Global Policy

Risk Management

Policy No.:	1.03 (Version 1.0)
Issue Date:	01.10.2022
Last Update:	--
Applies to (Region):	All
Applies to (Department):	Risk Management & Internal Audit
Contact Person:	Arthur Consalter, Head of Internal Audit and Risk Management
Approver:	Guillaume Luebke, Chief Financial Officer

Signature of Approver:

DocuSigned by:
Guillaume Luebke
F1A20B328127401...

Contents

1 Executive Summary 3
2 Purpose Statement 3
2.1 Policy Rationale 3
2.2 Risks to be mitigated 3
2.3 Groups Affected 4
3 Policy Content 4
3.1 Policy Statement 4
3.2 Roles and Responsibilities 4
3.3 Risk Management Process 4
3.3.1 Risk Management Cycles 5
3.3.2 Risk Identification 5
3.3.3 Risk Assessment 6
3.3.4 Risk Response 7
3.3.5 Risk Review, Revision & Monitoring 7
3.3.6 Risk Reporting 8
3.3.7 Framework Monitoring & Review 8
3.3.8 Risk Management System 8
3.4 Implementation, Training and Control 8
4 Appendix 8
4.1 Definitions and Abbreviations 8
4.2 References 9
4.3 Change Log 9

1 Executive Summary

The Risk Management Policy provides a systematic approach towards the proactive identification, assessment, treatment and reporting of relevant risks which may potentially endanger the achievement of the objectives of Envu.

Risk Management (RM) assigns clear ownership for each relevant risk, makes the decision on risk treatment transparent, provides a continuous risk reporting as well as regularly reviews and monitors the mitigation actions status.

In addition, RM is an early warning system that provides transparency on risks that could potentially endanger the continued existence of the company's and on their development over time.

2 Purpose Statement

2.1 Policy Rationale

A pro-active RM supports Management in achieving the objectives of the company, in safeguarding the company assets and in fulfilling legal requirements. On the other hand, a proactive RM reveals new opportunities by supporting risk-based decisions and offering effective and sustainable mitigation solutions.

Envu established a RM systematic approach based on the introduction of a Global RM function covering all functions. The globally and centrally steered RM process is established to generate transparency for the Senior Management over the relevant risks.

Driving a transparent and pro-active risk culture in the organization, RM aims to create a holistic view that allows an adequate focus and prioritization of risks as well as informed decision making.

This Policy has the objective to establish clear RM accountabilities in the organization and to provide the methodology for an Enterprise Risk Management (ERM) process.

2.2 Risks to be mitigated

Envu considers as risks all uncertain events or conditions that, in case of occurrence, may negatively impact its existing business or future value creation and therefore potentially endanger the achievement of the company´s short-to long-term objectives.

In scope of this Policy are relevant risks that are risks with a potential impact (assessed as described in section 3.3.4) that exceeds a defined and regularly reviewed financial threshold (established by the Assurance Committee) or are significant from a qualitative impact criterion (e.g., reputational risk).

The defined Risk Management process allows identifying, assessing, treating, and reporting any risks that are material and / or could endanger the continued existence of the company.

2.3 Groups Affected

This Policy applies to the Leadership Team (LT) and the entire line Management (first line of defense, as defined by the Institute of Internal Audit). It also applies to employees who are part of RM process (e.g., Risk Owners).

3 Policy Content

3.1 Policy Statement

RM follows two main principles:

- Focus on material risks to the objectives of the company
- Clear risk ownership with assigned accountability in line Management

With the definition of roles & responsibilities, a method, reporting formats, process and tools, RM lays the foundation for a pro-active and systematic process.

3.2 Roles and Responsibilities

Risk Management department: is responsible to establish, deploy and continuously improve a consistent and standardized Risk framework and processes. It drives the Risk cycle by supporting the involved parties. It defines the quantitative and qualitative thresholds, and it is responsible to prepare risk reporting to the Chief Financial Officer and the Assurance Committee.

Risk Owner (RO): each line management function is accountable for identifying risks in its own area of responsibility and for managing them adequately. In particular, the accountable line manager for an identified relevant risk is called Risk Owner and is responsible for the identification, assessment, treatment, and reporting of its relevant risk. The RO continuously monitors the development of the risks and the effectiveness of the mitigation measures. The RO may define further responsible persons, e.g., for mitigation actions.

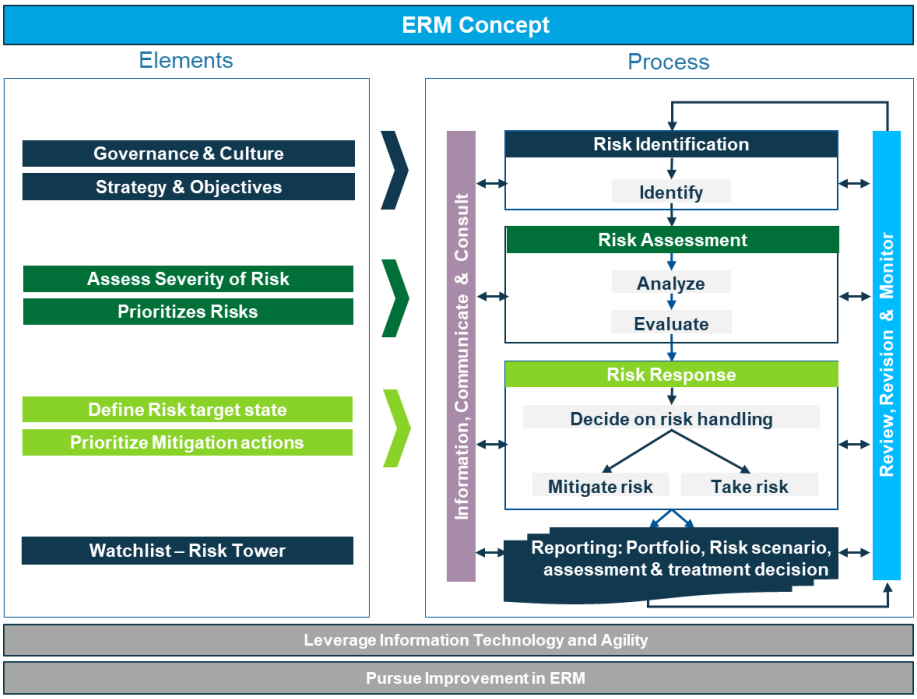
3.3 Risk Management Process

The process draws on the principles set forth in ISO 31000 and elements from COSO ERM, and consists of the following phases: Risk Identification, Risk Assessment and Risk Response. Further important activities of the process are Reviewing & Monitoring as well as Information, Communicating & Consulting within the organization. The process is carried out on a Global business and functional level. The process is linked with the Company's Governance & Culture and Strategy & Objectives (including M&A projects and the ESG strategy). During the Risk Assessment phase, it is critical for the process to Assess the severity of risks and Prioritize Risks based on the Company Risk Appetite and the Assurance Committee directions, and during the Risk response phase, the mitigations actions should be evaluated on a priority order, and the RO together with RM should identify the risk target state based on the impact and likelihood after implementing the critical actions plans.

As an overall target the ERM process aims to leverage Information Technology and Agility and its Continuous Improvement.

An overview of the Risk Management process is showed in Figure 1.

Figure 1:



3.3.1 Risk Management Cycles

Risk Management cycles are performed at least once a year, however depending on the severity and priority of the risk, specific cycles can be determined for one or more risks.

Each cycle includes a systematic identification of potentially new relevant risks, their assessment and the documentation of treatment plans and decisions, as well as an update for risks identified in previous cycles. All relevant risks are approved by the respective RO.

3.3.2 Risk Identification

To ensure a comprehensive identification of RM relevant risks, interviews are prepared by Global RM team. Relevant internal and external sources for potential risk information are reviewed. Independently from the annual RM cycles, whenever a new risk is identified, a RO in the responsible line management function must be assigned. New relevant risks that are identified in the course of the year need to be assessed and reported *ad-hoc*, as well as M&A project risks, whenever a new M&A project starts a specific Risk Identification process is necessary to evaluate the need of further steps (risk assessment, risk response, risk reporting, etc.).

During the risk identification phase, the Company's Governance & Culture and Strategy & Objectives (including ESG and M&A-related) is assessed, to make sure we have identified all relevant risks aligned with the company's risk appetite.

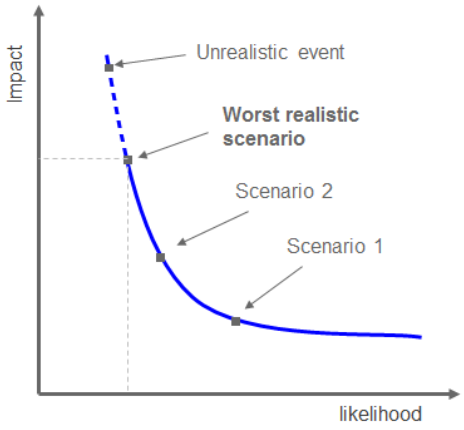
3.3.3 Risk Assessment

Risk assessment is the phase that aims to determine the dimensions of the risk, in general expressed in impact and likelihood. RM risks are consequently calibrated allowing prioritization. The RO is responsible for the assessment of the identified risks.

Risk scenario: worst realistic case

Only one specific risk scenario (i.e., a combination of source, event and consequence) linked to a specific risk has to be assessed. The scenario must describe a worst realistic case.

Figure 2: Worst Realistic Scenario



Risk Impact

The Risk Impact measures the potential financial and / or qualitative (non-financial) negative consequences in case the risk materializes today. The financial impact is expressed based on the company risk materiality (approved by the Assurance Committee).

For risks where the impact is not restricted to a financial damage, or representatively expressed by the financial quantification, qualitative impact dimensions can be used.

Compliance and ESG-related risks are considered Severe impact (risk appetite).

Global RM annually reviews and eventually adjusts the financial impact thresholds to adequately reflect current business size and objectives.

Risk Likelihood

The Risk Likelihood measures the probability that the worst realistic risk scenario will materialize as described within a defined timeframe.

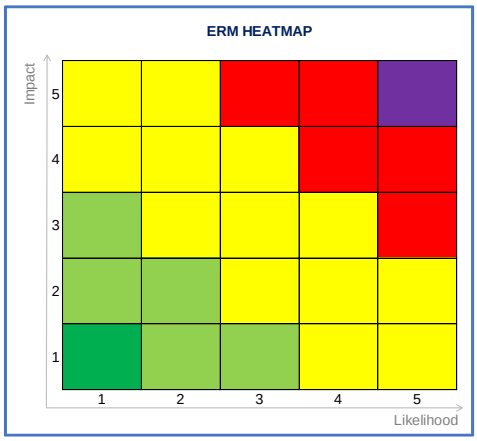
Different dimensions can be used to measure how likely the risk could materialize and are based on different approaches defined by Global RM (i.e., probability of occurrence, frequency of occurrence, qualitative explanation).

Risk Management Matrix (Heatmap)

The list of identified relevant risks constitutes the Global RM risk portfolio. After the assessment of impact and likelihood, the ranking of each relevant risk within the portfolio must be

established to allow prioritization and a transparent report. The ranking is defined using a 5x5 Matrix (Heatmap). Figure 3 shows the Global Risk Management Matrix.

Figure 3:



3.3.4 Risk Response

The risk treatment strategy depends on the acceptable target risk level for the respective risk. General fundamental treatment options are either taking the risk (accepting it as it is) or (further) mitigating it (reducing either the likelihood of the risk materializing or the potential impact in case it materializes).

The RO decides on the target risk level under consideration of risk appetite statements, if available, and initiates an adequate risk treatment strategy. When the decision is to (further) mitigate the risk, the RO is also responsible to set up the respective risk mitigation actions with due dates and responsibilities. RM department may support the ROs with regards to defining suitable risk mitigating actions.

The action plans of the Risk Response should also be prioritized in accordance with the level of influence on the target risk level for the respective risk. Compliance and ESG-related action plans are considered high priority.

3.3.5 Risk Review, Revision & Monitoring

The RO has the responsibility to regularly monitor the risk outside of the scheduled RM Cycles. In case of changes on Impact or Likelihood, the RO reviews and eventually modifies the treatment strategy of the specific risk and informs Global RM. Furthermore, the RO continuously monitors the risk development to detect possible risk materialization at an early stage and to react immediately, informing the right responsible and the Global RM.

As a result of the review activity a risk can be removed from the Global RM portfolio in cases of the risk has been mitigated, materialized, obsolete or has been mitigated to a residual risk level which is below the defined thresholds and all the planned mitigation actions have been completed. The responsible LT member or Global RM approves the removal of a risk from the Global RM portfolio.

Additionally, whenever we have a change on our ESG Strategy we review all the ESG-related risks and ESG-related action plans and whenever and M&A project starts we will start a specific Risk Assessment, evaluating and reporting the risks involved.

3.3.6 Risk Reporting

Global RM risk portfolios, presented in an integrated Matrix (heatmap) and a standard format (risk cards), are reported to the Assurance Committee after the cycle is completed or as needed (*ad hoc*). The entire risk portfolio and risk response / mitigation strategy are reviewed and discussed by the Assurance Committee for approval and prioritization.

All the risks are categorized, including ESG-related risks, Compliance, Financial, etc.

Global RM consolidates all critical risk responses in a Risk Watchlist, updating status with the RO and reporting pending actions as needed.

3.3.7 Framework Monitoring & Review

The Global RM department continuously monitors and reviews company´s RM framework, focusing on Information Technology and Agility and to ensure appropriate quality of process design, implementation, and outcomes.

3.3.8 Risk Management System

The RM process is technically supported by “RMS” (Risk Management System) SharePoint. This tool is used to document risk descriptions, assessments, and treatment plans. It also facilitates risk reporting and follow-up on mitigation actions.

3.4 Implementation, Training and Control

Global RM periodically provides Risk Awareness activities for the entire organization driving a trustful and pro-active risk culture and provides specific onboarding / update trainings to Managers that have an assigned role in the process.

Any organization of Envu that is considering implementing a local / functional RM process in its area of responsibility shall align with Global RM before the implementation and follow the framework described in this Policy when feasible.

4 Appendix

4.1 Definitions and Abbreviations

ERM – Enterprise Risk Management

ESG – Environment, Sustainability, and corporate Governance program

First Line of Defense – Line Management

LT – Leadership Team

M&A – Mergers and Acquisitions

RM – Risk Management

RMS – Risk Management System (SharePoint)

RO – Risk Owner

4.2 References

ISO 31000 (https://www.iso.org/iso-31000-risk-management.html)

COSO ERM (https://www.coso.org/SitePages/Guidance-on-Enterprise-Risk-Management.aspx?web=1)

The Institute of Internal Auditors – IIA (https://www.theiia.org/en/standards/international-professional-practices-framework/)

Organization Principles Policy # 1.01

Internal Audit Charter # 1.04

Compliance Management Policy # 1.09

4.3 Change Log

--