Kompetenzzentrum Sicheres Österreich

CYBER TRUST AUSTRIA

Cyber Risk Rating & Cyber Trust Label

Scheme Policy 2023

Version control

Version	Date	Approval
1.0	September 8, 2020	KSÖ Cyber Risk Advisory Board
2.0	September 14, 2021	KSÖ Cyber Risk Advisory Board
3.0	September 13, 2022	KSÖ Cyber Risk Advisory Board

Table of Contents

1 INTRODUCTION 4
2 BASIC PRINCIPLES AND GOALS 4
3 CYBER RISK RATING SCHEME 4
3.1 B Rating 5
3.2 A Rating 5
3.3 A+ Rating 6
3.4 C Score 6
3.5 Cyber Trust Label 7
3.6 Surveillance 7
3.7 Renewal Process 7
3.8 Surveillance-Audits and Withdrawal of Ratings 8
4 GOVERNANCE OF THE CYBER RISK SCHEME 8
5 IMPLEMENTATION OF THE CYBER RISK RATING 9
5.1 Process of requesting a cyber risk rating 9
5.2 Requirements for a Cyber Risk Rating 10
6 SECURITY OF THE PROCESSED DATA 10
7 APPENDIX A: REQUIREMENTS 11
7.1 Requirements for B Rating 11
7.2 Requirements for A Rating (additional to B) 13
7.3 C Score criteria 14
8 APPENDIX B: EXTENSION MODULES 14
8.1 Extension Module “Data Protection” 14
9 APPENDIX C: QUALIFICATIONS 16
9.1 Minimum requirements for auditors 16
9.2 Minimum requirements for validators 16

1 Introduction

The Cyber Risk Rating and the Cyber Trust Label, which is based on it, are a scheme for evaluating the cyber risk status of organizations (companies, associations, etc.). This document describes all relevant aspects of the scheme. It shall provide assurance to the verified organizations as well as to their customers about the degree of security which may be expected from the validated organization.

This document is based on international standards for conformity assessments (ISO/IEC 170xx, especially ISO/IEC 17000 and ISO/IEC 17029) and applies them accordingly.

Goal of conformity assessments is the establishment of trust in the validated organization, product or process. It aims to assure the fulfilment of defined requirements with the object of assessment and to demonstrate it in a suitable way. The value of such a conformity assessment is defined by the level of trust enjoyed by the underlying scheme. This is defined by the requirements themselves, the validation methods as well as the governance mechanisms for control and maintenance of the scheme.

2 Basic principles and goals

The founding values of the Cyber Risk Rating and the Cyber Trust Label are security and trust, as well as openness, transparency and traceability. The rating and the label shall create trust that the validated organization treats cybersecurity in a serious and responsible way. Publishing the scheme and its criteria and evaluation methods it shall assure that this happens in a transparent and traceable way. Consequently this strengthens the validity of the rating and the label and business partners can trust on sound security practices of organizations which carry a cyber trust label respectively enjoy a good cyber risk rating. This makes them a trustworthy business partner with a predictable cyber risk.

Especially the requirements of the B Rating are baseline security requirements. Any organization, even very small ones, should be able to fulfil them to a great extent. A broad availability of organizations with a Cyber Trust Label respectively a good cyber risk B rating therefore also gives an indication of the cyber resilience of a business sector or a country.

Every company that wants to evaluate the trustworthiness and cybersecurity posture of its suppliers can use the Cyber Risk Rating as an effective and efficient method to fulfil its duty of due care. Operators of essential services are obliged by the NIS directive to assure adequate cybersecurity of their providers and suppliers. This scheme gives them an instrument to fulfil this requirement according to state of the art.

3 Cyber Risk Rating Scheme

The Cyber Risk Rating Scheme describes the requirements, which have to be fulfilled in the course of the validation as well as the assurance methods and necessary evidences which are used for the objective evaluation of compliance or non-compliance with the requirements.

The Cyber Risk Rating offers three evaluation schemes which differ with respect to their security claim as well as to the assurance level: the B Rating, the A Rating and the A+ Rating. Based on these ratings the Cyber Risk Label is offered, which can be used to demonstrate a certain level of security towards the market.

3.1 B Rating

The B-Rating defines a **Baseline Security Claim** of an organization. The defined requirements relate to a basic protection level of an organization, a level that should be fulfilled by any organization, irrespective of its size. The requirements are sufficiently generic to be able to be mapped to any organization size, yet specific enough to assure a relevant minimum quality and protection level.

The evaluation method is a **self declaration** of the organization, therefore it is a *first-party conformity assessment*. The organizations rate themselves and indicate to which degree they fulfill the the requirements on basis of the defined criteria (see Appendix A). To assure traceability and plausibility of the self declaration, organizations have to describe for every positively rated question how it is concretely implemented in the organization. They have to be able to proof this with evidences on demand. Additionally the declarations are validated by a qualified validator (requirements see Appendix B) whether the descriptions made in the self declaration are complete, plausible and consistent. Only if the validator approves this the question is positively accepted by the scheme. To assure a neutral evaluation, the self declarations are anonymized for the validator, therefore it is not known which declaration relates to which organization. If a declaration is incomplete or unclear, there is the possibility to ask questions back to the validated organization. The organization then has two weeks to amend and clarity its declaration in order to assure its positive acceptance by the validator. An additional grace period of a maximum of two weeks can be granted once. Should the required answer not be given or the clarification should not be of the required quality, the question is not positively counted. Later clarifications can only be done as a completely new risk rating run. In order to additionally increase the quality and assurance level of the self declaration, the rated organizations oblige themselves to accept to provide evidences to the validating company or a third party auditor in case of a (random) surveillance/control audit. The rated organizations must therefore anytime be ready and able to provide on request evidences for all aspects of its self declaration. On basis of the validated self declaration the B rating is calculated. The rating is stored in the KSV1870 database. If the validated organization has requested and qualified for the label, it is issued accordingly.

In case it turns out that self declarations have been falsified or incorrect declarations have been made on purpose or in a grossly negligent way, the measures described in chapter 3.7 are taken. Any false declaration or obtaining a better rating by fraud are a violation of the rating agreement and can lead to a withdrawal of the rating and revocation of the label usage license.

3.2 A Rating

The A Rating defines an **Advanced Security Claim** of an organization. The defined requirements relate to an advanced protection level of an organization, a level that should be fulfilled by any organization which has an increased security requirement due to its

business model, sector or sensitivity of its operations. The defined requirements relate to an increased level of protection that should be complied with by every organization that has increased security requirements due to its field of activity.

The evaluation method is a **self declaration** of the organization and is conducted analogous to 3.1.

3.3 A+ Rating

The A+ Rating also defines an **Advanced Security Claim** of an organization, like the A Rating defined in chapter 3.2 (based on the same requirements).

However, in contrary to the A rating, the evaluation method for the A+ rating is an **independent Audit** of the organization, a *third-party conformity assessment*. The organization is evaluated by an independent qualified auditor who assesses whether the the requirements defined by the criteria of the scheme have been fulfilled. The check, which must be carried out promptly [1] after the rating, is carried out on the basis of the defined evidence (evidence), which must be presented to the auditor and made plausible. It rests on the the expert validation of the auditor, whether the provided evidences are complete and substantive to fulfill the requirements as defined by the scheme. It is furthermore discretionary to the auditor to request any additional evidences or to make sample tests to assure the validity of the provided controls. (Minimum requirements for auditors see Appendix B). On the basis of the audit results an audit report is produced which documents for each requirement of the scheme, whether it is fulfilled or not. This audit report is provided to the audited organization which can claim corrections within a period of two weeks if necessary. Such claims need to be justified, evtl. with additional evidences. The final decision whether a requirement is accepted as compliant or not lies with the auditor. After the audit has been carried out, the auditor sends information to KSV1870 or Cyber Trust Austria as to whether or not the determined risk rating could be confirmed by the audit. The audit report itself is not sent for security reasons. If the audit reveals deviations from the previously determined Cyber Risk Rating, the auditor must inform KSV1870 or Cyber Trust Austria which questions resulted in a (positive or negative) deviation. Based on this, the rating in the KSV1870 database is adjusted accordingly.

3.4 C Score

The C Score is a fully automated external security check, which analyzes Internet-connected applications of an organization in a non-intrusive way in order to get indications for technical and organizational cybersecurity of that organization. The domains related to the organization and the related IP-ranges have to be declared before start of the rating process and are complemented by technical assignable Internet connected applications. The C Score is used as an indicator for the B- and A-Ratings and is separately documented. If an organization has objections against the C Score, it has to raise them within two weeks.

[1] The period of validity of the rating (and, if applicable, the label based on it) generally refers to the point in time when the rating was created. If more than eight weeks elapse between the rating and the audit, the questionnaire must be answered again, and a processing fee may apply for this.

3.5 Cyber Trust Label

The Cyber Trust Label builds upon the Cyber Risk Rating. There are three different Cyber Trust Labels: the (Standard) Cyber Trust Label, the Cyber Trust Label Silver and the Cyber Trust Label Gold. The right to use the label depends on reaching a certain minimum Cyber Risk Rating:

Label	Logo	Precondition
Cyber Trust Label	CYBER TRUST AUSTRIA	B Rating of 190 or better on the scale from 700 (worst) to 100 (best)
Cyber Trust Label Silber	CYBER TRUST AUSTRIA	A Rating of 190 or better on the scale from 700 (worst) to 100 (best)
Cyber Trust Label Gold	CYBER TRUST AUSTRIA	A+ Rating of 190 or better on the scale from 700 (worst) to 100 (best)

After qualification and payment of the Label fee, the Label may be used on print media and electronic documents as well as on all qualified domains (see **Error! Reference source not found.**) of the qualified organization for information and marketing purposes.

The usage of the Cyber Trust Labels without valid Label usage license and good standing (valid, not withdrawn minimum rating see 3.8) is a breach of license and brand protection rights and will be legally prosecuted.

3.6 Surveillance

The surveillance of the Cyber Risk Ratings is done on a yearly basis. Accordingly, the Cyber Risk Rating has a validity period of one year, afterwards it needs to be renewed. This is true both fort he B and the A/A+ Rating. The Cyber Trust Label, which is based on the Cyber Risk Rating also has to be renewed annually.

3.7 Renewal Process

The Cyber Risk Rating and the Cyber Trust Label based on it are valid for one year. After that, the respective rating must be renewed. Holders of the Cyber Trust Label will be reminded to go through the rating process again 1 month before the expiry date. For the label to be valid throughout with the same key date, the renewed rating (for standard labels: completion of the CRR or for gold labels: completion of the audit) is permitted in a period of up to 4 weeks before and 8 weeks after the validity date. If the rating has not been renewed 8 weeks after

the validity date, it is set to inactive (gray) in the database; if it has not been renewed 6 months after the validity date, it will be deleted from the label database.

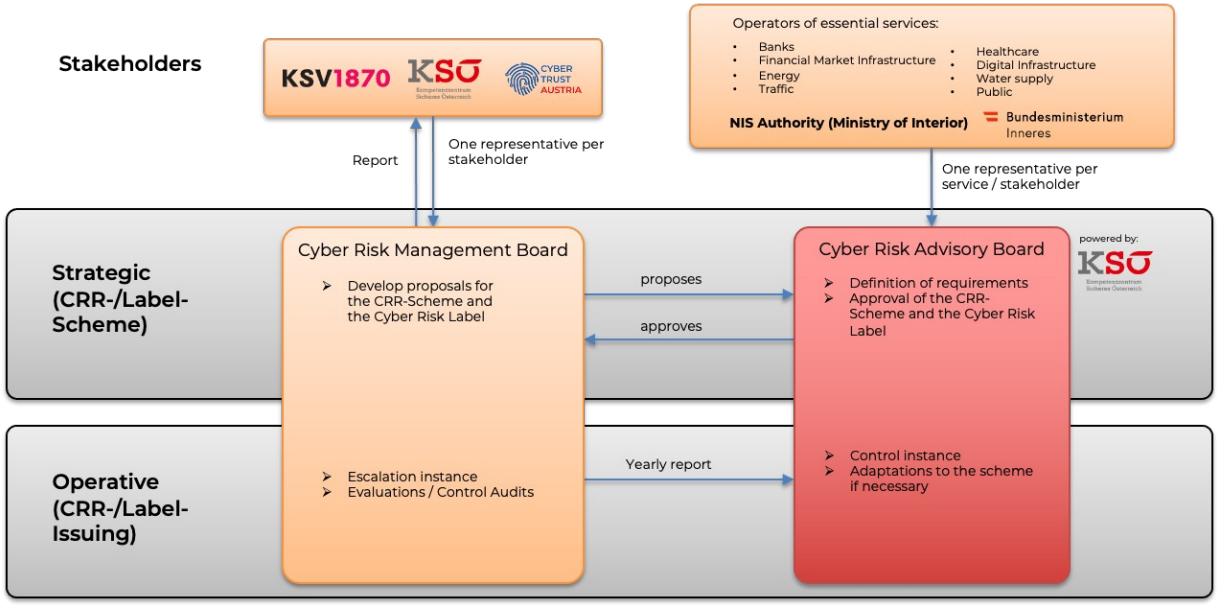
3.8 Surveillance-Audits and Withdrawal of Ratings

The value of a scheme is determined by the trust which is put into it. To achieve a high level of trust, the above mentioned mechanisms are used. However, no validation scheme can provide a 100% accuracy in determining the status quo – just as no security measure can guarantee 100% security. Due to this reason it is necessary to define clear rules how to deal with incidents, exceptions, suspicions and breaches of the rating agreement.

Principally every organizations undergoing a KSV1870 Cyber Risk Rating agrees upfront to an eventual surveillance audit. Such surveillance audits can become necessary e.g. after a severe security incident in an organization or there is suspicious fact about misuse or false information provided by an organization. Besides, surveillance audits can be performed randomized without specific reasoning. The decision for a surveillance audit lies with KSV1870. If all questions have been truly answered in the self declaration, the surveillance audit must lead to the same Cyber Risk Rating. Minor deviations are accepted as margins of discretion. However, if the difference is significant, then purposefully or grossly negligent falsifications have to be assumed. In such cases the rating will be withdrawn and a new rating can be started earliest after a 6 month “cooling off period” (at cost of the organization). In the meantime the rating is displayed as “Withdrawn” in the KSV1870 Rating database. Additionally all KSV1870 customers, who have enquired the rating during the preceding 12 months are actively informed about the new status. If the rating is withdrawn, also the usage right of a related Cyber Trust Label becomes obsolete and has to be removed from all documents and websites of the organization within one month after withdrawal. If there are significant deviations in organization more than once, then for this organization only A+ ratings are accepted from this point in time.

4 Governance of the Cyber Risk Scheme

The owner of the Cyber Risk Scheme is the **Kompetenzzentrum Sicheres Österreich** (KSÖ) as a neutral and impartial association, whose statutes foresee the fostering of cybersecurity in Austria. The KSÖ operates the Cyber Risk Advisory Board, which consists of eight elected representatives of Operators of essential services according to the NIS directive: one representative per NIS sector. These representatives must be qualified experts with responsible leading functions regarding cybersecurity within their companies. These experts provide their knowledge and expertise in defining, maintaining and further developing the Cyber Risk Scheme in order to optimally reflect the security requirements of OeS in the Cyber Risk Rating Scheme. The final approval of the scheme is in the responsibility of the Cyber Risk Advisory Board.
The operational management of the scheme is done by the Cyber Risk Management Board, which consists of three representatives of the involved partners (KSV1870, KSÖ, Cyber Trust Services). The Cyber Risk Management Board acts also as escalation instance.



Graph. 1 Governance Model of the Cyber Risk Rating

5 Implementation of the Cyber Risk Rating

Every organization can make a Cyber Risk Rating. This can be either requested by the organization itself or by other organizations (e.g. as a provider risk management service). Participation in the Cyber Risk Rating is voluntary. If an organization agrees, it accepts the rating agreement with KSV1870 according to this scheme policy.

5.1 Process of requesting a cyber risk rating

If a third party requests a company's cyber risk rating from KSV1870 (for example, as part of its supplier risk management) and this is not yet in the database, the company concerned receives an email from KSV1870 with the request to fill out the relevant questionnaire. The name of the requesting third party can be mentioned. The KSV1870 tries its best to identify the suitable contact person and to explain the purpose and necessity as well as the process to him.

- If the company agrees to the answers to the questions, it receives a link to the KSV1870 portal and the rest of the process is as described in Chapter 3. The company answers all questions to the best of its knowledge and belief and briefly but precisely describes the type of implementation for each positively answered question. After validation, the company is given the opportunity to choose whether also the A rating should also be displayed in the KSV database (for label customers, this results from the requested label).
- If, even after three telephone and electronic contact attempts, no or a negative answer is received by the company, KSV1870 sends a registered letter to the management as a final measure, explaining the situation and requesting that the request be complied with. If there is also no positive response to this letter within two weeks, the company receives a "null rating" in the Cyber Risk database, which is shown accordingly.

5.2 Requirements for a Cyber Risk Rating

The following information must be provided by an organization that undergoes a rating:

- Clear identification of the organization assessed (name, seat of the organization, commercial register number or association number, etc.)
- Contact person in the organization (name, function, telephone, e-mail)
- Specification of all known, associated qualified Internet domains (for C Score)

6 Security of the processed data

Security and risk evaluations of organizations represent sensitive and sensitive data. Correspondingly high security measures are observed by all participating partners of the Cyber Risk Rating to protect this data. The detailed evaluation documents including the information provided by the customer are encrypted and stored on the KSV1870 system for the duration of the evaluation. After the final rating is available, this data is sent encrypted and signed to the rated organization; According to the rating agreement, the rated organization is obliged to keep these documents (as well as the associated evidence) for at least one year beyond the validity period of the rating and to present them if necessary. The detailed evaluation documents will be deleted 2 weeks after the download by the evaluated organization at KSV1870. The rating (as well as the customer's confirmations when submitting the application) is stored in the Cyber Risk Rating database of KSV1870 and the authorization for the label, including the period of use, in the label database of Cyber Trust Services GmbH. No personal data going beyond the contact person in connection with the cyber risk rating or the cyber trust label is stored. Auditors are obliged by means of a code of conduct to also treat all documents received confidentially, to use them exclusively in the context of the audit and to delete them on all their systems after the assessment has been completed.

The complete communication with the rated organization is encrypted (if the client supports this):

- TLS encrypted web sites or
- S/MIME encrypted E-Mails.

7 Appendix A: Requirements

7.1 Requirements for B Rating

Requirements	Criteria
Do you have a current information security policy (resp. IT security policy) that applies to your organization?	The information security guideline must cover the essential requirements for information security (all core topics must be - if applicable - described in this guideline) and should be based on an existing standard (e.g. ISO 27002, NIST 800, BSI IT baseline protection, IT security manual of the WKO, etc.) The guideline must be approved by the management and must be available to employees.
Do you regularly train your employees in information security?	The training must cover the topics of the information security policy and address current cyber threats. The topics must cover at least the following topics: - Secure handling of computers and information - Correct selection and management of passwords - Internet Security - E-mails, Spam and Phishing - Dangerous malware - Response to suspected IT security incidents A complete training must take place at least upon entry and updated information must be communicated at least every two years.
Are there one or more persons in your company who are responsible for information security?	There must be at least one named person who is responsible for the topic of information security, i.e. who creates the guidelines and takes care of the implementation of the measures and is given the necessary time to do so. This person must have the necessary basic technical knowledge on the topics. This activity can be carried out in addition to other activities or can be performed by external persons on behalf of the company.
Do you regularly maintain an inventory of all your IT assets and services as well as related responsibilities?	- There must be a directory of all IT assets used (systems, services). This directory must contain at least the name and version of the system and the person responsible for it. - The directory must be kept complete and up-to-date.
Do you manage system access according to an authorization concept that grants everyone only the rights necessary for their work?	- Access to both applications and file systems must be regulated and correctly set permissions must ensure that only those people who have a need for it based on their job profile can access it (need-to-know). - There is a documented procedure for granting and revoking authorizations.
Do you require your employees to use passwords with a secure minimum strength for all applications?	There must be clearly described minimum criteria for passwords that implement the recommendations of current standards (password strength, no multiple use of passwords, etc.). Reference: BSI, NIST 800, etc.

Do you use the security settings recommended by the manufacturer and ensure that all your IT systems are securely configured?	There must be a document that describes the requirements for the secure configuration of the systems used. References to manufacturer recommendations are sufficient. These settings must actually be implemented on all devices used - as far as technically possible. Alternatively, an acceptance scan is verifiably carried out before commissioning.
Do you check - if applicable - individually developed applications, that are accessible from the Internet, for security gaps before commissioning?	Individual software (e.g. adapted open source software, but not standard software) that can be accessed from the Internet must be checked for vulnerabilities before it is put into operation by means of a penetration test adapted to the individual software.
Do you regularly update all your IT systems and applications with security updates?	- Regular updating of systems with updates provided by the manufacturer. No system update may be more than one quarter overdue (unless there is a documented reason why an update cannot be deployed). - Systems that are no longer provided with security updates by the manufacturer are taken out of service in a timely manner or there are defined exception processes including a deviation list.
Do you secure your network against unauthorized access from outside?	A network segmentation device (e.g. firewall, router, etc.) is in use that restricts network traffic from the Internet to the internal network based on rules that are set as restrictively as possible.
Do you monitor your IT systems for malware?	At least one anti-virus software must be in use that continuously checks the systems and files for malware. The software must be continuously updated and this update must be checked centrally at least once a month. In case of suspicion, an alert is raised in the company.
Do you encrypt sensitive data during transmission over the Internet?	-It must be possible to transfer files in encrypted form, either by e-mail (e.g. S/MIME, PDF encrypted, mandatory/ enforced TLS, etc.) or by encrypted upload. - Forms data on the website is uploaded exclusively via https.
Do they log the use of their IT systems to make security incidents traceable?	-At least the standard protocols of the operating systems must be activated. The protocols must be available to the company. -There is an overview of all active system logs and their location. -The records are kept for at least three months.
Do you have an emergency response plan to handle IT security incidents?	The emergency plan must describe how to respond to a serious IT security incident. Serious security incidents are for example: - Systems failure, - Malware attack (incl. cryptolocker) as well as - data leakage Plans must be tested at least every two years. The test must include at least data and service recovery.

7.2 Requirements for A Rating (additional to B)

Requirements	Criteria
Do you check your IT systems for security vulnerabilities?	- A vulnerability scanning tool must be in use and must be used at least once a month. - The scan must check internal IT systems and those accessible from the internet. - Measures are derived from the vulnerabilities found and implemented.
Do they have mechanisms in place to check the security of software when it is created or purchased?	There is a policy for secure software development, which includes security requirements, secure coding rules and a test concept. For the purchase of software there is a security requirements list and a vendor risk analysis process.
Do you perform penetration tests within your system infrastructure?	- Penetration tests are carried out at least every two years to check the vulnerability of the company. - Measures are derived from the vulnerabilities found and implemented.
Do you monitor your networks for unusual activities or anomalies?	At least one intrusion detection/prevention system must be in place that can identify suspected unauthorised activity on the network using either a baselining approach, heuristic processes or machine learning.
Do you use whitelisting to prevent unauthorized processes and applications from running?	A technology must be active on all clients and servers (e.g. behaviour-based malware detection) so that only approved processes and applications can be executed. Unknown activities are prevented, reported and the reports are followed up.
Do you protect identities, accesses and authorisations in a suitable and comprehensible manner?	- An identity and authorisation management system is in place that makes all identities and their authorisations clearly traceable on a person-by-person basis. - The authorisation management must also include administrative authorisations as well as authorisations for access to customer systems. - Use of multi-factor authentication, especially for externally accessible systems such as VPN, remote support tools, webmail and other web services.
Do you use a Security Information & Event Management system that correlates and analyzes the log files of your systems?	A SIEM is in use to which at least the critical network and security systems are connected and whose log files are continuously correlated and analyzed for irregularities.
Do you have a Security Operations Team?	-The necessary qualified data for monitoring must be available. - Employees with proven qualifications in IT security must be employed in the company to carry out ongoing monitoring as their main task, or there must be an SLA/contract with an appropriate company to take over ongoing monitoring. - Suspected incidents must be investigated and, if confirmed, an alert must be issued and - if relevant - affected customers must be informed.

Can you rely on qualified personnel if you have a serious security incident?	Staff with proven qualifications in in-depth incident response and IT forensics must be employed in the company or there must be an SLA/contract with an appropriate company, or access to one must be covered by cyber insurance.
Do you have a tested resilience concept that ensures your business continuity?	- The resilience concept must include preventive and reactive measures to respond to serious security incidents to ensure business continuity. Serious security incidents include: - Systems failure (incl. power failure, internet connection failure). - Malware attack (incl. cryptolocker) - Data leakage - Targeted hacking attacks (e.g. APTs) - When operating critical applications in the cloud, these measures and tests must be proven by the cloud operator (e.g. via ISAE 3402 reports). - Tests must be carried out at least once a year and necessary improvement measures must be implemented.
Do you have a process for managing your supplier risks?	There must be a documented process to ensure in advance and on an ongoing basis that suppliers also manage their cyber risks appropriately.

7.3 C Score criteria

- Indicators for IT-security incidents
  - Malware distribution
  - Defacements
- Indicators for quality of encryption
  - SSL-Ciphersuite
  - SSL-Validity
  - SSL-Hostname
  - SSL-Trustlevel
- Validation of effective usage of indicators for mitigation of IT security incidents
  - Security-Header Implementation
- Indicators for IT-Reputation
  - Blacklisting of own Domains
  - Blacklisting of foreign Domains, which link to own domains

8 Appendix B: Extension Modules

Extension modules provide an opportunity for the assessed company to provide additional information. These modules do not influence the rating value and are not validated. However, they can lead to the display of further quality indicators or supplement the information of the rating.

8.1 Extension Module “Data Protection”

The extension module "data protection" enables the evaluated company to show that it fulfills the basic requirements for a data processor within the meaning of the GDPR. This information can serve

as the basis of an agreement for order data processing, which subsequently enables the processing of personal data that is passed on by a person responsible. If the rated company fulfills all the requirements of the “data protection” extension module, a corresponding green icon is added to the rating.

The requirements of the "data protection" extension module are:

1. Are you transferring personal data to a country outside the EU / EEA?
   - Can you ensure that in the case of a transfer of personal data to a country outside the EU / EEA, the data protection security standards (e.g. EU standard contractual clauses) are complied with?
2. Do you have an up-to-date privacy policy that applies to your company?
3. Have you implemented all the technical and organizational security measures that are relevant to you in accordance with Art. 32 GDPR for the protection of personal data?
4. Does your company have a deletion concept in accordance with the requirements of Art. 17 GDPR?
5. Are there any regulations for the data protection compliant destruction of data carriers and documents (disposal companies, data bins, shredders, etc.)?
6. Is there a list of processing activities in accordance with Art. 30 GDPR, which is also maintained on a regular basis?
7. Has the need for a data protection impact assessment (risk analysis) in accordance with Art. 35 GDPR in conjunction with Art. 32 GDPR been evaluated for all processing activities?
8. Are there physical security measures to ensure confidentiality (e.g. Kensington locks, etc.)?
9. Are all employees involved in data processing sensitized and trained with regard to data protection about their obligations and expectations?
10. Are there internal guidelines on the confidentiality obligation of employees, freelancers, interns, etc.?
11. Is there a process in accordance with Articles 33 and 34 GDPR for reporting data protection violations, taking into account the requirements of Article 28 GDPR?
12. Do you use contractors to whom you transmit personal data of your customers?
13. If there is order data processing, does your company also use subcontractors who have become obligatory in accordance with the requirements of Art. 28 GDPR?
14. Do you conclude order data processing agreements and EU standard contractual clauses (if necessary) for the agreed services with your (sub) order processors?
15. Is there a process for answering inquiries about the rights of the data subjects (data subject rights) in accordance with the requirements in Art. 12ff GDPR?
16. Do you meet the legal information requirements according to Art. 13 GDPR?

9 Appendix C: Qualifications

9.1 Minimum requirements for auditors

Auditors must be named employees of companies which are accredited as qualified companies by the NIS authority.

9.2 Minimum requirements for validators

Qualified persons conducting validations of self-declarations must have a cybersecurity person certification and at least three years of relevant business experience in the cybersecurity area.