Statement of Applicability ISO 27001:2022 and NEN 7510:2024 - Fortes Group (2026)

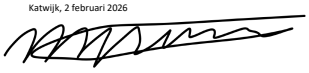
This statement of applicability summarizes the controls from ISO 27001 Annex A and NEN 7510 Annex A that apply and are certified by the Fortes Group.

Version 3.1
Date 02/02/2026
Authors Mark Velthuijsen, Niels Voskamp

Management statement

The management of Qics Holding B.V. (trading under the names of Fortes, Fortes Goup and Fortes Nordics) hereby declares that the measures listed in this Statement of Applicability have been endorsed in relation to the risk analyses carried out, and accepts the residual risk of measures not taken.

Katwijk, 2 februari 2026



M. Velthuijsen, CTO

The following columns are included in the table of control measures:

Nr. Number of the control element
Element Name of the control element
Measure Descirption of the measure
Applicable YES if the control is applicable
Implemented YES if the control is implemented
HLT YES Indicates a NEN7510 specific control or a control with an extra care spceific measure that is applicable and implemented
OS YES is the control is ***partly*** outsourced
Reason for application Indicates why we are applying the measure: WE = Laws and regulations, RA = Risk analysis, CV = Contractual obligation, BV/BP = Business obligation, Best practice
Reason not applicable Indicates why we do not apply the measure.

Nr.	Element	Measure	Applicable	Implemented	HLT	OS	Reason for application				Reason not applicable
							WR	CV	BV/BP	RA	
5.	Organisatorische beheersmaatregelen										
5.1	Information security policies	Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and interested parties, and reviewed at planned intervals and if significant changes occur.	YES	YES	YES		√		√	√	
5.2	Information security roles and responsibilities	Information security roles and responsibilities should be defined and allocated according to the organization's needs.	YES	YES	YES				√	√	
5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility should be segregated.	YES	YES				√	√	√	
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					√	√	
5.5	Contact with authorities	The organization should establish and maintain contact with relevant authorities.	YES	YES				√	√	√	
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				√	√	√	
5.7	Threat intelligence	Information relating to information security threats should be collected and analyzed to produce threat intelligence.	YES	YES				√	√	√	
5.8	Information security in project management	Information security should be integrated into project management.	YES	YES				√		√	
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	YES					√	
5.10	Acceptable use of information and other associated assets	Rules for the acceptable use of and procedures for handling information and other associated assets should be identified, documented, and implemented.	YES	YES						√	
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	YES				√	√	
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	YES		√	√	√	√	
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			√		√	√	
5.14	Information transfer	Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.	YES	YES	YES			√	√	√	
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	YES		√	√	√	√	
5.16	Identity management	The full life cycle of identities should be managed.	YES	YES	YES		√	√		√	
5.17	Authentication 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				√	√	√	
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			√	√		√	
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	YES					√	
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				√		√	
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						√	
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				√		√	
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				√		√	
5.24	Planning and preparing for information security incident management	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				√	√	√	
5.25	Assessing and deciding information security events	The organization should assess information security events and decide if they are to be categorized as information security incidents.	YES	YES				√	√	√	
5.26	Responding to information security incidents	Information security incidents should be responded to in accordance with the documented procedures.	YES	YES				√	√	√	
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				√	√	√	
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				√	√	√	
5.29	Information security during business disruption	The organization should plan how to maintain information security at an appropriate level during disruption.	YES	YES				√		√	
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				√		√	
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			√		√	√	
5.32	Intellectual property rights	The organization should implement appropriate procedures to protect intellectual property rights.	YES	YES			√		√	√	

Nr.	Element	Measure	Applicable	Implemented	HLT	OS	Reason for application				Reason not applicable
							WR	CV	BV/BP	RA	
5.33	Protection of records	Records should be protected from loss, destruction, falsification, unauthorized access, and unauthorized release.	YES	YES		YES	√		√	√	
5.34	Privacy and protection of personally identifiable information	The organization should identify and meet the requirements regarding the preservation of privacy and protection of personally identifiable information according to applicable laws and regulations and contractual requirements.	YES	YES			√	√	√	√	
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		YES		√	√	√	
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		YES		√	√	√	
5.37	Documented operating procedures	Operating procedures for information processing facilities should be documented and made available to personnel who need them.	YES	YES				√		√	
5.38	HLT – Analysis and specification of information security requirements	Information security requirements should be included in the requirements for new information systems or enhancements to existing information systems.			YES	YES	√			√	
5.39	HLT – Uniquely identifying care recipients	Each care recipient should be uniquely identified within the system and duplicate or multiple records should be merged (NEN 7510-specific).			YES	YES	√	√			
5.40	HLT – Validation of displayed/printed data	When data is displayed and/or printed by health information systems, it should include information that identifies the care recipient to whom the data relates (NEN 7510-specific).			YES		√				
5.41	HLT – Publicly available health information	Publicly available health information should be protected, preserved, and managed throughout its lifecycle (NEN 7510-specific).			NO						No publicly available health information is produced
5.42	HLT – Communication in emergencies	Emergency communication channels within a healthcare organization that are activated when there is a disruption in ICT continuity should be planned, implemented, maintained, and tested (NEN 7510-specific).			NO						Not involved in providing care
5.43	HLT – External reporting of incidents	Information security incidents should be reported according to legal or contractual obligations or obligations under laws and regulations (NEN 7510-specific).			YES		√	√			
6.	Mensgerichte beheersmaatregelen										
6.1	Screening	The background of all candidates for employment should be verified prior to employment and periodically thereafter, considering applicable laws, regulations, and business requirements.	YES	YES			√	√		√	
6.2	Terms and conditions of employment	Employment agreements should state the responsibilities of personnel and the organization regarding information security.	YES	YES	YES			√		√	
6.3	Information security awareness, education and training	Personnel and relevant interested parties should receive appropriate awareness, education, and training in information security and regular updates as relevant for their job function.	YES	YES				√	√	√	
6.4	Disciplinary process	A formal and communicated disciplinary process should exist to take action against personnel and other interested parties who have committed an information security breach.	YES	YES						√	
6.5	Responsibilities after termination or change of employment	Responsibilities and duties that remain in force after termination or change of employment should be defined, maintained, and communicated to relevant personnel and other interested parties.	YES	YES			√			√	
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 parties.	YES	YES	YES		√	√	√	√	
6.7	Remote working	Security measures should be implemented to protect information accessed, processed, or stored outside the organization's premises (remote working).	YES	YES		YES				√	
6.8	Information security event reporting	The organization should provide a mechanism for personnel to report observed or suspected information security events in a timely manner through appropriate channels.	YES	YES				√	√	√	
6.9	HLT – Management training	Management should receive appropriate training in information security management (NEN 7510-specific).			YES				√	√	
7.	Fysieke beheersmaatregelen										
7.1	Physical security perimeters	Areas containing information and other associated assets should be protected by defining and using security perimeters.	YES	YES		YES		√		√	
7.2	Physical entry controls	Secure areas should be protected by appropriate entry controls and access points.	YES	YES		YES	√	√		√	
7.3	Securing offices, rooms and facilities	Physical security should be designed and implemented for offices, rooms, and facilities.	YES	YES		YES		√		√	
7.4	Monitoring of physical security	The building and premises should be continuously monitored for unauthorized physical access.	YES	YES		YES		√		√	
7.5	Protection against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional threats to infrastructure, should be designed and implemented.	YES	YES		YES		√		√	
7.6	Working in secure areas	Security measures should be developed and implemented for working in secure areas.	YES	YES				√		√	
7.7	Clear desk and clear screen	Clear desk and clear screen rules should be defined and enforced for paper documents, removable storage media, and information processing facilities.	YES	YES						√	
7.8	Equipment siting and protection	Equipment should be sited and protected securely.	YES	YES		YES		√		√	
7.9	Security of assets off-premises	Assets outside the organization's premises should be protected.	YES	YES					√	√	
7.10	Storage media	Storage media should be managed throughout their lifecycle in accordance with the organization's classification scheme and handling requirements.	YES	YES	NO					√	We don't keep health information on devices
7.11	Supporting utilities	Information processing facilities should be protected against power failures and other disruptions caused by utility outages.	YES	YES		YES				√	
7.12	Cabling security	Power and data cables supporting information services should be protected against interception, interference, or damage.	YES	YES		YES				√	
7.13	Equipment maintenance	Equipment should be properly maintained to ensure availability, integrity, and reliability of information.	YES	YES		YES		√		√	
7.14	Secure disposal or re-use of equipment	Equipment containing storage media should be checked to ensure that sensitive data and licensed software have been removed or securely overwritten before disposal or reuse.	YES	YES						√	
8.	Technologische beheersmaatregelen										
8.1	User endpoint devices	Information stored on, processed by, or accessible via user endpoint devices should be protected.	YES	YES			√			√	
8.2	Privileged access rights	The assignment and use of privileged access rights should be restricted and managed.	YES	YES			√	√		√	
8.3	Information access restriction	Access to information and other associated assets should be restricted in accordance with the organization's access control policy.	YES	YES			√	√		√	
8.4	Access to source code	Read and write access to source code, development tools, and software libraries should be appropriately managed.	YES	YES		YES		√	√	√	
8.5	Secure authentication	Secure authentication technologies and procedures should be implemented based on access restrictions and the organization's access control policy.	YES	YES	YES	YES	√	√		√	
8.6	Capacity management	Resource usage should be monitored and adjusted according to current and expected capacity requirements.	YES	YES		YES		√		√	
8.7	Protection against malware	Protection against malware should be implemented and supported by appropriate user awareness.	YES	YES		YES				√	
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 evaluated, and appropriate measures taken.	YES	YES		YES		√		√	
8.9	Configuration management	Configurations, including security configurations, of hardware, software, services, and networks should be established, documented, implemented, monitored, and reviewed.	YES	YES		YES		√		√	
8.10	Information deletion	Information stored in information systems, devices, or other storage media should be erased when no longer required.	YES	YES			√		√	√	
8.11	Data masking	Data should be masked in accordance with the organization's access control policy and other relevant policies, and business requirements, considering applicable laws.	YES	YES				√	√	√	
8.12	Data leakage prevention	Measures to prevent data leakage should be applied to systems, networks, and other devices processing, storing, or transmitting sensitive information.	YES	YES		YES		√		√	

Nr.	Element	Measure	Applicable	Implemented	HLT	OS	Reason for application				Reason not applicable
							WR	CV	BV/BP	RA	
8.13	Backup of information	Backups of information, software, and systems should be maintained and regularly tested in accordance with the agreed backup policy.	YES	YES	YES	YES		√		√	
8.14	Redundancy of information processing facilities	Information processing facilities should be implemented with sufficient redundancy to meet availability requirements.	YES	YES				√		√	
8.15	Logging	Log files recording activities, exceptions, faults, and other relevant events should be produced, stored, protected, and analyzed.	YES	YES		YES		√		√	
8.16	Monitoring activities	Networks, systems, and applications should be monitored for abnormal behavior and appropriate measures taken to evaluate potential information security incidents.	YES	YES		YES		√		√	
8.17	Clock synchronization	Clocks of information processing systems used by the organization should be synchronized with approved time sources.	YES	YES		YES		√	√	√	
8.18	Use of privileged utility programs	The use of system utilities capable of bypassing security controls should be restricted and closely monitored.	YES	YES				√		√	
8.19	Installation of software on operational systems	Procedures and measures should be implemented to securely manage the installation of software on operational systems.	YES	YES						√	
8.20	Network security	Networks and network devices should be secured, managed, and controlled to protect information in systems and applications.	YES	YES		YES		√		√	
8.21	Security of network services	Security mechanisms, service levels, and service requirements for all network services should be identified, implemented, and monitored.	YES	YES		YES		√		√	
8.22	Network segregation	Groups of information services, users, and information systems should be segmented within the organization's networks.	YES	YES				√		√	
8.23	Web filtering	Access to external websites should be managed to limit exposure to malicious content.	YES	YES		YES		√		√	
8.24	Use of cryptography	Rules for the effective use of cryptography, including key management, should be defined and implemented.	YES	YES			√			√	
8.25	Secure development life cycle	Rules should be established and applied for the secure development of software and systems.	YES	YES				√		√	
8.26	Application security requirements	Information security requirements should be identified, specified, and approved when developing or acquiring applications.	YES	YES						√	
8.27	Secure system architecture and engineering principles	Principles for designing secure systems should be established, documented, maintained, and applied for all activities related to information system development.	YES	YES				√		√	
8.28	Secure coding	Secure coding principles should be applied to software development.	YES	YES				√		√	
8.29	Security testing in development and acceptance	Security testing processes should be defined and implemented in the development lifecycle.	YES	YES		YES		√		√	
8.30	Outsourced system development	The organization should direct, monitor, and review activities related to outsourced system development.	YES	YES				√		√	
8.31	Separation of development, test and production environments	Development, test, and production environments should be separated and secured.	YES	YES		YES		√		√	
8.32	Change management	Changes to information processing facilities and information systems should be subject to change management procedures.	YES	YES				√		√	
8.33	Test data	Test data should be appropriately selected, protected, and managed.	YES	YES		YES		√	√	√	
8.34	Protection of information systems during audits	Audit tests and other audit activities involving operational systems should be planned and agreed upon between the tester and responsible management.	YES	YES					√	√	
8.35	HLT – Zero trust principles	Zero trust principles should be applied to information security architecture and operations (NEN 7510-specific).			YES	YES		√	√	√	