THE CYBERRISK RATING by KSV1870

KSV1870

Requirements
CyberRisk Rating

basend on the cyber risk scheme of the KURATORIUM SICHERES ÖSTERREICH

Version 2.0

September 14, 2021

B-Rating requirements

B1 Do you have a current information security policy (or IT security policy) that applies to your organization??

The information security guideline must cover the essential requirements for information security and data protection (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.

EVIDENCE

- Document must be available and the last review must not be more than two years old.

B2 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 (e.g. ransomware)
- 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.

EVIDENCE

- Training documents as well as proof of enrollment at entry

B3 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.

EVIDENCE

- Proof of qualification of the named person (self-study is acceptable if this can be credibly demonstrated)

B4 Do you regularly maintain an inventory of all your IT assets and services and related responsibilities?

There must be a directory of all IT assets (systems, services) used. This directory must contain at least the name and version of the system and the person responsible for it.

EVIDENCE

- Repository of systems

B5 Do you manage system access according to an authorization concept that grants everyone only the rights necessary for his work?

Access to both applications and file systems must be regulated. Correctly set permissions must ensure that only those persons who have a need to do based on their job profile can access it. There must be a process for granting and removal of access rights.

EVIDENCE

- Authorization concept or authorization lists

B6 **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, which implement the recommendations of current standards (password strength, two-factor authentication where necessary and appropriate, separation of passwords, etc.) Reference: BSI, NIST 800, etc.

EVIDENCE

- Password policy (can be part of the security policy)
- Set your own password when accessing the assessment

B7 **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 safe configuration of the systems used. References to manufacturer recommendations are sufficient. These settings must also be actually implemented on all devices used - as far as technically possible. Alternatively there is a mandatory vulnerability scan before setting the device productive.

EVIDENCE

- Description of requirements (or written reference to manufacturer's recommendations)
- Sample verification on systems

B8 **Do you check - if applicable - individually developed applications, that are accessible from the Internet, for security gaps before commissioning?**

Individual software (e.g. customised open source software, but not standard software) that can be accessed from the Internet must be checked for vulnerabilities by means of a penetration test at least before it goes live.

EVIDENCE

- Penetration test report

B9 Do you regularly update all your IT systems and applications with security updates?

Regularly update the systems with updates provided by the manufacturer. No system update must be more than one quarter overdue (unless there is a documented reason why an update cannot be applied). Systems that are no longer supplied with security updates by the manufacturer will be taken out of service on time respectively there is a defined exception process and a documented exception list.

EVIDENCE

- Version reports of the operating systems and most important software products used

---

B10 Do you secure your network against unauthorized access from outside?

A network segmentation device (e.g. firewall, router, etc.) is used, which filters the network traffic with the Internet on the basis of rules set as restrictive as possible.

EVIDENCE

- Version reports of the systems used
- Rules of the network segmentation device

B11 Do you monitor your IT systems for malware?

At least an up-to-date anti-virus software must be in use, which continuously checks the systems and files for malware. In case of suspicion, an alert is created in the organisation.

EVIDENCE

- Version reports of the antivirus software used
- License for all used devices (according to system index)

B12 Do you encrypt sensitive data during transmission over the Internet?

There should be the possibility to transfer files encrypted, either by eMail (e.g. S/MIME, PDF encrypted, mandatory enforced TLS, etc.) or by encrypted upload. Forms on the website are uploaded exclusively via https.

EVIDENCE

- Proof of the encryption mechanisms used

B13 **Do you log the usage of your 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.

EVIDENCE

- Overview of the system logs

B14 **Do you have an emergency response plan to handle IT security incidents?**

The emergency plan including backup concept must describe how to react to a serious IT security incident. Serious security incidents are for example:

- Outage of the systems,
- Malware infections (incl. cryptolocker) and
- Data leakage

The plans must be tested at least every two years.

EVIDENCE

- Documented emergency plan. The last update must not be more than two years old.
- Proof of testing

A-Rating requirements (in addition to B)

A1 **Do you check your software for security vulnerabilities?**

A vulnerability scanning tool must be in place and must be used at least once a month.

EVIDENCE

- Monthly scan reports

A2 Do you have measures in place to verify 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.

EVIDENCE

- Policy for secure software development
- Security requirements list for software licensing

A3 Do you perform penetration tests within your system infrastructure?

At least every two years, penetration tests are performed to check vulnerabilities of the organisation. Based on the identified weaknesses there are measures identified and implemented.

EVIDENCE

- Test plan
- Test reports

A4 Do you monitor your networks for unusual activities or anomalies?

At least an intrusion detection / prevention system must be in use, which can identify suspected unauthorized activities in the network either via a baselining approach or via heuristic processes or machine learning.

EVIDENCE

- Version reports of the systems used
- Network chart
- Network logs (going back at least 1 month)

A5 Do you use whitelisting to prevent unauthorized processes and applications from running?

A mechanism must be active on all systems (clients/servers) that allows only approved processes and applications to run.

EVIDENCE

- Documentation of the whitelisting process

A6 Do you manage the identities and authorizations of all users in a traceable way?

An identity and access management system is in use, which makes all identities and their authorizations clearly traceable on a individual user basis. Authorization management must also include administrative authorizations and authorizations for access to customer systems.

EVIDENCE

- Description of the used processes (and systems if applicable)
- Authorization lists for normal and privileged users

A7 Do you use a Security Event & Information 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.

EVIDENCE

- Version reports of the used systems
- Documentation of the connected systems
- SIEM reports

A8 Do you have or do you use a Security Operations Team?

Employees with proven qualifications in the area of IT security must be employed by the company, or there must be an SLA with a corresponding company that will take over ongoing monitoring. Suspicious cases must be investigated and in case of confirmed incidents an alert must be issued and - if relevant - affected customers must be informed.

EVIDENCE

- Documentation of the monitoring and incident handling processes OR
- SLA with external SOC and proof of reports

A9 Can you rely on qualified personnel if you have a serious security incident?

Employees with proven qualifications in the areas sophisticated incident response and IT forensics must be employed by the company or there must be an SLA with a corresponding company, or access to such a company must be covered by cyber insurance.

EVIDENCE

- Proof of the technical qualification of the named person(s) with regards to forensics OR
- SLA with service provider and proof of qualification of the service provider OR
- Cyber insurance policy covering forensics

A10 Do you have a tested resilience concept that ensures your business continuity?

The resilience concept must include preventive and reactive measures to be able to react to serious security incidents and thus ensure business continuity. Serious security incidents include:

- System outage,
- Malware infection (incl. cryptolocker) and
- Data leakage
- Targeted hacking attacks (e.g. APTs)

When running critical services in the cloud, these measures and tests must be verified by the cloud operator (e.g. via ISAE 3402 reports). Tests must be performed at least once a year and necessary improvement measures must be implemented.

EVIDENCE

- Resilience concept
- Test concept
- Test report

A11 Do you have a process for managing your supplier risks?

There must be a documented process which assures from the initial selection phase and continuously, that critical suppliers manage their information security and business continuity management risks adequately.

EVIDENCE

- Process description, checklists
- Standard contracts with suppliers include security requirements and a Right to Audit

---

Questions about the CyberRisk Rating?
This is how you can reach us:

By email
crr@nimbusec.com

POWERED BY
nimbusec
Part of **KSV1870**

NIMBUSEC GMBH, A COMPANY OF THE **KSV1870** GROUP

Nimbusec GmbH | Fadingerstraße 15 | 4020 Linz
FN 394170m | FBG Linz | UID ATU67830957
Behörde gem. ECG: Magistrat der Stadt Linz/Donau