Governance

At Axis Bank, governance combines oversight, accountability, and ethical conduct to strengthen trust and support the long-term sustainability of our franchise.

Institutional excellence through a disciplined approach

Enduring value is created when leadership is anchored in transparency, rigorous oversight, and responsibility. Our governance framework helps ensure that every decision reflects integrity and fairness and upholds long-term stakeholder interests. Beyond mere compliance, this model reinforces our corporate culture, clarifies accountability, and strengthens institutional resilience.

Material Issues Linkage

M1 M2 M3

Capital Linkage

UN SDGs Linkage

At Axis Bank, our governance framework serves as a strategic compass, guiding decision-making, risk oversight and ethical conduct within a dynamic banking landscape. Built upon principles of transparency and fairness, this model ensures prudent expansion while upholding the highest standards of integrity and stakeholder confidence.

Our model includes an experienced and diverse Board, specialised Committees of the Board, disciplined leadership, robust control functions and clear lines of accountability, all of which safeguard stakeholder interests and promote sustainable growth and value creation.

Governance at a glance

13
Directors on the Board

8
Independent Directors

61.54%
Board independence

3
Women Directors

23%
Women's representation on the Board

>99%
Average attendance at Board meetings

10 of 11
Committees chaired by Independent Directors*

*Excluding the Committee of Whole-Time Directors and the Review Committee, which cannot be chaired by an Independent Director.

Why this matters

Governance is central to how we preserve trust, maintain regulatory rigour, strengthen oversight, and create enduring value for customers, shareholders & investors employees, regulators, and communities.

A governance framework designed for clarity, oversight and disciplined execution

Our governance framework is anchored in transparency, accountability and ethical conduct, reflecting our value system across every layer of our culture, policies and stakeholder relationships. With a commitment to responsible leadership and openness to scrutiny, it clearly defines roles, responsibilities and reporting structures across the Board, Board Committees, executive leadership, management and operating functions.

The Bank's governance structure is multi-tiered, enabling a strong balance between strategic guidance, independent oversight, disciplined execution and operational accountability. This ensures that decisions are aligned with the Bank's purpose, risk appetite and long-term strategic priorities, while responsibility remains clearly assigned at every level.

Multi-tiered governance architecture

Beyond compliance

The Bank believes in going beyond the law to uphold best-in-class corporate governance practices, supported by strong Board processes, internal control systems and a rigorous audit mechanism.

Governance supports value creation

Clear Accountability | Strong Oversight | Ethical Conduct | Effective Risk Governance | Better Institutional Resilience

A Board shaped by independence, diversity and depth of expertise

The Board is constituted in accordance with the relevant provisions of the Companies Act, 2013; the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015; the Banking Regulation Act, 1949; the RBI guidelines; the Articles of Association of the Bank; and other applicable laws and amendments as notified by the regulators from time to time. Its composition ensures a combination of executive insight, independent judgement, sectoral knowledge and long-range strategic perspective.

As of March 31, 2026, the Board comprised 13 Directors, including the Managing Director & CEO, three Executive Directors, eight Independent Directors and one Nominee Director from the Life Insurance Corporation of India, the Bank's promoter. The Board continues to be led by an Independent Director and Part-time Chairman, reinforcing the strength of balanced oversight and independent governance.

Board profile

- 62 years – average age of the Board
- 10 Directors with more than 35 years of experience
- 7.5 hours of training attended by Directors

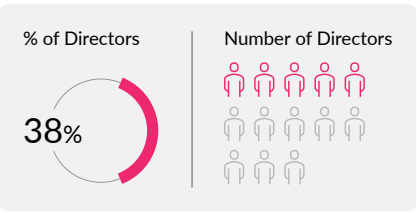
Board tenure

- 9 Directors with tenure of less than 4 years
- 2 Directors with tenure of 4–6 years
- 2 Directors with tenure of more than 6 years

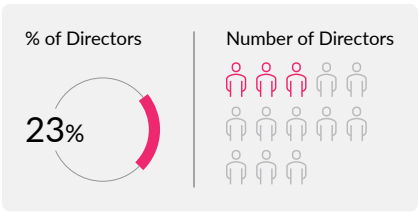
Diverse Board skills

We believe that a diverse and engaged Board is essential to long-term success. Our Board brings together distinguished professionals with experience across diverse fields, including finance, banking, risk management, information technology, business management, human resources, law, agriculture, & rural economy, small-scale industry and others. This breadth enables more informed oversight of both current priorities and future transitions.

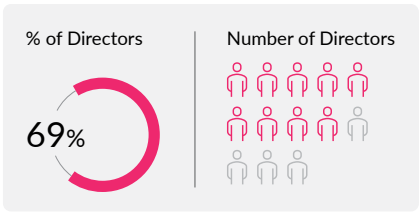
Accountancy



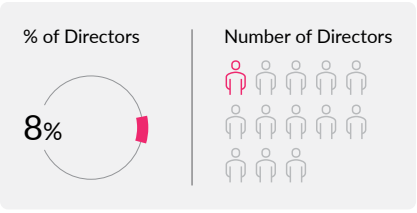
Agriculture & Rural Economy



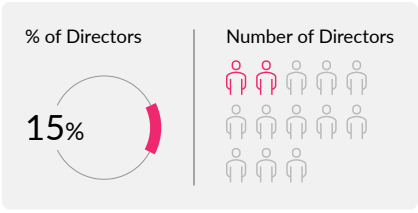
Banking



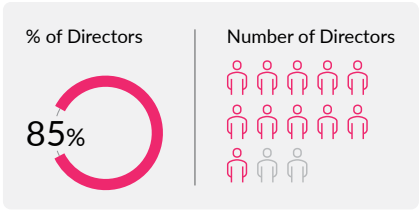
Co-operation



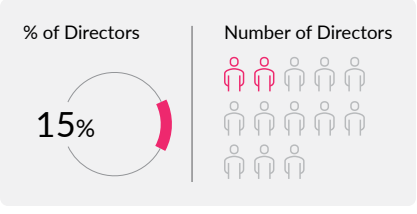
Economics



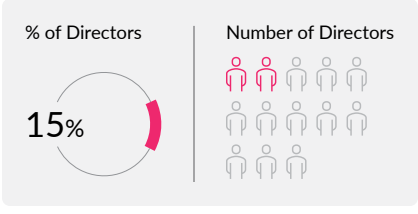
Finance



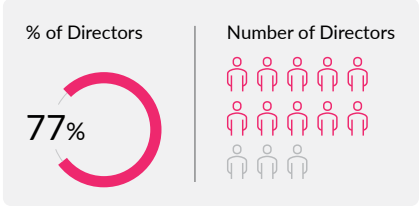
Law



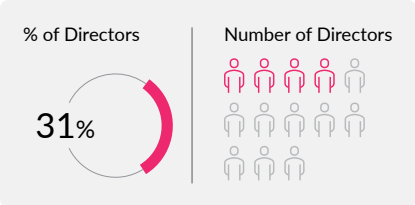
Small-Scale Industry



Information Technology



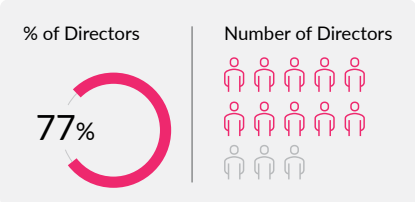
Payments & Settlement System



Human Resources

Risk Management

Business Management



Committee oversight that deepens rigour across the Bank's material priorities

To enable focused deliberation and more effective oversight, the Board has constituted several Board-level Committees. These ensure a detailed review of matters critical to the Bank's resilience, service quality, digital readiness, stakeholder trust and responsible growth. Committee Chairpersons regularly brief the Board on key discussions and outcomes, ensuring continuity of oversight and informed governance at the highest level.

Stewardship, Assurance and Control

Audit Committee

Reviews audit findings, internal controls, compliance matters, functioning of the whistleblower and vigilance mechanism, related party transactions and financial reporting integrity. It also oversees the appointment of auditors, the Group Chief Compliance Officer, and the Group Chief Audit Executive.

Capitals impacted

Stakeholders impacted: I, Re

Special Committee of the Board of Directors for Monitoring and Follow-up of cases of Frauds

Monitors fraud cases, staff accountability, and the functioning of the Fraud Review Council, ensuring systemic corrections and timely reporting to regulators.

Capitals impacted

Stakeholders impacted: C, I, Re

Risk Management Committee

Oversees the Bank's risk strategy, risk appetite, risk management policies, monitors limits across risk categories and reviews the appointment of the Chief Risk Officer.

Capitals impacted

Stakeholders impacted: I, Re

Review Committee

Considers proposals relating to the classification of borrowers as wilful defaulters.

Capitals impacted

Stakeholders impacted: C, I

Strategy, technology and future-readiness

IT and Digital Strategy Committee

Oversees IT strategy, cybersecurity incidents, technology alignment with business objectives, IT operations and digital transformation journey.

Capitals impacted

Stakeholders impacted: C, Re

Committee of Directors

Oversees credit policy, exposures, settlements, treasury investments and critical business proposals.

Capitals impacted

Stakeholders impacted: C, I, Re

Environmental, Social and Governance Committee

Guides the Bank's ESG strategy, highlights material ESG issues, reviews ESG-related policies and advises on performance metrics and targets.

Capitals impacted

Stakeholders impacted: N, Re, V, Ra

Acquisitions, Divestment and Mergers Committee

Reviews and recommends proposals relating to mergers, acquisitions, strategic investments and divestments.

Capitals impacted

Stakeholders impacted: I

People, stakeholders and service governance

Nomination and Remuneration Committee

Oversees Board and senior management composition, performance, remuneration and human resource strategy.

Capitals impacted

Stakeholders impacted: E

Stakeholders Relationship Committee

Oversees security holder grievances and adherence to service standards.

Capitals impacted

Stakeholders impacted: I, Re

Customer Service Committee

Reviews complaints, customer-centric policies, initiatives to enhance customer service standards and the overall customer experience.

Capitals impacted	Stakeholders impacted
	C

Corporate Social Responsibility Committee

Oversees CSR strategy, CSR projects, fund allocation and alignment with the Bank's social and environmental commitments.

Capitals impacted	Stakeholders impacted
	N I Re

The Bank has additionally established a Committee, comprising the Whole-Time Directors (i.e. the Committee of Whole-Time Directors), to oversee delegated operational, administrative, and business matters.

Read more about the Committees in the **Statutory Reports** section from page 301-312 forming part of this report.

A culture anchored in ethics, compliance and accountability

Our policy framework aims to strengthen integrity, fairness, accountability, and responsible decision-making in daily actions.

Our policies

Code of Conduct and Ethics

Our Code of Conduct and Ethics embodies the Bank's dedication to ethical conduct and integrity, and commitment to its fundamental values. It delineates expectations for employee behaviour, promotes adherence to regulatory standards, and establishes mechanisms for reporting ethical violations. New employees acknowledge the Code, while current personnel reaffirm their commitment annually.

Whistleblower and Vigil Mechanism

The Bank upholds a strict zero-tolerance policy regarding violations of the Code of Conduct and the Ethics Policy. Its Whistleblower Policy and vigil mechanism facilitate the reporting of fraudulent, illegal, corrupt, or unethical conduct while safeguarding the whistleblower's anonymity and interests through a dedicated online platform.

Anti-corruption and Anti-bribery

The Vigilance function of the Bank is overseen by a Board-approved policy and led by the Chief of Internal Vigilance. This role entails promoting preventive vigilance, assisting in policy development, and reporting to the Audit Committee. Principal initiatives include Vigilance Awareness Week, annual staff declarations, training programs, and measures to ensure that service providers also adhere to vigilance standards.

Conflict of Interest Policy

The policy aims to identify, prevent, and manage conflicts between employees and stakeholders. Employees are expected to avoid situations that compromise objectivity, to prioritise the Bank's interests, and report potential conflicts to the Ethics Department.

Strengthening compliance in a demanding regulatory environment

During fiscal 2026, the regulatory environment for Indian banking continued to evolve, with an increased emphasis on financial stability, digital resilience, customer protection, data privacy, governance discipline, and responsible banking. In response, the Bank continued to enhance its compliance framework, refine regulatory oversight, and reinforce enterprise-wide accountability.

The Compliance function provides critical support to the Board and senior management through periodic updates on regulatory developments, compliance risk exposures, and emerging vulnerabilities. Additionally, the Bank has utilised technology to automate regulatory tracking, compliance monitoring, and reporting, thereby enhancing visibility and responsiveness across the organisation.

People's capability in compliance

In fiscal 2026, the Bank conducted a comprehensive assessment of its compliance staffing and skill sets. It enhanced its capabilities through targeted recruitment and training initiatives, ensuring that each business sector is supported by advisory resources with the appropriate regulatory expertise.

Group governance and 'One Axis' alignment

As a financial conglomerate, the Bank has enhanced oversight across its subsidiaries through a more cohesive Group governance framework. This encompasses policy alignment, Group-level compliance monitoring, review of licensing conditions, structured oversight by the Subsidiary Governance Committee, and coordinated guidance from the Group Chief Compliance Officer. This strategy underpins the 'One Axis' philosophy by fostering enhanced conduct, aligned regulatory engagement, and integrated compliance oversight throughout the Group.

Building a resilient, trusted and fraud-resistant Bank

Safeguarding against fraud and money laundering is vital for customer trust, regulatory confidence, and financial system integrity. As digital banking grows, the Bank continues to improve governance, analytics, technology, and awareness to help customers transact with confidence and to make it more difficult for fraudsters to exploit systems.

The Financial Crime Intelligence function draws its mandate from the Bank's commitment to ethical conduct, regulatory compliance, and customer trust. Our fraud risk management strategy is founded on sustained investment in advanced controls, data intelligence, analytics, AI-enabled detection, and proactive risk management. Rather than merely mitigating risk, we aim to position fraud prevention as a significant differentiator for the Bank.

During fiscal 2026, the Bank reinforced its fraud prevention framework by implementing customer-controlled digital security features, zero-trust onboarding procedures, layered authentication protocols, 24/7 real-time transaction monitoring, enterprise analytics, and ecosystem-level interventions to combat scams, phishing, and cybercrime. Additionally, the Bank continued investing in more robust Anti-Money Laundering (AML) monitoring and enhanced due diligence through AI-driven and workflow-led systems.

Six pillars of the Fraud Prevention Framework

- Customer empowerment and control
- Zero-trust onboarding and identity verification
- Robust authentication and access security
- Real-time transaction monitoring
- Data-driven analytics and automation
- Ecosystem-level fraud prevention

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

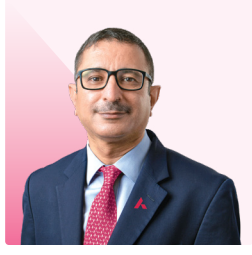
Risk Management Committee members

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

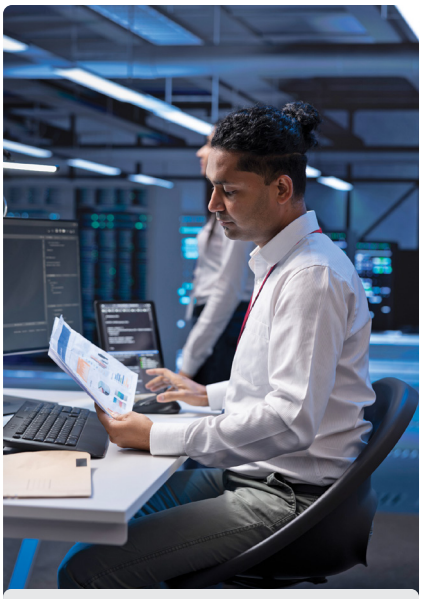
Global framework alignment and climate risk integration: The Bank publishes TCFD-aligned disclosures in line with RBI guidelines, recognising climate risk as a factor that impacts credit, operational, market, reputational, and liquidity risks. Through scenario analyses and stress testing, we monitor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

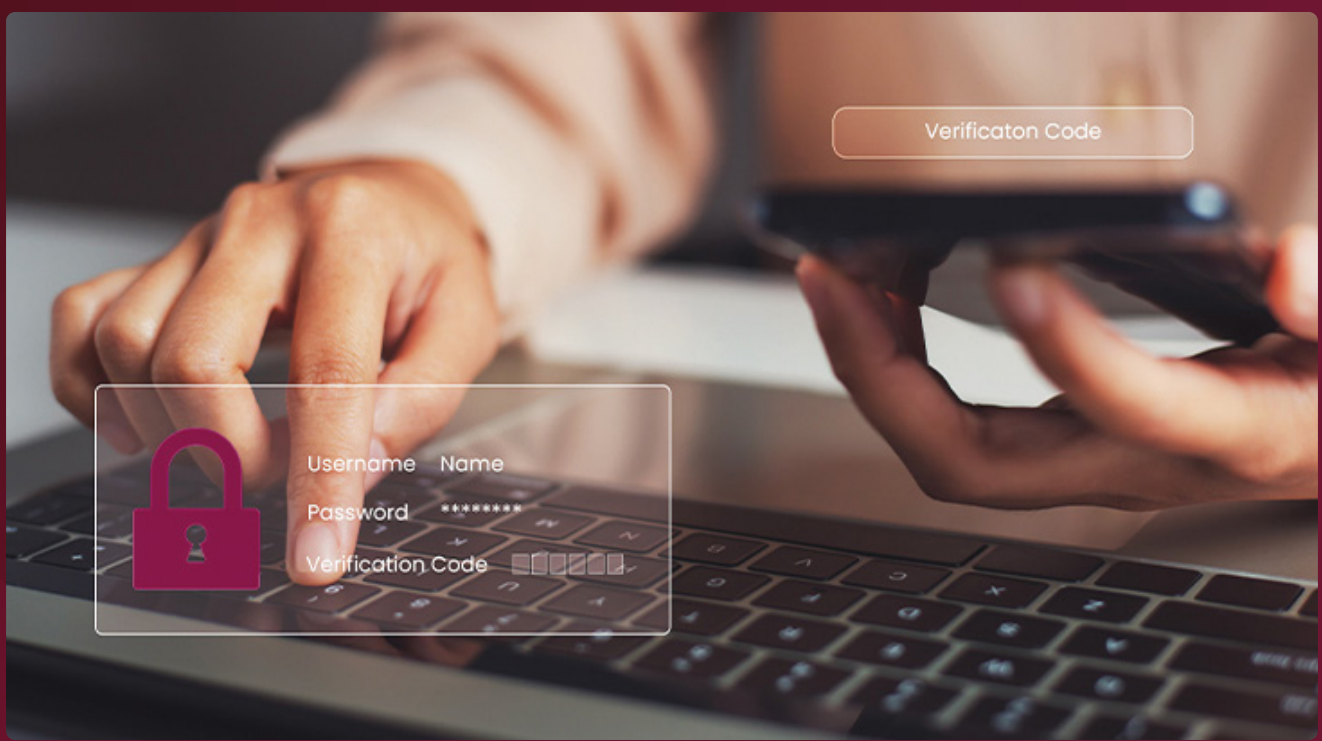
Business Continuity is managed by the Business Continuity Planning Management Committee, which guarantees effective implementation and testing of essential internal operations. Regular exercises and scenario-based reviews help prepare the Bank for disruptions and ensure continuous service and operational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

Security you can bank on

At Axis Bank, openness in banking is anchored in uncompromising security. Our cybersecurity and data privacy framework ensures that while digital engagement deepens, customer trust remains protected through strong governance, intelligent controls and resilient systems.



Material Issues Linkage

M1 M4 M5

Capital Linkage

UN SDGs Linkage

During fiscal 2026, the Bank bolstered its core infrastructure of trust and security by improving fraud prevention, enhancing authentication across digital touchpoints, tightening governance around in-house technology development and data platforms. These initiatives, which increased cyber resilience across enterprise systems, helped minimise risk, boost reliability, and ensure that customer data remains protected, well-governed and compliant with evolving regulatory standards.

Our approach is rooted in the conviction that openness in banking must always be supported by rigorous control, vigilance, and accountability. As digital engagement expands through mobile banking, internet banking, payments, APIs, AI-driven services, and cloud-enabled platforms, we continue to incorporate security, privacy, and resilience into every design. By integrating these baseline requirements into our cloud-enabled platforms, we ensure that innovation never comes at the expense of safety.

Trust, secured at scale

Security and privacy are treated as baseline requirements across all technology operations. Policy-led controls such as role-based access, advanced encryption, and auditable logs help the Bank ensure that digital engagement is both protected and transparent. These measures, alongside stronger authentication, governed data flows, and responsible AI practices, help the Bank deliver digital experiences that are secure, seamless, and dependable.

Security in action

High-reliability payments

A commitment to high-reliability infrastructure supports our strong performance in the UPI ecosystem, with high market share and near-zero UPI technical decline.

Responsible AI leadership

First BFSI organisation to secure ISO/IEC 42001:2023 certification, validating our leadership in responsible AI and robust technology governance.

Stronger digital authentication

Risk-based checks now strengthen authentication across major digital journeys.

Governed data foundation

A unified DataMart and centralised servicing of critical data are improving consistency, quality, and control.

Cyber resilience in action

We have fortified our enterprise defence through enhanced monitoring, automated SOC playbooks, and stronger controls over identity, access, and privileged operations.

Secure ecosystem expansion

Centralised API control, stronger encryption, and governed inventory management are reinforcing secure data exchange.

How cyber resilience is engineered across the enterprise

The Bank's cybersecurity employs a layered defence-in-depth model that incorporates policies, technology, governance, and continuous assurance. In an evolving threat landscape, we are proactively enhancing detection, response, and recovery while maintaining oversight across technology, third-party, and customer systems. Cybersecurity and data protection are vital and guided by policies on identity, access management, network security, encryption, monitoring, and data use to ensure compliance with regulations and the Bank's data protection obligations.

In fiscal 2026, the Bank's cyber defence saw major advancements with improved threat detection, automated incident response, vulnerability management, data controls, and governance. Measures such as endpoint hardening, network segmentation, analytics, and monitoring controls have provided enhanced visibility and faster response times. Cyber resilience was further fortified by a Zero Trust security model, which combined continuous monitoring, automated SOC playbooks and privileged access controls to reduce attack surface and threats. To ensure peak readiness, we conduct regular simulations, breach testing, and threat hunting to keep our defences robust.

Board and management oversight

Board-level oversight

- IT and Digital Strategy Committee
- Risk Management Committee

Management oversight

- Information System Security Committee
- Senior management reviews cyber risks, assurance, and compliance

Execution and assurance

- Security Operations Centre
- Technology, Risk, and Business teams
- Periodic audits
- KRI-based monitoring
- Structured cyber risk reporting

How cybersecurity became more robust in fiscal 2026

- Greater automation in incident response
- Expanded detection through threat hunting and simulations
- Tighter control over privileged operations and identity
- Stronger visibility through micro-segmentation and analytics
- Deeper oversight across third-party technology providers and cloud environments

Resilience by design

- **Zero-Trust in action:** Attack surface reduction, stronger visibility, and better protection against modern threats
- **Continuous monitoring:** Automated SOC playbooks and always-on security monitoring strengthen response readiness
- **Advanced testing:** Red teaming, breach-and-attack simulations, and proactive threat hunting expand detection coverage
- **Cloud and third-party control:** Risk-based onboarding, continuous assessments, and automated external monitoring via cybersecurity rating agencies

How security is embedded into every digital journey

As customer journeys become more digital and real-time, security must be integrated into the interaction. In fiscal 2026, the Bank upgraded mobile and internet banking with advanced monitoring, an intuitive interface, and new safety tools that give customers more control. With the development of key modules, such as mobile PIN and Safety Centre, entirely in-house, we have reduced reliance on external providers while improving governance, operational agility, and security. Risk-based authentication now supports core digital activities, building trust during onboarding, access, and transactions.

In the Payments domain, the Bank has achieved a high degree of reliability and security within the UPI ecosystem, with near-zero technical failures. AI-driven fraud detection and device biometric checks enhance safety. Additionally, the deployment of Smart Payout APIs enables secure, automated disbursements, improving control and customer experience.

AI-powered service tools speed up query resolution, secure interactions, and improve compliance through voice-enabled workflows and CRM integrations. AI tools also help identify risks early, reduce vulnerabilities, and automate remediation under a strict governance framework.

The Bank strengthens operational reliability with regular disaster recovery drills, Site Reliability Engineering (SRE) practices, automated testing, Infrastructure-as-Code, and centralised log analytics, reducing downtime and improving resilience.

Key advancements in fiscal 2026

- **Safer Digital Experiences:** New safety features across mobile and internet banking give customers more control over security settings
- **Secure Payments at Scale:** Strong UPI performance, with high reliability, high market share, and near-zero technical decline
- **AI with Accountability:** AI-based bots, voice-enabled workflows, and AI-supported development tools are improving service, security, and compliance
- **Operational Resilience:** Regular disaster recovery drills, SRE practices, automated testing, and Infrastructure-as-Code are improving continuity and stability
- **Technology Recognition:** Recognised at the Infosys Finacle Innovation Awards 2025 and ICC Emerging Asia Banking Awards for Best Bank in AI and ML Implementation

Privacy by design. Compliance by discipline. Trust by practice.

The Bank is continuously enhancing controls, governance, and accountability to protect data in a connected environment. Data protection is strengthened through encryption, data minimisation, tokenisation, and better consent management. Data classification, retention governance, and lineage support responsible data handling. Compliance with data protection laws is ensured through controlled access, API security, and privacy assessments, including the Digital Personal Data Protection framework.

A unified DataMart and improved data tracking ensure consistency, reduce errors, and enhance reporting. Data exchange is safeguarded through strengthened API security, with unified authentication and encryption. Secure coding, automated testing, and modernisation of contact centres and lending platforms further bolster application security and enable a Zero Operations model using low-code, no-code, and AI tools.

The Bank aligns with RBI, SEBI, CERT-In, and global standards, including ISO 27001, ISO 27017, ISO 27034, ISO 27018, NIST CSF, and PCI DSS. We achieved ISO/IEC 42001:2023 certification in fiscal 2026, bolstering our approach to responsible AI governance and security.

Backed by Certifications

- ISO 27001:2022 — Information Security Management
- ISO 27017:2015 — Cloud Security
- ISO 27034:2011 — Application Security Management
- ISO 27018:2025 — PII Protection in Public Cloud
- PCI DSS v4.0.1
- ISO/IEC 42001:2023 — Artificial Intelligence Management Systems

Recognition

The Bank's Information Security function received industry recognition at the IBA CISO Summit & Citations 2025 for:

- Cyber Security Incident Response Maturity
- Cyber Security Compliance Champion
- Cyber Security Metrics & Reporting Excellence

Shaping the future of financial services

We actively contribute to policy and industry dialogue to strengthen the resilience, inclusiveness, and future-readiness of the financial sector. Through strategic engagement with industry bodies, policymakers, academia, and global platforms, Axis Bank continues to offer informed perspectives on issues shaping banking, regulation, digital transformation, sustainability and economic growth.

Material Issues Linkage

M14

Capital Linkage

UN SDGs Linkage

From engagement to influence

During fiscal 2026, the Bank intensified its advocacy and outreach initiatives by actively participating in leading national and international forums. Axis Bank effectively executed the annual work plan of the FICCI National Banking Committee, under the stewardship of Amitabh Chaudhry, the Bank's MD & CEO, who brought together senior executives from across the BFSI industry. The Bank's spokespersons and subject-matter experts also served on a broad spectrum of industry committees, working groups, and policy consultations. Amitabh Chaudhry also served as Senior Vice President of ASSOCHAM throughout the year. The Bank's policy engagement encompassed regulatory submissions, review inputs, thought leadership perspectives, authored articles and active involvement in industry dialogues.

Key policy submissions and institutional engagements

The Bank's policy advocacy during the year covered a wide set of issues relevant to banking and the broader economy. Through its leadership of industry bodies, the Bank provided its recommendations, sectoral insights and structured inputs on regulatory, economic, technological, and sustainability matters.

FICCI

The Bank sustained strong engagement with FICCI during the year through policy submissions, committee participation, and contributions to working groups across key priority areas, such as

- Draft recommendations on the notified rules under the Digital Personal Data Protection Act from a BFSI perspective
- Inputs on the RBI framework for co-lending arrangements
- Participation in policy dialogue on the role of financial institutions in disaster risk reduction
- Submissions to the Parliamentary Committee on the future of banking
- Inputs on India's Climate Finance Taxonomy
- Contributions to compendiums on aspirational districts and AI vision
- Draft recommendations on GST rate rationalisation and the pre-budget memorandum for fiscal 2027
- Inputs on asset classification, provisioning, and income recognition norms
- Engagement on India-US trade and tariff-related matters
- Ongoing work under the FICCI DPDP Act Sub-Committee, including development of common personally identifiable information (PII) and privacy impact frameworks

CII

Through the Confederation of Indian Industry II, the Bank contributed research-based inputs and case studies, including:

- Submission of inputs on India's Climate Finance Taxonomy
- Contribution of a case study for the CII compendium on accelerating progress in aspirational districts

ASSOCHAM

Axis Bank's engagement with ASSOCHAM focused on macroeconomic dialogue, contribution of policy perspectives, and thought leadership interactions, including:

- Policy inputs for meetings with the Governor, Reserve Bank of India
- Submissions and perspectives ahead of Monetary Policy Committee meetings
- Thought leadership interactions with academic institutions
- Statements and insights on economic growth, GDP trends, trade agreements, GST reforms, and tariff-related developments
- Pre- and post-Union Budget interactions across leading business media platforms
- Participation in ASSOCHAM Media Connect and foundation-day engagements
- Contribution to ASSOCHAM communication and publications on India's growth and inclusion agenda

World Economic Forum and other platforms

- Publication of a thought leadership blog article focused on intelligent industries
- Inputs to global and regional benchmarking and league-table exercises
- Participation in DEI workshops in collaboration with industry chambers
- Development of a joint technology case study, highlighting digital transformation initiatives

Leadership representation across industry platforms

The Bank's contribution to policy and industry dialogue is strengthened by the active participation of its leaders across influential committees, councils, and advisory platforms. During fiscal 2026, senior leaders represented the Bank across forums on banking, treasury, digital business, marketing, human resources, DEI, legal, sustainability, CSR, and public policy.

Representation on industry platforms in fiscal 2026

Amitabh Chaudhry

MD & CEO

- Chairman, FICCI National Banking Committee
- Senior Vice President, ASSOCHAM
- Chairman, Finance and Audit Committee, ASSOCHAM
- Member, Managing Committee, IBA
- Member, CII Davos Steering Committee
- Author/Contributor, World Economic Forum

Sameer Shetty

Head DBAT & Strategic Programs

- Member, FICCI Working Group on Banks – FinTech Partnership
- Member, CII National Committee on FinTech
- Member, Steering Committee, ASSOCHAM International Fintech Festival

Damini Marwah

Group Chief Legal Counsel and Chief Ethics Officer

- Member, ASSOCHAM Steering Committee on IBC and Valuation
- Member, CII National Committee on Regulatory Affairs
- Lead, FICCI Working Group on DPDP Act

Neeraj Gambhir

Executive Director – Treasury/Global Markets

- Member, FICCI National Banking Committee
- Board Member, FIMMDA
- Member, RBI Committee on Treasury and Global Markets

Rajkamal Vempati

Head Human Resources

- Member, Advisory Board, Centre of Gender Equality and Inclusive Leadership, XLRI
- Member, CII National HR Council
- Chair, FICCI HR Committee

Abhejit Agarwal

SVP & Head – Sustainability and CSR

- Member, FICCI Task Force on ESG
- Member, CII Climate Change Council
- Member, CII Net Zero Council
- Member, WEF Steering Committee on Sustainable Finance

Dhruvi Shah

Executive Trustee and CEO – Axis Bank Foundation

- Member, FICCI Task Force on Climate Change and Sustainable Agriculture
- Member, CSR Committee, Bombay Chamber of Commerce and Industry
- Member, CII Council on Women Empowerment and Inclusion

Presence in public forums and institutional platforms

In addition to committee representation and policy submissions, the Bank's leaders actively shaped public dialogue through participation in leading conferences, seminars, and institutional forums. These engagements enabled the Bank to share perspectives on banking transformation, AI, economic developments, leadership, inclusion, sustainability and CSR partnerships.

Representation at key conferences and seminars in fiscal 2026

Speaker	Organiser	Event	Topic
Amitabh Chaudhry	FICCI	FIBAC 2025	CEO's Panel – Charting New Frontiers
Subrat Mohanty	IAMAI	GFF 2025	Can AI Manage Black Swan Events and How?
Damini Marwah	ET Legal	ET Global Legal Convention 2026	Women in Leadership — Dismantling Barriers to Partnership and Power
Neelkanth Mishra	FICCI	Banking Committee Members Roundtable	Impact of Tariffs and US-Iran War on the Indian Economy and the Banking Sector
Harish Iyer	ET Edge	Global DEI Alliance Summit 2025	Pride and Prejudice: The Economic Case for LGBTQIA+ Inclusion
Dhruvi Shah	NEWS	Investing in Nature	Ensuring Sustainability through Partnerships
Abhejit Agarwal	FICCI	FICCI CSR Summit and Awards	Innovating on the Edge – Impactful CSR Partnerships in Northeast India

Membership fees paid in fiscal 2026

(Name of the Institution: Amount paid)

- ASSOCHAM: ₹1,50,000
- FICCI: ₹1,50,000
- CII: ₹3,30,000
- BCCI: ₹90,000
- IBA: ₹88,50,000
- World Economic Forum: ₹1,99,00,000

Exclusive of applicable taxes