Risk management

TC-SI-550-a.2

Kaspersky created and actively developed its risk management system (RMS), beginning in 2022, and is based on the Global Problem Management process for managing technological risks it previously operated. The RMS ensures the management of operational and technological risks, across individual company departments or units, and also in areas where various functional responsibilities overlap.

The company's fundamental risk management principles were developed based on Russian legislation, Russian Central Bank regulations, and international risk management practices.

Goals and objectives of risk management

The objectives of operational risk management are to identify, assess, aggregate and monitor the scope of Kaspersky's operational risks across all of its divisions. In addition, the company strives to maintain operational risks at an acceptable level, ensuring the sustainable operation and development of its business, implementation of its overall strategy, and the preservation of assets while maintaining the quality of its products and services.

Kaspersky manages technological risks by promptly and proactively identifying them. At the same time, we also act to prevent incidents that may impact the high quality of worldwide products and services, internal IT infrastructure and business continuity.

Objectives of the RMS:

- Ensure that Kaspersky management is aware of key operational and technological risks, including their nature and possible consequences, as well as the level of control of these risks.
- Timely identify and assess the Company's operational and technological risks in all its divisions, including all new businesses, processes, systems and assets, and reduce the probability and magnitude of losses to the Company's operations.
- Ensure the Company's uninterrupted operation.

Principles of operational risk management

- **Creation of a risk-oriented environment at the Company**

Operational risk management is not an isolated process within a specific unit. It is an integral part of the work of each and every Kaspersky employee.

- **Continuity and necessity of the operational risk management process**

Operational risk management procedures apply to business processes and operations that ensure the Company achieves its business goals performs its functions.

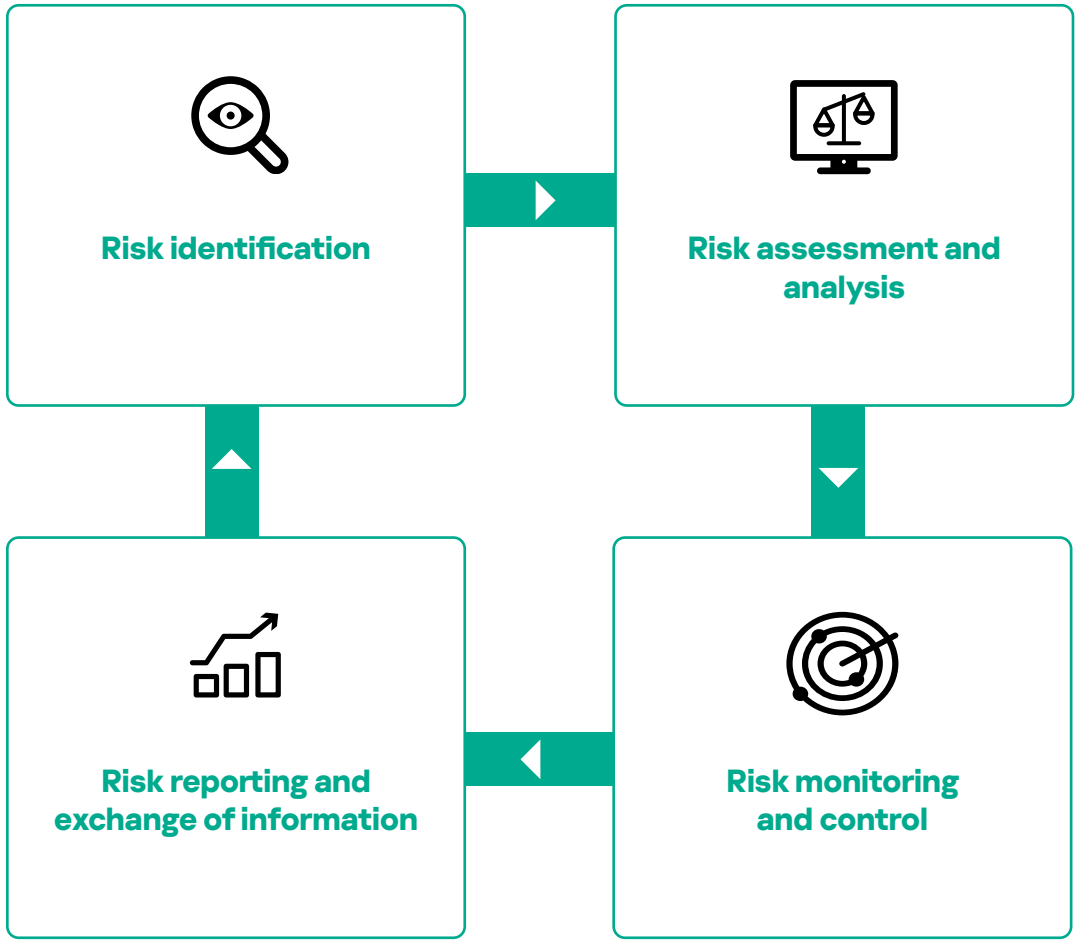
- **Awareness of operational risks for each level of decision-making at the Company**

The Company is creating a system to report on the level of operational risks and prioritizing risks so that decision makers have access to the most up-to-date information about the risks associated with the decisions they make. Thresholds are set for operational risk indicators, and when they are exceeded, higher-level managers are informed.

- **Openness and transparency of procedures and methods used to analyze operational risks**

The Company's risk analysis unit fully describes the approaches it takes to risk assessment in its internal regulatory documents and the procedure for analyzing operational risks. In the future, this will make it possible to assess the effectiveness of the operational risk management system.

Operational risk management process



Identifying risks involves defining and classifying risks that have been detected. A combination of various techniques and tools is used to identify risks. For each risk that is identified, the Company determines its owner, cause of the operational risk event; and assigns a person responsible for risk mitigation measures.

The significance of a risk is assessed and analyzed according to two parameters: an assessment of the Company's actual or potential losses in the event the risk materializes (impact) and the probability of an operational risk event occurring.

The Company regularly **monitors** actual and potential losses. This process involves identifying sources of risk, critical vulnerabilities in current business processes, compliance with the established risk level and violations of the acceptable risk level.

Kaspersky risk **control** is continuously conducted and primarily aims to:

- Comply with established procedures and powers when making and implementing management decisions that affect the interests of the Company and its customers.
- Manage operational risks that arise in the course of the Kaspersky's daily operations.
- Take timely and effective measures to help eliminate any shortcomings or violations that are found in the Company's activities.

Reporting and exchanging information about operational risks

Kaspersky has implemented a multi-level risk reporting system to facilitate the adoption of objective and effective management decisions. Such a reporting system contains information about actual or potential losses the Company could incur due to the materialization of operational risks, a breakdown of the categories of operational risks. This includes of operational risks as well as a quantitative analysis of events, map of operational risks and information about preventive and subsequent measures to minimize losses for the Company.

Kaspersky's CEO receives an annual report identifying the most significant risks and operational risk events. A quarterly report on operational risks is also presented to the governing board. In addition, the Company regularly discusses the status of incidents and risks with the department heads, managers and employees of its structural units.