

Risk management

Our Company has implemented and consistently develops a proactive risk management system focused on responding promptly to internal and external challenges.

Kaspersky not only strives to minimize the consequences of risks, but also seeks to prevent them materialising at an early stage.

When developing our risk management principles, we accounted for the requirements of the legislation of the Russian Federation, the regulations of the Central Bank of the Russian Federation, as well as international risk management practices. In developing the system, we focus on state-of-the-art approaches and the best industry standards related to risk management.

Development of our risk management system

In 2024–2025, Kaspersky actively developed a risk management system (RMS) based on the Global Problem Management (GPM) process, which was created from the outset to manage technological risks. New business units and subsidiaries were involved in the process, and user-friendly dashboards were developed for routine monitoring of risks and incidents.

Goals and tasks of risk management

Operational risk management seeks to promptly identify risks and mitigate their impact, to ensure that the Company can operate and grow sustainably, and to maintain the high quality of its products and services amid a highly turbulent external environment.

As part of the GPM process, the Company manages technological risks by promptly identifying them and continuously working to mitigate them. This approach helps prevent incidents related to the quality of products and services, as well as the functioning of internal and external IT infrastructure.

Key tasks of risk management:

1. identify risks that could significantly impact the Company or users of its products and services
2. analyze and assess the identified risks
3. develop and implement risk mitigation plans
4. monitor and control both new and previously identified risks, including cases where they cannot be completely eliminated.

Principles of operational risk management

Create a risk-oriented environment

Risk management is an integral part of the Company's activities and is not limited to the functions of a single business unit. The GPM process facilitates risk management both within individual departments and at the intersection of the areas of responsibility of several business units. As the RMS evolves, new functions and teams are involved in the process.

Ensure that the risk management process is continuous and mandatory

Risk management is an ongoing process. Within the business units involved in GPM, staff are assigned to help identify, analyze, and assess risks and develop risk mitigation plans. New risks and incidents are synchronized at least once every two weeks, and the status of active risks is updated at least once per quarter.

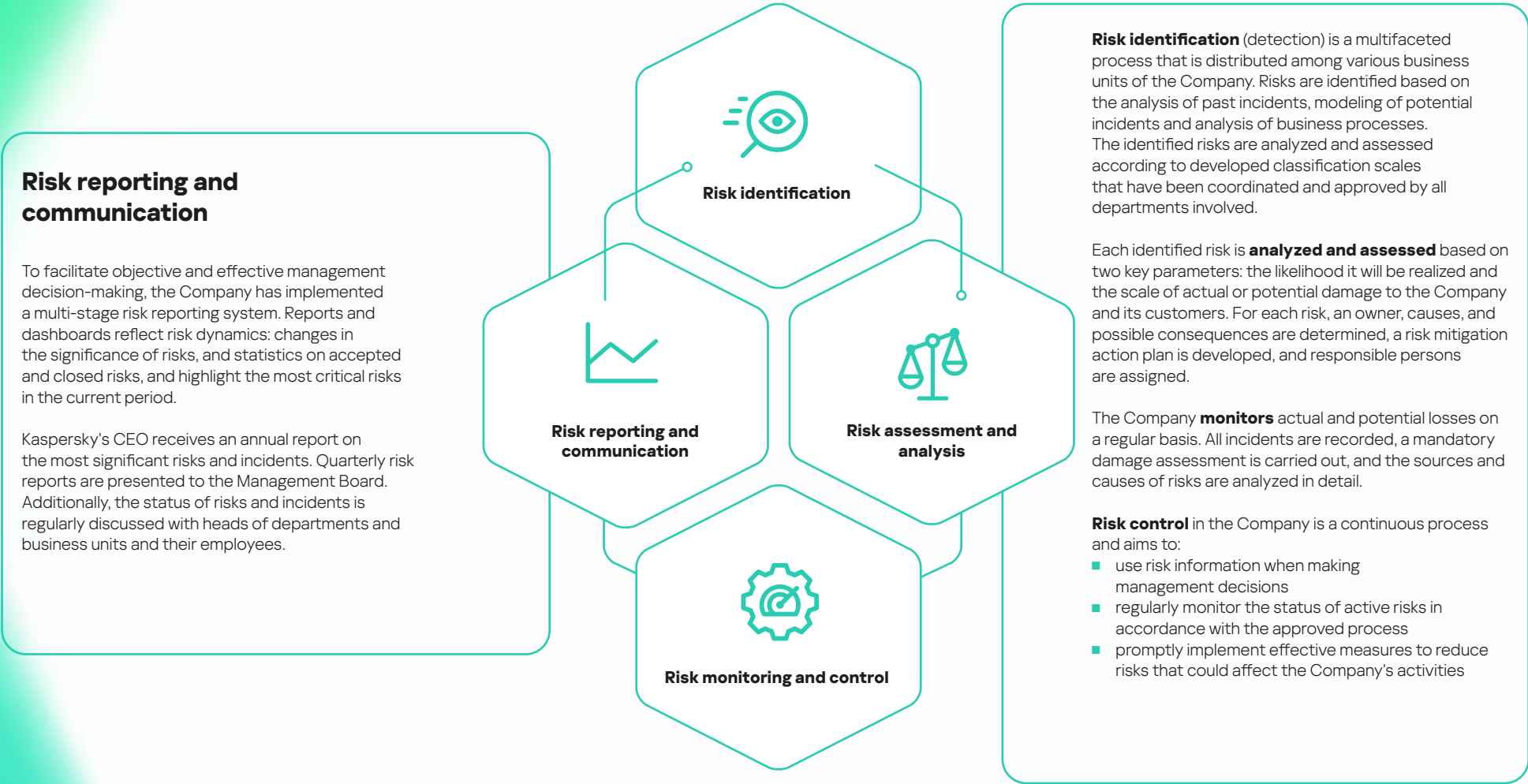
Keep managers informed at every level of decision-making

The Company has a communications and reporting system that allows managers at all levels to be promptly informed about the current risk map (active, accepted, and closed risks) associated with decisions they are making. This creates the basis for risk-based decision making.

Ensure openness and uniform assessment methods

To analyze risks, the Company uses uniform classifications and assessment scales, which are set out in the GPM documentation and used by all participating business units. If disagreements arise or methodological shortcomings are identified, facilitated sessions are held and then the classifiers and assessment methods are refined.

Operational risk management process



ESG risk management

At Kaspersky, senior managers and department heads are responsible for managing sustainable development risks. During the reporting period, the Company identified two significant¹ ESG risks: changes in the political and economic environment across its regions of presence, including regulatory changes, and the risk of increasing cybercrime.

Key ESG risks

SASB TC-SI-550a.2

Risk of changes in the political and economic environment across its regions of presence

Why the risk matters

Potential legislative changes could significantly limit the Company's ability to conduct business in a country/region where it has a presence

Risk management measures in 2024 and 2025

- Continuously monitor legislative changes in the political and economic environment across its regions of presence in order to promptly identify potential risks
- Ensure the Company and individual employees belong to various industry organizations in order to communicate with regulatory authorities
- Participate in public consultations conducted by government authorities in countries/regions where the Company has a presence in relation to draft amendments to existing regulations or the introduction of new regulations in order to promote the Company's position
- Further develop the GTI to allow customers, partners, and regulators to verify the reliability of the Company and its products

¹ Significant risks are risks that, in the opinion of the Company's management, may have a material impact on operating results.
² Threat intelligence is the collection, analysis, and interpretation of data on existing and potential cyberattacks.

Risk of increasing cybercrime

Why the risk matters

Currently, there has been a decline in the level of cooperation between law enforcement agencies and private companies in various countries. To prevent a surge in cybercrime, it is important to maintain cooperation and the exchange of expertise with the private sector.

Risk management measures in 2024 and 2025

The Company continued to actively cooperate with law enforcement agencies and international organizations during the reporting period:

- it contributed to several operations under the auspices of INTERPOL, including [Synergia](#) and [Synergia II](#), [Serengeti](#) and [Serengeti 2.0](#), [Red Card](#) and [Secure](#)
- it helped ensure the safety and security of major international sporting events such as [the Paris 2024 Summer Olympics](#) and [the Formula 1 Singapore Grand Prix 2025](#)
- it shared data for two editions of the INTERPOL African Cyberthreat Assessment Report ([2024](#), [2025](#)), which present the cyber threat and attack landscape on the African continent
- it participated in three meetings of expert working groups under the auspices of INTERPOL, held in Bangkok, Hanoi and Doha, sharing expertise in researching cyber threats with representatives of law enforcement agencies, cybersecurity agencies, other government organizations and private companies
- it participated in the formation of feedback and proposals for several documents developed under the auspices of the UN, including the Convention against Cybercrime and the Global Digital Compact
- it signed memorandums of understanding with AFRIPOL and several national cybersecurity regulators

Realized risks

SASB TC-SI-220a.5

During the reporting period, the following identified risks were realized amid geopolitical instability:

- termination of cooperation between individual counterparties and Kaspersky
- difficulties with paying for goods and services abroad

On June 20, 2024, the US Department of Commerce announced its decision to prohibit the sales and distribution of Kaspersky software in the United States. Following the release of the Final Determination, Kaspersky has stopped the sales of its cybersecurity products in the country and started to gradually wind down its U.S. operations and eliminate U.S.-based positions. Kaspersky maintains that the Department of Commerce made its decision based on the present geopolitical climate rather than on a comprehensive evaluation of the integrity of Kaspersky's products and services. The ban didn't cover Kaspersky's informational or educational products and services such as Kaspersky Threat Intelligence² and Kaspersky Cybersecurity Training, as well as Kaspersky consulting or advisory services (including SOC Consulting, Security Consulting, Ask the Analyst, and Incident Response), which continue to be available in the U.S. market.

Plans for 2026

In 2026, Kaspersky plans to focus on systematizing and aggregating its accumulated risk database, as well as further optimizing reporting formats and analytical tools.