒ Integrity

☒ Confidentiality

☒ Authenticity

State of technology classification



3.2.14 *Communication through instant messenger*

Instant messaging is the term for a form of digital communication in which two or more parties converse by means of swiftly transmitted text, image and voice messages. The parties use a common instant messenger for transmitting the messages via a network to do this. If one party is not online at the time a message is transmitted, it will generally be delivered to the recipient at a later time. Secure instant messaging attempts to protect instant messages from unauthorised access and modification.

Which IT security threat(s) is the measure used against?

When information is exchanged through instant messaging, the following threats must be considered:

1. Recording, analysing and modifying the contents by an unauthorised third party (man-in-the-middle attack)
2. Identity theft within a communication system
3. Theft of equipment for the purpose of subsequently analysing instant messaging data without authorisation

Which measure (procedure, equipment or operating mode) is described in this section?

1. Secure instant messaging contains technical security measures to preserve the confidentiality and integrity of communication content:
   - Message transmission protection using latest TLS in transit
   - Use of asymmetric end-to-end encryption with security comparable to at least RSA 2048 bit
   - Forward secrecy should also be part of the architecture in order to protect the data from subsequent decryption despite having the long-term key.
2. Reliable verification/authentication of identities
3. Securing access options and paths to content:
   - Locking screens on the mobile device used (strong password)
   - Activated device encryption
   - The communication app used should provide independent secure data storage and protection from extraction by unauthorised parties.

What protection objectives are covered by the measure?

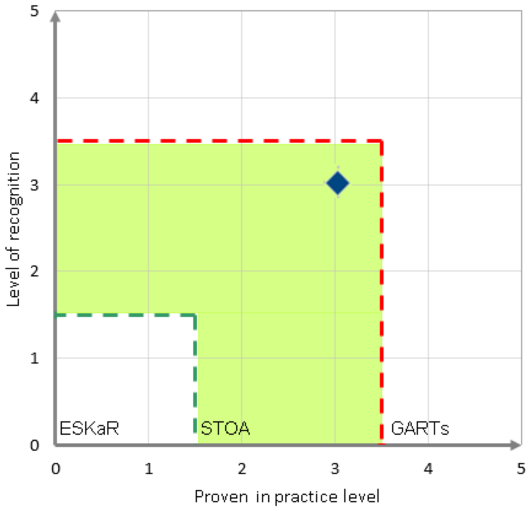
☐ Availability

☒ Integrity

☒ Confidentiality

☒ Authenticity

State of technology classification



3.2.15 Mobile Device Management

The use of Mobile Device Management (MDM) solutions lowers the security risks that arise due to uncontrolled use of mobile devices for business purposes. MDM solutions make it possible to centralise the administration and configuration of the mobile devices used.

Which IT security threat(s) is the measure used against?

1. Data loss: If important data is stored on the mobile devices and the device is lost or destroyed, the company will have to accept that this data is irrevocably lost in some situations.
2. Theft: If a mobile device is stolen, the thief may have access to confidential business data.
3. Malware: By using public WLAN networks, not installing available updates and not controlling the installation of applications from some questionable sources, mobile devices are frequently infected with malware.

Which measure (procedure, equipment or operating mode) is described in this section?

Mobile Device Management (MDM) solutions allow administrators to control the use of and access to mobile devices used for business purposes in different ways according to security guidelines defined in advance. MDM solutions can determine the mobile device's patch status and prompt updates to install as soon as they are available and have been checked. In addition, adequate password protection, regular backup and device encryption can all be forced centrally. In the event of theft or loss of the device, it can be forcibly deleted in order to protect the confidentiality of company data. The administrator will be able to set user rights for the mobile device in such a way that applications from random and potentially unsafe sources cannot be installed.

In order to meet the higher functionality requirements for using mobile devices for business purposes, some manufacturers have expanded current MDM features with Mobile Application Management (MAM) and Mobile Information Management (MIM) functions, including cloud connection to Enterprise Mobility Management (EMM) solutions.

What protection objectives are covered by the measure?

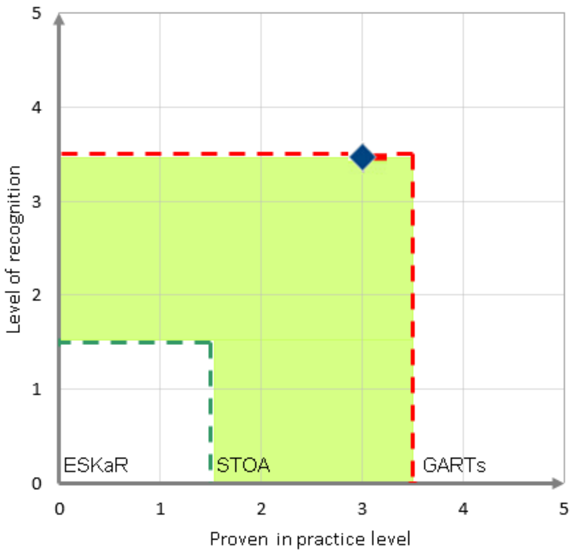
☒ Availability

☒ Integrity

☒ Confidentiality

☐ Authenticity

State of technology classification



3.2.16 Router security

Routers are central infrastructure components that facilitate the exchange of network packets between multiple networks/computers.

In the B2B sector, routers are not just used as internet access devices or for routing data. In most cases they also establish VPN networks. As telephony infrastructure has migrated (replacing ISDN/analogue technology with IP technology), routers have been used as ISDN-IP gateways so that ISDN systems still in place can still be used in IP networks. Both applications make the router a critical component for a company, with specific security requirements.

Due to its global prevalence in company, organisation and private networks alike, the router is a target for various types of attack that must be prevented by adequate protective measures. This section describes and assesses the threats to routers and current protective measures.

Which IT security threat(s) is the measure used against?

Routers are meant to redirect data reliably and securely while protecting it from unauthorised access. The following threats/risks may jeopardise these objectives:

1. Configuration manipulation
2. Attacks using known gaps in security and those that have not been closed

3. Attacks using newly discovered security gaps (zero-day exploits)
4. Attacks through IP telephony connections
5. Theft (especially outdoor/mobile communication routers)
6. Availability attacks (DoS attacks)
7. Access through undocumented interfaces (see so called “back doors")
8. Running third-party code and integration in botnets
9. Attacks via inadequately secured WLANs

Which measure (procedure, equipment or operating mode) is described in this section?

There are multiple security measures to minimise the risk of the above threats, which can be summarised below as a “router security" package of measures:

1. Password protection: Using secure access data protected against third-party access and avoiding the use of standard logins
2. Regular router firmware updates
3. Service contracts with the manufacturer and a set maximum response time in the event that a serious gap becomes known.
4. If a router manufacturer does not provide any updates after becoming aware of a security gap, it is necessary to consider using alternative devices from other manufacturers who are not affected by the gap.
5. The router should be set up in a sheltered location, e.g. a lockable room with access monitored by responsible administrators. It is seldom possible for a router to be set up outdoors in a location with protected access. The router should therefore be equipped with a GPS function. The router should be configured so that after a power outage, for example, it is checked to make sure it is still located on site. If this is not the case, its operation must be disrupted.
6. There should be filters for invalid addresses according to RFC 2267 and blacklists should be set in the firewall to protect against DoS attacks.
7. All ports and interfaces that are open or not needed should be closed.
8. If possible, the router should automatically deactivate during inactivity (e.g. at night) to reduce the window of exposure. This measure should not restrict the installation of updates.
9. Different network zones should be established to minimise the impact of successful attacks on routers (network segmentation).
10. WLAN routers: No open networks or only for guest access (direct outgoing line), otherwise use the highest encryption standards
11. VPN routers: Do not establish VPN connections via pre-shared keys but based on certificate where possible
12. Router as all-IP/ISDN gateway: Use devices with integrated session border controllers. Firewalls are not capable of handling SIP-based voice packets, resulting in the risk of an attack through voice-over-IP connections. Router operation should be centrally monitored.

What protection objectives are covered by the measure?

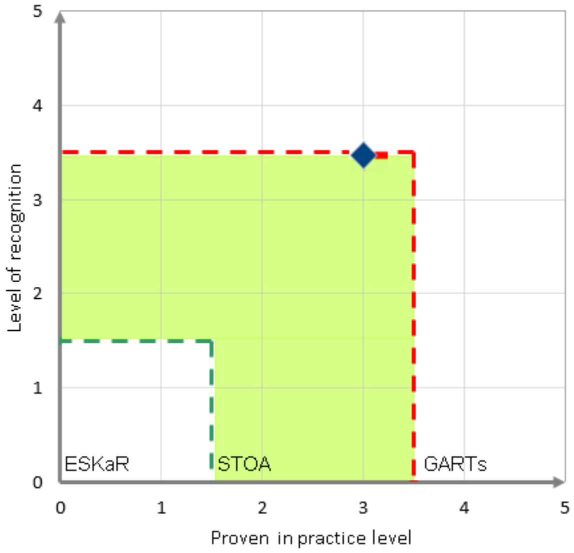
☒ Availability

☒ Integrity

☒ Confidentiality

☒ Authenticity

State of technology classification



3.2.17 *Network monitoring using Intrusion Detection System*

An intrusion detection system (IDS) or intrusion prevention system (IPS) identities and logs anomalies in the IT network. The objective of both systems is to detect intrusion and the spreading of malware before damage occurs, if possible. Unlike IDS, which only reports information from anomalous behaviour and generates alarms, an IPS is also able to intervene automatically. This should prevent malware from being spread further through the network. It should be noted that direct intervention by an IPS can have a direct impact on availability in industrial and production systems, among others, or fully automated ordering/delivery processes and reporting and security processes (including fire safety)

Which IT security threat(s) is the measure used against?

1. Information leaks due to interception of sensitive data
2. Misuse of services and communication protocols
3. Third-party IT system access to the IT network
4. Exploitation of opportunities to access linked IT systems
5. Manipulation of information or software
6. Spreading malware in the IT network

Which measure (procedure, equipment or operating mode) is described in this section?

There is a distinction between network-based and host-based IDS/IPS. Network-based IDS/IPS uses internal components and/or the network infrastructure to monitor communication. Host-based IDS and IPS use information from IT systems (via software agents, logfile analyses, etc.). In distributed system architecture, the data must be encrypted and signed for exchange or storage.

Detection is based on two different methods. “Pattern matching" identifies known malware based on patterns (signatures). New attack patterns have to be analysed as quickly as possible and their signatures need to be updated as secure against manipulation immediately because otherwise, attacks based on these patterns will remain undetected.

The second method is based on detecting changes in the communication patterns of network components caused by an attack. All communication outside of the expected data traffic profile is evaluated as an anomaly. This allows new attacks to be detected as well. There is no need to maintain attack patterns in a database. However, the communication patterns that are part of normal data traffic must be defined.

If malware is detected or if there are discrepancies from the valid nominal condition of communication, an IDS must automatically generate relevant incident reports. All incident reports should be retained in the system long enough to analyse them and be able to be exported in an open or standardised format if needed.

Incident reports must include all relevant information for incident analysis and to initiate countermeasures, such as recognised signature or anomalous communication connection. Alarm messages should be visible at the front of the management console, sent as mail to specified accounts and available on a general alarm system (see SIEM) through an export interface.

An IPS must also independently block all communication in the network on which an attempted attack is based. It must be ensured that, as far as possible, no communication that cannot be clearly attributed to any attack behaviour is prevented.

An IDS/IPS must provide components to analyse all communication to gateways and/or within IT systems (hosts) that automatically resynchronise after a temporary outage for stable operation.

No undesirable communication from IDS/IPS components to third parties can be allowed. Furthermore, all IDS and IPS components should be unidentifiable, should not impact data traffic or offer any services and should be protected themselves.

Symmetric and asymmetric algorithms should be used, in addition to signature and key lengths for certificates used, according to the current recommendations of the BSI.

What protection objectives are covered by the measure?

☒ Availability

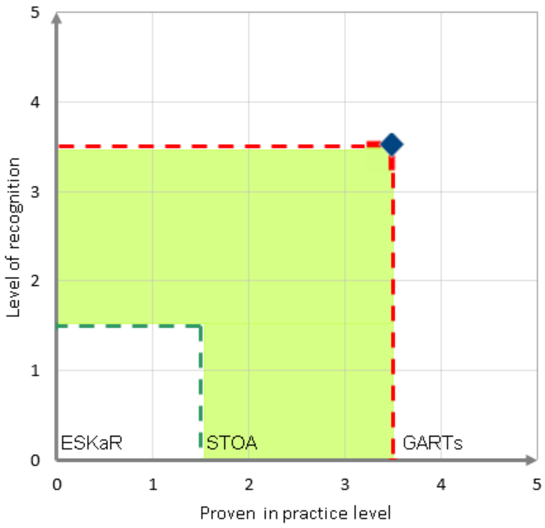
☒ I

ntegrity

☒ Confidentiality

☒ Authenticity

State of technology classification



3.2.18 Web traffic protection

Web servers are one of the main ways of spreading malware. In most cases, users are unaware when infected websites load and execute malware on the system. If data traffic is directed through a web filter while surfing, these attacks can be detected and blocked.

Which IT security threat(s) is the measure used against?

Web servers are one of the main ways of spreading malware. Infected web servers are often used where the operator is not directly involved in the attack. A large percentage of web servers have permanent security gaps through which they can be attacked by hackers, and which then store malware on the system, usually so-called root kits.

These websites are normally operated by the user. When visiting an infected website, the malware is loaded and activated on the local system without being notice by the user (drive-by downloads).

Attackers also use specially provided web servers that often imitate another website. In the case of “phishing", these fake copies of known websites are provided with the goal of tapping sensitive information from the user, usually usernames and passwords, in addition to bank information, credit card information, addresses, etc.

The actual destination address (URL with malicious code or the URL of an infected or fake web page) is often disguised through automatic redirection, and many times through URL shorteners (bit.ly, TinyURL, etc.), although these are not directly involved in the actual attack. Users are linked to dedicated websites through links placed in e-mails, on social media, etc.

Which measure (procedure, equipment or operating mode) is described in this section?

Web data traffic is directed through web filters to protect these types of attack. Web filters protect against these attacks by blocking the websites in question and analysing the data loaded by websites for malicious code. Web filters can be operated centrally as web filters in the cloud or as on-premises appliances, or as software operated on the end user’s system.

What protection objectives are covered by the measure?

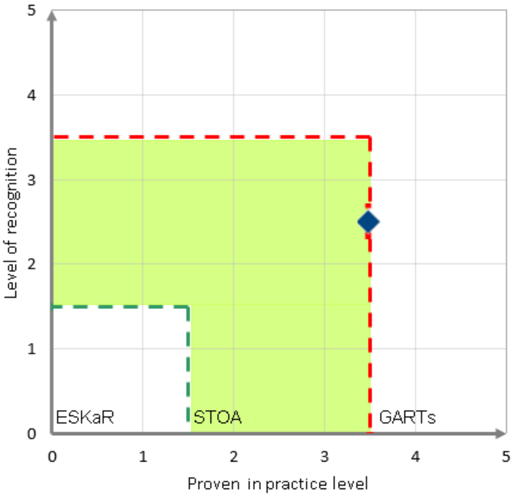
☒ Availability

☒ Integrity

☒ Confidentiality

☒ Authenticity

State of technology classification



3.2.19 *Web application protection*

A Web Application Firewall (WAF) protects web applications (homepages, online shops, home banking portals, etc.) from attacks. The WAF inspects the communication between users and web applications at the application level and blocks potentially harmful data traffic, such as SQL injections or cross-site scripting. The term “Web Service Firewall" (WSF) is also widely used for machine-to-machine communication.

Unlike a network firewall, which operates on OSI layers 3 and 4, WAFs treat OSI layer 7 - data traffic, and thus protect against threats that target the exploitation of security vulnerabilities in the applications.

Which IT security threat(s) is the measure used against?

Attacks on web applications or web service interfaces, such as

- SQL Injection
- Cross-Site Scripting (XSS)
- Information Leakage
- Command Injection
- Other OWASP threats

Which measure (procedure, equipment or operating mode) is described in this section?

Using a Web Application Firewall (WAF or WSF) that actives ahead of the web server.

A Web Application Firewall (WAF) protects web applications (homepages, online shops, home banking portals, etc.) from attacks. The WAF analyses communication between users and web applications at the application level and blocks potentially harmful data traffic. An adaptation of the WAF is sufficient for web application security gaps that need to be closed in the short term in most cases. Adapting or patching the web application to be protected can then be planned afterwards and carried out with enough notice for tests. A combination of different vulnerabilities is often exploited for attacks. Thus, blocking one central vulnerability per WAF can quickly repel many attacks.

The Web Services Firewall (WSF) is a special case of the WAF for machine-to-machine communication and is likewise processed via http/https. The attack vectors for WAF and WSF are very similar. The following applies to both the WSF and the WAF.

Modern web applications and services often provide a programming interface (API) that offers a wide range of functions for flexible machine use, which is seldom the best form of protection.

The WAF terminates encrypted data traffic on the user side, analyses the content and redirects it to the web server as encrypted requests that are classified as harmless. Harmful requests are blocked.

Operating web applications without using an appliance or virtual upstream WAF can no longer be considered state of the art.

A WAF should have the following features:

- Log data transfer to SIEM and anomaly detection systems with the option to conceal passwords, credit card information, etc.
- Cluster capabilities for high availability and load distribution
- Protection against OWASP top 10 attackers, such as SQL injection, cross-site scripting (XSS) and directory traversal through blacklisting, whitelisting and pattern recognition
- Strong authentication of web applications and services users
- Session management, i.e. inspection and manipulation protection of session cookies
- Broken Access Control prevents unauthorised access to paths (path traversal), files and API functions
- Filters for unnecessary http headers
- Protection against cross-site request forgery (CSRF) through header evaluation of http requests, e.g. referrer information

What protection objectives are covered by the measure?

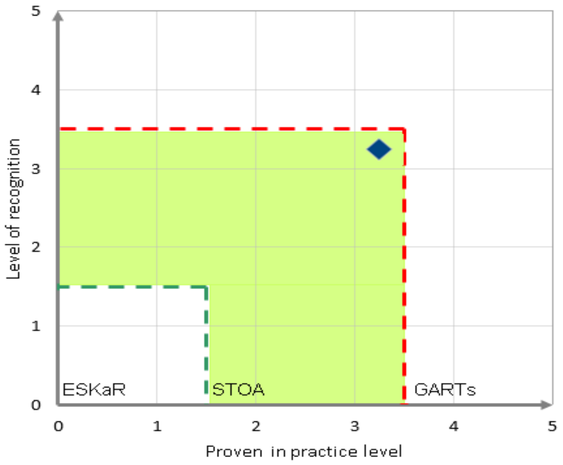
☒ Availability

☒ Integrity

☒ Confidentiality

☒ Authenticity

State of technology classification



3.2.20 Remote network access/ remote maintenance

Remote networks need to be reachable over the internet for the purposes of maintenance or software updates.

In an industrial environment, these participants are machine control components such as PLC, drive units and operating panels. In the event of maintenance or a software update, the remote user must access these systems online with their manufacturer tools (such as PLC programming software).

Which IT security threat(s) is the measure used against?

- Unauthorised access to the company network
- Unauthorised access to target systems
- Remote access cannot be traced
- Data tapping or exposure during a remote maintenance session

Which measure (procedure, equipment or operating mode) is described in this section?

The target systems are typically connected to the internet via routers to allow remote maintenance. They then use this to establish a VPN connection to what is called an “intermediate server." This intermediate point is the link between the target system and the remote user, which has likewise established a VPN connection to the intermediate server. Since both locations have their own connection, each participant is able to terminate it at any time. The task of the intermediate server in this process is to only allow the approved target systems for the respective remote user. Ideally this can be limited to remote users and target systems up to layer 3 (IP, port, protocol). This guarantees the connection for the specific application to the target system. Depending on the application, pure terminal connections can also be established through remote maintenance. This includes web, RDP, VNC and SSH access, for example. This depends on the availability of the target system. However, a direct 1:1 network coupling from the remote user to the target system’s network should be avoided in particular.

Encrypted VPN connections guarantee data integrity and protection against data tapping. Two-factor authentication should be available for authorisation of the remote user.

Each remote maintenance session must be logged. This is necessary in order to identity the most recent access to the network or router in the event of a security incident. If this happens, the remote user’s identification (IP address and name), time and duration of the connection should be logged. This is ideally stored on the intermediate server.

What protection objectives are covered by the measure?

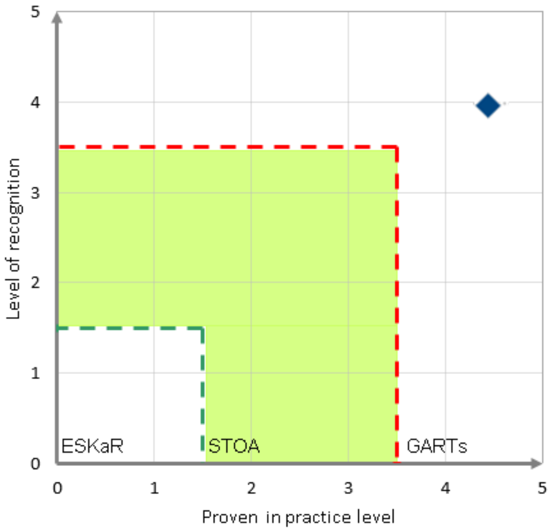
☐ Availability

☒ Integrity

☒ Confidentiality

☒ Authenticity

State of technology classification



3.2.21 Server hardening

Since server systems process and store the company's essential (often sensitive) data and personal data, the systems used must be specially protected. Server hardening is a very effective security measure. It protects the operating system, regardless of whether it is a physical, virtual or cloud-based server.

Common server operating systems like Microsoft Windows Server or several Linux Server systems do not have a very restrictive security configuration by default and are potentially equipped with unnecessary components. Often these unused and unconfigured functionalities are used by attackers to compromise the operating system.

Through server hardening, these functions and their interfaces will be disabled or configured more restrictively, which significantly increases the security level of server systems. Therefore, server hardening should be an integral part of the technical security strategy of a company or institution.

Against which IT security threats will the measure be used?

The main threats of non-hardened server systems are:

- Data manipulation of personal data and sensitive company data
- Data loss (e.g. entire database systems)
- Manipulation of applications or connected systems
- Manipulation, sabotage or espionage of operation and production processes
- Identity theft (e.g. attacks on domain controllers)
- Incorporate malware of any kind and distribute malware to other systems
- Abuse of server capacity for attacker’s benefits (e.g. crypto-mining)
- Misuse of servers for lateral movement to attack other systems

Which measure (procedure, facilities or modes of operation) is described in this section?

To harden server systems, the following measures must be implemented in particular:

1. Deactivation of components

    - Periodic verification whether active services are necessary for operation
    - Deactivation or deinstallation of unnecessary operating system components / services, including background services
    - Deactivation of unnecessary startup or time-controlled processes
    - Deactivation of unneeded, technically obsolete or unsafe interfaces or protocols
    - Deactivation of telemetry data transfers, unless they are needed for central monitoring according a central policy
    - Deactivation of unnecessary file shares
    - Deactivation or limitation of access to administrative websites

2. Activation of hardware-related protection features

    - Activation of CPU security features and testing of the proper operation of applications (e.g. Address Space Layout Randomization "ASLR", Data Execution Prevention "DEP")
    - Activation of a BIOS password, limitation of boot sequence to necessary devices
    - If applicable,activation of protection against side channel attacks
    - If applicable.activation of safe boot procedures

3. Security configurations

    - Use of secure communication protocols to ensure that sensitive data and authentication information are transmitted encrypted
    - Use of certificates for exchange of cryptographic keys
    - Deactivation of auto-start mechanisms (for example for USB media)
    - Activation of a screen saver with password protection

- Activation of strong user account control
- Activation of antivirus protection on the system already during the boot process
- Removal of unnecessary certificates from trust stores
- Preventing information leakage regarding installed services and version numbers
- Disable error or debug messages for end users or replace them with neutral error messages
- Operate services with minimal rights and a service user, run processes in an isolated environment if possible
- Activate logging

4. Minimal allocation of permissions (need-to-know principle, least-privilege principle)

   - Review of assigned permissions on a regular basis
   - Minimal rights for administrative activities
   - Minimal rights for file system and external data interfaces
   - Minimal rights for maintenance interfaces / access
   - Restrict access to operating system configuration files, restrict access to physical servers (especially to prevent attachment of unauthorized external disk drives)

5. Accounts and passwords

   - Use strong passwords and mechanisms (appropriate password length, complexity, account lock, change interval, etc.), do not re-use passwords for other applications or use a 2-factor authentication (see Section 3.2.1 ff)
   - Protect all accounts with a password according to password policy
   - Change all existing default passwords by own passwords according to password policy
   - Lock local administrator account after multiple incorrect attempts
   - Use of individual administrative accounts for administrative activities
   - Disable or rename standard user accounts
   - Disable local guest accounts
   - Use non-privileged service accounts to execute processes
   - Deny login of local user accounts over networks
   - Disable default, test and anonymous accounts for all installed services / software components

6. Network components

   - Set network restrictions (e.g. TCP/IP configuration), disable or uninstall unused network protocols
   - Restrict connections to services to a minimum
   - If applicable, activate packet filters / firewalls to restrict communication to the minimum required access

For common server operating systems, more detailed hardening guidelines are publicly available:

- STIGs (Security Technical Implementation Guides): https://iase.disa.mil/stigs
- CIS Benchmarks ("Center for Internet Security, Inc. “): https://www.cisecurity.org/cis-benchmarks
- Microsoft Security Guidance: https://blogs.technet.microsoft.com/secguide/

Most hardening measures can be realized by technical adjustments. These settings can be distributed to all the company's server systems automatically with a hardening package (such as hardening scripts). New server systems should be hardened immediately after installation with the respective package. When hardening existing systems, hardening could result in functional failure, so a backup must be made and the hardened server systems have to be tested extensively.

What protection objectives are covered by the measure?

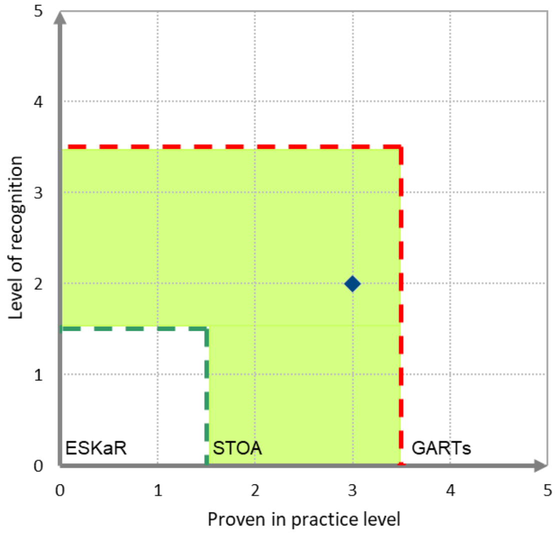
☒ Availability

☒ Integrity

☒ Confidentiality

☒ Authenticity

State of technology classification



3.2.22 *Endpoint Detection & Response Plattform*

The protection of end devices (e.g. PCs, laptops, smartphones or tablets) now requires much more than just an antivirus program. Modern solutions (Endpoint Detection & Response Platforms, EDR) combine the latest protection technologies to stop all types of cyber-attacks on client and server systems across operating systems and to identify the originators. Unlike conventional solutions, no specific prior knowledge, such as signatures or a first victim, is required.

Which IT security threat(s) is the measure used against?

- Malware
- Exploitation
- Malicious scripts
- Hacker activities
- Abuse of administrative tools and tools with malicious intent

Which measure (procedure, equipment or operating mode) is described in this section?

EDR platforms combine effective detection and prevention techniques to prevent client and server compromise across computers and operating systems, and even expose active attackers in computer networks.

Lightweight agents provide the attack-relevant process telemetry data, use locally effective machine learning models (artificial intelligence) and correlate and visualize tactics, techniques and procedures holistically.

Thanks to state-of-the-art sensor architecture, Next Generation EPP solutions only use up a computer to a fraction of the capacity of a classic AV scanner and regular downloads of signatures are no longer necessary. This means

- Signatureless detection and active blocking of malicious code by machine learning models (preferably local runtime),
- Audit and record program activity across process chains and optionally block malicious behavior,
- Protection against exploitation of vulnerabilities within legitimate applications (exploits and memory manipulation)
- Ideally, detections are correlated and the technique and tactics (including tools used such as malware, trojans, PowerShell scripting and the attacker's target are displayed (exfiltration of data, setting up a backdoor, lateral movement within the organization, rights escalation, etc.) are displayed.
- Additional threat intelligence shows who the suspected actor/opponent is (cybercrime or nationally motivated attack) and what targets and industries the attackers are pursuing.
- A fully integrated sandbox connection allows the safe "detonation" of found malicious code for further analysis without endangering production.

EDR platforms address the entire lifecycle of an attack attempt. This is the only way to draw conclusions about the actors and their motivation, which ideally have been contextually completed by current threat information. In addition, system telemetry data can be checked for harmful evidence by external experts.

In addition, it must be added that the following points in particular must be taken into account for a holistic protection of end devices if these aspects are not provided by the respective EDR solution itself:

- Authorizations / Roles (keyword: administrative authorizations)
- Update mechanisms (operating system and software)
- Limitations / control of the installed software
- Encryption of end devices
- Protection against threats / malware as described above
- Regulations / guidelines for permissible use (private use, use in external networks, travel, use of data carriers, storage of data, backup etc.); in particular if the user has administrative rights
- Use of authentication procedures (username/password, PIN, biometrics, etc.)

What protection objectives are covered by the measure?

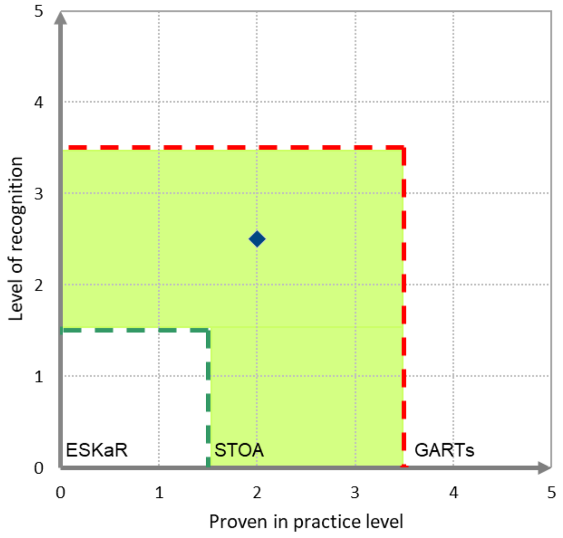
☒ Availability

☒ Integrity

☒ Confidentiality

☒ Authenticity

State of technology classification



3.2.23 *Using internet with web isolation*

Web isolation separates the user's desktop from browser sessions and enables secure Internet use without limiting content or functionality. Browser-assisted cyber attacks, data flow/loss and the associated productivity restrictions and image damage are effectively prevented.

Which IT security threat(s) is the measure used against?

Infection of the workstation computer, for example by

- Browser Vulnerabilities, Drive-by-Downloads, Infectious Websites
- Ransomware, APT, Trojans, Viruses, Worms
- zero-day exploits
- malicious links in emails

and thus spread of malware in the business-critical network.

Which measure (procedure, equipment or operating mode) is described in this section?

There are several ways to isolate browser sessions. The architecture used and its security mechanisms are decisive here. Examples are the so-called "remote controlled" browser environments or multi-layer local browser isolations.

A simple isolation of the browser environment (e.g. via simple virtualization based on Hyper-V or so-called browser sandboxing) does not offer a sufficiently high level of protection against the aforementioned threats, since it does not, for example, have a secure hardened operating system in which the browser runs as standard; does not use any additional secure network segmentation; does not enable secure copy & paste or does not use any additional security functions such as data locks. This is why this method is not suitable for countering the threats.

Remote controlled browser environments based on ReCoBS

The Remote-Controlled Browser System (ReCoBS) physically separates Internet usage from the user's work computer. Each browser session is executed outside the sensitive network area in a specially isolated environment within a specially hardened system on a separate hardware in a separate network segment (DMZ).

Via a technically secured communication channel, the browser is remotely controlled from the workstation via video stream on the remote system. The majority of attacks targeting Windows-based vulnerabilities are already successfully fended off in the hardened Linux environment. Further security mechanisms and zones in the overall architecture provide reliable protection against attacks even if the browser has been compromised. The physical separation of workstation and browser system also provides protection against hardware-related attacks (Spectre, Meltdown, ZombieLoad or vulnerabilities in the hypervisor).

At regular intervals (once a day by default), the remote system should be restored to its original state via a system image, so that any malicious code is effectively removed, and it must be ensured that the system image is preserved with integrity.

The user's workstation does not require direct access to the Internet at any time and is therefore additionally protected, e.g. against the reloading of malicious code by infectious documents that have reached the computer in other ways - e.g. via e-mail or USB stick.

Since the ReCoBS architecture allows common standard browser functions to be executed on the remote system, additional developments are necessary for user acceptance, so that the remote-controlled browser differs insignificantly from local browser use and all common functions such as personal bookmarks, copy & paste, printing or downloads and uploads are offered in principle.

For the optional transfer of files (browser download/upload) between remote system and workstation, additional checking mechanisms must be provided that quarantine conspicuous files and notify administrators. An example of such a checking mechanism is virus protection in the data gateway.

In addition, a central management of the overall solution is recommended so that, for example, an existing directory service can be linked and used to manage user roles.

Web isolation based on the local virtualization of the browser application

Another approach to web isolation is based on local encapsulation of the browser application through secure virtualization in combination with a right-limited Windows user account, hardened guest operating system and Internet/intranet separation through separate VPN tunnels to the Internet gateway. This prevents direct access from the browser session to the PC hardware.

One advantage of local browser isolation is the possibility of stand-alone use on mobile workstations. The non-existent physical separation between the sensitive workstation and the browser system could, however, allow local security gaps in the processor hardware or software to be exploited to break into the end device via an exploit package covering all protective layers.

What protection objectives are covered by the measure?

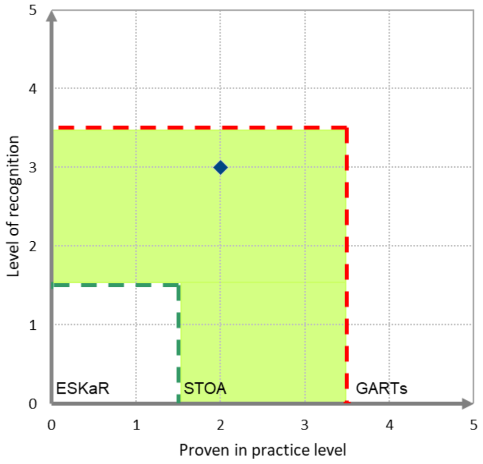
☐ Availability

☒ Integrity

☒ Confidentiality

☒ Authenticity

State of technology classification



3.2.24 *Attack detection and analysis (SIEM)*

Security Information and Event Management Systems (SIEM) are used to evaluate anomalies and detect attacks on the company infrastructure. They enable holistic, real-time recognition of security-critical events in the IT infrastructure and the implementation of appropriate measures (partially automated).

Which IT security threat(s) is the measure used against?

SIEM can help against the following threats:

- Attack activities by external parties (hacker attacks)
- Threats by insiders (e.g. unauthorized access to data from other departments, computer sabotage)
- Compliance violations

Which measure (procedure, equipment or operating mode) is described in this section?

A SIEM is used to collect log and event data from devices, network components, applications and security systems centrally. For example, the SIEM can map the following data sources:

- Log files from operating systems
- Firewall events from network firewalls
- Alarms from Intrusion Detection & Prevention Systems (IDS/IPS)
- Intelligent network sensors / network monitor systems with information about found assets / devices, vulnerabilities, compliance violations or abnormal network bevavior
- Directory services Authentication services (like Single Sign on systems)

- Endpoint Detection & Response Systems (EDR/XDR)

- Indicators to identify attackers and attacks such as IP addresses, hashes, hostnames, etc. (Threat Intelligence Feeds) as well as e.g. context information about attackers for enrichment

The security team in the company has the opportunity to obtain a holistic picture of the processes in its IT solution/infrastructure in real time through the targeted aggregation and analysis of security-relevant event and system logs. This makes attacks, unusual patterns and dangerous processes visible. Based on the knowledge gained, companies are able to react quickly and precisely to acute threats. Based on the available data, patterns can be analyzed in the wake of an attack (forensics) and existing measures can be improved.

Modern SIEM tools include reliable and immediately applicable detection rules that can be adapted to new threat scenarios. The operation of a SIEM solution requires the integration of suitable sources but also the provision of significant system resources (e.g. graph databases, data lakes and servers for operation and management). At the same time, a significant bandwidth utilization is achieved through continuous data exchange. The associated administrative complexity and the acquisition and operating costs are quite high, which is why the classic SIEM solutions are usually used in large and very large companies.

Cloud-based and third-party managed solutions such as SIEMaaS (SIEM as a Service) are a modern alternative with easily calculable costs. They enable the technology to be used in small and medium-sized companies as well. Similarly, a modern endpoint detection & response platform (DER/XDR) with its interfaces to Security Orchestration, Automation and Response (SOAR), network security products such as next-generation firewalls and integrated threat intelligence can be a sensible alternative.

What protection objectives are covered by the measure?

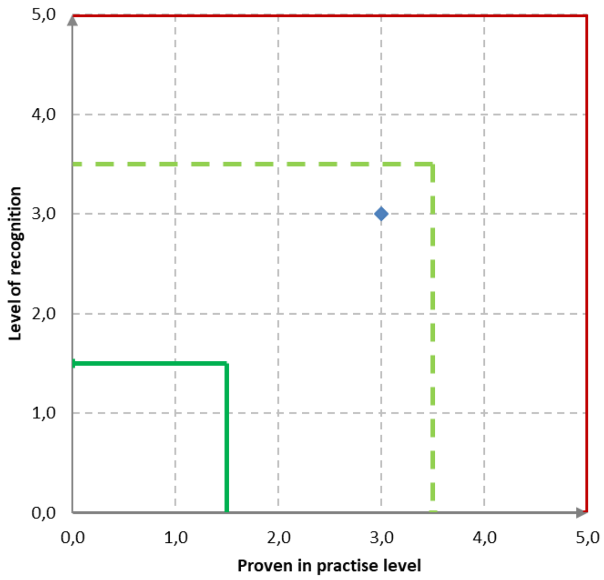
□ Availability

☒ Integrity

☒ Confidentiality

☒ Authenticity

State of technology classification



3.2.25 *Confidential computing*

Privileged access by administrators to data during processing is traditionally only secured with organizational or reactive measures against misuse of the privilege. With the help of confidential data processing (Confidential Computing), this data is tamper-proof and preventively protected against unauthorized access. This is particularly important for applications in the field of cloud computing. Confidential data processing corresponds to the protection requirement when cloud services are used for critical infrastructures or for sensitive data processing processes, e.g. in medicine, industry or in regulated areas (e.g. regTech).

Which IT security threat(s) is the measure used against?

Cloud administrators are responsible for the trouble-free operation of their systems. To be able to fulfil this task, they are granted numerous privileges. For example, they can adjust the system configuration and read out memory contents. This means that data can be compromised on its way into the cloud, stored in the cloud storage and during processing in the cloud not only by attacks from third parties but also by illegally acting employees of cloud service providers.

Which measure (procedure, equipment or operating mode) is described in this section?

Previous approaches to data access security relate to data at rest (storage) and data in transit (network). Confidential computing focuses on the protection of data during processing.

This is an area or capsule shielded from the outside world in which all data processing takes place in an unencrypted state. This shielding can be implemented either directly on the processor chip of the server and/or via several servers.

In order for the data to be processed, the necessary key must be available within the capsule. If an attacker were to attempt to gain access to the encapsulated area, the data processed there without encryption would inevitably be deleted as a precaution. In order to achieve increased security, the capsules can be sealed by independent auditors after prior examination using known cryptographic secrets.

In data processing systems equipped with the measures summarized under the heading "confidential computing", a single administrator cannot gain access to the data processed in the server.

Only a malicious coalition of several independent parties (e.g. system administrator together with their independent auditors) can override the technical measures. This reduces the probability of malicious access by several orders of magnitude.

Confidential computing

- allows data to be processed in central infrastructures without exposing them to the possibility of being read by the operators of these central infrastructures,
- offers users more control and, depending on the audit, also transparency
- offers new degrees of freedom, as new applications are conceivable that could not be implemented in a legally compliant manner under conventional data protection and security considerations.

What protection objectives are covered by the measure?

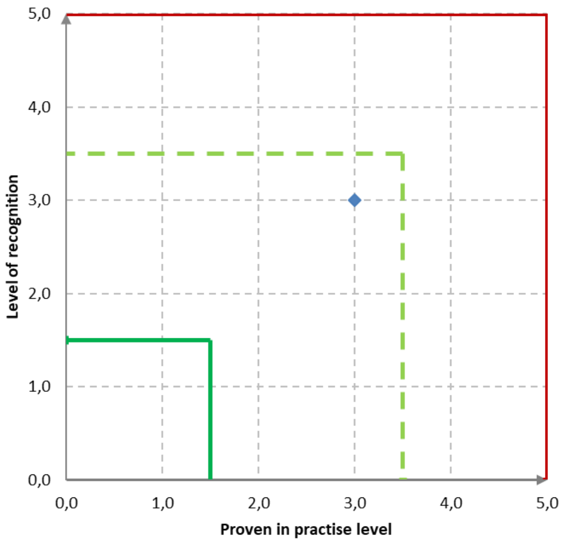
□ Availability

☒ Integrity

☒ Confidentiality

☒ Authenticity

State of technology classification



3.2.26 *Sandboxing for malicious code analysis*

Sandbox technology is used to run potentially dangerous files in an isolated environment and check for malicious behaviour. Running in a separate environment prevents possible infection.

Which IT security threat(s) is the measure used against?

- Hacker activities in general
- Malware (viruses, Trojans etc.)
- Phishing

Which measure (procedure, equipment or operating mode) is described in this section?

The use of the sandboxing method for automated malware analysis is common in two use cases:

Perimeter sandboxing

In perimeter sandboxing, file attachments (such as documents from the active environment, but also embedded content such as scripts) from e-mails are usually executed automatically. Sandbox analysis at the e-mail gateway usually generates a latency in access to the examined file attachment by the user, which is in the range of a few seconds to minutes.

Sandboxes can also be used at the web gateway (next-generation firewall or proxy) to check downloaded programs, for example. Here, too, a delay is caused before the file is delivered to the user. In addition, the use also influences the behavior of the browser and web-based software. Therefore, in addition to the classic sandboxing function (first check that delivery is delayed), a delivery of the file to the terminal device with parallel checking is also practiced. If malicious code is identified during the latter procedure, subsequent measures are taken. These include network isolation, blocking of "command and control" addresses that were identified during sandboxing.

Sandbox for the forensic examination of files that were detected or identified during

By connecting sandboxes to next-generation antivirus products (machine learning-based antivirus) and EDR solutions (endpoint detection and response), files with a harmful prognosis or from detected and actively suppressed chains of attack can be safely executed outside the effective environment. The execution then enables the extraction of further relevant indicators (files/hashes, URLs, IP addresses, registry activities, etc.) which provides more context to a case under investigation and even allows the attribution of a suspected attacker.

As sandbox solutions are quite widespread, attackers always try to prevent detection in a sandbox. For example, when executing their malicious code, they try to determine whether it is a virtualized runtime environment - as is usual with sandboxes - or an active environment with certain programs/processes and other specific features. The malicious code will then usually behave harmlessly in order to prevent its detection. However, this behavior can also be detected in the sandbox and used to identify suspicious content (cat and mouse principle).

The exploitation of so-called "Day-0 Exploits"/ Zero-Day Threats, i.e. weak points that are as yet unknown to the public, can also lead to sandbox circumvention. It can also happen that the emulated runtime environment does not correspond to the victim system and thus the behavior when executing in the sandbox differs from that on the target system of an attack. It is therefore necessary to master these tactics known as "sandbox evasion", for example by combining static and dynamic analysis.

Sandboxes also offer a great benefit due to their high degree of automation, massively reducing the need for manual analysis of malicious code (so-called malware reverse engineering) by an expert.

There are many open source and commercial sandboxes. These are offered as mostly cost-intensive hardware solutions, but also as public or private cloud solutions. Sandbox technology has also been used in browsers for some time now to detect common types of attack at an early stage.

What protection objectives are covered by the measure?

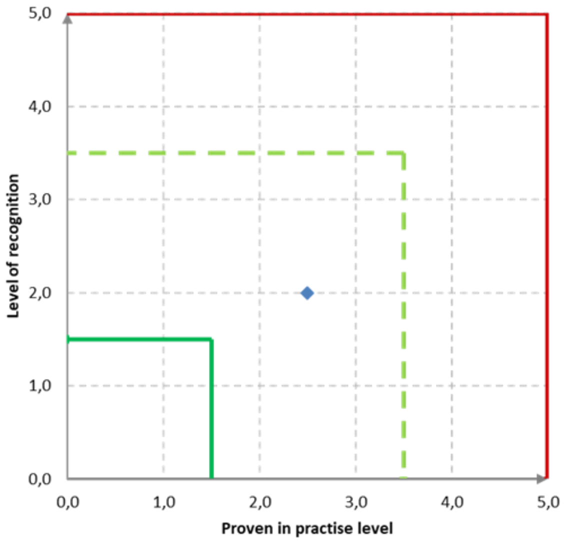
☐ Availability

☒ Integrity

☒ Confidentiality

☒ Authenticity

State of technology classification



3.2.27 Cyber threat intelligence

Cyber Threat Intelligence is an important element of modern defense strategies and provides indicators, reports and services to keep abreast of current attacks, identify cyber-attacks, determine their presumed authors and derive countermeasures.

Cyber Threat Intelligence is divided into three application areas:

- Tactical Cyber Threat Intelligence includes malware analysis and the import of individual, static and behavioral threat indicators into defensive IT security solutions such as network, endpoint and application security solutions to increase their effectiveness. Indicators obtained through Cyber Threat Intelligence can play an important role in measures such as system patching.

- Operational Cyber Threat Intelligence is used to improve knowledge about an attacker, his skills, infrastructure and attack tactics, as well as techniques and procedures (TTPs). This information can be used to implement significantly more targeted cyber security measures such as incident analysis, incident response and proactive threat hunting. This improves the performance of cyber security staff (e.g. from the Security Operation Center or CERT) such as threat hunting experts, vulnerability managers, incident response analysts and insider threat prevention experts.

- Strategic Threat Intelligence enables a better understanding of the current threat situation (threat assessment), the derivation of trends and the motivation of individual attacker groups. It supports strategic business decisions to improve cyber security.

Which IT security threat(s) is the measure used against?

Cyber Threat Intelligence provides information on all types of current and potential cyber threats and helps to defend against them.

Which measure (procedure, equipment or operating mode) is described in this section?

1. Tactical Cyber Threat Intelligence (TM)

Integration of threat indicators (feeds) into existing endpoint and network detection & response systems, system management solutions, firewalls, IDS/IPS and SIEM/SOAR solutions with the aim of identifying real attacks and supporting analysis (including retro hunting), as well as preventing compromises. For optimal effectiveness, it should be possible to use the indicators automatically for the detection and prevention of cyber-attacks. The sources for Threat Intelligence Indicators allow conclusions to be drawn about their reliability and are differentiated into:

- Open Source Intelligence (OSINT),
- Events from private honeypot systems,
- insights from attack analyses from real customer environments, or the
- Investigation work by experts trained by the secret services

2. Operational Cyber Threat Intelligence (TM/OM)

Organizations that operate a Security Operation Centre (SOC) and may have their own Computer Emergency Response Team (CERT) use Threat Intelligence operationally to keep themselves continuously informed about the actors and their TTPs. For this purpose, comprehensive Threat Intelligence platforms offer access to indicators, various report formats (short reports, situation reports, attacker profiles), access to malware databases, sandbox technology for automated malware analysis and malware reverse engineering. The provider should be able to cover customer-specific requirements. Furthermore, it should be possible to access analysts at the provider directly and to submit research requests (RFIs).

3. Strategic Threat Intelligence (OM)

Both the information security sector and the overall/corporate security of large companies use Threat Intelligence to obtain as complete a picture of the situation as possible. The geopolitical situation as well as sector-specific and global trends in the threat landscape are at the forefront of this. By having access to a dedicated employee at the provider, the own team is virtually expanded and it is ensured that direct access to the provider's data pool is possible and that customer-specific investigation work is optimally performed.

Providers of modern IT security solutions deliver, integrate and automate Threat Intelligence, so that threat indicators and relevant attack telemetry are meaningfully linked, preventive measures are automated and attacker attribution is made possible without the user needing additional systems or even personnel resources.

What protection objectives are covered by the measure?

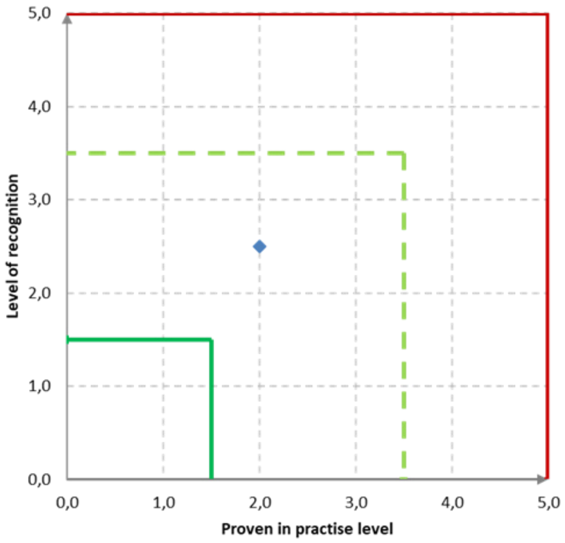
☒ Availability

☒ Integrity

☒ Confidentiality

☐ Authenticity

State of technology classification



3.3 Organisational measures

Because information and communication facilities are not always designed for security as a matter of principle and technical security is only effective when adequately accompanied by organisational and staffing measures, every organisation needs a system of methods, procedures and rules for managing corporate information security, or in other words, an Information Security Management System (ISMS).

An information security management system (ISMS) establishes and implements rules for classifying and dealing with sensitive information. The ISMS is an important component of the management system and runs through all important areas of the company. The ISMS includes methods for regular inspection and documentation of organisational and technical changes.

One important focus of the ISMS is considering changes in information security when important elements of the IT structure are scheduled to be modified or maintained. Another aspect is regular training and raising awareness for staff. The information security management system also determines how to carry out emergency prevention and how to respond to potential security incidents. The objective of the ISMS is to guarantee and maintain on a long-term basis a level of security that is efficient and consistently adequate.

In their “Information Security Management - Practical Guide for Managers" document, TeleTrusT has provided a workable guide for managing information security. The document shows that with information security management and the compliance and risk culture associated with it, there can be a strategic control instrument that illustrates the security situation at a glance.

3.3.1 Standards and norms

There are a number of international standards and norms that can serve as the basis for implementing an ISMS. Unlike with technical measures, the continuous changes in organisational measures are a long-term phenomenon, meaning that reference to standards and norms is possible even in the context of “state of the art." The ISO/IEC 27000 series is used as a reference point for further standards and norms. There are some overlaps, though the overlaps are generally used as synergies, resulting in a positive impact on the standards used, within the meaning of information security. Insofar as additional standards or norms are implemented for managing IT services, processes or risks, the overlaps addressed should be identified and used.

The ISO 27000 standards

The ISO/IEC 27000 series (sometimes also known as “ISO27K" for short) is a series of standards for IT security. These standards are issued by the International Organisation for Standardisation (ISO for short) and the International Electrotechnical Commission (IEC for short).

ISO/IEC 27001 is the most well-known standard in the ISO/IEC 27000 series. It formulates the requirements that must be met by an ISMS. There are other standards and guidelines for concrete implementation as well.

The ISO/IEC 27000 series includes the following key items, each of which functions as an independent standard and grouped together are a series of standards.

ISO/IEC standard	Tasks
ISO/IEC 27000	Terms and definitions used in the ISO/IEC 27000 standard series
ISO/IEC 27001	Requirements for an ISMS
ISO/IEC 27002	Recommendations for various information security control mechanisms
ISO/IEC 27003	Guide to implementing ISO/IEC 27001
ISO/IEC 27004	Assessment of ISMS effectiveness
ISO/IEC 27005	Developing and operating an information security risk management systems
ISO/IEC TR 27019	Information security management for energy supply systems based on ISO/IEC 27002
ISO/IEC 27031	Guide to concepts and principles regarding IT support for business continuity in an organisation
ISO/IEC 27034	Application Security
ISO/IEC 27035	Information Security Incident Management

Table 1: Overview of ISO/IEC 27000 series

Other standards and norms

Information security standards and criteria can be classified as company, system and product standards depending on the level at which they are considered. They can be grouped into technical, less technical and non-technical standards based on their formulation.

The structure levels mentioned above can be outlined as follows based on an earlier description of initiative D21:

Company		**BSI Standard 100/ ITGS catalogue**	**ISO 9000** **ISO 20000** **ISO 27000** **ISO 22301 CobiT** **The Standard**

	technical	less technical	not technical
System		ICPP data protection seal of approval, EuroPriSe, TÜViT Trusted Process/Site/ Product	
Product	ITSEC ISO 15408 (CC) ISO 19790 (FIPS 140)		

Figure 5: **Structure levels of standards relevant to information security**

The requirements of the limitations outlined in ISO 27001 of ISO 9001, ISO 20000-1, ISO 22301, CoBIT and The Standard apply in particular as a standard for companies and public institutions (organisations) formulated using non-technical language.

ISO 27000 et seq.

The series of standards in ISO 27000 et seq. includes several standards regarding ISMS. A crucial standard in this series is ISO/IEC 27001, which describes requirements for a functioning information security management system in the context of an organisation (see 3.3.1.1).

ISO 27001 based on BSI's IT basic protection

This is the implementation of ISO 27001 using the IT basic protection catalogue (IT Grundschutz) of the German Federal Office for Information Security (BSI)(also documented in BSI standard 100-2).

The BSI standard 100-1 sets the general requirements for an ISMS. In principle, it is compatible with ISO standard 27001 and furthermore considers the recommendations of other ISO standards in the ISO 2700x family, such as ISO 27002. It offers anyone interested an easily comprehensible and systematic introduction and set of instructions, regardless of which method they would like to use to implement the requirements.

With the procedure described by IT basic protection (IT Grundschutz), BSI standard 100-2 gives:

- specific and methodical assistance for step-by-step introduction of a management system for information security
- consideration of the individual phases of the information security process
- solutions derived from practical experience, i.e. "best practice" approaches
- possibility of certification

The limitation of the “native" ISO 27001 implementation of the basic protection approach from BSI can be found in the table below:

Category	ISO 27001	BSI's IT basic protection
Regulatory scope	Relevant standards < 100 pages	Basic protection catalogue > 4000 pages
Requirements	Abstract and generic framework conditions	Specific template for practical measures
Risk analysis	Full analysis of each target object	Simplified analysis in the event of increased protection requirement
Measures	67pprox.. 150 conceptual requirements	> 1100 specific measures
Certification	Certification	Auditor certificate + certification

Validity	3 years, annual monitoring audits	3 years, annual monitoring audits

Table 2: Differentiation of ISO 27001 vs. BSI's IT basic protection

ISO 20000-1
This standard specifies requirements of (internal or external IT) organisations regarding the performance of process-oriented services. Some of the processes required (primarily information security management, incident & event management and service continuity management) overlap with ISO 27001. Conventionally, ISO 20000-1 is applied to IT organisations, while the scope of ISO 27001 can cover all types of organisations.

ISO 22301
This standard is concerned with securing business continuity (Business Continuity Management, BCM for short) and specifies requirements of business continuity management systems in organisations. BCM systems as described in ISO 22301 also refer to IT (but not only to IT). The scope of ISO 27001 also covers BCM, but only from the perspective of information security (i.e. to what extent business continuity can be endangered by information security incidents).

ISO 9001
This standard specifies requirements of quality management systems, but also includes an incredible number of information security considerations, e.g. some relating to obligations regarding

- securing the availability of resources and information on the implementation and monitoring of processes
- labelling, storage, protection and retrievability of logs
- determination, provision and maintenance of infrastructure such as buildings, places of work and associated pension institutions, process equipment (e.g. hardware and software) and supporting services (e.g. communication and information systems)
- protection of customer property, such as intellectual property, personal data etc.

CobiT
CobiT is a method of controlling risk resulting from the use of IT to support business-relevant processes. It is a 'toolbox' for management oriented towards revision and controlling that defines results and performance measurement for all IT processes. CobiT describes several process areas, each with defined control aims, maturity models and measures. CobiT relates to all IT processes, while ISO 27001 focuses on the control of information security processes.

The Standard
ISF's Standard of Good Practice for Information Security is a good practice approach for business information security that also permits security benchmarking. The Standard handles several areas of information security (e.g. IT security management, business-critical applications, information processing, communication/networks, system development) from a business perspective and offers an alternative, sometimes with a view to complementing/supplementing ISO 27001.

3.3.2 Processes

According to the German Federal Office for Information Security (BSI), it is impossible to describe industry standards in a way that is definitive and applicable to all areas. Instead, they can be "determined using existing national or international standards, such as DIN or ISO standards, or using templates successfully applied to the relevant area in practice".

For companies directly or indirectly affected by ITSiG, this means that compliance with, testing of and certification of a multitude of general and sector-specific standards is required.

The sections below contain a short description of the organisational measures required, as well as an assessment of what standards from the ISO/IEC 27000 series should be implemented to meet the state of the art. The contents of this chapter are to be used as a guide. Constant technological advancement, however, ensures that even official frameworks and standards are subject to constant updates.

Consideration of the ‘state of the art’ therefore requires individual investigation of the extent to which an individual measure or bundle of measures is suitable, necessary and reasonable at a specific point in time.

In contrast to the technical measures according to which systems or technical processes ensure that information is protected, organisational measures describe (for example) processes, work instructions, guidelines or similar that are self-imposed by a company and are intended to increase security. Implementation and compliance are usually the responsibility of the people involved and are best supported by technical measures. Regular control and training ensure that the planned measures are correctly implemented.

The active support of management and the cooperation of specialist departments is critical when introducing an information security management system. Risks that affect company infrastructure, personnel, IT, processes and information, and that have a negative effect on one or more basic values of information security (e.g. confidentiality, integrity, availability), must be identified and assessed.

The following are the primary organisational processes and measures that can be derived from “state of the art" practices.

3.3.2.1 Security organisation

Security organisation aims to establish a management framework. The description of security organisation includes the tasks and responsibilities involved in initiating and monitoring the implementation and operation of information security within the organisation.

So that an ISMS can be successfully introduced and operated, the most senior management must

- take on overall responsibility for the ISMS and information security in the organisation
- be sensitised and inform all relevant responsible persons and employees of any potential risks, personal liability in the event of non-compliance with requirements, and the opportunities of an ISMS for the organisation itself and they must also pass on responsibilities regarding information security
- define, implement and continually improve effective security organisation in the form of roles, responsibilities and authorisations
- Meanwhile, the following must be established with a view to managing information security: organisational structures (e.g. departments, groups, competency centres), roles and tasks.

The following are minimum requirements of a security organisation:

- nomination of a responsible manager (which chairperson or director is directly responsible for information security?) and
- nomination of a chief information security officer (CISO) as a central role within an IS organisation.

The following basic rules must be observed under all circumstances:

- Overall responsibility is on the management level
- Every employee is responsible for information security in his/her working environment.

The important roles and responsibilities within a security organisation are:

Upper management (directors, board)

- Strategic responsibility (dedicated), but in the last instance, overall responsibility for information security as well
- Responsibility for all risk-related decisions

Chief Information Security Officer (CISO)

- Tactical or (sometimes) operational control of information security
- Support of management in IS task awareness
- Staff position with direct right and obligation to report to the highest level of management

Information Security Officer (ISO)

- Operational control of information security, tactical tasks for individual divisions where necessary
- Organisationally directly allocated to CISO

IS Management Team/IS Management Forum/Security Steering Committee

- Permanent committee to coordinate planning and implementation of measures for information security
- Consists of CISO, ISO(s), deputies for implementation, specialist managers, data protection officer, representatives of senior management
- Consultation and control function for CISO

Data Protection Officer

- Should not necessarily be seen as part of IS management team, but instead as an important contact in matters regarding compliance, ideally regularly involved in the IS management process

Audit Manager

- Central contact for internal and external audits
- Coordinates and controls planning and execution of audits
- Supports CISO in their tasks.

Organizational measures correspond to the “state of the art", if their implementation follows the currently valid standards. At minimum, standards ISO/IEC 27000 to ISO/IEC 27005 of ISO/IEC 27000 series must be observed in implementing these measures. If other applicable requirements, standards or results of risk assessments require them, other organisational measures may be necessary.

3.3.2.2 Requirements management

A targeted and effective ISMS can only be put in place within the context of the specific organisation and its requirements for information security. For this reason, requirements relevant to security must be determined and their implementation must be planned, realised, checked and constantly improved.

Requirements management forms the basis for orienting information security as a process and a state within the organisation.

The continuous fulfilment of requirements guarantees that interested parties (i.e. stakeholders) in an ISMS are satisfied. Because of the complexity of this, the establishment of a requirements management process is recommended.

The requirements of an organisation can be divided into:

- legal requirements,
- contractual requirements and
- other requirements.

Legal requirements arise from various areas of law, such as data protection law, labour law, IT law, criminal law, and many more (no unified "information security law" exists). However, requirements (and expectations), increasingly regarding traceable information security, may be put in place by various business partners of the organisation (e.g. by customers, suppliers, service providers, outsourcing partners, cooperation partners, insurance companies etc.).

Legal and contractual requirements are often called "primary" or "basic" requirements because they form the basis of the IS process.

Other requirements (and/or expectations/limitations) typically arise from the following entities:

- market
- general public
- company, head office
- shareholders
- employees
- business processes (incl. internally defined policies)
- technology.

A state-of-the-art requirements management process can be represented in a P-D-C-A model as follows:

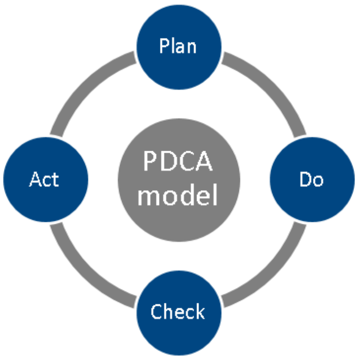


Figure 6: PDCA model

PLAN: All types of requirements and expectations of the institution,

- recording,
- analysing
- assessing and
- converting into internal (security) specifications for the institution.

DO: Meeting information security specifications of the institution (and therefore implicitly the requirements and expectations of the institution as well), e.g. in the form of:

- organisational measures: policies, regulations, guidelines
- personnel-related measures including personnel review, sensitisation, continual training
- technical measures of access control, encryption etc.
- infrastructural measures for access control, safety zones

CHECK: Monitoring and reviewing the degree to which institutional information security specifications are met (and therefore implicitly the requirements and expectations of the institution as well):

- querying indicators and parameters
- identifying deficits (in interaction with the stakeholders)
- planning corrective measures.

ACT: Continually improving the degree to which institutional information security specifications are met (and therefore implicitly the requirements and expectations of the institution as well):

- implementing corrective measures and checking their efficacy
- communicating improvements.

Effective requirements management guarantees compliance with legal, contractual and other requirements and ensures that violations of legal, regulatory, contractual and other obligations with regard to information security are avoided.

Positive assessment of the ISMS and the information security achieved by this ensures that they are implemented appropriately and are operated in compliance with company guidelines, processes and relevant requirements.

3.3.2.3 Management of scope of application

The scope of application of an ISMS should always take into account the organisation's information security requirements. The scope of application is developed accordingly. Corresponding changes should be planned and implemented carefully. Documentation and justification for the scope of application must be kept to prove that it is compliant with the strictest industry standards.

3.3.2.4 Management of information security guidelines

As a basis for an information security management system, company management must be oriented towards information security. The goal is that company management will provide a direction and the protective goals will be commensurate with company requirements and the relevant laws and regulations.

In order to comply with the "state of the art", information security policy and information security objectives must be defined in the form of a guideline and made known within the organisation. Furthermore, sufficient resources must be provided and the importance of meeting the requirements must be communicated. The guiding principle (including the information security goals) should be checked at least once per year to ensure they are up to date and improved if necessary.

3.3.2.5 Risk management

Risk management consists of systematic risk assessment and identification, monitoring and handling of risk areas. The goal is to systematically identify opportunities and risks to a company and to assess these risks with reference to the likelihood they will occur and to their quantitative effects on company values.

For state-of-the-art risk management, guidelines must be established to determine the organisation's values, weak points, threats, effects and likelihood of events and the permissible extent of residual risk. The methodology for implementing risk assessment and treatment, as well as adoption of residual risks by senior management, must also be established.

Existing risks must be analysed, assessed and handled on this basis. Residual risks must be taken on by senior management in a demonstrable manner and the overall risk exposure of the organisation must be continually optimised.

Further details are explained in the chapter "Management of Information Security Risks".

3.3.2.6 Management of statement of applicability

A statement of applicability must continually update documentation recording which controls from Annex A of ISO 27001 (and other security measures where applicable) are applicable and which are not, the reasons for this decision, and a description of how these measures must be implemented. The statement of applicability communicates a current picture of the target and actual state of information security in an organisation in the relevant review cycle in accordance with state-of-the-art practices.

3.3.2.7 Resource management

The organisation must determine the resources required for the development, implementation, maintenance and continual improvement of the ISMS and constantly adjust the actual requirements.

State-of-the-art practices require that the resources provided meet at least the basic requirements.

3.3.2.8 Knowledge and competency management

For an ISMS to be managed professionally, the persons responsible for it must have the corresponding competencies or be trained to this level through further education. To meet state-of-the-art practices, the need for knowledge and competencies must be determined, the competencies must be acquired and the actual need must be constantly adjusted.

3.3.2.9 Documentation and communication management

The goal here is to document both the assessments and the actual state of the ISMS and information security, including the achievement of goals, how risks are handled and how requirements are met and to communicate this to interested parties, taking into account the requirements of target groups.

To meet state-of-the-art practices, the necessary documentation must be created and communicated demonstrably for all controls that are checked.

3.3.2.10 IT service management

IT service management provides a procedure on all IT management levels, as well as all actual levels, beginning with business orientation and including service methodology and information security, through to implementation and infrastructure management and the use of technology associated with this. It is important to embed the security process in the process landscape of the company.

In addition to the interfaces and processes described in the TeleTrusT+ document “Information security management - a practical manual for managers", the following processes must be followed to comply with state-of-the-art practices:

Asset Management
Asset management describes three aspects important for company values and forms the basis for analysis and assessment of risks (see also 3.3.2.5). The responsibilities, classification and handling of media. To determine responsibilities, company values are identified and suitable responsibility for protection is defined. Once the values and roles of responsibility are defined, it must be ensured using the classification that the information is subject to a suitable level of security commensurate with its importance to the organisation. A guideline on handling media ensures that unauthorised dissemination, alteration, disposal or destruction of information stored on media is avoided.

Training and awareness
The sensitisation of employees is an important prerequisite to the implementation of the desired level of security. Employees should know how important information security is to the organisation and how they can personally contribute to reaching this goal. They should also know how to conduct themselves if they suspect, or uncover, a security incident. So that they can perform these tasks effectively, employees should be trained periodically in the interest of information security so that they are aware of all relevant organisational and technical conditions. Training helps employees to operate (IT) systems properly and comply with all necessary regulations. These aspects must be controlled as part of the resource management process if applicable (see 3.3.2.7).

Operation

The operation of a security organisation and environment serves to maintain everything necessary to keep the network, computer and server systems, applications and solutions in a secure and protected state. It ensures that employees, applications and servers have the correct permissions to access the resources they need and that monitoring, audits and reporting are controlled. Operation takes place after implementation and system testing and ensures continuous maintenance, updates and monitoring.

Reference models and IT service management (e.g. ITIL) provide a framework for successful operation. This allows information security management processes to be tightly coordinated with other IT processes.

Incident Management
Incident management combines technical and organisational measures in response to identified or potential security incidents. In addition to detection, analysis and management of problems, weak points and targeted attacks, methods for dealing with incidents of this nature are also described and planned, which also includes organisational and legal considerations.

The objective of incident management is to promote planning and identify and implement requirements so that effective, efficient measures to protect the organisation can be implemented without delay in the event of an incident.

Continuity Management
Continuity management involves summarising technical and organisational measures for avoiding business interruptions. In addition to recording, analysing and managing the risks of failure and their effects along the timeline, it also describes and plans how to deal with the escalation of incidents in emergencies, including organisational and legal issues.

The objective of continuity management is to promote planning, identify and implement requirements so that effective, efficient measures to protect the organisation can be implemented without delay in the event of an emergency.

Procurement
Prior to the actual procurement of IT systems or services, there are some preparatory steps to take to ensure that the result meets the company's requirements. This applies to aspects related to both content and security. These points include:

- Requirements analysis
- Risk analysis
- Security analysis (requirements regarding function and reliability)
- Test and acceptance plan.

If suppliers are involved in providing software, solutions or services in the longer term, it must be ensured that corporate assets accessible to suppliers have guaranteed protection. This includes, in particular, service level and a level of security described in a supplier agreement.

Software development and IT projects
IT projects must address the issue of information security transparently and quantifiably from the outset. Project organisations in companies need to move towards a more rigorous, repeatable process that includes the issue of security as a basic component in each phase and determines binding responsibilities for the security manager in each stage of the project. These targets must be reinforced and legitimised by company management. During phase transitions in particular, a formal rule for approval must be made to emphasise the obligatory aspect of “secure by design" in the IT process.

Experience shows that the security team should coordinate closely with the project team, especially in the planning and implementation phase. The security team should define additional security requirements and a binding security architecture, as well as conduct a threat analysis. The results are then incorporated into the overall concept, preventing expensive corrections at later phases in the project. (see chapter 3.3.3)

3.3.2.11 Performance monitoring management

This process includes all monitoring, measuring, analysis and assessment activities related to the ISMS and the information security produced in this context. These must be monitored and inspected for compliance with “state of the art." This means, among other things, recording and regularly evaluating protocols, but also conducting internal audits and technical system audits at regular intervals to obtain information about whether the ISMS and the information security produced by it (still) satisfy the requirements, have been effectively implemented and are being upheld. The top level of management must evaluate the ISMS at least once a year to determine whether and to what extent it fulfils its defined purpose and contributes to the implementation of information security objectives. This constitutes the basis for further decisions.

Technical system audits, internal and external audits can be considered sub-processes (see below) of the process discussed here. The same is true for all other categories of monitoring, measuring, analysis and assessment activities.

3.3.2.11.1 Technical system audits

Technical system audits (inspections at the network, system and application level) must be performed regularly by or on behalf of the organisation. These are typically carried out as penetration tests or web checks.

- For a small IS penetration test, configurations and policies related to security in the IT systems used are examined randomly in the form of a technical audit, and recommendations are given for eliminating any vulnerabilities. IT system inspection is carried out jointly with the administrators.
- For a comprehensive IS penetration test, in addition to the technical audit, vulnerabilities in the IT systems tested are rooted out through technical investigations using special security tools, among other things. In doing so, the testers access the IT systems to be inspected on site under supervision by the administrators.
- An IS web check inspects the security status of the organisation’s internet, intranet and/or extranet presence. The majority of the tests in this process are performed using automated methods over the internet and, where applicable, via the internal network (for intranet and extranet).

3.3.2.11.2 Internal and external audits, ISMS certification

ISMS audits serve the following purposes:

- Checking the progress of implementing the ISMS
- Determining the ISMS’s compliance with the organisation’s audit criteria
- Determining the ISMS’s ability to meet legal, regulatory and contractual requirements
- Checking the ISMS’s utilisation and effectiveness
- Identifying vulnerabilities/potential for improvement in the ISMS

Internal audits within a scope of application of the ISMS must be performed at least once a year as a general rule by or on behalf of the organisation. To meet the state of the art, each organisational unit (or each component of the scope of application such as location, building, etc.) is internally audited at least once every three years.

External ISMS audits are performed by parties interested in the organisation (e.g. Customers) (second party audit) or by external, independent auditor organisations (third party audit).

As part of conducting certification audits, the audit team checks that the requirements from ISO 27001 are met, which must be implemented with consideration for standards ISO 27002 and ISO 27005. Auditors from certification bodies are required to comply with ISO 19011 and ISO 27007 standards in the course of the audit procedure. ISO/IEC TR 27008 includes a guide on auditing ISMS controls and is likewise applicable.

The certification body undertakes the following tasks as part of a certification procedure:

- Checking the audit results including audit conclusions
- Documenting the review of the audit results including audit conclusions
- Certification report with certificate approval
- Issuing the certificate.

Accredited certification bodies for ISO 27001 have accreditation according to ISO 17021 and ISO 27006 An overview of bodies accredited in Germany for ISMS certification can be found on the website of the National Accreditation Body (DAkkS).

Certification under ISO 27001 is valid for three years and is observed as part of “surveillance audits" at least once a year. If the certificate is renewed after three years, the organisation must successfully pass a re-certification audit before the three-year period has expired.

3.3.2.12 Improvement management (continual improvement process)

The organisation must continually improve the adequacy, suitability and effectiveness of their ISMS.

The essential activities related to maintenance and continual improvement of an ISMS are intended to evaluate and continually optimise the ISMS performance. The following aspects must be addressed here in particular:

- Dealing with non-conformities resulting from monitoring, measuring, analysing and assessing the ISMS and the information security produced in this context
- Defining and implementing corrective measures to eliminate the cause of non-conformities

Continual improvement of the adequacy, suitability and effectiveness of the ISMS and the information security produced by it.

3.3.3 Secure software development

The security of an application must be considered throughout the entire software development process. Measures for secure application development must be taken into account, regardless of the development method used. Procedural models and best practices for secure software development are described in BSIMM, OWASP SAMM, OWASP ASVS, the BSI Guidelines for the Development of Secure Web Applications or ISO/IEC 27034 and taught in TeleTrusT Professional for Secure Software Engineering T.P.S.S.E.. The essential protective measures within the software development process are listed in the individual chapters.

3.3.3.1 Requirements analysis

Secure application development begins with requirements analysis. The foundation of the requirements analysis is a threat analysis. The (company) assets to be protected must be defined and the threats that exist for these assets described. The architecture of the application - in particular the data retention and the data flows - as well as their confidence borders must be considered. The risks of these identified threats must then be assessed and countermeasures and security requirements for the application derived. A helpful method for identifying concrete threats is a definition of so-called abuse cases. These describe concrete attacks as well as the desired behavior of the application in the event of an attack. Further security requirements for the application result, for example, from legal regulations or contractual obligations. These security requirements, like the functional requirements, flow into the subsequent design phase of the software development process and also into the specification of the test cases for the later tests of the application.

The Volere template[28], which is often seen as the standard of the general requirement specification, already defines a number of security requirements that should be considered:

- 15a. Access Requirements
- 15b. Integrity Requirements
- 15c. Privacy Requirements
- 15d. Audit Requirements
- 15e. Immunity Requirements

3.3.3.2 Software design

A secure design must take all security requirements into account in order to counteract the identified threats. One result of the design process is the security architecture including a data handling strategy. A secure design considers aspects such as secure authentication, cryptographic requirements, error handling, system configuration, trust relationship between application components and the business logic of the application. An insufficient consideration of security in the design of an application is often the cause of weak points in the application, such as missing or incorrect authentication and authorization, and can only be remedied with great effort afterwards. Other causes are keys or passwords built into the code, incorrect handling of sensitive data or insecure error handling that provides the attacker with useful information. Adherence to Secure Design Principles helps an architect to create a robust design for his application. Examples of such proven design principles are Least Privilege, Defense in Depth or Secure by Default. Design principles such as Privacy by Default are becoming increasingly important, especially with regard to the EU Basic Data Protection Regulation. In addition, so-called design patterns and security best practices can be used by an architect which, in contrast to design principles, offer a more concrete, yet language-independent approach to solving recurring problems. The design, or at least the design aspects relevant from a security perspective, must be subjected to a design review before the implementation of the application begins.

3.3.3.3 Implementation

Typical implementation errors, such as the unchecked processing of input including the output of this data or the blending of code and data, can lead to security vulnerabilities such as injections, cross-site scripting or buffer overflows. Specific programming guidelines help developers to focus on security during implementation. These should be individually tailored to the programming languages, libraries and frameworks used. When using frameworks, these must be used correctly in order not to undermine their security functions. For example, it can be specified that only certain functions and objects may be used or that software modules may only be checked in after successful testing with a code analysis tool. Using static code checks, the source code must be automatically checked for typical implementation errors. The source code or at least the security relevant parts of the source code (according to the results of the threat analysis) should additionally be subjected to a manual code review.

However, weaknesses in the application can also result from the use of unsafe components from other manufacturers. Therefore, such components must be carefully selected and the security bulletins published by these vendors as well as the CVE database of known vulnerabilities must be continuously checked. Such third-party component auditing should be performed automatically using a dependency checking tool. When using application deployment programs, such as container solutions, these must also be checked for known vulnerabilities.

3.3.3.4 Security tests

Using black box/grey box/whitebox tests as well as static and dynamic security scans, vulnerabilities in the application are searched for. If applicable, a combination of black box/grey box and whitebox tests as well as static and dynamic security scans should be preferred in order to achieve the highest possible efficiency. For example, encryption algorithms used can be easily identified and evaluated by static

[28] https://www.volere.org/templates/volere-requirements-specification-template/

analysis of the source code, whereas security gaps that arise due to the integration of different components or only at runtime (such as in communication with an authentication service) are well identified by dynamic scans of the system. In contrast to manual penetration testing, security scans can be automated as part of the software development process to ensure a security check of each software version. In addition, the required security measures of the application must be checked during the test phase, i.e. the extent to which the application is protected against the attacks identified in the threat analysis. Defined abuse cases are a good source for creating test cases.

However, these security tests do not provide an absolute statement about the security of the application. Security cannot be proven - as with functionality tests - by the fact that expected behavior corresponds to observed behavior. Safety is a negative criterion; it usually consists of preventing undesired behavior. Here the creativity of an attacker is almost infinite. So there can still be further threats and thus also further test cases, which were not considered so far yet. Nevertheless, security tests are an important part of the secure software development process.

3.3.3.5 Protection of source code and resources

In order to preserve the integrity of code and resources and thus protect the application from manipulation such as backdoors, Trojan horses or changes in the flow logic, source code control systems should be used and, if necessary, individual code parts should only be assigned to specific developers. Sensitive information must not be stored in source code control systems in order to prevent it from unintentionally reaching the public. In addition, a secure development environment must be ensured by, among other things, restricting access rights and hardening systems, ensuring that developers only use personalized user accounts, do not work with admin rights, and are trained in security.

3.3.3.6 Software certification

Prior to delivery of the software, it makes sense to have it checked and certified by a neutral body. While the functionality of the software has been ensured by tests, certification ensures that the architecture, requirements management, configuration management and risk management are suitable for a secure development and, above all, troubleshooting process.
In order to be able to eliminate weak points later on, architecture and design should be designed in such a way that not only bugs can be eliminated, but also faulty components can be replaced in an emergency.

For more complex software, requirements management is essential. Before delivery, the requirements should be (re)checked whether they are clearly defined according to IREB (International Requirements Engineering Board). The implementation of requirements must be traceable to the source code. In the simplest case, this can be done by assigning identifiers, which are then also used in code comments. This makes it possible to react quickly to weak points that become known.

Configuration management is closely linked to requirements management. Here it must be checked whether a software version with source code and all its associated documents can be clearly assigned to a version status (and later to a software release). When requirements are changed, it must be clear which documents are already on a new status and which consider the requirements and which not. Since documents are developed further individually, the documents usually have different versions. Therefore, in addition to the mere versioning of the documents, a so-called baseline must also be defined, which determines which documents belong together in which version number and thus correspond to a release. This makes it possible to see which software version has already corrected which errors and weaknesses.

In the first step, risk management serves to become aware of possible risks and dangers that could occur, among other things, due to weak points. Risk management is especially essential when human lives can be endangered. In the case of software certification, it must be checked before delivery whether a risk management system is in place that

- Risks identified,
- Risks classified by probability of occurrence and severity,
- Risk mitigation measures defined,
- reclassify the risks after the measures have been implemented,
- is continued at regular intervals and in the event of changes.

If the software runs in a system group, the whole system group should be certified as well.

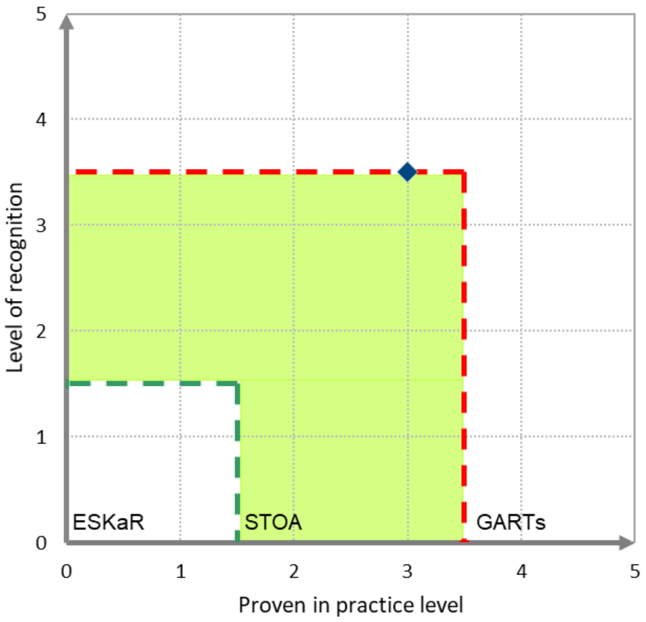
3.3.3.7 Software delivery

A vulnerability in the delivery and setup of the software destroys the result of all previous security measures in the software development process. Therefore, a secure delivery and deployment process must ensure the integrity of the deployed software to prevent the productive application environment from being compromised. Code signatures can be used for this purpose. Attacks on the deployed application can also be possible through an insecure configuration of the application itself. Therefore, a secure configuration of the software in the production environment must be ensured and unauthorized changes to the configuration must be prevented. Suitable standard settings (Secure by Default) and manuals for administrators are available here as security measures. In order to minimize the potential damage of an attack, the application must have as few permissions as possible (Least Privilge). Especially in container environments, applications are often executed unnecessarily as root users, which should be avoided at all costs. It is also essential for the security of the application that it is always kept up-to-date with security updates.

3.3.3.8 Security response

Since weak points can never be completely excluded, every manufacturer must be prepared for such notifications and be able to react quickly. The so-called Security Response Process of a manufacturer describes its approach in dealing with security problems that have become known to it. Security patches are time-critical and must therefore be delivered promptly. This includes self-developed components as well as known vulnerabilities in standard software such as libraries and frameworks. In order to motivate security researchers to report the vulnerability, Responsible Vulnerability Disclosure or Bug-Bounty programs are available. It is essential that reported vulnerabilities flow back into the software development process in such a way that they are eliminated.

State of technology classification



3.3.4 Process certification

To successfully implement information security and data protection in a company, processes must be identified and appropriate measures implemented. However, the implementation of such measures is only effective if their effectiveness is regularly reviewed. This review can be performed by internal or external resources. A special external effect, but not obligatory for all companies, is achieved by certification according to current standards. This chapter describes the possibilities of process certification.

Context Information Security

In the context of information security, an ISMS can be certified according to ISO 27001ff or (at least in Germany) on the basis of BSI IT-Grundschutz.

The ISMS certification audits have the following objectives:

- Checking the progress of the implementation of an ISMS
- Determination of the compliance of the ISMS with the audit criteria of the organization
- Determine the ability of the ISMS to meet legal, regulatory and contractual requirements
- Review of the application and effectiveness of the ISMS
- Identification of weak points / potential for improvement of the ISMS

Internal audits (so-called "First Party Audits") within a scope of the ISMS should in principle be carried out at least once a year by or on behalf of the organisation. These audits are mandatory for ISMS certification. Each organizational unit (or each component of the scope such as location, building, etc.) shall be subject to regular internal audits. In the case of an internal audit, it is essential to ensure that the departments do not audit themselves, but that the audits are always carried out by an independent person.

The so-called "second party audits" are external ISMS audits carried out by parties interested in the organization (e.g. own customers). If the external audits are performed by independent auditing organizations, they are called "Third Party Audits". In the case of an outsourcing contract, appropriate supplier audits may be required.

However, the supplier (or outsourcer) can also demonstrate compliance with the information security requirements by means of a suitable certificate (e.g. ISO 27001 or ISO 27001 based on BSI IT-Grundschutz).

If an ISMS is to be certified, the audit procedure must be carried out by an accredited certification body. Certification bodies for ISO 27001 have an accreditation according to ISO 17021 and ISO 27006. An overview of ISMS certification bodies accredited in Germany can be found on the website of the German Accreditation Body (DAkkS). The Federal Office for Information Security (BSI) is the responsible certification body for basic IT protection.

In the certification audit, the audit team checks the fulfilment of the requirements of ISO 27001 or the BSI IT-Grundschutz from the BSI. The audits must be realized at ISO 27001 under consideration of the standards ISO 27002 and ISO 27005 (and if necessary further branch-specific supplements of the standards of the 27 series). Auditors of certification bodies for ISO 27001 are required to consider the standards ISO 19011 and ISO 27007 within the audit procedure. For audits according to BSI IT-Grundschutz, the respective valid certification scheme of the BSI must be observed.

Certifications according to ISO 27001 or ISO 27001 on the basis of BSI IT-Grundschutz have a validity period of 3 years and are checked at least once a year within the scope of so-called surveillance audits. Should the certificate be renewed after 3 years, the organization must have successfully passed a re-certification audit before the end of the 3-year period.

Depending on the sector, it may be that so-called sector-specific requirements must also be met. It must be checked whether the relevant sector-specific requirements demand proof of a certified ISMS. In addition, further requirements can be defined, which must be implemented and proven according to the specification. An overview of the published sector-specific standards can be found on the BSI website.

In addition, there are other, partly sector-specific norms, standards and guidelines that also cover individual aspects of information security (e.g. VdS10000, ISIS12, IDW980, HIPAA, EuroCloud Star Audit, CSA CCM, ITIL).

Further advantages that speak for ISMS certification are

- Proof of appropriate risk assessment and handling
- Confirmation of the functionality of the ISMS by independent third parties
- Proof of the continuous improvement of the ISMS
- Reduction of liability in case of incidents, because compliance with a harmonised standard in the EU gives a presumption of conformity with the recognised rules of technology (standards) and the state of the art.
- External presentation in the context of corporate marketing/ for the reputation towards others

Context Data protection

The implementation of a data protection management system (DSMS) also lends itself to checking the effectiveness of measures in connection with the requirements of the European basic data protection regulation (DSGVO). Although the DSGVO does not explicitly prescribe such a system, it nevertheless shows the necessity of such a system in many places. For example[29], Art. 32 para. 1 lit. d) DSGVO requires a "procedure for the regular review, assessment and evaluation of the effectiveness of technical and organisational measures to ensure the security of processing".

Since such a procedure requires a planned and structured approach within the organisation, i.e. requires implementation of the classic PDCA model, the establishment of a DSMS is a logical step. If it is aligned

[29] See also Art. 5(2) DPA "The controller (...) must (...) demonstrate compliance" and Art. 24(1) DPA "(...) ensure and provide proof (...) that the processing is carried out in accordance with this Regulation".

with the elements of the ISO high-level structure, it can also be integrated into an existing ISMS based on ISO 27001.

Just like an ISMS, the DSMS can also be audited and thus the degree of maturity of such a system can be determined. Based on the ISO 19011 guidelines, audits can be carried out on the basis of an audit program and an audit plan. An audit can be carried out by the data protection officer. In larger organizations, the audits can also be carried out by expertly trained employees of the organization or by consulting firms specializing in data protection.

Within the scope of the so-called supplier audits, any contract processors of the organization can also be monitored.

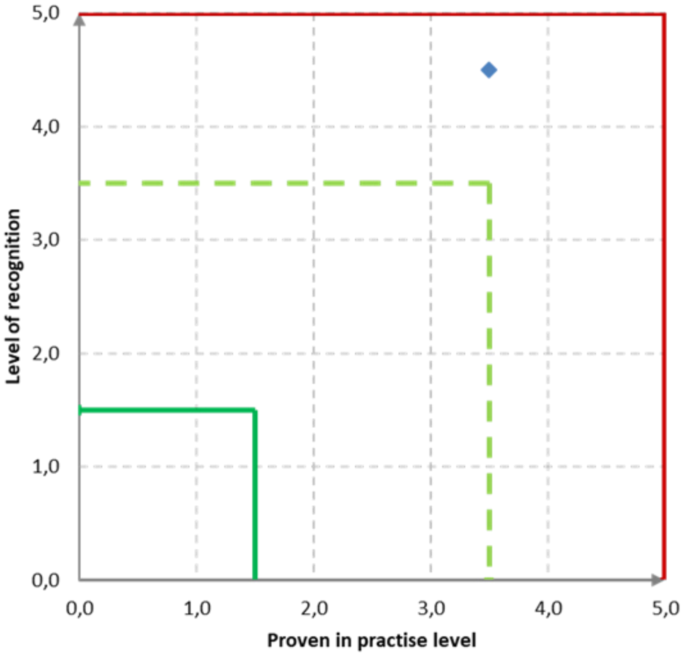
Irrespective of the above, in the data protection context there is also the possibility of certification to obtain proof of compliance with the provisions of the DSGVO (cf. Art. 42 para. 1 DSGVO). Under Article 42(5) DSGVO, however, "data protection-specific certification procedures and data protection seals and test marks" must first be approved by accredited certification bodies under Article 43 DSGVO (in Germany, for example, the DAkks) or the competent supervisory authority. This has not yet been done.

As can be seen from the wording of Recital 100 DSGVO, however, such "data protection-specific certification procedures and data protection seals and test marks" only relate to product, process and service certification (cf. ISO/IEC 17065). In this context, the DSGVO itself mentions, for example

- proof of the fulfilment of the duties of a responsible person (cf. Art. 24 para. 3 DSGVO);
- proof of compliance with the design of the technology and data protection-friendly presettings (cf. Art. 25 para. 3 FADP);
- proof of sufficient guarantees of a processor (cf. Art. 28, paras. 5 and 6);
- proof of the security of the processing (cf. Art. 32 para. 3 DSGVO);
- proof of suitable guarantees in connection with data processing in a third country (cf. Art. 46 para. 2 lit. f) FADP).

A DSMS cannot be certified by means of "data protection-specific certification procedures and data protection seals and test marks" within the meaning of the DSGVO. Nevertheless, these are complementary to a DSMS and can in principle be taken into account as evidence of compliance with the provisions of the DSGVO when auditing a DSMS.

State of technology classification



3.3.5 Vulnerability and patch management

The purpose of vulnerability and patch management is to identify and correct security and functionality weaknesses in software and firmware. Patches are intended to eliminate identified vulnerabilities in order to prevent their exploitation. The vulnerability and patch management process includes assessment, identification, evaluation and deployment for all company products and systems. For the vulnerability and patch management process, responsibilities for implementation and effectiveness testing within the organization must be defined.

3.3.5.1 Assessment

To efficiently manage patches and vulnerabilities, the company's IT landscape must first be inventoried. Since this can change over time, such a survey must be carried out regularly and kept up to date. Components that are not located in the internal network (e.g. smartphones and notebooks of service providers) must be managed using special guidelines. These guidelines are intended to encourage the owners of these components to update the software status on their devices themselves or to connect them regularly to the corporate network for updating.

3.3.5.2 Identification und Evaluation

To identify vulnerabilities, software fixes and threats, relevant information sources (vendor websites, CERTs, CVSS databases, software and hardware vendor mailing lists, third-party newsgroups, etc.) should be monitored, as well as professional enterprise patch management tools should be considered. All those responsible for IT systems, applications, network components, etc. must periodically provide an overview / summary of the current patch status. From this, a report must be created for the evaluation of the current patch situation and used to assess the current risk (e.g. CVSS score). The following solutions are available as treatment options

- Handover to patch management to close identified vulnerabilities with a suitable patch (update).

- Define workarounds (configuration customization, code analysis, etc.) to handle the vulnerability.
- Shut down or isolate the affected system.

If patches are downloaded manually to fix the vulnerability, their authenticity must be verified using standardized methods (cryptographic checksums, signatures, or digital certificates), especially for downloads from the Internet. Paches should primarily be obtained directly from manufacturers' sources. Only in exceptional cases (e.g. with integrated third-party products such as run-time libraries) are patches from other trusted sources permitted.

3.3.5.3 Provisioning

3.3.5.3.1 Preparation

Once the authenticity of the patches has been verified, they should be verified in test systems. If possible, the test systems should be equipped and configured in the same or comparable way as the production system.
Before the final implementation of the patches in the production environment, a backup of the affected systems should be created to enable a reinstallation of the patches in case of an error. If performance is undesirable or functionality is limited, troubleshooting measures should be identified and implemented.

3.3.5.3.2 Implementation
In order for the implementation process to proceed properly, appropriate preparations should be made. This includes, for example, notifying all system administrators and defining the time period for deploying patches. The installation should also be announced to the users so that they can complete their operational processes in good time before the announced installation period.

Normally, patches should be distributed automatically (e.g. with an Enterprise Patch Management Tool). However, administrators may have to install individual patches locally. In this case, communication should be kept secure and files should be exchanged with an authentication check.
As soon as patches are rolled out, the progress must be monitored and communicated in order, for example, to detect failed implementation attempts in good time. Appropriate corrective action must be taken promptly.

3.3.5.4 Treatment of exceptions

3.3.5.4.1 Not patchable systems

For systems or applications, for which

- there are no more updates available from the manufacturer (so-called legacy systems),
- no operating system updates have been released by the manufacturer yet,
- no maintenance window can be made available at short notice for operational reasons (e.g. automation in process technology),
- a recertification of the entire system becomes necessary during an update,

technical measures must be identified and implemented. Since a shutdown or simple reconfiguration is usually not compatible with operational requirements, the following should be taken into consideration

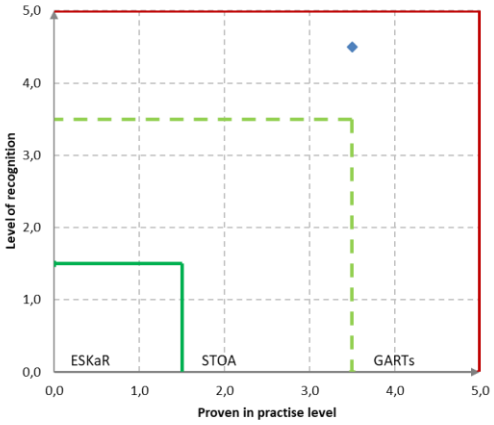
- Separation, zoning, encapsulation or application firewalls as well as
- Network monitoring via Intrusion Detection System

be used to protect against and detect the exploitation of existing vulnerabilities.

3.3.5.4.2 Manufacturer‘s approval

If the approval by the manufacturer is required for the import of patches (e.g. releases for patches of database or operating systems), most available patches cannot be imported because a loss of function would be possible, and no guarantee would be given by the manufacturer. For this reason, periods for the release and provision of patches and updates or alternative workarounds for vulnerabilities must be contractually agreed with the manufacturer.

State of technology classification



3.3.6 Management of information security risks

Risk management is an essential instrument for managing corporate risks and thus the prerequisite for selecting appropriate risk-reducing security measures. In business practice, the use of security measures is decided by weighing up their costs and benefits. To determine the benefits, security risks must be identified and evaluated. A good and structured management of information security risks (short: ISRM) creates the necessary transparency that enables the management level to make appropriate decisions in this context. Furthermore, the management of information security risks[30] is a core element in the implementation and repeated updating of information security management systems (short: ISMS) or data protection management systems (short: DSMS).

Standards

The most important international standard for risk management in general is ISO 31000, while the standard specifically applicable to information security risks is ISO/IEC 27005[31]. The process of the latter is very closely oriented to ISO 31000, but it contains additional (non-normative) information on the identification and evaluation of assets, examples of threats and vulnerabilities, and methods of risk assessment in the context of information security. In Germany, the BSI basic protection is also relevant, especially BSI 200-3 (short: BSI-GS). For industrial automation systems, the standard IEC 62443 Part 3-2 for "Security Risk Assessment and System Design" is also available.

Depending on the regulatory environment, organizations may have to comply with additional specifications, such as the European Data Protection Basic Regulation (DSGVO) or the IT Security Catalogue of the Federal Network Agency (IT-SiKat), both of which contain supplementary specifications for risk management. Sector-specific security standards, the so-calledB3S, have also been defined for individual sectors with regard to the IT Security Act and provide recommendations for the implementation of risk management for KRITIS operators.

[30] In this text, "IT risks" and "IT security" refer to risks and security for all types of information, not just electronically processed data.

[31] The ISO/IEC 27005 standard is currently being revised.

Process

Risk management is a cyclical process (according to PDCA = Plan, Do, Check, Act). As conditions such as the threat situation, system weaknesses or the technological environment change, the risk assessment must be kept up-to-date and its effectiveness monitored. Figure 1 shows the risk process according to ISO 31000.

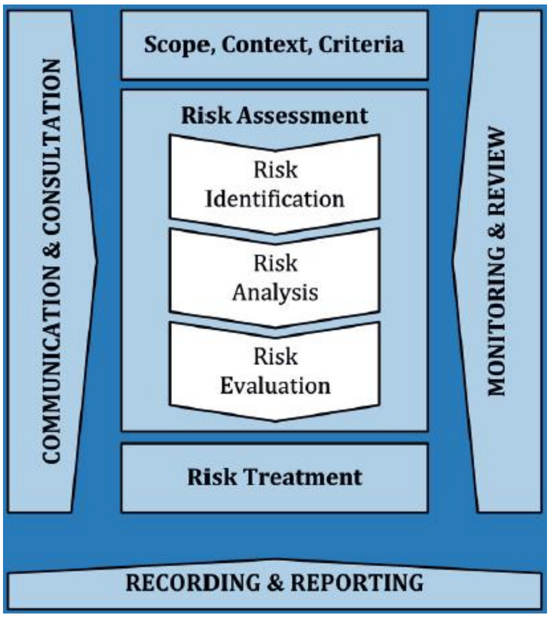


Figure 7: Risk process according to ISO 31000

In the first step (**creating the context**), the basic requirements for ISRM are created. First of all, it is determined to which parts of the organization the ISRM is applicable; if the ISRM is introduced as part of an ISMS, this is generally determined by the scope of the ISMS. The business processes to be included in ISRM must be selected. Based on the business processes, the associated organizational units, IT and OT systems and applications, data and voice communication facilities, service providers and also real estate or buildings are considered. An ISRM organization with corresponding task allocation is created (e.g. under the chairmanship of a risk manager), unless this has already been done within an ISMS or DSMS. It is also advisable to define interfaces between ISRM and central corporate risk management, if available.

Hazards are determined during **risk identification**. Hazards work against values (assets). In an ISRM system, assets are primarily information, and secondarily systems and components for processing and protecting them. During risk identification, the hazards are determined against the assets. According to the BSI [Glossary] definition, threats are the interaction of threats (e.g. natural disasters, pandemics, burglary, hackers, criminals) and weak points (e.g. software errors, organizational deficiencies, technical defects). The challenge is to identify as many of these threats as possible. Standardized hazard catalogues such as those in Annex D of ISO/IEC 27005 or the hazard overview from the BSI Basic Protection Compendium provide support in this. However, these catalogues must be adapted according to the selected context and existing values. In this process, the cooperation of information security managers and technical experts - for example in a working group - is important.

Risk analysis means assessing the hazard in terms of its probability of occurrence and its potential for damage. As mentioned above, it is rarely possible to fall back on solid figures for IT risks. Here, too, the assessments of technical experts - if possible, from several disciplines - are decisive. Losses can be of various kinds (e.g. financial losses, danger to life and limb, impairment of supply or generation/production, damage to reputation, etc.). Since probability figures are subject to a high degree of uncertainty and damage cannot always be clearly quantified, IT risks cannot normally be expressed as a concrete number (cardinal), but rather within an ordinal scale, for example "high", "medium", "low". Annex E in

ISO/IEC 27005 provides helpful guidance on this type of classification. A hazard classified in this way is called a "risk".

Risks must be **assessed** and appropriately **addressed**, for which there are several options. For example, one can consciously bear them (accept them), insure against them or introduce countermeasures (see Chapter 6.4.4 in ISO 31000), but one should not "ignore" them. In this way a conscious decision is made. This decision must be made by a person who takes responsibility, whether for the cost of measures or damage when a risk occurs. This person is usually called the "risk owner"[32]. If the risk is to be reduced, technical experts propose countermeasures, the costs of which and the reduction of the risk form the basis for deciding whether to implement the measures. The "risk owner" then takes the decision on their implementation and the acceptance of the residual risk remaining after the implementation of the measures. Due to legal requirements at CRITIS operators or in the environment of the DSGVO, the "risk owner" is not entirely free to accept or transfer risks without further treatment.

Communication, **reporting** (especially towards management) and **monitoring** are supporting processes. Within an ISMS or DSMS they are established anyway and must be applied to ISRM accordingly. If a central corporate risk management system is in place, efficient communication and mutual complementarity between it and the ISRM is important, and that criteria for the escalation of information security risks to the central corporate risk management system are defined that are understandable and acceptable to both sides.

Practical tips

The complete new implementation of an ISRM is often a comprehensive task for companies (in terms of time and costs). Like other processes, ISRM is subject to a continuous improvement process, which means that you cannot expect to establish a perfect process at the first attempt. On the contrary, a too heavyweight approach can prove to be a burden for the future: There is then the danger that the process will "fall asleep" in the long run or will only be implemented as a formally necessary relic without any recognizable benefit. In this respect, it is advisable to choose a pragmatic approach at the beginning, which pays less attention to completeness than to quality. It is important that high-priority risks are identified, analysed and appropriately dealt with, and that there is the greatest possible consensus on this among the decisive parties.

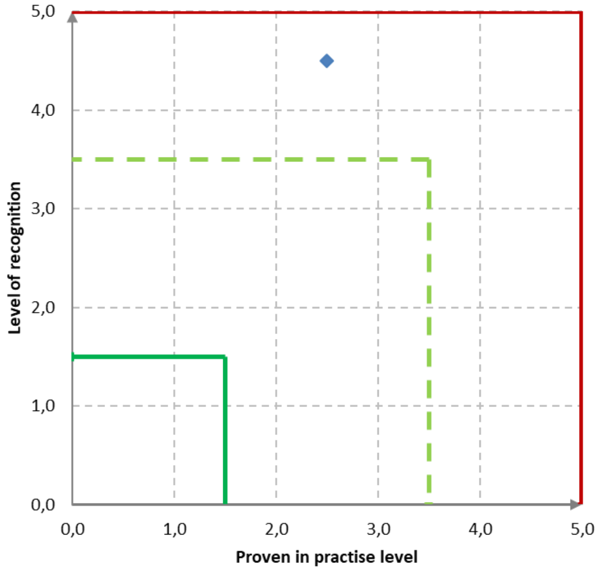
The identification of threats and their appropriate categorisation are particularly challenging at the beginning. Standard threat catalogues such as those in ISO/IEC 27005 can be used for this. Nevertheless, there is seldom a clear answer to the question of whether the threat of "lightning strike" should be classified under "force majeure" and treated as a major overall risk, for example, and whether risks can be treated independently of one another, i.e. whether, for example, "lightning strike" should not be treated together with the risk of "power failure". The interrelationships can become as complex as you like, so that you have to accept certain inaccuracies. Inaccuracies come into play anyway via estimates of the probability of occurrence. Here it is important not to lose sight of the objective, namely that the results of the risk analysis can be used to make a comprehensible decision as to whether or not action is required.

Hardly less difficult is the estimation of probabilities of occurrence. It is advisable to use as many external and internal sources of information as possible. The former include CVE[33] lists, vendor information, CERT services (e.g. from the BSI), and the latter include the evaluation of information security incidents, penetration tests, audits or awareness measures. The values should be adjusted regularly, e.g. at least once a year, to the current situation.

State of technology classification

[32] The term "risk owner" from ISO 27001 is often used as "risk manager" or "risk bearer", depending on the responsibilities of the person concerned.

[33] Common Vulnerabilities and Exposures (CVE) is a standardized list of vulnerabilities and security risks of computer systems.


5,0
4,0
3,0
2,0
1,0
0,0
Level of recognition
0,0
1,0
2,0
3,0
4,0
5,0
Proven in practise level

IT Security Association Germany (TeleTrusT)

The IT Security Association Germany (TeleTrusT) is a widespread competence network for IT security comprising members from industry, administration, consultancy and research as well as national and international partner organizations with similar objectives. With a broad range of members and partner organizations TeleTrusT embodies the largest competence network for IT security in Germany and Europe. TeleTrusT provides interdisciplinary fora for IT security experts and facilitates information exchange between vendors, users, researchers and authorities. TeleTrusT comments on technical, political and legal issues related to IT security and is organizer of events and conferences. TeleTrusT is a non-profit association, whose objective is to promote information security professionalism, raising awareness and best practices in all domains of information security. TeleTrusT is carrier of the "European Bridge CA" (EBCA; PKI network of trust), the IT expert certification schemes "TeleTrusT Information Security Professional" (T.I.S.P.) and "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) and provides the trust seal "IT Security made in Germany". TeleTrusT is a member of the European Telecommunications Standards Institute (ETSI). The association is headquartered in Berlin, Germany.

Contact:

IT Security Association Germany (TeleTrusT)
Dr. Holger Muehlbauer
Managing Director
Chausseestrasse 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.

TeleTrusT
Pioneers in IT security.