STATEMENT OF APPLICABILITY

VAN ROEY AUTOMATION | 23/01/2025

vanroey

INGE VAN BEERS | INGE.VANBEERS@VANROEY.BE | +32 14 470 600

TABLE OF CONTENTS

InTroduction 2

Objective 2

Version Control 2

Annex A Controls 0

Approvals 0

Review & Revision 0

INTRODUCTION

Objective

The Statement of Applicability (SoA) describes the security controls implemented within the Information Security Management System (ISMS) of VanRoey. This document provides an overview of the relevant controls from Annex A of the ISO 27001:2022 standard, explaining which measures have been implemented, which are not applicable, and the justification for these decisions.

The Statement of Applicability (SoA) applies to all systems and processes within the scope of VanRoey's ISMS, covering the entire organization where information security measures are relevant.

Version Control

Versie document	Datum wijziging	Auteur	Samenvatting wijzigingen
0.0	09/09/2024	Inge Van Beers	Initial document layout
1.0	09/12/2024	Inge Van Beers	Update and adjustment of 'Reason for Inclusion'

ANNEX A CONTROLS

The Statement of Applicability provides justification for the inclusion and exclusion of Annex A controls.

Control	Requirement	Relevant	Reason	Status
A.5.1 Information Security Policies	Information security policies and topic-specific policies must be defined, approved by management, published, communicated to, and acknowledged by relevant personnel and stakeholders. These policies must be reviewed at planned intervals or whenever significant changes occur.	Yes	Risk Assessment	Implemented
A.5.2 Roles and Responsibilities for Information Security	Roles and responsibilities for information security must be defined and allocated according to organizational needs.	Yes	Risk Assessment	Implemented
A.5.3 Segregation of Duties	Conflicting tasks and responsibilities must be segregated	Yes	Risk Assessment	Implemented
A.5.4 Management Responsibilities	Management must require all personnel to apply information security in accordance with the defined policies and procedures.	Yes	Risk Assessment	Implemented
A.5.5 Contact with Authorities	The organization must establish and maintain contact with relevant authorities.	Yes	Risk Assessment	Implemented
A.5.6 Contact with Special Interest Groups	The organization must establish and maintain contact with special interest groups, security forums, and professional associations.	Yes	Risk Assessment	Implemented
A.5.7 Threat Intelligence	Information on information security threats must be collected and analyzed to produce threat intelligence.	Yes	Risk Assessment	Implemented
A.5.8 Information Security in Project Management	Information security must be integrated into project management.	Yes	Risk Assessment	Implemented
A.5.9 Inventory of Assets	An inventory of information and related assets, including ownership, must be established and maintained.	Yes	Risk Assessment	Implemented
A.5.10 Acceptable Use of Assets	Rules for the acceptable use of information and related assets must be identified, documented, and implemented.	Yes	Risk Assessment	Implemented

Control	Requirement	Relevant	Reason	Status
A.5.11 Return of Assets	Personnel and relevant stakeholders must return all organizational assets in their possession upon termination of their employment, contract, or agreement.	Yes	Risk Assessment	Implemented
A.5.12 Classification of Information	Information must be classified according to the organization's information security requirements, based on confidentiality, integrity, availability, and stakeholder requirements.	Yes	Risk Assessment	Implemented
A.5.13 Labeling of Information	Appropriate procedures must be developed and implemented to label information in accordance with the organization's classification scheme.	Yes	Risk Assessment	Implemented
A.5.14 Information Transfer	Rules, procedures, or agreements for information transfer must be established for all forms of communication facilities within and between the organization and other parties.	Yes	Risk Assessment	Implemented
A.5.15 Access Control	Rules based on business and information security requirements must be established and implemented to control physical and logical access to information and related assets.	Yes	Risk Assessment	Implemented
A.5.16 Identity Management	The full lifecycle of identities must be managed.	Yes	Risk Assessment	Implemented
A.5.17 Authentication Information	The allocation and management of authentication information must be controlled through a management process that includes advising personnel on appropriate handling of authentication information.	Yes	Risk Assessment	Implemented
A.5.18 Access Rights	Access rights for information and related assets must be provided, reviewed, adjusted, and removed according to the organization's specific policies and access control rules.	Yes	Risk Assessment	Implemented
A.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 supplier products or services.	Yes	Risk Assessment	Implemented
A.5.20 Addressing Information Security in Supplier Agreements	Relevant information security requirements must be established and agreed upon with each supplier based on the type of supplier relationship.	Yes	Risk Assessment	Implemented
A.5.21 Managing Information Security in the ICT Supply Chain	Processes and procedures must be established to manage information security risks associated with the ICT supply chain	Yes	Risk Assessment	Implemented

Control	Requirement	Relevant	Reason	Status
A.5.22 Monitoring Supplier Services	The organization must regularly monitor and evaluate supplier services for compliance with agreed-upon security practices.	Yes	Risk Assessment	Implemented
A.5.23 Information Security for Cloud Services	Security processes for acquiring, managing, and terminating cloud services must align with organizational security requirements.	Yes	Risk Assessment	Implemented
A.5.24 Incident Management Preparation	Plans must be developed to prepare for and manage information security incidents effectively.	Yes	Risk Assessment	Implemented
A.5.25 Evaluating Security Incidents	The organization must evaluate and classify security incidents as needed, documenting the process.	Yes	Risk Assessment	Implemented
A.5.26 Responding to Security Incidents	Security incidents must be addressed according to documented procedures.	Yes	Risk Assessment	Implemented
A.5.27 Learning from Security Incidents	Lessons from security incidents must be used to strengthen and improve security controls.	Yes	Risk Assessment	Implemented
A.5.28 Collecting Evidence	Procedures must be defined for collecting and preserving evidence related to security incidents.	Yes	Risk Assessment	Implemented
A.5.29 Information Security During Disruption	Plans must be in place to ensure security during organizational disruptions.	Yes	Risk Assessment	Implemented
A.5.30 ICT Readiness for Business Continuity	ICT systems must be planned, maintained, and tested to meet business continuity objectives.	Yes	Risk Assessment	Implemented
A.5.31 Compliance with Legal Requirements	Legal, regulatory, and contractual requirements must be identified and addressed.	Yes	Risk Assessment	Implemented
A.5.32 Intellectual Property Rights	Processes must protect intellectual property rights.	Yes	Risk Assessment	Implemented
A.5.33 Protecting Records	Records must be protected from loss, destruction, forgery, unauthorized access, and release.	Yes	Risk Assessment	Implemented
A.5.34 Privacy and Data Protection	Privacy and data protection requirements must be identified and met.	Yes	Risk Assessment	Implemented
A.5.35 Independent Review of Information Security	Information security management must be independently reviewed at planned intervals.	Yes	Risk Assessment	Implemented

Control	Requirement	Relevant	Reason	Status
A.5.36 Compliance with Security Policies	Compliance with security policies and procedures must be regularly reviewed.	Yes	Risk Assessment	Implemented
A.5.37 Documented Operating Procedures	Operating procedures for information processing facilities must be documented and made available to personnel who require them.	Yes	Risk Assessment	Implemented
A.6.1 Screening	Background checks for personnel must be conducted prior to employment.	Yes	Risk Assessment	Implemented
A.6.2 Employment Terms	Responsibilities for security must be defined in employment terms.	Yes	Risk Assessment	Implemented
A.6.3 Security Awareness and Training	Staff must receive security training and updates appropriate to their roles.	Yes	Risk Assessment	Implemented
A.6.4 Disciplinary Process	A formal process must address security policy violations.	Yes	Risk Assessment	Implemented
A.6.5 Post-Employment Responsibilities	Security-related responsibilities must remain clear after employment ends.	Yes	Risk Assessment	Implemented
A.6.6 Confidentiality Agreements	Confidentiality agreements must be documented, regularly reviewed, and enforced.	Yes	Risk Assessment	Implemented
A.6.7 Remote Working Security	Security measures must protect information accessed during remote work.	Yes	Risk Assessment	Implemented
A.6.8 Reporting Security Incidents	Mechanisms must be in place for timely incident reporting.	Yes	Risk Assessment	Implemented
A.7.1 Secure Areas	Secure areas must protect sensitive information and assets.	Yes	Risk Assessment	Implemented
A.7.2 Physical Entry Controls	Physical access must be controlled at secure areas.	Yes	Risk Assessment	Implemented
A.7.3 Securing Offices, Rooms, and Facilities	Security must be designed for offices and facilities.	Yes	Risk Assessment	Implemented
A.7.4 Monitoring Physical Security	Secure areas must be monitored for unauthorized access.	Yes	Risk Assessment	Implemented
A.7.5 Environmental Threat Protection	Measures must protect against environmental threats.	Yes	Risk Assessment	Implemented
A.7.6 Working in Secure Areas	Policies must govern work conducted in secure areas.	Yes	Risk Assessment	Implemented
A.7.7 Clear Desk and Clear Screen Policy	Rules must define secure desk and screen practices.	Yes	Risk Assessment	Implemented
A.7.8 Equipment Placement and Protection	Equipment must be safely placed and protected.	Yes	Risk Assessment	Implemented
A.7.9 Security of Assets Off-Premises	Measures must protect off-premises assets.	Yes	Risk Assessment	Implemented

Control	Requirement	Relevant	Reason	Status
A.7.10 Secure Disposal of Media	Information on media must be securely removed or destroyed.	Yes	Risk Assessment	Implemented
A.7.11 Utility Supply	Information processing facilities must be protected against utility outages.	Yes	Risk Assessment	Implemented
A.7.12 Secure Cabling	Data and power cabling must be secured against damage and interception.	Yes	Risk Assessment	Implemented
A.7.13 Maintenance of Equipment	Equipment must be maintained to ensure availability and integrity.	Yes	Risk Assessment	Implemented
A.7.14 Secure Reuse of Equipment	Sensitive information must be removed from equipment before reuse or disposal.	Yes	Risk Assessment	Implemented
A.8.1 User Endpoint Devices	Information stored on, processed by, or accessible through user endpoint devices must be protected.	Yes	Risk Assessment	Implemented
A.8.2 Special Access Rights	The allocation and use of special access rights must be restricted and managed.	Yes	Risk Assessment	Implemented
A.8.3 Limiting Access to Information	Access to information and related assets must be restricted in accordance with the organization's access control policies.	Yes	Risk Assessment	Implemented
A.8.4 Access Control to Source Code	Read and write access to source code, development tools, and software libraries must be appropriately managed.	Yes	Risk Assessment	Implemented
A.8.5 Secure Authentication	Secure authentication technologies and procedures must be implemented based on access control policies.	Yes	Risk Assessment	Implemented
A.8.6 Capacity Management	The use of resources must be monitored and adjusted in line with current and anticipated capacity requirements.	Yes	Risk Assessment	Implemented
A.8.7 Protection Against Malware	Protection against malware must be implemented and supported by appropriate user awareness.	Yes	Risk Assessment	Implemented
A.8.8 Management of Technical Vulnerabilities	Information on technical vulnerabilities must be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken.	Yes	Risk Assessment	Implemented
A.8.9 Configuration Management	Configurations, including security configurations of hardware, software, services, and networks, must be established, documented, implemented, monitored, and reviewed.	Yes	Risk Assessment	Implemented

Control	Requirement	Relevant	Reason	Status
A.8.10 Secure Deletion of Information	Information stored in systems, devices, or other storage media must be securely deleted when no longer required.	Yes	Risk Assessment	Implemented
A.8.11 Data Masking	Data must be masked in accordance with access control policies and other relevant organizational requirements, taking into account applicable legal requirements.	Yes	Risk Assessment	Implemented
A.8.12 Data Leak Prevention	Measures to prevent data leaks must be implemented in systems, networks, and other devices where sensitive information is processed, stored, or transmitted.	Yes	Risk Assessment	Implemented
A.8.13 Information Backup	Backups of information, software, and systems must be maintained and regularly tested in accordance with the organization's backup policy.	Yes	Risk Assessment	Implemented
A.8.14 Redundancy of Information Processing Facilities	Information processing facilities must be implemented with sufficient redundancy to meet availability requirements.	Yes	Risk Assessment	Implemented
A.8.15 Logging	Logs recording activities, exceptions, errors, and other relevant events must be generated, stored, protected, and analyzed.	Yes	Risk Assessment	Implemented
A.8.16 Monitoring Activities	Networks, systems, and applications must be monitored for unusual behavior, and appropriate measures must be taken to evaluate potential information security incidents.	Yes	Risk Assessment	Implemented
A.8.17 Clock Synchronization	Clocks of information processing systems used by the organization must be synchronized with approved time sources.	Yes	Risk Assessment	Implemented
A.8.18 Use of Privileged System Utilities	The use of system utilities capable of bypassing security controls for systems and applications must be restricted and carefully controlled.	Yes	Risk Assessment	Implemented
A.8.19 Secure Installation of Software on Operational Systems	Procedures and measures must be implemented to manage the secure installation of software on operational systems.	Yes	Risk Assessment	Implemented
A.8.20 Network Component Security	Networks and network devices must be secured, managed, and controlled to protect information in systems and applications.	Yes	Risk Assessment	Implemented
A.8.21 Network Service Security	Networks and network devices must be secured, managed, and controlled to protect information in systems and applications.	Yes	Risk Assessment	Implemented

Control	Requirement	Relevant	Reason	Status
A.8.22 Network Segmentation	Groups of information services, users, and information systems must be segmented within the organization's networks.	Yes	Risk Assessment	Implemented
A.8.23 Use of Web Filtering	Web filtering must be applied to information services, users, and information systems as required.	Yes	Risk Assessment	Implemented
A.8.24 Use of Cryptography	Rules for the effective use of cryptography, including key management, must be defined and implemented.	Yes	Risk Assessment	Implemented
A.8.25 Security During Development Lifecycle	Rules for secure development of software and systems must be established and applied.	Yes	Risk Assessment	Implemented
A.8.26 Application Security Requirements	Information security requirements must be identified, specified, and approved when developing or procuring applications.	Yes	Risk Assessment	Implemented
A.8.27 Secure System Architecture and Principles	Secure system design principles must be established, documented, maintained, and applied during information system development activities.	Yes	Risk Assessment	Implemented
A.8.28 Secure Coding	Secure coding principles must be applied to software development.	Yes	Risk Assessment	Implemented
A.8.29 Security Testing During Development and Acceptance	Security testing processes must be defined and implemented in the development lifecycle.	Yes	Risk Assessment	Implemented
A.8.30 Outsourced System Development	The organization must direct, monitor, and review activities related to outsourced system development.	Yes	Risk Assessment	Implemented
A.8.31 Separation of Development, Test, and Production Environments	Development, test, and production environments must be separated and secured.	Yes	Risk Assessment	Implemented
A.8.32 Change Management	Changes to information processing facilities and information systems must be subject to change management procedures.	Yes	Risk Assessment	Implemented
A.8.33 Test Data	Test data must be appropriately selected, protected, and managed.	Yes	Risk Assessment	Implemented
A.8.34 Protection of Information Systems During Audits	Audit tests and activities involving operational systems must be planned and agreed upon with responsible management.	Yes	Risk Assessment	Implemented

APPROVALS

This document and the security measures described herein are formally approved by the management of VanRoey. The approval signifies the management's commitment to the implementation and continuous management of the ISMS.

REVIEW & REVISION

This Statement of Applicability is reviewed annually or whenever substantial changes occur in the organization, information security risks, or relevant regulations. Changes are documented and approved by management.