

SOCIAL

Sovereign Citizen Alliance – SOCIAL

Information Security Assessment for SME and SMO – CISA50plus

Output document of the Erasmus+ project
“SOCIAL – Sovereign Citizen Alliance”



Co-funded by
the European Union



This document was produced as part of the Erasmus+ project:

"Sovereign Citizen Alliance – SOCIAL"

Project Partners:



Betriebswirtschaftliches Forschungszentrum für
Fragen der mittelständischen Wirtschaft e.V.

Betriebswirtschaftliches Forschungszentrum für Fragen
der mittelständischen Wirtschaft e. V. an der Universität
Bayreuth
(*Business Research Center for Small and Medium-Sized
Enterprises e. V. at the University of Bayreuth*),
Germany

<https://www.bfm-bayreuth.de>



IT-Sicherheitscluster e. V.,
Germany

<https://www.it-sicherheitscluster.de>



MYKOLO ROMERIO UNIVERSITETAS,
Lithuania

<https://www.mruni.eu>

This document is licensed under CC BY-NC-SA 4.0.

This document was produced as part of the ERASMUS+ project "Sovereign Citizen Alliance – SOCIAL", Project ID: 2021-2-DE02-KA210-VET-000051512

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

CISA50plus Information Security Analysis

Questionnaire/Assessment

Within the framework of SOCIAL, the project CISA50plus (*Compliance Information Security Analysis plus*) was developed by IT-Sicherheitscluster e. V. on the basis of the existing assessment ISA+ Information Security Analysis. This is a systematic approach that offers a low-threshold introduction to information security. As SOCIAL has shown, it is easier to start by filling out a questionnaire to find out the status or information security level of an organization that has not yet developed any protective measures. Therefore, an assessment was adapted to the needs of SME's.

This work is licensed under [CC BY-NC-SA 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/)

The following block of questions consists of three addressed fields:

Organisational issues (including on policies, instructions, training, and responsibilities)

Technical issues (including existing IT systems, data backup, emergency preparedness)

Legal issues (including on compliance and third-party services)

On the basis of the evaluation of the basic requirements in information security, the company could be declared compliant through an audit procedure which has to be developed. For the survey and evaluation of the level of protection achieved in the company, it is necessary to answer the most questions on a high maturity level.

Partner Information in SOCIAL

<https://www.it-sicherheitscluster.de>

Contact:

IT-Sicherheitscluster e. V.
Dr. Matthias Kampmann, CEO
Franz-Mayer-Str. 1
93053 Regensburg


Tel.: 0941/604889-32
Matthias.Kampmann@it-sicherheitscluster.de

How does CISA50plus works?

1. Start gathering information alongside the questionnaire.
2. Find out the level of fulfillment.
3. Arrange the results in the matrix which is given to each question.
4. Count the results.
5. If you experience more than maturity level 3 in each block, a sufficient level of protection is given in order to continue working with an ISMS.
6. If a ko question could not be answered, you must start again.

Procedure model



#	Question	Recommendation for action	Level of maturity	
1.	<p>Is there a dedicated guideline on information security and is it signed by the management?</p> 	<p>The guideline on information security is not intended to be a complete concept paper on information security. It represents the high importance of information security to the company must affirm management's exhaustive support of the measures necessary to implement the guideline accordingly. At a minimum, the information security policy should be communicated throughout the company in such a way that its meaning is apparent to users, everyone affected by it has access to it and can understand it.</p> <p>The guideline should contain the following points (based on BSI IT-Grundschutz):</p> <ul style="list-style-type: none"> • the importance of information security and the significance of the company's essential information, business processes and IT, • the security objectives and the relationship of the security objectives to the company's business objectives and tasks, • the core elements of the security strategy, • the readiness of the company's management to enforce the policy and statements on implementation control, • the description of the organizational structure for the implementation of the security process, • the signature of the management. <p>The following are subsequently required for more in-depth measures to implement the security guideline:</p> <ul style="list-style-type: none"> • Security concept(s) (framework requirements, e.g., for virus protection, data backup, etc.), • detailed elaborations (instructions for action) for the security concept, e.g., concrete administration settings 	<p>Maturity level 0:</p> <ul style="list-style-type: none"> • Not available. <p>Maturity level 1:</p> <ul style="list-style-type: none"> • The topic is known to the management and the creation of a guideline is planned <p>Maturity level 2:</p> <ul style="list-style-type: none"> • Document is being prepared and results can be presented; Document is available but not signed; Document is available and signed, but a statement is missing on the following topics: Importance of information security, description of the security objectives and their relation to the company's business goals or tasks, the core elements of the security strategy (for example: we do not use WLAN in the company), willingness of the company management to enforce the guideline and statements on implementation control, description of the organizational structure for the implementation of the security process (responsibilities). <p>Maturity level 3:</p> <ul style="list-style-type: none"> • Finished formulated guideline on information security, which is available in printed form, signed by the management and contains statements on each of the following topics: importance of information security, description of the security objectives and their relation to the business objectives or tasks of the company, the core elements of the security strategy (for example: we do not use WLAN in the company), readiness of the management to enforce the guideline and statements on implementation control, description of the organizational structure for the implementation of the security process (responsibilities). 	File inspection




#	Question	Recommendation for action	Level of maturity	
2.	Is the role of information security officer filled in your organization?	<p>The central role of an information security officer is essential for effective implementation and, above all, for regular review and adaptation of the information security guideline. Due to the quite existing requirements for security know-how, coordination/communication skills and also ability for training and consulting, the corresponding officer should be selected according. The officer must have the explicit support of the company's management.</p> <p>In small companies, this task can also be performed by the IT officer or the administrator. In some cases, the data protection officer is also appointed as the IS officer and vice versa. In principle, it is also possible to commission an external service provider.</p>	<p>Maturity level 0:</p> <ul style="list-style-type: none"> Not available. <p>Maturity level 1:</p> <ul style="list-style-type: none"> The search for an IS envoy has been initiated. <p>Maturity level 2:</p> <ul style="list-style-type: none"> An IS officer is identified (appointed), but no certificate of appointment (signed by management and the employee) or (service) contract with an assurance of coverage from the service provider (through insurance) can be provided. <p>Maturity level 3:</p> <ul style="list-style-type: none"> A certificate of appointment (signed by management and the employee) or a (service) contract with an assurance of coverage from the service provider (through an insurance company) can be provided. 	File inspection
3.	Is the appointee suitable for the task?	<p>The tasks of the Information Security Officer include initiating, coordinating and documenting the development, implementation, control and updating of the rules and regulations for information security. The Information Security Officer must be involved at an early stage in the introduction of new procedures/processes, systems or rules and in the modification of existing procedures/processes, systems or rules. It is also his task to advise and raise awareness internally (management and employees) and externally (e.g., partners/customers) on information security issues with reference to the company's guideline.</p> <p>Measured against this task, the suitability of the officer should be verified and, if necessary, established through training or external consulting. These tasks can be carried out as a secondary activity. The information security officer is expected to have relevant training or continuing education.</p>	<p>Maturity level 0:</p> <ul style="list-style-type: none"> Not suitable. <p>Maturity level 1:</p> <ul style="list-style-type: none"> The appointee is an employee with (management's) expected competence. <p>Maturity level 2:</p> <ul style="list-style-type: none"> The appointee shall have completed training in IT or have at least 5 years of professional experience as an IT supervisor. <p>Maturity level 3:</p> <ul style="list-style-type: none"> The officer has successfully completed an additional qualification (seminar/training) on information security (maximum 2 years ago), or the officer has at least 5 years of professional experience and has successfully completed training in the IT field. 	Interview

#	Question	Recommendation for action	Level of maturity	
4.	Has a necessary data protection officer been appointed and has he or she drawn up an operational data protection concept?	<p>Under certain conditions, the applicable laws require the appointment of a company data protection officer. This function can also be provided by an external service provider or performed by the IS officer.</p> <p>In small and medium-sized enterprises (SMEs), the handling of the most important framework data of the data protection organization can also be mapped in a central security concept for information security (see question 7).</p>	<p>Maturity level 0:</p> <ul style="list-style-type: none"> • Not available. <p>Maturity level 1:</p> <ul style="list-style-type: none"> • Implementation started. <p>Maturity level 2:</p> <ul style="list-style-type: none"> • A data protection officer has been appointed or there is a data protection concept. <p>Maturity level 3:</p> <ul style="list-style-type: none"> • A data protection officer has been appointed and a data protection concept is in place. 	File inspection
5.	Is there an overview of the important applications and IT systems and their protection needs?	<p>A complete inventory of hardware, software, applications, systems, networks, etc. is the basic requirement for this overview. Current network plans should be available. Changes in the environment should be documented regularly.</p> <p>An assessment of the probability of occurrence of threats and subsequently an appropriate risk evaluation (risk analysis, need for protection) should be supported by the network partner and internal staff, but not carried out in its entirety by the network partner itself, in order to exclude conflicts of interest and to ensure the objectivity of an evaluation.</p> <p>The assessment considers the protection goals of confidentiality, availability and integrity. Important systems are all systems for which a violation of the protection goals can seriously damage the company or even threaten its existence.</p>	<p>Maturity level 0:</p> <ul style="list-style-type: none"> • There is no overview. <p>Maturity level 1:</p> <ul style="list-style-type: none"> • Work has begun on creating an inventory of the important systems. <p>Maturity level 2:</p> <ul style="list-style-type: none"> • All important systems are listed in an inventory. <p>Maturity level 3:</p> <ul style="list-style-type: none"> • Confidentiality, Integrity and Availability assessments are made for each key system, and damage assessments are stored with appropriate units of measure. 	File inspection



#	Question	Recommendation for action	Level of maturity	
6.	Are there checklists of what to look for when new employees join and when employees leave?	Checklists are necessary for the complete implementation of security processes. They must contain items such as a new employee's acknowledgement of the guideline and instructions for the concrete implementation of information security in the company (e.g., private Internet use at the workplace, password policy, etc.), granting and revoking access/access authorizations, user rights, key return, handling of user data, etc.. The processes of on- and off boarding should be regulated and documented.	<p>Maturity level 0:</p> <ul style="list-style-type: none"> • Checklist not available. <p>Maturity level 1:</p> <ul style="list-style-type: none"> • Creation of a checklist started. <p>Maturity level 2:</p> <ul style="list-style-type: none"> • The checklist(s) provided address at least the following items: granting/withdrawing access to the premises, granting/withdrawing access authorization to the IT systems, deleting/blocking the employee's data and user account, returning equipment, data and documents provided. <p>Maturity level 3:</p> <ul style="list-style-type: none"> • In addition to maturity level 2, a process exists in which it is defined WHO is responsible or accountable for the following: granting/withdrawing access to the premises, granting/withdrawing access authorization to the IT systems, deleting/blocking the employee's data and user account, returning provided equipment, data and documents. 	File inspection
7.	Is there an information security concept?	In small and medium-sized enterprises (SMEs), the treatment of the most important framework data can be mapped in a central security concept. All important topics must be included, such as virus protection, data backups, emergency measures, etc. Security concepts do not yet contain detailed descriptions of technical implementation. They serve to provide direction for action instructions and to sensitize and train all employees. For example, they must contain information about the duties of employees/users, the reasons for implementing measures, and the processes that have been implemented. Preventive measures, damage scenarios, rules of conduct, general knowledge about threats should be conveyed in the security concept.	<p>Maturity level 0:</p> <ul style="list-style-type: none"> • Concept not available. <p>Maturity level 1:</p> <ul style="list-style-type: none"> • Creation of a concept started. <p>Maturity level 2:</p> <ul style="list-style-type: none"> • An information security concept (the concept does not have to be a stand-alone document) can be submitted. <p>Maturity level 3:</p> <ul style="list-style-type: none"> • The information security concept specifies in more detail the requirements and guiding principles (core statements) of the guideline on information security (cf. test approach 1.). 	File inspection



#	Question	Recommendation for action	Level of maturity	
8.	<p>Are there measures in place to ensure information security in the company (also includes hacker attacks, phishing, social engineering, etc.)?</p> 	<p>Technical IT security measures are essential for information security, but are by no means sufficient on their own. For complete implementation, information security must be seen as an ongoing process that must be constantly improved. This applies not only to IT employees, but to everyone in the company. Measures therefore also include, for example:</p> <ul style="list-style-type: none"> • Regular training of all employees on information security topics. • Up-to-date information on threats • Raising employee awareness (e.g., to prevent phishing attacks) • Continuous reaffirmation of the importance of information security for the company 	<p>Maturity level 0:</p> <ul style="list-style-type: none"> • Not available. <p>Maturity level 1:</p> <ul style="list-style-type: none"> • Information security fact sheet or training materials exist for employees. <p>Maturity level 2:</p> <ul style="list-style-type: none"> • In addition to maturity level 1, there is a documented process or concept for identified threats or the distribution of information, which informs employees about the threat situation and the necessary (and expected) actions. <p>Maturity level 3:</p> <ul style="list-style-type: none"> • In addition to maturity level 2, recurring (regular or ongoing) training measures are established: Awareness campaigns, online courses, classroom events, reporting system, wiki / intranet. 	Interview
9.	<p>Do all employees have sufficient knowledge to ensure information security?</p>	<p>Technical IT security measures are essential for information security, but are by no means sufficient on their own. For complete implementation, information security must be seen as an ongoing process that must be constantly improved. This applies not only to IT employees, but to everyone in the company. Measures therefore also include, for example:</p> <ul style="list-style-type: none"> • Regular training of all employees on information security topics. • Up-to-date information on threats • Raising employee awareness (e.g., to prevent phishing attacks) • Continuous reaffirmation of the importance of information security for the company 	<p>Interview with (at least) one employee (who may not be the IT supervisor, IS officer, data protection officer or a member of the management at the same time)</p> <p>Maturity level 0:</p> <ul style="list-style-type: none"> • Not guaranteed. <p>Maturity level 1:</p> <ul style="list-style-type: none"> • Employees are aware of the existence of an information security policy. <p>Maturity level 2:</p> <ul style="list-style-type: none"> • Employee can name the location of the (for their work or task area) essential action instructions / guidelines - at least, however, the guideline for information security. <p>Maturity level 3:</p> <ul style="list-style-type: none"> • In addition to maturity level 2, employees can correctly identify the information security officer by name. 	Interview



#	Question	Recommendation for action	Level of maturity	
10.	Are all employees encouraged to report safety incidents?	A process (contact person, communication channel) should be made known and employees should be made aware of their obligation to report security incidents. In order to clarify which incidents are to be reported, employees should be made aware of unusual occurrences through training measures and made aware of the importance of reporting. This also applies to areas beyond IT security, such as access regulations to company premises.	<p>Maturity level 0:</p> <ul style="list-style-type: none"> Security incidents are not reported. <p>Maturity level 1:</p> <ul style="list-style-type: none"> concept is currently being implemented. <p>Maturity level 2:</p> <ul style="list-style-type: none"> There is a hotline (central contact person) or contact persons are defined for each department / topic / area and reporting channels are described <p>Maturity level 3:</p> <ul style="list-style-type: none"> In addition to maturity level 2, characteristics for a security incident are described. 	File inspection
11.	Are systems secured with screen locks and passwords on exit?	Here, an explicit instruction for action and an accompanying training measure (why is this necessary?) is helpful. Automatic locking of the computer or activation of password protection in the event of inactivity should be set up in such a way that it does not unduly interfere with the user's normal work (e.g. automatic locking after 5 minutes of inactivity).	<p>Demonstration with (at least) one employee (who may not also be the IT supervisor, IS officer, the privacy officer, or a member of management) by asking them to leave the workplace.</p> <p>Maturity level 0:</p> <ul style="list-style-type: none"> Will not be implemented. <p>Maturity level 1:</p> <ul style="list-style-type: none"> There is a corresponding instruction (guideline, regulation, etc.) for the employees or an automatic blocking of the system in case of absence is technically brought about (for example via a guideline). <p>Maturity level 2:</p> <ul style="list-style-type: none"> During the demonstration, the employee locks his or her system immediately upon leaving the workplace or carries it with him or her (in the case of mobile devices). <p>Maturity level 3:</p> <ul style="list-style-type: none"> The implemented action instruction or technically induced blocking of the systems explicitly considers mobile devices as well. 	Observation / Control



#	Question	Recommendation for action	Level of maturity	
12.	Is there a password policy?	<p>Users must be made aware that the security of data and information is directly related to the strength and careful handling of passwords. A password that is easy to guess or a password for a large number of different applications significantly reduces the security of IT systems. The password policy should specify and make users specifically aware of how passwords should be designed, how they should be handled (no sharing, etc.), how often they should be changed, etc. Passwords should be changed regularly and should not be based on older passwords. Default passwords for access to systems (e.g., routers) must be changed immediately.</p> <p>A password policy should also include processes for password management and recovery.</p>	<p>Interview with (at least) one employee (who may not be the IT supervisor, IS officer, data protection officer or a member of the management at the same time)</p> <p>Maturity level 0:</p> <ul style="list-style-type: none"> Not available. <p>Maturity level 1:</p> <ul style="list-style-type: none"> A policy governs the use of passwords and may be submitted (by the IS Officer). <p>Maturity level 2:</p> <ul style="list-style-type: none"> The employee may specify the storage or repository location of the policy. <p>Maturity level 3:</p> <ul style="list-style-type: none"> The guideline also explicitly takes mobile devices into account. 	Interview
13.	Are password policy settings technically enforced?	<p>In network domain environments, a password policy can be enforced technically, e.g., via the server and the domain controllers. This measure should definitely be implemented, as a policy or action instruction alone is still too often circumvented by users. These administrative procedures should only be performed by specialists. Strong authentication measures should be implemented technically for access to information and systems that require special protection (e.g., smart card, biometrics, 2-factor authentication).</p>	<p>Here, the statement of a sufficiently qualified employee (for example, the IT supervisor or administrator) should be used as evidence.</p> <p>Maturity level 0:</p> <ul style="list-style-type: none"> Not implemented. <p>Maturity level 1:</p> <ul style="list-style-type: none"> Implementation started <p>Maturity level 2:</p> <ul style="list-style-type: none"> In the directory service (at least) one policy is implemented. <p>Maturity level 3:</p> <ul style="list-style-type: none"> A technical solution is also implemented for mobile devices. 	Interview



#	Question	Recommendation for action	Level of maturity	
14.	Is the private use of e-mail and the Internet in the company clearly regulated by a policy and do leaflets or instructions exist on the safe use of these services?	<p>If there is no regulation, the company should inform itself about the legal provisions and determine the appropriate regulation for itself individually. These should be set out in writing and communicated to the employees in supplementary agreements to the employment contract. If there are no leaflets on the safe use of e-mail and the Internet, clear instructions should be drawn up and made known to every employee. These should be enriched with practical examples. The guideline and instructions or leaflets should also address the use of social media.</p> <p>The company can obtain support from its own data protection officer or IT security expert. Training employees in this area also minimizes the risks.</p>	<p>Interview with (at least) one employee (who may not be the IT supervisor, IS officer, data protection officer or a member of the management at the same time)</p> <p>Maturity level 0:</p> <ul style="list-style-type: none"> The issue has not yet been settled or is (still) under discussion. <p>Maturity level 1:</p> <ul style="list-style-type: none"> Documents regulating the use and informing the users are being prepared. <p>Maturity level 2:</p> <ul style="list-style-type: none"> Documents, such as a fact sheet, policy, or (work) instruction, that regulate use and inform the user can be submitted by the IS officer and have already been communicated. <p>Maturity level 3:</p> <ul style="list-style-type: none"> There is a concept of control of the use regulation and audit reports can be submitted and a staff member is aware of the existence of this regulation and information. 	Interview
15.	Are browsers and email clients configured to a reasonable security level?	<p>The company should keep a list of which employees need which browser functions for their activities with which end device. For example, is Java really necessary for everyone? The same is true for e-mail clients. Here, the spam settings, permitted attachments, etc. must be taken into account. Then the security levels on the end devices are set up and documented.</p>	<p>Maturity level 0:</p> <ul style="list-style-type: none"> Not implemented. <p>Maturity level 1:</p> <ul style="list-style-type: none"> Necessary applications and services are identified (white list). <p>Maturity level 2:</p> <ul style="list-style-type: none"> Configuration specifications are formulated in writing, and the specifications also take mobile devices into account. <p>Maturity level 3:</p> <ul style="list-style-type: none"> A process for adapting the released applications and services as well as the implemented protection mechanisms is documented. 	Interview




#	Question	Recommendation for action	Level of maturity	
16.	Are the systems configured uniformly? And cannot they be changed by users?	After working through question 15, it should be checked whether a uniform configuration can be implemented on all end devices. Irrespective of this, it should be ensured that the user rights are set up in such a way that the user cannot change the defined and set-up security levels himself.	<p>Maturity level 0:</p> <ul style="list-style-type: none"> • Not implemented. <p>Maturity level 1:</p> <ul style="list-style-type: none"> • The configuration of systems is predefined and the implementation is regulated in a process. <p>Maturity level 2:</p> <ul style="list-style-type: none"> • In addition to maturity level 1, (uniform) refueling of the systems is carried out by defined bodies before handover to the user. <p>Maturity level 3:</p> <ul style="list-style-type: none"> • The systems are monitored and a change of the configuration by the user is technically reset to the default or prevented. 	Interview



#	Question	Recommendation for action	Maturity level	
17.	Are unneeded programs and services on endpoints uninstalled or disabled and individual extensions secured?	If there are programs and services on the computer that are no longer needed, they should be uninstalled by the administrator. Outdated programs and services no longer receive updates and emerging security gaps can be exploited by attackers. This process (in combination with question 18.) is also called "system hardening".	<p>Maturity level 0:</p> <ul style="list-style-type: none"> Not implemented. <p>Maturity level 1:</p> <ul style="list-style-type: none"> For the operating system the released or required programs and services are defined and additionally the released or required further applications (apps) are defined. <p>Maturity level 2:</p> <ul style="list-style-type: none"> There is a regulation (process, concept, instruction) for matching the actual configuration with the definition for released programs and services for the operating system (OS) and the further applications (APP). This regulation also takes into account mobile devices. <p>Maturity level 3:</p> <ul style="list-style-type: none"> In addition to maturity level 2, software enhancements are documented in writing and there is a person responsible for this or enhancements are explicitly prohibited. 	File inspection
18.	Are all unnecessary programs uninstalled and services disabled on the servers and active network devices?	If there are programs and services on the servers that are no longer needed, they should be uninstalled by the administrator. Outdated programs and services no longer receive updates and emerging security gaps can be exploited by attackers. This process (in combination with question 17.) is also called "system hardening".	<p>Maturity level 0:</p> <ul style="list-style-type: none"> Not implemented. <p>Maturity level 1:</p> <ul style="list-style-type: none"> For the operating system, the released or required programs and services are defined. <p>Maturity level 2:</p> <ul style="list-style-type: none"> In addition to maturity level 1, the released or required further applications (apps) are defined. <p>Maturity level 3:</p> <ul style="list-style-type: none"> There is a regulation (process, concept, instruction) for matching the actual configuration with the definition for released programs and services for the operating system (OS) and the other applications (APP). 	File inspection

#	Question	Recommendation for action	Maturity level	
19.	Are the systems used (operating systems, software, browsers, etc.) up to date and are all applicable security updates for the entire software applied promptly?	Security gaps can occur in operating systems, software, browsers, etc. over a longer period of time. To close these, operating systems etc. should always be updated. For this purpose, the administrator should operate a patch or update management system. The validation and release of updates must be described in this documented process.	<p>Sample of the most important IT systems identified (See also question 5)</p> <p>Maturity level 0:</p> <ul style="list-style-type: none"> Not implemented. <p>Maturity level 1:</p> <ul style="list-style-type: none"> Automatic updates are configured according to availability. <p>Maturity level 2:</p> <ul style="list-style-type: none"> Updates are installed automatically after release. <p>Maturity level 3:</p> <ul style="list-style-type: none"> There is a documented process that governs the validation and release of updates. 	Observation / Control
20.	Is access to networks and the WLAN secured?	If WLAN is used in the company, it is essential to ensure that it is encrypted. If networks are not encrypted, attackers can read out security-critical data such as passwords, etc. and thus obtain company data. To prevent this, the latest WPA standard (from WPA2) and a password with at least 13 digits should be used for the encryption method.	<p>Maturity level 0:</p> <ul style="list-style-type: none"> Not implemented. <p>Maturity level 1:</p> <ul style="list-style-type: none"> The existing WLAN is included in the network documentation. <p>Maturity level 2:</p> <ul style="list-style-type: none"> The available WLAN is taken into account in the overview of important applications (see question 5). <p>Maturity level 3:</p> <ul style="list-style-type: none"> There is no WLAN in use or there is a concept for using and securing the WLAN accesses used. 	File inspection

#	Question	Recommendation for action	Maturity level	
21.	Is it regulated which functions each employee may use and which databases he or she may access?	Before the roles and profiles for the employees can be created, it must first be defined which functions or to which databases an employee has or may have access. Once the roles and profiles have been created for employees (see also question 22.), they should be restricted by means of appropriate rights (see question 23.). These rights define which functions or which databases an employee has access to.	<p>Maturity level 0:</p> <ul style="list-style-type: none"> Not regulated. <p>Maturity level 1:</p> <ul style="list-style-type: none"> The regulations are in preparation. <p>Maturity level 2:</p> <ul style="list-style-type: none"> A reconciliation of the scope of available data / information and available functions / resources are documented. <p>Maturity level 3:</p> <ul style="list-style-type: none"> In addition to maturity level 2, change management for tracking necessary changes (for example, in a concept) is documented. 	File inspection
22.	Are user roles defined and assigned to all system users accordingly? 	Appropriate roles and profiles should be set up for each employee for daily work on any systems. This makes it easier to track who is working on a computer and what rights they need to do so.	<p>Here, the statement of a sufficiently qualified employee (for example, the IT supervisor or administrator) should be used as evidence</p> <p>Maturity level 0:</p> <ul style="list-style-type: none"> Not implemented. <p>Maturity level 1:</p> <ul style="list-style-type: none"> Role definitions are available. <p>Maturity level 2:</p> <ul style="list-style-type: none"> 1. roles exist for all functions mentioned in question 21. 2. described roles are created in the directory service and the applications mentioned in question 5. <p>Maturity level 3:</p> <ul style="list-style-type: none"> In addition to maturity level 2, there are exclusively person-related accesses (no anonymous accesses and group accesses). In special areas of application, recommendations from other standards can be incorporated, e.g. BSI ICS Security Compendium 	Interview



#	Question	Recommendation for action	Maturity level	
23.	Are the rights restricted according to the work environment?	<p>Depending on the work environment, appropriate rights should be defined. An administrator should have all rights, for example, to be able to perform maintenance work, etc. A clerk should not have access rights to accounting data, but only the accounting department itself or the managing director.</p> <p>Access rights should be adjusted according to the work environment and appropriate roles should be defined. In the event of resignation or change of department, these should be adjusted immediately.</p>	<p>Spot check of individual applications and roles</p> <p>Maturity level 0:</p> <ul style="list-style-type: none"> Not implemented. <p>Maturity level 1:</p> <ul style="list-style-type: none"> Documentation of the process has begun. <p>Maturity level 2:</p> <ul style="list-style-type: none"> A process for granting (additional) roles is documented. <p>Maturity level 3:</p> <ul style="list-style-type: none"> In addition to maturity level 2, a process for withdrawing roles is documented. 	File inspection
24.	Are virus scanners available on the systems used?	<p>To avoid security risks, a virus scanner should be installed on every system. Good virus scanners are already available as freeware; however, licenses should be purchased for the company. The virus scanners should scan the system for viruses, Trojans, etc. at regular intervals.</p>	<p>Sample from both the main IT systems identified (question 5.) and the end devices.</p> <p>Maturity level 0:</p> <ul style="list-style-type: none"> Not implemented. <p>Maturity level 1:</p> <ul style="list-style-type: none"> Virus scanners are installed on some systems. <p>Maturity level 2:</p> <ul style="list-style-type: none"> Virus scanners are installed on all systems (accessing the corporate network). Virus scanners are also installed on mobile devices (if available on the market). <p>Maturity level 3:</p> <ul style="list-style-type: none"> In addition to maturity level 2, centralized management solutions are in place to distribute and monitor virus protection. 	Observation / Control



#	Question	Recommendation for action	Maturity level	
25.	Are virus protection updates performed regularly at short intervals?	The manufacturers regularly release updates for their virus scanners, which are usually installed automatically by the software. These updates are important because new viruses, Trojans, etc. become known every day.	<p>Maturity level 0:</p> <ul style="list-style-type: none"> Not implemented. <p>Maturity level 1:</p> <ul style="list-style-type: none"> Automatic updates are configured according to availability. <p>Maturity level 2:</p> <ul style="list-style-type: none"> Updates are installed automatically after release. <p>Maturity level 3:</p> <ul style="list-style-type: none"> There is a documented process that governs the validation and release of updates. 	File inspection
26.	Is there a fact sheet on how to protect against malware?	The information security officer must create a guideline or fact sheet for the workforce in which the employees are sensitized with regard to protection against malware. Regular training sessions for employees are also recommended for this purpose.	<p>Maturity level 0:</p> <ul style="list-style-type: none"> Not available. <p>Maturity level 1:</p> <ul style="list-style-type: none"> Instruction sheet is being prepared. <p>Maturity level 2:</p> <ul style="list-style-type: none"> Leaflet is available and can be provided by the IS Officer. <p>Maturity level 3:</p> <ul style="list-style-type: none"> In addition to maturity level 2, characteristics of malware and possible ways of spreading it within the company are described. 	File inspection
27.	Is there a fact sheet on what to do when an incident occurs?	Employees should be prepared for the occurrence of an incident via guidelines, regulations or fact sheets. In these guidelines, the employee should be informed about which clues he or she should pass on to the information security officer. In general, employees should report any incident to the administrator immediately to prevent further damage. This memo can be combined with the malware policy from question	<p>Maturity level 0:</p> <ul style="list-style-type: none"> Not available. <p>Maturity level 1:</p> <ul style="list-style-type: none"> Instruction sheet is being prepared. <p>Maturity level 2:</p> <ul style="list-style-type: none"> Leaflet is available and can be provided by the IS Officer <p>Maturity level 3:</p> <ul style="list-style-type: none"> In addition to maturity level 2, characteristics of malware and possible ways of spreading it within the company are described.. 	File inspection



#	Question	Recommendation for action	Maturity level	
28.	Are all employees aware of the leaflets on protection against malware and what to do if an incident occurs?	Employees should be familiarized with the regulations, leaflets and guidelines in training sessions. In this context, incomprehensible points in the regulations, leaflets and guidelines or questions from the employees can be addressed.	<p>Interview with (at least) one employee (who may not be the IT supervisor, IS officer, data protection officer or a member of the management at the same time)</p> <p>Maturity level 0:</p> <ul style="list-style-type: none"> Not implemented. <p>Maturity level 1:</p> <ul style="list-style-type: none"> The employee is aware of the existence of the leaflets. <p>Maturity level 2:</p> <ul style="list-style-type: none"> The employee can name the storage or filing location of the leaflets or can show a copy of the leaflets themselves. <p>Maturity level 3:</p> <ul style="list-style-type: none"> In addition to maturity level 2, the employee can describe the process for distributing fact sheets. 	Interview
29.	Is the corporate network protected by a firewall?	If there is no firewall in the company, the information security officer or administrator should install a firewall immediately. Without a firewall, attackers can gain targeted access to company data. There are a large number of suitable solutions on the subject of "Firewall for small businesses".	<p>Definition of "firewall": Bidirectional packet filter</p> <p>Here, the statement of a sufficiently qualified employee (for example, the IT supervisor or administrator) should be used as evidence.</p> <p>Maturity level 0:</p> <ul style="list-style-type: none"> No, partly, with restrictions etc. <p>Maturity level 3:</p> <ul style="list-style-type: none"> Yes. 	Interview



#	Question	Recommendation for action	Maturity level	
30.	Are firewall configuration and functionality critically reviewed and controlled on a regular basis, and are penetration tests performed regularly in all areas?	In order to detect security vulnerabilities, the administrator should regularly perform penetration tests. The regular installation of new updates is also of great importance here. In addition, so-called "pentesters" can be hired externally to test the firewall for possible open security gaps. Based on the report of the pentester, the respective steps should then be initiated to disclosed the gaps as quickly as possible.	<p>Maturity level 0:</p> <ul style="list-style-type: none"> Is not implemented. <p>Maturity level 1:</p> <ul style="list-style-type: none"> There is an ongoing contract for software maintenance and system updates for the firewall used. <p>Maturity level 2:</p> <ul style="list-style-type: none"> A concept is available that also covers the modification of the existing configuration and the installation of updates. <p>Maturity level 3:</p> <ul style="list-style-type: none"> A process for configuring as well as monitoring the firewall exists and audit trails can be provided or an external service provider is contracted to configure and monitor the firewall. 	File inspection
31.	Is there adequate protection of IT systems against fire, overheating, water damage, overvoltage, power failure and burglary?	To ensure adequate protection of IT systems, rooms or parts of buildings containing IT systems should be located in a secure environment. Attention should also be paid to fire protection regulations or hazardous situations such as water damage or lightning strikes. Fire detectors, water detectors and lightning rods, for example, can help. Burglar alarms should be installed to protect against theft.	<p>The following hazards are considered: Fire, overheating, water damage, overvoltage, power failure, burglary</p> <p>Maturity level 0:</p> <ul style="list-style-type: none"> There is no adequate protection. <p>Maturity level 1:</p> <ul style="list-style-type: none"> Concept is in preparation. <p>Maturity level 2:</p> <ul style="list-style-type: none"> For some important systems from question 5 with availability requirements, statements are made about possible hazards. <p>Maturity level 3:</p> <ul style="list-style-type: none"> Statements are made about all hazards for all major systems from question 5 with availability requirements. 	File inspection


#	Question	Recommendation for action	Maturity level	
32.	Is access to IT systems and to the company's premises regulated?	<p>In general, only the administrator and management should have access to important IT systems. Rooms with servers or other important IT systems should always be locked and care should be taken as to who is allowed to enter such rooms. For this purpose, access regulations and controls should be established. This can be done, for example, by means of an employee ID card, an RFID chip or biometric methods.</p> <p>In order to physically prevent unauthorized persons from accessing the respective systems, individual systems should be physically separated from one another according to content.</p>	<p>Maturity level 0:</p> <ul style="list-style-type: none"> Not regulated. <p>Maturity level 1:</p> <ul style="list-style-type: none"> Security areas and (access-) authorized groups of persons are defined. <p>Maturity level 2:</p> <ul style="list-style-type: none"> In addition to maturity level 1, instructions / regulations exist for dealing with external persons. <p>Maturity level 3:</p> <ul style="list-style-type: none"> In addition to maturity level 2, access to server and storage systems is monitored and logged. 	File inspection
33.	Are visitors, craftsmen, service personnel, etc. accompanied or supervised?	<p>External visitors should always be accompanied or supervised due to data protection and preventive measures. Important rooms should therefore be locked and care should be taken to ensure that tradesmen, for example, only have access to unobjectionable rooms.</p>	<p>Interview with (at least) one employee (who may not also be the IS officer, the data protection officer or a member of the management)</p> <p>Maturity level 0:</p> <ul style="list-style-type: none"> No, partial, limited, etc. <p>Maturity level 3:</p> <ul style="list-style-type: none"> Yes. 	Interview
34.	Are there suitable substitution arrangements for responsible persons and are the substitutes familiar with their tasks?	<p>Viable substitution arrangements must be in place for all key business processes and tasks. These must be updated regularly. The assumption of tasks in the event of a substitution requires that the status of the process or project is adequately documented.</p> <p>It must be specified which tasks are to be performed by whom in the event of a substitution.</p> <p>It must be checked what the substitute's level of knowledge is for the task to be taken over; the substitute may have to be trained accordingly in advance.</p>	<p>Maturity level 0:</p> <ul style="list-style-type: none"> Not regulated. <p>Maturity level 1:</p> <ul style="list-style-type: none"> Functions and their tasks are described. <p>Maturity level 2:</p> <ul style="list-style-type: none"> A substitution (here for the functions security and IT administration) is described. <p>Maturity level 3:</p> <ul style="list-style-type: none"> A concept regulates the representation and handover. 	File inspection



#	Question	Recommendation for action	Maturity level	
35.	Are the most important passwords securely stored for emergencies?	Passwords required for configuration and maintenance should be stored securely for emergencies. When storing passwords, the required current passwords must be stored by each employee in a suitable place (e.g. in the secretary's office in a safe in a closed envelope). Each time one of the passwords is changed, it must be updated. No password may be forgotten in the process.	<p>Maturity level 0:</p> <ul style="list-style-type: none"> Not implemented. <p>Maturity level 1:</p> <ul style="list-style-type: none"> Documentation of passwords and access IDs for all major applications referenced in question 5. exists.. <p>Maturity level 2:</p> <ul style="list-style-type: none"> In addition to maturity level 1, access to this information is restricted to defined groups of people. <p>Maturity level 3:</p> <ul style="list-style-type: none"> In addition to maturity level 2, the use of this information and the tracking of changes is regulated (process for using). 	File inspection
36.	Is there a list of emergency contacts?	Preparation of an emergency plan with responsibilities, contact addresses of all employees with specific tasks in emergency management as well as external contact persons, such as cooperation partners, service providers, aid organizations or supervisory authorities. Possibly appointment of an emergency officer by the management.	<p>Maturity level 0:</p> <ul style="list-style-type: none"> Not available. <p>Maturity level 1:</p> <ul style="list-style-type: none"> A list of emergency contact addresses is being compiled. <p>Maturity level 2:</p> <ul style="list-style-type: none"> The list contains contact addresses for all important applications and IT systems from question 5. <p>Maturity level 3:</p> <ul style="list-style-type: none"> In addition to maturity level 2, a process governs the revision and updating of the list of contact addresses. 	File inspection



#	Question	Recommendation for action	Maturity level	
37.	Is there a procedure in case of system failure or data loss (conceptually written contingency plans, disaster recovery plans, business continuity plans)?	The failure of an IT system can have serious consequences. As part of emergency preparedness, a concept must therefore be drawn up for how the consequences of a failure can be minimized and what activities are to be carried out in the event of a failure. A system failure can also result in data loss. A corresponding concept must therefore be drawn up as part of the general data backup concept.	<p>Maturity level 0:</p> <ul style="list-style-type: none"> There is no procedure. <p>Maturity level 1:</p> <ul style="list-style-type: none"> A concept can be presented. <p>Maturity level 2:</p> <ul style="list-style-type: none"> The concept makes statements about all important applications and IT systems from question 5. <p>Maturity level 3:</p> <ul style="list-style-type: none"> In addition to maturity level 2, a process regulates the revision and updating of the concept. 	File inspection
38.	Does each employee know the list of contact addresses as well as the procedure and are they easily accessible?	The emergency plan must be made known to the employees in a suitable form. It is recommended to document the announcement. In addition, all regulations must be kept in their current form in one place and made accessible in the event of justified interest.	<p>Interview with (at least) one employee (who may not also be the IT supervisor, IS officer, the data protection officer or a member of the management)</p> <p>Maturity level 0:</p> <ul style="list-style-type: none"> Not implemented. <p>Maturity level 1:</p> <ul style="list-style-type: none"> The employee is aware of the existence of the list of contact addresses or the procedure. <p>Maturity level 2:</p> <ul style="list-style-type: none"> The employee is aware of the existence of the list of contact addresses and the procedure. <p>Maturity level 3:</p> <ul style="list-style-type: none"> The employee can name the storage or filing location of the list of contact addresses and the procedure. 	Interview

#	Question	Recommendation for action	Maturity level	
39.	Are data files backed up regularly? 	<p>Regular data backups must be performed in order to prevent data loss and to ensure that the obligation to provide evidence and data backup are sustainable. In most computer systems, these backups can be largely automated. Regulations must be made as to which data is backed up by whom and when. The creation of a data backup concept is recommended.</p> <p>The backup concept should include the secure storage of data media, the backup types for the respective analyses (incremental, full, etc.) and the frequency of backups (daily, weekly, etc.).</p>	<p>Maturity level 0:</p> <ul style="list-style-type: none"> Data files are not backed up. <p>Maturity level 1:</p> <ul style="list-style-type: none"> The data to be backed up is identified. <p>Maturity level 2:</p> <ul style="list-style-type: none"> A concept for securing the identified data can be presented. <p>Maturity level 3:</p> <ul style="list-style-type: none"> The concept also takes into account mobile devices and cloud services. 	File inspection
40.	Are the backups stored in a protected manner?	<p>Access to these data carriers must only be possible for authorized persons, so that theft can be ruled out. The storage location must also ensure the climatic conditions for longer-term storage of data media. In the event of a disaster, the backup data carriers must be stored spatially separate from the computer, if possible in a different fire compartment.</p>	<p>Here, the statement of a sufficiently qualified employee (for example, the IT supervisor or administrator) should be used as evidence.</p> <p>Maturity level 0:</p> <ul style="list-style-type: none"> Data backups are not stored in a protected manner. <p>Maturity level 1:</p> <ul style="list-style-type: none"> Access to the secured data is restricted (for example, by encryption). <p>Maturity level 2:</p> <ul style="list-style-type: none"> In addition to maturity level 1, the data is backed up spatially separated from the place of processing. <p>Maturity level 3:</p> <ul style="list-style-type: none"> In addition to maturity level 2, there is a concept for using backups and restoring information. 	Interview



#	Question	Recommendation for action	Maturity level	
41.	Are information and data carriers classified and handled accordingly?	Confidential information must be protected from unauthorized disclosure. The backup media must be stored in a secure location, preferably outside the company or the office building. The storage location should also be adequately protected against elemental damage such as fire, water and the like. Access to these data media must be possible only for authorized persons, so that theft can be ruled out.	<p>Maturity level 0:</p> <ul style="list-style-type: none"> • Handling is not regulated. <p>Maturity level 1:</p> <ul style="list-style-type: none"> • Classes of information are defined. <p>Maturity level 2:</p> <ul style="list-style-type: none"> • The handling of classified information is regulated. <p>Maturity level 3:</p> <ul style="list-style-type: none"> • In addition to maturity level 2, a process governs the revision and update of classification and handling. 	File inspection
42.	Are maintenance, service and support tasks performed by appropriate personnel?	Maintenance and administration personnel require detailed knowledge of the IT components used. For this reason, they should be trained at least to the extent that they can carry out everyday administrative tasks themselves, detect and correct simple errors themselves, perform regular data backups themselves, track the interventions of external maintenance personnel, and detect and quickly correct attempts at manipulation or unauthorized access to the systems. Appropriate training courses are usually offered by the manufacturers of the IT systems or PBXs.	<p>Maturity level 0:</p> <ul style="list-style-type: none"> • Not implemented. <p>Maturity level 1:</p> <ul style="list-style-type: none"> • Persons for individual maintenance tasks are designated. <p>Maturity level 2:</p> <ul style="list-style-type: none"> • In addition to maturity level 1, the scope of maintenance tasks and the expected (positive) outcome of maintenance are described. <p>Maturity level 3:</p> <ul style="list-style-type: none"> • In addition to maturity level 2, the employee is additionally qualified for the maintenance task (for example, through instruction or training) or an external service provider is commissioned to perform maintenance tasks. 	File inspection



#	Question	Recommendation for action	Maturity level	
43.	Is confidential information protected during maintenance or repair work on data carriers or IT systems?	For maintenance and repair work on the premises, especially if it is carried out by external persons, regulations must be made concerning their supervision: during the work, a competent person should supervise the work to such an extent that he or she can judge whether unauthorized actions are being carried out during the work. Furthermore, it should be checked whether the maintenance order has been carried out to the agreed extent. Access to data by the maintenance technician must be avoided as far as possible.	<p>Maturity level 0:</p> <ul style="list-style-type: none"> Not implemented. <p>Maturity level 1:</p> <ul style="list-style-type: none"> Statements are made in writing on the technical and organizational protection of confidential information. <p>Maturity level 2:</p> <ul style="list-style-type: none"> The statements made also include the topics of maintenance, repair and the decommissioning of systems. <p>Maturity level 3:</p> <ul style="list-style-type: none"> The statements from maturity level 2 also include the topics of mobile devices and cloud services. 	File inspection



#	Question	Recommendation for action	Maturity level	
44.	<p>Is there an overview of essential contractual and legal requirements for information processing in the company with regard to the collection, processing, storage, protection, deletion and transfer of information?</p>	<p>For companies, regardless of their size, various legal regulations apply today that directly or indirectly affect information technology, since information technology is integrated into almost all areas of business processes. Typical well-known regulations from the tax code with regard to archiving regulations as well as the GoBD or valid data protection law are to be mentioned here. For certain industries, more extensive requirements also apply, e.g., for banks and financial service providers with MaRisk or in the medical sector. These requirements can be extended by contractual arrangements under private law (e.g., in the context of customer-supplier relationships, due to integration into group structures, or through outsourcing agreements).</p> <p>If a company does not have an overview of which legal and private law requirements apply directly or indirectly to its information processing, a corresponding analysis should be carried out. This should include the requirements from the classic areas of data protection, data security, archiving, industry standards, and others (e.g., requirements under private law). The first point of contact for this can generally be associations, the Chamber of Industry and Commerce or your own tax advisor.</p> <p>Significant contractual and legal requirements are characterized by the fact that non-compliance can have significant consequences for the company, even threatening its existence, or criminal consequences for employees / management.</p>	<p>Reifegrad 0:</p> <ul style="list-style-type: none"> No overview available. <p>Maturity level 1:</p> <ul style="list-style-type: none"> Collection of legal regulations available (for example, information from the Chamber of Industry and Commerce, tax consultants, etc.). <p>Maturity level 2:</p> <ul style="list-style-type: none"> Structured collection of material available (for example, information from the Chamber of Industry and Commerce, tax advisor, etc.) OR there is an up-to-date directory of information processing procedures / processes (e.g., directory of processing activities) <p>Maturity level 3:</p> <ul style="list-style-type: none"> Allocation of the essential contractual and legal requirements to the procedures in place in the company with regard to the collection, processing, storage, protection, deletion and transfer of information (list of processing activities) OR to documented business processes. 	File inspection

K.O.
Question



#	Question	Recommendation for action	Maturity level	
45.	Is there a binding, company-wide policy for outsourcing data to external service companies and using cloud services?	Outsourcing data to external service companies can have an impact on internal processes, concepts and protection levels. This decision should also always be checked against existing agreements and contracts. For the outsourcing of data, an understandable process should therefore be introduced for checking against the existing framework conditions or the decision is made not to outsource data. The use of cloud services is also to be regarded as outsourcing of data. Is there a strategy to prevent the company from a vendor lockin?	<p>Reifegrad 0:</p> <ul style="list-style-type: none"> The topic is still unregulated. <p>Maturity level 1:</p> <ul style="list-style-type: none"> The documentation of a process (concept) and the framework conditions to be examined has been started. <p>Maturity level 2:</p> <ul style="list-style-type: none"> A process (concept) has been developed or the framework conditions to be tested have been documented. <p>Maturity level 3:</p> <ul style="list-style-type: none"> There is a written statement from the company's management to refrain from outsourcing data to external service companies / using cloud services (for example, in the security guideline) or a process (concept) is implemented that describes how the outsourcing of data is checked, evaluated and controlled against the existing and documented framework conditions. 	File inspection



#	Question	Recommendation for action	Maturity level	
46.	Are employees and recipients of information (service providers, etc.) aware of or communicated the due diligence obligations resulting from the outsourcing of data / use of cloud services with regard to the storage, processing, deletion and transfer of data?	<p>A lack of awareness among employees and close business partners can be remedied by training sessions as well as information sheets - possibly even with an obligation character in the form of instructions. Furthermore, structured document categorization (e.g., classification of information as "public," "internal only," or "confidential") can provide employees with clear guidance on how to handle information (For assistance, see Question 41. Classification of information).</p> <p>Addressees outside the company's direct sphere of influence must be informed of corresponding regulations or, if necessary, be subject to binding obligations via corresponding contractual regulations (e.g., in the form of the agreements on commissioned processing). If it is not possible to agree on a binding regulation with third parties (e.g., by using standard contracts without the possibility of influencing the form of the contract), possible further protective measures (e.g., cryptography) must be taken, depending on the need for protection of the information in question.</p>	<p>Maturity level 0:</p> <ul style="list-style-type: none"> Not implemented. <p>Maturity level 1:</p> <ul style="list-style-type: none"> Documentation is in preparation. <p>Maturity level 2:</p> <ul style="list-style-type: none"> Current contracts (e.g., for commissioned processing), guidelines, fact sheets, or training materials exist on this topic <p>Maturity level 3:</p> <ul style="list-style-type: none"> In addition to maturity level 2: <ul style="list-style-type: none"> The current extended directory of information processing procedures / processes (e.g. directory of processing activities) is extended to include the requirements / due diligence obligations for outsourcing / transfer of data, is up to date and is known to the employees and the external recipients of information OR Information or documents are classified with respect to the intended recipient group (for example, "Internal", "Public", "Secret"). OR A process is established that informs and obligates the persons involved of the (special) duties of care when handling this information. 	File inspection / Interview




#	Question	Recommendation for action	Maturity level	
47.	Are checks made to ensure that contractual and legal requirements for information processing are met?	More important than the factual verification is the conception of an effective control system that ensures, on the basis of process-organizational regulations, that compliance with the requirements already becomes a natural part of the work processes. This may require reorganizing workflows and responsibilities / accountabilities.	<p>Maturity level 0:</p> <ul style="list-style-type: none"> • Will not be tested. <p>Maturity level 1:</p> <ul style="list-style-type: none"> • Implementation started. <p>Maturity level 2:</p> <ul style="list-style-type: none"> • In the current directory of information processing procedures/processes (e.g. extended directory of processing activities), a person responsible for the procedure/process is named for each procedure/process, who reviews the procedures/processes on a regular and/or ad hoc basis. <p>Maturity level 3:</p> <ul style="list-style-type: none"> • A process is established that provides for requirements testing (optionally checks dependencies against the requirement in question 44.) when changing or implementing a procedure/process for collecting, processing, or using information. 	File inspection



#	Question	Recommendation for action	Maturity level	
48.	Are there regulations governing which data must or may be stored and for how long?	<p>The entrepreneur must obtain an overview of the data available in his company. Where is data generated, where is it processed, where is it stored, and what does it contain? On the basis of this analysis, lifecycle management can then be defined for data groups, which structures the storage but also deletion of data in accordance with regulations. Another added value of this analysis is that the data protection concept can be adapted to the various life cycles and priorities, and important insights for emergency management also emerge from it.</p> <p>In many companies, there is a lack of clarity about which data must be stored for how long or when there are obligations to delete data again. The typical requirements for data storage result from operational concerns and legal regulations, such as the German Fiscal Code (Abgabenordnung) and the German Commercial Code (HGB) with regard to archiving requirements. However, the applicable data protection law also imposes obligations to delete data again at specific points in time and not at some point in time when there happens to be time to do so.</p>	<p>Maturity level 0:</p> <ul style="list-style-type: none"> • Not implemented. <p>Maturity level 1:</p> <ul style="list-style-type: none"> • Documentation in progress. <p>Maturity level 2:</p> <ul style="list-style-type: none"> • In the documented business processes, statements are made about the storage and deletion periods for information or information classes. The statements on the storage and deletion periods refer to the relevant requirement (law, contract, etc.) OR • There is an up-to-date directory of information processing procedures/processes (e.g. directory of processing activities) known to the employees, which, in addition to the storage/deletion periods for personal data, also includes corresponding information on the other data. <p>Maturity level 3:</p> <ul style="list-style-type: none"> • In addition to maturity level 2, it is demonstrably documented that the storage and deletion of data is carried out in a systematized manner in accordance with the specified information. 	File inspection



#	Question	Recommendation for action	Maturity level	
49.	<p>Is there an overview of how third parties are involved in IT operations or which external services are used?</p> 	<p>To analyze and identify the third parties involved, a matrix of the rule and individual activities for planning, implementing and maintaining the company's IT landscape should be created.</p> <p>Examples:</p> <ul style="list-style-type: none"> • Maintenance of the telephone system and TC terminals • Provision of Internet access / connection • Maintenance and care of archiving system • Care and maintenance of the network infrastructure • Maintenance of the IT plant systems • General IT support • Hardware maintenance (server) • Hardware maintenance (printers and multifunction devices) • Supply of spare parts and consumables • External data protection officer • Cleaning services / Building cleaning • Cleaning services / glass and frames • Care and maintenance of internet presence, CMS and newsletter system 	<p>Maturity level 0:</p> <ul style="list-style-type: none"> • Not available. <p>Maturity level 1:</p> <ul style="list-style-type: none"> • Overview is in preparation. <p>Maturity level 2:</p> <ul style="list-style-type: none"> • An overview of essential service areas in which information is collected, processed and used and where external persons can gain entry, access or access to information is available for download. The list includes information on general network support, service providers for building cleaning (if available), service providers for the enterprise resource planning system or the ERP application, service providers for (financial / payroll) accounting, service providers who provide data center services (if available). <p>Maturity level 3:</p> <ul style="list-style-type: none"> • In the overview, information is provided for each entry from the "Overview of important IT systems and applications" (see question 5.). 	File inspection



#	Question	Recommendation for action	Maturity level	
50.	Have the security-related requirements resulting from contracts been identified and do the company's own contracts contain corresponding regulations?	<p>To ensure that all security-relevant issues are adequately taken into account, the IS Officer and/or, if applicable, the Data Protection Officer must be involved in the preparation and receipt of contracts. This must be taken into account in particular for contracts in which security-specific requirements and obligations are addressed that are imposed both by the company on third parties (e.g., service providers) and by third parties on the company.</p> <p>All existing contracts should be made available to the IS Officer and/or, if applicable, the Data Protection Officer for review so that an assessment can be performed with regard to security-related requirements.</p> <p>With this question, a fundamental understanding on the part of (company) management of the fact that many areas of operational activity also have a legal component/dimension is expected.</p>	<p>Maturity level 0:</p> <ul style="list-style-type: none"> Not available. <p>Maturity level 1:</p> <ul style="list-style-type: none"> Creation started. <p>Maturity level 2:</p> <ul style="list-style-type: none"> An information security officer (question 2) and (if necessary) a data protection officer have been appointed in writing. The certificate of competence (training) is available (see also question 3). For DPOs, the following applies: If the (basic) training took place more than 18 months ago, a confirmation of participation in a data protection-specific continuing or advanced training event is available, or the DPO participates in a comprehensible exchange with other DPOs by participating in working groups. <p>Maturity level 3:</p> <ul style="list-style-type: none"> There is an up-to-date security concept (question 7) and an up-to-date data protection concept (documents have been signed) in which the early involvement of the ISB and (if necessary) the DPO is provided for when concluding contracts with suppliers / customers / service providers or when changes are made to model contracts / agreements. A person responsible for legal issues is defined in the organization chart (e.g. member of the management, lawyer, external consultant). 	File inspection

We thank the co-authors from:

BF/M-Bayreuth

IT-Security Cluster

Mykolas Romeris University

Sovereign Citizen Alliance - SOCIAL

Co-funded by the European Union



Co-funded by
the European Union

SOCIAL