RISK MANAGEMENT POLICY

18th August 2021

Granite company level

1. Overview

Granite's risk management policy describes the risk management practices and responsibilities. The main purpose is to maintain and accelerate the growth of Granite's business and to ensure that the services Granite is providing are secure and operating smoothly. In addition, the aim is to achieve the level of risk management practices, which meets industry standards and the requirements of the customers.

There are mainly two types of risks:

- Business risks are related to Granite's growth and business plans including strategy and operational aspects.
- Security, privacy and continuity risks are related to information security, physical security, privacy and business continuity both in Granite and Granite's services.

All risks are assessed according to their impact and possibility. ISO31000 standard will be used as a reference for defining the actual terms used in the assessments. Risk assessment results will be taken into account when making decisions, defining goals and updating all policies and guidelines.

This risk management policy concerns all of Granite's operations, i.e. all the different areas of business and services. This plan is observed in terms of applicable parts between Granite and its service providers and subcontractors.

2. Organization and responsibilities

Granite's Board of Directors is the highest party making decisions on business risks. The CEO is the highest party making decisions on security, privacy and continuity risks.

The Board of Directors will approve the risk management policy and the amendments made to it. Policy is reviewed annually by the CEO and reported to the Board of Directors.

The CEO is responsible for coordinating risk management and may allocate responsibility for parts of the whole to other members of Granite personnel. The CEO is responsible for organizing a Security Team to handle all security, privacy and continuity risks. The Security Team consists of members with sufficient expertise in the whole domain of the team.

Each employee is responsible for risk management for their own part by operating in accordance with the training and guidelines provided. Each employee is responsible for reporting problems and deviations related to risk management to the CEO or Security Team.

3. Implementation methods and principles

Business risks

- Granite's own web-based tool is used for risk assessments, reporting and managing the risk mitigation actions.
- Granite's Board of Directors will assess and approve the risks at least annually in board meetings.
- Opportunities are assessed together with the risks based on business goals. Framework used for this assessment is defined by the CEO.

Security, privacy and continuity risks

- Granite's own web-based tool is used for risk assessments, reporting and managing the risk mitigation actions.
- Granite's Security Team will assess and approve the risks at least quarterly in team meetings.
- All necessary parties will take part in the risk management process in the specific risk areas.

4. Risk controls

For every risk that has been assessed to medium level or higher, there needs to be proper risk controls identified. After the controls' status has been updated or completed, the assessment of the risk level needs to be updated.