GOVERNANCE

Ethics and GOVERNANCE

Business ethics and corporate governance are key value drivers, and we ensure our practices are aligned to the regulatory requirements as well as global best practices. Policies, systems, and procedures, are in place to ensure transparency, efficiency and accountability.[43]

21 years
Average tenure of the Executive leadership team at the Bank

Zero
Reported breaches of customer privacy

'Leadership' category
as assessed by IiAS on the IFC-BSE-IiAS Indian Corporate Governance Scorecard based on G20/OECD corporate governance principles.

Material topic(s) covered

- Corporate governance
- Ethical business processes
- Regulatory compliance
- Data security
- Brand and reputation
- Contributing to development of regulations and policies

Impact on SDGs

5 GENDER EQUALITY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
13 CLIMATE ACTION
16 PEACE, JUSTICE AND STRONG INSTITUTIONS

At Kotak Mahindra Group, we believe that strong governance is the foundation to continued success. Our principles of governance encompassing accountability, responsibility, integrity, independence, transparency in dealings as well as fair and timely disclosures guide our business processes and are intrinsic to our work culture. We have instituted Codes of Conduct for our employees and Directors, which outline our ethical practices, culture, values, and standards. We have a zero-tolerance policy to any violations of the Code of Conduct. Our Board of Directors along with our top management team play an indispensable role in ensuring a strong governance approach in all our business functions. Dedicated Board level committees oversee the formulation, implementation and revision of various policies that guide our operations and we also have management level committees that closely guide and monitor the functional teams. Our Board provides a combination of professionalism, knowledge and experience required in the banking industry bringing a wealth of experience. Details of our governance structure and its effectiveness can be found on page 197 onwards in the Corporate Governance Report. Further, details on evaluation of Board effectiveness can be found on page 171 onwards in the Directors' Report.

FOSTERING A CULTURE OF ETHICS[43]

We are invested in nurturing the values of ethics, transparency and humility that are fundamental to our work culture. We inspire commitment to our corporate values through training programmes, employee engagement sessions and through daily interactions of our leadership team with employees. We have curated a suite of programmes that aim to entrench our values and standards of corporate ethics in the minds of our workforce. The employee induction programmes and other mandatory trainings covers the Bank's commitment to ethics while cultivating a risk management oriented mindset.

We are steadfast in our approach to combat corruption, money-laundering and associated malpractices. Our Vigilance Committee is responsible for instituting the anti-corruption measures and the vigilance policy covers both preventive and detective vigilance. We also have a Board-approved Anti-Money Laundering (AML) policy that promotes high ethical and professional standards to prevent us from being used, intentionally or unintentionally by criminal elements. This policy is supported by Board approved KYC standards, which enable us to understand our customers or beneficial owners and their financial dealings in turn helping us to manage risks prudently. In addition, we have numerous self-paced mandatory ethics focused courses and classroom trainings on various ethics and governance topics that are crucial to effectively running a financial institution.

We established a Trading Code of Conduct that governs our employees by laying down standard procedures for seeking compliance approval before trading shares and states the reporting requirements for securities trades carried out by our employees and their immediate relatives. Further details can be found in the Director's Report under Code for prevention of insider trading.

We imparted over 22,200 hours of training on Anti-Money Laundering at the Bank

We also collaborate with various associations to understand industry-wide issues and opportunities. We leverage this knowledge to update and modify our internal policies. We are also member of prestigious Indian industry bodies. These industry associations enable us along with our stakeholders to collectively identify, understand and address industry-wide issues, as well as implement responsible decisions within the organisation. Further, details can be found in our BRSR disclosures under Principle 7.[44]

[43] GRI 102-16, GRI 102-17, GRI 103-2, GRI 103-3, GRI 205-2 | [44] GRI 102-13

INFORMATION SECURITY AND DATA PRIVACY[45]

Digital transformation backed with robust information technology (IT) infrastructure plays an indispensable role in meeting the ever-evolving needs of our customers. In recent times, the role of IT in facilitating business continuity and customer servicing has grown significantly. In this context, we recognise our fiduciary duty to protect the integrity of our IT systems and customers' data. Our Chief Information Security Officer (CISO) is responsible for the implementation, oversight, review, and monitoring of our cybersecurity strategy and Information and Cyber Security Policy.

We ensure compliance with Unique Identification Authority of India (UIDAI), EU General Data Protection Regulations (GDPR) in applicable geographies, as well as other relevant domestic and international regulations on data privacy, personal data protection and cyber security. We have instituted a Privacy Policy that applies to all our employees and contractors of our non-resident business where GDPR is applicable. Further, this policy also applies wherever Aadhar is used for conducting business activities in India. For our operations where EU GDPR is applicable, we inform our customers about privacy protection issues which include the nature of customer information captured, the use of collected information, information on data protection, and third-party disclosure policy among others. We have appointed a Data Protection Officer (DPO) who is responsible for monitoring privacy compliance. The DPO is supported by a data protection task force which includes staff from different teams such as Information Risk Management (IRM), Operational Risk Management team and Legal team to assist with privacy compliance.

Apex Information Technology Policy

We have instituted an Apex Information Technology Policy to ensure the effective protection and proper usage of the computer systems within the Bank. The Board-approved Policy focuses on ensuring the integrity, reliability, and availability of the IT systems and processes, while also providing guidance for dealing with violations and exceptions appropriately. The IT Policy applies to all our employees, consultants, contractors, vendors, and third parties.

APPROACH TO CYBERSECURITY

We are cognisant of cyber threats and associated risks. A programmatic approach encompassing a cyber-resilience framework has been established to mitigate threats such as data breaches, malware, denial-of-service attacks, etc. We conduct cyber drills to assess the effectiveness of prevention, detection, and response controls. We have invested in best-in-class IT infrastructure to proactively detect malicious behavior or anomalies. Our Information Systems are ISO 27001 certified and periodic third-party security assessments are conducted to assure its security. These systems are continually upgraded through significant investments in information security systems. Each new digital product offering is assessed for cybersecurity risks before roll out and subsequently monitored on an ongoing basis. Periodic audits or assessments and thematic assessments of critical systems are conducted to assess the robustness of technology controls and minimise the impact of incidents, if any. A designated e-mail address has been put in place for reporting cyber security incidents or weaknesses. We did not have any instances of reported data breaches during FY 2021-22.[46]

A layered technology architecture is implemented to manage risks due to system failures, cyber-attacks etc. Disaster recovery and Business Continuity Plans (BCP) have been established and various functional and technology initiatives have been taken to enhance system resilience.

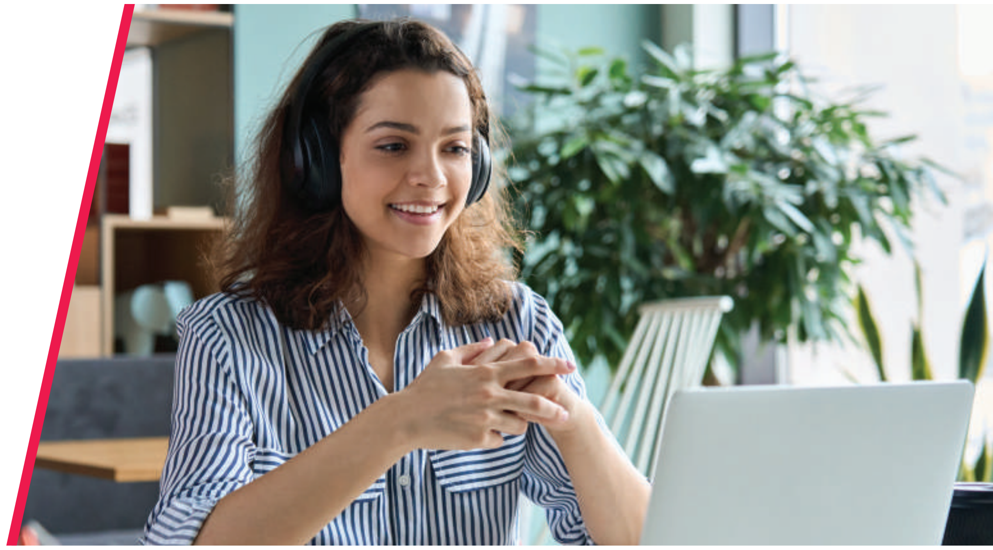
The Information Security Management Systems are ISO 27001 certified. Periodic third-party vulnerability analysis is conducted to assure the security of IT systems.

Cyber Crisis Management Plan (CCMP)

We have developed a CCMP as part of our cyber resilience framework to respond to and counter cyber-crisis. The CCMP lays out the governance mechanism for dealing with a cyber-crisis scenario, and also guides our responses to act in similar scenarios.

We have also taken initiatives to spread awareness and train employees and other stakeholders to effectively respond to a cyber-crisis.

Amongst our subsidiaries, KMAMC has subscribed to various services like threat intelligence and Distributed Denial of Service (DDoS) prevention. It has deployed solutions like Data Loss Prevention (DLP), USB blocking, hybrid proxy solutions, data encryption, simulated attacks, and Vulnerability Assessment and Penetration Testing (VAPT) activities, amongst others to ensure data privacy and information security.



TRAINING ON INFORMATION SECURITY AND DATA PRIVACY

During FY 2021-22, we undertook several initiatives to generate employee and management awareness on information security. An induction training is provided to all new joiners, which includes a dedicated module on information and cyber security awareness. Employees are also required to complete an Information Security course annually and to ensure completion periodic reminders are sent. The IRM team and CISO team also send periodic e-mails with security tips and cyber-security related updates to our employees (including contractual employees). Additionally, we conduct regular phishing awareness exercises to increase awareness amongst our employees.

With our investments, training, and awareness sessions, we make sure that we do not have any instances of data breaches.

[45] GRI 103-2, GRI 103-3 | [46] GRI 418-1