goodhabitz online training **Statement of Applicability ISO 27001:2013**

Annex A	Control title	Control description	In scope?	Reason (not) in scope	Implemented?	Implemented control
A.5	Information security policies					
A.5.1	Management direction for information security					
A.5.1.1	Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	Yes	• Basic (documentation) • Awareness • Management commitment	Yes	A formal information security policy has been implemented.
A.5.1.2	Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Yes	• Risk reduction with regard to information security • Improve continuously	Yes	All policies and controls and subjected to periodical reviews.
A.6	Organization of information security					
A.6.1	Internal organization					
A.6.1.1	Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	Yes	• Basic (documentation)	Yes	Security is part of all roles in the organization. All responsiblities have been described in job descriptions and are maintained. Segregation of duties is implemented.
A.6.1.2	Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	Yes	• Reduction of risks with regard to information security	Yes	Security is part of all roles in the organization. All responisiblities have been described in job descriptions and are maintained Segregation of duties is implemented.
A.6.1.3.	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	Yes	• Requirments of authorities	Yes	Is part of security officers role.
A.6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	Yes	• Requirements of stakeholders	Yes	Is part of security officers role.
A.6.1.5	Information security in project management	Information security shall be addressed in project management, regardless of the type of the project.	Yes	• Reduction of risks with regard to information security • Protection of company values	Yes	Security by design is integrated into project management process.
A.6.2	Mobile devices and teleworking					
A.6.2.1	Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	Yes	• Basic (documentation) • Reduction of risks with regard to information security • Protection of company values	Yes	A formal policy has been implemented and is maintained (code of conduct).
A.6.2.2	Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	Yes	• Basic (documentation) • Reduction of risks with regard to information security • Protection of company values	Yes	A formal policy has been implemented and is maintained (code of conduct).
A.7	Human resource security					
A.71	Prior to employment					
A.7.1.1	Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Yes	• Basic (documentation) • Reduction of risks with regard to information security • Protection of company values	Yes	Screening and background checks are part of the procedures for all personell.
A.7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	Yes	• Basic (documentation) • Reduction of risks with regard to information security • Protection of company values	Yes	Responsibilities are part of the personnel manual which forms an integral part of the employment of an employee.
A.7.2	During employment					
A.7.2.1	Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	Yes	• Awareness • Reduction of risks with regard to information security • Protection of company values • Management commitment	Yes	All responisiblities have been described in job descriptions and are maintained. Special protocol for third parties have been designed and implemented.
A.7.2.2	Information security awareness, education and training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	Yes	• Awareness • Reduction of risks with regard to information security • Protection of company values • Management commitment	Yes	Awareness campagnes are held and continuously monitored. A formal procedure 'on boarding' is in place and explicitly linked to awareness instruction.
A.7.2.3	Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	Yes	• Awareness • Reduction of risks with regard to information security • Protection of company values • Management commitment	Yes	A formal disciplinary process has been implemented.
A.7.3	Termination and change of employment					
A.7.3.1	Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	Yes	• Reduction of risks with regard to information security • Protection of company values	Yes	Formal procedures "offboarding" and "changes personnel" are in place and explicitly linked to access control.
A.8	Asset management					
A.8.1	Responsibility for assets					
A.8.1.1	Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	Yes	• Reduction of risks with regard to information security • Protection of company values	Yes	A formal asset management policy and procedure has been implemented and is maintained.

goodhabitz online training **Statement of Applicability ISO 27001:2013**

Annex A	Control title	Control description	In scope?	Reason (not) in scope	Implemented?	Implemented control
A.8.1.2	Ownership of assets	Assets maintained in the inventory shall be owned.	Yes	• Reduction of risks with regard to information security • Protection of company values	Yes	All assets have been assigned an owner, with adequate responsibilities and rights.
A.8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	Yes	• Reduction of risks with regard to information security • Protection of company values	Yes	An acceptable use policy has been implemented.
A.8.1.4	Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	Yes	• Reduction of risks with regard to information security • Protection of company values	Yes	A formal procedure "off boarding" is in place and is explicitly linked to asset management.
A.8.2	Information classification					
A.8.2.1	Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	Yes	• Reduction of risks with regard to information security • Protection of company values	Yes	A formal policy and procedure for the guidelines of classification has implemented.
A.8.2.2	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 organization.	Yes	• Reduction of risks with regard to information security • Protection of company values	Yes	A policy how to handle labelling of information is formalized.
A.8.2.3	Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes	• Reduction of risks with regard to information security • Protection of company values	Yes	A procedure for handling assets in accordance with the information classification scheme is available (code of conduct).
A.8.3	Media handling					
A.8.3.1	Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	Yes	• Reduction of risks with regard to information security • Protection of company values • Complying with laws and regulations	Yes	Procedures have been implemented and are maintained.
A.8.3.2	Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.	Yes	• Reduction of risks with regard to information security • Protection of company values • Complying with laws and regulations	Yes	Procedures have been implemented and are maintained.
A.8.3.3	Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	Yes	• Awareness • Reduction of risks with regard to information security • Protection of company values • Complying with laws and regulations	Yes	Procedures have been implemented and are maintained.
A.9	Access control					
A.9.1	Business requirements of access control					
A.9.1.1	Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	An access and authorisation policy has been implemented.
A.9.1.2	Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	An access and authorisation policy has been implemented.
A.9.2	User access management					
A.9.2.1	User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Access and authorisation procedures have been implemented.
A.9.2.2	User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Access and authorisation procedures have been implemented.
A.9.2.3	Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Access and authorisation procedures have been implemented.
A.9.2.4	Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Access and authorisation procedures have been implemented.
A.9.2.5	Review of user access rights	Asset owners shall review users' access rights at regular intervals.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Access and authorisation procedures have been implemented.
A.9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Access and authorisation procedures have been implemented.
A.9.3	User responsibilities					
A.9.3.1	Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information.	Yes	• Awareness • Reduction of risks with regard to information security • Protection of business values	Yes	Access and authorisation procedures have been implemented.
A.9.4	System and application access control					
A.9.4.1	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Access and authorisation procedures have been implemented.
A.9.4.2	Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Access and authorisation procedures have been implemented.
A.9.4.3	Password management system	Password management systems shall be interactive and shall ensure quality passwords.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	• Reduction of risks with regard to information security • Protection of business values

goodhabitz online training **Statement of Applicability ISO 27001:2013**

Annex A	Control title	Control description	In scope?	Reason (not) in scope	Implemented?	Implemented control
A.9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Access and authorisation procedures have been implemented.
A.9.4.5	Access control to program source code	Access to program source code shall be restricted.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Access and authorisation procedures have been implemented.
A.10	Cryptography					
A.10.1	Cryptographic controls					
A.10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	A policy for the use of cryptographic controls have been implemented.
A.10.1.2	Key Management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	A policy for the use of cryptographic controls have been implemented.
A.11	Physical and environmental security					
A.11.1	Secure areas					
A.11.1.1	Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Physical security is divided: the GoodHabitz offices and the data centre. The datacentre responsibilities have been outsourced and are monitored by OBI Automatisering to ensure compliance. The datacentre itself is ISO27001 certified.
A.11.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Physical security is divided: the GoodHabitz offices and the data centre. The datacentre responsibilities have been outsourced and are monitored by OBI Automatisering to ensure compliance. The datacentre itself is ISO27001 certified.
A.11.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Physical security measures for GoodHabitz offices are applied.
A.11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Physical security is divided: the GoodHabitz offices and the data centre. The datacentre responsibilities have been outsourced and are monitored by OBI Automatisering to ensure compliance. The datacentre itself is ISO27001 certified.
A.11.1.5	Working in secure areas	Procedures for working in secure areas shall be designed and applied.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Areas and procedures are defined for entering/working in secure areas.
A.11.1.6	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Unauthorized access is controlled for delivery and loading areas.
A.11.2	Equipment					
A.11.2.1	Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Yes	• Reduction of risks with regard to information security • Protection of company values • Business continuity	Yes	Physical security is divided: the GoodHabitz offices and the data centre. The datacentre responsibilities have been outsourced and are monitored by OBI Automatisering to ensure compliance. The datacentre itself is ISO27001 certified.
A.11.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes	• Reduction of risks with regard to information security • Protection of company values • Business continuity	Yes	Physical security is divided: the GoodHabitz offices and the data centre. The datacentre responsibilities have been outsourced and are monitored by OBI Automatisering to ensure compliance. The datacentre itself is ISO27001 certified.
A.11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	Yes	• Reduction of risks with regard to information security • Protection of company values • Business continuity	Yes	Physical security is divided: the GoodHabitz offices and the data centre. The datacentre responsibilities have been outsourced and are monitored by OBI Automatisering to ensure compliance. The datacentre itself is ISO27001 certified.
A.11.2.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	Yes	• Reduction of risks with regard to information security • Protection of company values • Business continuity	Yes	A formal policy has been implemented and is maintained (code of conduct).
A.11.2.5	Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization.	Yes	• Awareness • Reduction of risks with regard to information security • Protection of company values	Yes	A formal policy has been implemented and is maintained (code of conduct).
A.11.2.6	Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	Yes	• Awareness • Reduction of risks with regard to information security • Protection of company values	Yes	A formal policy has been implemented and is maintained (code of conduct).
A.11.2.7	Secure disposal or re-use of equipment	All 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.	Yes	• Reduction of risks with regard to information security • Protection of company values • Business continuity	Yes	A formal procedure has been implemented and is maintained (on-/off boarding procedure).
A.11.2.8	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	Yes	• Awareness • Reduction of risks with regard to information security • Protection of company values	Yes	A formal policy has been implemented and is maintained (code of conduct).

goodhabitz online training **Statement of Applicability ISO 27001:2013**

Annex A	Control title	Control description	In scope?	Reason (not) in scope	Implemented?	Implemented control
A.11.2.9	'Clear desk'- and 'clear screen'-policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	Yes	• Awareness • Protection of company values	Yes	A formal policy has been implemented and is maintained (code of conduct).
A.12	Operations security					
A.12.1	Operational procedures and responsibilities					
A.12.1.1	Documented operating procedures	Operating procedures shall be documented and made available to all users who need them.	Yes	• Reduction of risks with regard to information security • Protection of company values	Yes	Part of the ISMS manual.
A.12.1.2	Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	Yes	• Reduction of risks with regard to information security • Protection of company values	Yes	A change management procedure is implemented.
A.12.1.3	Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Yes	• Reduction of risks with regard to information security • Protection of company values	Yes	Performance of systems is ensured within process.
A.12.1.4	Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	Yes	• Reduction of risks with regard to information security • Protection of company values	Yes	GoodHabitz has implemented a separation between development, testing, acceptance and operational environment (OTAP).
A.12.2	Protection from malware					
A.12.2.1	Controls against mal-ware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Yes	• Awareness • Reduction of risks with regard to information security • Protection of company values • Business continuity	Yes	The SLA with OBI Automatisering describes the implemented methods, such as virus scanners, detection, monitoring, etc. Requirements are part of the supplier protocol.
A.12.3	Back-up					
A.12.3.1	Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Yes	• Protection of company values • Business continuity	Yes	GoodHabitz has an information backup policy in place. The process is outsourced to OBI Automatisering and documented in the GoodHabitz Business Continuity Plan.
A.12.4	Logging and monitoring					
A.12.4.1	Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	Yes	• Reporting purposes • Reduction of risks with regard to information security • Protection of company values • Improve continuously • Complying with laws and regulations	Yes	Procedures have been designed and are in place.
A.12.4.2	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	Yes	• Reporting purposes • Reduction of risks with regard to information security • Protection of company values • Improve continuously	Yes	Procedures have been designed and are in place.
A.12.4.3	Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	Yes	• Reporting purposes • Reduction of risks with regard to information security • Protection of company values • Improve continuously	Yes	Procedures have been designed and are in place.
A.12.4.4	Clock synchronisation	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	Yes	• Reporting purposes • Reduction of risks with regard to information security • Improve continuously	Yes	Procedures have been designed and are in place.
A.12.5	Control of operational software					
A.12.5.1	Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems	Yes	• Awareness • Reduction of risks with regard to information security • Business continuity	Yes	Procedures have been designed and are in place
A.12.6	Technical vulnerability management					
A.12.6.1	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	Yes	• Reduction of risks with regard to information security • Business continuity • Improve continuously	Yes	A regular pentesting procedure is in place. The procedure also includes prompt follow-up on vulnerabilities.
A.12.6.2	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.	Yes	• Awareness • Reduction of risks with regard to information security	Yes	A formal policy has been implemented and is maintained (code of conduct).
A.12.7	Information systems audit considerations					
A.12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	Yes	• Reduction of risks with regard to information security • Improve continuously	Yes	Procedures have been designed and are in place.
A.13	Communications security					
A.13.1	Network controls					
A.13.1.1	Management controls of network services	Networks shall be managed and controlled to protect information in systems and applications.	Yes	• Reduction of risks with regard to information security • Protection of company values • Business continuity	Yes	Procedures have been designed and are in place.
A.13.1.2	Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Yes	• Reduction of risks with regard to information security • Protection of company values • Business continuity	Yes	Procedures have been designed and are in place.

goodhabitz online training **Statement of Applicability ISO 27001:2013**

Annex A	Control title	Control description	In scope?	Reason (not) in scope	Implemented?	Implemented control
A.13.1.3	Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	Yes	• Reduction of risks with regard to information security • Protection of company values • Business continuity	Yes	Procedures have been designed and are in place.
A.13.2	Information transfer					
A.13.2.1	Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	Yes	• Basic (documentation) • Awareness • Reduction of risks with regard to information security • Protection of company values	Yes	Procedures and protocols have been designed and are in place. A formal policy has been implemented and is maintained (code of conduct).
A.13.2.2	Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.	Yes	• Basic (documentation) • Complying with laws and regulations	Yes	Procedures and protocols have been designed and are in place.
A.13.2.3	Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	Yes	• Awareness • Reduction of risks with regard to information security • Protection of company values	Yes	Procedures and protocols have been designed and are in place.
A.13.2.4	Confidentiality or non disclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	Yes	• Basic (documentation) • Protection of company values • Complying with laws and regulations	Yes	Procedures and protocols have been designed and are in place.
A.14	System acquisition, development and maintenance					
A.14.1	Security requirements of information systems					
A.14.1.1	Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	Yes	• Reduction of risks with regard to information security • Business continuity	Yes	Procedures and protocols have been designed and are in place.
A.14.1.2	Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	Yes	• Reduction of risks with regard to information security • Protection of company values	Yes	Procedures have been designed and are in place.
A.14.1.3	Protecting applications services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	Yes	• Reduction of risks with regard to information security • Protection of company values	Yes	Procedures have been designed and are in place.
A.14.2	Security in development and support processes					
A.14.2.1	Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization.	Yes	• Basic (documentation) • Reduction of risks with regard to information security	Yes	Procedures and protocols have been designed and are in place.
A.14.2.2	System change control	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	Yes	• Basic (documentation) • Reduction of risks with regard to information security	Yes	Procedures and protocols have been designed and are in place.
A.14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	Yes	• Reduction of risks with regard to information security • Business continuity	Yes	Procedures and protocols have been designed and are in place.
A.14.2.4	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	Yes	• Reduction of risks with regard to information security • Business continuity	Yes	Procedures have been designed and are in place.
A.14.2.5	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	Yes	• Reduction of risks with regard to information security • Business continuity	Yes	Procedures and protocols have been designed and are in place.
A.14.2.6	Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	Yes	• Reduction of risks with regard to information security • Business continuity	Yes	Procedures and protocols have been designed and are in place.
A.14.2.7	Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.	Yes	• Reduction of risks with regard to information security • Business continuity	Yes	Procedures have been designed and are in place.
A.14.2.8	System security testing	Testing of security functionality shall be carried out during development.	Yes	• Reduction of risks with regard to information security • Protection of company values • Business continuity	Yes	Procedures and protocols have been designed and are in place.
A.14.2.9	System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	Yes	• Reduction of risks with regard to information security • Business continuity	Yes	Procedures and protocols have been designed and are in place.
A.14.3	Test data					
A.14.3.1	Protection of test data	Test data shall be selected carefully, protected and controlled.	Yes	• Reduction of risks with regard to information security • Protection of company values	Yes	Procedures and protocols have been designed and are in place.
A.15	Supplier relationships					
A.15.1	Information security in supplier relationships					
A.15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	Yes	• Reduction of risks with regard to information security • Protection of company values • Complying with laws and regulations	Yes	Security is part of the supplier policy. All contracts and agreements of critical suppliers are reviewed periodically.
A.15.1.2	Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	Yes	• Reduction of risks with regard to information security • Protection of company values • Complying with laws and regulations	Yes	Security is part of the supplier policy. All contracts and agreements of critical suppliers are reviewed periodically.

Annex A	Control title	Control description	In scope?	Reason (not) in scope	Implemented?	Implemented control
A.15.1.3	Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	Yes	• Reduction of risks with regard to information security • Protection of company values • Complying with laws and regulations	Yes	Security is part of the supplier policy. All contracts and agreements of critical suppliers are reviewed periodically.
A.15.2	Supplier service delivery management					
A.15.2.1	Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery.	Yes	• Reduction of risks with regard to information security • Business continuity	Yes	Part of the security officers role. A supplier protocol has been designed and in place.
A.15.2.2	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re- assessment of risks.	Yes	• Reduction of risks with regard to information security • Protection of company values • Business continuity	Yes	Part of the security officers role. A supplier protocol has been designed and in place.
A.16	Information security incident management					
A.16.1	Management of information security incidents and improvements					
A.16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	Yes	• Reduction of risks with regard to information security • Improve continuously • Management commitment	Yes	A formal Information security incident management has been implemented.
A.16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	Yes	• Awareness • Reduction of risks with regard to information security • Improve continuously	Yes	All roles in the organisation have been clearly instructed to report all information security events. Part of awareness.
A.16.1.3	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	Yes	• Awareness • Reduction of risks with regard to information security • Improve continuously	Yes	All roles in the organisation have been clearly instructed to report all information security events. Part of awareness.
A.16.1.4	Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	Yes	• Reduction of risks with regard to information security • Improve continuously • Management commitment	Yes	A formal Information security incident procedure has been implemented.
A.16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Yes	• Reduction of risks with regard to information security • Improve continuously • Management commitment	Yes	A formal Information security incident procedure has been implemented.
A.16.1.6	Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	Yes	• Reduction of risks with regard to information security • Improve continuously • Management commitment	Yes	A formal Information security incident procedure has been implemented.
A.16.1.7	Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Yes	• Reduction of risks with regard to information security • Improve continuously	Yes	A formal Information security incident procedure has been implemented.
A.17	Information security continuity					
A.17.1	Planning information security continuity					
A.17.1.1	Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Yes	• Business continuity	Yes	A business continuity plan has been established. Also formal methods for the prevention of potential calamities have been implemented.
A.17.1.2	Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Yes	• Basic (documentation) • Business continuity	Yes	A business continuity plan has been established. Also formal methods for the prevention of potential calamities have been implemented.
A.17.1.3	Verify, review and evaluate information security continuity	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	Yes	• Business continuity • Improve continuously	Yes	Business continuity plans are tested and updated periodically.
A.17.2	Redundancies					
A.17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Yes	• Business continuity	Yes	A business continuity plan has been established. Also formal methods for the prevention of potential calamities have been implemented.
A.18	Compliance					
A.18.1	Compliance with legal and contractual requirements					
A.18.1.1	Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	Yes	• Complying with laws and regulations	Yes	All relevant statutory, regulatory and contractual requirements have been identified, documented are kept up to date.
A.18.1.2	Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	Yes	• Complying with laws and regulations	Yes	Procedures for the protection of intellectual property rights has been implemented.
A.18.1.3	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.	Yes	• Complying with laws and regulations	Yes	Procedures for the protection of organisational records have been implemented.

Annex A	Control title	Control description	In scope?	Reason (not) in scope	Implemented?	Implemented control
A.18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	Yes	• Complying with laws and regulations	Yes	Formal policies to protect data and privacy according to relevant legislation, regulations and contractual clauses have been implemented.
A.18.1.5	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations	Yes	• Complying with laws and regulations	Yes	Implemented cryptographic controls are a subject to relevant laws and regulations.
A.18.2	Information security reviews					
A.18.2.1	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	Yes	• Basic (documentation) • Improve continuously	Yes	A formal audit plan and audit procedures have been implemented.
A.18.2.2	Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	Yes	• Improve continuously • Management commitment	Yes	A formal audit plan and audit procedures have been implemented.
A.18.2.3	Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	Yes	• Basic (documentation) • Improve continuously • Complying with laws and regulations	Yes	A formal audit plan and audit procedures have been implemented.