Kompetenzzentrum Sicheres Österreich

CYBER TRUST AUSTRIA

Cyber Risk Rating & Cyber Trust Label

Scheme Policy 2025

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
4.0	September 7, 2023	KSÖ Cyber Risk Advisory Board
4.1	February 23, 2024	KSÖ Cyber Risk Advisory Board (Circular resolution)
5.0	September 5, 2024	KSÖ Cyber Risk Advisory Board
5.1	March 4, 2025	KSÖ Cyber Risk Advisory Board

Table of Contents

1 INTRODUCTION 4
2 BASIC PRINCIPLES AND GOALS 4
3 SCOPE 4
4 CYBER RISK RATING SCHEME 5
4.1 B Rating 5
4.2 A Rating 6
4.3 A+ Rating 6
4.4 WebRisk Indicator 7
4.5 Cyber Trust Label 7
4.5.1 Cyber Trust Platinum Label 8
4.6 Surveillance 8
4.7 Renewal Process 8
4.8 Transfer of Cyber Risk Ratings 9
4.9 Surveillance-Audits and Withdrawal of Ratings 9
5 GOVERNANCE OF THE CYBER RISK SCHEME 10
6 IMPLEMENTATION OF THE CYBER RISK RATING 11
6.1 Process of requesting a cyber risk rating 11
6.2 Requirements for a Cyber Risk Rating 11
7 SECURITY OF THE PROCESSED DATA 11
8 APPENDIX A: REQUIREMENTS 13
8.1 Requirements for B Rating 13
8.2 Requirements for A Rating (additional to B) 15
8.3 WebRisk Indicator 16
8.4 Requirements for a Platinum Label 17
9 APPENDIX B: EXTENSION MODULES 19
9.1 Extension Module “Data Protection” 19
10 APPENDIX C: QUALIFICATIONS 19
10.1 Minimum requirements for auditors 19
10.2 Minimum requirements for validators 20

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 Scope

The Cyber Risk Rating always refers to a specific company, defined by a commercial register number (or equivalent). The answer to the questions relates to the sphere of influence of the company itself, i.e. the systems, processes and personnel under the company's own control. Companies that operate IT for customers have a corresponding duty of care, but only to the extent that the company can independently decide on protective measures for customer systems.

4 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 four evaluation schemes which differ with respect to their security claim as well as to the assurance level: the B Rating, the A Rating, the A+ Rating as well as the Platinum Label Scheme which is based on the Implementing Regulation (EU) 2024/2690. Based on these ratings the Cyber Trust Label is offered, which can be used to demonstrate a defined level of security towards the market.

4.1 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. Deviations from the questions may be possible to a certain extent if they are compensated for by appropriate and acceptable measures that address the risk in a comparable way in accordance with the security objective. It is up to the validators or auditors to assess the appropriateness and comparability. 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 4.9 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.

4.2 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 4.1.

4.3 A+ Rating

The A+ Rating also defines an **Advanced Security Claim** of an organization, like the A Rating defined in chapter 4.2 (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 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 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.

[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.

4.4 WebRisk Indicator

The WebRisk Indicator 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 WebRisk Indicator is used as an indicator for the B- and A-Ratings and is separately documented. If an organization has objections against the WebRisk Indicator, it has to raise them within two weeks.

4.5 Cyber Trust Label

The Cyber Trust Label builds upon the Cyber Risk Rating resp. the Implementing Regulation (EU) 2024/2690. There are four different Cyber Trust Labels: the (Standard) Cyber Trust Standard Label, the Cyber Trust Silver Label, the Cyber Trust Gold Label and the Cyber Trust Platinum Label. The right to use the label depends on reaching a certain minimum Cyber Risk Rating:

Label	Logo	Precondition
Cyber Trust Standard Label	CYBER TRUST AUSTRIA	B Rating of 190 or better on the scale from 700 (worst) to 100 (best)
Cyber Trust Silver Label	CYBER TRUST AUSTRIA	A Rating of 190 or better on the scale from 700 (worst) to 100 (best)
Cyber Trust Gold Label	CYBER TRUST AUSTRIA	A+ Rating[2] of 190 or better on the scale from 700 (worst) to 100 (best)
Cyber Trust Platinum Label	CYBER TRUST AUSTRIA	Achievement of >= 85% in the validated self-declaration according to the Implementing Regulation (EU) 2024/2690

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 of the qualified organization for information and marketing purposes.

[2] Only in the first year and then every third year, in between A rating of 190 or better (see 4.7 Renewal process)

The usage of the Cyber Trust Labels without valid Label usage license and good standing (valid, not withdrawn minimum rating see 4.9) is a breach of license and brand protection rights and will be legally prosecuted.

4.5.1 Cyber Trust Platinum Label

In contrast to the other labels, the Cyber Trust Platinum Label is based directly on the Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024. This Implementing Regulation comprises a total of 50 requirements, which, analogous to the procedure for Cyber Risk Ratings, are checked and qualified by validators as part of a validated self-declaration. For each question, there is only 'fulfilled' or 'not fulfilled', whereby the decision as to whether the information provided is sufficient to adequately fulfil the required requirements lies with the validator. If there are rejections, these are justified and recommendations are provided. If necessary, the validator can, at his own discretion, demand artefacts (evidence) from the customer being evaluated if he considers this to be necessary for a sufficient plausibility check of the questions.

If the sum of the questions assessed as fulfilled exceeds 85% (this is analogous to a CRR <= 190), the qualification for a Platinum Label is considered fulfilled and one is issued. The period of validity is also one year, after which the assessment must be renewed, with a delta analysis based on the result of the previous year.

4.6 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.

4.7 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.

If the rating is renewed, this can be carried out as a *delta analysis*. Based on the information provided in the previous year, the audited company can limit itself to describing any changes compared to the information provided in the previous year. In the event of changes to the questions in the schema or adjustments to the definitions of the requirement criteria, the new/changed requirements must be addressed in the answer. If nothing has changed in the company or in a question, the answer from the previous year can simply be re-used, but must be confirmed again.

When renewing a Gold Label, a new external audit is only necessary after three years. However, the questions must be answered again every year - in the sense of the delta analysis described above. The cycle at Gold Labels is therefore:

- Year 1 (first issuance of the Gold Label): A rating plus external audit (= A+)
- Year 2: A rating
- Year 3: A rating
- Year 4: A rating plus external audit (= A+)
- Year 5: A rating
- Year 6: A rating
- Year 7: A rating plus external audit (= A+)
- etc.

4.8 Transfer of Cyber Risk Ratings

Principally, a cyber risk rating always refers to a defined company with a defined commercial register number. However, in exceptional cases it is possible to transfer ratings within a group of companies, under the following conditions:

- The security regulations and processes are the same for all companies mentioned
  - This must be expressly recorded in the scope of the internal security policy
- The security systems and the people involved must also be the same

This must be confirmed by the company in writing and with a company drawing.

4.9 Surveillance-Audits and Withdrawal of Ratings

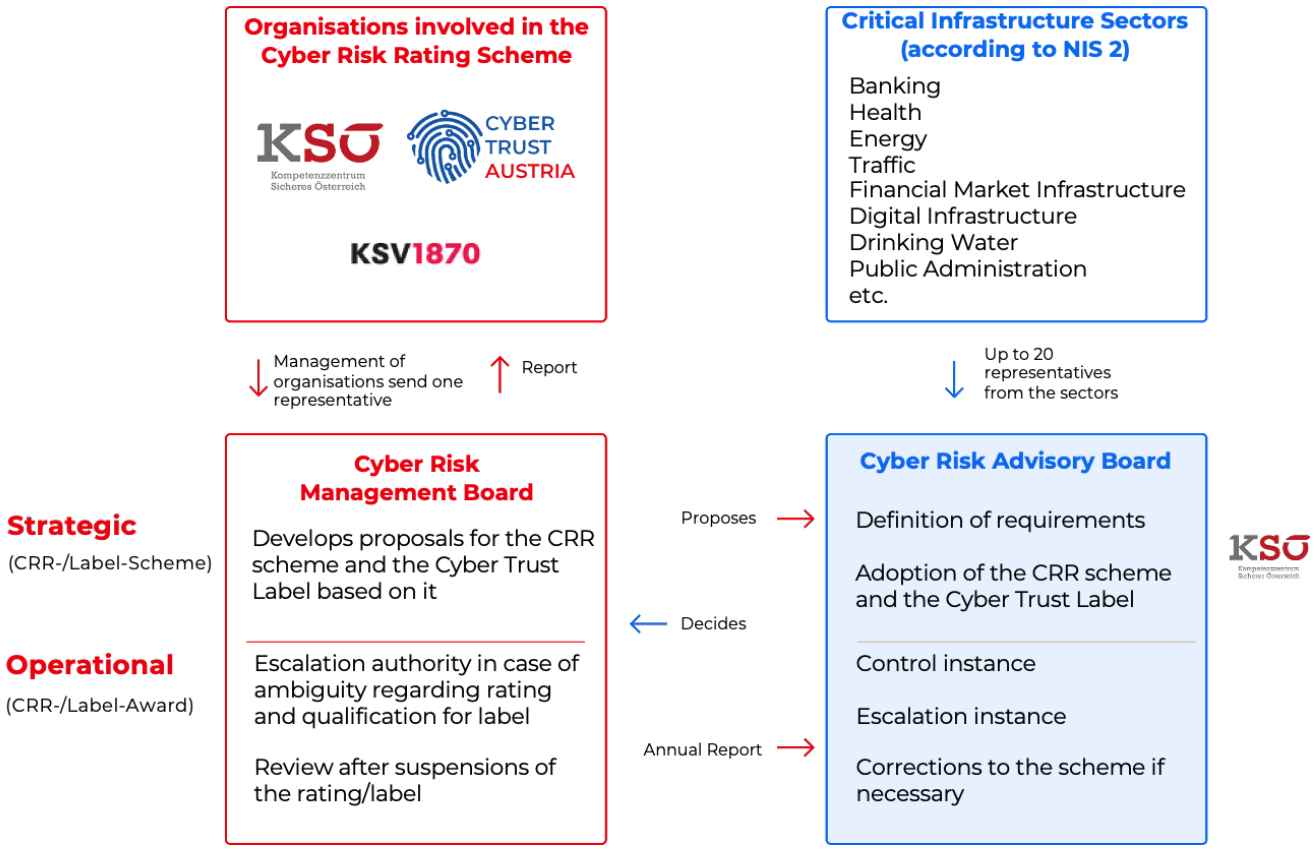
The value of a scheme is determined by the trust which is put into it. To achieve a high level of trust, the above mentioned mechanisms are used. However, no validation scheme can provide a 100% accuracy in determining the status quo – just as no security measure can guarantee 100% security. Due to this 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. Surveillance audits relate only to the submission of evidence relating to the questions from the scheme, so it does not encompass a *general* right to 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 (in a negative sense), 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 negative deviations in organization more than once, then for this organization only A+ ratings are accepted from this point in time.

5 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 according to its own rules of procedure, which is composed of representatives from the NIS sectors. 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 first escalation instance. The Cyber Risk Advisory Board is the second and final escalation instance.



Graph. 1 Governance Model of the Cyber Risk Rating

6 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.

6.1 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.

6.2 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 WebRisk Indicator)

7 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.

8 Appendix A: Requirements

8.1 Requirements for B Rating

Requirements	Criteria
Do you have a current information security policy (or IT security policy) that applies to your company?	The information security policy must cover the essential requirements for information security (all core topics - if applicable - must be described in this policy) and should be based on an existing set of rules (e.g. ISO 27001/27002, NIST 800, IT Grundschutz, IT security manual). WKO etc.). The policy must be approved by management and available to all employees. At least every two years, a review of the actuality, suitability and effectiveness of the security measures must take place and, if necessary, the policy must be adjusted.
Do you regularly train your employees in information security?	The training must cover the content of the information security policy and address current threats. The content must include at least the following topics: -Proficient use of computers and information -Select and manage passwords correctly -Safe on the Internet (e.g. use of company data in AI services and social networks) -Emails, spam, and phishing -Dangerous malware -Behavior and procedure if an IT security incident is suspected Full training must take place at least upon entry and updated information must be communicated at least every two years.
Is there one or more designated people 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 policy and takes care of the implementation of the measures and is given the necessary time for this. This person must have the necessary basic technical knowledge of the topics and keep themselves informed about cyber risks. This activity can be carried out in addition to other activities or can also be carried out by external parties on behalf of the company.
Do you regularly maintain a record of all your IT assets and services (including cloud services) and associated responsibilities?	- There must be a directory of all IT assets used (systems, services - cloud and on-premise). This directory must at least contain 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 access to your systems according to an authorization concept that only grants everyone the rights necessary for their work?	- Both access to the applications and to the file systems must be regulated and correctly set authorizations must be used to ensure that only those people who have a need for it based on their job profile (need-to-know) can access it.

	- There is a documented procedure for granting and revoking permissions.
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 do you 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, a vulnerability scan is verifiably carried out before commissioning.
Do you check - if available - individually developed applications accessible from the Internet for security gaps before going live (or don't you use such software at all)?	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 being put into operation using a penetration test (resp. code review) adapted to the individual software.
Do you regularly update all IT systems and applications with security updates?	- Regularly updating systems with updates provided by the manufacturer. No security 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 decommissioned in a timely manner or there are defined exception processes including a list of deviations and compensating measures.
Do you protect your network from unauthorized access from outside?	A network segmentation device (e.g. firewall, router, etc.) is in use, which limits network traffic from the Internet to the internal network based on rules that are as restrictive as possible.
Do you monitor your IT systems for malware?	At least antivirus software must be in use, which continuously checks the systems and files for malware. The software must be continually updated and this update must be checked centrally at least once a month. There is a well-known process for handling security incidents.
Do you encrypt sensitive data when transmitted over the Internet?	- It must be possible to transfer files in encrypted form, either via email (e.g. S/MIME, PDF encrypted, mandatory enforced TLS, etc.) or via encrypted upload. - Form data on the website is only uploaded via https.
Do you log the use of your IT systems to make security incidents traceable?	- At least the standard protocols of the operating systems which are security relevant must be activated. The logs must be available to the company. - There is an overview of all active system logs and their storage location. - Server logs are kept for at least 90 days, and client logs for at least 60 days.

Do you have an emergency plan in place to respond to an IT security incident?	The emergency plan (incl. backup concept) must describe how to respond to a serious IT security incident. Serious security incidents include: - system failure, - Malware infection (including cryptolocker) as well - Data leakage Plans must be tested at least every two years. The test must include at least data and service recovery.

8.2 Requirements for A Rating (additional to B)

Requirements	**Criteria**
Do you check IT systems in your network for security gaps?	- A vulnerability scanning tool must be in use and must be used at least once per month. - The scan must check the entire IP range of the internal IT networks as well as IT systems accessible from the Internet. Unauthorized devices must also be identified. - Measures are derived and implemented from the security gaps found.
Do you have mechanisms in place that check the security when creating or purchasing individually developed software?	There is a policy for secure software development, which includes security requirements, secure coding rules and a testing concept. The policy for secure software development must also address the issue of Software Bill of Materials (SBOM); it must be clear which components are used in self developed software. When purchasing software, there is a security requirements list and a risk analysis process from the provider/manufacturer.
Do you carry out penetration tests in your system landscape?	- Penetration tests are carried out at least every two years to check the vulnerability of the company. - Measures are derived and implemented from the vulnerabilities found.
Do you monitor your system landscape for unusual activities and anomalies?	At least one technology must be in use that is able to detect and centrally report intrusions or anomalies in the system landscape (network, endpoint, clients, server, cloud).
Do you have whitelisting and Cloud Access Security Brokers (CASB) in place to prevent unauthorized processes and applications from running?	A technology must be active on all clients and servers so that only allowed processes and applications can run. A CASB is used for cloud services to only be able to run approved cloud applications. Unknown activities are prevented, reported and the reports are investigated.
Do you protect identities, access and authorizations in an appropriate and traceable manner?	- Identity and authorization management is in use, which makes all identities and their authorizations clearly traceable on a person-by-person basis. - Authorization management must also include administrative authorizations and authorizations for access to customer systems. - Use of multi-factor authentication, especially for externally accessible systems such as: VPN, Jump hosts, Remote Support Tools, Webmail and other web services.

Do you use technology that automatically correlates and analyzes the log files of your systems?	A technology (e.g. 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 or use a security operations team?	- The company must have employees with proven qualifications in the area of IT security who perform ongoing monitoring as their main task, or there must be an SLA/contract with a corresponding company that takes over ongoing monitoring. - Suspected cases must be investigated and, in the case of confirmed incidents, an alarm must be raised and, if relevant, affected customers must be informed. - The necessary qualified data for monitoring must be available.
Can you access qualified resources in the event of a serious security incident?	Employees with proven qualifications in the areas of in-depth incident response and IT forensics must be employed in the company or there must be an SLA/contract with a corresponding company, or access to one must be covered by cyber insurance.
Do you ensure their operational continuity through a tested resilience concept or a resilient architecture?	- The resilience concept must include preventive and reactive measures in order to be able to respond to serious security incidents and thus ensure operational continuity. Serious security incidents include: - Failure of the systems (including power failure, failure of the internet connection) - Malware infection (including 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 their supplier risks?	There must be a documented process that ensures in advance and on an ongoing basis that suppliers also manage their cyber risks appropriately.

8.3 WebRisk Indicator

- 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

8.4 Requirements for a Platinum Label

No.	Requirement
1.1	Please describe your **rules and regulations** (e.g. information security guidelines, policies, etc.) and the extent to which they address the security objectives of your network and information systems, including implementation measures, are known to all employees and have been formally approved by top management.
1.2	Please describe your **roles and responsibilities** for information security and whether a person is directly responsible to the top management with regards to network and information systems security.
2.1	Please describe your **information security risk management system** and the extent to which it is integrated into the overall risk management of the organisation and identifies, assesses and appropriately addresses all information security risks relevant to the organisation.
2.2	Please describe whether and how you regularly review **compliance with your** information security **concepts, policies and guidelines** and whether you report the results to your top management.
2.3	Please describe whether and how you regularly arrange for **independent reviews** of your approach to managing the security of network and information systems and its implementation, and report the results to your top management.
3.1	Please describe your concept or **process for recognising, analysing and managing security incidents**, the associated responsibilities, and how you test and update this at regular intervals.
3.2	Please describe what **logging measures** are in place in your systems, what events they cover and whether and how you monitor them on an ongoing basis? Please also provide information on the retention period of the logs.
3.3	Please describe the mechanism by which suspicious events can be **reported** to you and to what extent providers and customers are informed about this reporting mechanism.
3.4	Please describe your mechanism for **evaluating and classifying events**.
3.5	Please describe how you respond to **security incidents** in a timely manner, document your response and follow your own security incident procedures as described in 3.1.
3.6	Please describe whether and how you conduct a **review** after security incidents, analysing the causes of the incident and the appropriateness of your response and, if necessary, deriving improvements for the future.
4.1	Please describe your business continuity and **disaster recovery plan** and how it is based on a scenario analysis and a business impact analysis (BIA) and is regularly tested and updated.
4.2	Please describe your **backup and redundancy concept** that enables you to achieve the recovery times required according to the risk analysis and how you test its effectiveness.
4.3	Please describe your **crisis management**, including appropriate roles and responsibilities and means of communication, and the extent to which this is regularly tested and updated.
5.1	Please describe your **supply chain security policy** or **process** and the extent to which it checks the quality and resilience of ICT products and services in the area of cyber security at your direct suppliers on the basis of a risk assessment and also contractually requires this.
5.2	Please describe your **register of providers and service providers** and to what extent this includes all ICT products, services and processes.
6.1	Please describe your procedure for ensuring appropriate **security measures when purchasing ICT services or ICT products**, including defined security requirements.
6.2	Please describe your requirements and associated **process for secure software development**, and how this covers all phases of development, including specification, design, development, implementation and testing.

6.3	Please describe your **configuration management** and the extent to which it defines, documents, implements and monitors security configurations of hardware, software, services and networks.
6.4	Please describe your **change management** and the extent to which it checks planned and unplanned changes (emergency changes) to the network and information systems for risks before they are implemented.
6.5	Please describe your **specifications and procedures for security testing**, to what extent this is based on a risk assessment (in accordance with 2.1) and, if applicable, risk minimisation measures are applied.
6.6	Please describe your **security patch management** and the extent to which it ensures the application of security patches within a reasonable period of time.
6.7	Please describe your **network security measures** and the extent to which they limit communication within your network and access from outside to the necessary minimum and also ensure integrity and confidentiality at network level.
6.8	Please describe how you have implemented **network segmentation** and the extent to which this appropriately separates systems with different security requirements.
6.9 a	Please describe how you use software to **detect and prevent malware**.
6.9 b	Please describe how you use software to **detect and prevent unauthorised software.**
6.10	Please describe your procedures for **detecting, assessing and addressing vulnerabilities**.
7.1	Please describe your procedures for **assessing the effectiveness of risk management measures** in the area of cyber security.
8.1	Please describe your **awareness-raising measures** and how they ensure that your employees, including members of top management, are aware of cybersecurity risks and apply basic cyber hygiene procedures.
8.2	Please describe whether and to what extent you provide **role-specific security training** that covers all security-related skills and expertise required for the respective role.
9.1	Please describe your concepts and procedures in relation to **cryptography** and how these define the type, strength and quality of cryptographic measures and key management.
10.1	Please describe how you ensure that your employees and, where applicable, your direct suppliers and service providers understand and fulfil their **responsibilities** according to their roles in the area of security.
10.2	Please describe if and how you conduct **background checks** on your employees if this is necessary for their role.
10.3	Please describe your **contractual arrangements** with your employees regarding security and confidentiality and whether these remain valid after termination of employment or contract.
10.4	Please describe if and what **procedures** you have in place for dealing with breaches of network and information system security concepts.
11.1	Please describe your concept for the **logical and physical control of access** to your network and information systems for all persons and how it provides for appropriate authentication.
11.2	Please describe whether and to what extent you have a documented and logged **management of access rights**, which only grants and withdraws rights according to "need-to-know" and "need-to-use".
11.3	Please describe your concept for the **management of privileged accounts** and system administration accounts, which defines and restricts system administration rights as far as possible on an individual basis and provides for strong authentication procedures (e.g. multi-factor authentication).
11.4	Please describe whether you use **system administration systems** exclusively for the purposes of system administration and how you protect access to them through authentication and encryption.

11.5	Please describe whether and to what extent you manage **identities** throughout their lifecycle and ensure that each identifier is always linked to a unique user or, in the case of (absolutely necessary) shared identifiers, that authorisation and traceability of use is guaranteed.
11.6	Please describe which secure **authentication methods** you use and to what extent these authentication methods are appropriate to the criticality of the accessed assets.
11.7	Please describe whether and to what extent you use **multi-factor authentication**, if appropriate to the criticality of the assets accessed.
12.1	Please describe how you perform an ongoing **asset classification** that specifies the protection required for all assets based on confidentiality, integrity, authenticity and availability requirements according to their criticality and risk.
12.2	Please describe your approach to the proper treatment of assets (including information) throughout their **lifecycle** (including acquisition, use, storage, transport and disposal), based on the classification of assets.
12.3	Please describe your concept for the **management of removable media** with regard to security.
12.4	Please describe how you maintain a complete, accurate, up-to-date and coherent **inventory of your assets.**
12.5	Please describe how you ensure the handover, **return or deletion of assets** upon termination of employment in a documented manner.
13.1	Please describe your concept and **measures to prevent interruptions to your operations** due to the failure or disruption of supporting utility services such as electricity and telecommunications and the extent to which you regularly test them.
13.2	Please describe your **concept for protection against physical and environmental threats** and the extent to which you regularly test it.
13.3	Please describe whether and to what extent you protect your **perimeter** and take suitable measures to prevent unauthorised physical access to, damage to and interference with your network and information systems and to what extent you regularly test these protective measures.

9 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.

9.1 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.

10 Appendix C: Qualifications

10.1 Minimum requirements for auditors

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

10.2 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.