Summary and purpose of the document

This document represents,

- which technical and organisational measures from ISO 27001 Annex A are implemented by TEMA-Q (and why);
- which technical and organisational measures from ISO 27001 Annex A TEMA-Q does not implement (and why not).

The document is public and can be handed out to all interested parties (customers, auditors, interested parties) if required. The Information Security Officer will be happy to answer any queries.

Applied and non-applied technical and organisational measures

In principle, TEMA-Q implements all measures from Annex A of ISO 27001, as they reduce information security risks. In the event that certain measures are also implemented for other reasons (e.g. for contractual reasons vis-à-vis customers or for legal reasons that apply in our industry or for intrinsic reasons), this is noted in the explanatory text and can be found there.

Measure from ISO 27001:2022 Appendix A	Application*	Reason for application or exclusion*
A.5.1	Yes	Role-specific guidelines enable all employees and external parties involved in ensuring information security to work together effectively. Regular updates and reviews of the guidelines ensure that the latest developments and tasks are included and that the guidelines remain effective and appropriate.
A.5.2	Yes	Role assignments help us to determine who has which responsibilities with regard to information security measures in which situations.
A.5.3	Yes	We implement segregation of duties as far as possible to ensure that a system of mutual protection is created for safety-critical tasks. However, this ends where it leads to inflexibility and cannot be achieved with the existing staffing levels.
A.5.4	Yes	Information security is only taken seriously if the management is behind it and demands compliance in the long term. That's why management is in the driving seat with us.
A.5.5	Yes	Contacts with relevant authorities provide us with early information on vulnerabilities, threats and legislative developments that could be relevant to information security.

A.5.6	Yes	Contacts with relevant interest groups provide us with early information on vulnerabilities, threats and other developments that could be relevant to information security.
A.5.7	Yes	Threat intelligence enables organisations to react proactively and actively to potential threats and strengthen their security strategies.
A.5.8	Yes	By analysing planned information security requirements in our projects, we can introduce and implement them in a targeted and timely manner. We analyse which information security requirements we place on the systems developed by us (or purchased by us) so that we can implement them.
A.5.9	Yes	Devices (and other assets) can only be operated safely if they are registered. The pflege of devices (and other assets) is only possible if someone feels responsible for each asset. We therefore ensure this.
A.5.10	Yes	Securing devices (and other assets) is only possible if it is clear for each device which use is permitted - i.e. "secure". We therefore ensure that assets are only used securely. To ensure that devices (and other assets) are handled as intended (and that information security is not unintentionally jeopardised by improper use), there are rules for all important devices as to how they may be used.
A.5.11	Yes	To ensure that devices are not left unattended when the employee responsible for them leaves the company or in the event of a change of employment, there is a requirement for regulated return.
A.5.12	Yes	Different types of information are critical in different ways. We have therefore categorised the types of information that we consider to be in need of protection.
A.5.13	Yes	This information is defined and visible to every employee so that it is quickly clear to everyone which information is classified and how.
A.5.14	Yes	To ensure that employees know how to protect which information when transferring it, we have established transfer guidelines that can be referred to at any time. We make agreements with our partners on how critical business information is transferred so that it is adequately protected during transfer. We also protect sensitive information when we store it in send electronic messages. We do this because the

		fast exchange via messages/chats is important for us and is used frequently - and must therefore be secure.
A.5.15	Yes	An access control policy regulates who can access which devices and information and for what reason. This ensures that access to devices and information is not arbitrary. We secure access to our networks so that information that flows into them is not compromised or the networks themselves cannot meet our availability requirements due to excessive load.
A.5.16	Yes	To ensure that users are created and deleted correctly and cleanly, we have a process that we use to register or deregister users.
A.5.17	Yes	We allocate secret authentication information (passwords etc.) via a regulated process to ensure that it remains secret during allocation. We require all users to keep their access data secret so that unauthorised persons cannot use it and gain access to sensitive information. have. To ensure that passwords cannot be guessed or spied out by brute force, we use system and organisational guidelines to ensure that they are secure (long enough, complex enough).
A.5.18	Yes	To ensure that registered users are granted rights correctly and cleanly, we have a process that we use to grant and withdraw rights to users. All employees who are responsible for devices (and other assets) at our company regularly check whether the access rights granted are still required. In this way, we ensure that unauthorised persons no longer have access. If employees (or freelancers who work for us) change their area of responsibility or leave us, we adjust or delete their access rights so that they do not have unauthorised access to sensitive information.
A.5.19	Yes	If our service providers need to access our organisation's assets, we regulate this in advance to ensure that no security gaps arise.
A.5.20	Yes	We conclude contracts with all service providers relevant to information security, which contain the service providers' pflects on information security.
A.5.21	Yes	In the contracts, we include provisions relating to Information security risks that occur or may occur at service providers because we are exposed to information security risks.

		even if they occur with our service providers.
A.5.22	Yes	We continuously check whether our service providers comply with the information security regulations agreed with them so that we can be sure of this. Our suppliers' services may change: we keep an eye on this so that we can adjust the information security regulations with our service providers if necessary.
A.5.23	Yes	We have defined how we deal with the use of cloud services and take information security requirements into account.
A.5.24	Yes	We have established a procedure that enables us to respond quickly and reliably to information security incidents. This is important to us in order to be able to resolve information security incidents quickly.
A.5.25	Yes	We assess every information security event (i.e. every suspicion that the targeted information security has been compromised) to determine whether it is an incident (i.e. the security has been demonstrably compromised) in order to be able to respond appropriately.
A.5.26	Yes	We ensure that we respond appropriately to recognised information security incidents so that they can be rectified as quickly as possible.
A.5.27	Yes	We make sure that we learn from previous information security incidents so that they do not occur again in the future.
A.5.28	Yes	In the event of acute information security incidents, all employees and service providers are required to collect evidence in order to simplify the assessment of the incident or to be able to reconstruct it later.
A.5.29	Yes	We have determined in which exceptional situations we want to maintain which level of information security so that we can communicate this to our interested parties and in particular contractual partners and focus on maintaining the defined information security. We define procedures with which we can ensure information security in the defined exceptional situations in order to be able to react if necessary. We test the above procedures to ensure that they work when we need them.
A.5.30	Yes	We have determined the exceptional situations in which we what degree of availability of the

		information in order to ensure uninterrupted business operations. We define procedures with which we can ensure information security in the defined exceptional situations in order to be able to react if necessary. We test the above procedures to ensure that they work when we need them.
A.5.31	Yes	We collect all legal, contractual and regulatory provisions relating to information security that apply to us so that we know which requirements we have to fulfil from this perspective. We comply with all legal, contractual and regulatory provisions that apply to us.
A.5.32	Yes	We have procedures in place to ensure that we use copyrighted works as intended or in accordance with the contract.
A.5.33	Yes	We store documents in accordance with the laws, contracts and other regulatory requirements that apply to us, so that information security in this area is taken into account.
A.5.34	Yes	We comply with the GDPR with regard to personal data.
A.5.35	Yes	We have our information security regulations reviewed by independent external organisations (e.g. certification organisations) to ensure that we are nothing important is overlooked.
A.5.36	Yes	We check internally whether all our employees are complying with the specified information security regulations so that they do not just pay lip service to them. We also check the information systems we use to ensure that they comply with all security guidelines to prevent unintentional information security leaks.
A.5.37	Yes	If information security depends on operating procedures for devices or systems being strictly adhered to, then we document these operating procedures. We make these documents available to the personnel who need them.
A.6.1	Yes	We are dependent on only hiring employees who are able to fulfil our safety requirements. We therefore carefully scrutinise who we hire (or have work for us as freelancers).

A.6.2	Yes	Agreements on information security that employees must adhere to can only be reliably honoured if all parties can see what has been agreed at any time. This is why we rely on contractual regulations.
A.6.3	Yes	In order to ensure that our employees can also implement information security, we focus on training in this area and develop each employee so that they can fulfil the tasks assigned to them with regard to information security.
A.6.4	Yes	If employees do not fulfil their information security duties, we are not indifferent. We talk about it and point it out. This ensures that the importance of the issue is recognised.
A.6.5	Yes	As we know that information security does not simply stop at the end of an employee's employment, we make sure that we also regulate the pflects that exist beyond the end of working hours.
A.6.6	Yes	Our non-disclosure agreements are always up to date to ensure that we always keep what is important to us secret.
A.6.7	Yes	Similar to mobile devices, remote workplaces are not completely "controllable" and can be a gateway for attacks and security vulnerabilities. We therefore regulate how remote work should be carried out in order to create security.
A.6.8	Yes	We ensure that information security incidents and -incidents are reported and processed as quickly as possible using the above procedures, as this ensures that we can restore security as quickly as possible if it is compromised. We encourage our employees and service providers to report information security incidents and events promptly so that we can deal with them quickly and effectively.
A.7.1	Yes	We have defined physical security zones in which certain information security regulations apply. In this way, we ensure that security-critical information cannot be compromised on our premises.
A.7.2	Yes	We ensure that our security zones are protected in such a way that unauthorised access is not possible. In this way, we improve the security of the information and devices in the zones. We have defined access points to our premises and monitor these so that no unauthorised persons can access them.

		and compromise information security.
A.7.3	Yes	We protect our offices, rooms and facilities so that no sensitive information can be compromised.
A.7.4	Yes	We carry out security monitoring of our access points to our premises so that no unauthorised persons can enter these points and compromise information security.
A.7.5	Yes	We ensure adequate protection against natural disasters, malicious attacks and assaults so that we do not lose any information worth protecting as a result of these events.
A.7.6	Yes	We have established procedures that apply to work in secure areas so that we do not unintentionally compromise the security of sensitive information.
A.7.7	Yes	To prevent sensitive information from being compromised by employees, we have a "clean desk policy".
A.7.8	Yes	We ensure that important devices and other operating equipment are set up safely so that they do not break down.
A.7.9	Yes	When devices are removed (and operated away from their actual location), we have rules that specify how they must be secured so that sensitive information processed with them is not compromised.
A.7.10	Yes	Removable data carriers can quickly get lost. We have therefore regulated how and under what conditions they may be used. When data carriers are disposed of, critical information may still be stored on them. We have therefore regulated how todispose of them securely. If critical information is stored on transportable data carriers, the risk of it being compromised is higher than on non-transportable data carriers. We have therefore strictly regulated transport. Anyone wishing to remove devices or other assets from their intended locations must agree this in advance. In this way, we ensure that we always know where important devices are located and recognise their loss at an early stage so that we can react.
A.7.11	Yes	Designing and installing supply lines (electricity, water, etc.) we protect them so that failures and leaks are minimised.

		or, if they do, that they do not compromise the security of the sensitive information.
A.7.12	Yes	We protect cables that transport power, data or supporting information services to ensure that they are not interrupted or tapped and that sensitive information is not compromised.
A.7.13	Yes	To prevent devices that are important for information security from failing, we ensure that they are professionally maintained at the scheduled intervals.
A.7.14	Yes	We delete devices and equipment that contain storage media before we dispose of or recycle them. This ensures that no sensitive information (including copyrighted information) is stored on them.
A.8.1	Yes	Endpoint devices are an easy gateway for attacks and security vulnerabilities. We therefore regulate how they may and may not be used. To prevent unauthorised persons from gaining access to unattended devices that are important for information security, we protect such devices in an appropriate manner when they are not being monitored by employees: By locking them away, by blocking them and by other appropriate measures.
A.8.2	Yes	To ensure that information security is not compromised intentionally or unintentionally by privileged access (admin accounts), we restrict and manage such access to only those people who need it.
A.8.3	Yes	We restrict access to information according to the need-to-know principle to those employees who need to have access to this information in order to carry out their work - all others are denied access. In this way, we ensure as far as possible that no-one who does not actually need access to information worthy of protection handles it unintentionally or intentionally insecurely.
A.8.4	Yes	Our source code repository is also a system to which we only grant access in accordance with our access control policy, so that no unauthorised persons can misuse or modify source code.
A.8.5	Yes	To ensure that secret authentication information is not compromised after it has been entered into information systems, we only use secure login procedures in which the authentication information is securely transported.

A.8.6	Yes	If the utilisation of certain resources (systems, employees) is important for information security, we monitor these in order to identify trends towards overloads at an early stage and counteract them.
A.8.7	Yes	We implement measures against malware on all systems where this is reasonably possible so that the systems are hardened against malicious attacks and can maintain information security. We support this through employee training.
A.8.8	Yes	We obtain information on technical vulnerabilities in the systems we use so that we can rectify them quickly and ensure that sensitive information is not compromised. We also check and evaluate the information systems we use to ensure that they comply with all security guidelines so that information security leaks do not occur unintentionally.
A.8.9	Yes	We use configuration management to ensure the consistency, control and quality of IT systems, software and other technical assets.
A.8.10	Yes	We do not store sensitive information for longer than is necessary for the purpose or for longer than the legal retention periods. By deleting information, we avoid unnecessary disclosure of sensitive information and comply with legal and contractual requirements for deletion.
A.8.11	Yes	We protect confidential information by masking the data without compromising operation or analysability.
A.8.12	Yes	By preventing data leaks on systems, networks and other systems that process, store or transmit sensitive information, we ensure the security and integrity of confidential information.
A.8.13	Yes	To ensure that important information is not lost, we have a backup policy for all information whose availability requires protection.
A.8.14	Yes	We plan the infrastructure that we need in such a redundant way that the risks arising from failure can be reduced to an acceptable level.
A.8.15	Yes	We log all important events in order to be able to analyse which events affect our systems either in advance or forensically. The log information is in turn backed up so that it cannot be deliberately or unconsciously falsified, deleted or disclosed

		can. The same applies to log information resulting from admin activities.
A.8.16	Yes	We monitor activities to minimise security threats, ensure compliance with regulations, optimise resources and improve the efficiency and stability of systems.
A.8.17	Yes	In order to be able to use log information correctly for analysis, we synchronise the clocks of all systems that generate log information.
A.8.18	Yes	We restrict the use of privileged utilities ("Run as...") as much as possible, because these programmes can be a gateway for attacks if malware can suddenly work with admin rights.
A.8.19	Yes	To prevent critical information systems from suddenly failing or not working as required, we ensure that new or modified software is not simply installed on them. A software and organisational installation policy ensures that the risk of unintentionally installing malware is reduced.
A.8.20	Yes	We design and manage the networks used by our systems so that they do not suddenly fail or are unable to cope with the expected traffic.
A.8.21	Yes	We think about what network performance we need (internally and externally) and make sure that this is available so that we are not taken by surprise. We monitor this because we want to ensure that the systems are secure.
A.8.22	Yes	Where necessary, we separate the networks in which our employees work and the networks in which our productive systems operate so that they cannot interfere with each other.
A.8.23	Yes	Through the use of webfilters, we protect the corporate network and minimise the risks.
A.8.24	Yes	We have guidelines according to which we encrypt information - both when it is stored and when it is sent. We also ensure that we protect critical information appropriately against spying. And for the use of cryptographic keys, because encrypted and authenticated information is only as secure as the storage and use of its keys.

A.8.25	Yes	We have a software development policy and require all those who develop software for us to apply it to ensure that software is developed safely.
A.8.26	Yes	We protect our online systems so that they are safe from fraudulent attacks that result in us not being able to honour our contracts with our customers. We protect all transactions that our customers carry out with our applications so that they remain complete, unaltered, authentic and confidential.
A.8.27	Yes	We have principles for the development of secure systems. We apply these to ensure that the systems we develop are safe.
A.8.28	Yes	Through secure programming, we ensure that the number of potential security vulnerabilities in the software is reduced.
A.8.29	Yes	We test all the safety functions of the systems we develop so that we can be sure that they work as intended. We also carry out acceptance tests for all systems that we purchase or develop so that we can ensure that their security functions work not only in individual cases, but also in the overall context.
A.8.30	Yes	We outsource development activities to partners. We monitor these partners because we want to ensure that the systems they develop are as secure as we need them to be.
A.8.31	Yes	We deliberately separate development, staging and production systems so that changes to one do not have unexpected consequences for the information security of the other. As security risks can also be introduced into developed systems via development environments, we ensure that the development environments we use are as secure as possible.
A.8.32	Yes	We make sure that important processes, information systems etc. are not changed "just like that" because this can jeopardise information security. We do not change the systems we use to develop software or the software products we develop "just like that", but only after thoroughly examining what we change - because we know that changes can also mean information security leaks. And we want to avoid that. When we update the operating systems used indevelopment, we check whether our development systems are still fit for purpose work flawlessly - because we know that not

		error-free behaviour can lead to information security leaks. We do not update software packages "because it works", but because we see the need to do so. We check the new packages in advance.
A.8.33	Yes	As we know that test data sometimes originates from production databases, we ensure that our test data is carefully protected.
A.8.34	Yes	If our production systems are to be audited, we will ensure that this does not take place during peak business hours so that we can also ensure the availability of our systems for our customers during the audit.

*** Application:** Yes, if the Annex A measure is applied. No, if not. Reason for application or exclusion: The reason why the measure is applied or not excluded.