Elevaite365

ISMS Clause Requirements

Version 1.0

PURPOSE

This document defines and establishes the ISMS clause requirements, which include the scope and boundaries for establishing an information security management system based on the ISO 27001:2022 standard. Other requirements include Internal and External Issues, Interested Parties and their requirements, communication, and ISMS Security Objective Metrics.

SCOPE

This document applies to the Information Security Management System (ISMS) at Elevaite365 (herein referred to as the Organization).

DEFINITION

- ISMS: Information Security Management System
- Information Security: Confidentiality, Integrity, Availability of information
- ISG: Information Security Group
- LT: Leadership Team

RESPONSIBILITIES

- ISG: Information Security Group
- LT: Leadership Team

POLICY

ISMS SCOPE

Scope Statement

“Information Security Management System applies to {{ISMS_Scope_Statement}}"

This is as per the latest Statement of Applicability (SoA) version.

Products and Services

The main products and services included in the scope of the ISMS are –

Products

Elevaite365 - Test Automation

Services-

We provide automated testing as a SaaS platform targeted towards D365 applications

Locations in scope

The Information Security Management System in the organization applies to the following sites:

Elevaite365 Group AB
Tfw 992-M Billo, 106 46 Stockholm, Sweden

Departments and Functions

The following Departments have been included in the scope of the organization’s ISMS –

1. DevOps
2. IT
3. HR
4. Finance & Admin
5. Sales

Exclusions

Refer statement of applicability

UNDERSTANDING OF THE ORGANIZATION AND ITS CONTEXT

The organization uses Managed Services to host and manage infrastructure components of the production environment.

Given the nature of its operations and the sensitivity of the information handled, the organization is exposed to numerous internal and external risks. Such risks include:

1. Fraud risk
2. Legal and Compliance Risk
3. Operational Risk
4. Technology Risk
5. Financial Risk
6. Staffing and Organization Risk
7. Contractual Risk
8. Business Continuity Risk

Internal Issues

Table 1: Internal Issues

Internal Issues Affecting ISMS Outcomes	Needs / Expectations
Available Resources	Identifying infrastructure resources, including systems and processes, personnel, technologies, equipment, knowledge, and time, will guide the development of solutions, competencies, and acquisitions.
Governance, Organisation Structure, and Roles & Responsibilities	Ensure certain activities are directed and aligned to achieve the organization's long-term goals. This involves knowing the roles and responsibilities of team members involved in implementing ISMS.
Organization Objectives	Ascertain the organization's information security strategies, objectives, and policies, including its mission, vision, and values.
Operations	Understand the Organization's critical process information flow and integration of information security through each step.

External Issues

Table 2: External Issues

Internal Issues Affecting ISMS Outcomes	Needs / Expectations
Legal and Regulatory Compliance	Assess and keep track of applicable legal and regulatory requirements to the organization
External Relationships	Consideration of external interested parties' values, beliefs, and perceptions. Dependencies on external parties
Technological Advancements	Analyzing the impact of technology changes on the business and information security management system

Internal Issues Affecting ISMS Outcomes	Needs / Expectations
Economic and Political Factors	Monitor changes in political and economic concerns, both locally and globally, since this can have a significant impact on how a firm runs
Environment Factors	Natural disasters such as earthquakes, tsunamis, pandemics, floods, etc.

The organization has identified relevant interested parties to achieve its Information Security objectives and ensure that their needs and expectations are taken into consideration when establishing its Information Security framework.

Table 3: Interested Parties and Expectations

Interested Party	Internal / External	Relationship with the organization	Needs / Expectations
Top Management	Internal	Provide Information Security strategic and tactical directions for the organization.	Expect to continuously maintain the Information Security Management System to protect the organization's Product, Customer, and Employee data from major incidents/breaches and gain customer confidence.
Employees (Full-time contractors)	Internal	Work for business processes and comply with the practices outlined in the ISMS.	Expect the organization to provide a safe and secure environment and training and support on good information security practices.
Customers	External	Customers who accelerate business growth and share critical data.	Expect that customer data's confidentiality, integrity, and availability within the product are always secured.
Third Parties/ Suppliers/ Vendors	External	Support organization to perform business activities.	Expect that the organization adheres to the contractual agreements and enforces the Information Security requirements of its vendor's information.
Auditors	Internal / External	Assess the organization's conformity to applicable standards and regulations, such as ISO 27001, SOC 2, relevant laws, etc.	Expect that a proportionate level of information security controls are in place at all times to protect critical data.
Regulatory bodies	External	Define legal and regulatory requirements for organizations.	Expect that the organization adheres to the legal and regulatory requirements.
Business Unit Heads	Internal	Work for business processes and, lead respective business units and manage the overall business function and manpower.	Expect that the organiztion provides a safe and secure environment, required resources, and support from Top Management to safeguard information assets.

COMMUNICATION

The organization shall determine the need for internal and external communication relevant to the information security management systems, including:

1. On what to communicate
2. When to communicate
3. With whom to communicate
4. How to communicate

Table 4: Communication Channel

What	When	To Whom	How
ISMS Policies and procedures	During induction, annual and on a need basis as appropriate	Internal and external interested parties such as Organization name Employees, Customers, and Third Parties	GRC Portal/Intranet
Security Risk Management Methodology, Risk Assessment & Treatment Report	Start and on culmination of the annual risk assessment process	Top Management, Department Heads and ISG	Email
Internal/external Infosec audit, scope, and plan	2 weeks prior to the start of any audit	Top Management, Department Heads and ISG	Email
Audit findings and recommendations	Post-completion of audit/assessment	Top Management, Department Heads and ISG	Email
Management Review Meetings (MRM)	During annual MRM and on a need basis as appropriate	ISG and Top Management	Email
Training calendar and modalities	During induction, annual and targeted role-based quarterly training	Employees	Email & Company Messaging Platform
Application changes	When changes result in product downtime	Customers and ISG	Email Notification / Social Media Channels
Information Security Incidents	When an incident has led to disruption of services/disclosure of confidential information	ISG, Top Management, and Regulators as applicable	Email

INFORMATION SECURITY OBJECTIVES AND PLANNING TO ACHIEVE THEM

ISMS aims to provide a secure environment for processing, storing, or transmitting information. The specific information security objectives are to:

1. Be consistent with ISMS policies
2. Conduct risk assessments to ensure that information risk is minimized or eliminated.d
3. Establish a strong culture of security across the organization
4. Ensure the organization's products and necessary resources are available for the customers
5. Continue to innovate and enhance the service provided to make the ISMS more effective
6. Ensure customer data are protected with adequate safeguards
7. Liaise with all interested parties to improve overall ISMS
8. Ensure that there is no adverse impact (Information security incidents/breaches) on the organization's brand in the public domain with regard to security
9. The above ISMS objectives are updated at least annually during the ISMS Manual revision activity to ensure continual improvement of the Information Security Management System to meet all its security objectives aligned with business goals.

The "ISMS Security Objectives_Metrics" defines specific measurements, such as setting KPIs for each objective, and timeframes are described in the *"ISMS Security Objectives_Metrics "* to track the effectiveness of ISMS.

Table 5: ISMS Security Objectives_Metrics

Area	Security Objective	Task	Resource Assigned	Measurement Method	Target	Result	Timescale	Owner
Achievement of ISO 27001 certification	Obtain ISO 27001 certification	Achieve certification	ISG	Certificate obtained from the registrar	100%	Update	Annual	TBD
Availability	Maintain 99.8% uptime	Review utilization and uptime reports	IT	External APM	99.80%	Update	Annual	TBD
BCP	Ensure that the BIA and sampled business	Obtain management approval for exercise	ISG	All exercise objectives were met	100%	Update	Annual	TBD

Area	Security Objective	Task	Resource Assigned	Measurement Method	Target	Result	Timescale	Owner
	continuity plans have been exercised within the last year	schedule and type of exercise.						
Document approval process	% of documents reviewed and approved for ISMS	Review and update policies as necessary	ISG	Percentage of ISMS documentation and controls in place	100%	Update	Annual	TBD
Incident Management	Respond to Information Security incidents within approved time frames after a reported incident.	Review incident response logs/tickets for acknowledgment	ISG	% of InfoSec incident responses within the approved time period	100%	Update	Quarterly	TBD
Security Awareness	Establish Security Awareness Program	Implement security awareness training	ISG	Number of people trained	100%	Update	Annual	TBD
Access Review	Establish Access Review Program	Implement Access Control Review control for all the applications and IAM solutions.	ISG	Review of Access Review reports against active HR records against all IAM solutions	100%	Update	Quarterly	TBD

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	-	Initial Release	Borhan	-	-