

SoA (Statement of Applicability)

Organisation

Cyberfusion B.V.

Version

1.2

Date

2025-03-04

Norm

NEN-EN-ISO/IEC 27001:2023/A1:2024 en

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
✓	✓	5.1 (Policies for information security)	Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to	RC (NIS2), BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
			and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	
✓	✓	5.2 (Information security roles and responsibilities)	Information security roles and responsibilities shall be defined and allocated according to the organisation needs.	BR, RA
✓	✓	5.3 (Segregation of duties)	Conflicting duties and conflicting areas of responsibility shall be segregated.	BR, RA
✓	✓	5.4 (Management responsibilities)	Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
✓	✓	5.5 (Contact with authorities)	organisation. The organisation shall establish and maintain contact with relevant authorities.	BR, RA
✓	✓	5.6 (Contact with special interest groups)	The organisation shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	BR, RA
✓	✓	5.7 (Threat intelligence)	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	BR, RA
✓	✓	5.8 (Information security in project management)	Information security shall be integrated into project management.	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
✓	✓	5.9 (Inventory of information and other associated assets)	An inventory of information and other associated assets, including owners, shall be developed and maintained.	BR, RA
✓	✓	5.10 (Acceptable use of information and other associated assets)	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	BR, RA
✓	✓	5.11 (Return of assets)	Personnel and other interested parties as appropriate shall return all the organisation's assets in their possession upon change or termination of their employment, contract or agreement.	BR, RA
✓	✓	5.12 (Classification of	Information shall be classified according	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
		information)	to the information security needs of the organisation based on confidentiality, integrity, availability and relevant interested party requirements.	
✓	✓	5.13 (Labelling of information)	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organisation.	BR, RA
✓	✓	5.14 (Information transfer)	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organisation and between the organisation and other parties.	BR, RA
✓	✓	5.15 (Access control)	Rules to control physical and logical access to	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
			information and other associated assets shall be established and implemented based on business and information security requirements.	
✓	✓	5.16 (Identity management)	The full life cycle of identities shall be managed.	BR, RA
✓	✓	5.17 (Authentication information)	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	BR, RA
✓	✓	5.18 (Access rights)	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organisation's	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
✓	✓	5.19 (Information security in supplier relationships)	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	BR, RA
✓	✓	5.20 (Addressing information security within supplier agreements)	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	BR, RA
✓	✓	5.21 (Managing information security in the ICT supply chain)	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
✓	✓	5.22 (Monitoring, review and change management of supplier services)	chain. The organisation shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	BR, RA
✓	✓	5.23 (Information security for use of cloud services)	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organisation's information security requirements.	BR, RA
✓	✓	5.24 (Information security incident management planning and preparation)	The organisation shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
✓	✓	5.25 (Assessment and decision on information security events)	management processes, roles and responsibilities. The organisation shall assess information security events and decide if they are to be categorised as information security incidents.	BR, RA
✓	✓	5.26 (Response to information security incidents)	Information security incidents shall be responded to in accordance with the documented procedures.	BR, RA
✓	✓	5.27 (Learning from information security incidents)	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	BR, RA
✓	✓	5.28 (Collection of evidence)	The organisation shall establish and implement procedures for the identification, collection,	RC, BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
✓	✓	5.29 (Information security during disruption)	<p>acquisition and preservation of evidence related to information security events.</p> <p>The organisation shall plan how to maintain information security at an appropriate level during disruption.</p>	BR, RA
✓	✓	5.30 (ICT readiness for business continuity)	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	BR, RA
✓	✓	5.31 (Identification of legal, statutory, regulatory and contractual requirements)	Legal, statutory, regulatory and contractual requirements relevant to information security and the organisation's approach to meet these requirements shall be identified, documented and	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
			kept up to date.	
✓	✓	5.32 (Intellectual property rights)	The organisation shall implement appropriate procedures to protect intellectual property rights.	BR, RA
✓	✓	5.33 (Protection of records)	Records shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release.	RC, BR, RA
✓	✓	5.34 (Privacy and protection of PII)	The organisation shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	RC, BR, RA
✓	✓	5.35 (Independent review of information)	The organisation's approach to managing information	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
		security)	security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	
✓	✓	5.36 (Compliance with policies and standards for information security)	Compliance with the organisation's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.	BR, RA
✓	✓	5.37 (Documented operating procedures)	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	BR, RA
✓	✓	6.1 (Screening)	Background verification checks on all candidates to become personnel shall be carried out prior to joining the	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
			<p>organisation 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.</p>	
✓	✓	6.2 (Terms and conditions of employment)	The employment contractual agreements shall state the personnel's and the organisation's responsibilities for information security.	BR, RA
✓	✓	6.3 (Information security awareness, education and training)	Personnel of the organisation and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organisation's	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
			information security policy, topic-specific policies and procedures, as relevant for their job function.	
✓	✓	6.4 (Disciplinary process)	A disciplinary process shall be formalised and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	BR, RA
✓	✓	6.5 (Responsibilities after termination or change of employment)	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
✓	✓	6.6 (Confidentiality or non-disclosure agreements)	Confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	BR, RA
✓	✓	6.7 (Remote working)	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organisation's premises.	BR, RA
✓	✓	6.8 (Information security event reporting)	The organisation shall provide a mechanism for personnel to report observed or suspected information security events	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
			through appropriate channels in a timely manner.	
✓	✓	7.1 (Physical security perimeter)	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	BR, RA
✓	✓	7.2 (Physical entry controls)	Secure areas shall be protected by appropriate entry controls and access points.	BR, RA
✓	✓	7.3 (Securing offices, rooms and facilities)	Physical security for offices, rooms and facilities shall be designed and implemented.	BR, RA
✓	✓	7.4 (Physical security monitoring)	Premises shall be continuously monitored for unauthorised physical access.	BR, RA
✓	✓	7.5 (Protecting against physical and environmental threats)	Protection against physical and environmental threats, such as natural disasters and other	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
✓	✓	7.6 (Working in secure areas)	intentional or unintentional physical threats to infrastructure shall be designed and implemented. Security measures for working in secure areas shall be designed and implemented.	BR, RA
✓	✓	7.7 (Clear desk and clear screen)	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	BR, RA
✓	✓	7.8 (Equipment siting and protection)	Equipment shall be sited securely and protected.	BR, RA
✓	✓	7.9 (Security of assets off-premises)	Off-site assets shall be protected.	BR, RA
✓	✓	7.10 (Storage media)	Storage media shall be managed through their life cycle of acquisition,	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
✓	✓	7.11 (Supporting utilities)	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	BR, RA
✓	✓	7.12 (Cabling security)	Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	BR, RA
✓	✓	7.13 (Equipment maintenance)	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
✓	✓	7.14 (Secure disposal or re-use of equipment)	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.	BR, RA
✓	✓	8.1 (User endpoint devices)	Information stored on, processed by or accessible via user end point devices shall be protected.	BR, RA
✓	✓	8.2 (Privileged access rights)	The allocation and use of privileged access rights shall be restricted and managed.	BR, RA
✓	✓	8.3 (Information access restriction)	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
✓	✓	8.4 (Access to source code)	Read and write access to source code, development tools and software libraries shall be appropriately managed.	BR, RA
✓	✓	8.5 (Secure authentication)	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	BR, RA
✓	✓	8.6 (Capacity management)	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	BR, RA
✓	✓	8.7 (Protection against malware)	Protection against malware shall be implemented and supported by appropriate user awareness.	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
✓	✓	8.8 (Management of technical vulnerabilities)	Information about technical vulnerabilities of information systems in use shall be obtained, the organisation's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	BR, RA
✓	✓	8.9 (Configuration management)	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	BR, RA
✓	✓	8.10 (Information deletion)	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
✓	✓	8.11 (Data masking)	Data masking shall be used in accordance with the organisation's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	BR, RA
✓	✓	8.12 (Data leakage prevention)	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	BR, RA
✓	✓	8.13 (Information backup)	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
✓	✓	8.14 (Redundancy of information processing facilities)	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	BR, RA
✓	✓	8.15 (Logging)	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	BR, RA
✓	✓	8.16 (Monitoring activities)	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	BR, RA
✓	✓	8.17 (Clock synchronisation)	The clocks of information processing systems used by the organisation shall be synchronised to	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
			approved time sources.	
✓	✓	8.18 (Use of privileged utility programs)	The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	BR, RA
✓	✓	8.19 (Installation of software on operational systems)	Procedures and measures shall be implemented to securely manage software installation on operational systems.	BR, RA
✓	✓	8.20 (Network security)	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	BR, RA
✓	✓	8.21 (Security of network services)	Security mechanisms, service levels and service requirements of network services	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
✓	✓	8.22 (Segregation in networks)	shall be identified, implemented and monitored. Groups of information services, users and information systems shall be segregated in the organisation's networks.	BR, RA
✓	✓	8.23 (Web filtering)	Access to external websites shall be managed to reduce exposure to malicious content.	BR, RA
✓	✓	8.24 (Use of cryptography)	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	BR, RA
✓	✓	8.25 (Secure development lifecycle)	Rules for the secure development of software and systems shall be established and applied.	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
✓	✓	8.26 (Application security requirements)	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	BR, RA
✓	✓	8.27 (Secure system architecture and engineering principles)	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	BR, RA
✓	✓	8.28 (Secure coding)	Secure coding principles shall be applied to software development.	BR, RA
✓	✓	8.29 (Security testing in development and acceptance)	Security testing processes shall be defined and implemented in the development life cycle.	BR, RA
✓	✓	8.30 (Outsourced development)	The organisation shall direct, monitor	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
			and review the activities related to outsourced system development.	
✓	✓	8.31 (Separation of development, test and production environments)	Development, testing and production environments shall be separated and secured.	BR, RA
✓	✓	8.32 (Change management)	Changes to information processing facilities and information systems shall be subject to change management procedures.	BR, RA
✓	✓	8.33 (Test information)	Test information shall be appropriately selected, protected and managed.	BR, RA
✓	✓	8.34 (Protection of information systems during audit and testing)	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate	BR, RA

Applicable?	Implemented?	Control	Objectives and measures	Reason for selection: RC / BR / RA
			management.	

Legend

- RC: regulatory and contractual demands
- BR: business requirements / best practices
- RA: risk analysis