ISO/IEC 27001 Statement of Applicability

ISMS-FORM-06-2

SECURITY CLASSIFICATION:	[Public]
LAST UPDATED:	[February 1st 2024]
VERSION:	[2.1]

Terms used
ISMS: ISMS

ISMSs: Requirements

Note: Only those controls that are listed in Annex A of the ISO/IEC 27001:2022 standard are shown here.

AREA/CONTROL	CONTROL DETAILS	CONTROL APPLICABLE	CONTROL IMPLEMENTED	CONTROL REFERENCE	JUSTIFICATION FOR INCLUSION OR EXCLUSION	COMMENTS
A.5 Organizational controls						
A.5.1 Policies for information security	Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Yes	Yes	ISMS-DOC-05-1 Information Security Management System Manual ISMS-DOC-05-4 Information Security Policy	ScanmarQED operates an ISMS.	All controls are defined, approved and publised on ScanmarQED communication channels available to the entire company and reviewed at least once per annum or as a result of significant change; controls are tested and reviewed during audits and management reviews.
A.5.2 Information security roles and responsibilities	Information security roles and responsibilities should be defined and allocated according to the organization needs.	Yes	Yes	ISMS-DOC-05-1 Information Security Management System Manual	ScanmarQED operates an ISMS with roles and responsibilities defined, allocated and documented.	All security-related roles and responsibilities are defined, reviewed and documented. Competences evaluation and training is done in a recurrent manner.
A.5.3 Segregation of duties	Conflicting duties and conflicting areas of responsibility should be segregated.	Yes	Yes	ISMS-DOC-A06-1 Segregation of Duties Worksheet	ScanmarQED size allows for minimal effective segregation of duties.	Segregation is applied to source code, change management, and equipment and user accounts management.
A.5.4 Management responsibilities	Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	Yes	Yes	ISMS-DOC-A07-4 HR Security Policy ISMS-DOC-A07-5 Employee Acceptable Use Manual	ScanmarQED personnel fulfill the requirements of its ISMS.	Management responsibilities include ensuring that ScanmarQED information security-related policies and procedures are always followed by personnel within their supervision.
A.5.5 Contact with authorities	The organization should establish and maintain contact with relevant authorities.	Yes	Yes	ISMS-DOC-A06-2 Authorities and Specialist Group Contacts	ScanmarQED is subject to law enforcement and regulatory.	Authorities and interest groups are identified and contact methods defined.
A.5.6 Contact with special interest groups	The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Yes	Yes		ScanmarQED needs to maintain knowledge and awareness of security threats.	Authorities and interest groups are identified and contact methods defined.
A.5.7 Threat intelligence	Information relating to information security threats should be collected and analysed to produce threat intelligence.	Yes	Yes	ISMS-DOC-A06-2 Authorities and Specialist Group Contacts	ScanmarQED needs to maintain knowledge and awareness of security threats.	ScanmarQED receives curated threat information from various sources that is sufficient to stay informed and take mitigation actions.

AREA/CONTROL	CONTROL DETAILS	CONTROL APPLICABLE	CONTROL IMPLEMENTED	CONTROL REFERENCE	JUSTIFICATION FOR INCLUSION OR EXCLUSION	COMMENTS
A.5.8 Information security in project management	Information security should be integrated into project management.	Yes	Yes	ISMS-DOC-A06-3 Information Security Guidelines for Project Management	ScanmarQED implements project-based activity such as consultancy and software development, involving information security-related matters.	ScanmarQED has implemented appropriate controls and decision stages included in project management methodology to ensure potential security risks or implications are considered and addressed thereafter as required.
A.5.9 Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, should be developed and maintained.	Yes	Yes	ISMS-DOC-A08-1 Information Asset Inventory	ScanmarQED utilizes information requiring inventorying and rules or procedures for appropriate handling.	Asset inventories and associated controls are implemented and regularly reviewed to ensure appropriate protection and ownership are denoted for all such assets.
A.5.10 Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented.	Yes	Yes	ISMS-DOC-A07-5 Employee Acceptable Use Manual ISMS-DOC-A08-4 Asset Handling Procedure	ScanmarQED utilizes information requiring rules and procedures including appropriate handling.	Acceptable use controls and contractual agreements are deployed to ensure agreed rules are in situ and communicated accordingly.
A.5.11 Return of assets	Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	Yes	Yes	ISMS-DOC-A07-4 HR Security Policy	ScanmarQED utilizes assets allocated to personnel that require controls of the return after employment ends.	All assets are required for return upon change or termination of contract.
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 interested party requirements.	Yes	Yes	ISMS-DOC-05-1 Information Security Management System Manual	ScanmarQED utilizes information requiring classification and labelling.	Information assets are classified as per requirements of the policy being defaulted to public if no specific label is stablished.
A.5.13 Labelling of information	An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes	Yes	ISMS-DOC-05-1 Information Security Management System Manual	ScanmarQED utilizes information requiring classification and labelling.	Information assets are classified as per requirements of the policy being defaulted to public if no specific label is stablished.
A.5.14 Information transfer	To maintain the security of information transferred within an organization and with any external interested party.	Yes	Yes	ISMS-DOC-A07-5 Employee Acceptable Use Manual	ScanmarQED transfers information both internally and externally.	ScanmarQED has implemented policies and controls for acceptable and authorized methods to transfer of information.
A.5.15 Access Control	Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.	Yes	Yes	ISMS-DOC-A09-1 Access Control Policy	ScanmarQED operates systems and networks requiring access controls.	All access rights are securely managed, using role-based access controls (RBAC).
A.5.16 Identity Management	The full life cycle of identities should be managed.	Yes	Yes	ISMS-DOC-A09-2 User Access Management Process	ScanmarQED operates systems and networks requiring access controls.	All access rights are securely managed, using role-based access controls (RBAC).

AREA/CONTROL	CONTROL DETAILS	CONTROL APPLICABLE	CONTROL IMPLEMENTED	CONTROL REFERENCE	JUSTIFICATION FOR INCLUSION OR EXCLUSION	COMMENTS
A.5.17 Authentication of information	Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information.	Yes	Yes	ISMS-DOC-A09-1 Access Control Policy ISMS-DOC-A09-2 User Access Management Process ISMS-DOC-A07-5 Employee Acceptable Use Manual	ScanmarQED operates system requiring access controls and management of secret authentication information.	All secret authentication (including password management) is controlled and verified (e.g. two-factor authentication controls, passwords, etc).
A.5.18 Access rights	Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	Yes	Yes	ISMS-DOC-A09-2 User Access Management Process	ScanmarQED operates systems and networks requiring access controls.	All access rights assigned to user IDs are appropriately authorized, maintained, regularly reviewed and appropriately revoked upon termination of duties.
A.5.19 Information security in supplier relationships	Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Yes	Yes	ISMS-DOC-A15-1 Information Security Policy for Supplier Relationships	ScanmarQED and its core business exists in a wider economic environment in which effective relationships with suppliers are critical to its continued success.	ScanmarQED has implemented polices, standards and controls to manage third party supplier access to any secure assets.
A.5.20 Addressing information security within supplier agreements	Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.	Yes	Yes	ISMS-DOC-A15-1 Information Security Policy for Supplier Relationships	ScanmarQED and its core business exists in a wider economic environment in which effective relationships with suppliers are critical to its continued success.	ScanmarQED has implemented and communicated security-related requirements, including those contractual, to its suppliers.
A.5.21 Managing information security in the ICT supply chain	Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Yes	Yes	ISMS-DOC-08-1 Supplier Information Security Evaluation Process	ScanmarQED and its core business exists in a wider economic environment in which effective relationships with suppliers are critical to its continued success.	ScanmarQED has implemented and communicated security-related requirements, including those contractual, to its suppliers.
A.5.22 Monitoring, review and change management of supplier services	The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Yes	Yes	ISMS-DOC-A15-1 Information Security Policy for Supplier Relationships ISMS-DOC-A12-2 Change Management Process	ScanmarQED and its core business exists in a wider economic environment in which effective relationships with suppliers are critical to its continued success.	ScanmarQED has implemented auditing and checking policies & controls for its suppliers.
A.5.23 Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements.	Yes	Yes	ISMS-DOC-A15-1 Information Security Policy for Supplier Relationships	ScanmarQED makes use of cloud computing services in the delivery of its core business systems.	ScanmarQED has implemented a procedure for evaluating and using cloud services suppliers.
A.5.24 Information security incident management planning and preparation	The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	Yes	Yes	ISMS-DOC-A16-2 Information Security Incident Response Procedure	ScanmarQED operates an ISMS.	ScanmarQED has implemented a security incident management policy and associated procedures and responsibilities.

AREA/CONTROL	CONTROL DETAILS	CONTROL APPLICABLE	CONTROL IMPLEMENTED	CONTROL REFERENCE	JUSTIFICATION FOR INCLUSION OR EXCLUSION	COMMENTS
A.5.25 Assessment of and decision on information security events	The organization should assess information security events and decide if they are to be categorized as information security incidents.	Yes	Yes	ISMS-DOC-A16-2 Information Security Incident Response Procedure	ScanmarQED operates an ISMS.	ScanmarQED has implemented a security incident management policy and associated procedures for logging, monitoring, reporting and reviewing incidents.
A.5.26 Response to information security incidents	Information security incidents should be responded to in accordance with the documented procedures.	Yes	Yes	ISMS-DOC-A16-2 Information Security Incident Response Procedure	ScanmarQED operates an ISMS.	ScanmarQED has implemented a security incident management policy and associated procedures for logging, monitoring, reporting and reviewing incidents.
A.5.27 Learning from information security incidents	Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.	Yes	Yes	ISMS-DOC-A16-2 Information Security Incident Response Procedure	ScanmarQED operates an ISMS.	ScanmarQED has implemented a security incident management policy and associated procedures with lessons learned feedback.
A.5.28 Collection of evidence	The organization should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Yes	Yes	ISMS-DOC-A16-2 Information Security Incident Response Procedure	ScanmarQED operates an ISMS.	ScanmarQED has implemented a security incident management policy and associated procedures for logging, monitoring, reporting and reviewing incidents.
A.5.29 Information security during disruption	The organization should plan how to maintain information security at an appropriate level during disruption.	Yes	Yes	ISMS-DOC-A17-2 Business Continuity Plan	ScanmarQED operates business continuity controls.	ScanmarQED has identified key business continuity requirements in context of security-related incidents based on a Business Impact Assessment.
A.5.30 ICT readiness for business continuity	ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Yes	Yes	ISMS-DOC-A16-2 Information Security Incident Response Procedure	ScanmarQED operates business continuity controls.	ScanmarQED has identified key business continuity requirements in context of security-related incidents based on a Business Impact Assessment.
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 meet these requirements should be identified, documented and kept up to date.	Yes	Yes	ISMS-DOC-A18-1 Legal, Regulatory and Contractual Requirements Procedure	ScanmarQED operates an ISMS requiring conformance to legal requirements in all operational territories.	ScanmarQED operates an ISMS in conformance with local regulatory requirements.
A.5.32 Intellectual property rights	The organization should implement appropriate procedures to protect intellectual property rights.	Yes	Yes	ISMS-DOC-A18-3 Compliance and Data Protection Manual	ScanmarQED operates a system requiring conformance with local intellectual property laws.	ScanmarQED operates an ISMS in conformance with local regulatory requirements.
A.5.33 Protection of records	Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Yes	Yes	ISMS-DOC-A07-5 Employee Acceptable Use Manual	ScanmarQED utilizes information in form of records requiring security protection.	ScanmarQED has implemented controls to prevent the loss and unauthorized access to records in accordance with local laws.
A.5.34 Privacy and protection of PII	The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Yes	Yes	ISMS-DOC-A16-2 Information Security Incident Response Procedure	ScanmarQED utilizes information in form of records requiring security protection.	ScanmarQED has implemented controls for the appropriate control of PII in compliance with local laws.

AREA/CONTROL	CONTROL DETAILS	CONTROL APPLICABLE	CONTROL IMPLEMENTED	CONTROL REFERENCE	JUSTIFICATION FOR INCLUSION OR EXCLUSION	COMMENTS
A.5.35 Independent review of information security	The organization’s approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur.	Yes	Yes	ISMS-DOC-05-1 Information Security Management System Manual	ScanmarQED operates an ISMS requiring independent review.	ScanmarQED operates internal and external auditing processes.
A.5.36 Compliance with policies, rules and standards for information security	Compliance with the organization’s information security policy, topic-specific policies, rules and standards should be regularly reviewed.	Yes	Yes	ISMS-DOC-A18-3 Compliance and Data Protection Manual	ScanmarQED operates an ISMS requiring appropriate compliance with the requirement of the systems.	ScanmarQED operates an ISMS in conformance with local regulatory requirements.
A.5.37 Documented operating procedures	Operating procedures for information processing facilities should be documented and made available to personnel who need them.	Yes	Yes	-	ScanmarQED operates assets in a secure environment.	Policies and procedures are in place for the correct operation of the ISMS and operational procedures are created for other internal tasks.
	Totals:	**37**	**37**	**36**		

A.6 People controls

AREA/CONTROL	CONTROL DETAILS	CONTROL APPLICABLE	CONTROL IMPLEMENTED	CONTROL REFERENCE	JUSTIFICATION FOR INCLUSION OR EXCLUSION	COMMENTS
A.6.1 Screening	Background verification checks on all candidates to become personnel should be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Yes	Yes	ISMS-DOC-A07-4 HR Security Policy	ScanmarQED employees fulfill the requirements of its ISMS.	Background verification assessed ahead of commencement of duties in proportion to the nature of those duties.
A.6.2 Terms and conditions of employment	The employment contractual agreements should state the personnel’s and the organization’s responsibilities for information security.	Yes	Yes	ISMS-DOC-A07-4 HR Security Policy	ScanmarQED employees fulfill the requirements of its ISMS.	Employment contracts, including those with contract staff, specify relevant requirements for information security, including a commitment to comply with ScanmarQED policies in this area.
A.6.3 Information security awareness, education and training	Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	Yes	Yes	ISMS-DOC-A07-5 Employee Acceptable Use Manual	ScanmarQED employees fulfill the requirements of its ISMS, including awareness, education and training.	Business- wide security training and awareness program is in operation to ensure all employees and contractor are aware of their specific duties and responsibilities as well as general and ongoing education and awareness as appropriate.
A.6.4 Disciplinary process	A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	Yes	Yes	ISMS-DOC-A07-3 Employee Disciplinary Process	ScanmarQED operates a disciplinary process.	Company disciplinary process is communicated to all employees via appropriate channels.
A.6.5 Responsibilities after termination or change of employment	To protect the organization’s interests as part of the process of changing or terminating employment or contracts.	Yes	Yes	ISMS-DOC-A07-4 HR Security Policy	ScanmarQED employees fulfill the requirements of its ISMS.	The information security responsibilities and duties must continue to be observed post-employment as is already agreed upon in the employment contract.

AREA/CONTROL	CONTROL DETAILS	CONTROL APPLICABLE	CONTROL IMPLEMENTED	CONTROL REFERENCE	JUSTIFICATION FOR INCLUSION OR EXCLUSION	COMMENTS
A.6.6 Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Yes	Yes	ISMS-DOC-A07-3 Employee Disciplinary Process ISMS-DOC-A15-1 Information Security Policy for Supplier Relationships	ScanmarQED creates and operates confidential information.	ScanmarQED requires personnel and third parties (suppliers or contractors) to sign specific non-disclosure agreements.
A.6.7 Remote working	Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization’s premises.	Yes	Yes	ISMS-DOC-A07-5 Employee Acceptable Use Manual	ScanmarQED employees can access email and work documents remotely from other than standard location of work.	The Virtual Private Network and Remote Access use authentication methods that control access by remote users.
A.6.8 Information security event reporting	The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Yes	Yes	ISMS-DOC-A16-2 Information Security Incident Response Procedure	ScanmarQED operates an ISMS.	ScanmarQED has implemented a security incident management policy and associated procedures for logging, monitoring, reporting and reviewing incidents.
	Totals:	**8**	**8**	**8**		

A.7 Physical controls

A.7.1 Physical security perimeter	Security perimeters should be defined and used to protect areas that contain information and other associated assets.	Yes	Yes	ISMS-DOC-A11-1 Physical Security Policy	ScanmarQED has facilities requiring physical security controls.	Physical perimeter is identified and facilities are guarded by appropriate controls.
A.7.2 Physical entry	Secure areas should be protected by appropriate entry controls and access points.	Yes	Yes	ISMS-DOC-A11-1 Physical Security Policy	ScanmarQED has facilities requiring physical security controls.	Access to the offices and sesitive areas is determined by physical entry controls.
A.7.3 Securing offices, rooms and facilities	Physical security for offices, rooms and facilities should be designed and implemented.	Yes	Yes	ISMS-DOC-A11-1 Physical Security Policy	ScanmarQED has facilities requiring physical security controls.	Access to the offices and sesitive areas is determined by physical entry controls.
A.7.4 Physical security monitoring	Premises should be continuously monitored for unauthorized physical access.	Yes	Yes	ISMS-DOC-A11-1 Physical Security Policy	ScanmarQED has facilities requiring physical security controls.	Access to the offices and sesitive areas is determined by physical entry controls.
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 should be designed and implemented.	Yes	Yes	ISMS-DOC-A11-1 Physical Security Policy	ScanmarQED has facilities requiring protection against natural disaster and physical threats.	ScanmarQED facilities protection against potential natural disaster, accidents, or malice is managed by the landlord.
A.7.6 Working in secure areas	Security measures for working in secure areas should be designed and implemented.	Yes	Yes	ISMS-DOC-A07-5 Employee Acceptable Use Manual	ScanmarQED has secure areas requiring physical security controls.	ScanmarQED secure areas are assessed for risks and secured proportionate to it.
A.7.7 Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.	Yes	Yes	ISMS-DOC-A07-5 Employee Acceptable Use Manual	ScanmarQED personnel work with sensitive infomration that might be viewable.	All equipment and personnel are subject to acceptable use requirements that include clear desk and clear screen.
A.7.8 Equipment siting and protection	Equipment should be sited securely and protected.	Yes	Yes	ISMS-DOC-A11-1 Physical Security Policy	ScanmarQED has equipment that requires being appropiately secured and sited.	ScanmarQED equipment is sited and secured in a restricted secure area.

AREA/CONTROL	CONTROL DETAILS	CONTROL APPLICABLE	CONTROL IMPLEMENTED	CONTROL REFERENCE	JUSTIFICATION FOR INCLUSION OR EXCLUSION	COMMENTS
A.7.9 Security of assets off-premises	Off-site assets should be protected.	Yes	Yes	ISMS-DOC-A07-5 Employee Acceptable Use Manual	ScanmarQED allows certain assets to be taken off site (e.g. portable projector, personal laptops).	All use off-site of such assets are controlled via contract, policy and/or agreements.
A.7.10 Storage media	Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Yes	Yes	ISMS-DOC-A08-4 Asset Handling Procedure	ScanmarQED uses some kinds of physical storage media included in laptops and servers.	It is explicitly forbidden in the corresponding procedure for classified information. All media disposed of via procedural requirements and appropriately accounted for.
A.7.11 Supporting utilities	Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes	Yes	ISMS-DOC-A11-1 Physical Security Policy	ScanmarQED has equipment that requires protection from any failure or disruption of power.	ScanmarQED equipment is is controled with backups and UPS systems.
A.7.12 Cabling security	Cables carrying power, data or supporting information services should be protected from interception, interference or damage.	Yes	Yes	ISMS-DOC-A11-1 Physical Security Policy	ScanmarQED uses wireless connections in all its offices and server space is protected from unauthorized access.	Cabling security is managed by the building and facilities provider.
A.7.13 Equipment maintenance	Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.	Yes	Yes	ISMS-DOC-A08-8 Asset Management Manual	ScanmarQED has equipment that requires maintenance.	All such equipment is maintained according to manufacturer guidelines and scheduled quarterly.
A.7.14 Secure disposal or re-use of equipment	Items of equipment containing storage media should 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	ISMS-DOC-A08-4 Asset Handling Procedure	ScanmarQED equipment can be reused during its lifespan, then securely disposed.	All assets designated for reuse or removal are adequately wiped and destroyed.
		14	**14**	**14**		

A.8 Technological controls

AREA/CONTROL	CONTROL DETAILS	CONTROL APPLICABLE	CONTROL IMPLEMENTED	CONTROL REFERENCE	JUSTIFICATION FOR INCLUSION OR EXCLUSION	COMMENTS
A.8.1 User endpoint devices	Information stored on, processed by or accessible via user endpoint devices should be protected.	Yes	Yes	ISMS-DOC-A08-8 Asset Management Manual ISMS-DOC-A07-5 Employee Acceptable Use Manual	ScanmarQED operations are based on the use of mobile devices.	ScanmarQED has implemented controls for the appropriate risks associated to the use of mobile devices.
A.8.2 Privileged access rights	The allocation and use of privileged access rights should be restricted and managed.	Yes	Yes	ISMS-DOC-A09-2 User Access Management Process	ScanmarQED operates system requiring the allocation and control of privileged access rights.	All privileged access is assigned according to the requirements of the role and controlled accordingly, (including any system administration duties) are on a need-to-use basis.
A.8.3 Information access restriction	Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.	Yes	Yes	ISMS-DOC-A09-1 Access Control Policy	ScanmarQED operates systems requiring access controls be restricted accordingly with access policy requirements.	Centrally managed Single Sign-On solution for access to internal network and two-factor authentication for all managed systems.
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	ISMS-DOC-A14-1 Secure Development Guidelines	ScanmarQED develops applications which must meet corporate standards.	All program source code is centrally stored and segregated from operational systems with access assigned and controlled accordingly.

AREA/CONTROL	CONTROL DETAILS	CONTROL APPLICABLE	CONTROL IMPLEMENTED	CONTROL REFERENCE	JUSTIFICATION FOR INCLUSION OR EXCLUSION	COMMENTS
A.8.5 Secure authentication	Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.	Yes	Yes	ISMS-DOC-A09-1 Access Control Policy	ScanmarQED operates systems and system requiring secure log-on to managed systems and tools.	All systems and tools access is by secure log-on only (including single sign-on, two-factor authentication, etc.).
A.8.6 Capacity management	The use of resources should be monitored and adjusted in line with current and expected capacity requirements.	Yes	Yes	ISMS-DOC-A06-3 Information Security Guidelines for Project Management	ScanmarQED implements project-based activity such as consultancy and software development, involving capacity management.	Project Managers and Product Owners are informed of the guidelines to apply for capacity management and planning in their projects.
A.8.7 Protection against malware	Protection against malware should be implemented and supported by appropriate user awareness.	Yes	Yes	ISMS-DOC-A12-8 Technical Vulnerability Management Manual	ScanmarQED operates systems that need protection against malware.	Specific malware control software is made available to all user devices provided by ScanmarQED.
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 evaluated and appropriate measures should be taken.	Yes	Yes	ISMS-DOC-A12-8 Technical Vulnerability Management Manual	ScanmarQED operates systems that need protection against technical vulnerabilities.	ScanmarQED ensures technical vulnerabilities are identified and updates are applied in a timely basis.
A.8.9 Configuration management	Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.	Yes	Yes	ISMS-DOC-A12-2 Change Management Process	ScanmarQED uses hardware and software that requires controls over their configurations.	All changes to software, configurations, policies and procedures are assessed and implemented accordingly.
A.8.10 Information deletion	Information stored in information systems, devices or in any other storage media should be deleted when no longer required.	Yes	Yes	ISMS-DOC-A08-4 Asset Handling Procedure ISMS-DOC-A07-5 Employee Acceptable Use Manual	ScanmarQED processes a limited amount of PII as part of its normal business operations.	ScanmarQED personnel commit to an acceptable use policy for classified information.
A.8.11 Data masking	Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	Yes	Yes	ISMS-DOC-A08-4 Asset Handling Procedure ISMS-DOC-A07-5 Employee Acceptable Use Manual	ScanmarQED processes a limited amount of PII as part of its normal business operations.	ScanmarQED personnel commit to an acceptable use policy for classified information.
A.8.12 Data leakage prevention	Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Yes	Yes	ISMS-DOC-A12-8 Technical Vulnerability Management Manual ISMS-DOC-A07-5 Employee Acceptable Use Manual	ScanmarQED operates systems that need protection against data leakage.	ScanmarQED personnel commit to an acceptable use policy for data leak prevention, and monitors sensitive infomration for data leakage events.
A.8.13 Information backup	Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Yes	Yes	ISMS-DOC-A12-8 Technical Vulnerability Management Manual	ScanmarQED operates systems that need backup protection.	Backups are delegate to ScanmarQED's ISO/IEC 27001 certified IT provider.

AREA/CONTROL	CONTROL DETAILS	CONTROL APPLICABLE	CONTROL IMPLEMENTED	CONTROL REFERENCE	JUSTIFICATION FOR INCLUSION OR EXCLUSION	COMMENTS
A.8.14 Redundancy of information processing facilities	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	Yes	Yes	ISMS-DOC-A12-8 Technical Vulnerability Management Manual	ScanmarQED operates business continuity controls.	ScanmarQED operates systems with clustering of virtual servers.
A.8.15 Logging	Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.	Yes	Yes	ISMS-DOC-A12-8 Technical Vulnerability Management Manual	ScanmarQED operates a secure environment requiring logging and monitoring management controls.	Logging and monitoring is delegate to ScanmarQED's ISO/IEC 27001 certified IT provider.
A.8.16 Monitoring activities	Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Yes	Yes	ISMS-DOC-A12-8 Technical Vulnerability Management Manual	ScanmarQED operates a secure environment requiring logging and monitoring management controls.	All access to ScanmarQED networks is suitably controlled and monitored via access controls throughout, with all due consideration to access roles, rights and privileges, authorization, segregation and lifecycle management.
A.8.17 Clock synchronisation	The clocks of information processing systems used by the organization should be synchronized to approved time sources.	Yes	Yes	ISMS-DOC-A12-8 Technical Vulnerability Management Manual	ScanmarQED operates a secure environment requiring logging management controls.	Clock synchronization is delegate to ScanmarQED's ISO/IEC 27001 certified IT provider.
A.8.18 Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.	Yes	Yes	ISMS-DOC-A09-1 Access Control Policy	ScanmarQED allows users to install software on their computers.	Utility programs installation is controled both externally and internally to ensure regular users cannot make use of them.
A.8.19 Installation of software on operational systems	Procedures and measures should be implemented to securely manage software installation on operational systems.	Yes	Yes	ISMS-DOC-A12-8 Technical Vulnerability Management Manual	ScanmarQED allows users to install software on their computers.	Software installation is controled externally to ensure all devices share the same configuration.
A.8.20 Network security	Networks and network devices should be secured, managed and controlled to protect information in systems and applications.	Yes	Yes	ISMS-DOC-A12-8 Technical Vulnerability Management Manual	ScanmarQED uses networks, systems and applications.	Networks are managed and controlled by internal and external ICT.
A.8.21 Security of network services	Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.	Yes	Yes	ISMS-DOC-A12-8 Technical Vulnerability Management Manual	ScanmarQED uses networks, systems and applications.	Networks are managed and controlled by internal and external ICT.
A.8.22 Segregation in networks	Groups of information services, users and information systems should be segregated in the organization's networks.	Yes	Yes	ISMS-DOC-A12-8 Technical Vulnerability Management Manual	ScanmarQED uses networks, systems and applications.	ScanmarQED has segregated its networks and systems, including wireless and VPN controls.
A.8.23 Web filtering	Access to external websites should be managed to reduce exposure to malicious content.	Yes	Yes	ISMS-DOC-A12-8 Technical Vulnerability Management Manual	ScanmarQED is exposed to websites containing malicious content.	Networks are managed and controlled by internal and external ICT.

AREA/CONTROL	CONTROL DETAILS	CONTROL APPLICABLE	CONTROL IMPLEMENTED	CONTROL REFERENCE	JUSTIFICATION FOR INCLUSION OR EXCLUSION	COMMENTS
A.8.24 Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.	Yes	Yes	ISMS-DOC-A12-8 Technical Vulnerability Management Manual	ScanmarQED operates an ISMS requiring cryptographic controls are in operation to protect information.	Cryptographic controls are in operation across all systems and tools as required by the policy.
A.8.25 Secure development lifecycle	Rules for the secure development of software and systems should be established and applied.	Yes	Yes	ISMS-DOC-A14-2 Secure Development Policy	ScanmarQED uses and creates software that requires information security controls.	Policies, procedures and guidelines are in place for secure software development.
A.8.26 Application security requirements	Information security requirements should be identified, specified and approved when developing or acquiring applications.	Yes	Yes	ISMS-DOC-A06-3 Information Security Guidelines for Project Management	ScanmarQED uses and creates software that requires information security controls.	ScanmarQED has implemented policies, rules and controls for the selection, testing, deployment and maintenance of information systems.
A.8.27 Secure system architecture and engineering principles	Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities.	Yes	Yes	ISMS-DOC-A14-3 Principles for Secure Software Development	ScanmarQED uses and creates software that requires information security controls.	Software development principles are in place including secure systems design and secure coding.
A.8.28 Secure coding	Secure coding principles should be applied to software development.	Yes	Yes	ISMS-DOC-A14-1 Secure Development Guidelines	ScanmarQED uses and creates software that requires information security controls.	Software development principles are in place including secure systems design and secure coding.
A.8.29 Security testing in development and acceptance	Security testing processes should be defined and implemented in the development life cycle.	Yes	Yes	ISMS-DOC-A14-2 Secure Development Policy	ScanmarQED uses and creates software that requires information security controls.	Policies, procedures and guidelines are in place for secure software development.
A.8.30 Outsourced development	The organization should direct, monitor and review the activities related to outsourced system development.	Yes	Yes	ISMS-DOC-A14-2 Secure Development Policy	ScanmarQED makes use of third party contractors for software development.	Policies, procedures and guidelines are in place for secure software development including the ones for contractors.
A.8.31 Separation of development, test, and production environments	Development, testing and production environments should be separated and secured.	Yes	Yes	ISMS-DOC-A14-1 Secure Development Guidelines ISMS-DOC-A14-2 Secure Development Policy	ScanmarQED uses and creates software that requires information security controls.	ScanmarQED segregates these environments and applies security controls to each of them.
A.8.32 Change management	Changes to information processing facilities and information systems should be subject to change management procedures.	Yes	Yes	ISMS-DOC-A12-2 Change Management Process	ScanmarQED uses and creates software that requires information security controls.	All changes to software, configurations, policies and procedures are assessed and implemented accordingly.
A.8.33 Test information	Test information should be appropriately selected, protected and managed.	Yes	Yes	ISMS-DOC-A14-2 Secure Development Policy	ScanmarQED uses and creates software that requires information security controls.	Policies, procedures and guidelines are in place for adequate treatment of testing data.
A.8.34 Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management.	Yes	Yes	ISMS-DOC-09-5 Internal Audit Report Template	ScanmarQED operates systems requiring auditing.	ScanmarQED has implemented processes for planning and executing audits aiming to avoid affecting business operations.
		34	34	34		