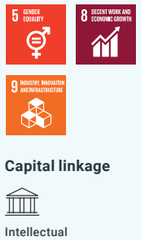
ETHICS AND GOVERNANCE

Maintaining Highest **Standards.**

At Kotak, business ethics and corporate governance are entrenched in every aspect of our business and decision-making. We strive to align our business practices with the highest governance standards. Our policies, systems and procedures have been designed with the intent of communicating our values, priorities and strategy across all levels of the organisation. We regularly review all our policies and modify them periodically to comply with the most recent regulatory requirements and industry best practices.

SDG linkage



Capital linkage

Intellectual capital

Relevant material topics

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

KPIs

20+ yrs
Average tenure of the Kotak Leadership Team with the Group

Zero
Data security and customer privacy breaches

47,923
Employees undertook the AML and anti-terrorist financing training recording 36,240 learning hours

48,548
Employees undertook trainings on data security and/or privacy-related risks and procedures recording 24,437 learning hours

Fostering a Culture of Ethics and Integrity[1]

At Kotak Mahindra Group, our processes are designed with a strong emphasis on sound governance practices. Our key principles of governance include accountability, responsibility, integrity, independence, transparency in dealings as well as fair and timely disclosures. We expect our employees to consistently embed responsible behaviour in their day-to-day activities by embracing our corporate values and principles. We ensure that our employees receive adequate training on our policies, procedures and values. We also undertake regular awareness-building initiatives to keep them up to date with evolving practices.

The Bank's Board consists of eminent individuals with expertise and experience in various fields. The Board members understand and respect their fiduciary roles and responsibilities towards KMBL's stakeholders and strive to meet their expectations. The Boards of the bank and subsidiary companies provide a combination of professionalism, knowledge and experience required in the financial industry. All the board members of the Bank are above the age of 50 bringing a wealth of experience.[2]

The Board approved employee CoC communicates our ethics, values and position on crucial business issues. This Code articulates the standards of professional conduct and ethics we expect our employees to imbibe and guides them to adopt practices that promote anti-bribery and corruption-free business, anti-money laundering, among other aspects linked to ethics. All our employees are required to undergo training and required formally acknowledge adherence to the CoC at the time of joining and annually throughout their course of employment with us.

During FY 2022-23, above 22,000 employees undertook training on ethical standards and over 99% of employees acknowledged their adherence to the CoC digitally. We have imbibed a zero-tolerance approach to any violations of the Code, wherein any observed violations are treated seriously, resulting in timely disciplinary action depending on the severity of the breach of the Code. We have also implemented a Trading Code of Conduct that provides employees with guidance on responsible trading and sets out the standard procedures and approvals they must follow before trading.

We have employed robust systems to combat bribery, corruption and money laundering. Our approach is built on a strong foundation of the Board-approved Anti-Money Laundering (AML) Policy and the CoC. The AML Policy also covers 'Know Your Customer' (KYC) standards which help us become familiar with our customers and beneficial owners, enabling us to prudently manage our risks. The details of the Policy can be found on page 363 of the Annexures of this Report.

We also have in place a Board-approved Vigilance Policy which includes preventive as well as detective vigilance. The vigilance policy is implemented by the Vigilance, HR and numerous other departments of the Bank. The Chief of Internal Vigilance (CIV) heads the vigilance department and is appointed by the Board. The CIV presents quarterly updates on vigilance activities to the Audit Committee of the Board as well as to the Board of Directors. The Vigilance department under the oversight of the CIV is responsible to undertake independent investigations of reported cases. Each business unit or function is governed by the Board approved delegation matrix for expense approvals and loan sanctioning alongside their policies and processes which adds another layer of protection against fraud and corruption. Our vigilance oversight also extends to relevant complaints concerning outsourced agencies or vendors. The internal audit and Risk Control Unit (RCU) teams monitor the adherence of teams to the respective policies. We have put in place systems that monitor employee transactions and flag and investigate unusual patterns of transactions. We have also identified certain roles which may be more prone to bribery and corruption and categorised them as high-risk roles, where clearance from the Vigilance department is required to enable the movement of employees to these high-risk roles. The Bank has also put in place Risk Control Self-Assessment (RCSA) for each function or business which supports the identification of risks related to corruption. We receive incidents of corruption through the whistle-blower portal. In the case where any incidents are reported through any channel, an independent investigation is followed by disciplinary action wherever required, an update of which is reported to the Board of Directors as well as the RBI. Our subsidiaries' policies, procedures and practices are also aligned with the Group's overall values and principles.

During FY 2022-23, we provided 36,240 hours of training on KYC norms and AML measures to 47,927 employees.

Managing Data Privacy and Data Security with Integrity

At Kotak, it is our constant endeavour to deliver digitally differentiated services and products tailored to the diverse needs of our customers. Our digital capabilities are augmented by resilient information technology infrastructure built to safeguard the integrity of our customers' data and our IT systems. We have Cybersecurity and Data Privacy policies accessible to all our employees. Our employees are required to undergo cybersecurity and data privacy-linked training. The details of the policy can be found on page 363 of the Annexures of this Report.

Our Cybersecurity Policy and Information Security Policy and the Apex IT Policy are formulated to complement each other, enabling our employees to deliver services to our customers responsibly while ensuring the security and privacy of their data. The details of these policies can be found on page 363 of the Annexures of this Report. Formulated with regulatory direction in mind, both these policies also take into consideration the best practices in the industry such as the NIST Cybersecurity framework and ISO 27001. Our Governance framework for managing technology and cyber-related risks is guided by a three-line defence system, which is as follows:

1 First Line of Defence
Information Technology (IT) Team and Business Units

2 Second Line of Defence
Chief Information Security Officer (CISO) who reports to the Head of Risk Management

3 Third Line of Defence
Internal Audit

The CISO oversees the implementation, reviews and monitors our cybersecurity policy and strategy. We have two Board-level Committees, namely the Risk Management Committee and the IT Strategy and Digital Payments Promotion Committee, and a Management Committee, the Information Security Committee, which are responsible for the oversight of the Bank's IT infrastructure and cybersecurity. As part of the first line of defence, the IT team conducts periodic self-risk assessments to evaluate the effectiveness of security controls and areas for improvement to prevent and mitigate risk and threats to the Bank's digital and physical infrastructure. Further, the audit function provides an independent assessment of the first and second line of defence and reports to the Audit Committee of the Board.

[1]GRI 2-23, 2-26, 3-3, 205-2 | [2]GRI 405-1

ETHICS AND GOVERNANCE

We are committed to upholding compliance with regulatory standards such as the UIDAI, and the European Union's General Data Protection Regulations (GDPR) in applicable regions, as well as other relevant domestic and international guidelines. During this financial year, there were zero reported cases of data security breaches and incidents related to personally identifiable information of customers.[3]

We comply with the regulatory standards governing data privacy, personal data protection and cybersecurity. To ensure adherence, we have introduced an Information Security and Cybersecurity Policy, which applies to all our employees. Further, we have a Privacy Policy that applies to all our employees and contractors in our overseas business, especially in areas where GDPR is in effect. In addition, we have established an Apex Information Technology Policy to ensure the optimal and appropriate use of computer systems, strengthen our IT infrastructure and protect the integrity of the IT systems within the organisation. This Board-approved policy applies to all our employees (i.e., permanent, temporary or trainee), consultants, contractors, third parties and vendors associated with the Bank.

We have identified three IT focus areas to create significant improvement in our operations

Architecture and infrastructure

As part of this focus area, we have established an architecture review board to ensure strategic growth. We have also established a near Disaster Recovery site for improved resiliency of the core systems. We have also launched a Salesforce-assisted savings account onboarding platform and an Xpress Do-it-Yourself platform to facilitate the opening of savings accounts directly by customers, reducing customer acquisition time and ease of operation for customers.

Talent and culture

We have introduced a new operating model wherein software engineers and product managers, along with programme managers are building new in-house platforms. We are also focusing on recruiting new STEM talent, which is poised to help us in the digital journey Kotak is undertaking. Further details can be found on page 63 of the 'Empowering Our Employees' section of this Report.

Risk and security

We conduct weekday Business Continuity runs for all core platforms, implement best practices of cyber security monitoring and analysis, along with upgrading systems to operate on a real-time basis—a few of these upgrades go beyond daily transactions such as NEFT and RTGS, and extend to service requests. We are also in the process of extending these real-time solutions to benefit pensioners registered with the Central Pension Accounting Office.

Recently, we have integrated a behavioural biometrics solution for Net Banking and Payment Gateway, which monitors user behaviour to identify any potential deviations. Without impacting the user experience, this solution triggers a high-risk score and highlights the key factors contributing to the score and alerts the RCU team. We are also intending to extend this service to the Mobile banking application helping us identify and arrest threats.

Furthermore, with an aim to strengthen our IT systems and processes, we conduct disaster recovery drills and put in place various security solutions such as database activity monitoring, application log integration (for relevant critical applications), data leak prevention across all IT system endpoints and micro-segmentation for the SWIFT application. This ensures that only whitelisted traffic reaches the SWIFT application server thus ring-fencing and reducing the attack surface of the application and strengthening its infrastructure's security posture, and endpoint detection and response solution to proactively prevent and/or detect advance persistent threat attacks. SaaS solutions in place of anti-malware solutions have been implemented to improve signature compliance. In addition to these initiatives, the IT assets inventory is centralised and our firewall architecture has been transformed to maintain continued security. As part of this transformation, the Bank has deployed an additional layer of firewall cluster with a two-tier hyper scalable architecture at both data centres and disaster recovery sites.

DATA PRIVACY

The Group's Privacy Policy is in alignment with relevant and applicable laws and regulations and is pertinent to everyone who has provided information to the Bank with the intention of establishing a relationship. We inform our customers on privacy protection concerns, including the collection and use of their information, data protection, and third-party disclosure policy among others. In addition, we have appointed a Data Protection Officer (DPO) to oversee and ensure compliance with privacy regulations. The DPO is accountable for the implementation and management of the privacy programme at the Bank and is assisted by a data protection task force comprising personnel from various teams, such as the Information Risk Management (IRM) team, Operational Risk Management (ORM) team and the Legal team, collectively enabling privacy compliance. We have a Cyber Security and Information Security Strategy in place, which is centred around three main pillars namely, people, process and technology.

In addition, as a part of the operational measures to help monitor and swiftly respond to data breaches, we have in place a Cyber Crisis Management Plan and an Incident Management Plan. Our Security Operations Centre (SOC) operates 24x7 to handle any data breaches and cyberattacks, and we also undertake routine privacy impact assessments.

OUR APPROACH TO CYBERSECURITY

As a Group, we recognise the severity of cyber threats and the associated risks they pose. To effectively combat and mitigate these threats, we have established a programmatic approach that includes a cyber-resilience framework designed to address potential risks such as data breaches, malware, denial-of-service attacks and others. The established controls and mechanisms are as follows:

Risk Assessment
Identifying risks across products, processes and systems.

Security testing
The systems are assessed for security requirements at the time of on-boarding and an ongoing basis. The Vulnerability Assessment and Penetration Testing (VAPT) of the systems is conducted as per defined schedule based on the criticality of the systems.

RED Team exercise and Cyber drills
The drills are conducted periodically to measure the effectiveness of prevention, detection and response controls implemented by the Bank.

24x7 security operations centre (SOC) monitoring
The SOC operates around the clock for identifying and responding to security incidents.

Threat hunting
Threat hunting is done for proactively identifying anomalies and vulnerabilities.

Threat intelligence
The threat intelligence feeds that are received from various sources (security partners, regulators, etc.) are utilised for hunting.

Our IT infrastructure is designed to proactively identify malicious behaviour or anomalies. Our information systems are ISO 27001 certified, and we conduct regular third-party security evaluations to ensure their robustness. These systems are continuously upgraded through significant investments in information security systems. Each of our digital products is thoroughly assessed for cybersecurity risks before being launched for public use. These products are also consistently monitored to ensure seamless service and security. We also perform periodic audits and thematic assessments of our critical systems to assist in evaluating the robustness of technological controls and reduce the impact of incidents. To facilitate the reporting of cybersecurity incidents or vulnerabilities, a specific email address has been established. Additionally, we have implemented a layered technology architecture to manage risks associated with system failures, cyber-attacks, and other similar events.

We have also established Disaster Recovery (DR) and Business Continuity Plans (BCP), along with various functional and technological initiatives. These activities have been undertaken to enhance the overall resilience of our systems.

To complement these activities, we also perform ad-hoc exercises regularly initiated both internally and externally, for application security testing, vulnerability assessment and source code review, to identify any vulnerabilities in our mobile or web applications, source codes and the larger IT Infrastructure.

We aim to continue focusing on four main critical areas to strengthen our long-term business growth trajectory. These four critical areas include: building scalable IT infrastructure, the development of robust business continuity and disaster recovery plans, retention of skilled and competent IT professionals, and the adoption of effective data management, analytical tools and systems.

CAPACITY BUILDING TO ENHANCE THE EFFICACY OF OUR SYSTEMS

Every new member of the workforce undergoes induction training which includes specific modules that promote awareness of data privacy for customers and cybersecurity. Our employees are also required to complete an Information Security Course on the Learning Management System annually which provides insights into the latest information security procedures. In addition to these training and awareness sessions, during FY 2022-23, we implemented several measures to generate employee and management awareness on information security including how to identify phishing scams and other potential threats. Further, our IRM team and CISO send out regular emails with cybersecurity-related updates and security tips to all our employees, including contractual employees.

Ethics and Governance will continue to be an important focus area for us going forward. We will continue to make our IT and cybersecurity infrastructure more robust and strengthen our governance practices to ensure that our systems are aligned with industry best practices.

[3] *GRI 418-1*