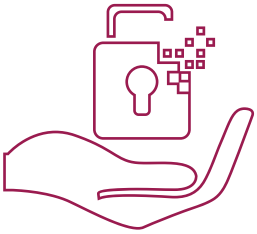
ETHICS & RISK MANAGEMENT

Ethics is one of the key aspects that define our values. Stakeholders' interests are important to us and we always strive to protect them. We conduct our business in an ethical and transparent manner and have put in place policies, procedures and controls across our operations to guide us in doing so.

G4-56-58
G4-SO4

Codes and Policies

Our Code of Conduct and Ethics is the guiding document for our employees on ethical behaviour and acceptable conduct. The Code address various aspects including, but not limited to ethics, conflict of interest, non-discrimination, and bribery and corruption.



- Regular trainings and awareness on the Code are conducted through e-learning programmes, training sessions and an annual sign off on the Code by the employees.
- The Board of Directors and the Senior Management of the Bank are also guided by similar codes which guide them in adopting high ethical standards in managing the affairs of the Bank.
- There is an induction programme for new Directors covering areas relating to Board governance, finance and accounts, compliance, internal audit, human resource and operations.
- The Board members are also apprised of various emerging trends including sustainability topics through presentations made to the Board at its meetings.
- The Code of Commitment to Customers is a voluntary code adopted by us.
  - It is based on codes and standards of Banking Codes and Standards Board of India (BCSBI) and is aimed at safeguarding customer interest and promoting fair and transparent dealings with our customers.

A whistle-blower mechanism has been put in place to provide a platform for reporting of suspected or actual occurrence of illegal, unethical or inappropriate actions, behaviour or practices by staff without fear of retribution. An Ethical Counsellor has been appointed to help employees who are in need of counselling regarding any wrongdoing that they may have witnessed, and guide them through their roles and responsibilities in seeking redressal of such wrongdoing.

Policy frameworks for various aspects of organisational and employee behaviour are put in place and are supported by well-documented procedures with defined accountability at various levels.

Code of Conduct for Directors and Code of Conduct & Ethics for Senior Management

Code of Commitment and Whistle-blower Policy

Policy Framework

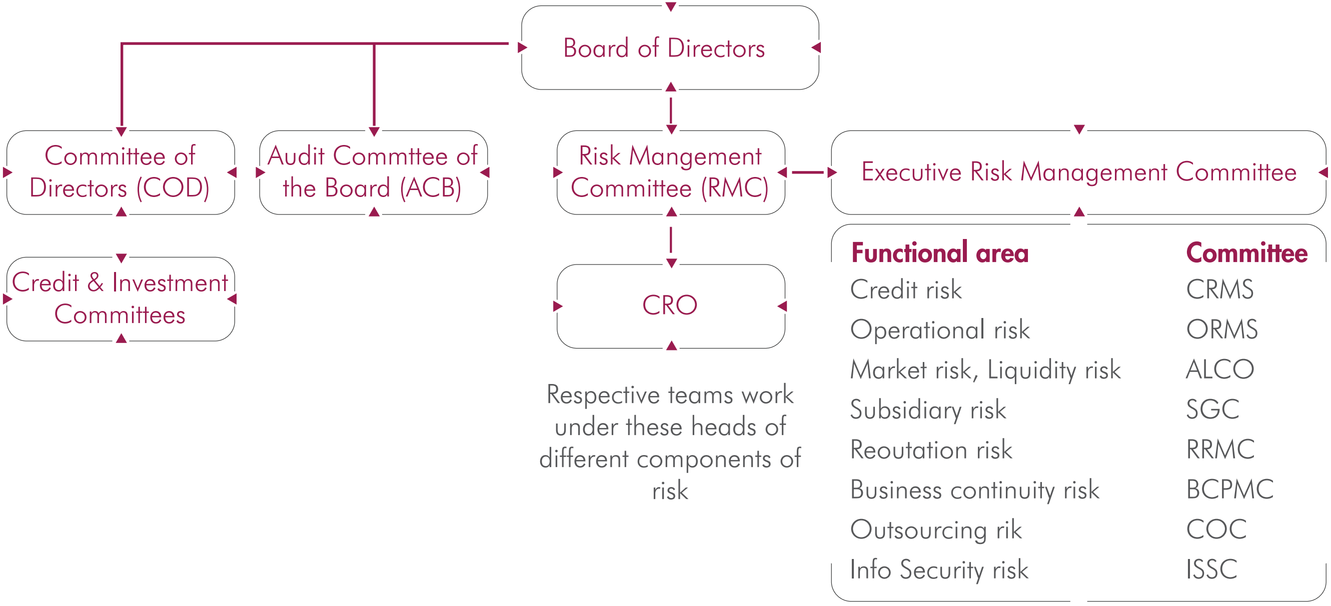
Risk Management

G4-46

The primary objective of our risk management framework is to balance the trade-off between risk and return and ensure we operate within the Board-approved Risk Appetite Statement.

The risk management framework rests on key pillars of the risk governance architecture, comprehensive processes and internal control mechanisms based on approved policies and guidelines.

The key areas of risk covered under our risk governance architecture include credit, market (including liquidity) and operational risk.


Board of Directors
Committee of Directors (COD)
Audit Commttee of the Board (ACB)
Risk Mangement Committee (RMC)
Executive Risk Management Committee
Credit & Investment Committees
CRO
Respective teams work under these heads of different components of risk

Functional area	Committee
Credit risk	CRMS
Operational risk	ORMS
Market risk, Liquidity risk	ALCO
Subsidiary risk	SGC
Reoutation risk	RRMC
Business continuity risk	BCPMC
Outsourcing rik	COC
Info Security risk	ISSC

The risks are quantified, wherever possible, for effective and continuous monitoring and control.

The risk management processes are guided by well-defined policies appropriate for various risk categories, independent risk oversight and periodic monitoring through the sub-committees of the Board of Directors.

New products and/or changes in products and processes are subject to robust risk management processes.

The Product Management Committee (PMC) reviews and approves new products. The objective of PMC process is to ensure that the new products are introduced as per the laid down process, the risks associated with such products at various stages of its lifecycle have been duly identified, and that the requisite controls have been put in place.

The Change Management Committee (CMC) reviews and approves change in any product and/or any process that might have a bearing on other products, customer base, or on the existing system in place.

We have a Business Continuity Policy (BCP) and an IT Disaster Recovery Policy in place wherein critical activities and system applications have been defined, recovery plan is in place for these critical activities, and system applications to ensure timely recovery of our critical products and services in the event of an emergency.

The BCP framework guides us to safeguard the interest of our clients, protect the life of our employees and minimise losses to our assets.

The Emergency Response Plan (ERP) and Crisis Management Plan (CMP) under the BCP framework are activated during an emergency to minimise losses and strategise the recovery process after disaster.

Our 'Sustainable Lending Policy & Procedures' (SLPP) is designed to supplement the credit risk policies. SLPP, based on international standards, sets the framework to identify and assess the environmental and social risks associated with Project Finance activities of a certain size. We also actively engage with clients to put in place appropriate mitigation plans to address the environmental and social risks identified.

During the year, we have developed a comprehensive 'Vendor Management Framework' (VMF) to address various facets of vendor management. Vendor Risk Assessment is a key component of the VMF.

Scan the QR Code to know more about our Risk Management Practices (Management Discussion & Analysis and Basel III Disclosures sections of the Annual Report 2016-17)

G4-57 Compliance

Compliance with regulatory prescriptions and internal guidelines is very crucial, and we have robust policies and systems in place to guide us in adhering to the highest standards of compliance.

Accountability is set at various levels within the organisation to ensure compliance, with the Audit Committee of the Board, at the apex level, reviewing the status of compliances with the regulatory guidelines on a periodic basis. We use enablers such as dissemination of regulatory changes and percolation of compliance knowledge through training, newsletters, e-learning initiatives and other means of communication apart from direct interaction to continually enhance the compliance culture.

Regular compliance monitoring and testing programmes enable the identification of deviations, evaluation of internal controls and examination of systemic corrections as required. The Enterprise-wide Governance Risk and Compliance Framework is an online tool that is central to addressing operational, compliance and financial reporting risks, bringing efficiency in processes and improvement in compliance levels, besides facilitating an annualised assessment of said risks.

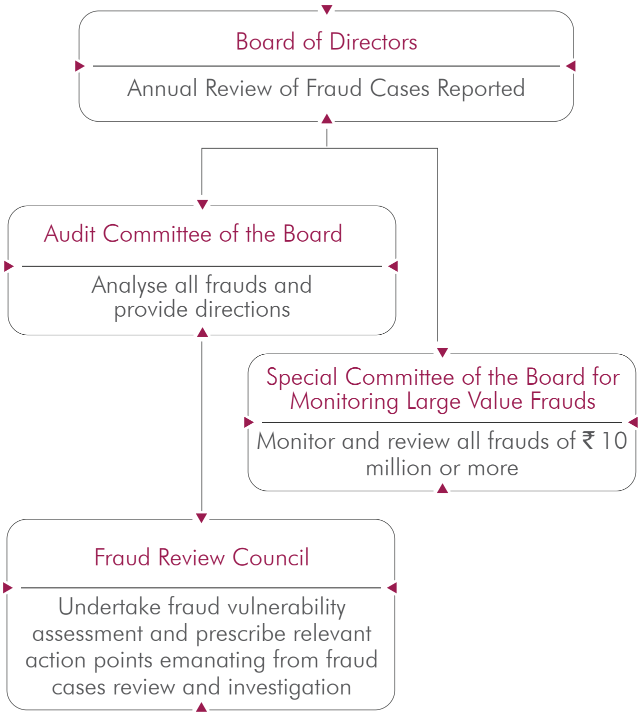
Scan the QR Code to know more about our Compliance Framework (Management Discussion & Analysis section of the Annual Report 2016-17)

G4-58 Fraud Detection and Mitigation

16 PEACE, JUSTICE AND STRONG INSTITUTIONS

We endeavour to create a secure, 'least vulnerable to fraud' environment in the Bank and have adopted a Policy on Fraud Management and Reporting, which serves as a reference document and guidance for the internal oversight and fraud management framework. The Policy is supported by procedures across operations. Round-the-clock transaction monitoring is undertaken to generate alerts in real/near-real-time, to detect fraudulent or suspicious transactions through an Information Technology (IT) enabled system (both online and offline).

We have an enterprise level end-to-end anti-money laundering software system with enhanced functions aiding scenario-based alerts generation from various source data systems for monitoring, investigation and filing of Suspicious Transactions Reports (STRs). A separate fraud management system is deployed for fraud detection and prevention in both credit and debit card


Board of Directors
Annual Review of Fraud Cases Reported
Audit Committee of the Board
Analyse all frauds and provide directions
Special Committee of the Board for Monitoring Large Value Frauds
Monitor and review all frauds of ₹ 10 million or more
Fraud Review Council
Undertake fraud vulnerability assessment and prescribe relevant action points emanating from fraud cases review and investigation

- The employees play a critical role in the detection and prevention of fraud, and we encourage their active participation through our Policy on Recognition and Reward for Detection / Prevention of Fraud.
- Employees are also sensitised and made aware of ethics and prevention of frauds through policy updates, periodic newsletters and employee communications such as 'Ethical Times', 'Due Diligence' and ' Information Security Awareness Series'.
- Information and case studies are disseminated among employees to provide information and insights on frauds detected and actions taken, incident analysis of industry fraud cases and latest regulatory updates.

The employees are also informed on the actions taken for alleged breaches of policies along with representative case studies.

Stakeholder Awareness on Cybercrimes

With the growth of digital adoption amongst the public in general, susceptibility to fall prey to new and innovative cybercrimes is registering a marked increase. We believe that awareness on such cybercrimes has to be created across various sets of stakeholders, including the judiciary and the law enforcement authorities. During the year, we have engaged with these stakeholders through training and awareness sessions to help them understand the changing dynamics of economic offences in the digital banking space. Live case studies were used in the training programmes organised for the officers from police department, working in the areas of economic offences and cybercrime. A special training session on awareness on banking fraud was organized for 'Maharashtra State Judicial Academy',and similar workshop was facilitated for the officials of Economic Offense Wing (EOW), Mumbai.

Awareness session on 'Banking Fraud' organised by Axis Bank functionaries.