Control A.X	Control A.X.X	Control A.X.X.X	Applicability	Reason for including or excluding in/from scope	Implementation status
A.05 Information Security Policies	A.05.1 Management direction for information security	**A.05.1.1 Policies for information security**	yes	Declaring information security objectives, formulating processes, procedures and requirements for related tasks, ensuring that security is maintained	implemented
A.05 Information Security Policies	A.05.1 Management direction for information security	**A.05.1.2 Review of the policies for information security**	yes	Declaring information security objectives, formulating processes, procedures and requirements for related tasks, ensuring that security is maintained	implemented
A.06 Organisation of information security	A.06.1 Internal Organisation	**A.06.1.1 Information security roles and responsibilities**	yes	base requirements to operate the management system and to have responsible persons	implemented
A.06 Organisation of information security	A.06.1 Internal Organisation	**A.06.1.2 Segregation of duties**	yes	risk reduction with regard to the operational and other security tasks	implemented
A.06 Organisation of information security	A.06.1 Internal Organisation	**A.06.1.3 Contact with authorities**	yes	legal requirements in certain cases and requirements of authorities	implemented
A.06 Organisation of information security	A.06.1 Internal Organisation	**A.06.1.4 Contact with special interest groups**	yes	needs required by stakeholders, partners, clients etc	implemented
A.06 Organisation of information security	A.06.1 Internal Organisation	**A.06.1.5 Information security in project management**	yes	risk possibility: when serving business purposes, information security considerations may be	implemented
A.06 Organisation of information security	A.06.2 Mobile devices and teleworking	**A.06.2.1 Mobile device policy**	yes	risk reduction connected to mobile and remote working (home office) information security protection of business	implemented
A.06 Organisation of information security	A.06.2 Mobile devices and teleworking	**A.06.2.2 Teleworking**	yes	risk reduction connected to mobile and remote working (home office) information security protection of business	implemented
A.07 Human resources security	A.07.1 Prior to employment	**A.07.1.1 Screening**	yes	One critical element of the risks associated with information systems is the reliability of the persons	implemented
A.07 Human resources security	A.07.1 Prior to employment	**A.07.1.2 Terms and conditions of employment**	yes	One of the critical elements of the risks related to information systems is the reliability of the persons accessing the systems, their knowledge of their	implemented
A.07 Human resources security	A.07.2 During employment	**A.07.2.1 Management responsibilities**	yes	Without proper management attention and commitment, and without spending resources, the security of information and systems can be	implemented
A.07 Human resources security	A.07.2 During employment	**A.07.2.2 Information security awareness, education and training**	yes	The organization must pay special attention to the security training and awareness of its employees.	implemented

A.07 Human resources security	A.07.2 During employment	**A.07.2.3 Disciplinary process**	yes	There is a risk of violating confidentiality rules connected to business goals that need to be	implemented
A.07 Human resources security	A.07.3 Termination and change of employment	**A.07.3.1 Termination or change of employment responsibilities**	yes	One of the critical elements of the risks related to information systems is the reliability of the persons accessing the systems, their knowledge of their	implemented
A.08 Asset management	A.08.1 Responsibility for assets	**A.08.1.1 Inventory of assets**	yes	The organization manages security-critical tangible and intangible assets. The inventory is one of the starting points for risk management.	implemented
A.08 Asset management	A.08.1 Responsibility for assets	**A.08.1.2 Ownership of assets**	yes	Every device, information, information system element or system has to be an owner.	implemented
A.08 Asset management	A.08.1 Responsibility for assets	**A.08.1.3 Acceptable use of assets**	yes	There are tangible and informational assets that require proper user behaviour to access in order to maintain confidentiality, integrity, and availability.	implemented
A.08 Asset management	A.08.1 Responsibility for assets	**A.08.1.4 Return of assets**	yes	The organization manages security-critical tangible and intangible assets. The inventory is one of the starting points for risk management. It must be	implemented
A.08 Asset management	A.08.2 Information classification	**A.08.2.1 Classification of information**	yes	A distinction can be made between the C-I-A categories, different risks can be assumed and assigned to different information and tangible	implemented
A.08 Asset management	A.08.2 Information classification	**A.08.2.2 Labelling of information**	no	Reason for exclusion that it is only planned, not implemented yet.	planned
A.08 Asset management	A.08.2 Information classification	**A.08.2.3 Handling of assets**	yes	Risks must be reduced for business purposes, for example, projects and business, development information should not be disclosed.	implemented
A.08 Asset management	A.08.3 Media handling	**A.08.3.1 Management of removable media**	yes	Risks must be reduced for business purposes, for example, projects and business, development information should not be disclosed.	implemented
A.08 Asset management	A.08.3 Media handling	**A.08.3.2 Disposal of media**	yes	Data left on media may be information security risk, thus it must be handled by disposal rules.	implemented
A.08 Asset management	A.08.3 Media handling	**A.08.3.3 Physical media transfer**	yes	Data on media may be disclosed, deleted or modified if not handled properly during media	implemented
A.09 Access control	A.09.1 Business requirements for access control	**A.09.1.1 Access control policy**	yes	There is a need for access control in the organization processes to implement the need-to-know principle.	implemented
A.09 Access control	A.09.1 Business requirements for access control	**A.09.1.2 Access to networks and network services**	yes	Access control principles must be implemented with regard to different technology aspects (e.g. network operation).	implemented

A.09 Access control	A.09.2 User access management	**A.09.2.1 User registration and de-registration**	yes	access rules by job and role can only be interpreted for registered users	implemented
A.09 Access control	A.09.2 User access management	**A.09.2.2 User access provisioning**	yes	Access should not be set up on an ad-hoc basis	implemented
A.09 Access control	A.09.2 User access management	**A.09.2.3 Management of privileged access rights**	yes	privileged access is managed in a controlled manner	implemented
A.09 Access control	A.09.2 User access management	**A.09.2.4 Management of secret authentication information of users**	yes	Passwords are sensitive parameters that are at risk of being compromised by the entities it protects.	implemented
A.09 Access control	A.09.2 User access management	**A.09.2.5 Review of user access rights**	yes	not to have an access setting status that reflects a obsolete state	implemented
A.09 Access control	A.09.2 User access management	**A.09.2.6 Removal or adjustment of access rights**	yes	not to have an access setting status that reflects a obsolete state	implemented
A.09 Access control	A.09.3 User responsibilities	**A.09.3.1 Use of secret authentication information**	yes	Passwords are sensitive parameters that must be handled securely.	implemented
A.09 Access control	A.09.4 System and application access control	**A.09.4.1 Information access restriction**	yes	Access control rules include access to system functions and information.	implemented
A.09 Access control	A.09.4 System and application access control	**A.09.4.2 Secure log-on procedures**	yes	reducing the risks of network logon risks for network access	implemented
A.09 Access control	A.09.4 System and application access control	**A.09.4.3 Password management system**	yes	Passwords are sensitive parameters that must be handled securely.	implemented
A.09 Access control	A.09.4 System and application access control	**A.09.4.4 Use of privileged utility programs**	yes	Privileged programs present an increased or new risk of improper application.	implemented
A.09 Access control	A.09.4 System and application access control	**A.09.4.4 Use of privileged utility programs**	yes	Privileged programs present an increased or new risk of improper application.	implemented
A.09 Access control	A.09.4 System and application access control	**A.09.4.5 Access control to program source code**	yes	source codes present an increased or new risk if improperly handled	implemented
A.10 Cryptography	A.10.1 Cryptographic controls	**A.10.1.1 Policy on the use of cryptographic controls**	yes	open access or storing data in open from would be a high risk	implemented
A.10 Cryptography	A.10.1 Cryptographic controls	**A.10.1.2 Key management**	yes	open access or storing data in open from would be a high risk	implemented
A.11 Physical and environmental security	A.11.1 Secure areas	**A.11.1.1 Physical security perimeter**	yes	risk of malicious physical access	implemented
A.11 Physical and environmental security	A.11.1 Secure areas	**A.11.1.2 Physical entry controls**	yes	risk of malicious physical access	implemented
A.11 Physical and environmental security	A.11.1 Secure areas	**A.11.1.3 Securing offices, rooms and facilities**	yes	risk of malicious physical access	implemented

A.11 Physical and environmental security	A.11.1 Secure areas	**A.11.1.4 Protecting against external and environmental threats**	yes	Proportionate protection for business purposes.	implemented
A.11 Physical and environmental security	A.11.1 Secure areas	**A.11.1.4 Protecting against external and environmental threats**	yes	Proportionate protection for business purposes.	implemented
A.11 Physical and environmental security	A.11.1 Secure areas	**A.11.1.5 Working in secure areas**	yes	Proportionate protection for business purposes.	implemented
A.11 Physical and environmental security	A.11.1 Secure areas	**A.11.1.6 Delivery and loading areas**	yes	Proportionate protection for business purposes.	implemented
A.11 Physical and environmental security	A.11.2 Equipment	**A.11.2.1 Equipment siting and protection**	yes	Proportionate protection for business purposes.	implemented
A.11 Physical and environmental security	A.11.2 Equipment	**A.11.2.2 Supporting utilities**	yes	Proportionate protection for business purposes.	implemented
A.11 Physical and environmental security	A.11.2 Equipment	**A.11.2.3 Cabling security**	yes	Proportionate protection for business purposes.	implemented
A.11 Physical and environmental security	A.11.2 Equipment	**A.11.2.4 Equipment maintenance**	yes	Equipment failure risk is an ongoing risk	implemented
A.11 Physical and environmental security	A.11.2 Equipment	**A.11.2.5 Removal of assets**	yes	Removal of assets must be done only with authorization	implemented
A.11 Physical and environmental security	A.11.2 Equipment	**A.11.2.6 Security of equipment and assets off-premises**	yes	reduction of risks regarding company values in off-premises cases	implemented
A.11 Physical and environmental security	A.11.2 Equipment	**A.11.2.7 Secure disposal or reuse of equipment**	yes	risks are to be managed due in different asset life-cycle stages	implemented
A.11 Physical and environmental security	A.11.2 Equipment	**A.11.2.8 Unattended user equipment**	yes	An unattended item of property can be attacked physically and logically.	implemented
A.11 Physical and environmental security	A.11.2 Equipment	**A.11.2.9 Clear desk and clear screen policy**	yes	Existence of risk of accidentally omitted papers or screens read by unauthorized persons.	implemented
A.12 Operations security	A.12.1 Operational procedures and responsibilities	**A.12.1.1 Documented operating procedures**	yes	Occurrence of operating and use errors due to ignorance	implemented
A.12 Operations security	A.12.1 Operational procedures and responsibilities	**A.12.1.2 Change management**	yes	Unmanaged changes to the system can compromise system security.	implemented

A.12 Operations security	A.12.1 Operational procedures and responsibilities	**A.12.1.3 Capacity management**	yes	Achieving business goals can be compromised by a lack of resources.	implemented
A.12 Operations security	A.12.1 Operational procedures and responsibilities	**A.12.1.4 Separation of development, testing and operational environments**	yes	Risks must be managed connected to different development phases.	implemented
A.12 Operations security	A.12.2 Protection from malware	**A.12.2.1 Controls against malware**	yes	The real risk of malicious code entering the system	implemented
A.12 Operations security	A.12.3 Backup	**A.12.3.1 Information backup**	yes	Installing systems from scratch in the event of a complete system loss or data loss could delay work, or the loss of data from previous projects would be	implemented
A.12 Operations security	A.12.4 Logging and monitoring	**A.12.4.1 Event logging**	yes	In case of extraordinary events, safe suspicious circumstances, no information would be available to	implemented
A.12 Operations security	A.12.4 Logging and monitoring	**A.12.4.2 Protection of log information**	yes	In case of extraordinary events, safe suspicious circumstances, no authentic information would be	implemented
A.12 Operations security	A.12.4 Logging and monitoring	**A.12.4.3 Administrator and operator logs**	yes	Administrators must be monitored in some way.	implemented
A.12 Operations security	A.12.4 Logging and monitoring	**A.12.4.4 Clock synchronisation**	yes	The time data in the logs shows real values.	implemented
A.12 Operations security	A.12.5 Control of operational software	**A.12.5.1 Installation of software on operational systems**	yes	installations can cause unwanted effects without proper preparation	implemented
A.12 Operations security	A.12.6 Technical vulnerability management	**A.12.6.1 Management of technical vulnerabilities**	yes	need for up-to-date information on vulnerabilities in information systems	implemented
A.12 Operations security	A.12.6 Technical vulnerability management	**A.12.6.2 Restrictions on software installation**	yes	Unrestricted software installation by users can lead to the appearance of programs that hide	implemented
A.12 Operations security	A.12.7 Information systems audit considerations	**A.12.7.1 Information systems audit controls**	yes	Audits have to be planned, managed and achieved.	implemented
A.13 Communications security	A.13.1 Network security management	**A.13.1.1 Network controls**	yes	The availability of information systems over a network threatens the security of the systems and	implemented
A.13 Communications security	A.13.1 Network security management	**A.13.1.2 Security of network services**	yes	weakness, or failure of network security services can compromise the confidentiality, integrity, or availability of systems and information.	implemented
A.13 Communications security	A.13.1 Network security management	**A.13.1.3 Segregation in networks**	yes	Risk of mixing different data/function/system categories has to be handled	implemented

A.13 Communications security	A.13.2 Information transfer	**A.13.2.1 Information transfer policies and procedures**	yes	In different processing states of information, especially during transmission, the risk of damaging confidentiality and integrity may increase.	implemented
A.13 Communications security	A.13.2 Information transfer	**A.13.2.2 Agreements on information transfer**	yes	The use of services and the purchase of products whose IT security aspects of the service providers and manufacturers satisfy the organisation's confidentiality, availability and integrity security	implemented
A.13 Communications security	A.13.2 Information transfer	**A.13.2.3 Electronic messaging**	yes	When using electronic messaging mechanisms, information is subject to risks of loss of	implemented
A.13 Communications security	A.13.2 Information transfer	**A.13.2.4 Confidentiality or nondisclosure agreements**	yes	There is a potential risk for leakage of confidential business information where business partners are in	implemented
A.14 System acquisition, development and maintenance	A.14.1 Security requirements of information systems	**A.14.1.1 Information security requirements analysis and specification**	yes	During the introduction and operation of a new developed or purchased system, security deficiencies and weaknesses are revealed, due to which the existing IT security rules of the organization are	implemented
A.14 System acquisition, development and maintenance	A.14.1 Security requirements of information systems	**A.14.1.2 Securing application services on public networks**	yes	In different processing states of information, especially during transmission, the risk of damaging confidentiality and integrity may increase.	implemented
A.14 System acquisition, development and maintenance	A.14.1 Security requirements of information systems	**A.14.1.3 Protecting application services transactions**	no	Organizational processes do not include application transactions referenced in the measure.	n/a
A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	**A.14.2.1 Secure development policy**	yes	Risks of application security vulnerabilities and development process security	implemented
A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	**A.14.2.2 System change control procedures**	yes	Risks of application security vulnerabilities and development process security	implemented
A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	**A.14.2.3 Technical review of applications after operating platform changes**	yes	Changing the operating mode of security-critical applications in a negative way or losing compatibility in the event of a platform change.	implemented
A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	**A.14.2.4 Restrictions on changes to software packages**	yes	Do not modify, update, or compromise the integrity of legitimate software obtained from reputable manufacturers.	implemented
A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	**A.14.2.5 Secure system engineering principles**	yes	Lack of knowledge of secure system design principles poses a risk to individual developments and the development of customers' systems and products.	implemented

A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	**A.14.2.6 Secure development environment**	yes	Development environment may be exposed to risks from different aspects, it must be handled.	implemented
A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	**A.14.2.7 Outsourced development**	yes	Risks associated with an application, product, component developed by an external resource	implemented
A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	**A.14.2.8 System security testing**	yes	Risks associated with testing during the different system development cycles	implemented
A.14 System acquisition, development and maintenance	A.14.2 Security in development and support processes	**A.14.2.9 System acceptance testing**	yes	Risks associated with testing during the different system development cycles	implemented
A.14 System acquisition, development and maintenance	A.14.3 Test data	**A.14.3.1 Protection of test data**	yes	Risks associated with testing during the different system development cycles	implemented
A.15 Supplier relationships	A.15.1 Information security in supplier relationships	**A.15.1.1 Information security policy for supplier relationships**	yes	The possibility of compromising the security of information and systems when working with business partners.	implemented
A.15 Supplier relationships	A.15.1 Information security in supplier relationships	**A.15.1.2 Addressing security within supplier agreements**	yes	The possibility of compromising the security of information and systems when working with	implemented
A.15 Supplier relationships	A.15.1 Information security in supplier relationships	**A.15.1.3 Information and communication technology supply chain**	yes	The use of services and the purchase of products whose IT security aspects of service providers and manufacturers satisfy the organisation's confidentiality, availability and integrity security	implemented
A.15 Supplier relationships	A.15.2 Supplier service delivery management	**A.15.2.1 Monitoring and review of supplier services**	yes	The possibility of compromising the security of information and systems when working with	implemented
A.15 Supplier relationships	A.15.2 Supplier service delivery management	**A.15.2.2 Managing changes to supplier services**	yes	The possibility of compromising the security of information and systems when working with	implemented
A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	**A.16.1.1 Responsibilities and procedures**	yes	Risk: there is no designated responsible person (notifier, investigator, decision maker) in the event of a security incident	implemented
A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	**A.16.1.2 Reporting information security events**	yes	Risk: a security incident that compromises the acceptable level of security features of information and / or systems is not detected in a timely manner.	implemented
A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	**A.16.1.3 Reporting information security weaknesses**	yes	Risk: a security vulnerability that compromises the acceptable level of security features of information and / or systems is not detected in a timely manner.	implemented

A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	**A.16.1.4 Assessment of and decision on information security events**	yes	Risk: an security incident that compromises the acceptable security features of information and / or systems is not handled properly.	implemented
A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	**A.16.1.5 Response to information security incidents**	yes	Risk: an security incident that compromises the acceptable security features of information and / or systems is not handled properly.	implemented
A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	**A.16.1.6 Learning from information security incidents**	yes	A security incident that has occurred in the past and can be traced back to similar causes that compromises the acceptable security features of the	implemented
A.16 Information security incident management	A.16.1 Management of information security incidents and improvements	**A.16.1.7 Collection of evidence**	yes	There is little or no data available to investigate a security incident.	implemented
A.17 Information security aspects of business continuity management	A.17.1 Information security continuity	**A.17.1.1 Planning information security continuity**	yes	Deploying systems from scratch in the event of a complete loss of functionality or data loss could delay work, or the loss of data from previous projects would be unacceptable from security and	implemented
A.17 Information security aspects of business continuity management	A.17.1 Information security continuity	**A.17.1.2 Implementing information security continuity**	yes	Deploying systems from scratch in the event of a complete loss of functionality or data loss could delay work, or the loss of data from previous projects would be unacceptable from security and	implemented
A.17 Information security aspects of business continuity management	A.17.1 Information security continuity	**A.17.1.3 Verify, review and evaluate information security continuity**	yes	Deploying systems from scratch in the event of a complete loss of functionality or data loss could delay work, or the loss of data from previous projects would be unacceptable from security and	implemented
A.17 Information security aspects of business continuity management	A.17.2 Redundancies	**A.17.2.1 Availability of information processing facilities**	yes	Deploying systems from scratch in the event of a complete loss of functionality or data loss could delay work, or the loss of data from previous projects would be unacceptable from security and	implemented
A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	**A.18.1.1 Identification of applicable legislation and contractual requirements**	yes	Complying with law and regulations	implemented
A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	**A.18.1.2 Intellectual property rights**	yes	Complying with law and regulations	implemented
A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	**A.18.1.3 Protection of records**	yes	Complying with law and regulations	implemented

A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	**A.18.1.4 Privacy and protection of personally identifiable information**	yes	Complying with law and regulations	implemented
A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	**A.18.1.5 Regulation of cryptographic controls**	yes	Complying with law and regulations	implemented
A.18 Compliance	A.18.1 Compliance with legal and contractual requirements	**A.18.2.1 Independent review of information security**	yes	Complying with law and regulations	implemented
A.18 Compliance	A.18.2 Information security reviews	**A.18.2.2 Compliance with security policies and standards**	yes	Ensuring compliance with standards, good practices, legislation	implemented
A.18 Compliance	A.18.2 Information security reviews	**A.18.2.3 Technical compliance review**	yes	Ensuring compliance with standards, good practices, legislation	implemented