Building resilience in a changing world

As the operating environment grows more complex, resilience becomes defined by strong judgement and governance. At Axis Bank, we see risk management as a strategic lever for sustainable growth, enabling us to anticipate emerging risks, respond with agility, and advance with confidence and responsibility.

In an environment characterised by regulatory change, rapid digital transformation, evolving customer behaviours and climate change, our approach to risk management remains proactive, disciplined, and thoroughly integrated into decision-making processes.

Risk Management Framework

Our approach to risk management extends beyond merely safeguarding assets; it aims to reinforce confidence in each decision. Founded on clearly articulated governance structures, comprehensive policies, disciplined oversight, and collective accountability, our Risk Management Framework empowers the Bank to anticipate uncertainties, respond proactively, and pursue opportunities with responsibility.

The framework facilitates the proactive identification, evaluation, monitoring, and mitigation of risks across the organisation. Supported by an independent Risk function and strict Board oversight, this framework enhances resilience across the Bank's business units, operational processes, and digital ecosystem.

Risk Governance Structure

The Board of Directors maintains overarching responsibility for risk oversight. This obligation is exercised directly through the Board's Risk Management Committee (RMC), which serves as the primary authority for risk governance at the Board level. The RMC is supported by an independent Risk function led by the Chief Risk Officer (CRO), ensuring risk considerations remain integrated into strategic and operational decision-making.

At the executive level, specialised committees provide targeted oversight across critical risk domains. These include the Credit Risk Management Committee, Operational Risk Management Committee, Asset and Liability Management Committee, Information Systems Security Committee, Central Outsourcing Committee, Business Continuity Planning Management Committee, APEX Committee, Subsidiary Governance Committee, and Enterprise & Group Risk Management Committee. Collectively, these committees promote enterprise-wide vigilance, prompt escalation, and disciplined implementation of authorised policies and frameworks.

Board of Directors Ultimate Oversight

Risk Management Committee Primary Risk Governance

Chief Risk Officer (CRO) and Independent Risk Function Strategic & Operational Integration

Executive Level Committees

Credit Risk Management Committee (CRMC)	Information Systems Security Committee (ISSC)	Apex Committee
Operational Risk Management Committee (ORMC)	Central Outsourcing Committee (COC)	Subsidiary Governance Committee (SGC)
Asset & Liability Management Committee (ALCO)	Business Continuity Planning Management Committee (BCPMC)	Enterprise & Group Risk Management Committee (EGRMC)

Enterprise-Wide Risk Visibility | Timeline Escalation | Disciplined Execution

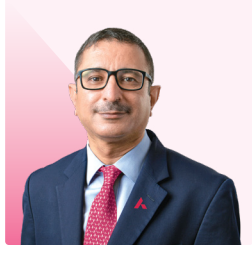
Risk Management Committee members

G. Padmanabhan
Chairperson,
Independent Director

Amitabh Chaudhry
Managing Director
& CEO

Girish Paranjpe
Member,
Independent Director

Pranam Wahi
Member,
Independent Director



Munish Sharda
Member,
Executive Director

Key achievements of RMC in fiscal 2026

- Enhanced governance around risk appetite
- Stress testing framework
- Strengthened cybersecurity
- Enhanced monitoring for unsecured lending, including models
- Regulatory reporting enhancement
- Risk & compliance culture

Key focus areas for fiscal 2027

- Process simplification
- Ensuring cybersecurity
- More focus on unsecured lending, Bharat & Digital
- AI-led processes and technology
- Risk & compliance culture

Proactive management of these issues will contribute to credit-led growth in the retail space while maintaining a necessary focus on cybersecurity, technological resilience, and the embedding of sustainability through a robust risk culture.

Foundational pillars of Risk Management

Risk philosophy

At Axis Bank, risk management is regarded as a collective responsibility. We acknowledge that trust is priceless; consequently, adherence to compliance standards, integrity, and safeguarding stakeholder interests are imperative. This understanding cultivates a culture where prudent behaviour and responsible development coexist harmoniously.

Risk appetite and policies

A clearly defined risk appetite, approved by the RMC and the Board, supports informed decision-making across the organisation. Board-approved policies transparently define our risk-taking boundaries, while executive committees and the Risk Management Department ensure disciplined implementation.

Risk identification and mitigation

The Risk Management Department monitors emerging risks vigilantly and reports them through established mechanisms such as ICAAP and risk dashboards. In close coordination with business units, it facilitates prompt mitigation measures and promotes greater ownership of risk in daily operations.

Risk culture

A robust risk culture is reinforced at all levels of the Bank. The Board and senior management lead by example, while the Compliance function and Risk Management Department help embed accountability, transparency, and openness across the enterprise.

Managing material risks with discipline and depth

Our Risk Management Framework is designed to address material risks proactively through clear accountability, defined methodologies, and regular review. Across financial and non-financial risks alike, our objective is to protect balance sheet strength, preserve stakeholder confidence, and support responsible growth in a changing operating environment.

Credit Risk

Credit risk is the potential financial loss arising when a counterparty, such as a customer, borrower, or security issuer, fails to fulfil contractual obligations. Our credit risk management aims to maintain asset quality and control concentration risk across both individual exposures and the overall portfolio.

Capitals impacted

Risk status

UN SDGs impacted

Mitigation measures

Wholesale Banking: Internal ratings form the core of our risk management, guiding risk acceptance, setting exposure limits, supporting sanction approvals, informing pricing, and determining review cycles.

Retail portfolio: Product-specific scorecards are employed for retail clients, including small businesses and small agricultural borrowers. An independent validation team rigorously assesses these credit models to ensure strong discriminatory power, accurate calibration, and sustained performance over time.

Market Risk

Market risk stems from potential losses in both on- and off-balance sheet positions due to movement and volatility in market prices, which can affect the Bank's earnings and capital. Key drivers include changes in interest rates, equity prices, and foreign exchange rates. This risk primarily stems from our trading and investment activities, conducted for both client facilitation and proprietary purposes.

Capitals impacted

Risk status

UN SDGs impacted

Mitigation measures

Comprehensive framework: The Bank's market risk management framework is guided by well-defined policies and processes for identifying, measuring, monitoring, and reporting exposures within its risk appetite.

Independent oversight: RMD monitors portfolios independently, ensuring adherence to risk limits and timely reporting of deviations.

Measures: The Bank uses statistical tools like VaR, stress tests, back tests, and scenario analyses, along with non-statistical measures like position limits, mark-to-market (MTM) evaluations, and stop-loss limits to manage risk.

VaR methodology: VaR is calculated through historical simulation at 99% confidence over a one-day horizon, based on 250 days of data, and supplemented with regular backtesting and stress tests.

Increase in Risk No change

Liquidity Risk

Liquidity refers to a bank's ability to finance asset growth and fulfil expected and unexpected cash and collateral obligations at a reasonable cost. Liquidity risk arises when the bank cannot meet these obligations without compromising its financial condition.

Capitals impacted

Risk status

UN SDGs impacted

Mitigation measures

Comprehensive framework: The Bank's Asset Liability Management (ALM) Policy details a comprehensive liquidity risk management system, supported by supplementary policies on intraday liquidity, stress testing, contingency funding, and branch-level liquidity.

Monitoring & oversight: Liquidity profiles are assessed through static and dynamic gap analyses, key ratios, and stress testing, with continuous supervision by the ALCO and the RMC.

Regulatory adherence: The Bank complies with RBI guidelines and Basel III requirements, such as the Liquidity Coverage Ratio (LCR) and Net Stable Funding Ratio (NSFR), ensuring metrics remain within regulatory norms and the Bank's risk appetite.

Operational Risk

Operational risks can arise from inadequate or missing controls within internal processes, personnel management, and systems, as well as from external events or a combination of these factors.

Capitals impacted

Risk status

UN SDGs impacted

Mitigation measures

Comprehensive ORM Policy and governance: A structured Operational Risk Management (ORM) Policy guides proactive risk identification, assessment, mitigation, and risk monitoring, reinforced by a clear governance framework.

Evaluation and Committee oversight: All new products, processes, and changes undergo rigorous risk assessment by the Operational Risk team, with support from Product/Change Management Committees and the Outsourcing Committee. The Information System Security Committee oversees risks related to information systems.

Measurement system and continuous enhancement: A dedicated Operational Risk Measurement System documents, assesses, and periodically reviews risks and controls across all business lines.

 Increase in Risk  No change

Information and Cyber Security Risks

Information and cybersecurity risks for banks arise from the possibility of unauthorised access, manipulation, or theft of sensitive data and assets. Cybersecurity breaches, whether through hacking, phishing, or malware, can disrupt services, compromise customer information, and erode trust in the Bank's operations. Strong security measures, such as encryption, multi-factor authentication, and regular audits, protect the institution and its customers from evolving cyber threats.

Capitals impacted

Risk status

UN SDGs impacted

Mitigation measures

Robust framework and governance:
The Bank has established a comprehensive information and cyber security framework to address risks arising from unauthorised access, misuse, manipulation, or loss of sensitive data and digital assets. Oversight is maintained by the Information System Security Committee in accordance with defined policies, standards, and oversight mechanisms aligned to recognised regulatory and industry frameworks, including NIST, ISO/IEC 27001, ISO/IEC 27017 (cloud security controls), ISO/IEC 27018 (protection of personally identifiable information in cloud environments), ISO/IEC 27034 (application security), ISO/IEC 42001 (AI management systems), and PCI DSS. These frameworks ensure alignment with evolving threat scenarios, emerging technologies, and regulatory expectations.

Proactive security measures:
The Bank has implemented a combination of technical and administrative controls to mitigate cybersecurity risks and protect the confidentiality, integrity, and availability of systems and data. These include strong access controls, encryption, secure configuration standards, and identity and authentication mechanisms. Prior to deployment of IT infrastructure or applications, security reviews, vulnerability assessments, and penetration testing are conducted to identify and address weaknesses.

Defence-in-Depth and 24x7 Monitoring:
A layered defence-in-depth approach is adopted, supported by continuous monitoring through 24x7 Security Operations Centres (SOC). This enables timely detection and response to cyber threats and suspicious activities, thereby reducing the likelihood and impact of service disruption, data compromise, and cybersecurity incidents. The Bank also engages with regulators and industry bodies to strengthen cyber resilience and implement recommended security measures.

Increase in Risk No change

Climate Risk

Climate risks broadly fall into two categories:

Physical Risks: This category includes both chronic and acute impacts of climate change. Chronic risks involve long-term changes in temperature, precipitation patterns, agricultural productivity, and sea levels, whereas acute risks encompass more immediate events, such as heat waves, floods, cyclones, and wildfires.

Transition Risks: These arise from shifts in policy, regulation, technology, or consumer preferences as the world moves toward a low-carbon future.

Capitals impacted

Risk status

UN SDGs impacted

Mitigation Measures

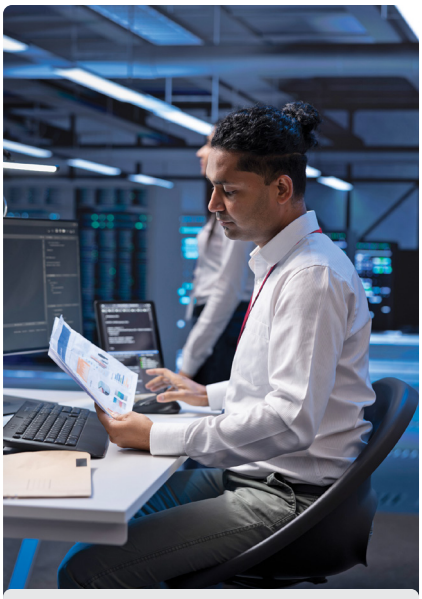
Global framework alignment and climate risk integration: The Bank publishes TCFD-aligned disclosures in line with RBI guidelines, recognising climate risk as a factor that impacts credit, operational, market, reputational, and liquidity risks. Through scenario analyses and stress testing, we monitor physical and transition risks, with the oversight of the ESG Committee.

Robust governance and strategic oversight: Since 2021, the ESG Committee has guided the Bank's approach to climate and ESG risks, focusing on high-transition-risk sectors and natural hazards to strengthen risk management and resilience across retail, rural, and SME portfolios.

Building capabilities and fostering a climate-conscious culture: Our Climate Risk Dashboards and ESG e-modules, along with specialised training, promote climate awareness. Partnership with industry bodies and regulators helps safeguard operations and advance the Bank's broader sustainability goals.

Increase in Risk No change

Other components of Risk Management



Internal Audit

The Bank's Internal Audit function independently assesses internal controls, governance mechanisms, and risk management practices and reports to the Board on compliance with internal and regulatory guidelines. Guided by the RBI's Risk-Based Internal Audit standards, the function maintains a strategic focus on emerging risks while enhancing its effectiveness through technology-enabled audits and continuous capability development.

Business Continuity Management

Business Continuity is managed by the Business Continuity Planning Management Committee, which guarantees effective implementation and testing of essential internal operations. Regular exercises and scenario-based reviews help prepare the Bank for disruptions and ensure continuous service and operational resilience.

Fraud Detection and Mitigation

Guided by a comprehensive Fraud Risk Management Policy, the Bank maintains robust processes and systems to prevent, detect, investigate, and respond to fraud risks. Real-time transaction monitoring, enterprise-wide AML systems, prompt alert generation, and dedicated fraud management platforms enhance cross-channel surveillance and enable timely intervention.