Company Name: AIMMS B.V.
ISO27001 Scope: Development, maintenance, deliv
Version: 3.0
Date: 8/13/2024

Nr.	Chapter	Topic
5.1	Organizational controls	Policies for information security
5.2	Organizational controls	Information security roles and responsibilities
5.3	Organizational controls	Segregation of duties
5.4	Organizational controls	Management responsibilities
5.5	Organizational controls	Contact with authorities
5.6	Organizational controls	Contact with special interest groups
5.7	Organizational controls	Threat intelligence
5.8	Organizational controls	Information security in project management
5.9	Organizational controls	Inventory of information and other associated assets
5.10	Organizational controls	Acceptable use of information and other associated assets
5.11	Organizational controls	Return of assets
5.12	Organizational controls	Classification of information
5.13	Organizational controls	Labelling of information
5.14	Organizational controls	Information transfer

5.15	**Organizational controls**	**Access control**
5.16	**Organizational controls**	**Identity management**
5.17	**Organizational controls**	**Authentication information**
5.18	**Organizational controls**	**Access rights**
5.19	**Organizational controls**	**Information security in supplier relationships**
5.20	**Organizational controls**	**Addressing information security within supplier agreements**
5.21	**Organizational controls**	**Managing information security in the information and communication technology (ICT) supply chain**
5.22	**Organizational controls**	**Monitoring, review and change management of supplier services**
5.23	**Organizational controls**	**Information security for use of cloud services**
5.24	**Organizational controls**	**Information security incident management planning and preparation**
5.25	**Organizational controls**	**Assessment and decision on information security events**
5.26	**Organizational controls**	**Response to information security incidents**
5.27	**Organizational controls**	**Learning from information security incidents**
5.28	**Organizational controls**	**Collection of evidence**
5.29	**Organizational controls**	**Information security during disruption**
5.30	**Organizational controls**	**ICT readiness for business continuity**
5.31	**Organizational controls**	**Legal, statutory, regulatory and contractual requirements**
5.32	**Organizational controls**	**Intellectual property rights**

5.33	Organizational controls	Protection of records
5.34	Organizational controls	Privacy and protection of personal identifiable information (PII)
5.35	Organizational controls	Independent review of information security
5.36	Organizational controls	Compliance with policies, rules and standards for information security
5.37	Organizational controls	Documented operating procedures
6.1	People controls	Screening
6.2	People controls	Terms and conditions of employment
6.3	People controls	Information security awareness, education and training
6.4	People controls	Disciplinary process
6.5	People controls	Responsibilities after termination or change of employment
6.6	People controls	Confidentiality or non-disclosure agreements
6.7	People controls	Remote working
6.8	People controls	Information security event reporting
7.1	Physical controls	Physical security perimeters
7.2	Physical controls	Physical entry
7.3	Physical controls	Securing offices, rooms and facilities
7.4	Physical controls	Physical security monitoring

7.5	**Physical controls**	**Protecting against physical and environmental threats**
7.6	**Physical controls**	**Working in secure areas**
7.7	**Physical controls**	**Clear desk and clear screen**
7.8	**Physical controls**	**Equipment siting and protection**
7.9	**Physical controls**	**Security of assets off-premises**
7.10	**Physical controls**	**Storage media**
7.11	**Physical controls**	**Supporting utilities**
7.12	**Physical controls**	**Cabling security**
7.13	**Physical controls**	**Equipment maintenance**
7.14	**Physical controls**	**Secure disposal or re-use of equipment**
8.1	**Technological controls**	**User endpoint devices**
8.2	**Technological controls**	**Privileged access rights**
8.3	**Technological controls**	**Information access restriction**
8.4	**Technological controls**	**Access to source code**
8.5	**Technological controls**	**Secure authentication**
8.6	**Technological controls**	**Capacity management**
8.7	**Technological controls**	**Protection against malware**
8.8	**Technological controls**	**Management of technical vulnerabilities**
8.9	**Technological controls**	**Configuration management**
8.10	**Technological controls**	**Information deletion**
8.11	**Technological controls**	**Data masking**

8.12	Technological controls	Data leakage prevention
8.13	Technological controls	Information backup
8.14	Technological controls	Redundancy of information processing facilities
8.15	Technological controls	Logging
8.16	Technological controls	Monitoring activities
8.17	Technological controls	Clock synchronization
8.18	Technological controls	Use of privileged utility programs
8.19	Technological controls	Installation of software on operational systems
8.20	Technological controls	Networks security
8.21	Technological controls	Security of network services
8.22	Technological controls	Segregation in networks
8.23	Technological controls	Web filtering
8.24	Technological controls	Use of cryptography
8.25	Technological controls	Secure development lifecycle
8.26	Technological controls	Application security requirements
8.27	Technological controls	Secure system architecture and engineering principles
8.28	Technological controls	Secure coding
8.29	Technological controls	Security testing in development and acceptance
8.30	Technological controls	Outsourced development
8.31	Technological controls	Separation of development, test and production environments
8.32	Technological controls	Change management
8.33	Technological controls	Test information

8.34	**Technological controls**	**Protection of information systems during audit testing**

Stateme

very and support of software products and cloud services for analytics

Control
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.
Information security roles and responsibilities shall be defined and allocated according to the organization needs.
Conflicting duties and conflicting areas of responsibility shall be segregated.
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.
The organization shall establish and maintain contact with relevant authorities.
The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.
Information relating to information security threats shall be collected and analysed to produce threat intelligence.
Information security shall be integrated into project management.
An inventory of information and other associated assets, including owners, shall be developed and maintained.
Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.
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.
Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.
An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information clas sification scheme adopted by the organization.
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.

Rules to control physical and logical access to information and other associated assets shall be established and implemented based on busi ness and information security requirements.
The full life cycle of identities shall be managed.
Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.
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.
Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.
Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.
Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.
The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.
Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.
The organization shall plan and prepare for managing information secu rity incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.
The organization shall assess information security events and decide if they are to be categorized as information security incidents.
Information security incidents shall be responded to in accordance with the documented procedures.
Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.
The organization shall establish and implement procedures for the iden tification, collection, acquisition and preservation of evidence related to information security events.
The organization shall plan how to maintain information security at an appropriate level during disruption.
ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity 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.
The organization shall implement appropriate procedures to protect intellectual property rights.

Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.
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.
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.
Compliance with the organization’s information security policy, topic-specific policies, rules and standards shall be regularly reviewed.
Operating procedures for information processing facilities shall be documented and made available to personnel who need them.
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.
The employment contractual agreements shall state the personnel’s and the organization’s responsibilities for information security.
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.
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.
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.
Confidentiality or non-disclosure agreements reflecting the organ ization’s needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.
Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization’s premises.
The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.
Security perimeters shall be defined and used to protect areas that contain information and other associated assets.
Secure areas shall be protected by appropriate entry controls and access points.
Physical security for offices, rooms and facilities shall be designed and implemented.
Premises shall be continuously monitored for unauthorized physical access.

Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.
Security measures for working in secure areas shall be designed and implemented.
Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.
Equipment shall be sited securely and protected.
Off-site assets shall be protected.
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.
Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.
Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.
Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.
Items of equipment containing storage media shall be verified to en sure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
Information stored on, processed by or accessible via user end point devices shall be protected.
The allocation and use of privileged access rights shall be restricted and managed.
Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.
Read and write access to source code, development tools and software libraries shall be appropriately managed.
Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.
The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.
Protection against malware shall be implemented and supported by appropriate user awareness.
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.
Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.
Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.
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.

Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.
Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.
Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.
Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.
Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential infor mation security incidents.
The clocks of information processing systems used by the organization shall be synchronized to approved time sources.
The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.
Procedures and measures shall be implemented to securely manage software installation on operational systems.
Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.
Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.
Groups of information services, users and information systems shall be segregated in the organization’s networks.
Access to external websites shall be managed to reduce exposure to malicious content.
Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.
Rules for the secure development of software and systems shall be established and applied.
Information security requirements shall be identified, specified and approved when developing or acquiring applications.
Principles for engineering secure systems shall be established, docu mented, maintained and applied to any information system development activities.
Secure coding principles shall be applied to software development.
Security testing processes shall be defined and implemented in the development life cycle.
The organization shall direct, monitor and review the activities related to outsourced system development.
Development, testing and production environments shall be separated and secured.
Changes to information processing facilities and information systems shall be subject to change management procedures.
Test information shall be appropriately selected, protected and managed.

Audit tests and other assurance activities involving assessment of op erational systems shall be planned and agreed between the tester and appropriate management.

ent of Applicability (SoA)
ISO27001

Control included?	Primary reason for inclusion
Yes	Best Practice
Yes	Best Practice
Yes	Best Practice
Yes	Best Practice
Yes	Best Practice
Yes	Best Practice
Yes	Best Practice
Yes	Best Practice
Yes	Best Practice
Yes	Best Practice
Yes	Best Practice
Yes	Best Practice
Yes	Best Practice
Yes	Risk Analysis

Yes	Best Practice
Yes	Risk Analysis
Yes	Best Practice
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Best Practice
Yes	Best Practice
Yes	Risk Analysis
Yes	Best Practice
Yes	Best Practice
Yes	Best Practice
Yes	Risk Analysis
Yes	Regulatory Compliance
Yes	Best Practice

Yes	Best Practice
Yes	Regulatory Compliance
Yes	Risk Analysis
Yes	Best Practice
Yes	Best Practice
Yes	Risk Analysis
Yes	Best Practice
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Best Practice
Yes	Best Practice
Yes	Best Practice
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis

Yes	Risk Analysis
Yes	Risk Analysis
Yes	Best Practice
Yes	Risk Analysis
Yes	Best Practice
Yes	Best Practice
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Best Practice
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Best Practice
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis

Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Best Practice
Yes	Best Practice
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis
No	
Yes	Risk Analysis
Yes	Best Practice
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis
Yes	Risk Analysis

Yes	Best Practice

Motivation for exclusion

Web filtering is not implemented due to the decentralized structure of our workforce, with employees operating from various locations without a centralized firewall. To mitigate the potential threat of malicious content, each device is secured with Microsoft Defender, which actively detects and blocks known malware that could be inadvertently downloaded. Consequently, the perceived added value of deploying web filtering software across all devices is low, and AIMMS has decided not to pursue its implementation.

Control	implemented?
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes
	Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes


Yes

Control included?	*“Is the control included in our management system and within*
Yes	*"The control is included in our management system and is therefor*
No	*"The control is excluded from our management system and is there*

Primary reason for inclusion	*“What is the main reason for the control to be included?”*
Regulatory Compliance	*"The control is mandatory under applicable law".*
Contractual Compliance	*"We have contractually agreed to implement the control with a cus*
Best Practice	*"The control is a recognized standard within the information securi*
Risk Analysis	*"The control is needed to mitigate an identified risk as determined*

Motivation for exclusion “Why is the control excluded?”

Free format answer based on the specific situation.

Control implemented?	*“Is the control implemented within our organization?”*
Yes	*"The control is fully implemented within our organization".*
Partially	*"Parts of the control are implemented within our organization".*
No	*"The control is not (yet) implemented within our organization".*

Explanation for partially implemented controls

Free format answer to further explain why a control is only partially implemented.

ty and/or privacy realm to mitigate commonly known and shared information security and/or privacy risks".