STATEMENT OF APPLICABILITY

ISO27001:2022 V1.2 06/03/2025

TABLE OF CONTENTS

INTRODUCTION

This document contains the Statement of Applicability (SAT) for certification to the ISO 27001 standard. The purpose of this document is to identify the applicable control measures that must be implemented to monitor and manage threats to Scope4mation BV and its business processes.

The applicable control measures are identified based on the control measures specified in Annex 1 of ISO 27001. For the applicable control measure, please refer to the defined ISO 27002 best practices guidelines, which are specifically designed for application in Scope4mation BV business processes. If a control measure is not applicable, an explanation is provided.

MANAGEMENT STATEMENT

The Management of Scope4mation BV hereby declares that the measures stated in this VVT have been ratified in relation to the risk analyses performed and accepts the residual risk of any measures not taken.

Ede, 01/11/2025,

JAC Ale

SCOPE

Development, installation and support of data integration software based on SaaS and on-premise.

VERSION

The current version is V1.2

STATEMENT OF APPLICABILITY

5 ORGANIZATIONAL CONTROL MEASURES

Standard	Description	Control measure	Relevant and implemented	Justification for exclusion	Basis RB: Risk assessment WG: Legislation CV: Contractual Obligation
5.1	Information security policy rules	Information security policies and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and stakeholders, and reviewed at planned intervals or as significant changes occur.	Yes		☒RB ☒WG ☒CV
5.2	Roles and responsibilities in information security	Roles and responsibilities in information security should be defined and assigned according to the needs of the organization	Yes		☒RB ☐WG ☐CV
5.3	Separation of duties	Conflicting tasks and conflicting responsibilities must be separated.	Yes		☒RB ☐WG ☐CV
5.4	Management responsibilities	Management must require all personnel to implement information security practices in accordance with the organization's established information security policy, subject-specific policies, and procedures.	Yes		☒RB ☐WG ☐CV
5.5	Contact with government agencies	The organization must establish and maintain contact with the relevant authorities.	Yes		☒RB ☐WG ☐CV
5.6	Contact with special interest groups	The organization shall establish and maintain contacts with special interest groups or other specialized security forums and professional associations.	Yes		☒RB ☐WG ☐CV
5.7	Threat information and analysis	Information related to information security threats must be collected and analyzed to produce threat intelligence and analysis.	Yes		☒RB ☐WG ☐CV
5.8	Information security in project management	Information security must be integrated into project management.	Yes		☒RB ☐WG ☐CV
5.9	Inventory of information and other related assets	An inventory list of information and other related assets, including their owners, shall be established and maintained.	Yes		☒RB ☐WG ☐CV
5.10	Acceptable use of information and other related assets	Rules for the acceptable use of and procedures for handling information and other related assets shall be established, documented and implemented.	Yes		☒RB ☐WG ☐CV
5.11	Return of company assets	Employees and other stakeholders, as the case may be, must return all organizational assets in their possession upon termination of their employment, contract, or agreement.	Yes		☒RB ☐WG ☐CV
5.12	Classifying information	Information should be classified according to the information security needs of the organization, based on the requirements for confidentiality, integrity, availability and relevant stakeholders.	Yes		☒RB ☐WG ☐CV
5.13	Labeling information	For labelling information, an appropriate set of procedures shall be established and implemented in accordance with the information classification scheme established by the organization.	Yes		☒RB ☐WG ☐CV
5.14	Transferring information	Information transfer rules, procedures or agreements must be established for all types of transfer within the organization and between the organization and other parties.	Yes		☒RB ☐WG ☐CV
Standard	**Description**	**Control measure**	**Relevant and implemented**	**Justification for exclusion**	**Basis** RB: Risk assessment WG: Legislation CV: Contractual Obligation
5.15	Access security	Rules based on business and information security requirements must be established and implemented to	Yes		☒RB ☐WG

		control physical and logical access to information and other related assets.			☐CV
5.16	Identity management	The entire lifecycle of identities needs to be managed.	Yes		☒RB ☐WG ☐CV
5.17	Managing authentication information	The assignment and management of authentication information must be controlled through a management process that includes educating personnel on the appropriate way to handle authentication information.	Yes		☒RB ☐WG ☐CV
5.18	Access rights	Access rights to information and other related assets must be granted, reviewed, modified, and removed in accordance with the organization's subject-specific access security policies and rules.	Yes		☒RB ☐WG ☐CV
5.19	Information security in supplier relationships	Processes and procedures must be established and implemented to manage information security risks associated with the use of the supplier's products or services.	Yes		☒RB ☐WG ☐CV
5.20	Addressing information security in supplier agreements	Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.	Yes		☒RB ☐WG ☐CV
5.21	Managing information security in the ICT chain	Processes and procedures must be established and implemented to manage information security risks associated with the supply chain of ICT products and services.	Yes		☒RB ☐WG ☐CV
5.22	Monitoring, assessing and managing changes to supplier services	The organization shall regularly monitor, assess, evaluate and manage changes to its information security practices and vendor services.	Yes		☒RB ☐WG ☐CV
5.23	Information security for the use of cloud services	Processes for purchasing, using, managing, and terminating cloud services must be established in accordance with the organization's information security requirements.	Yes		☒RB ☐WG ☐CV
5.24	Planning and preparing for information security incident management	The organization must plan for and prepare for managing information security incidents by defining, establishing and communicating processes, roles and responsibilities for information security incident management.	Yes		☒RB ☐WG ☐CV
5.25	Assessing and deciding on information security events	The organization must assess information security events and decide whether they should be categorized as information security incidents.	Yes		☒RB ☐WG ☐CV
5.26	Responding to information security incidents	Information security incidents must be responded to in accordance with documented procedures.	Yes		☒RB ☐WG ☐CV
5.27	Learning from information security incidents	Knowledge gained from information security incidents should be used to strengthen and improve information security controls.	Yes		☒RB ☐WG ☐CV
5.28	Collecting evidence	The organization shall establish and implement procedures for identifying, collecting, obtaining, and preserving evidence related to information security events.	Yes		☒RB ☐WG ☐CV
5.29	Information security during a disruption	The organization must make plans to ensure information security at the appropriate level during a disruption.	Yes		☒RB ☐WG ☐CV
5.30	ICT readiness for business continuity	ICT readiness must be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Yes		☒RB ☐WG ☒CV
Standard	**Description**	**Control measure**	**Relevant and implemented**	**Justification for exclusion**	**Basis** **RB: Risk assessment** **WG: Legislation** **CV: Contractual Obligation**
5.31	Legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meeting these requirements must be identified, documented and kept up to date.	Yes		☒RB ☒WG ☒CV
5.32	Intellectual property rights	The organization shall implement appropriate procedures to protect intellectual property rights.	Yes		☒RB ☒WG ☒CV
5.33	Protecting registrations	Records must be protected from loss, destruction, falsification, unauthorized access, and unauthorized disclosure.	Yes		☒RB ☒WG ☐CV

5.34	Privacy and protection of personal data	The organization shall identify and meet requirements related to the maintenance of privacy and the protection of personal data in accordance with applicable laws, regulations and contractual requirements.	Yes		☒RB ☒WG ☒CV
5.35	Independent assessment of information security	The organization's approach to information security management and its implementation, including people, processes and technologies, should be assessed independently and at planned intervals or as significant changes occur.	Yes		☒RB ☐WG ☐CV
5.36	Compliance with information security policies, rules and standards	Compliance with the organization's information security policy, subject-specific policies, rules, and standards should be assessed regularly.	Yes		☒RB ☐WG ☐CV
5.37	Documented operating procedures	Operating procedures for information processing facilities should be documented and made available to personnel who need them.	Yes		☒RB ☐WG ☐CV

6 HUMAN-ORIENTED MEASURES

Standard	Description	Control measure	Relevant and implemented	Justification for exclusion	Basis RB: Risk assessment WG: Legislation CV: Contractual Obligation
6.1	Screening	The background of all candidates considered for positions within the organization must be checked before they begin employment and periodically thereafter. This check must take into account applicable laws, regulations, and ethical considerations, and must be proportionate to business requirements, the classification of the information being accessed, and the identified risks.	Yes		☒RB ☐WG ☒CV
6.2	Employment contract	Employment contracts should specify the responsibilities of personnel and the organization regarding information security.	Yes		☒RB ☐WG ☐CV
6.3	Awareness, education and training in information security	The organization's personnel and relevant stakeholders should receive appropriate information security awareness, education, training and refresher courses and regular updates on the organization's information security policy, subject-specific policies and procedures as relevant to their roles.	Yes		☒RB ☐WG ☐CV
6.4	Disciplinary procedure	There should be a formal and communicated disciplinary procedure to take action against staff and other stakeholders who have committed a breach of the information security policy.	Yes		☒RB ☐WG ☐CV
6.5	Responsibilities after termination or change of employment	Information security responsibilities and duties that continue after termination or change of employment should be defined, maintained, and communicated to relevant personnel and other stakeholders.	Yes		☒RB ☐WG ☐CV
6.6	Confidentiality or non-disclosure agreements	Information related to information security threats must be collected and analyzed to produce threat intelligence and analysis.	Yes		☒RB ☐WG ☐CV
6.7	Working remotely	When employees work remotely, security measures should be implemented to protect information that is accessed, processed, or stored outside the organization's building and/or premises.	Yes		☒RB ☐WG ☐CV
6.8	Reporting information security events	The organization shall provide a mechanism for personnel to report observed or suspected information security events in a timely manner through appropriate channels.	Yes		☒RB ☐WG ☐CV

7 PHYSICAL CONTROL MEASURES

Standard	Description	Control measure	Relevant and implemented	Justification for exclusion	Basis RB: Risk assessment WG: Legislation CV: Contractual Obligation
7.1	Physical security zones	Zones containing information and other related assets must be protected by defining and using security zones.	Yes		☒RB ☐WG ☐CV
7.2	Physical access security	Secure areas must be protected by appropriate access controls and access points.	Yes		☒RB ☐WG ☐CV
7.3	Securing offices, spaces and facilities	Physical security must be designed and implemented for offices, spaces and facilities.	Yes		☒RB ☐WG ☐CV
7.4	Monitoring physical security	The building and grounds must be continuously monitored for unauthorized physical access.	Yes		☒RB ☐WG ☐CV
7.5	Protect against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to the infrastructure, must be designed and implemented.	Yes		☒RB ☐WG ☐CV
7.6	Working in secured zones	When working in secured areas, security measures must be developed and implemented.	Yes		☒RB ☐WG ☐CV
7.7	'Clear desk' and 'clear screen'	Clear desk rules for paper documents and removable storage media and clear screen rules for information processing facilities should be defined and implemented appropriately.	Yes		☒RB ☐WG ☐CV
7.8	Placing and protecting equipment	Equipment must be safely placed and protected.	Yes		☒RB ☐WG ☐CV
7.9	Securing company assets off-site	Assets outside the building and/or grounds must be protected.	Yes		☒RB ☐WG ☐CV
7.10	Storage media	Storage media must be managed throughout their entire life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Yes		☒RB ☐WG ☐CV
7.11	Utilities	Information processing facilities must be protected from power outages and other disruptions caused by utility failures.	Yes		☒RB ☐WG ☐CV
7.12	Securing cabling	Power supply cables and cables for transmitting data or supporting information services must be protected against interception, interference or damage.	Yes		☒RB ☐WG ☐CV
7.13	Equipment maintenance	Equipment must be properly maintained to ensure the availability, integrity and reliability of information.	Yes		☒RB ☐WG ☐CV
7.14	Safe disposal or reuse of equipment	Parts of the equipment containing storage media must be checked to ensure that sensitive data and licensed software have been removed or securely overwritten before disposal or reuse.	Yes		☒RB ☐WG ☐CV

8 TECHNOLOGICAL CONTROLS

Standard	Description	Control measure	Relevant and implemented	Justification for exclusion	Basis RB: Risk assessment WG: Legislation CV: Contractual Obligation
8.1	User endpoint devices	Information stored on, processed by, or accessed through user endpoint devices must be protected.	Yes		☒RB ☐WG ☐CV
8.2	Special access rights	The assignment and use of special access rights should be restricted and managed.	Yes		☒RB ☐WG ☐CV
8.3	Restricting access to information	Access to information and other related assets must be restricted in accordance with established subject-specific access security policies.	Yes		☒RB ☐WG ☐CV
8.4	Access protection on source code	Read and write access to source code, development tools, and software libraries must be appropriately managed.	Yes		☒RB ☐WG ☐CV
8.5	Secure authentication	Secure authentication technologies and procedures should be implemented based on information access restrictions and subject-specific or additional access security policies.	Yes		☒RB ☐WG ☐CV
8.6	Capacity management	The use of resources must be monitored and adjusted in accordance with current and expected capacity requirements.	Yes		☒RB ☐WG ☐CV
8.7	Malware protection	Malware protection must be implemented and supported by appropriate user awareness.	Yes		☒RB ☐WG ☐CV
8.8	Technical Vulnerability Management	Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be assessed, and appropriate measures should be taken.	Yes		☒RB ☐WG ☐CV
8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks must be identified, documented, implemented, monitored and assessed.	Yes		☒RB ☐WG ☐CV
8.10	Erasing information	Information stored in information systems, devices or other storage media must be erased when it is no longer needed.	Yes		☒RB ☐WG ☐CV
8.11	Masking data	Data must be masked in accordance with the organization's subject-specific access security policy and other related subject-specific policies and business requirements, taking into account applicable law.	Yes		☒RB ☒WG ☐CV
8.12	Data leakage prevention	Measures to prevent data leaks must be applied to systems, networks and other devices on or through which sensitive information is processed, stored or transported.	Yes		☒RB ☐WG ☐CV
8.13	Backing up information	Backups of information, software, and systems must be maintained and regularly tested in accordance with agreed-upon, subject-specific backup policies.	Yes		☒RB ☐WG ☐CV
8.14	Redundancy of information processing facilities	Information processing facilities should be implemented with sufficient redundancy to meet availability requirements.	Yes		☒RB ☐WG ☐CV
8.15	Logging	Log files recording activities, exceptions, errors, and other relevant events shall be produced, stored, protected, and analyzed.	Yes		☒RB ☐WG ☐CV
Standard	**Description**	**Control measure**	**Relevant and implemented**	**Justification for exclusion**	**Basis** RB: Risk assessment WG: Legislation CV: Contractual Obligation
8.16	Monitoring activities	Networks, systems and applications should be monitored for anomalous behavior and appropriate measures should be taken to evaluate potential information security incidents.	Yes		☒RB ☐WG ☐CV
8.17	Clock synchronization	The clocks of information processing systems used by the organization must be synchronized with approved time sources.	Yes		☒RB ☐WG ☐CV

8.18	Use of special system tools	The use of system tools that may be able to circumvent system and application controls should be restricted and closely monitored.	Yes		☒RB ☐WG ☐CV
8.19	Installing software on operational systems	Procedures and controls must be implemented to safely manage the installation of software on operational systems.	Yes		☒RB ☐WG ☐CV
8.20	Securing network components	Networks and network devices must be secured, managed and controlled to protect information in systems and applications.	Yes		☒RB ☐WG ☐CV
8.21	Securing network services	Security mechanisms, service levels and service requirements for all network services must be identified, implemented and monitored.	Yes		☒RB ☐WG ☐CV
8.22	Network segmentation	Groups of information services, users, and information systems need to be segmented within the organization's networks.	Yes		☒RB ☐WG ☐CV
8.23	Applying web filters	Access to external websites should be controlled to limit exposure to malicious content.	Yes		☒RB ☐WG ☐CV
8.24	Use of cryptography	Rules for the effective use of cryptography, including the management of cryptographic keys, must be defined and implemented.	Yes		☒RB ☐WG ☐CV
8.25	Securing during the development lifecycle	To develop software and systems safely, rules must be established and applied.	Yes		☒RB ☐WG ☐CV
8.26	Application security requirements	Information security requirements must be identified, specified and approved when developing or acquiring applications.	Yes		☒RB ☐WG ☐CV
8.27	Secure system architecture and technical principles	Principles for secure system design must be established, documented, maintained, and applied to all information systems development activities.	Yes		☒RB ☐WG ☐CV
8.28	Secure coding	Secure coding principles should be applied to software development.	Yes		☒RB ☐WG ☐CV
8.29	Security testing during development and acceptance	Security testing processes should be defined and implemented in the development lifecycle.	Yes		☒RB ☐WG ☐CV
8.30	Outsourced system development	The organization shall direct, monitor and assess activities related to outsourced systems development.	Yes		☒RB ☐WG ☐CV
8.31	Separation of development, test and production environments	Development, test, and production environments must be separated and secured.	Yes		☒RB ☐WG ☐CV
8.32	Change management	Changes to information processing facilities and information systems must be subject to change control procedures.	Yes		☒RB ☐WG ☐CV
Standard	**Description**	**Control measure**	**Relevant and implemented**	**Justification for exclusion**	**Basis** **RB: Risk assessment** **WG: Legislation** **CV: Contractual Obligation**
8.33	Test data	Test data must be selected, protected and managed appropriately.	Yes		☒RB ☐WG ☐CV
8.34	Protection of information systems during audits	Audits and other assurance activities that assess operational systems should be planned and agreed upon between the tester and responsible management.	Yes		☒RB ☐WG ☐CV