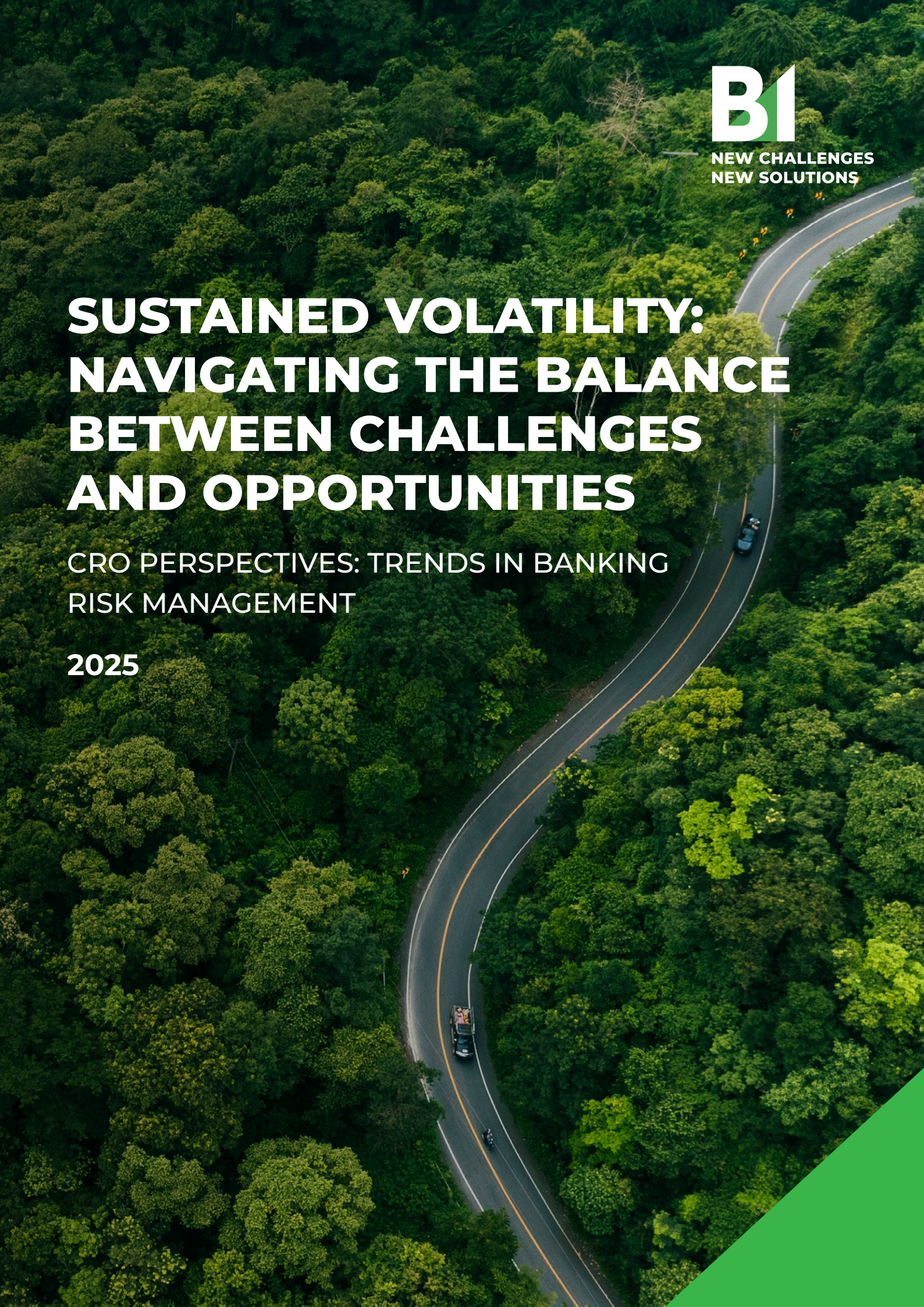


NEW CHALLENGES
NEW SOLUTIONS

SUSTAINED VOLATILITY: NAVIGATING THE BALANCE BETWEEN CHALLENGES AND OPPORTUNITIES

CRO PERSPECTIVES: TRENDS IN BANKING RISK MANAGEMENT

2025

CONTENTS

FOREWORD

GENNADIY SHININ

Partner, Financial Services Leader

MICHAIL TSIBULEVSKY

Partner, Head of Financial Services Consulting

The Russian banking sector continues to evolve, driven by a wide range of dynamic internal and external factors. Geopolitical and macroeconomic shifts, sanctions pressure, regulatory challenges, emerging technologies and changing consumer behavior all demand significant investment and effort from banks as they adapt and strive to remain competitive.

Despite these substantial pressures, the sector demonstrated strong resilience in 2024. Data from the Bank of Russia suggests that net profit rose year-on-year to RUB 3.8 trillion.[1] Meanwhile, market sentiment towards the economic outlook remains cautious and skeptical. A 2024 survey of Chief Financial Officers (CFOs) by B1 and NCR[2] reveals that a more pronounced increase in the cost of risk is expected across all segments compared to the previous year. Inflationary pressures also remain elevated, while monetary policy easing is projected for late 2025 or early 2026.

This study aims to explore and compare banks' expectations around systematic risk assessment and management, and to analyze challenges and opportunities currently shaping the agenda of Chief Risk Officers (CROs).

The survey captures the perspectives of 24 credit institutions of varying size and structure. Of these, 46% are banks with total assets below RUB 500 billion and 29% are subsidiaries of foreign banking groups. Collectively, the participating institutions represent 78% of the total assets in the Russian banking sector.[3]

This is the first comprehensive study of its kind in the Russian market. Going forward, we plan to publish annual updates, providing insight into how the sector's views and expectations on current and emerging risks evolve over time.

We extend our sincere thanks to all respondents for their thoughtful input and detailed commentary. Their contributions have formed the basis for a meaningful analysis of risk management practices across the Russian banking sector and helped highlight the top priorities and most pressing concerns facing today's risk leaders.

---

1 Russian Banking Sector Development, December 2024 (Bank of Russia, https://cbr.ru/Collection/Collection/File/55056/razv_bs_24_12.pdf)

2 Adaptation and Stability: How the Banking System Will Navigate 2024 (https://b1.ru/analytics/banking-trends-survey-march-2024/)

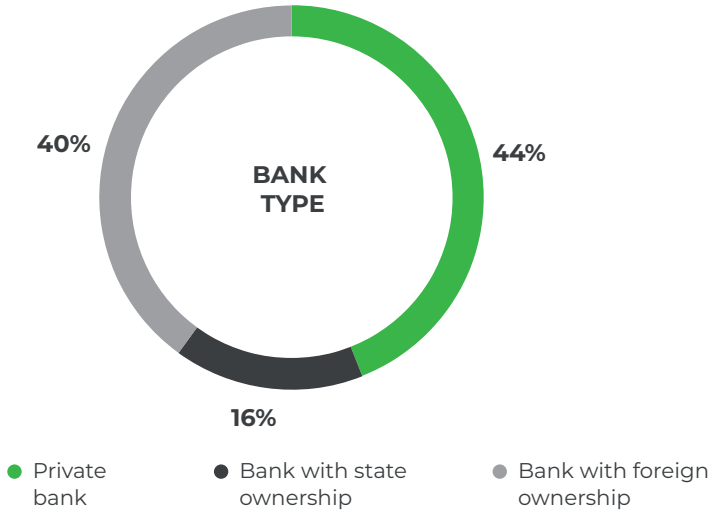
3 Monetary Policy Guidelines for 2025–2027 (Bank of Russia, https://cbr.ru/Content/Document/File/165597/on_eng_2025(2026-2027).pdf)

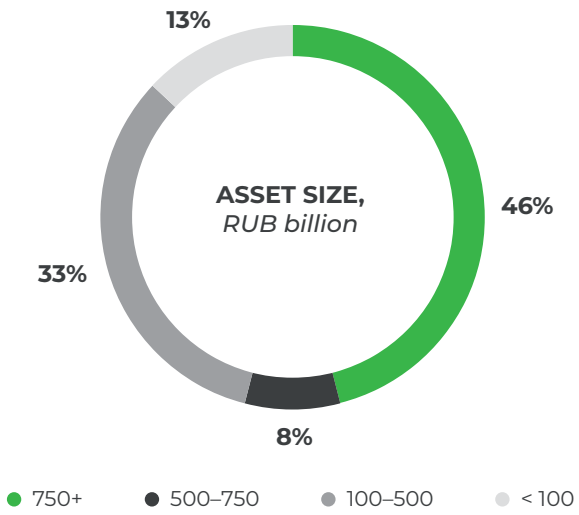
RESPONDENT PROFILE

24 credit institutions across Russia, including SIFIs[4]

78% of the total assets in the Russian banking sector

79% of respondents belong to banking groups





[4] Systemically important financial institutions

KEY FINDINGS AND INSIGHTS

RISK MANAGEMENT SYSTEM

DRIVERS OF DEVELOPMENT

88% Leadership expectations

71% Employee engagement

50% Regulatory requirements

NEW OPPORTUNITIES

Enhancing capital management through advanced approaches

Embedding new technologies and AI into core processes

KEY CHALLENGES

- Significant effort needed to implement new regulatory requirements
- Persistent market volatility and growing relevance of credit and interest rate risks
- Low data management maturity, hindering the development of information systems and adoption of new technologies
- Upskilling employees and developing future-ready capabilities
- Strengthening risk culture across the first line of defense

01

CROs note the **rising significance of traditional risks**—credit, liquidity and interest rate risks—for maintaining effective banking operations and achieving strategic goals. This shift is largely driven by ongoing geopolitical tensions, monetary policy trends and an evolving regulatory landscape shaped by the Bank of Russia.

02

The **base rate remains high**, with a possibility of further hikes should disinflation prove slower than expected. While market inflation expectations continue to run high, most participants agree that the peak of monetary tightening has passed. Predictably, a slowdown in the pace and volume of lending is observed across both corporate and retail segments, except for subsidized loans, as banks anticipate a higher cost of credit risk in 2025.[5]

Looking ahead to 2025–2026, the Bank of Russia will focus on several key regulatory areas: tightening capital adequacy standards, introducing more advanced risk quantification approaches, strengthening requirements for managing specific risk categories, and launching initiatives to foster competition and enhance consumer protection. These developments will require banks to be more agile and allocate additional resources to ensure timely compliance.

Our analysis indicates that risk management in the Russian banking industry is undergoing a profound transformation, as traditional challenges intertwine with emerging issues linked to information technology (IT) risk management. Regardless of size, banks face a largely similar set of top risks. Key trends shaping the future of risk management include tighter regulations, the adoption of new technologies and software, shifts in the macroeconomic and geopolitical landscape, and an increasing focus on data quality.

03

The **emergence of new technologies**—such as the use of artificial intelligence and machine learning in business and risk management processes, the digitalization and automation of data handling, import substitution, and the rollout of new IT systems—has a **dual impact on risk management.** On the one hand, these innovations drive process optimization and efficiency, as well as enhance the quality, depth and speed of analytics. On the other hand, they give rise to a host of new risks, from hidden vulnerabilities and implementation flaws to challenges in integrating new types of algorithms into existing model risk management procedures. In some cases, the deployment of advanced algorithms may require clarification from the Bank of Russia and could be subject to restrictions under evolving regulatory requirements.

04

The **persistent issue of immature data quality management is affecting more areas**—from the automation of a growing range of regulatory reporting to the use of advanced risk assessment approaches, and the adoption of AI and machine learning.

The **Bank of Russia continues to place a strong emphasis on combating cyber fraud,** a concern shared by market players as new types of cyber threats come to the fore. At the same time, shifting consumer behavior and intensifying market competition are pushing banks to strike the right balance between caution and innovation.

Effective management of data quality is becoming a cornerstone for robust risk management systems. While most banks have yet to appoint a dedicated Chief Data Officer (CDO), many favor a hybrid model where the CRO and the CDO work closely together.

Efforts to substitute imported software are hindered by multiple hurdles, from a lack of mature domestic alternatives to high implementation costs, resulting in diverse budgeting strategies across banks.

Many institutions are either using or planning to adopt in-house software or have already transitioned to domestic solutions.

[5] Monetary Conditions and Monetary Policy Transmission Mechanism: Information and Analytical Commentary, Bank of Russia, March 2025 (https://cbr.ru/Collection/Collection/File/55578/DKU_2503-33_e.pdf)

05

Emerging regulations around artificial intelligence in Russia could soon add new pressures on banks, potentially imposing stringent requirements that financial institutions need to start preparing for today.

06

Amid evolving regulatory landscapes, rapid tech adoption and rising competition, the **foundation of an effective risk management system lies in people.** Right now, building a solid risk culture and developing relevant skills among employees is more of a challenge than a strength for many banks. Yet, improving in this area will not only help banks anticipate new trends and technologies, and better identify and manage risks, but also minimize the impact should those risks come to pass.

The study has revealed significant differences in the maturity of risk culture across the three lines of defense. For CROs, raising risk awareness within business units remains a top priority. Additionally, there is also a growing emphasis on developing staff capabilities in the domains of integrated risk management, data analysis and soft skills. In the coming years, demand is set to rise for expertise in artificial intelligence, data science and operational resilience.

PRIORITY AREAS FOR THE DEVELOPMENT OF BANKING RISK MANAGEMENT SYSTEMS

As identified by CROs

ADAPTING TO REGULATORY CHANGE

MANAGING DATA QUALITY

ENHANCING INFORMATION SECURITY RISK FRAMEWORKS

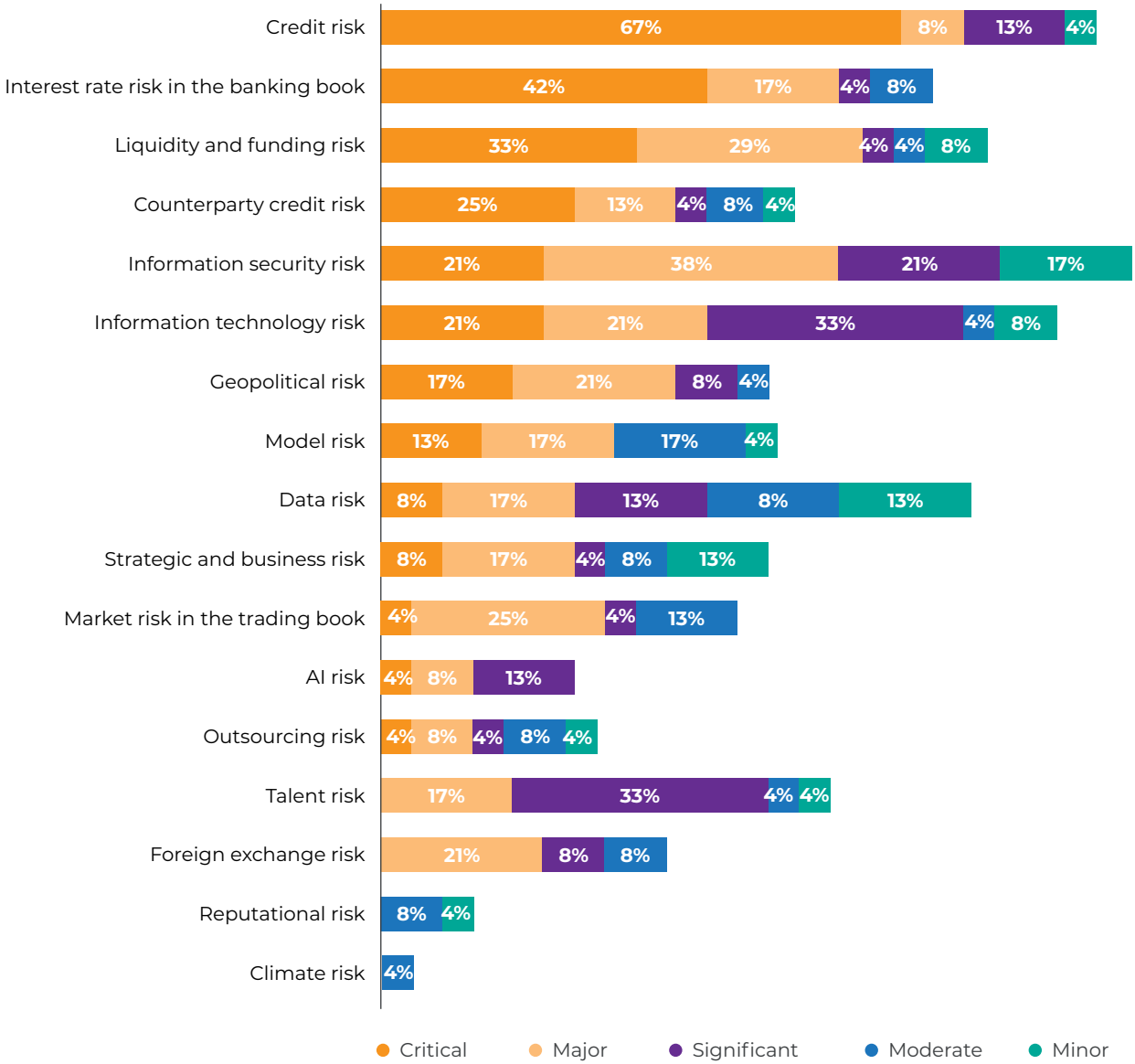
OPTIMIZING CAPITAL ALLOCATION FOR RISK COVERAGE

DEPLOYING AI AND MACHINE LEARNING IN LINE WITH REGULATORY REQUIREMENTS AND RESTRICTIONS

BUILDING A STRONGER RISK CULTURE AND UPSKILLING STAFF

CRO PRIORITIES FOR THE YEAR AHEAD

WHICH RISKS ARE EXPECTED TO BE THE MOST SIGNIFICANT OVER THE COMING YEAR IN TERMS OF THEIR POTENTIAL IMPACT?*



* Respondents were asked to select up to 10 key risks and rank them by significance. The same level of significance could be assigned to multiple risks. Responses were grouped based on the following ranking: 1–2 – critical risks, 3–4 – major risks, 5–6 – significant risks, 7–8 – moderate risks, 9–10 – minor risks.

Existing traditional risks are evolving, prompting the need to adapt current management methods and tools. For most CROs, priority risks include credit risk, interest rate risk in the banking book, liquidity and funding risk, information security risk (including cyber risk), and information technology risk.

TRENDS OBSERVED IN THE BANKING SECTOR

01 Current monetary policy drives focus on managing credit risk, interest rate risk, and liquidity risk

The portfolios of large banks are still mostly made up of long-term loans—including mortgages—issued before 2022 at relatively low rates. With the base rate currently set high and expected to remain elevated in the medium term, banks continue to experience growing interest rate risk.[6] In view of potential rate changes, this risk remains significant.

At the same time, a slowdown in retail and SME lending, reduced demand for funds, and lower welcome premiums[7] have allowed major players to cut deposit rates and somewhat improve margins. A survey of CFOs at large banks showed that about half (51%) anticipate an increase in the cost of credit risk (COR), which could weigh on financial performance in 2025.[8] The Bank of Russia's regulations aim to curb banks' risk appetite by, for example, raising risk-weight add-ons for loans to highly leveraged borrowers, and introducing measures to mitigate concentration risk.

The Bank of Russia has indicated that further rate hikes may be necessary if the pace of disinflation proves insufficient to bring inflation back to target by 2026.[9]

While market inflation expectations remain high, most survey participants believe that the peak of monetary tightening has passed, and anticipate possible easing of policy in the late first half or early second half of 2025.[10]

02 As digitalization accelerates, new vulnerabilities emerge, reinforcing the ongoing need for robust information security

Protecting against cyber threats stays front and center for all players in the banking sector, including the mega-regulator. To combat cyber fraud, the Bank of Russia has introduced requirements for new protective measures, such as cooling-off periods for loans, faster information exchange with credit bureaus, and plans to deploy new tactics to crack down on droppers.[11]

In parallel, the Ministry of Digital Development is considering amendments to the law on combating telephone and Internet scammers that would oblige banks to partially compensate clients for stolen funds, increasing the impact from information security risk events.[12]

In 2024, anti-fraud systems at large banks reportedly achieved a 99.7% success rate.[13] However, banks acknowledge that they are not fully prepared for emerging information security threats, especially with the rise of AI technologies that can enable criminals to completely overcome language barriers, giving their attacks and fraud a global reach. Meanwhile, domestic regulations targeting local banks will offer limited protection to victims, as phishing schemes become increasingly sophisticated and complex.

Evolving and ever-changing, intricate threats are forcing banks to develop new control methods, such as employee-initiated transaction verification calls via mobile apps, reverse verification of employees by clients through apps, or the implementation of services that recognize scam calls, including those powered by AI.

---

6 Monetary Policy Guidelines for 2025–2027 (Bank of Russia, https://cbr.ru/Content/Document/File/165597/on_eng_2025(2026-2027).pdf)

7 Frank RG: The Deposit Market Is Flooded with New Clients — Bank Abusers (RBC, https://www.rbc.ru/quote/news/article/680898119a79474a1a2bfaa8)

8 Cautious Optimism and a Bet on Long-Term Growth: How the Banking System Will Navigate 2025 (https://b1.ru/analytics/b1-banking-trends-2025-survey/)

9 Monetary Policy Guidelines for 2025–2027 (Bank of Russia, https://cbr.ru/Content/Document/File/165597/on_eng_2025(2026-2027).pdf)

10 Monetary Conditions and Monetary Policy Transmission Mechanism: Information and Analytical Commentary, Bank of Russia, March 2025 (https://cbr.ru/Collection/Collection/File/55578/DKU_2503-33_e.pdf)

11 Cyber Fraud: Countering New Threats, 2025 (Bank of Russia, https://www.cbr.ru/content/document/file/174841/cyberfraudcounteringnewthreats.pdf)

12 Victims of Fraudsters May Be Permitted to Seek Compensation from Banks with Security Gaps (Interfax, https://www.interfax.ru/russia/1016427)

13 Cyber Fraud: Countering New Threats, 2025 (Bank of Russia, https://www.cbr.ru/content/document/file/174841/cyberfraudcounteringnewthreats.pdf)

03 The evolution of information systems brings both new opportunities and additional risks

Information technology risk remains significant amid active import substitution, restricted support for foreign solutions, frequent system failures, and the emergence of new technologies—including AI—that introduce new risks, ranging from algorithm errors to massive failures with critical consequences for the entire bank.

Additionally, future AI-related regulatory requirements (see *New Technologies: Opportunities and Challenges for Risk Functions*) will also place added pressure on banks over the course of their implementation.

04 Market players do not anticipate a significant impact from the materialization of conduct risk

Despite the Bank of Russia introducing new regulatory requirements related to conduct risk and tightening consumer protection standards, none of the respondents identified conduct risk as significant in terms of its impact.

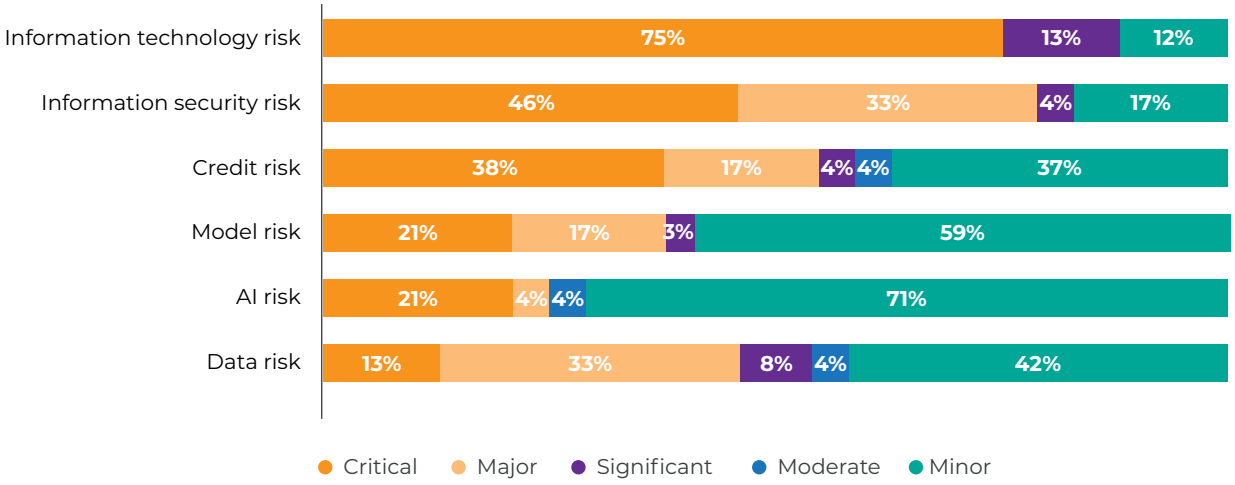
The Bank of Russia aims to increase fines on banks for violating consumer rights concerning financial products and services, ensuring that each violation has a tangible effect on the bank's income, and that any benefits gained do not outweigh the penalties[14]

Some respondents rate this risk as moderate based on the budget allocated to improve its management framework.

05 Banks primarily allocate their budgets to improving the management of traditional risks in the coming year

The observed trends call for additional investments in developing risk management systems.

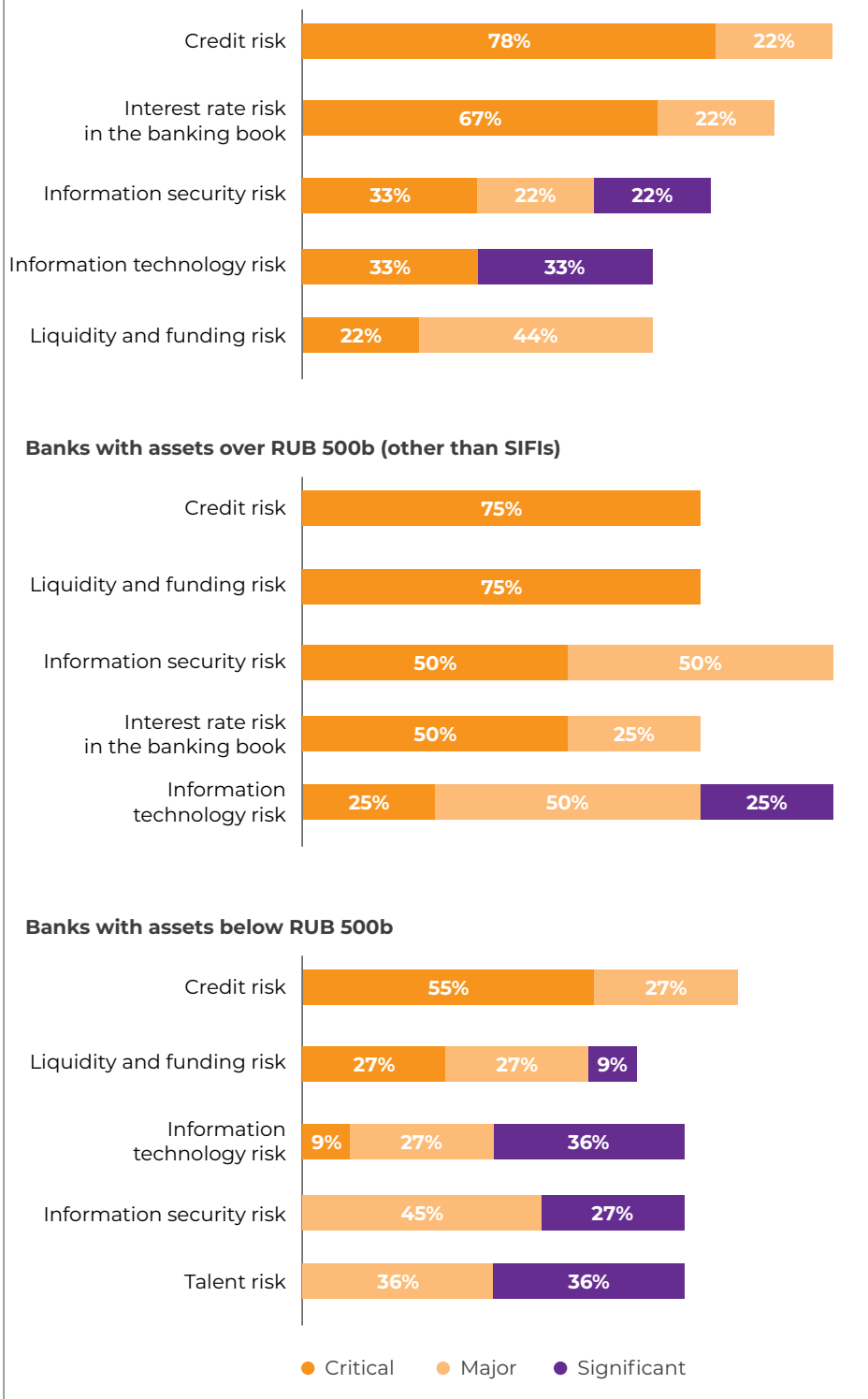
WHICH RISKS ARE EXPECTED TO BE THE MOST SIGNIFICANT OVER THE COMING YEAR IN TERMS OF PLANNED BUDGET?*



* Respondents were asked to select up to 10 key risks and rank them by significance. The same level of significance could be assigned to multiple risks. Responses were grouped based on the following ranking: 1–2 – critical risks, 3–4 – major risks, 5–6 – significant risks, 7–8 – moderate risks, 9–10 – minor risks.

[14] Protective Measures: The Central Bank Proposes to Increase Fines for Banks for Violating Consumer Rights (Expert RA: https://raexpert.ru/researches/publications/iz_apr05_2025/)

WHICH RISKS ARE EXPECTED TO BE THE MOST SIGNIFICANT OVER THE COMING YEAR IN TERMS OF THEIR POTENTIAL IMPACT (TOP 5 RISKS)?*



* The figures exclude respondents who rated these risks as moderate or minor. Respondents were asked to select up to 10 key risks and rank them by significance. The same level of significance could be assigned to multiple risks. Responses were grouped based on the following ranking: 1–2 – critical risks, 3–4 – major risks, 5–6 – significant risks, 7–8 – moderate risks, 9–10 – minor risks.

Additionally, the priorities facing CROs were analyzed separately for systemically important financial institutions (SIFIs), banks with assets over RUB 500 billion (excluding SIFIs), and banks with assets below RUB 500 billion.

SIFIs and banks of different sizes show only slight differences in the profiles of their top five most significant risks.

Credit risk, information security risk, information technology risk, and liquidity and funding risks are highlighted as the most significant risks for the coming year across all bank categories.

Information security and information technology risks are more prominent for large banks than for SIFIs, likely due to ongoing import substitution efforts and the adoption of new technologies to address vulnerabilities and threats—areas where SIFIs generally show greater maturity.

For smaller-sized banks, interest rate risk in the banking book is less significant due to a smaller volume of assets exposed, reflecting the structure and specifics of their business.

Smaller banks also report a greater need for qualified personnel and face more challenges related to talent risk.

For a detailed breakdown of responses, please refer to the Annex at the end of the study.

CHANGE AND TRANSFORMATION OF RISK MANAGEMENT

KEY DRIVERS OF THE SHIFT IN RISK MANAGEMENT

01 REGULATORY REQUIREMENTS

Stricter standards for assessing certain types of risk, combined with increased capital pressure from tougher adequacy requirements, are restraining banks' growth potential.

Concentration risk remains a rising concern, fueled by regulatory changes and a lack of sufficient tools and resources to manage it.

02 TECHNOLOGY, AI AND MACHINE LEARNING

The advancement of AI and machine learning, supported by broad access to external data, will drive the shift towards predictive risk management.

At the same time, digitalization introduces new vulnerabilities and raises the need for maintaining process transparency.

03 MACROECONOMIC ENVIRONMENT AND GEOPOLITICS

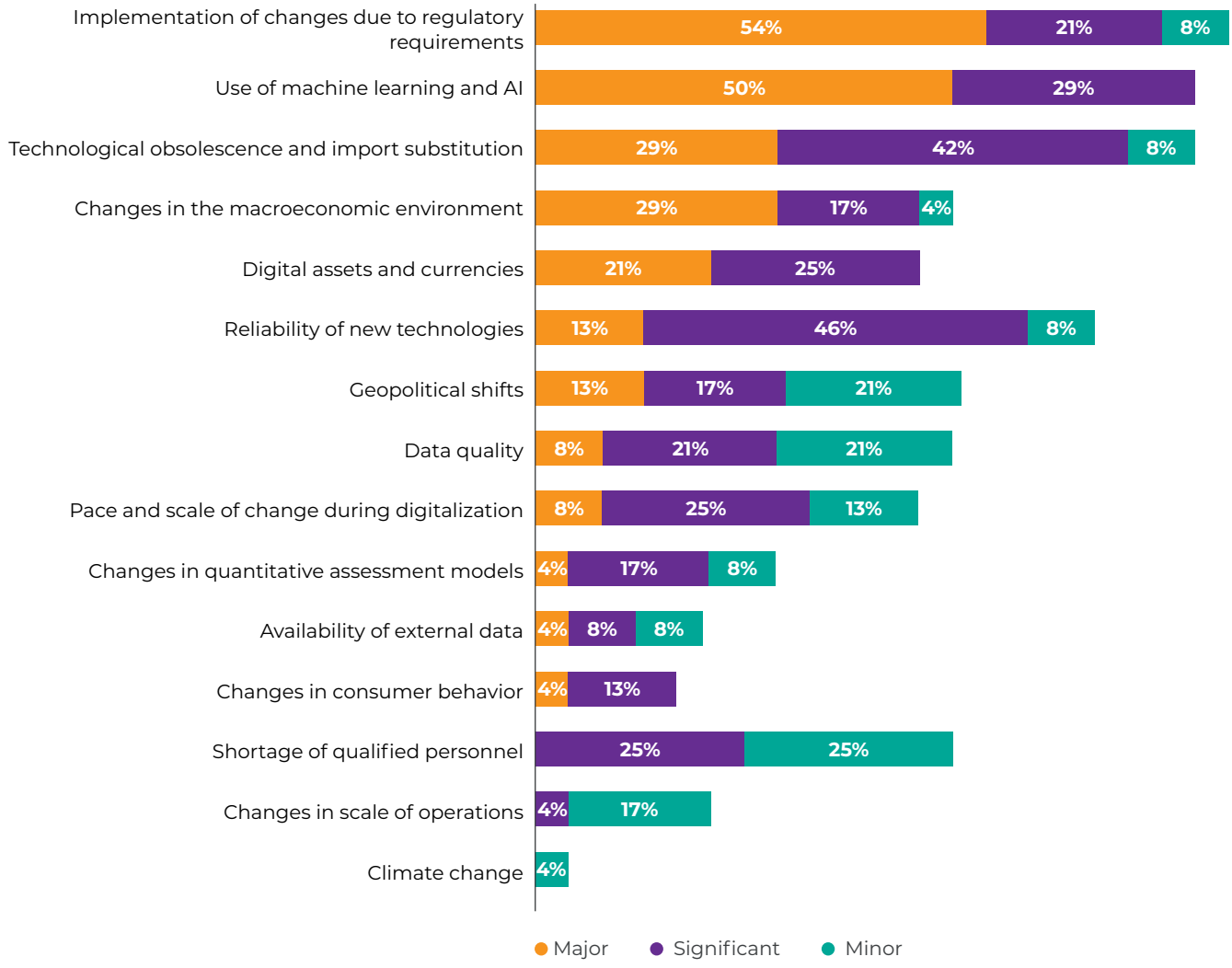
Geopolitical shifts are giving rise to new risks, reshaping regulatory demands, and impacting access to capital markets.

Amid external volatility and shortened planning horizons, banks emphasize the importance of adaptable and agile approaches to business planning and strategy.

04 DATA QUALITY

Banks generally rate their data management systems as established (see *Data Management Maturity*). Yet, data quality is crucial across many aspects of risk management—from enabling advanced risk assessment techniques and ensuring technologies function correctly to enhancing existing tools, accelerating and improving decision-making, and increasing product accuracy.

PLEASE ASSESS THE IMPACT OF INDIVIDUAL FACTORS ON THE EMERGENCE OF NEW RISKS AND/OR CHANGES IN RISK MANAGEMENT OVER THE NEXT FIVE YEARS.*



* Respondents were asked to select up to 7 factors, ranking them from 1 to 7, with 1 indicating the greatest impact. Multiple factors could share the same ranking. Responses were grouped by impact level as follows: 1–2 – major impact, 3–5 – significant impact, and 6 or higher – minor impact. Each respondent's selection contributed to the percentage for the impact level assigned to each factor.

KEY DRIVERS OF RISK MANAGEMENT SYSTEM DEVELOPMENT IN RUSSIAN BANKS

As identified by CROs[15]

75%
Management Board

46%
Board of Directors

LEADERSHIP STANDS OUT AS THE MOST CRITICAL DRIVER, CITED BY THE MAJORITY OF CROs:

- Sets requirements for the risk management system, its key objectives, and develops strategy aligned with the bank's risk profile.
- Cultivates a strong risk culture through clear tone from the top, open dialogue, and by fostering risk-aware behavior among employees, thereby defining the true role of risk management within business processes.

71%
Employees

EMPLOYEES ARE RECOGNIZED BY MOST RESPONDENTS AS VITAL CONTRIBUTORS DUE TO THEIR HANDS-ON ROLE IN RISK MANAGEMENT:

- Actively engage in advancing the risk management system by developing new tools, receiving training, and providing feedback to improve system components.
- Serve as the frontline for early risk detection and reporting, bringing in expertise on their business processes.
- Embed risk management practices into their daily workflows, applying relevant knowledge and tools effectively.

50%
Bank of Russia

THE BANK OF RUSSIA IS IDENTIFIED BY HALF OF THE BANKS AS A KEY DRIVER, GIVEN ITS ROLE AS MEGA-REGULATOR:

- Oversees risk management across a broad range of regulatory areas in the banking sector, including stricter capital adequacy standards, new requirements for specific risks (credit, conduct and outsourcing risks, operational resilience, etc.), the implementation of advanced risk assessment methods, and initiatives to foster competition through special regulatory conditions.

21%
Clients

DESPITE THE TREND TOWARDS GREATER CLIENT AND TRUST CENTRICITY,[16] CLIENTS ARE NOT RECOGNIZED BY RISK MANAGERS AS A KEY DRIVER. HOWEVER, THEY REMAIN FAIRLY IMPORTANT, PARTICULARLY FOR LARGE BANKS AND SIFIs.

[15] Respondents could select multiple options.

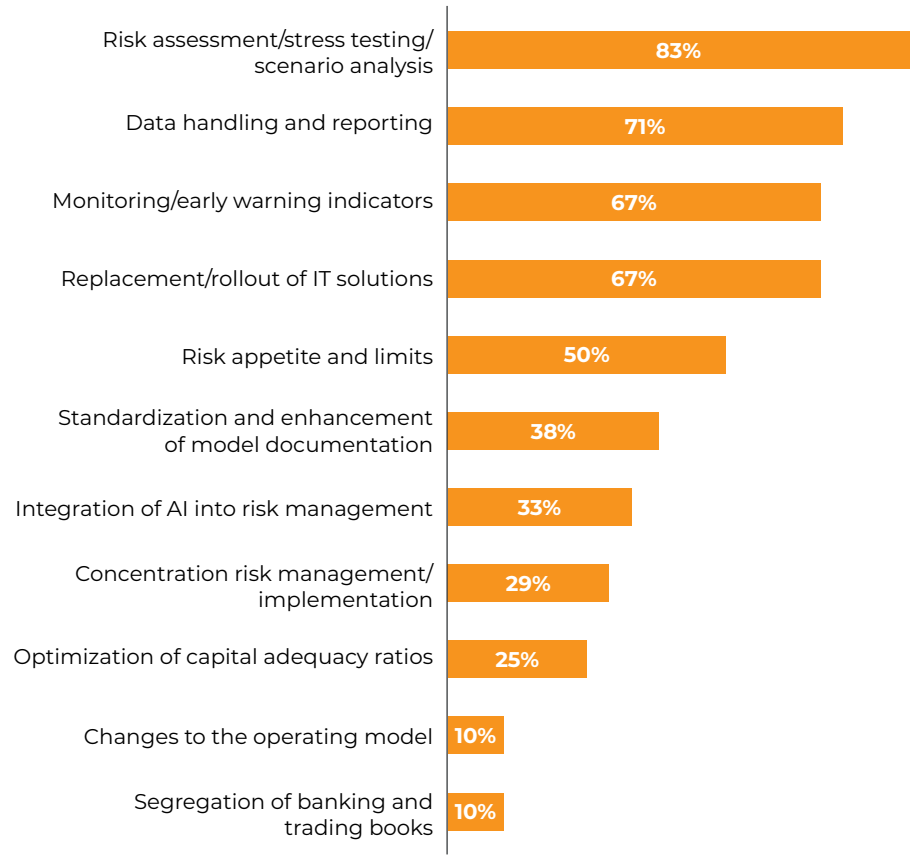
[16] 3x10 Trends in 2025, a study by AFT (https://www.fintechru.org/press-center/issledovaniya/3kh10-trendov-2025-goda/)

The emergence of new factors and drivers impacting the risk management system creates a **clear need to enhance specific risk management tools.**

Many of these changes stem primarily from the **need to adapt to evolving regulatory requirements.** While improvements may span all risk categories, specific areas warrant closer attention:

- Enhancements to risk assessment, stress testing and scenario analysis will be especially relevant for interest rate, credit and liquidity risks.
- Adjustments to risk appetite and limit frameworks affect all risk categories and are driven in part by new clarifications and recommendations from the Bank of Russia regarding ICAAP.[17]
- Standardizing and refining model documentation, alongside strengthening monitoring systems, have been highlighted by some banks as key areas for improving credit risk management, particularly during the transition to the IRB approach.[18]
- Replacement or deployment of IT solutions is largely driven by import substitution efforts and new requirements for certain risk types. Budgets for these initiatives vary depending on a bank's size and ownership structure (see *New Technologies: Opportunities and Challenges for Risk Functions*).
- Data management and reporting will be focus areas during the implementation of regulatory requirements, such as preparations for the IRB transition. Respondents cite data management as a significant challenge when applying advanced credit risk assessment methods (see *Adapting to Regulatory Change*).

WHICH RISK MANAGEMENT AREAS DO BANKS PLAN TO IMPROVE OVER THE NEXT YEAR?*



* Respondents could select one or more options.

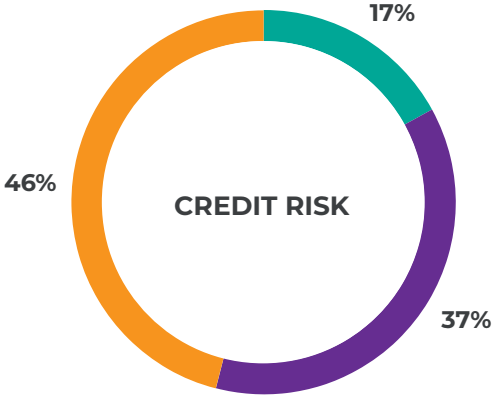
[17] Internal capital adequacy assessment procedures

[18] Internal ratings-based approach

ADAPTING TO REGULATORY CHANGE

WHAT APPROACH DO YOU USE TO CALCULATE CAPITAL ADEQUACY?

- ILM (under Bank of Russia Regulation 744-P) is currently applied
- ILM (under Bank of Russia Regulations 744-P and 814-P) is currently applied
- Transition to ILM (under Bank of Russia Regulation 744-P) is planned within the next 1–5 years
- No plans to apply ILM



- The IRB approach is currently applied
- Transition to the IRB approach is planned within the next 1–5 years
- No plans to apply the IRB approach

In the context of regulatory change and increasing capital requirements, including the introduction of additional capital conservation buffers, **banks are seeking ways to optimize capital management,** including through advanced risk measurement approaches. Some respondents **aim to achieve optimization not only on a standalone basis, but also at the group level.**

Seventy-nine percent of respondents already use or plan to adopt the Basel III Standardized Measurement Approach ILM[19] for operational risk assessment.

Fifty-four percent apply or intend to apply the IRB approach, with the majority being SIFIs and the remainder consisting of banks with assets below RUB 500 billion.

[19] Internal Loss Multiplier

Most respondents (70%) anticipate a positive effect from transitioning to the IRB approach for credit risk assessment. However, half of them believe this benefit may only be short-term.

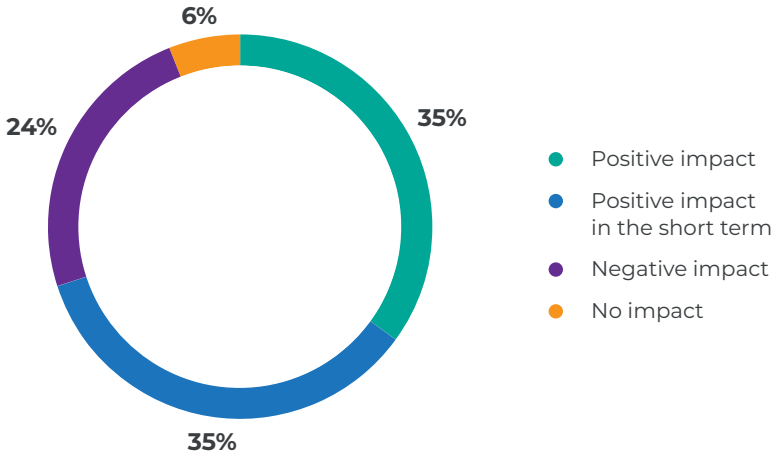
Major banks that have already adopted the IRB approach report improvements in capital adequacy ratios, and average capital savings of approximately RUB 1.7 trillion[20] per institution.

New regulatory requirements for the IRB approach (Bank of Russia Regulation 845-P) have posed several challenges for banks:

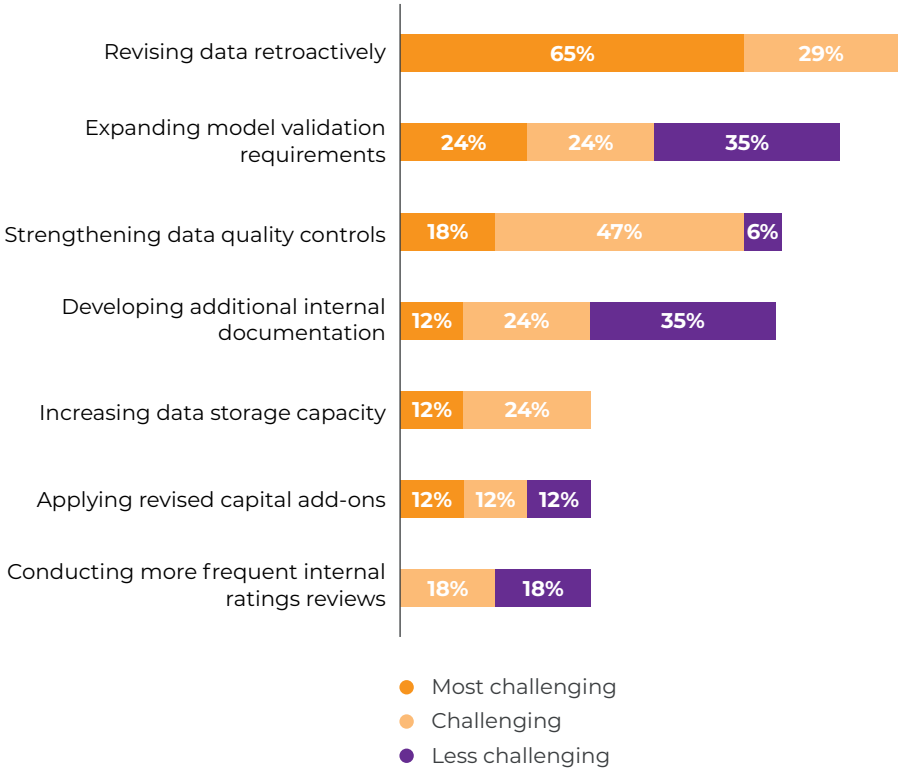
1. Banks that have already transitioned to the IRB approach under Bank of Russia Regulation 483-P must now adapt their credit risk management systems to meet the updated standards.
2. Banks preparing for the transition face a host of new priorities.
3. The Bank of Russia has announced plans to mandate the adoption of the IRB approach by SIFIs in the near future, prompting banks to mobilize resources and align their methodologies, systems, data, internal documentation and processes with the new regulatory framework.

According to 94% of CROs, the most labor-intensive task is the retrospective revision of historical data to reflect updated default definitions. The second greatest challenge is the expanded requirements for model validation. Data management is also a critical focus area within the IRB framework (see *Data Management Maturity*), as stronger data management helps improve data quality across internal systems, leading to greater process predictability and more robust analytics for decision-making.

WHAT IMPACT ON CAPITAL IS EXPECTED FROM TRANSITIONING TO THE IRB APPROACH?



WHAT ARE THE KEY CHALLENGES BANKS FACE DUE TO THE NEW REGULATIONS ON THE IRB APPROACH?*



* Respondents could select up to five challenges and rank them on a scale from of 1 (most challenging) to 5 (least challenging). Equal ranks could be assigned to multiple challenges. Responses were then grouped as follows: 1 – most challenging; 2–3 – challenging; 4-5 – less challenging.

[20] Bank of Russia's 2024 Annual Report (https://cbr.ru/Collection/Collection/File/55239/ar_2024.pdf).

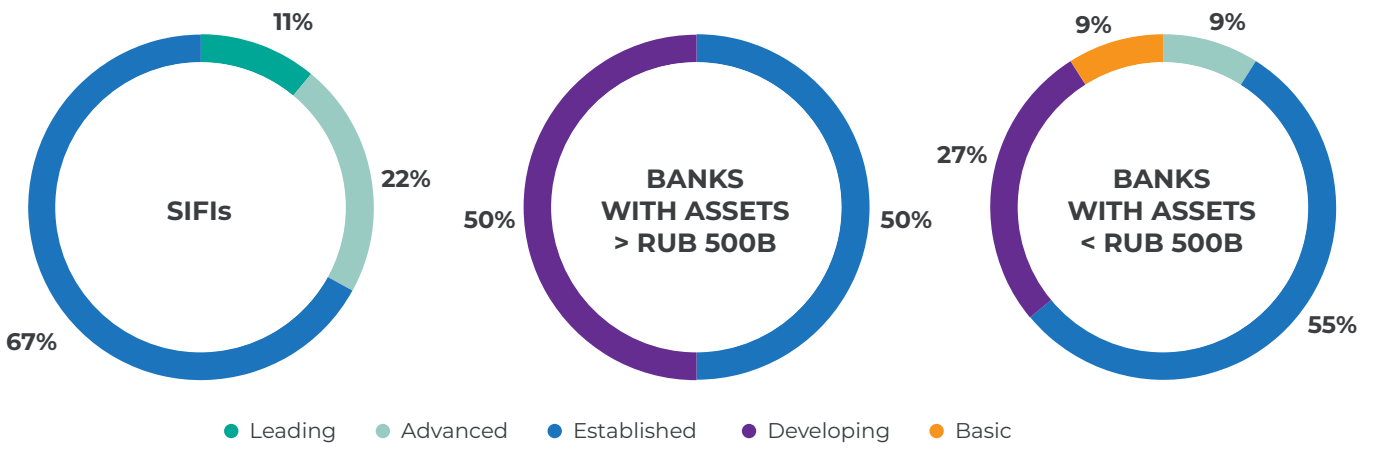
DATA MANAGEMENT MATURITY

HOW WOULD YOU RATE THE MATURITY OF DATA QUALITY MANAGEMENT (DQM) WITHIN YOUR BANK'S RISK FRAMEWORK?

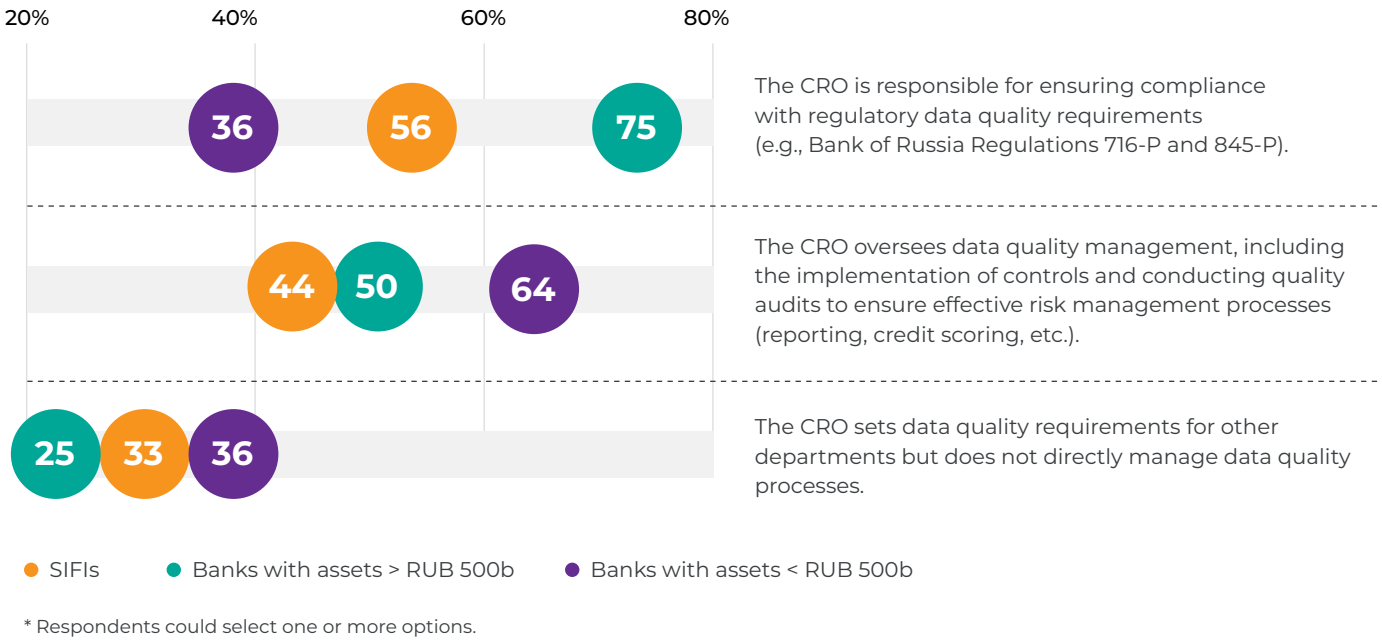
DQM component/ maturity level	Basic (4%)	Developing (21%)	Established (58%)	Advanced (13%)	Leading (4%)
DQM system: roles and responsibilities	Ad hoc; no defined roles or responsibilities	Some tools partially implemented; certain roles described	Some tools implemented; certain roles defined	Centralized management	Centralized management with clearly defined roles and responsibilities
Data management policy/guidelines	Partially developed/ absent	Some elements implemented	Implemented and in use	Implemented and actively used	Detailed standards/ guidelines are well understood by employees
Control mechanisms	Absent/not aligned	Absent/not aligned/ under discussion	Minimal regulator-required metrics	DQM performance metrics	Metrics assessing DQM and process effectiveness
Data quality level	Low	Low; key issues identified	Medium	Measurable improvement in data quality	High, with a focus on analytics and data quality
Automation level	Very low	Low	Medium	High	Very high
Process and data quality predictability	None or poor	Poor	Fair	Good	Excellent
Data quality risk management system	Not implemented	Not implemented	Not implemented	Implemented	Implemented, risk mitigation available

Only 17% of surveyed banks reported advanced or leading maturity in data quality management within their risk frameworks. Lower maturity levels at other banks appear to be influenced by limited resources and legacy systems. Regulatory mandates and ongoing digital transformation, particularly in risk management, are expected to narrow this gap over the next 3–5 years. However, maturity levels vary significantly across banks depending on their size and technological capabilities.

MATURITY LEVELS OF DATA QUALITY MANAGEMENT ACROSS BANKS' RISK FRAMEWORKS

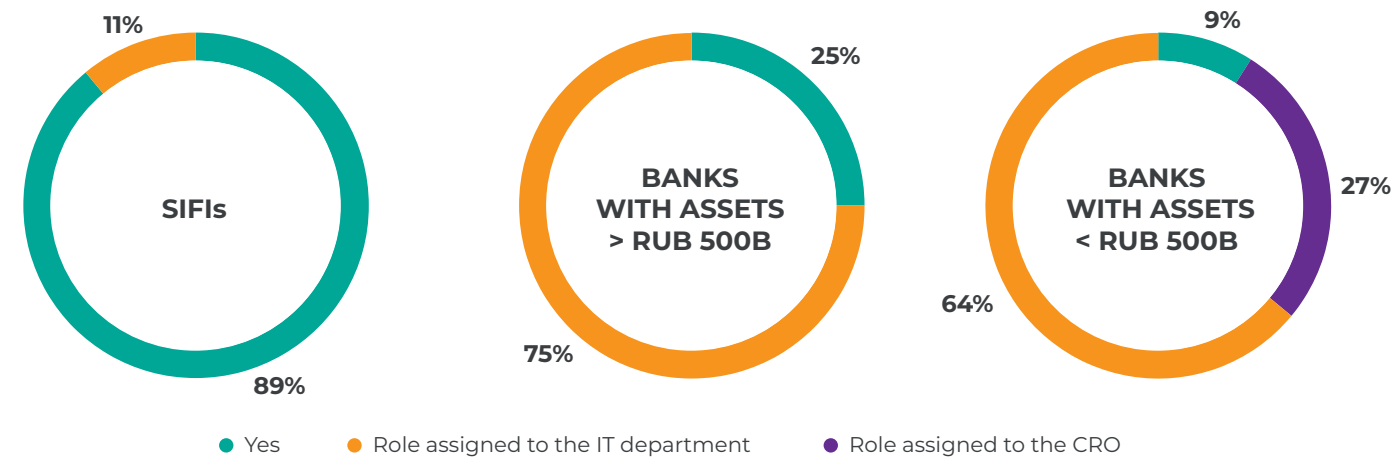


WHAT ROLE DOES YOUR BANK'S CRO PLAY IN DATA QUALITY ASSURANCE?*



* Respondents could select one or more options.

HAS YOUR BANK ESTABLISHED A STANDALONE CDO ROLE?



The role of the CRO in data quality management varies with the scale of the bank. In large institutions, the CRO's expanded involvement in implementing regulatory data quality requirements reflects the adoption of advanced risk assessment methodologies that demand higher data standards. In smaller banks, CROs are often more directly engaged in data quality management, as implementing centralized process tends to be less complex at a smaller scale.

Most surveyed banks do not have a formal CDO role; these responsibilities are typically handled by the IT department. Given the heavy workload of IT teams, accountability for data quality management can become fragmented. A hybrid model may offer an optimal solution, with the CDO overseeing data strategy and the CRO accountable for data use within risk domains.

NEW TECHNOLOGIES: OPPORTUNITIES AND CHALLENGES FOR RISK FUNCTIONS

Successful adoption of new technologies depends on high data quality and a robust technological foundation. After major international software providers pulled out of Russia, banks were compelled to shift to domestic software or develop in-house solutions. Budgeting for import substitution varies depending on the bank's size and readiness for the mandated transition to domestic platforms.

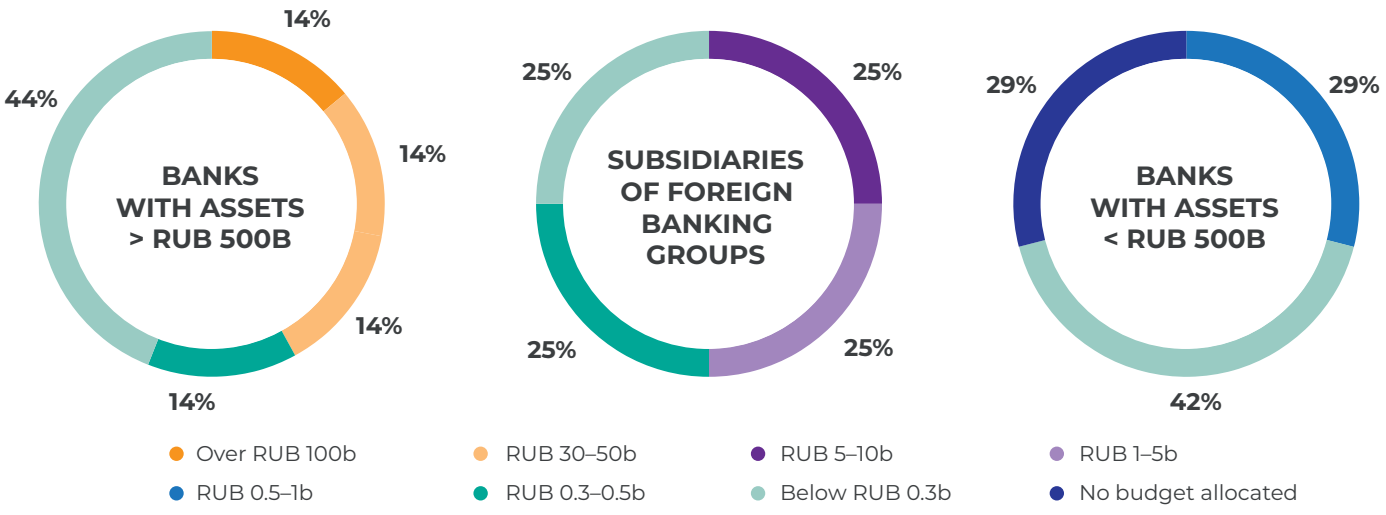
Large banks, which historically relied heavily on foreign software for risk management, face greater pressure to allocate sufficient funding for this transition. Many are planning to migrate to in-house solutions.[21] Meanwhile, smaller banks generally prioritize import substitution less, partly due to their initially lower automation levels or use of less costly domestic software.

Several additional challenges complicate this transition:

- Fully replacing foreign software requires significant investment.
- There are no mature domestic alternatives for key software modules. Banks are focusing on maintaining current IT infrastructure, client solutions, and urgent regulatory priorities, such as adopting IRB models.
- The Bank of Russia permits temporary use of foreign software as long as data is stored within Russia and there is an action plan to migrate to domestic software by 2025–2027.

Russia's National Development Goals target at least 80% import substitution among players in key sectors of the economy by 2030, with up to 95% adoption of domestic solutions planned for state-owned corporations and companies.

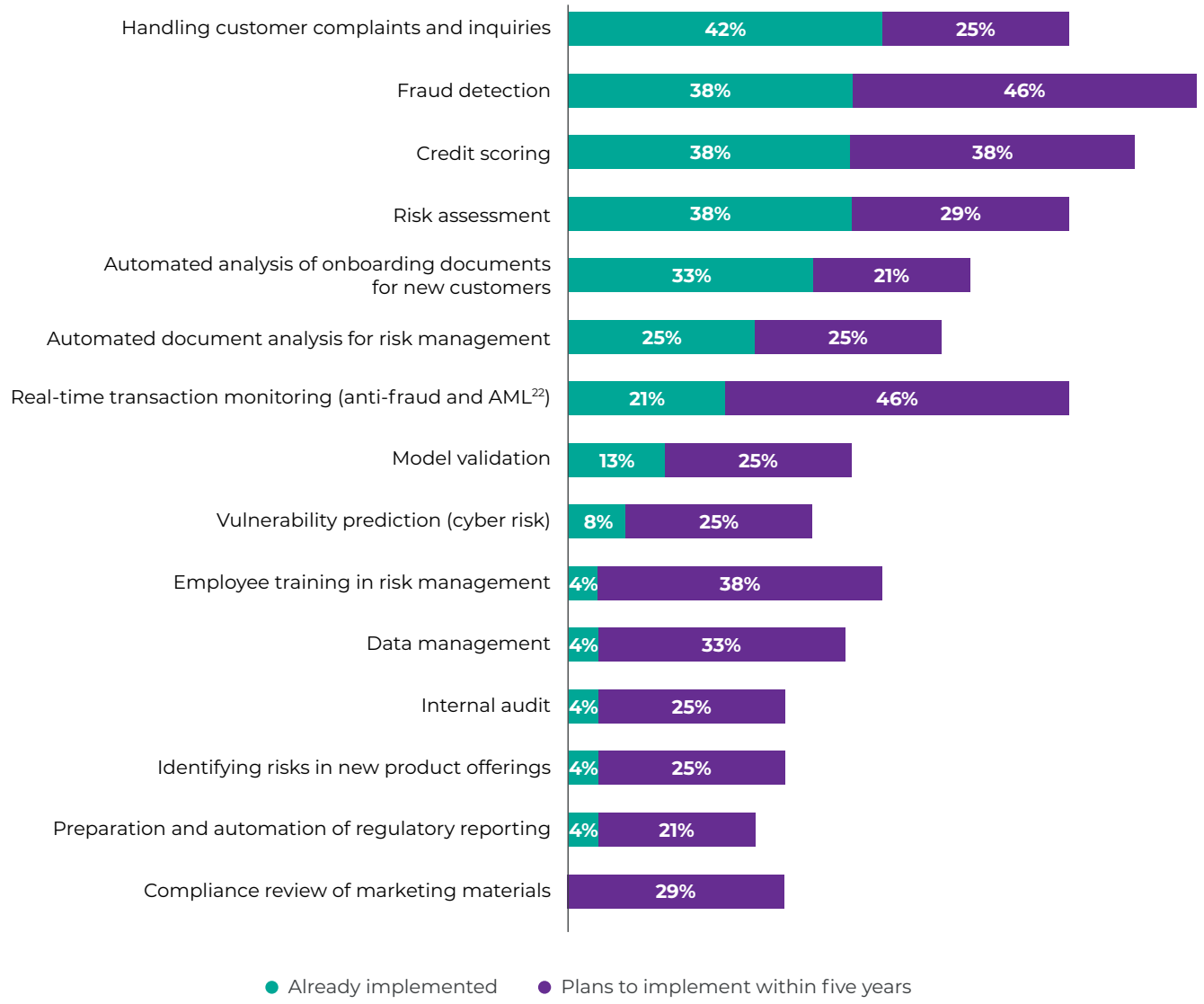
WHAT IS THE PLANNED BUDGET FOR REPLACING IMPORTED RISK MANAGEMENT INFORMATION SYSTEMS?*



* None of the respondents selected the RUB 50–100b or RUB 10–30b option.

[21] Cautious Optimism and a Bet on Long-Term Growth: How the Banking System Will Navigate 2024 (https://b1.ru/analytics/b1-banking-trends-2025-survey/)

PLEASE INDICATE THE PROCESSES WHERE YOUR BANK HAS ALREADY IMPLEMENTED OR PLANS TO IMPLEMENT ARTIFICIAL INTELLIGENCE OVER THE NEXT FIVE YEARS*



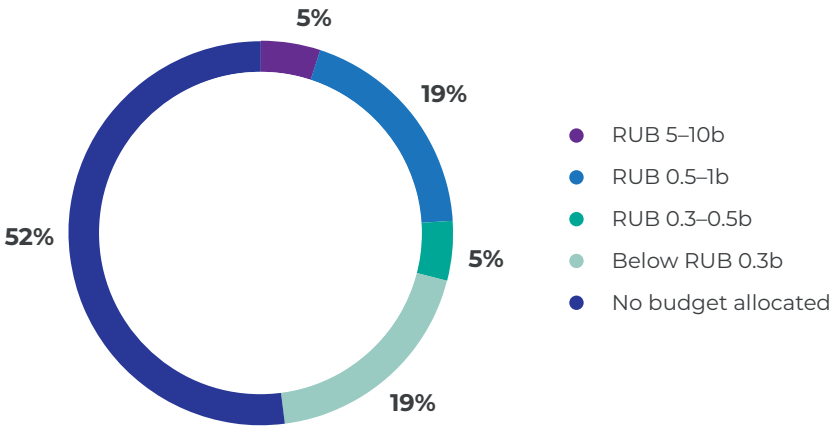
* Respondents could select one or more options.

Artificial intelligence remains a key innovation in the banking sector. The technology is already widely used to automate document analysis, risk assessment, transaction monitoring, credit scoring, model validation, customer inquiry handling, and fraud prevention.

While AI helps optimize processes, its uncontrolled deployment—or implementation by employees lacking adequate expertise—can lead to systemic errors in lending, discriminatory scoring practices, data breaches, and other serious implications violating ethical principles of AI use. Instances have already emerged where excessive automation has compromised service quality and eroded customer trust in financial institutions.

22 AML (Anti-Money Laundering) refers to a set of measures aimed at preventing money laundering and the financing of terrorism.

HOW MUCH ARE BANKS BUDGETING FOR THE IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE IN RISK MANAGEMENT?*



* None of the respondents selected the RUB 0.5-5b option.

The limited growth in AI investment can be attributed to several factors:

- **Regulatory uncertainty.** Clear standards for AI solutions in risk management have yet to be established, while potential regulatory restrictions remain a concern.
- **Market saturation.** The abundance of AI solutions makes banks more cautious, as they seek to ensure sufficient security and quality before adoption.

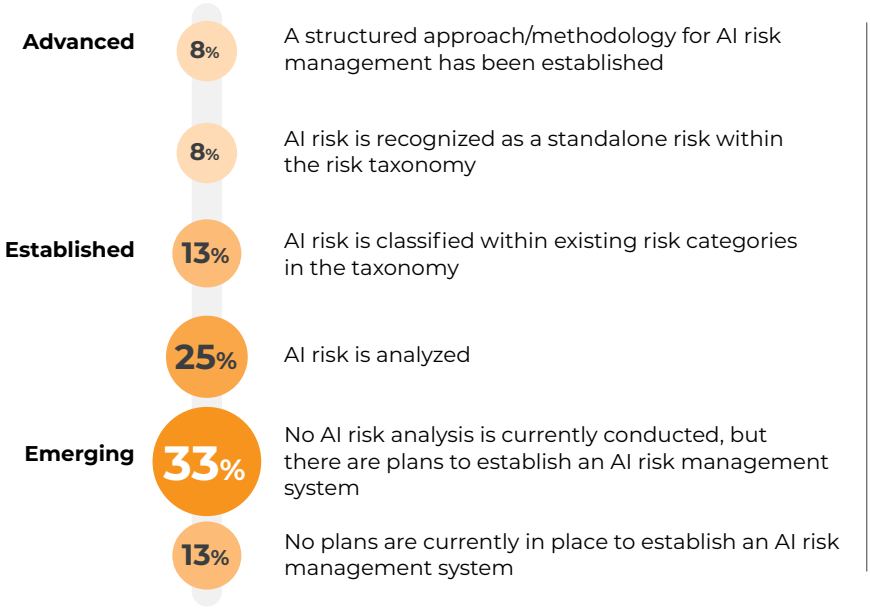
Some banks do not set aside a dedicated budget for AI initiatives; instead, funding decisions are made on a case-by-case basis as part of ongoing operations.

Allocating budget for AI in risk management systems often takes a back seat, as leadership tends to focus more on core business challenges and back-office optimization.

In particular, AI adoption is proving particularly effective in reducing the cost of routine operations. Chatbots and voice assistants now handle standard customer inquiries, enabling employees to concentrate on more complex and high-value tasks. This trend is reflected in analytical forecasts: global banks could cut up to 200,000 jobs in the coming years as automation advances.[23] Meanwhile, as digital solutions mature, customers increasingly value personalized service, emotional intelligence, and creative problem-solving—which could make human-to-human customer interaction a premium offering.

[23] Wall Street Job Losses May Top 200,000 as AI Replaces Roles (Bloomberg: https://www.bloomberg.com/news/articles/2025-01-09/wall-street-expected-to-shed-200-000-jobs-as-ai-erodes-roles)

HAS YOUR BANK SET UP A SYSTEM FOR MANAGING ARTIFICIAL INTELLIGENCE RISK?



Widespread AI adoption, especially in business, is giving rise to new risks that banks are not yet prepared to handle. Currently, **most AI risk management systems in banking remain in early stages of development.**

To address this, the Bank of Russia plans to **closely monitor and analyze AI risk management practices** across financial institutions—a move expected to significantly impact banks' budget priorities in the medium term.[24]

New AI regulations[25] will act as both a **strong driver** for developing risk management systems and a **major challenge** for banks:

1 For systems classified as high-risk or restricted-risk, banks will need to implement enhanced control measures and tools.

2 Banks will also need to develop dedicated components within their risk management systems, such as AI application methodologies, risk assessment approaches, and AI risk management frameworks.

3 While the Bank of Russia intends to take a light-touch regulatory approach, transparency and clarity of AI systems remain top priorities. For example, the regulator plans to establish dedicated registries to ensure transparency of, and supervision over, AI use across the financial sector, meaning banks will have to put in extra effort when rolling out AI solutions.

With experimental regulatory regimes[26] and new legislation on the horizon, maintaining an open dialogue with the regulator will be essential for banks to succeed in their AI ambitions while ensuring reliability and security.

[24] Monetary Policy Guidelines for 2025–2027 (Bank of Russia, https://cbr.ru/Content/Document/File/165597/on_eng_2025(2026-2027).pdf)

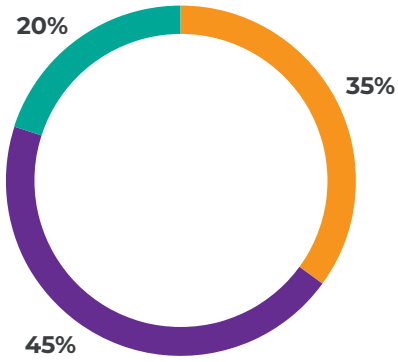
[25] The Authors of the Draft AI Law Have Clarified Its Essence (RBC, https://www.rbc.ru/technology_and_media/15/04/2025/67fe02d89a79472cf8ca1af4)

[26] Digitalization of Payments and Innovation in the Payment Market, 2024: Analytical Report (Bank of Russia, https://www.cbr.ru/Content/Document/File/161600/analytical_report_20240605.pdf)

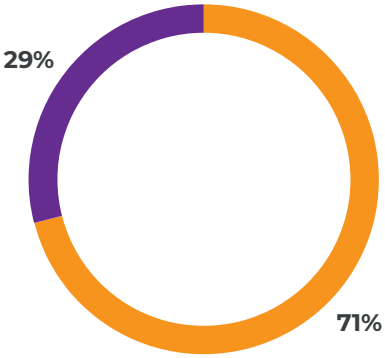
RISK CULTURE AND TALENT: THE CORNERSTONES OF RESILIENCE

HOW WOULD YOU RATE THE LEVEL OF RISK CULTURE IN YOUR BANK ACROSS THE THREE LINES OF DEFENSE?

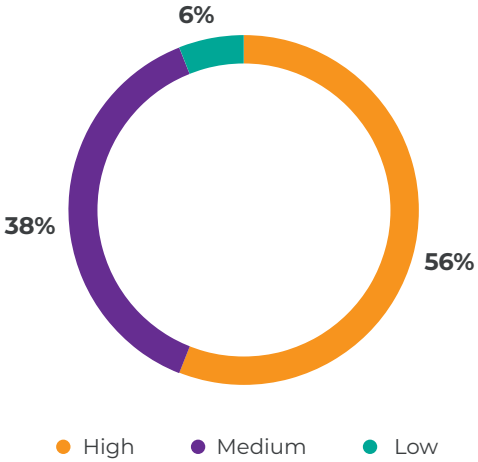
1ST LINE OF DEFENSE (BUSINESS UNITS) – **A PRIORITY AREA FOR DEVELOPMENT**



2ND LINE OF DEFENSE (RISK MANAGEMENT FUNCTION) – **AMBASSADOR FOR ADVANCEMENT**



3RD LINE OF DEFENSE (INTERNAL AUDIT FUNCTION) – **ENHANCING IN-HOUSE COMPETENCIES**



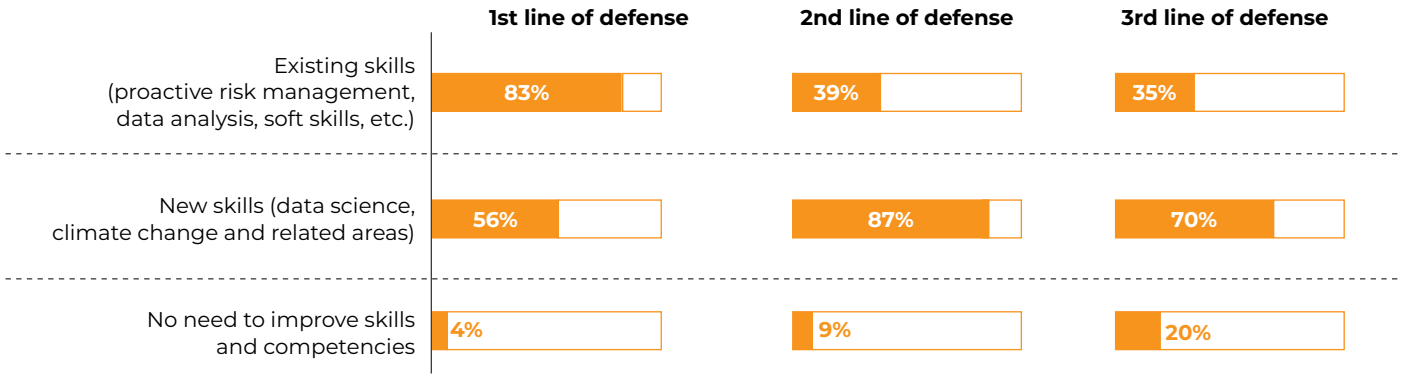
According to CROs, the **current level of risk awareness** and the knowledge and skills of staff in the first and second lines of defense remain **insufficient to fully unlock the benefits of transforming risk management approaches.**

Building a strong risk culture is becoming increasingly critical as traditional risks regain prominence and emerging threats come to the fore. The new challenges are driven by the adoption of advanced technologies, sophisticated data management practices, a rapidly changing environment, and shifting regulatory requirements.

Together, these factors place added pressure on banks to detect new risks early and respond swiftly to change.

To manage risks effectively, minimize significant losses, streamline business processes and enhance resilience and agility, banks need employees who are not only actively engaged in risk management but also equipped with a broad range of competencies. This is especially urgent at a time when emerging trends and technologies bring fresh challenges and risks.

WHICH LINES OF DEFENSE REQUIRE STRONGER EMPLOYEE COMPETENCIES AND SKILLS FOR MORE EFFECTIVE RISK MANAGEMENT?*



* Respondents could select one or more options.

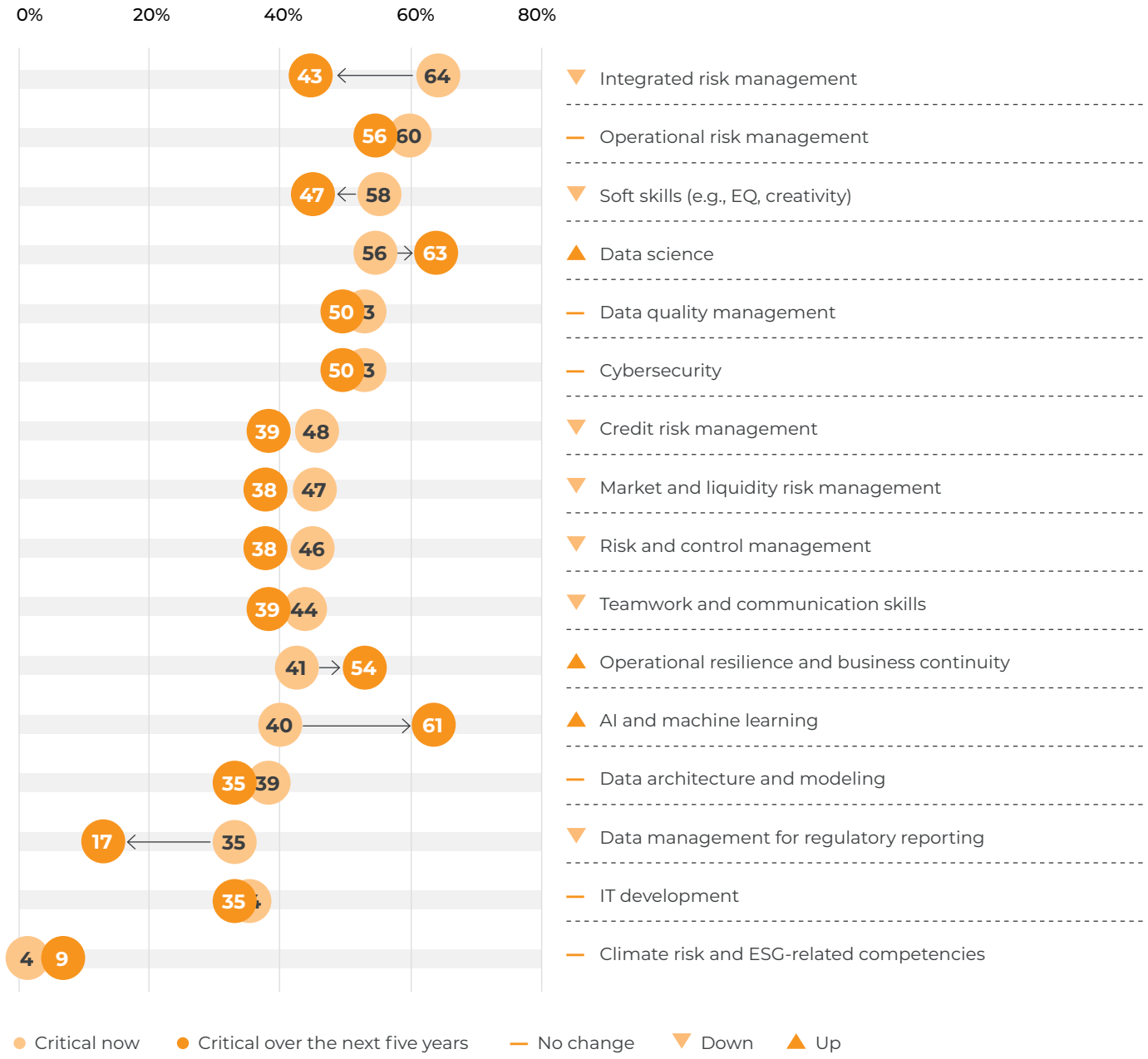
It is important to highlight that CROs currently stress the **critical need to both enhance existing competencies and acquire new skills** across all lines of defense.

This skills gap is especially acute among business unit staff who have to combine commercial responsibilities with frontline risk identification and management, often without the specialized expertise needed for the task. More than 80% of respondents emphasize the need to build fundamental risk management competencies within the first line of defense, while over half also point to the importance of expanding existing skills with new capabilities.

Rapid adoption of technologies in banking, coupled with the emergence of new risk types, requires second-line risk managers to deepen their knowledge in advanced areas. Key skill sets now include data management, a solid understanding of artificial intelligence processes and emerging risks such as ESG, and a comprehensive grasp of current regulatory requirements. A lack of expertise in these areas hinders the development of up-to-date methodologies and effective control frameworks needed to respond to today's challenges.

In the third line of defense, limited skill levels often lead internal audits to become overly checklist-driven and make it difficult for them to develop a comprehensive view of existing vulnerabilities. Moreover, evolving regulatory demands—particularly those related to the IRB approach—call for internal audit teams to possess advanced capabilities in model validation and IT systems analysis, including the ability to detect flaws in models and codes, and to assess data completeness and quality.

WHICH AREAS OF EXPERTISE DO YOU CONSIDER CRITICAL FOR RISK MANAGEMENT PROFESSIONALS?*



* Respondents selected and ranked up to 10 knowledge and skill areas by criticality, with 1 indicating the most critical. Final scores were calculated using a weighted ranking method based on these assigned ranks.

The strongest demand currently is for professionals with expertise in traditional risk management, soft skills, data management, and information security. Meanwhile, emerging trends are fueling a rising need for competencies in data science, artificial intelligence, and business continuity and resilience.

Banks see data management skills for reporting becoming less critical as standardization increases.

Yet, the talent shortage remains a major roadblock to stronger risk management. As finding qualified professionals with sufficient knowledge proves difficult, banks should double down on comprehensive training and upskilling initiatives across all three lines of defense. These efforts are designed to close the skills gap and build competencies tailored to the unique needs of financial institutions. Still, high staff turnover continues to slow sustained progress in this area.

METHODOLOGY

1. THE ASSET BASE OF PARTICIPATING BANKS WAS ASSESSED USING DATA FROM BANKI.RU AND ANALYTICAL MATERIALS PUBLISHED BY THE BANK OF RUSSIA, AS OF 30 APRIL 2025.

2. ALL SURVEY PARTICIPANTS WERE ASSURED COMPLETE CONFIDENTIALITY. THE STUDY IS BASED ON DATA THAT HAS BEEN ANONYMIZED, CONSOLIDATED, AND PROCESSED FOR ANALYSIS.

3. FOR MULTIPLE-CHOICE QUESTIONS, EACH RESPONDENT WAS COUNTED TOWARDS THE PERCENTAGE FOR EVERY OPTION THEY SELECTED.

CONCLUSION

The trends highlighted in our study reveal an **increasing complexity in the responsibilities of Chief Risk Officers** (CROs). Global events, macroeconomic shifts, tighter regulation and oversight, evolving consumer behavior, ongoing technological innovation, and emerging threats are all reshaping the CRO agenda, influencing both immediate priorities and long-term strategies.

CROs must navigate the intricate interplay between diverse risk types and associated business areas. The ability to respond swiftly to unexpected threats and crises—alongside forecasting, prevention and proactive risk management—is making the CRO role more strategic than ever.

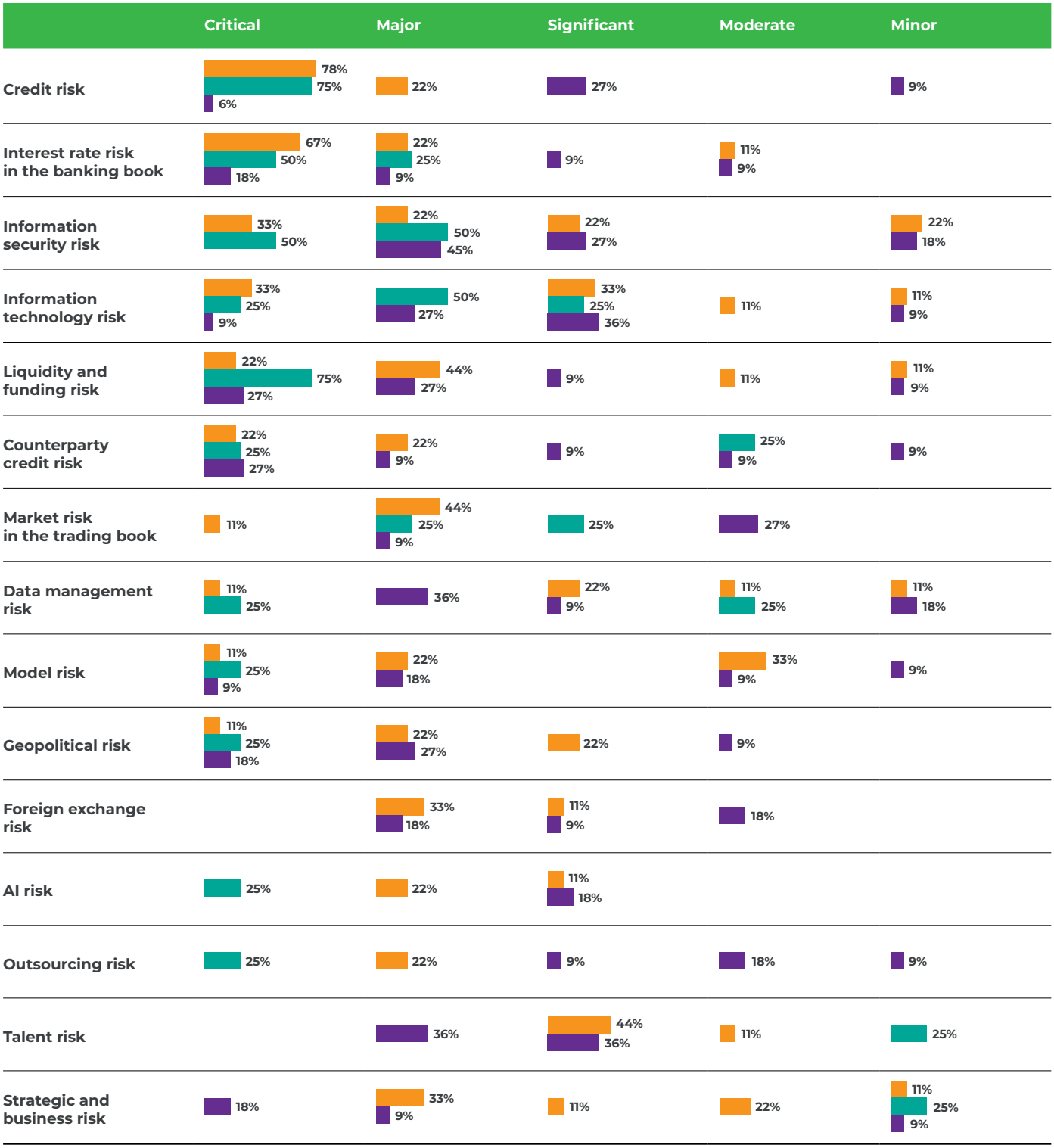
Effective risk management going forward will require **agility, adaptability and resilience amid economic volatility.** A highly mature data management and quality system, a robust risk culture across all lines of defense, and the continuous development of both new and existing skills—from soft skills to technical capabilities related to emerging technologies, trends, and risk management—will remain key enablers of success.

By advancing in these areas, **CROs will be better equipped to handle a broad range of tasks more effectively, streamline operations and** ultimately **deliver greater value to their organizations.**

Achieving this transformation **requires banks to make balanced investments** in technology, people and methodology—tailored to their unique context and scale.

ANNEX. TOP RISKS FOR THE YEAR AHEAD

WHICH RISKS ARE EXPECTED TO BE THE MOST SIGNIFICANT OVER THE COMING YEAR IN TERMS OF THEIR POTENTIAL IMPACT?*



● SIFIs ● Banks with assets > RUB 500b ● Banks with assets < RUB 500b

* Respondents were asked to select up to 10 key risks and rank them by significance. The same level of significance could be assigned to multiple risks. Responses were grouped based on the following ranking: 1–2 – critical risks, 3–4 – major risks, 5–6 – significant risks, 7–8 – moderate risks, 9–10 – minor risks.

CONTACTS

GENNADIY SHININ

Partner,
Financial Services Leader
gennadiy.a.shinin@b1.ru

MICHAIL TSIBULEVSKY

Partner,
Head of Financial Services Consulting
michail.tsibulevsky@b1.ru

ANNA BAGAEVA

Senior Manager,
Financial Services Consulting
anna.bagaeva@b1.ru

NELLI RAMAZYAN

Senior Manager,
Financial Services Consulting
nelli.ramazyan@b1.ru

TAMARA CHERNYSHOVA

Manager,
Financial Services Consulting
tamara.chernyshova@b1.ru

ABOUT B1 GROUP

B1 Group offers a comprehensive suite of professional services, including assurance, strategy, technology, consulting, transactions, valuation, tax, law and business support.

With over 35 years in Russia and 25 years in Belarus, we have built a strong team of professionals with diverse expertise and a wealth of experience in delivering the most challenging projects. B1 Group operates across 12 cities: Moscow, Minsk, Vladivostok, Ekaterinburg, Kazan, Krasnodar, Novosibirsk, Rostov-on-Don, Samara, St. Petersburg, Togliatti and Chelyabinsk.

Our mission is to help clients uncover innovative solutions, drive growth, transform their business and achieve success—all while boosting their financial resilience and nurturing talent.

B1.RU | B1.BY

Toll-free number for calls within Russia:
8 800 500 9700

Moscow office phone:
+7 495 755 9700