

Committed to Ethical Business Standards



Axis Bank is committed to achieving and adhering to the highest standards of corporate governance and it constantly benchmarks itself with best practices worldwide.

Our Policy on Corporate Governance

To enhance the long-term interest of its shareholders, provide good management, adopt prudent risk-management techniques and comply with the required standards of capital adequacy, thereby safeguarding the interests of its stakeholders such as shareholders, depositors, creditors, customers, suppliers and employees.

To institutionalise accountability, transparency and equality of treatment for all its stakeholders, as central tenets of good corporate governance and to articulate this approach in its day-to-day functioning and in dealing with all its stakeholders.

The Report on Corporate Governance for FY 2020-21 along with a Certificate issued by the Statutory Auditors of the Bank, confirming compliance with the mandatory requirements relating to Corporate Governance as stipulated under Chapter IV of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, forms part of the Bank's Annual Report 2020-21. The Report on Corporate Governance can be accessed from page 111 onwards of the Bank's Annual Report 2020-21 at www.axisbank.com/docs/default-source/annual-reports/for-axis-bank/annual-report-for-the-year-2020-2021.pdf.

Code of Conduct

Axis Bank's Code of Conduct and Ethics is a statement of its commitment to integrity and the highest standards of ethical practices, bolstered by the Bank's 5 Core Values. The Code defines the standards of conduct that is expected of all employees to ensure that the right decisions are taken while performing their roles and responsibilities. The Code is intended to serve as a charter to enable employees to make the right decisions, that underline the fundamental commitment to compliance with regulatory guidelines, set forth basic parameters of ethical and acceptable social behaviour and establish a system for detection and reporting of known or suspected ethical or regulatory violations. Each new employee at the Bank must mandatorily affirm to the Code; the Bank requires all employees to re-affirm to the Code at least once annually. The Code of Conduct can be accessed online at www.axisbank.com/docs/default-source/quarterlyreports/03code-of-conduct-and-ethics-senior-mgt.pdf.

Whistle Blower Policy and Vigil Mechanism

The Bank has in place the Whistle Blower Policy and Vigil Mechanism to encourage reporting of suspected or occurrence of illegal, unethical or inappropriate actions, behaviour or practices by the Bank's employees, without fear of retribution. Stakeholders may choose to report anonymously on an independently managed web-based application – axisbank.whistleblownetwork.net. In addition, the Bank provides for reporting of concerns directly to the Chairman of the Audit Committee of the Board in case reporting is on senior management of the Bank. In FY 2020-21, 329 incidents were reported under the Whistle Blower Policy, of which, 4 were categorised as potential cases of corruption/bribery. Of the total reported incidents, 44 were reported by the Bank's external stakeholders. 74 incidents are pending as on 31 March 2021.

Vigilance

The Bank has in place a Board-approved Internal Vigilance Policy, which outlines the Internal Vigilance Framework and the roles and responsibilities of the Vigilance Function. The Chief of Internal Vigilance (CIV), reports to the Executive Director. The roles and responsibilities of CIV include creating awareness about vigilance and implementation of a preventive culture in the Bank and arrange for submission of necessary reports to the Audit Committee of the Board/Board.

The Bank has taken several measures for creating a preventive vigilance culture. All employees are required to execute a Vigilance Declaration on joining and thereafter, annually. The Declaration clearly articulates the relevant acts and policies constituting the Vigilance angle, and any violations may be reported through the Bank's Whistle Blower mechanism of the Bank as part of the declaration.

Anti-Bribery and Anti-Corruption Policy

The Bank has in place an Anti-Bribery and Anti-Corruption Policy that reiterates the Bank's zero tolerance to bribery and corruption at the Bank. As a governance best practice, the Bank's Anti-Bribery and Anti-Corruption Policy has been made accessible on its website at www.axisbank.com/docs/default-source/quarterly-reports/anti-bribery-and-anti-corruption-policy.pdf.

Anti-bribery and Anti-corruption are integral parts of the Bank's training and awareness modules and feature in-training as well as e-learning sessions for employees to sensitise them in vigilance practices. In addition, all employees are communicated with regularly through electronic mailers on pertinent bribery and corruption related topics to reinforce the vigilance culture. Notably, Anti-Bribery and Anti-Corruption requirements are also advised and incorporated in agreements executed by the Bank with service providers.

The Bank observes the Vigilance Awareness week annually as per CVC guidelines wherein all stakeholders are encouraged to take the integrity pledge after strengthening their understanding of the bribery and corruption risks. Quizzes are also organised for employees to raise awareness.

In FY 2020-21, 171 cases were handled under the Bank's Vigilance Framework, of which a vigilance angle was established in 134 cases and other violations of the Bank's Code of Conduct were established in 23 cases. 206 officials were examined during investigations of cases and disciplinary action was initiated against 176 officials, resulting in punitive action.

Of the Vigilance cases handled in FY 2020-21, 122 cases were handled in the category of corruption and bribery. Of these, allegations in 95 cases were found to be true, resulting in stringent disciplinary action against 106 officials. Out of above cases, Suo moto investigation was initiated in 33 cases as part of preventive vigilance measures, resulting in disciplinary action against 52 officials.

Tax Strategy

Axis Bank is committed to acting responsibly at all times in relation to its tax affairs and maintaining its reputation as a responsible taxpayer. The Bank has in place a Tax Policy that seeks to address the management of tax risks arising for the Bank and its various operations and is also guided by relevant global standards such as the OECD guidelines. The Policy also addresses disclosures related to tax payments

made in each country that the Bank operates in (known as Country by Country Reporting).

As a governance best practice, the Bank has placed its Tax Policy on its website and can be accessed at www.axisbank.com/docs/default-source/quarterly-reports/tax-policy-of-the-bank.pdf.

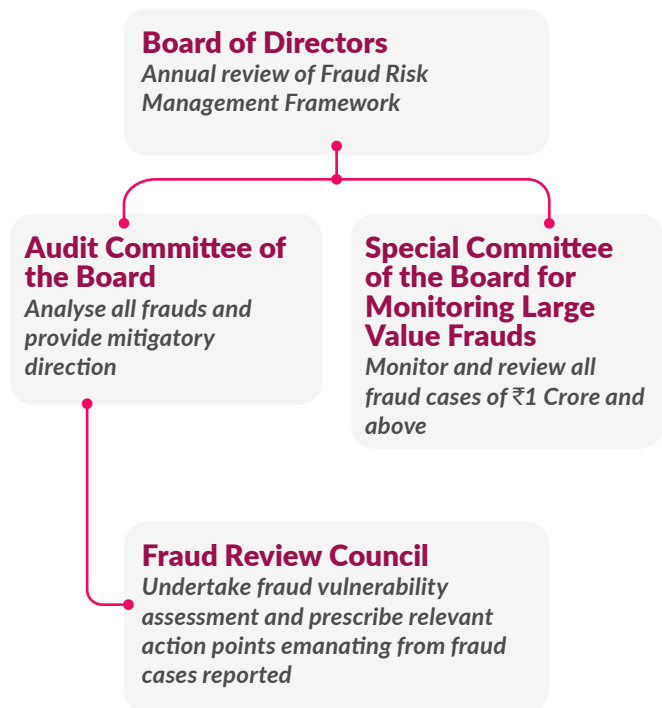
Fraud Detection and Mitigation

The Bank has expanded in geographical reach, systems, products and human resources. The introduction of anywhere banking and digital channels has led to the creation of a complex banking transaction scenario. While it is the Bank's endeavour to ensure that there is no fraud vulnerability within its domain, customers must be vigilant while using their own devices to complete online transactions and not fall prey to fraudsters who use various techniques to deceive the customers. Additionally, the Bank has set up a process to monitor customer transactions through a combination of value thresholds and velocity checks to help mitigate the fraud risk.

The Bank, on an ongoing basis, takes measures to prevent, detect and respond to incidents to protect and minimise frauds, by sharpening detection through learnings from incidents, initiating proactive control measures and other early detection systems. Fraud has an independent oversight within the operational framework. Our Risk Department, which directly reports to the Managing Director and has complete independence in its functioning, also has the overall responsibility of identifying and mitigating fraud risks.

As a financial institution, fraud detection and mitigation are an organisational priority at Axis Bank and we make every effort to maintain a secure, 'least vulnerable to fraud' environment, driven from the highest level by our Board of Directors.

The Bank's Policy on Fraud Management & Reporting serves as a reference document and guidance for the internal oversight and detection framework. The policy focuses on pillars including deterrence, prevention, detection, investigation, staff accountability, recovery and reporting. We have an end-to-end fraud risk management system for fraud detection and prevention in our cards, accounts and loan businesses.



The Bank has a sustained Safe Banking strategy aimed at creating an environment of banking-without-fear, for the customers in particular and public in general, to empower them with greater degree of awareness creation to create a safer environment for their banking transactions.

Artificial Intelligence & Machine Learning

The Bank uses advanced technologies including Artificial Intelligence & Machine Learning, which is extremely effective in fraud detection and prevention, as it deploys automated techniques to reveal fraudulent patterns across large volume of transactions. They further aid in proactive identification of suspicious activities that may result in fraudulence and thus prevent its occurrence.

Customer Engagement Programme

- Let's Talk - The Bank held conversations with ~2010 customers spanning across its branches. In these sessions, the customers were informed about cultivating safe banking habits while transacting through digital channels
- As a matter of routine practice, the Bank makes continuous efforts to create awareness among its customers and public through various channels such as WhatsApp video clips, among others
- Safe banking contents displayed on LED Screens at branches, SMS, emails, webinar and safe banking banners on our website, and so on

To create awareness among employees, theme-based Electronic Digital Mailers (EDMs) were sent to all the employees of the Bank highlighting:

- Recent fraudulent cases
- Key learnings
- Best practices which would empower them to educate customers for cultivating safe banking habits

These initiatives were great confidence-building measures among the customers of the Bank in collectively fighting fraudulence in the banking and financial services industry. The positive feedback received from the customers/ participants across sections sums up the effectiveness of this multi-faceted initiative undertaken by the Bank.



Information and Cyber Security

Axis Bank pursues a holistic information and cyber security programme with a comprehensive Information Security Policy, Cyber Security Policy and standards based on the best industry practices, with compliance to regulatory guidelines and in alignment to regulatory directives on Information and Cyber security.

Governance

At the executive level, as part of the Information & Cyber Security governance framework, the Bank has in place the Information System Security Committee constituting key business functions that meet at least once in a quarter to assess the threat landscape and validate the controls enforced by the Bank commensurate with the cyber risks. The Bank has invested in strong technical and administrative controls to proactively prevent, detect, and timely contain and respond to any suspicious activity. The Bank is compliant to ISO 27001 standard and PCI DSS standards.

The Bank conducts various assessments to identify and remediate risks before any application and/or IT infrastructure component is deployed, including application security, vulnerability assessment, penetration testing, security architecture review and data security assessment. The Bank also has adopted the defence-in-depth methodology to protect its crown jewels from intrusion by malicious actors. The Bank has a 24 x 7 Security Operation Centre (SOC) to keep vigil on its digital assets and coordinates with RBI, CERT-IN, NCIIPC and NPCI, among

others, for the implementation of their recommendations to strengthen its defense against cyber attacks.

Axis Bank has enabled its teams for work-from-home by provisioning them with laptops and secure remote applications to connect to the Bank's Network during the pandemic-related restrictions and regulations. It took cognisance of heightened levels of cyber security risks and enforced technical and administrative controls (based on the changing scenario of remote access for a sizable number of teams) to ensure protection against the potential cyber risks emanating from the work-from-home arrangement.

Details of the Bank's Information Technology and Cyber Security governance, controls and initiatives during the year are provided in the 'Information Technology and Cyber Security' section of the Management Discussion and Analysis on pages 102-13 in the Annual Report 2020-21, accessible at www.axisbank.com/docs/default-source/annual-reports/for-axis-bank/annual-report-for-the-year-2020-2021.pdf.

Customer Privacy & Data Security

The Bank remains committed to adopting the highest standards for customer privacy and data security, and is guided by its Customer Privacy Policy, accessible at www.axisbank.com/privacy-policy.

The Bank has also rolled out the Digital Cookie Policy that gives information to the visitors and customers about the safe usage of their information through cookies to assist in providing better services.

Axis Bank has also rolled out a feature on curating consents from existing customers for Internet Banking. Through such consents from customers, their choices of processing data for various purposes like marketing, service and support are recorded and this information may be used further in alignment with customers' preferences.

Axis Bank is committed to always updating its privacy policy on its website that provides more information on the importance the Bank enforces on ensuring customer privacy and private data protection. As the new update is available, all the customers will be notified on the same, along with access to an online portal to manage their preferences.

Protecting Customer Data from Breaches

Axis Bank's control environment for privacy is supported by strong information security systems to maintain poise in managing alerts related to data breaches. All private data, that internal data consumers consume, is masked to ensure that customer identity is not revealed for general processing purposes.

From the reporting year onwards, Axis Bank has initiated entering into data sharing contracts with all vendors processing its customer data towards further protecting customers' interests.

In alignment with EU's GDPR regulation, the Bank maintains records of personal data processing activities for businesses conducted, where personal data of non-residents is in scope, helping the Bank implement the privacy and protection controls across data operations and further changes to operational processes that include personal data. Additionally, the Bank also performs a legitimate interest assessment – a balancing activity that assesses if

personal data of customers being processed, that is not consented, does not override rights of customers over the Bank's interests. This includes detecting and stopping fraudulent transactions.

Under Internet Banking, the Bank has also introduced a consent notice to inform consumers about storage, processing and transfer of their personal information. Notably, all changes to processes and Information Technology systems within the Bank are monitored within the control environment of a framework known as Privacy-by-Design, wherein a data governance team assesses, monitors and directs changes to put in controls that protect personal data of customers.

Product Responsibility

Axis Bank's products and services cater to a wide spectrum of the Indian economy and society, and are designed to best meet their needs and requirements. The Bank has the necessary checks and balances in place to ensure that its product offerings meet the stringent norms put in place by the Reserve Bank of India, and that its representatives, especially those dealing directly with customers, whether in person, on the phone, or online, are adequately trained on critical 'Know Your Customer' policies, and equipped with the relevant product information. In this regard, the Bank's key codes, policies and commitments towards customers, such as the Code of Commitment, Citizen's Charter and Customer Rights Policy, among others, are accessible on the Bank's website at www.axisbank.com/webforms/code-of-commitment.

The Bank is cognisant of its responsibility to adequately cater to people with disabilities, and has in place branches, ATMs, offices and digital services that enable easier physical and digital access to avail Bank's products and services. The Bank has also made its corporate website more user-friendly. Additional, details on the Bank's services for customers with disabilities is provided on its website at www.axisbank.com/services-for-customers-with-disabilities.

Human Rights

We remain committed to respecting and imbibing internationally recognised human rights principles and standards and putting in place the systems and processes to ensure no human rights violations occur across the range of our operations. In the reporting year, the Bank's Human Rights Policy, which was so far an internal policy at the Bank, was revised and expanded in its scope and commitments, and put in the public domain. The Policy has been framed referencing the key global human rights frameworks and principles including the OECD Guidelines for Multinational Enterprise, ILO Declaration on Fundamental Principles and Rights at Work and United Nations Guiding Principles on Business and Human Rights, among others. The Policy is accessible at www.axisbank.com/docs/default-source/default-document-library/human-rights-policy.pdf.

Ensuring Business Continuity

The criticality of having agile business continuity management in place has been amply demonstrated by the COVID-19 pandemic. Since January 2020, when the COVID-19 pandemic first began spreading across India, the Bank proactively began to take the necessary measures to put in place adequate policies and systems to ensure the continuity of its business activities, the safety of its employees, customers and other stakeholders, and the integrity of its systems.

The Bank's Business Continuity Plan (BCP) is an integral component of its overall risk governance framework and managed by BCP & Crisis Management Committee (BCPMC) under the Board of Directors. The BCP was tested well in advance prior to the pandemic and continues to be managed by the Central Emergency Response Team (CERT), led by the Board members. Training on the BCP is mandatory for all employees. The Policy is accessible at www.axisbank.com/docs/default-source/default-document-library/human-rights-policy.pdf.