Clause	Title	Type	Description	Applicable	Implemented	Reason inclusion	Comment
A.5	Information security policies	Section					
A.5.1	Management direction for information security	Objective	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.				
A.5.1.1	Policies for information security	Control	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	Yes	Yes	Best Practices / Business Requirements	
A.5.1.2	Review of the policies for information security	Control	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Yes	Yes	Best Practices / Business Requirements	
A.6	Organization of information security	Section					
A.6.1	Internal organization	Objective	To establish a management framework to initiate and control the implementation and operation of information security within the organization.				
A.6.1.1	Information security roles and responsibilities	Control	All information security responsibilities shall be defined and allocated.	Yes	Yes	Best Practices / Business Requirements	
A.6.1.2	Segregation of duties	Control	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	Yes	Yes	Best Practices / Business Requirements	
A.6.1.3	Contact with authorities	Control	Appropriate contacts with relevant authorities shall be maintained.	Yes	Yes	Laws and regulations	
A.6.1.4	Contact with special interest groups	Control	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	Yes	Yes	Best Practices / Business Requirements	
A.6.1.5	Information security in project management	Control	Information security shall be addressed in project management, regardless of the type of the project.	Yes	Yes	Best Practices / Business Requirements	
A.6.2	Mobile devices and teleworking	Objective	To ensure the security of teleworking and use of mobile devices.				
A.6.2.1	Mobile device policy	Control	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	Yes	Yes	Contractual agreements	
A.6.2.2	Teleworking	Control	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	Yes	Yes	Contractual agreements	
A.7	Human resource security	Section					
A.7.1	Prior to employment	Objective	To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.				
A.7.1.1	Screening	Control	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Yes	Yes	Contractual agreements	
A.7.1.2	Terms and conditions of employment	Control	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	Yes	Yes	Contractual agreements	
A.7.2	During employment	Objective	To ensure that employees and contractors are aware of and fulfil their information security responsibilities.				
A.7.2.1	Management responsibilities	Control	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	Yes	Yes	Best Practices / Business Requirements	
A.7.2.2	Information security awareness, education and training	Control	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	Yes	Yes	Best Practices / Business Requirements	
A.7.2.3	Disciplinary process	Control	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	Yes	Yes	Best Practices / Business Requirements	

Clause	Title	Type	Description	Applicable	Implemented	Reason inclusion	Comment
A.7.3	Termination and change of employment	Objective	To protect the organization's interests as part of the process of changing or terminating employment.				
A.7.3.1	Termination and change of employment responsibilities	Control	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	Yes	Yes	Contractual agreements	
A.8	**Asset management**	**Section**					
A.8.1	Responsibility for assets	Objective	To identify organizational assets and define appropriate protection responsibilities.				
A.8.1.1	Inventory of assets	Control	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	Yes	Yes	Best Practices / Business Requirements	
A.8.1.2	Ownership of assets	Control	Assets maintained in the inventory shall be owned.	Yes	Yes	Best Practices / Business Requirements	
A.8.1.3	Acceptable use of assets	Control	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	Yes	Yes	Best Practices / Business Requirements	
A.8.1.4	Return of assets	Control	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	Yes	Yes	Best Practices / Business Requirements	
A.8.2	Information classification	Objective	To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.				
A.8.2.1	Classification of information	Control	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	Yes	Yes	Best Practices / Business Requirements	
A.8.2.2	Labelling of information	Control	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes	Yes	Best Practices / Business Requirements	
A.8.2.3	Handling of assets	Control	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes	Yes	Best Practices / Business Requirements	
A.8.3	Media handling	Objective	To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.				
A.8.3.1	Management of removable media	Control	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	Yes	Yes	Risk Assessment	
A.8.3.2	Disposal of media	Control	Media shall be disposed of securely when no longer required, using formal procedures.	Yes	Yes	Best Practices / Business Requirements	
A.8.3.3	Physical media transfer	Control	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	Yes	Yes	Best Practices / Business Requirements	
A.9	**Access control**	**Section**					
A.9.1	Business requirements of access control	Objective	To limit access to information and information processing facilities.				
A.9.1.1	Access control policy	Control	An access control policy shall be established, documented and reviewed based on business and information security requirements.	Yes	Yes	Best Practices / Business Requirements	
A.9.1.2	Access to networks and network services	Control	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	Yes	Yes	Best Practices / Business Requirements	
A.9.2	User access management	Objective	To ensure authorized user access and to prevent unauthorized access to systems and services.				
A.9.2.1	User registration and de-registration	Control	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	Yes	Yes	Best Practices / Business Requirements	
A.9.2.2	User access provisioning	Control	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	Yes	Yes	Best Practices / Business Requirements	
A.9.2.3	Management of privileged access rights	Control	The allocation and use of privileged access rights shall be restricted and controlled.	Yes	Yes	Best Practices / Business Requirements	
A.9.2.4	Management of secret authentication information of users	Control	The allocation of secret authentication information shall be controlled through a formal management process.	Yes	Yes	Best Practices / Business Requirements	
A.9.2.5	Review of user access rights	Control	Asset owners shall review users' access rights at regular intervals.	Yes	Yes	Best Practices / Business Requirements	
A.9.2.6	Removal or adjustment of access rights	Control	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Yes	Yes	Best Practices / Business Requirements	

Clause	Title	Type	Description	Applicable	Implemented	Reason inclusion	Comment
A.9.3	User responsibilities	Objective	To make users accountable for safeguarding their authentication information.				
A.9.3.1	Use of secret authentication information	Control	Users shall be required to follow the organization's practices in the use of secret authentication information.	Yes	Yes	Best Practices / Business Requirements	
A.9.4	System and application access control	Objective	To prevent unauthorized access to systems and applications.				
A.9.4.1	Information access restriction	Control	Access to information and application system functions shall be restricted in accordance with the access control policy.	Yes	Yes	Best Practices / Business Requirements	
A.9.4.2	Secure log-on procedures	Control	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	Yes	Yes	Best Practices / Business Requirements	
A.9.4.3	Password management system	Control	Password management systems shall be interactive and shall ensure quality passwords.	Yes	Yes	Best Practices / Business Requirements	
A.9.4.4	Use of privileged utility programs	Control	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	Yes	Yes	Best Practices / Business Requirements	
A.9.4.5	Access control to program source code	Control	Access to program source code shall be restricted.	Yes	Yes	Best Practices / Business Requirements	
A.10	Cryptography	Section					
A.10.1	Cryptographic controls	Objective	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.				
A.10.1.1	Policy on the use of cryptographic controls	Control	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	Yes	Yes	Best Practices / Business Requirements	
A.10.1.2	Key management	Control	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	Yes	Yes	Best Practices / Business Requirements	
A.11	Physical and environmental security	Section					
A.11.1	Secure areas	Objective	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.				
A.11.1.1	Physical security perimeter	Control	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Yes	Yes	Best Practices / Business Requirements	
A.11.1.2	Physical entry controls	Control	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Yes	Yes	Best Practices / Business Requirements	
A.11.1.3	Securing offices, rooms and facilities	Control	Physical security for offices, rooms and facilities shall be designed and applied.	Yes	Yes	Best Practices / Business Requirements	
A.11.1.4	Protecting against external and environmental threats	Control	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	Yes	Yes	Best Practices / Business Requirements	
A.11.1.5	Working in secure areas	Control	Procedures for working in secure areas shall be designed and applied.	No	No		AIMMS staff do not work in datacenters. All actions are performed via remote access.
A.11.1.6	Delivery and loading areas	Control	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	No	No		AIMMS does not use or sell any heavy equipment and therefore a delivery and loading area is not needed.
A.11.2	Equipment	Objective	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.				
A.11.2.1	Equipment siting and protection	Control	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Yes	Yes	Best Practices / Business Requirements	
A.11.2.2	Supporting utilities	Control	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes	Yes	Best Practices / Business Requirements	
A.11.2.3	Cabling security	Control	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	Yes	Yes	Best Practices / Business Requirements	
A.11.2.4	Equipment maintenance	Control	Equipment shall be correctly maintained to ensure its continued availability and integrity.	Yes	Yes	Best Practices / Business Requirements	
A.11.2.5	Removal of assets	Control	Equipment, information or software shall not be taken off-site without prior authorization.	Yes	Yes	Best Practices / Business Requirements	
A.11.2.6	Security of equipment and assets off-premises	Control	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	Yes	Yes	Best Practices / Business Requirements	

Clause	Title	Type	Description	Applicable	Implemented	Reason inclusion	Comment
A.11.2.7	Secure disposal or reuse of equipment	Control	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Yes	Yes	Best Practices / Business Requirements	
A.11.2.8	Unattended user equipment	Control	Users shall ensure that unattended equipment has appropriate protection.	Yes	Yes	Best Practices / Business Requirements	
A.11.2.9	Clear desk and clear screen policy	Control	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	Yes	Yes	Best Practices / Business Requirements	
A.12	**Operations security**	**Section**					
A.12.1	Operational procedures and responsibilities	Objective	To ensure correct and secure operations of information processing facilities.				
A.12.1.1	Documented operating procedures	Control	Operating procedures shall be documented and made available to all users who need them.	Yes	Yes	Best Practices / Business Requirements	
A.12.1.2	Change management	Control	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	Yes	Yes	Best Practices / Business Requirements	
A.12.1.3	Capacity management	Control	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Yes	Yes	Best Practices / Business Requirements	
A.12.1.4	Separation of development, testing and operational environments	Control	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	Yes	Yes	Best Practices / Business Requirements	
A.12.2	Protection from malware	Objective	To ensure that information and information processing facilities are protected against malware.				
A.12.2.1	Controls against malware	Control	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Yes	Yes	Best Practices / Business Requirements	
A.12.3	Backup	Objective	To protect against loss of data.				
A.12.3.1	Information backup	Control	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Yes	Yes	Best Practices / Business Requirements	
A.12.4	Logging and monitoring	Objective	To record events and generate evidence.				
A.12.4.1	Event logging	Control	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	Yes	Yes	Best Practices / Business Requirements	
A.12.4.2	Protection of log information	Control	Logging facilities and log information shall be protected against tampering and unauthorized access.	Yes	Yes	Best Practices / Business Requirements	
A.12.4.3	Administrator and operator logs	Control	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	Yes	Yes	Best Practices / Business Requirements	
A.12.4.4	Clock synchronisation	Control	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	Yes	Yes	Best Practices / Business Requirements	
A.12.5	Control of operational software	Objective	To ensure the integrity of operational systems.				
A.12.5.1	Installation of software on operational systems	Control	Procedures shall be implemented to control the installation of software on operational systems.	Yes	Yes	Best Practices / Business Requirements	
A.12.6	Technical vulnerability management	Objective	To prevent exploitation of technical vulnerabilities.				
A.12.6.1	Management of technical vulnerabilities	Control	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	Yes	Yes	Best Practices / Business Requirements	
A.12.6.2	Restrictions on software installation	Control	Rules governing the installation of software by users shall be established and implemented.	Yes	Yes	Contractual agreements	
A.12.7	Information systems audit considerations	Objective	To minimise the impact of audit activities on operational systems.				
A.12.7.1	Information systems audit controls	Control	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	Yes	Yes	Best Practices / Business Requirements	
A.13	**Communications security**	**Section**					
A.13.1	Network security management	Objective	To ensure the protection of information in networks and its supporting information processing facilities.				
A.13.1.1	Network controls	Control	Networks shall be managed and controlled to protect information in systems and applications.	Yes	Yes	Best Practices / Business Requirements	

Clause	Title	Type	Description	Applicable	Implemented	Reason inclusion	Comment
A.13.1.2	Security of network services	Control	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Yes	Yes	Best Practices / Business Requirements	
A.13.1.3	Segregation in networks	Control	Groups of information services, users and information systems shall be segregated on networks.	Yes	Yes	Best Practices / Business Requirements	
A.13.2	Information transfer	Objective	To maintain the security of information transferred within an organization and with any external entity.				
A.13.2.1	Information transfer policies and procedures	Control	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	Yes	Yes	Best Practices / Business Requirements	
A.13.2.2	Agreements on information transfer	Control	Agreements shall address the secure transfer of business information between the organization and external parties.	Yes	Yes	Best Practices / Business Requirements	
A.13.2.3	Electronic messaging	Control	Information involved in electronic messaging shall be appropriately protected.	Yes	Yes	Best Practices / Business Requirements	
A.13.2.4	Confidentiality or nondisclosure agreements	Control	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	Yes	Yes	Best Practices / Business Requirements	
A.14	**System acquisition, development and maintenance**	**Section**					
A.14.1	Security requirements of information systems	Objective	To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.				
A.14.1.1	Information security requirements analysis and specification	Control	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	Yes	Yes	Best Practices / Business Requirements	
A.14.1.2	Securing application services on public networks	Control	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	Yes	Yes	Best Practices / Business Requirements	
A.14.1.3	Protecting application services transactions	Control	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	Yes	Yes	Best Practices / Business Requirements	
A.14.2	Security in development and support processes	Objective	To ensure that information security is designed and implemented within the development lifecycle of information systems.				
A.14.2.1	Secure development policy	Control	Rules for the development of software and systems shall be established and applied to developments within the organization.	Yes	Yes	Best Practices / Business Requirements	
A.14.2.2	System change control procedures	Control	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	Yes	Yes	Best Practices / Business Requirements	
A.14.2.3	Technical review of applications after operating platform changes	Control	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	Yes	Yes	Best Practices / Business Requirements	
A.14.2.4	Restrictions on changes to software packages	Control	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	Yes	Yes	Best Practices / Business Requirements	
A.14.2.5	Secure system engineering principles	Control	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	Yes	Yes	Best Practices / Business Requirements	
A.14.2.6	Secure development environment	Control	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	Yes	Yes	Best Practices / Business Requirements	
A.14.2.7	Outsourced development	Control	The organization shall supervise and monitor the activity of outsourced system development.	Yes	Yes	Other	
A.14.2.8	System security testing	Control	Testing of security functionality shall be carried out during development.	Yes	Yes	Best Practices / Business Requirements	
A.14.2.9	System acceptance testing	Control	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	Yes	Yes	Best Practices / Business Requirements	
A.14.3	Test data	Objective	To ensure the protection of data used for testing.				
A.14.3.1	Protection of test data	Control	Test data shall be selected carefully, protected and controlled.	Yes	Yes	Best Practices / Business Requirements	

Clause	Title	Type	Description	Applicable	Implemented	Reason inclusion	Comment
A.15	**Supplier relationships**	**Section**					
A.15.1	Information security in supplier relationships	Objective	To ensure protection of the organization's assets that is accessible by suppliers.				
A.15.1.1	Information security policy for supplier relationships	Control	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	Yes	Yes	Contractual Agreements	
A.15.1.2	Addressing security within supplier agreements	Control	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	Yes	Yes	Contractual Agreements	
A.15.1.3	Information and communication technology supply chain	Control	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	Yes	Yes	Contractual Agreements	
A.15.2	Supplier service delivery management	Objective	To maintain an agreed level of information security and service delivery in line with supplier agreements.				
A.15.2.1	Monitoring and review of supplier services	Control	Organizations shall regularly monitor, review and audit supplier service delivery.	Yes	Yes	Best Practices / Business Requirements	
A.15.2.2	Managing changes to supplier services	Control	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	Yes	Yes	Best Practices / Business Requirements	
A.16	**Information security incident management**	**Section**					
A.16.1	Management of information security incidents and improvements	Objective	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.				
A.16.1.1	Responsibilities and procedures	Control	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	Yes	Yes	Best Practices / Business Requirements	
A.16.1.2	Reporting information security events	Control	Information security events shall be reported through appropriate management channels as quickly as possible.	Yes	Yes	Best Practices / Business Requirements	
A.16.1.3	Reporting information security weaknesses	Control	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	Yes	Yes	Best Practices / Business Requirements	
A.16.1.4	Assessment of and decision on information security events	Control	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	Yes	Yes	Best Practices / Business Requirements	
A.16.1.5	Response to information security incidents	Control	Information security incidents shall be responded to in accordance with the documented procedures.	Yes	Yes	Best Practices / Business Requirements	
A.16.1.6	Learning from information security incidents	Control	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	Yes	Yes	Best Practices / Business Requirements	
A.16.1.7	Collection of evidence	Control	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Yes	Yes	Best Practices / Business Requirements	
A.17	**Information security aspects of business continuity management**	**Section**					
A.17.1	Information security continuity	Objective	Information security continuity shall be embedded in the organization's business continuity management systems.				
A.17.1.1	Planning information security continuity	Control	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Yes	Yes	Best Practices / Business Requirements	
A.17.1.2	Implementing information security continuity	Control	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Yes	Yes	Best Practices / Business Requirements	
A.17.1.3	Verify, review and evaluate information security continuity	Control	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	Yes	Yes	Best Practices / Business Requirements	

Clause	Title	Type	Description	Applicable	Implemented	Reason inclusion	Comment
A.17.2	Redundancies	Objective	To ensure availability of information processing facilities.				
A.17.2.1	Availability of information processing facilities	Control	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Yes	Yes	Best Practices / Business Requirements	
A.18	Compliance	Section					
A.18.1	Compliance with legal and contractual requirements	Objective	To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.				
A.18.1.1	Identification of applicable legislation and contractural requirements	Control	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	Yes	Yes	Best Practices / Business Requirements	
A.18.1.2	Intellectual property rights	Control	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	Yes	Yes	Laws and Regulations	
A.18.1.3	Protection of records	Control	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.	Yes	Yes	Laws and Regulations	
A.18.1.4	Privacy and protection of personally identifiable information	Control	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	Yes	Yes	Laws and Regulations	
A.18.1.5	Regulation of cryptographic controls	Control	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	Yes	Yes	Best Practices / Business Requirements	
A.18.2	Information security reviews	Objective	To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.				
A.18.2.1	Independent review of information security	Control	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	Yes	Yes	Best Practices / Business Requirements	
A.18.2.2	Compliance with security policies and standards	Control	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	Yes	Yes	Best Practices / Business Requirements	
A.18.2.3	Technical compliance review	Control	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	Yes	Yes	Best Practices / Business Requirements	