goodhabitz online training

Annex A	Control title	Control description	In scope?	Reason (not) in scope	Implemented?	Implemented control

Statement of Applicability ISO 27001:2022

Statement of Applicability ISO 27701:2019 (below)

Annex A	Control title	Control description	In scope?	Reason (not) in scope	Implemented?	Implemented control
A.5	Organizational controls					
A.5.1	Policies for information security	Information security policy and topic-specific policies shall 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	• Basic (documentation) • Awareness • Management commitment	Yes	A formal information security policy has been implemented.
A.5.2	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	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.5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	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.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 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.5.5	Contact with authorities	The organization shall establish and maintain contact with relevant authorities.	Yes	• Requirments of authorities	Yes	Management actively engages with relevant authorities, such as regulatory bodies and law enforcement, to stay informed on legal requirements and cybersecurity threats.
A.5.6	Contact with special interest groups	The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Yes	• Requirments of authorities	Yes	We maintain active participation in professional associations and special interest groups to stay updated on emerging threats, best practices, and industry standards.
A.5.7	Threat intelligence	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	Yes	• Awareness • Reduction of risks with regard to information security • Protection of company values • Business continuity	Yes	Vulnerability-, threat-, update- and incident response policies are in place.

Annex A	Control title	Control description	In scope?	Reason (not) in scope	Implemented?	Implemented control
A.5.8	Information security in project management	Information security shall be integrated into project management.	Yes	• Reduction of risks with regard to information security • Protection of company values	Yes	Security by design is integrated into project management process.
A.5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained.	Yes	• Reduction of risks with regard to information security • Protection of company values	Yes	A formal asset management policy as well as an autorisation matrix have been implemented and are maintained.
A.5.10	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	Yes	• Reduction of risks with regard to information security • Protection of company values	Yes	A Code of Conduct has been implemented.
A.5.11	Return of assets	Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or 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.5.12	Classification of information	Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	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.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 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.5.14	Information transfer	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	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.5.15	Access control	Rules to control physical and logical access to information and other associated assets shall be established and implemented 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.5.16	Identity management	The full life cycle of identities shall be managed.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Procedures for the protection of identities have been implemented.
A.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.	Yes	• Awareness • Reduction of risks with regard to information security	Yes	Access and authorisation procedures have been implemented.

Annex A	Control title	Control description	In scope?	Reason (not) in scope	Implemented?	Implemented control
A.5.18	Access rights	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Access and authorisation procedures have been implemented.
A.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.	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.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.	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.5.21	Managing information security in the information and communication technology (ICT) supplychain	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services 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.5.22	Monitoring, review and change management of supplier services	The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Yes	• Reduction of risks with regard to information security • Protection of company values • Business continuity	Yes	A supplier protocol has been designed and in place.
A.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 organization's information security requirements.	Yes	• Reduction of risks with regard to information security • Protection of company values • Business continuity • Improve continuously	Yes	Business Impact Analysis including security checks and Vulnerability scanning procedures are in place
A.5.24	Information security incident management planning and preparation	The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	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.5.25	Assessment and decision on information security events	The organization shall assess information security events and decide if they are to be categorized 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.5.26	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.

Annex A	Control title	Control description	In scope?	Reason (not) in scope	Implemented?	Implemented control
A.5.27	Learning from information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	Yes	• Reduction of risks with regard to information security • Improve continuously • Management commitment	Yes	A formal Information security incident procedure has been implemented.
A.5.28	Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Yes	• Reduction of risks with regard to information security • Improve continuously	Yes	A formal Information security incident procedure has been implemented.
A.5.29	Information security during disruption	The organization shall plan how to maintain information security at an appropriate level during disruption.	Yes	• Improve continuously • Management commitment • Business continuity	Yes	GoodHabitz has an information backup policy in place. The process is part of the GoodHabitz Business Continuity Plan.
A.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.	Yes	• Improve continuously • Management commitment • Business continuity	Yes	Goodhabitz Periodically conducts BCP tests
A.5.31	Legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	Yes	• Complying with laws and regulations	Yes	All relevant statutory, regulatory and contractual requirements have been identified, documented are kept up to date.
A.5.32	Intellectual property rights	The organization shall implement appropriate procedures to protect intellectual property rights.	Yes	• Complying with laws and regulations	Yes	Procedures for the protection of intellectual property rights has been implemented.
A.5.33	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Yes	• Complying with laws and regulations	Yes	Procedures for the protection of intellectual property rights has been implemented.
A.5.34	Privacy and protection of personal identifiable information (PII)	The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	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.5.35	Independent review of information security	The organization's approach to managing information security and its implementation including people, processes and technologies 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.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 shall be regularly reviewed.	Yes	• Improve continuously • Management commitment	Yes	A formal audit plan and audit procedures have been implemented.

Annex A	Control title	Control description	In scope?	Reason (not) in scope	Implemented?	Implemented control
A.5.37	Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	Yes	• Reduction of risks with regard to information security • Protection of company values	Yes	Part of the ISMS manual.
A.6	People controls					
A.6.1	Screening	Background verification checks on all candidates to become personnel shall 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	• 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.6.2	Terms and conditions of employment	The employment contractual agreements shall state the personnel's 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.6.3	Information security awareness, education and training	Personnel of the organization and relevant interested parties shall 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	• 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 'onboarding' is in place and explicitly linked to awareness instruction.
A.6.4	Disciplinary process	A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	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.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.	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.6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Yes	• Basic (documentation) • Protection of company values • Complying with laws and regulations	Yes	Procedures and protocols have been designed and are in place.
A.6.7	Remote working	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Yes	• Awareness • Reduction of risks with regard to information security • Improve continuously	Yes	Procedures and protocols have been designed and are in place.

Annex A	Control title	Control description	In scope?	Reason (not) in scope	Implemented?	Implemented control
A.6.8	Information security event reporting	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	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.7	Physical controls					
A.7.1	Physical security perimeters	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	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 itself is ISO27001 certified.
A.7.2	Physical entry	Secure areas shall be protected by appropriate entry controls and access points.	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 itself is ISO27001 certified.
A.7.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and implemented.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Physical security measures for GoodHabitz offices are applied.
A.7.4	Physical security monitoring	Premises shall be continuously monitored for unauthorized physical access.	Yes	• Reduction of risks with regard to information security • Protection of business values • Awareness	Yes	Staffed reception at HQ and securely lockable local sales offices
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 shall be designed and implemented.	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 itself is ISO27001 certified.
A.7.6	Working in secure areas	Security measures for working in secure areas shall be designed and implemented.	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.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.	Yes	• Awareness • Protection of company values	Yes	A formal policy has been implemented and is maintained (code of conduct).
A.7.8	Equipment siting and protection	Equipment shall be sited securely and protected.	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 itself is ISO27001 certified.

Annex A	Control title	Control description	In scope?	Reason (not) in scope	Implemented?	Implemented control
A.7.9	Security of assets off-premises	Off-site assets shall be protected.	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.7.10	Storage media	Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Yes	• Awareness • Reduction of risks with regard to information security • Protection of company values	Yes	A formal policy has been implemented and is maintained.
A.7.11	Supporting utilities	Information processing facilities 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 itself is ISO27001 certified.
A.7.12	Cabling security	Cables carrying power, 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 itself is ISO27001 certified.
A.7.13	Equipment maintenance	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	Yes	• Reduction of risks with regard to information security • Protection of company values • Business continuity	Yes	Update policy is place.
A.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.	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.8	Technological controls					
A.8.1	User end point devices	Information stored on, processed by or accessible via user end point devices shall be protected.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Password procedures in place. Devices are equiped with malware protection and data encryption.
A.8.2	Privileged access rights	The allocation and use of privileged access rights shall be restricted and managed.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Access and authorisation procedures have been implemented.
A.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.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Access and authorisation procedures have been implemented.

Annex A	Control title	Control description	In scope?	Reason (not) in scope	Implemented?	Implemented control
A.8.4	Access to source code	Read and write access to source code, development tools and software libraries shall be appropriately managed.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Access and authorisation procedures have been implemented.
A.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.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Access and authorisation procedures have been implemented.
A.8.6	Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Performance of systems is ensured within process.
A.8.7	Protection against malware	Protection against malware shall be implemented and supported by 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.8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	Yes	• Reduction of risks with regard to information security • Business continuity • Improve continuously	Yes	A pentesting procedure is in place. The procedure also includes prompt follow-up on vulnerabilities.
A.8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	Yes	• Reduction of risks with regard to information security • Business continuity • Improve continuously	Yes	Code scanning software and technically enforced measures
A.8.10	Information deletion	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	Yes	• Complying with laws and regulations	Yes	At end of storage period the data of students is anonymized. For employees data deletion periods exist.
A.8.11	Data masking	Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	A policy for the use of cryptographic controls has been implemented.
A.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.	Yes	• Protection of company values • Business continuity • Reduction of risks with regard to information security	Yes	Role based access and technically enforced measures.

Annex A	Control title	Control description	In scope?	Reason (not) in scope	Implemented?	Implemented control
A.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.	Yes	• Protection of company values • Business continuity	Yes	GoodHabitz has an information backup policy in place. The process is part of the GoodHabitz Business Continuity Plan.
A.8.14	Redundancy 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.8.15	Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	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.8.16	Monitoring activities	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	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.8.17	Clock synchronization	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	Yes	• Reporting purposes • Reduction of risks with regard to information security • Improve continuously	Yes	Procedures have been designed and are in place.
A.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.	Yes	• Reduction of risks with regard to information security • Protection of business values	Yes	Access and authorisation procedures have been implemented.
A.8.19	Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation 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.8.20	Networks security	Networks and network devices shall be secured, 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.8.21	Security of network services	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	Yes	• Reduction of risks with regard to information security • Protection of company values • Business continuity	Yes	Procedures have been designed and are in place.

Annex A	Control title	Control description	In scope?	Reason (not) in scope	Implemented?	Implemented control
A.8.22	Segregation of networks	Groups of information services, users and information systems shall be segregated in the organization's 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.8.23	Web filtering	Access to external websites shall be managed to reduce exposure to malicious content.	Yes	• Awareness • Reduction of risks with regard to information security	Yes	Code of conduct in place
A.8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined 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.8.25	Secure development life cycle	Rules for the secure development of software and systems shall be established and applied.	Yes	• Basic (documentation) • Reduction of risks with regard to information security	Yes	Secure development procedures and protocols have been designed and are in place.
A.8.26	Application security requirements	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	Yes	• Reduction of risks with regard to information security • Protection of company values	Yes	Procedures have been designed and are in place.
A.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.	Yes	• Reduction of risks with regard to information security • Business continuity	Yes	Secure development procedures and protocols have been designed and are in place.
A.8.28	Secure coding	Secure coding principles shall be applied to software development.	Yes	• Reduction of risks with regard to information security • Business continuity	Yes	Secure development procedures and protocols have been designed and are in place.
A.8.29	Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development life cycle.	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.8.30	Outsourced development	The organization shall direct, monitor and review the activities related to outsourced system development.	Yes	• Reduction of risks with regard to information security • Business continuity	Yes	Procedures have been designed and are in place.

Annex A	Control title	Control description	In scope?	Reason (not) in scope	Implemented?	Implemented control
A.8.31	Separation of development, test and production environments	Development, testing and production environments shall be separated and secured.	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.8.32	Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.	Yes	• Reduction of risks with regard to information security • Protection of company values	Yes	A change management procedure is implemented.
A.8.33	Test information	Test information shall be appropriately selected, protected and managed.	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.8.34	Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	Yes	• Reduction of risks with regard to information security • Improve continuously	Yes	Procedures have been designed and are in place.

Statement of Applicability ISO 27701:2019

Annex A	Control title	Control description	In scope?	Reason (not) in scope	Implemented?	Implemented control
A.7.2	Conditions for collection and processing					
A.7.2.1	Identify and document purpose	The organization shall identify and document the specific purposes for which the PII will be processed.	Yes	• Complying with laws and regulations	Yes	Privacy notices (general privacy notice; privacy notice Learning Platform; Privacy Notice Employees), Monday board (Register of processing activities)