RISK MANAGEMENT POLICY

COMPUTER 2000

Revision 01
May 2023

RISK MANAGEMENT POLICY

Table of Contents

Purpose

All activities undertaken by COMPUTER 2000 Bulgaria (the Company) carry an element of risk. The Company recognizes that managing enterprise risk is an integral part of effective governance and management. Risk management is crucial for realizing business goals and maximizing the opportunities to achieve the Company vision and strategy.

This Risk Management Policy aims at providing a structured and focused approach to managing risks. It relates to the identification, assessment, monitoring and mitigation of various risks to our business. Our risk management practices seek to sustain and enhance the competitive advantage of the Company.

Risk Management Framework

Definition

A risk is defined as the effect an uncertainty has on the objectives of the organization and can be both negative (threat) or positive (opportunity).

The Company considers the following broad risk categories:

- Strategic
- Operational
- IT and cyber security
- Human capital
- Legal
- Macroeconomic

Risk Management Process

The risk management process follows five steps illustrated in Figure 1 below.

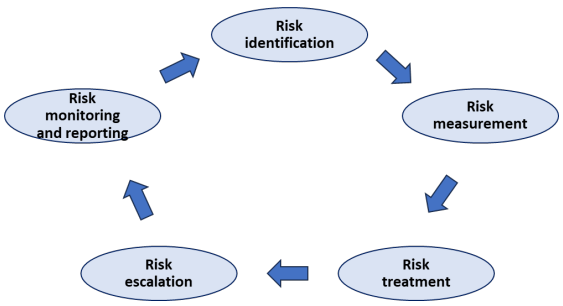

Figure 1: Risk Management Process

Risk Identification aims to review and present what, why and how risks impact the achievement of business objectives, vision and strategy. This includes reviewing relevant

processes, systems, and projects with a view of identifying critical elements that can prevent the achievement of the objectives.

This step is designed to involve all relevant staff members. Any employee can identify a risk and suggest it be captured in the risk register. Thus, managers are to provide the opportunity to discuss risks at any time.

Risk Measurement aims to determine if the risk is acceptable to the Company. It results in prioritising the order and efforts to manage each risk identified. The inherent risk level of each risk is to be assessed in terms of the *likelihood* that the risk will affect the Company's prospects of achieving its business objectives, vision and strategy, and the *impact* on the Company's objective. The assessment requires sound judgment, common sense, and experience.

Once the inherent risk level has been determined, the process requires the development of the relevant actions to mitigate it. These measures are designed to either reduce the likelihood, the impact or both. The resulting likelihood and impact are the residual risk level.

The residual risk level can then be assessed towards the Company's risk appetite for this objective or type of risk, to determine if additional actions are required to mitigate the risk to within the acceptable risk appetite.

Risk Treatment is directed to plan for additional mitigation actions for residual risks outside of the risk appetite of the Company. The options include:

- Terminate the risk – do things differently to remove the risk when feasible
- Treat the risk – take actions to control the risk by reducing the likelihood, the impact or both
- Transfer – pass the management of the risk to a third party, such as via insurance policy or penalty clause
- Tolerate the risk – accept that either nothing can be done at a reasonable cost and effort to mitigate it, or the likelihood and impact levels are acceptable
- Take more – accept more risk with the appropriate controls at place, in the cases when the identified risk presents an opportunity for the Company to achieve its business objectives, vision and strategy

Risk Escalation is needed when the level of the Company that has identified it does not have the proper controls and ability to take mitigation actions. In such instances, the risk is escalated to the next level of authority that may decide how to treat it.

Risk Monitoring and Reporting ensures that risks are monitored and reviewed regularly in line with the fast pace of change in the environment which may produce them.

The Company keeps the risk register up to date. This will ensure the information gathered can be used to identify potential opportunities to exploit and as a source of institutional memory for future managers of similar operations or functions.

Roles and Responsibilities

The core management team is responsible for ensuring that the Company maintains effective risk management and internal control systems and processes.

It is responsible for designing and implementing risk management and internal control systems which identify material risks for the Company and aim to provide the Company with warnings of risks before they escalate. The core management team must implement the action plans developed to address material business risks across the Company.

All employees are responsible for implementing, managing and monitoring action plans with respect to material business risks, as appropriate.

Review of Risk Management Program

The Company regularly evaluates the effectiveness of its risk management program to ensure that its internal control systems and processes are monitored and updated on an ongoing basis.

The core management team steers a risk review meeting on a regular basis to review the framework and make amendments where necessary.