

# Statement of Applicability ISO27001:2022

The Statement of Applicability (SoA) is a mandatory component of our Information Security Management System (ISMS) and provides an overview of the controls selected based on our risk assessment. This document clarifies which controls from Annex A of ISO/IEC 27001:2022 have been implemented, which are not applicable, and the rationale for each decision.

## Purpose of the SoA:

- To provide transparency on how risks are managed and controlled.
- To demonstrate accountability to internal and external stakeholders.
- To support the continual improvement of our ISMS.

## Contents of this SoA:

- A register of all controls from Annex A.
- The implementation status for each control, including a brief justification.

## Scope of the SoA:

The SoA applies to the scope of the ISMS as defined in the scope statement. The scope describes the applicability of the ISMS, including relevant departments, processes, systems, and locations.

## Maintenance and Updates

The SoA is reviewed and updated periodically to ensure ongoing alignment with changing risks, legal and regulatory requirements, and organizational objectives. Any changes are recorded and communicated to the relevant stakeholders.

For any substantive questions arising from this Statement of Applicability, please contact our CISO, Geert Koster, at [geert.koster@witteveenbos.com](mailto:geert.koster@witteveenbos.com).

Control	Objective	Status	Description	Basis			
				Jur.	Cl. dem.	Best pr.	Risk.
5.1 Policies for Information Security	Control: Information security policies and topic-specific policies shall be defined, approved by management, published, communicated to, and acknowledged by relevant personnel and interested parties, and shall be reviewed at planned intervals and upon the occurrence of significant changes.  Objective: To ensure the continuing	Fully implemented	The organization has an established information security policy that complies with the requirements of the ISO/IEC 27001 and BIO 2.0 standards.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Control	Objective	Status	Description	Basis			
				Jur.	Cl. dem.	Best pr.	Risk.
	suitability, adequacy, and effectiveness of management direction and support in accordance with business requirements as well as legal, statutory, regulatory, and contractual obligations.	Fully implemented					
5.2 Information Security Roles and Responsibilities	Control: Roles and responsibilities for information security shall be defined and assigned in accordance with the needs of the organization.  Objective: To establish a defined, approved, and clearly understandable structure for the implementation, operation, and management of information security within the organization.	Fully implemented	Roles and responsibilities for information security are defined and documented in the strategic information security policy	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.3 Segregation of Duties	Control: Conflicting duties and conflicting responsibilities shall be segregated.  Objective: To reduce the risk of fraud, errors, and the circumvention of information security controls.	Fully implemented	Witteveen+Bos applies segregation of duties where necessary, such as the separation between defining access rights and granting them.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.4 Management Responsibilities	Control: Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies, and organizational procedures.  Objective: To ensure that management understands its role in information security and takes measures to make certain that all personnel are aware of their information security responsibilities and comply with them.	Fully implemented	The board of directors and management require in the strategic information security policy that management ensures compliance with all information security policies. In topic-specific policy documents, employees are made aware of their responsibilities.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.5 Contact With Authorities	Control: The organization shall establish and maintain contact with relevant authorities.  Objective: To ensure an appropriate flow of information regarding information security between the organization and relevant legal, regulatory, and supervisory authorities.	Fully implemented	The organisation maintains contact with government authorities where this is legally required. In addition, the CISO is registered with the Digital Trust Center of the Ministry of Economic Affairs, and W+B participates in government-wide cyber exercises.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Control	Objective	Status	Description	Basis			
				Jur.	Cl. dem.	Best pr.	Risk.
5.6 Contact With Special Interest Groups	Control: The organization shall establish and maintain contacts with special interest groups or other specialized security forums and professional associations.  Objective: To ensure an appropriate flow of information regarding information security.	Fully implemented	The ICT department stays informed through contact with various suppliers and by visiting security-related websites on a daily basis. Regular consultations take place between CISOs, security specialists, and IT Managers from major engineering and construction companies.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.7 Threat Intelligence	Control: Information related to information security threats shall be collected and analyzed in order to produce threat intelligence and analyses.  Objective: To provide awareness of potential threats to the organization so that appropriate mitigating measures can be taken.	Fully implemented	Through various channels (suppliers, government, forums, RSS feeds, etc.), the organization stays informed about threats and assess whether developments require action from our organization.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.8 Information Security in Project Management	Control: Information security shall be integrated into project management.  Objective: To ensure that information security risks related to projects and the products and services to be delivered are effectively addressed within project management throughout the entire project lifecycle.	Fully implemented	During the proposal phase of projects, a risk analysis is conducted for QHSEI risks, which also includes information security risks.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.9 Inventory of Information and Other Associated Assets	Control: An inventory of information and other associated assets, including their owners, shall be established and maintained.  Objective: To identify the organization's information and other associated assets in order to preserve their information security and assign appropriate ownership.	Fully implemented	ICT Asset Management is carried out using inventory and registration software, through which all physical and virtual assets are managed.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.10 Acceptable Use of Information and Other Associated Assets	Control: Rules for the acceptable use of, and procedures for handling, information and other associated assets shall be identified, documented, and implemented.  Objective: To ensure that information and other associated assets are appropriately protected, used, and handled.	Fully implemented	Employees are required to sign for the responsible use of IT resources. In addition, upon entering employment, they receive IT awareness training. Throughout the year, employees are kept informed of current developments in the field of information security.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Control	Objective	Status	Description	Basis			
				Jur.	Cl.	dem.	Best pr.
5.11 Return of Assets	<p>Control: Personnel and other interested parties, as appropriate, shall return all organizational assets in their possession upon termination of their employment, contract, or agreement.</p> <p>Objective: To protect the organization's assets as part of the procedure for changing or terminating employment, contracts, or agreements.</p>	Fully implemented	A process has been established to ensure that employees return their belongings after the end of their employment. In addition, they are requested to delete or return all data they acquired during their work at W+B.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.12 Classification of Information	<p>Control: Information shall be classified in accordance with the organization's information security requirements, based on the needs for confidentiality, integrity, availability, and relevant stakeholder requirements.</p> <p>Objective: To ensure that the identification and understanding of protection needs for information are aligned with its importance to the organization.</p>	Fully implemented	The organization has a classification policy in place, in which the aspects of Availability, Integrity, and Confidentiality are explicitly specified.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.13 Labelling of Information	<p>Control: To label information, an appropriate set of procedures shall be developed and implemented in accordance with the information classification scheme established by the organization.</p> <p>Objective: To enable the communication of information classification and to support the automation of information processing and management.</p>	Fully implemented	In the folder structure of data storage, documents are placed in a separate "Finals" folder once they are finalized.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.14 Information Transfer	<p>Control: Rules, procedures, or agreements for information transfer shall be established for all types of communication facilities within the organization and between the organization and other parties.</p> <p>Objective: To maintain the security of information exchanged within the organization and with external stakeholders.</p>	Fully implemented	Where necessary and feasible, encrypted communication is applied, making use of modern technologies.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Control	Objective	Status	Description	Basis			
				Jur.	Cl. dem.	Best pr.	Risk.
5.15 Access Control	<p>Control: Rules based on business and information security requirements shall be established and implemented to control physical and logical access to information and other associated assets.</p> <p>Objective: To enable access for authorized individuals and prevent unauthorized access to information and other associated assets.</p>	Fully implemented	Access to the environment, systems, and data is granted based on a process that requires approval.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.16 Identity Management	<p>Control: The entire lifecycle of identities shall be managed.</p> <p>Objective: To enable the unique identification of individuals and systems that have access to the organization's information and other associated assets, and to ensure the proper assignment of access rights.</p>	Fully implemented	Access to networks, systems, and applications is managed in a controlled manner through automated HR integrations, role-based authorization management, and secure password procedures, with manual checks upon termination of employment.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.17 Authentication Information	<p>Control: The allocation and management of authentication information shall be controlled through a management process that includes advising personnel on the proper handling of authentication information.</p> <p>Objective: To ensure proper authentication and to prevent failures in authentication processes.</p>	Fully implemented	The policy, developed on the basis of risk analyses, focuses on secure access through password management, key management, logging, and periodic changes, carried out with specific tools.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.18 Access Rights	<p>Control: Access rights to information and other associated assets shall be granted, reviewed, adjusted, and removed in accordance with the organization's topic-specific policy and access control rules.</p> <p>Objective: To ensure that access to information and other associated assets is determined and approved in accordance with business requirements.</p>	Fully implemented	Access to systems and data is granted based on functional necessity through automated HR integrations, periodic reviews, and strict procedures during onboarding, changes, and offboarding.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Control	Objective	Status	Description	Basis			
				Jur.	Cl.	dem.	Best pr. Risk.
5.19 Information Security in Supplier Relationships	Control: Processes and procedures shall be established and implemented to manage the information security risks associated with the use of supplier products or services.  Objective: To maintain an agreed level of information security within supplier relationships.	Fully implemented	Suppliers are granted only strictly necessary access, with monitoring, logging, and documentation in TOPdesk. Permanent access to cloud environments is contractually arranged and periodically reviewed.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.20 Addressing Information Security Within Supplier Agreements	Control: Relevant information security requirements shall be defined and agreed upon with each supplier, based on the type of supplier relationship.  Objective: To maintain an agreed level of information security within supplier relationships.	Fully implemented	Suppliers with an impact on information security are assessed against defined criteria, with annual checks on certification and compliance with contractual security requirements.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.21 Managing Information Security in the ICT Supply Chain	Control: Processes and procedures shall be defined and implemented to manage the information security risks associated with the supply chain of ICT products and services.  Objective: To maintain an agreed level of information security within supplier relationships.	Fully implemented	Suppliers and applications are assessed based on certification, data location, and response times, with risk analyses and mitigation plans in place to ensure continuity and information security within the supply chain.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.22 Monitoring, Review and Change Management of Supplier Services	Control: The organization shall regularly monitor, review, evaluate, and manage changes to the information security practices and services of suppliers.  Objective: To maintain an agreed level of information security and service in accordance with supplier agreements.	Fully implemented	Suppliers with an impact on information security are selected based on defined criteria, registered and assessed annually, with changes being analyzed and managed on a project basis.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.23 Information Security for Use of Cloud Services	Control: Processes for the acquisition, use, management, and termination of cloud services shall be established in accordance with the organization's information security requirements.  Objective: To specify and manage information security for the use of cloud services.	Fully implemented	W+B has established processes for the selection, use, management, and termination of cloud services in line with the organization's information security requirements.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Control	Objective	Status	Description	Basis			
				Jur.	Cl. dem.	Best pr.	Risk.
5.24 Information Security Incident Management Planning and Preparation	<p>Control: The organization shall establish plans and prepare for managing information security incidents by defining, approving, and communicating processes, roles, and responsibilities for incident management.</p> <p>Objective: To ensure a prompt, effective, consistent, and orderly response to information security incidents, including communication regarding information security events.</p>	Fully implemented	The organization has a contingency plan to respond to incidents, and data breaches in particular, with direct coordination between ICT, the Privacy Officer, and other departments to ensure a rapid and adequate response in the event of an information security incident.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.25 Assessment and Decision on Information Security Events	<p>Control: The organization shall assess information security events and determine whether they should be classified as information security incidents.</p> <p>Objective: To ensure effective categorization and prioritization of information security events.</p>	Fully implemented	All incidents are recorded in TOPdesk, classified by the ICT Service Desk or system administration, and evaluated during annual risk sessions, with immediate escalation to the Privacy Officer and CISO in the event of potential data breaches.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.26 Response to Information Security Incidents	<p>Control: Information security incidents shall be responded to in accordance with documented procedures.</p> <p>Objective: To ensure an efficient and effective response to information security incidents.</p>	Fully implemented	Incidents are coordinated in consultation with the Privacy Officer and CISO, with actions based on the continuity plan and specific procedures, such as those for data breaches, phishing, and theft.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.27 Learning From Information Security Incidents	<p>Control: Knowledge gained from information security incidents shall be used to strengthen and improve information security controls.</p> <p>Objective: To reduce the likelihood or impact of future incidents.</p>	Fully implemented	Incidents are evaluated with continuous improvements such as anti-phishing programs, 2FA implementation, and internal awareness campaigns to strengthen information security measures.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.28 Collection of Evidence	<p>Control: The organization shall establish and implement procedures for identifying, collecting, acquiring, and preserving evidence related to information security events.</p> <p>Objective: To ensure consistent and effective handling of evidence related to information security incidents in the context of disciplinary and legal proceedings.</p>	Fully implemented	All information security incidents are recorded in our ticketing system, with relevant log information attached to the ticket as evidence. Tickets are retained for several years.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Control	Objective	Status	Description	Basis			
				Jur.	Cl. dem.	Best pr.	Risk.
5.29 Information Security During Disruption	Control: The organization shall establish plans to ensure information security at the appropriate level during a disruption.  Objective: To protect information and other associated assets during a disruption.	Fully implemented	The ICT continuity plan ensures recoverability and continuity through backups, fallback locations, and redundant systems, accessible via secured documentation and shared with the organization.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.30 ICT Readiness for Business Continuity	Control: ICT readiness shall be planned, implemented, maintained, and tested based on business continuity objectives and ICT continuity requirements.  Objective: To ensure the availability of the organization's information and other associated assets during a disruption.	Fully implemented	A continuity plan is in place, containing procedures to be followed in the event of a disruption of essential ICT services.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.31 Legal, Statutory, Regulatory and Contractual Requirements	Control: Legal, statutory, regulatory, and contractual requirements relevant to information security, as well as the organization's approach to meeting these requirements, shall be identified, documented, and kept up to date.  Objective: To ensure compliance with legal, statutory, regulatory, and contractual requirements related to information security.	Fully implemented	Applicable requirements are recorded in a central register, evaluated annually, communicated through training, and monitored with audits and reports to ensure compliance.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.32 Intellectual Property Rights	Control: The organization shall implement appropriate procedures to protect intellectual property rights.  Objective: To ensure compliance with legal, statutory, regulatory, and contractual requirements related to intellectual property rights and the use of patented products.	Fully implemented	Intellectual property rights are protected through centralized license management, compliance checks, internal guidelines, and training to ensure the proper use and protection of the rights of Witteveen+Bos and third parties.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.33 Protection of Records	Control: Records shall be protected against loss, destruction, falsification, unauthorized access, and unauthorized disclosure.  Objective: To ensure compliance with legal, statutory, regulatory, and contractual requirements, as well as community or societal expectations, regarding the protection and availability of records.	Fully implemented	Records are sustainably protected through retention periods, access control, and data consistency, with backups and standardized data formats to ensure long-term readability.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Control	Objective	Status	Description	Basis			
				Jur.	Cl. dem.	Best pr.	Risk.
5.34 Privacy and Protection of PII	<p>Control: The organization shall identify and comply with requirements regarding privacy and the protection of personal data in accordance with applicable laws, regulations, and contractual obligations.</p> <p>Objective: To ensure compliance with legal, statutory, regulatory, and contractual requirements concerning the information security aspects of personal data protection.</p>	Fully implemented	Personal data is protected through GDPR compliance, restricted access, technical security measures, and internal awareness training, with compliance monitored through audits and the privacy officer.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.35 Independent Review of Information Security	<p>Control: The organization's approach to information security management and its implementation, including people, processes, and technologies, shall be independently reviewed at planned intervals or whenever significant changes occur.</p> <p>Objective: To ensure that the organization continuously maintains an appropriate, adequate, and effective approach to information security management.</p>	Fully implemented	Witteveen+Bos is ISO 27001 certified and is audited annually by Lloyd's Register through external audits, complemented by internal audits focused on continuous improvement and compliance.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.36 Compliance With Policies, Rules and Standards for Information Security	<p>Control: Compliance with the information security policy, topic-specific policies, rules, and organizational standards shall be reviewed regularly.</p> <p>Objective: To ensure that information security is implemented and carried out in accordance with the information security policy, topic-specific policies, rules, and organizational standards.</p>	Fully implemented	Annual internal audits and penetration tests, and weekly external vulnerability scans ensure compliance and strengthen information security measures. In addition, managers are responsible for ensuring compliance within their teams.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.37 Documented Operating Procedures	<p>Control: Operating procedures for information processing facilities shall be documented and made available to personnel who require them.</p> <p>Objective: To ensure the correct and secure operation of information processing facilities.</p>	Fully implemented	Official vendor documentation and internal knowledge items in an internal ticketing system ensure consistent and secure execution of system and network management, with regular updates and restructuring of documentation.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Control	Objective	Status	Description	Basis			
				Jur.	Cl. dem.	Best pr.	Risk.
6.1 Screening	<p>Control: The background of all candidates for employment shall be verified before they join the organization and thereafter repeated at appropriate intervals. Such verification shall take into account applicable laws and regulations, ethical considerations, and shall be proportionate to business requirements, the classification of information to be accessed, and the identified risks.</p> <p>Objective: To ensure that all personnel are eligible and suitable for the roles for which they are considered and that they remain eligible and suitable throughout their employment.</p>	Fully implemented	New employees are screened through the document Pre- and Employment Screening, including physical identity checks, document uploads in Mijn PenO, and additional requirements on a project basis.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6.2 Terms and Conditions of Employment	<p>Control: Employment agreements shall specify the responsibilities of personnel and the organization with regard to information security.</p> <p>Objective: To ensure that personnel understand their information security responsibilities for the roles for which they may be considered.</p>	Fully implemented	New employees receive documents upon onboarding with information about working at Witteveen+Bos, including guidelines on information security, as part of their employment agreement.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6.3 Information Security Awareness, Education and Training	<p>Control: Organizational personnel and relevant stakeholders shall receive appropriate awareness, education, and training in information security, as well as regular updates on the organization's information security policy, topic-specific policies, and procedures, as relevant to their role.</p> <p>Objective: To ensure that personnel and relevant stakeholders are aware of their information security responsibilities and comply with them.</p>	Fully implemented	Employees receive regular training and information on information security, supplemented with simulations, intranet messages, and ICT-specific knowledge development to minimize risks and strengthen skills.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Control	Objective	Status	Description	Basis			
				Jur.	Cl. dem.	Best pr.	Risk.
6.4 Disciplinary Process	<p>Control: A formal and communicated disciplinary procedure shall be in place to take action against personnel and other stakeholders who have committed a breach of the information security policy.</p> <p>Objective: To ensure that personnel and other relevant stakeholders understand the consequences of breaching the information security policy, to deter them from committing a breach, and to appropriately address personnel and other relevant stakeholders who have committed a breach.</p>	Fully implemented	A policy has been established for handling violations of information security rules. This includes measures such as warnings, denial of access, and, if necessary, termination of employment.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6.5 Responsibilities After Termination or Change of Employment	<p>Control: Responsibilities and duties related to information security that remain in effect after termination or change of employment shall be defined, enforced, and communicated to relevant personnel and other stakeholders.</p> <p>Objective: To protect the interests of the organization as part of the employment or contract change or termination process.</p>	Fully implemented	In the employment agreement and related regulations, ongoing confidentiality obligations are stipulated. The proper handling of information security responsibilities upon termination of employment is enforced through checklists.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6.6 Confidentiality or Non-Disclosure Agreements	<p>Control: Confidentiality or non-disclosure agreements reflecting the organization's needs for information protection shall be identified, documented, regularly reviewed, and signed by personnel and other relevant stakeholders.</p> <p>Objective: To maintain the confidentiality of information to which personnel or external parties have access.</p>	Fully implemented	General confidentiality requirements are laid down in the Witteveen+Bos regulations, with additional project-specific agreements under the responsibility of the project manager and/or project director.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6.7 Remote Working	<p>Control: When personnel work remotely, security measures shall be implemented to protect information that is accessed, processed, or stored outside the organization's premises and/or facilities.</p> <p>Objective: To ensure the security of information when personnel are working remotely.</p>	Fully implemented	Remote working is facilitated through a secure VPN connection using a laptop provided by Witteveen+Bos, supported by a remote working policy and a checklist with specific attention to information security.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Control	Objective	Status	Description	Basis			
				Jur.	Cl. dem.	Best pr.	Risk.
6.8 Information Security Event Reporting	<p>Control: The organization shall provide a mechanism that enables personnel to report observed or suspected information security events in a timely manner through appropriate channels.</p> <p>Objective: To support the timely, consistent, and effective reporting of information security events that may be identified by personnel.</p>	Fully implemented	Incidents are reported via the ICT Service Desk, email or form, or the QHSEI reporting point, then escalated and subsequently evaluated to implement improvements.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.1 Physical Security Perimeters	<p>Control: Areas containing information and other associated assets shall be protected by defining and using security zones.</p> <p>Objective: To prevent unauthorized physical access to, damage to, and interference with the organization's information and other associated assets.</p>	Fully implemented	Witteveen+Bos defines physical security zones based on risk, with specific measures such as access control, monitoring, and secure storage, aligned with risks and client requirements.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.2 Physical Entry	<p>Control: Secure areas shall be protected by appropriate access control measures and entry points.</p> <p>Objective: To ensure that only authorized physical access to the organization's information and other associated assets takes place.</p>	Fully implemented	Access to offices is controlled through keys and badges. In addition, offices are equipped with alarm systems, security personnel, and/or video surveillance.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.3 Securing Offices, Rooms and Facilities	<p>Control: Physical security shall be designed and implemented for offices, rooms, and facilities.</p> <p>Objective: To prevent unauthorized physical access to, damage to, and interference with the organization's information and other associated assets in offices, rooms, and facilities.</p>	Fully implemented	Offices and ICT rooms are secured with access control and physical barriers. Additional project-specific measures, such as window shielding, door locking, and video surveillance, are applied when necessary.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.4 Physical Security Monitoring	<p>Control: The building and premises shall be continuously monitored for unauthorized physical access.</p> <p>Objective: To detect and deter unauthorized physical access.</p>	Fully implemented	Based on a risk assessment, video surveillance is applied. Access badges are logged, and access rights are periodically reviewed. Incidents are recorded and followed up.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Control	Objective	Status	Description	Basis			
				Jur.	Cl. dem.	Best pr.	Risk.
7.5 Protecting Against Physical and Environmental Threats	Control: Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure, shall be designed and implemented.  Objective: To prevent or minimize the impact of events resulting from physical and environmental threats.	Fully implemented	ICT environments are distributed across secured data centers in the Netherlands, with additional security measures in place for international offices and a continuity plan to mitigate physical threats.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.6 Working In Secure Areas	Control: Security measures shall be developed and implemented for working in secure areas.  Objective: To protect information and other associated assets in secure areas from damage and unauthorized disruption by personnel working in these areas.	Fully implemented	Access to secure areas is regulated with specific rights for standard, light security, and high security zones. Activities are logged, and access is regularly reviewed.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.7 Clear Desk and Clear Screen	Control: 'Clear desk' rules for paper documents and removable storage media, and 'clear screen' rules for information processing facilities, shall be defined and appropriately enforced.  Objective: To reduce the risks of unauthorized access to, loss of, and damage to information on desks, screens, and other accessible areas during and outside of working hours.	Fully implemented	Screens are locked and documents are securely stored to ensure confidentiality. Additional measures, such as physical security, are implemented on a project basis.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.8 Equipment Siting and Protection	Control: Equipment shall be securely placed and protected.  Objective: To reduce the risks of physical and environmental threats, unauthorized access, and damage.	Fully implemented	Equipment is placed in data centers, locked rooms, or racks, with monitoring of environmental requirements and additional protection against DDoS attacks for critical systems and connections.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.9 Security of Assets Off-Premises	Control: Assets outside the organization's premises and/or facilities shall be protected.  Objective: To prevent loss, damage, theft, or compromise of assets outside the organization's premises and/or facilities and to avoid disruption of the organization's business operations.	Fully implemented	Assets are securely transported by infrastructure staff or designated carriers, stored in locked rooms, and laptops are encrypted and managed through contracts. Project-specific arrangements are coordinated and documented.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Control	Objective	Status	Description	Basis			
				Jur.	Cl. dem.	Best pr.	Risk.
7.10 Storage Media	<p>Control: Storage media shall be managed throughout their entire lifecycle— procurement, use, transport, and disposal—in accordance with the organization’s classification scheme and handling requirements.</p> <p>Objective: To ensure that information on storage media is disclosed, modified, deleted, or destroyed only in an authorized manner.</p>	Fully implemented	The use of unencrypted storage media is not permitted for sensitive data. Storage media are securely managed, registered, and disposed of. Removable media are only used in controlled situations. Hardware is securely and responsibly disposed of.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.11 Supporting Utilities	<p>Control: Information processing facilities shall be protected against power failures and other disruptions caused by utility outages.</p> <p>Objective: To prevent loss, damage, or compromise of information and other associated assets, and to avoid disruption of the organization’s business operations due to failures or disturbances in supporting utilities.</p>	Fully implemented	Redundant power supply (UPS and generator) and multi-homed internet ensure continuity in the Netherlands and Belgium. International locations have additional provisions such as stabilizers and redundant internet lines where possible.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.12 Cabling Security	<p>Control: Power and telecommunications cables carrying data or supporting information services shall be protected against interception, interference, or damage.</p> <p>Objective: To prevent loss, damage, theft, or compromise of information and other associated assets, and to avoid disruption of the organization’s business operations related to power and communications cables.</p>	Fully implemented	Data and internet cables are secured through physical shielding and surge protection, with fiber optics being the preferred option. Power cables are placed in locked meter cabinets, and telephony in the Netherlands and Belgium is fully conducted via VoIP and mobile networks.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.13 Equipment Maintenance	<p>Control: Equipment shall be properly maintained to ensure the availability, integrity, and reliability of information.</p> <p>Objective: To prevent loss, damage, theft, or compromise of information and other associated assets, and to avoid disruption of the organization’s business operations due to inadequate maintenance.</p>	Fully implemented	Witteveen+Bos ensures availability through preventive and corrective maintenance on servers, network equipment, and mobile devices, supported by monitoring, inventory management, and defined depreciation periods.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Control	Objective	Status	Description	Basis			
				Jur.	Cl. dem.	Best pr.	Risk.
7.14 Secure Disposal or Re-Use of Equipment	Control: Equipment components containing storage media shall be checked to ensure that sensitive data and licensed software have been removed or securely overwritten before disposal or reuse.  Objective: To prevent information leakage through disposed of or reused equipment.	Fully implemented	Equipment is wiped, recorded, and securely disposed of in accordance with standardized workflows, minimizing the risk of data breaches while ensuring compliance with environmental requirements.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.1 User Endpoint Devices	Control: Information stored on, processed by, or accessible through user endpoint devices shall be protected.  Objective: To protect information against risks arising from the use of user endpoint devices.	Fully implemented	Devices such as laptops, mobile phones, and tablets are secured through encryption, firewalls, and MDM. Their use and disposal are managed through standardized workflows, with additional attention to project-specific tablets and (e)SIM card management.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.2 Privileged Access Rights	Control: The allocation and use of privileged access rights shall be restricted and managed.  Objective: To ensure that only authorized users, software components, and services are granted privileged access rights.	Fully implemented	Privileged access rights are managed for critical systems. Access is logged, monitored, and periodically reviewed to ensure security.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.3 Information Access Restriction	Control: Access to information and other associated assets shall be restricted in accordance with the established topic-specific access control policy.  Objective: To ensure that only authorized access is granted and to prevent unauthorized access to information and other associated assets.	Fully implemented	Data is only accessible through individual accounts with permissions aligned to the user's role and responsibilities. Access requests and management are carried out through documented procedures in a ticketing system.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.4 Access to Source Code	Control: Read and write access to source code, development tools, and software libraries shall be appropriately managed.  Objective: To prevent the introduction of unauthorized functionality, avoid unintended or malicious changes, and maintain the confidentiality of valuable intellectual property.	Fully implemented	Source code in the source code library is secured with AD-based authentication and is only accessible to authorized developers. Access rights are aligned with project needs and reviewed regularly.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Control	Objective	Status	Description	Basis			
				Jur.	Cl. dem.	Best pr.	Risk.
8.5 Secure Authentication	<p>Control: Secure authentication technologies and procedures shall be implemented based on access restrictions to information and the topic-specific access control policy.</p> <p>Objective: To ensure that a user or entity is securely authenticated when access to systems, applications, and services is granted.</p>	Fully implemented	Access to workstations, internal systems, and cloud services requires personal authentication with two-factor authentication. For laptops, a computer certificate is additionally required. Conditional Access prevents unauthorized access. Accounts are blocked after multiple failed login attempts; access is managed and monitored by ICT.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.6 Capacity Management	<p>Control: The use of resources shall be monitored and adjusted in accordance with current and anticipated capacity requirements.</p> <p>Objective: To ensure the required capacity of information processing facilities, personnel, offices, and other facilities.</p>	Fully implemented	Servers and storage are continuously monitored through monitoring systems. Additional capacity is determined on an ad hoc basis for new projects, and capacity bottlenecks are proactively managed.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.7 Protection Against Malware	<p>Control: Protection against malware shall be implemented and supported by appropriate user awareness.</p> <p>Objective: To ensure that information and other associated assets are protected against malware.</p>	Fully implemented	Malware is actively countered through endpoint protection and firewalls. Regular updates, penetration tests, and awareness campaigns strengthen the defense, and incidents are managed through ticketing software.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.8 Management of Technical Vulnerabilities	<p>Control: Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated, and appropriate measures shall be taken.</p> <p>Objective: To prevent the exploitation of technical vulnerabilities.</p>	Fully implemented	Updates are installed in a timely manner following monitoring through advisories and CVSS scores. Regular audits, penetration tests, and internal checks ensure effective vulnerability management.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.9 Configuration Management	<p>Control: Configurations, including security configurations, of hardware, software, services, and networks shall be established, documented, implemented, monitored, and reviewed.</p> <p>Objective: To ensure that hardware, software, services, and networks operate correctly with the required security settings and that configurations are not altered by unauthorized or incorrect changes.</p>	Fully implemented	A standard template for servers and workstations is applied, providing a secure baseline with responsible settings. These standards are centrally enforced.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Control	Objective	Status	Description	Basis			
				Jur.	Cl.	dem.	Best pr.
8.10 Information Deletion	<p>Control: Information stored in information systems, devices, or other storage media shall be erased when no longer required.</p> <p>Objective: To prevent the unnecessary disclosure of sensitive information and to comply with legal, statutory, regulatory, and contractual requirements for information erasure.</p>	Fully implemented	Information is deleted once the retention period has expired. Deletion procedures exist for both digital and physical data, in accordance with the GDPR and internal classification. Data is deleted or destroyed in a way that makes reuse or recovery impossible.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.11 Data Masking	<p>Control: Data shall be masked in accordance with the topic-specific access control policy and other related topic-specific policies, as well as the organization's business requirements, taking into account applicable legislation.</p> <p>Objective: To limit the disclosure of sensitive information, including personal data, and to comply with legal, statutory, regulatory, and contractual requirements.</p>	Fully implemented	W+B restricts access to data entirely wherever possible. Where this is not feasible, data masking is applied to protect sensitive information.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.12 Data Leakage Prevention	<p>Control: Measures to prevent data leaks shall be applied in systems, networks, and other devices on which or through which sensitive information is processed, stored, or transmitted.</p> <p>Objective: To detect and prevent the unauthorized disclosure and extraction of information by individuals or systems.</p>	Fully implemented	W+B prevents unintentional data leaks through a coherent system of technical security measures, access control, encryption, monitoring, and awareness programs to detect and prevent data leaks in systems, networks, and devices where sensitive information is processed.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.13 Information Backup	<p>Control: Backups of information, software, and systems shall be retained and regularly tested in accordance with the agreed topic-specific backup policy.</p> <p>Objective: To enable recovery after data or system loss.</p>	Fully implemented	Daily backups are performed and tested. Immutable backups and snapshots ensure continuity. Recovery procedures are documented and user-friendly, with a focus on critical systems such as file servers, Teams, email, and SharePoint.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.14 Redundancy of Information Processing Facilities	<p>Control: Information processing facilities shall be implemented with sufficient redundancy to meet availability requirements.</p> <p>Objective: To ensure the uninterrupted operation of information processing facilities.</p>	Fully implemented	Data centers and servers are designed with redundancy, including dual internet connections where possible. Measures such as remote working and spare parts minimize the impact of disruptions and support continuity.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Control	Objective	Status	Description	Basis			
				Jur.	Cl. dem.	Best pr.	Risk.
8.15 Logging	<p>Control: Log files that record activities, exceptions, faults, and other relevant events shall be generated, stored, protected, and analyzed.</p> <p>Objective: To record events, generate evidence, ensure the integrity of information in log files, prevent unauthorized access, identify information security events that may lead to an information security incident, and support investigations.</p>	Fully implemented	Logs are centrally stored in a log manager, checked daily, and backed up with immutable copies. Access is restricted. Logging supports forensic investigations and security monitoring.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.16 Monitoring Activities	<p>Control: Networks, systems, and applications shall be monitored for abnormal behavior, and appropriate measures shall be taken to assess potential information security incidents.</p> <p>Objective: To detect abnormal behavior and potential information security incidents.</p>	Fully implemented	The organization monitors critical systems using Endpoint Detection & Response (EDR). Abnormal behavior is detected, and tickets for follow-up are automatically generated.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.17 Clock Synchronization	<p>Control: The clocks of information processing systems used by the organization shall be synchronized with approved time sources.</p> <p>Objective: To enable the correlation and analysis of security-related events and other recorded data, and to support investigations of information security incidents.</p>	Fully implemented	A central time server synchronizes timestamps for all servers and network equipment. This is a requirement to ensure proper network functionality and logging.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.18 Use of Privileged Utility Programs Access Rights	<p>Control: The use of system utilities that could be capable of bypassing system and application controls shall be restricted and closely monitored.</p> <p>Objective: To ensure that the use of system utilities does not compromise system and application information security controls.</p>	Fully implemented	Access to system utilities is restricted to authorized personnel and requires AD authentication. Activities are logged and administrative rights are centrally managed and recorded. End users do not have administrative privileges.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Control	Objective	Status	Description	Basis			
				Jur.	Cl. dem.	Best pr.	Risk.
8.19 Installation of Software on Operational Systems	Control: Procedures and measures shall be implemented to securely manage the installation of software on operational systems.  Objective: To ensure the integrity of operational systems and to prevent the exploitation of technical vulnerabilities.	Fully implemented	End users do not have administrative rights on their laptops. Software installations are carried out according to documented procedures and through controlled distribution mechanisms. All installations are recorded and monitored.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.20 Networks Security	Control: Networks and network devices shall be secured, managed, and controlled to protect information in systems and applications.  Objective: To protect information in networks and supporting information processing facilities from compromise through the network.	Fully implemented	Availability is supported by redundant infrastructure and high-quality network facilities. Networks are secured and centrally managed.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.21 Security of Network Services	Control: Security mechanisms, service levels, and service requirements for all network services shall be identified, implemented, and monitored.  Objective: To ensure security in the use of network services.	Fully implemented	Network services such as DNS, DHCP, and IPSEC are secured and monitored using monitoring software. Redundancy and 802.1x authentication ensure access and availability. Procedures are documented in the central registration software.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.22 Segregation of Networks	Control: Groups of information services, users, and information systems shall be segmented within the organization's networks.  Objective: To partition the network with security boundaries and control traffic between them based on business requirements.	Fully implemented	The network is segmented into VLANs for different purposes such as corporate, BYOD, and management. Firewalls, encryption, and access rules protect network segments and restrict access.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.23 Web filtering	Control: Access to external websites shall be managed to limit exposure to malicious content.  Objective: To protect systems from being compromised by malware and to prevent access to unauthorized internet resources.	Fully implemented	The organization uses Advanced DNS Protection to effectively mitigate the risks of malicious websites. In addition, our EDR solution intervenes when unwanted behavior (including in the browser) is detected.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Control	Objective	Status	Description	Basis			
				Jur.	Cl.	dem.	Best pr.
8.24 Use of Cryptography	<p>Control: Rules for the effective use of cryptography, including the management of cryptographic keys, shall be defined and implemented.</p> <p>Objective: To ensure the correct and effective use of cryptography in order to protect the confidentiality, authenticity, and integrity of information, in accordance with business and information security requirements, and in compliance with legal, statutory, regulatory, and contractual requirements related to cryptography.</p>	Fully implemented	<p>Encryption is applied to data traffic, storage media, and mobile devices to protect sensitive information.</p> <p>Cryptographic keys are managed via Intune and MBAM, and all connections are secured with SSL/TLS.</p>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.25 Secure Development Life Cycle	<p>Control: Rules for the secure development of software and systems shall be established and applied.</p> <p>Objective: To ensure that information security is designed and implemented within the secure development lifecycle of software and systems.</p>	Fully implemented	<p>Software development takes place in secure environments, with access control through Active Directory and version control in the source code library. Risk assessments and test results are documented in registration software.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.26 Application Security Requirements	<p>Control: Information security requirements shall be identified, specified, and approved when developing or acquiring applications.</p> <p>Objective: To ensure that all information security requirements are identified and incorporated when developing or acquiring applications.</p>	Fully implemented	<p>When external services or software are acquired, a checklist is followed in which information security is central. This includes aspects such as the data storage location, authentication, and authorization.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.27 Secure System Architecture and Engineering Principles Learning From Information Security Incidents	<p>Control: Security principles for system design shall be established, documented, maintained, and applied for all activities related to the development of information systems.</p> <p>Objective: To ensure that information systems are securely designed, implemented, and managed within the development lifecycle.</p>	Fully implemented	<p>Architecture requirements include data protection, encryption, and the use of secure APIs. Open-source software requires a risk assessment, and debug information is removed before production. Backups of test environments follow the same policy as production.</p>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.28 Secure Coding	<p>Control: Secure coding principles shall be applied in software development.</p> <p>Objective: To ensure that software is written securely, thereby reducing the number of potential information security vulnerabilities in the software.</p>	Fully implemented	<p>Ensured through the mandatory application of secure coding principles, training and education supported by tools, code reviews, and security testing.</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Control	Objective	Status	Description	Basis			
				Jur.	Cl. dem.	Best pr.	Risk.
8.29 Security Testing in Development and Acceptance	<p>Control: Security testing processes shall be defined and implemented within the development lifecycle.</p> <p>Objective: To validate that information security requirements are met when applications or code are deployed into the production environment.</p>	Fully implemented	Security tests are mandatory for application changes, including authentication, authorization, and encryption. Impact and risk determine the testing requirements, with a second tester involved for critical changes.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.30 Outsourced Development	<p>Control: The organization shall direct, monitor, and review activities related to outsourced system development.</p> <p>Objective: To ensure that the information security measures required by the organization are implemented in outsourced system development.</p>	Fully implemented	Outsourcing requires a project plan with acceptance criteria, handover steps, and technical documentation. Acceptance is recorded, and additional requirements are reviewed.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.31 Separation of Development, Test and Production Environments	<p>Control: Development, test, and production environments shall be separated and secured.</p> <p>Objective: To protect the production environment and data from compromise due to development and testing activities.</p>	Fully implemented	Critical systems and software implementations are tested in separate test environments. Alternative solutions, such as snapshots, are applied where separate environments are not feasible. Development environments do not contain privacy-sensitive data.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.32 Change Management	<p>Control: Changes to information processing facilities and information systems shall be subject to change management procedures.</p> <p>Objective: To maintain information security during the implementation of changes.</p>	Fully implemented	Changes to systems and processes are carried out on a project basis, documented in registration software, and classified according to impact. Major changes are discussed and reviewed, while minor changes are implemented and recorded directly.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8.33 Test Information	<p>Control: Test data shall be appropriately selected, protected, and managed.</p> <p>Objective: To ensure the relevance of testing and the protection of operational data used for testing.</p>	Fully implemented	Carefully selected test data sets are used for system testing, preferably synthetic and, if necessary, masked.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Control	Objective	Status	Description	Basis			
				Jur.	Cl. dem.	Best pr.	Risk.
8.34 Protection of Information Systems During Audit Testing	<p>Control: Audit tests and other audit activities involving operational systems shall be planned and agreed upon between the tester and the responsible management.</p> <p>Objective: To minimize the impact of audit tests and other audit activities on operational systems and business processes.</p>	Fully implemented	Auditors do not have direct access to systems. Data for audits, such as license and account information, is collected manually and provided after verification.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>