Dillien

Statement of Applicability (SOA): ISO 27001 (2022) Annex A controls

All controls must be implemented OR excluded

					Justification for inclusion					
Clause	**#**	**Control Title**	**Control Objective**	**Justification for exclusion**	**Regulatory**	**Contractual**	**Best Practice**	**Mitigate Risk**	**Status**	**Implementation**
5 Organizational Controls	**A.5**									
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?section=A.5&controlId=ihtowh2e
	5.2	Information security roles and responsibilities	Information security roles and responsibilities should be defined and allocated according to the organization needs				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=6i8ettoj
	5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility should be segregated.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=v4vhjfvh
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=69z2hplm
	5.5	Contact with authorities	The organization should establish and maintain contact with relevant authorities.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=dm9a5emm
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=5sd6imyl
	5.7	Threat Intelligence	Information relating to information security threats should be collected and analysed to produce threatintelligence.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=mjnl61h4
	5.8	Information security in project management	Information security should be integrated into project management.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=1lbwjsfo
	5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, should be developed andmaintained.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=duwec37o
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=425x42p9
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=23wj3sby

Clause	#	Control Title	Control Objective	Justification for exclusion	Regulatory	Contractual	Best Practice	Mitigate Risk	Status	Implementation
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=m8r0bfbq
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=5qzssew8
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=nogvv3hw
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=v2ygke7o
	5.16	Identity management	The full life cycle of identities should be managed.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=pggqq813
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=5c4gnshh
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=xtd1rde4
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=dz91o1f8
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=v9blvnxj
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=69evj2pe
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=r7xxjkaz
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=zrx7kjgo

Clause	#	Control Title	Control Objective	Justification for exclusion	Regulatory	Contractual	Best Practice	Mitigate Risk	Status	Implementation
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=lggb5g7c
	5.25	Assessment 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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=tp0kv7ho
	5.26	Response to information security incidents	Information security incidents should be responded to in accordance with the documented procedures.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=qmodzmvg
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=47fxwco1
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=2qki93x0
	5.29	Information security during disruption	The organization should plan how to maintain information security at an appropriate level during disruption.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=x14j0x47
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=9t2qdzle
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=p87muahm
	5.32	Intellectual property rights	The organization should implement appropriate procedures to protect intellectual property rights.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=gonqt473
	5.33	Protection of records	Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=mtbrd5ny
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=zz8z506w
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=7pn1c8nr

Clause	#	Control Title	Control Objective	Justification for exclusion	Regulatory	Contractual	Best Practice	Mitigate Risk	Status	Implementation
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=9yz4l6l3
	5.37	Documented operating procedures	Operating procedures for information processing facilities should be documented and made available to personnel who need them.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=o9q0idpd
6 People Controls	**A.6**									
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?section=A.5&controlId=i9up48pp
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=erq8anhq
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=h46r2403
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=zn5t4xav
	6.5	Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=15al5zi7
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=uxoiizoh
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=wka7s1yw
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=qgkw4h74

Clause	#	Control Title	Control Objective	Justification for exclusion	Regulatory	Contractual	Best Practice	Mitigate Risk	Status	Implementation
7 Physical Controls	**A.7**									
	7.1	Physical security perimeters	Security perimeters should be defined and used to protect areas that contain information and other associated assets.	Physical security controls are excluded from the ISMS scope as the company does not maintain any on-premise infrastructure. All systems and privileged information are hosted on secure, cloud-based platforms (e.g., Google Cloud Platform), and no critical assets are stored or processed locally.					Excluded	N/A
	7.2	Physical entry	Secure areas should be protected by appropriate entry controls and access points.	Physical security controls are excluded from the ISMS scope as the company does not maintain any on-premise infrastructure. All systems and privileged information are hosted on secure, cloud-based platforms (e.g., Google Cloud Platform), and no critical assets are stored or processed locally.					Excluded	N/A
	7.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities should be designed and implemented.	Physical security controls are excluded from the ISMS scope as the company does not maintain any on-premise infrastructure. All systems and privileged information are hosted on secure, cloud-based platforms (e.g., Google Cloud Platform), and no critical assets are stored or processed locally.					Excluded	N/A
	7.4	Physical security monitoring	Premises should be continuously monitored for unauthorized physical access.	Physical security controls are excluded from the ISMS scope as the company does not maintain any on-premise infrastructure. All systems and privileged information are hosted on secure, cloud-based platforms (e.g., Google Cloud Platform), and no critical assets are stored or processed locally.					Excluded	N/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.	Physical security controls are excluded from the ISMS scope as the company does not maintain any on-premise infrastructure. All systems and privileged information are hosted on secure, cloud-based platforms (e.g., Google Cloud Platform), and no critical assets are stored or processed locally.					Excluded	N/A
	7.6	Working in secure areas	Security measures for working in secure areas should be designed and implemented.	Physical security controls are excluded from the ISMS scope as the company does not maintain any on-premise infrastructure. All systems and privileged information are hosted on secure, cloud-based platforms (e.g., Google Cloud Platform), and no critical assets are stored or processed locally.					Excluded	N/A

Clause	#	Control Title	Control Objective	Justification for exclusion	Regulatory	Contractual	Best Practice	Mitigate Risk	Status	Implementation
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=35g7wvxd
	7.8	Equipment siting and protection	Equipment should be sited securely and protected.	Physical security controls are excluded from the ISMS scope as the company does not maintain any on-premise infrastructure. All systems and privileged information are hosted on secure, cloud-based platforms (e.g., Google Cloud Platform), and no critical assets are stored or processed locally.					Excluded	N/A
	7.9	Security of assets off-premises	Off-site assets should be protected.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=dzm2dexq
	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.	Physical security controls are excluded from the ISMS scope as the company does not maintain any on-premise infrastructure. All systems and privileged information are hosted on secure, cloud-based platforms (e.g., Google Cloud Platform), and no critical assets are stored or processed locally.					Excluded	N/A
	7.11	Supporting utilities	Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.	Physical security controls are excluded from the ISMS scope as the company does not maintain any on-premise infrastructure. All systems and privileged information are hosted on secure, cloud-based platforms (e.g., Google Cloud Platform), and no critical assets are stored or processed locally.					Excluded	N/A
	7.12	Cabling security	Cables carrying power, data or supporting information services should be protected from interception, interference or damage.	Physical security controls are excluded from the ISMS scope as the company does not maintain any on-premise infrastructure. All systems and privileged information are hosted on secure, cloud-based platforms (e.g., Google Cloud Platform), and no critical assets are stored or processed locally.					Excluded	N/A
	7.13	Equipment maintenance	Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.	Physical security controls are excluded from the ISMS scope as the company does not maintain any on-premise infrastructure. All systems and privileged information are hosted on secure, cloud-based platforms (e.g., Google Cloud Platform), and no critical assets are stored or processed locally.					Excluded	N/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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=2yosmk08

Clause	#	Control Title	Control Objective	Justification for exclusion	Regulatory	Contractual	Best Practice	Mitigate Risk	Status	Implementation
8 Technological Controls	**A.8**									
	8.1	User endpoint devices	Information stored on, processed by or accessible via user endpoint devices should be protected.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?section=A.5&controlId=2zhexo15
	8.2	Privileged access rights	The allocation and use of privileged access rights should be restricted and managed.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=zxjp1hkl
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=mwwihowm
	8.4	Access to source code	Read and write access to source code, development tools and software libraries should be appropriately managed.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=axwe26mw
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=iubivdgx
	8.6	Capacity management	The use of resources should be monitored and adjusted in line with current and expected capacity requirements.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=fpa4156z
	8.7	Protection against malware	Protection against malware should be implemented and supported by appropriate user awareness.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=4e2usbzc
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=z01cfd6c
	8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=hrnf9oqw
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=kt5aajg7
	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.	No use cases require masking of production or sensitive data.					Excluded	N/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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=zv2sb0to
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=o7ssnlfi

Clause	#	Control Title	Control Objective	Justification for exclusion	Regulatory	Contractual	Best Practice	Mitigate Risk	Status	Implementation
	8.14	Redundancy of information processing facilities	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=oufs0z8u
	8.15	Logging	Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=3osnyf10
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=i7xairas
	8.17	Clock synchronization	The clocks of information processing systems used by the organization should be synchronized to approved time sources.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=puuo9pwr
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=5o51jc7h
	8.19	Installation of software on operational systems	Procedures and measures should be implemented to securely manage software installation on operational systems.	Systems are managed in cloud environments.					Excluded	N/A
	8.20	Networks security	Networks and network devices should be secured, managed and controlled to protect information in systems and applications.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=jqyhc6kq
	8.21	Security of network services	Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=z58ieqyf
	8.22	Segregation of networks	Groups of information services, users and information systems should be segregated in the organization's networks.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=k3eilu6n
	8.23	Web filtering	Access to external websites should be managed to reduce exposure to malicious content.	The organization does not centrally manage employee devices. Risks are addressed through endpoint and browser security.					Excluded	N/A
	8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=07i98tv1
	8.25	Secure development life cycle	Rules for the secure development of software and systems should be established and applied.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=c7diea1e
	8.26	Application security requirements	Information security requirements should be identified, specified and approved when developing or acquiring applications.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=m6u2mvnk
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=27qd09no
	8.28	Secure coding	Secure coding principles should be applied to software development.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=qi8ey5na

Clause	#	Control Title	Control Objective	Justification for exclusion	Regulatory	Contractual	Best Practice	Mitigate Risk	Status	Implementation
	8.29	Security testing in development and acceptance	Security testing processes should be defined and implemented in the development life cycle.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=ise32uno
	8.30	Outsourced development	The organization should direct, monitor and review the activities related to outsourced system development.	No outsourced system development.					Excluded	N/A
	8.31	Separation of development, test and production environments	Development, testing and production environments should be separated and secured.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=sbiopz10
	8.32	Change management	Changes to information processing facilities and information systems should be subject to change management procedures.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=sbjgr7xz
	8.33	Test information	Test information should be appropriately selected, protected and managed.				Yes	Yes	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=bqnpwe6c
	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	Implemented	Implementation is tracked within the Vanta application: https://app.eu.vanta.com/frameworks/iso27001_2022/controls?controlId=dzsaee29

Document History

Version	Date	Description	Written by	Approved by
1.0.0	2025-05-20	Initial Version	Ryan Rich	Elin Schanke Funnemark
1.0.1	2025-06-27	Updated to reflect scope	Yuan Jing Chow	Elin Schanke Funnemark
1.0.2	2025-07-20	Updated to reflect scope	Håkon Hultman Tømte	Elin Schanke Funnemark
1.0.3	2025-08-25	Updated to reflect scope	Håkon Hultman Tømte	Elin Schanke Funnemark
1.1.0	2026-09-21	Implemented A.8.12 (Data leakage prevention); corrected A.7.8 to Excluded; editorial alignment of exclusion wording across A.7.	Håkon Hultman Tømte	Elin Schanke Funnemark