AROBS
Transilvania Software

POLICY

Risk Management

(P-GEN-8)

DOCUMENT HISTORY

VERSION	AUTHOR	DESCRIPTION	DATE	APPROVERS
2.0	RMSI Team	Initial issuing	17 January 2024	Executive Management
3.0	RMSI Team	Added sustainability details	25 November 2025	Management Board

CONTENT

1. SCOPE & APPLICABILITY

This policy outlines the process and responsibilities of identifying and evaluating the risks associated with business activities and sustainability (own workforce, value chain, affected communities, end-users, financial, climate impact, geopolitical, etc). It covers those aspects that the organization can control or influence, including planned or new developments and modified activities. The aim is to identify, analyze, assess, manage, control, and report risks arising in the course of all the group company's activities., and to implement appropriate control measures for AROBS Transilvania Software S.A., both at the Company level and at the Group level.

The Policy applies to those responsible for managing risks, assessing risks, or implementing controls to mitigate risks, including department heads, sustainability coordinator or Sustainability Committee (if available) project managers, and resource owners, both at the level of AROBS Transilvania Software SA and at the Group level.

The Board of Directors determines the nature and extent of the risks the Company is willing to assume in pursuit of its strategic objectives (risk appetite) and ensures that appropriate structures, policies, and procedures are in place for the identification, assessment, reporting, management, and monitoring of significant and emerging risks, including those related to sustainability, cybersecurity, and the use of digital technologies. The Board shall also disclose in the annual report the mechanisms and processes for risk management.

The Board adopts a formal risk management policy that ensures the accurate, complete, and timely identification, measurement, and reporting of risks, the implementation of appropriate control measures, and the integration of environmental and social (E&S) risks into the overall risk management framework.

2. DEFINITIONS & ABBREVIATIONS

AROBS – AROBS Transilvania Software SA;
Board – the Board of Directors;
Group – all companies in which AROBS Transilvania Software S.A. is the majority shareholder;
Resources - any value for the organization.
Risk - the effect of uncertainty in obtaining the desired results; risk should be seen as a combination of probability and impact
Risk identification - global risk analysis and assessment process
Risk analysis - systematic use of information to identify sources and estimate risk
Risk assessment - risk assessment process with agreed risk criteria and risk import risk assessment
Risk Management - Coordination activities to guide and control an organization taking into account risk
Risk Treatment - process of selection and implementation of measures to mitigate risk

Security measure (means of control) - a means of dealing with risk including policies, procedures, guidelines, practices, equipment, devices, actions or organizational structures that may be of an administrative, technical, managerial or legal nature.
Inherent risk - the amount of risk that exists when some threat goes untreated or unaddressed.
Residual risk - the risk that remains after the treatment of the risk
Threat - potential cause of an undesirable incident that could result in damage to a system or organization
Vulnerability - weakness of a resource or group of resources or a security measure that could be exploited by one or more threats

IMSR-Integrated Management System Responsible
PM – Project Manager
HoD – Head of Department
SC – Sustainability Coordinator
ISMS – Information Security Management System

3. REFERENCES

SR ISO/IEC 27001:2022 – Information Security Management System.
ISO/IEC 27005 – Information Security Risk Management. Guidelines.
SR ISO 31000:2009 – Risk management - Principles and guidelines.
SR EN ISO 9001:2015 – Quality Management Systems. Requirements.
SR EN ISO 14001:2015 – Environmental Management Systems. Specifications and guidelines for use.
SR EN ISO 45001:2018 – Occupational Health and Safety Management systems. Specifications and guidelines for use.
CSRD – Corporate Sustainability Reporting Directive

4. PROCEDURE DESCRIPTION

4.1 Establishing Organizational Context

By setting the context, AROBS Transilvania Software also defines, at Group level, the relevant internal and external parameters that need to be considered in risk management process. These parameters need to be detailed and considered from the perspective of the scope of ISMS.

The context will be established and documented every time the risk management process is conducted, either before or during the collection of information regarding the inventory of information resources. Background documentation must be an integral part of risk analysis/risk register.

The internal context is the internal environment in which AROBS seeks to achieve its objectives. The internal context of AROBS includes, but is not limited to:

- scope of ISMS

- availability in terms of resources and knowledge (e.g. competencies, capital, time, people, processes, systems and technologies)
- information systems, information flows, decision-making processes (formal and informal)
- internal stakeholders
- existing policies, procedures, objectives, measures, methodologies and strategies
- perceptions, values, organizational culture
- standards and reference models adopted by the organization
- structure (authority, roles and responsibilities)

The external context is the external environment in which AROBS seeks to achieve its goals. In understanding the external context is important to ensure that stakeholders, their goals and concerns are considered when developing risk criteria. The external context is based on the broader context of AROBS, but with specific details on legal and regulatory requirements, stakeholder perceptions, and other risk issues specific to the scope of the risk management process.

Aspects of **the external context** of AROBS include, but are not limited to, the following:

- cultural, political, geo-political legal, legislative, financial, technological, economic, value chain, natural and competitive environment, both internationally and nationally, regionally or locally
- key trends and elements that can impact AROBS objectives
- the perceptions and values of external stakeholders

The Board of Directors and the Audit Committee shall give ongoing attention to emerging risks generated by information technology and artificial intelligence, including cybersecurity risks. In this regard, sufficient time should be allocated on the Board's agenda to analyze the risks and opportunities associated with AI and to ensure an adequate level of understanding of cybersecurity protection.

4.2 Risk Identification

Risk identification is a first crucial step in risk management, involving systematically finding, documenting, and describing potential events (threats) that could affect AROBS objectives, using methods or root cause analysis to create a comprehensive list for further analysis and control. It's about understanding potential impacts and build strategies to manage them proactively.

Identifying risks (logical and physical) means determining what might happen to cause a loss or an event to adversely affect the organization, including **confidentiality**, **integrity** and **availability** of information resources, and how, where and why loss could occur.

AROBS identifies risks through a structured process that includes regular assessments of internal operations, engagement with stakeholders across the value chain, ongoing monitoring of environmental, social, financial, political, and geopolitical factors that may impact the organization.

Risks associated with the Corporate Sustainability Reporting Directive (CSRD) include **financial penalties, reputational damage, legal disputes, and loss of trust** from stakeholders due to non-compliance.

Identifying risks includes: brainstorming about possible risks / opportunities, inventory of information assets, threats and vulnerabilities applicable, existing security control measures, consequences of a data loss, etc.

The identified risks are recorded in the **Risk Register by the risk owner**.

For a good approach to Risk identification, each process owner will identify its own information security risks, with IMSR/SC support. The risk owner will accept the risks identified and assessed by each process owner.

4.2.1 Identifying & evaluating assets

AROBS identifies all relevant assets by maintaining an updated inventory of all physical facilities, technological systems, human capital, natural resources, intellectual property, and supply-chain relationships that influence the organization's environmental performance, social impact, and governance obligations.

The organization's resources are identified and inventoried by resource owner, with the support of asset responsible and other internal interested parties. The following types of resources are considered in the identification process:

- **Financial resources**: cash, available in bank accounts, loans, investments, capital, credit lines etc.
- **Information**: databases and data files (about Group companies, clients, employees of the Group companies), contracts and agreements, system documentation, specialized know-how, specific instructions, operational procedures, business continuity plans, business intelligence, knowledge, etc.;
- **Software resources**: application software, system software
- **Physical resources**: vehicles, inventory, raw materials, office space, IT and communications equipment, mobile media, audio, photo and video equipment, other equipment
- **Services**: IT and communications services and products, general utilities (electricity, air conditioning, heating, etc.)
- **Human resources**: professional abilities, experience and loyalty
- **Intangible resources/Intellectual property:** such as reputation and image of the organization, Patents, trademarks, copyrights, trade secrets, brand, culture.
- **Network Resources:** Partnerships, supplier relationships, customer base.

IMSR/SC, along with resource owners, records resources identified, in the **Informational Asset Register (related to P-GEN-3) & other asset inventories**, indicating the type, format, location, and information required for disaster recovery. Resource identification is conducted for each process/dep.

For each identified resource, an accountable owner is appointed. The owner is responsible for the administration, storage, and security of that resource.

The identified resources are evaluated by the asset/risk owner. All information resources have a certain value for AROBS and this value can be measured by the following criteria:

- depending on the impact of compromising the asset or data
- depending on the inventory value, replacement or remedy of that resource

4.2.2 Identifying the internal processes; analysis from process owners

For the identification of main processes, the organization chart is analyzed; in the **Risk Register**, main departments and processes are approached accordingly (ex: IT, HR/Administrative, Project Management /Software development, Financial, Legal, Procurement, SC etc.).

Process owners have responsibilities in identifying all significant sources of uncertainty, mainly by discussing internally.

For specific Risk Assessment / Project

Each Project Manager/Process Owner will seek to identify project-specific, sustainability and information security risks.

To identify the risks arising from the implementation of projects/process, the following must be established before the purpose of the project:

- the roles and functions of the staff involved in the project/process;
- contract terms if applicable
- legal requirements
- professional practices
- project/process documentation

Based on the listed elements and interviews with project managers/process owners and key partners, critical milestones affecting information security can be identified.
For each stage, at least the following vulnerabilities and threats will be considered:

- infrastructure
- personnel
- project management (cost, quality, deadlines)
- legal
- financial
- reputation

Regardless of the project/process methodology used, the critical project/process stages will be framed in:

- project/process definition (concept, requirements and architecture, detail design, planning, sequence of activities, responsibilities, and controls and execution of tasks etc.)
- implementation
- test and integration (Integration, Testing, Verification, Validation, Maintenance, etc.)

4.2.3 Analyzing vulnerabilities and threats

Threats occur accidentally, either naturally or deliberately (intentionally). For each main process/department, vulnerabilities and threats are identified in the context of AROBS, considering existing security measures (see risk register). Risk analysis includes only possible and probable vulnerabilities and threats, excluding hypothetical threats and vulnerabilities that cannot be exploited in the context of AROBS.

When defining vulnerabilities and threats, available **catalogues (Annex 1 - Vulnerabilities, risks and threats) of vulnerabilities and threats** to information security, process quality, project management, human resources, etc are used.

The initial step of identifying vulnerabilities and threats involves the process owner collaborating with IMSR. They will indicate those vulnerabilities and threats specific to the area of responsibility. IMSR will complete and correct the list of vulnerabilities and threats based on AROBS's global knowledge.

4.3 Risk analysis/assessment

Risk analysis refers to understanding the risk, possible causes, sources of risk, if the risk is negative or positive, what are the possible consequences and what would be the likelihood. Risk analysis involves grading through qualitative and/or quantitative assessments to ascertain the risks associated with a process and resource.

For each identified risk, a probability of occurrence and impact from 1-3 is established, as detailed in **Risk Register**.

4.4 Risk evaluation

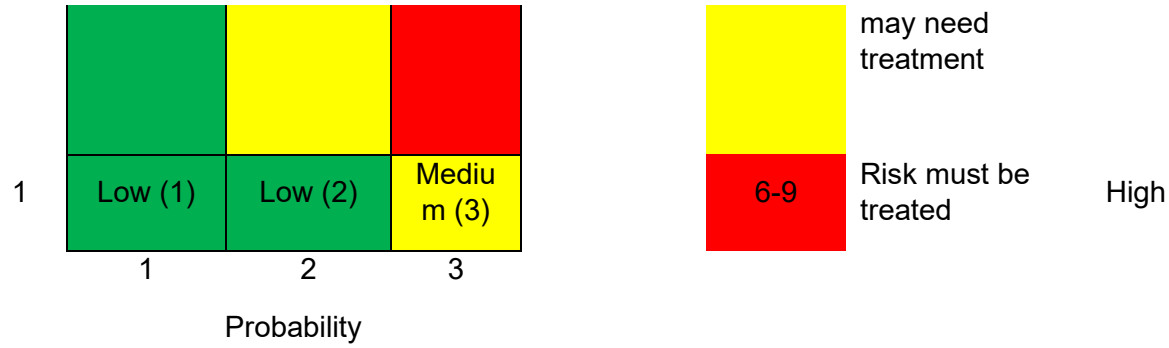
Risk evaluation is the comparison of the estimated risk levels with the default risk acceptance criteria. This allows for a classification and prioritization of risks.

Based on the value of the information resource, probability level and impact level, risk value is determined in accordance with the following table:

Impact				
	3	Medium (3)	High (6)	High (9)
	2	Low (2)	Medium (4)	High (6)

Legend

1-2	Risk low, acceptable ; risk is retained by default	Low
3-4	Low risk, not urgent, but it	Medium



AROBS has set a minimum acceptable level of risk to 2 (green). For risks ranging from 3 to 4 (yellow), the treatment measures will be determined on a case-by-case basis. Risks between 6 and 9 (red) are to be treated mandatory.

4.5 Risk treatment

The risk treatment options are selected according to the results of the risk assessment, the estimated cost of implementation and the benefits of these options. The treatment options are identified and established together with the resource owner, IMSR and other interested parties.

Four possible options for dealing with risks are considered:

- avoiding risks
- risk reduction
- risk transfer
- accept the risk

The four options are not mutually exclusive. In some cases, the use of a combination of options, such as risk reduction, risk mitigation and transfer or assumption of residual risks, may have considerable advantages for AROBS.

a) Risk reduction (changing likelihood/ impact)

The risk level must be reduced by selecting the measures so that the residual risk becomes acceptable (lowering the probability or impact of the risk). This selection will consider the criteria for accepting risks, adding backups, enhancing security, training staff, or designing protective equipment (is applicable) to lessen severity, making it a core part of managing threats by controlling potential damage before it escalate.

b) Avoiding risks (by deciding not to start or continue with the activity that give rise to risk)

The activity or condition leading to the risk must be avoided. When identified risks or risk management implementation costs are considered too high, options outweigh the benefits, a

complete risk avoidance decision may be taken by withdrawing from the activity or set of planned activities or by changing the operating conditions of the activity.

c) Risk transfer

It involves a decision to distribute certain risks to other external parties. Transferring risks may create new risks or change existing ones that have already been identified. Thus, additional risk management measures may be necessary. The transfer can be done through insurance covering the consequences of the materialization of the risk.

d) Accept the risks

The decision to accept/retain the risks without any further action must be taken according to the risk assessment. If the risk level falls within the risk acceptance criteria - usually for low-impact risks or when treatment costs outweigh benefits, documenting it as residual risk -, it is no longer necessary to implement the additional measures and the risk can be assumed.

4.5.1 Risk Treatment Plan

The Risk Treatment Plan must be defined in such a way as to clearly identify the order of priorities for the implementation of the risk management and the duration of the treatments.

The risk management plan is coordinated by IMSR/SC along with other AROBS functions, depending on the risk.

After establishing and implementing the risk management plan, residual risks must be determined. This involves an update or re-iteration of the risk assessment considering the expected effects of the proposed treatment. If residual risks do not meet the organization's acceptance criteria, a further iteration of risk management may be required before proceeding to acceptance.

Note:
Regardless of the risk treatment options and the results obtained following the implementation of treatment measures, monitoring and re-evaluation of risks are carried out periodically (**annualy**), including the accepted residual risks, **or whenever there is a change in the organization internal or external context** that could alter the nature and level of risk.

The Board of Directors, supported by the Audit Committee, assesses at least annually the adequacy and effectiveness of the Company's risk management framework and internal control system. This assessment includes the effectiveness of the internal audit function, the adequacy of risk management and compliance processes, internal control reports, and management's ability to address identified deficiencies, as well as the reporting of conclusions to the Board.

4.6 Risk acceptance

Risk owner with the support of IMSR has the responsibility to review, analyze and confirm the risks recorded by process owners in **Risk Register**, focusing on subjects such as the Risk Treatment Plan, other recurrent dates for reviewing the risks, etc.

4.7 Risk communication

Process owners have the responsibility to inform IMSR/SC whenever they update the **Risk Register**.

Further, IMSR/SC has the responsibility of informing Top Management regarding risks, if necessary, after evaluating the impact within the business process.

Note:
Special attention must be paid whenever it is about risks of yellow label and red label.

The risk owner has the responsibility to review, analyze and confirm the risks recorded by process owners in **Risk Register**, focusing on subjects such as the Risk Treatment Plan, other recurrent dates for reviewing the risks, etc.

4.8 Monitoring & review the risks

This step represents the monitoring and review of the risk management system and any changes that could affect it (e.g., changes in resources, impact, threats, vulnerabilities and/or likelihood of occurrence, actions taken as a result of internal analyses).

Monitoring and review take place simultaneously during the risk management process. Monitoring and review are done by the process owner along with the risk owners with the support of IMSR/SC. IMSR/SC will coordinate monitoring and global review of AROBS through:

- observing significant changes in the internal and external context
- incidence of risk materialization in information security incidents.

Risk assessments must be conducted at least annually, or whenever one of the following situations occurs:

- changes in security policy that affect the risk assessment methodology
- changes in benchmarking standards impacting on risk management
- major changes to existing systems (eg scope)
- major, unexpected or unplanned changes in senior management
- significant changes in facilities or location change of facilities
- introducing new resources in IMS
- required changes in resource values, for example, due to different business requirements
- new active threats either from within AROBS GROUP or from outside, which have not yet been evaluated (changes in the threats landscape)
- the possibility of new or increased vulnerabilities to allow threats to exploit these vulnerabilities
- known vulnerabilities become exposed to new threats
- changing the impact in terms of increased risk exposure
- a security incident occurred, or the audit findings identified a need for this

5. RECORDS & ANNEXES

Annex 1 - Vulnerabilities, risks and threats database

Risk Register