Statement of applicability ISO 27001:2023 (en) Shipitsmarter.com B.V. April 14, 2024 version 1.0			Applicable	Implemented	Law	Contract	Risk anlysis	Reason for exclusion
A.5	**Organizational Controls**							
A.5.1	**Policies for information security**	Information security policies and subject-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and stakeholders and reviewed at planned intervals and as significant changes occur.	Yes	Yes			X	
A.5.2	**Information security roles and responsibilities**	Roles and responsibilities in information security should be defined and assigned according to the needs of the organization.	Yes	Yes			X	
A.5.3	**Segregation of duties**	Conflicting tasks and conflicting responsibilities must be separated.	Yes	Yes			X	
A.5.4	**Management responsibilities**	Management must require all personnel to practice information security in accordance with the organization's established information security policy, subject-specific policies and procedures.	Yes	Yes			X	
A.5.5	**Contact with authorities**	The organization must establish and maintain contact with the relevant authorities.	Yes	Yes	X		X	
A.5.6	**Contact with special interest groups**	The organization should establish and maintain contacts with special interest groups or other specialized security forums and professional associations.	Yes	Yes	X		X	
A.5.7	**Threat intelligence**	Information related to information security threats must be collected and analyzed to produce threat intelligence.	Yes	Yes			X	
A.5.8	**Information security in project management**	Information security must be integrated into project management.	Yes	Yes			X	
A.5.9	**Inventory of information and other associated assets**	An inventory of information and other related assets, including owners, should be established and maintained.	Yes	Yes			X	
A.5.10	**Acceptable use of information and other associated assets**	Rules for the acceptable use of and procedures for handling information and other related assets must be identified, documented and implemented.	Yes	Yes			X	
A.5.11	**Return of assets**	Personnel and other stakeholders, as appropriate, must return all organizational assets in their possession upon termination of their employment, contract or agreement.	Yes	Yes			X	
A.5.12	**Classification of information**	Information should be classified according to the information security needs of the organization, based on confidentiality, integrity, availability and relevant stakeholder requirements.	Yes	Yes			X	
A.5.13	**Labelling of information**	To label information, an appropriate set of procedures must be developed and implemented in accordance with the information classification scheme established by the organization.	Yes	Yes			X	
A.5.14	**Information transfer**	Information transfer rules, procedures or agreements must be in place for all types of communication facilities within the organization and between the organization and other parties.	Yes	Yes			X	
A.5.15	**Access control**	Rules based on business and information security requirements should be established and implemented to control physical and logical access to information and other related assets.	Yes	Yes			X	
A.5.16	**Identity management**	The entire identity lifecycle must be managed.	Yes	Yes			X	
A.5.17	**Authentication information**	The allocation and management of authentication information should be controlled through a management process that includes advising staff on the appropriate way to handle authentication information.	Yes	Yes			X	
A.5.18	**Access rights**	Access rights to information and other related assets must be provided, reviewed, modified, and removed in accordance with the organization's subject-specific access security policies and rules.	Yes	Yes			X	
A.5.19	**Information security in supplier relationships**	Processes and procedures must be established and implemented to manage information security risks associated with the use of the supplier's products or services.	Yes	Yes			X	
A.5.20	**Addressing information security within supplier agreements**	Relevant information security requirements must be identified and agreed with each supplier based on the type of supplier relationship.	Yes	Yes			X	
A.5.21	**Managing information security in the ICT supply chain**	Processes and procedures should be defined and implemented to manage information security risks associated with the supply chain of ICT products and services.	Yes	Yes			X	
A.5.22	**Monitoring, review and change management of supplier services**	The organization must regularly monitor, assess, evaluate and manage changes to information security practices and supplier services.	Yes	Yes			X	
A.5.23	**Information security for use of cloud services**	Processes for acquiring, using, managing, and terminating cloud services should be established in accordance with the organization's information security requirements.	Yes	Yes			X	
A.5.24	**Information security incident management planning and preparation**	The organization must plan and prepare for managing information security incidents by defining, establishing and communicating processes, roles and responsibilities for managing information security incidents.	Yes	Yes			X	
A.5.25	**Assessment and decision on information security events**	The organization must assess information security events and decide whether they should be categorized as information security incidents.	Yes	Yes			X	
A.5.26	**Response to information security incidents**	Information security incidents must be responded to in accordance with documented procedures.	Yes	Yes			X	
A.5.27	**Learning from information security incidents**	Knowledge gained from information security incidents should be used to strengthen and improve information security.	Yes	Yes			X	
A.5.28	**Collection of evidence**	The organization must establish and implement procedures for identifying, collecting, obtaining and retaining evidence related to information security events.	Yes	Yes			X	

A.5.29	**Information security during disruption**	The organization must plan for ensuring information security at the appropriate level during a disruption.	Yes	Yes			X	
A.5.30	**ICT readiness for business continuity**	ICT readiness must be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Yes	Yes			X	
A.5.31	**Legal, statutory, regulatory and contractual requirements**	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meeting these requirements must be identified, documented and kept up to date.	Yes	Yes	X	X	X	
A.5.32	**Intellectual property rights**	The organization must implement appropriate procedures to protect intellectual property rights.	Yes	Yes	X		X	
A.5.33	**Protection of records**	Records must be protected against loss, destruction, falsification, unauthorized access and unauthorized disclosure.	Yes	Yes	X		X	
A.5.34	**Privacy and protection of PII**	The organization must identify and comply with privacy preservation and personal data protection requirements under applicable laws, regulations and contractual requirements.	Yes	Yes	X		X	
A.5.35	**Independent review of information security**	The organization's approach to information security management and implementation, including people, processes and technologies, should be reviewed independently and at planned intervals or as significant changes occur.	Yes	Yes			X	
A.5.36	**Compliance with policies, rules and standards for information security**	Compliance with the organization's information security policies, subject-specific policies, rules and standards should be assessed regularly.	Yes	Yes		X	X	
A.5.37	**Documented operating procedures**	Operating procedures for information processing facilities should be documented and made available to the personnel who need them.	Yes	Yes			X	
6	**People Controls**							
A.6.1	**Screening**	The background checks of all candidates for employment must be checked prior to joining the organization and repeated at regular intervals thereafter. This should take into account applicable legal, regulatory and ethical considerations and be proportionate to the business requirements, the classification of the information accessed and the risks identified.	Yes	Yes			X	
A.6.2	**Terms and conditions of employment**	Employment contracts should state the responsibilities of staff and the organization with regard to information security.	Yes	Yes			X	
A.6.3	**Information security awareness, education and training**	Organizational personnel and relevant stakeholders should receive appropriate information security awareness, education and training and regular updates on the organization's information security policies, subject-specific policies and procedures, as relevant to their role.	Yes	Yes			X	
A.6.4	**Disciplinary process**	There must be a formal and communicated disciplinary process to take action against staff and other stakeholders who have committed a breach of the information security policy.	Yes	Yes			X	
A.6.5	**Responsibilities after termination or change of employment**	Responsibilities and duties related to information security that survive termination or change of employment must be defined, enforced and communicated to relevant personnel and other stakeholders.	Yes	Yes			X	
A.6.6	**Confidentiality or non-disclosure agreements**	Confidentiality or nondisclosure agreements that reflect the organization's information protection needs should be identified, documented, regularly reviewed and signed by staff and other relevant stakeholders.	Yes	Yes			X	
A.6.7	**Remote working**	When staff are working remotely, security measures should be implemented to protect information accessed, processed or stored outside the organization's building and/or premises.	Yes	Yes			X	
A.6.8	**Information security event reporting**	The organization must provide a mechanism for personnel to report observed or suspected information security events in a timely manner through appropriate channels.	Yes	Yes			X	
7	**Physical Controls**							
A.7.1	**Physical security perimeters**	Areas containing information and other related assets must be protected by defining and using security zones.	Yes	Yes			X	
A.7.2	**Physical entry**	Secure areas must be protected by appropriate access security measures and access points.	Yes	Yes			X	
A.7.3	**Securing offices, rooms and facilities**	Physical security must be designed and implemented for offices, spaces and facilities.	Yes	Yes			X	
A.7.4	**Physical security monitoring**	The building and grounds must be continuously monitored for unauthorized physical access.	Yes	Yes			X	
A.7.5	**Protecting against physical and environmental threats**	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure, must be designed and implemented.	Yes	Yes			X	
A.7.6	**Working in secure areas**	Security measures must be developed and implemented when working in secure areas.	Yes	Yes			X	
A.7.7	**Clear desk and clear screen**	Clear desk rules for paper documents and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.	Yes	Yes			X	
A.7.8	**Equipment siting and protection**	Equipment must be securely located and protected.	Yes	Yes			X	
A.7.9	**Security of assets off-premises**	Assets outside the building and/or grounds must be protected.	Yes	Yes			X	
A.7.10	**Storage media**	Storage media must be managed throughout their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Yes	Yes			X	
A.7.11	**Supporting utilities**	Information processing facilities must be protected from power outages and other disruptions caused by utility disruptions.	Yes	Yes			X	
A.7.12	**Cabling security**	Power cables and cables transmitting data or supporting information services must be protected from interception, interference or damage.	Yes	Yes			X	
A.7.13	**Equipment maintenance**	Equipment must be properly maintained to ensure the availability, integrity and reliability of information.	Yes	Yes			X	

A.7.14	Secure disposal or re-use of equipment	Equipment components containing storage media should be checked to ensure that sensitive data and licensed software have been deleted or securely overwritten before disposal or reuse.	Yes	Yes			X	
8	Technical Controls							
A.8.1	User endpoint devices	Information stored on, processed by, or accessible through user endpoint devices must be protected.	Yes	Yes			X	
A.8.2	Privileged access rights	The assignment and use of special access rights must be restricted and managed.	Yes	Yes			X	
A.8.3	Information access restriction	Access to information and other related assets must be restricted in accordance with established subject-specific access security policies.	Yes	Yes			X	
A.8.4	Access to source code	Read and write access to source code, development tools and software libraries should be appropriately managed.	Yes	Yes			X	
A.8.5	Secure authentication	We need secure authentication technologies and procedures are implemented based on information access restrictions and subject-specific access security policies.	Yes	Yes			X	
A.8.6	Capacity management	The use of resources should be monitored and adjusted according to current and expected capacity requirements.	Yes	Yes			X	
A.8.7	Protection against malware	Protection against malware must be implemented and supported by appropriate user awareness.	Yes	Yes			X	
A.8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be assessed and appropriate measures should be taken.	Yes	Yes			X	
A.8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks must be identified, documented, implemented, monitored and assessed.	Yes	Yes			X	
A.8.10	Information deletion	Information stored in information systems, devices or other storage media should be deleted when it is no longer required.	Yes	Yes			X	
A.8.11	Data masking	Data must be masked in accordance with the organization's subject-specific access security policy and other related subject-specific policies, and business requirements, taking into account applicable law.	Yes	Yes			X	
A.8.12	Data leakage prevention	Measures to prevent data leaks should be applied in systems, networks and other devices on or through which sensitive information is processed, stored or transported.	Yes	Yes	X		X	
A.8.13	Information backup	Backups of information, software and systems should be retained and tested regularly in accordance with the agreed subject-specific backup policy.	Yes	Yes			X	
A.8.14	Redundancy of information processing facilities	Information processing facilities must be implemented with sufficient redundancy to meet availability requirements.	Yes	Yes			X	
A.8.15	Logging	Log files recording activities, exceptions, errors and other relevant events must be produced, stored, protected and analyzed.	Yes	Yes			X	
A.8.16	Monitoring activities	Networks, systems and applications should be monitored for anomalous behavior and appropriate measures should be taken to evaluate potential information security incidents.	Yes	Yes			X	
A.8.17	Clock synchronization	The clocks of information processing systems used by the organization must be synchronized with approved time sources.	Yes	Yes			X	
A.8.18	Use of privileged utility programs	The use of system tools that may be capable of bypassing systems and applications should be limited and closely monitored.	Yes	Yes			X	
A.8.19	Installation of software on operational systems	Procedures and measures should be implemented to safely manage the installation of software on operational systems.	Yes	Yes			X	
A.8.20	Networks security	Networks and network devices must be secured, managed and controlled to protect information in systems and applications.	Yes	Yes			X	
A.8.21	Security of network services	Security mechanisms, service levels and service requirements for all network services must be identified, implemented and monitored.	Yes	Yes			X	
A.8.22	Segregation of networks	Groups of information services, users, and information systems must be segmented into the organization's networks.	Yes	Yes			X	
A.8.23	Web filtering	Access to external websites should be controlled to limit exposure to malicious content.	Yes	Yes			X	
A.8.24	Use of cryptography	Rules for the effective use of cryptography, including the management of cryptographic keys, should be defined and implemented.	Yes	Yes	X		X	
A.8.25	Secure development life cycle	Rules must be established and applied for the safe development of software and systems.	Yes	Yes			X	
A.8.26	Application security requirements	Information security requirements must be identified, specified and approved when developing or purchasing applications.	Yes	Yes			X	
A.8.27	Secure system architecture and engineering principles	Secure systems design principles must be established, documented, maintained, and applied to all information systems development activities.	Yes	Yes			X	
A.8.28	Secure coding	Secure coding principles should be applied to software development.	Yes	Yes			X	
A.8.29	Security testing in development and acceptance	Security testing processes must be defined and implemented in the development cycle.	Yes	Yes			X	
A.8.30	Outsourced development	The organization must direct, monitor and assess the activities associated with outsourced system development.	No	No				
A.8.31	Separation of development, test and production environments	Development, test and production environments must be separated and secured.	Yes	Yes			X	
A.8.32	Change management	Changes to information processing facilities and information systems must be subject to change control procedures.	Yes	Yes			X	
A.8.33	Test information	Test data must be appropriately selected, protected and managed.	Yes	Yes			X	
A.8.34	Protection of information systems during audit testing	Audit testing and other audit activities assessing operational systems should be planned and agreed between the tester and responsible management.	Yes	Yes			X	