RISK GOVERNANCE FRAMEWORK

Focussed on responsible and sustainable growth, the Bank continuously endeavours to maintain effective governance, risk culture and enterprise risk management framework.

As a financial intermediary, the Bank is exposed to various risks, primarily credit risk, market risk, liquidity risk, operational risk, technology risk, cyber risk, third-party risk, compliance risk, legal risk and reputation risk. The Bank is committed to managing material risks and participating in opportunities as part of the strategic approach of risk-calibrated growth in profit before tax excluding treasury. The Board of Directors of the Bank has oversight on all risks in the Bank with specific committees of the Board constituted to facilitate focussed oversight. Most Board-level committees are chaired by Independent Directors and there is adequate representation of Independent Directors on each of these committees. The Board has framed specific mandate for each of these committees. The proceedings and the decision taken by these committees are reported to the Board. The policies approved by the Board of Directors or committees of the Board, from time to time constitute the governing framework within which business activities are undertaken.

Several groups and sub-groups have been constituted to facilitate independent evaluation, monitoring and reporting of risks. These groups function independently of the business groups.

The Risk Management Group is further organised into the Credit Risk Management Group, Market Risk Management Group, Operational Risk Management Group and Financial Crime Prevention Group. The Group is headed by the Chief Risk Officer who reports to the Risk Committee of the Board of Directors. The Bank also has Information Security Group for managing cyber and information security risks.

The roles of specific committees of the Board constituted to facilitate focussed oversight of various risks are:

- **Credit Committee:** Approval of credit proposals as per the authorisation approved by the Board and review of developments in key industrial sectors, non-performing loans, accounts under watch, incremental sanctions, non-fund based exposures, unsecured portfolio, capital market exposures, commercial real estate exposures, retail exposures, exposures to top business groups etc.

- **Audit Committee:** Provides direction to the audit function and monitors the quality of internal and statutory audit; responsibilities include examining the financial statements and auditors' report and overseeing the financial reporting process to ensure fairness, sufficiency and credibility of financial statements.

- **Information Technology Strategy Committee:** Approve strategy for IT and policy documents, review performance with reference to IT & IS Key Risk Indicators (KRIs) and conduct periodic review of KRIs to ensure coverage of IT & IS risks, ensure that the IT strategy is aligned with business strategy, ensure proper balance of IT investments for sustaining the Bank's growth, oversee the aggregate funding of IT at Bank-level, ascertain if the management has resources to ensure the proper management of IT risks, review contribution of IT to business, oversee the activities of Digital Council, review technology from a future readiness perspective, overseeing key projects progress and critical IT systems performance including review of IT capacity requirements and adequacy and effectiveness of Business Continuity Management and Disaster Recovery, review of special IT initiatives, review cyber risk, consider the RBI inspection report/directives received from time to time by the Bank in the areas of information technology and cybersecurity and to review the compliance of various actionables arising out of such reports/directives as may be deemed necessary from time to time and review deployment of skilled resources within Technology and Information Security function so as to ensure effective and efficient deliveries.

- **Risk Committee:** Review risk management policies pertaining to credit, market, liquidity, operational, outsourcing, reputation risks, business continuity plan and disaster recovery plan. The functions of the committee also include setting limits for industry

or country, review the Bank's Enterprise Risk Management Framework, Risk Appetite Framework, Stress Testing Framework, Internal Capital Adequacy Assessment Process and Framework for Capital Allocation. In addition, the Risk Committee reviews risk dashboard covering various risks. The Bank has put in place an Enterprise Risk Management (ERM) and Risk Appetite Framework (RAF) that articulates the risk appetite and drills the same down into a limit framework for various risk categories under which various business lines operate. In addition to the ERM and RAF, portfolio reviews are carried out and presented to the Credit and Risk Committees as per the approved calendar of reviews.

The Internal Capital Adequacy Assessment Process (ICAAP) encompasses capital planning for a four-year time horizon, assessment of material risks and the relationship between risk and capital. Stress testing, which is a key aspect of the ICAAP and the risk management framework, provides an insight on the impact of extreme but plausible scenarios on the Bank's risk profile and capital position.

The Internal Audit Group, being the third line of defence, provides independent assurance that the aforesaid independent groups monitoring the risks in the Bank, are operating in line with policies, regulations and internal standards defined for management of the various risks in the Bank.

The Compliance Group, headed by the Group Chief Compliance Officer, oversees regulatory compliance of the Bank, both at the policy and procedures level and at the level of implementation by the respective groups. The Group has unrestricted access to information within the Bank to assess compliance with the regulatory guidelines.

The Compliance Group and the Internal Audit Group report to the Audit Committee of the Board of Directors. The Group Chief Compliance Officer also reports to the MD & CEO of the Bank. The Risk Management Group reports to the Risk Committee of the Board of Directors. The Risk Management, Compliance and Internal Audit Groups have administrative reporting to the Executive Director responsible for Corporate Centre.

Independent Groups for Monitoring Risks

- Risk Management Group
- Compliance Group
- Internal Audit Group
- Information Security Group

With increasing digitisation, ensuring effective management and governance of data has become a critical business enabler. To further strengthen data quality, data standardisation and governance around data, a Chief Data Officer (CDO) was appointed in fiscal 2023. The role of the CDO includes creating the governance and processes around data generation and processing and compliance with regulations for customer data captured by the Bank. The CDO is also responsible for implementation of the Bank's Data Governance Policy.

CYBERSECURITY GOVERNANCE

Cyber risk management is a key component of the risk management framework. In response to the evolving threat landscape, the Bank has established a dedicated Information Security Group (ISG) responsible for cyber and information risk management.

Cybersecurity has multi-level oversight governance, with the Board of Directors holding ultimate responsibility. Regular updates are provided by the Information Security Group (ISG) of the Bank. Executive Committees, composed of cross-functional members, operate under clearly defined terms of reference and report their proceedings to the IT Strategy Committee.

The Bank maintains a comprehensive suite of policies including the Information Security Policy, Cyber Security Policy and Information Security Standards and Procedures. These are based on global and domestic regulatory frameworks and industry standards, including: RBI Cyber Security Framework, NCIIPC Guidelines for Protection of Critical Information Infrastructure, FFIEC Cybersecurity Assessment Tool, SEBI Cyber Security and

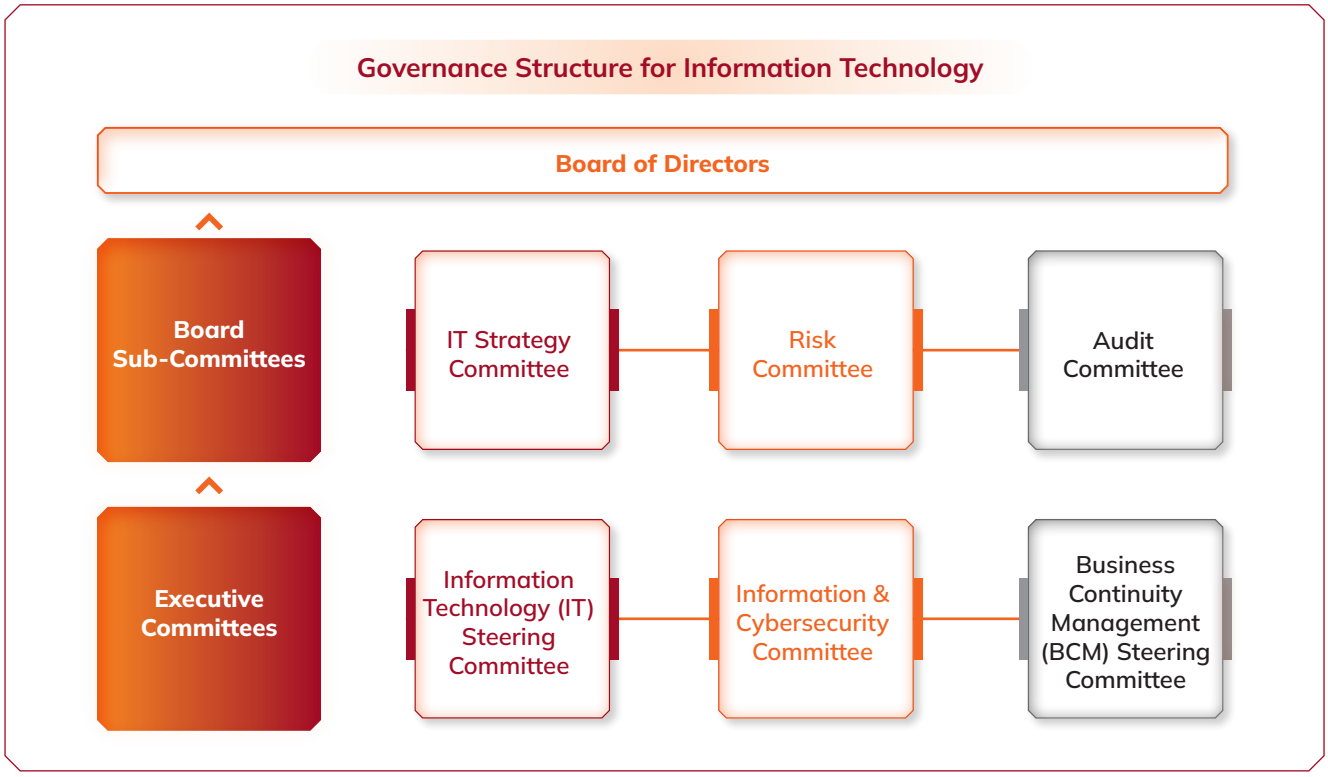
RISK GOVERNANCE FRAMEWORK

Resilience Framework, IRDA Guidelines on Information and Cyber Security, Framework for Reporting of Unusual Cyber Security Incidents, NIST Cybersecurity Framework. In jurisdictions outside India, the Bank also complies with relevant local regulatory requirements.

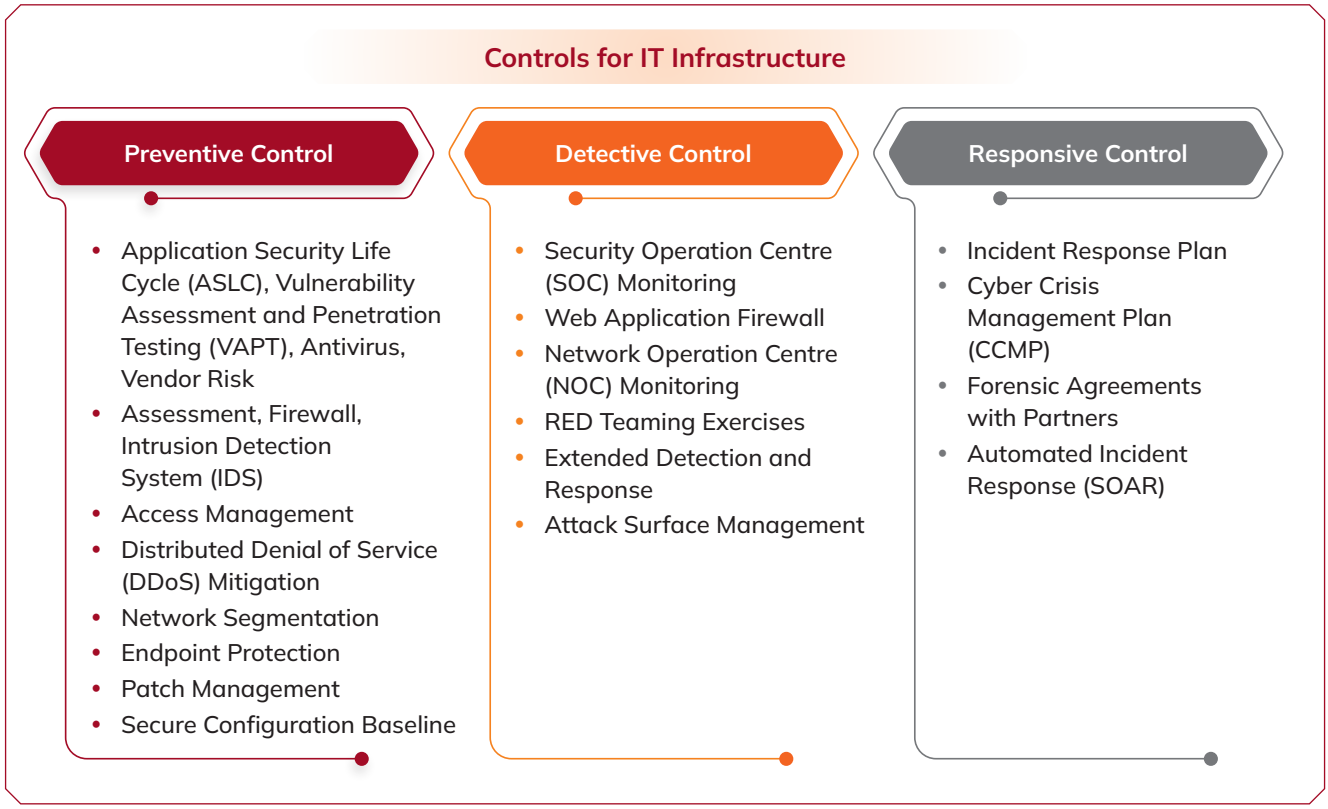
Cyber risk is monitored through multiple Key Risk Indicators (KRIs) and dashboards. A 24x7 Security Operations Centre (SOC) enables real-time monitoring and threat detection, while periodic internal and external audits help strengthen controls.

To safeguard sensitive information, the Bank has implemented a Data Loss Prevention (DLP) system covering endpoints, emails and web gateways. The Bank's Data Centre and SOC are ISO 27001 certified, underscoring our commitment to maintaining enhanced cybersecurity and data protection standards.

Through high-standard of governance, proactive risk management, and a culture of security awareness, the Bank aims to safeguard stakeholder interests and reinforce resilience in an increasingly digital environment.



RISK GOVERNANCE FRAMEWORK



PARTICIPATION IN EXTERNAL CYBERATTACK SIMULATIONS

The Bank places emphasis on continuous preparedness to counter evolving cyber threats. As part of this commitment, the Bank conducts and actively participates in a range of cybersecurity attack simulation exercises, including:

- Spear phishing simulations targeting employees to strengthen user awareness.
- Distributed Denial of Service (DDoS) attack drills involving Internet Service Providers (ISPs).
- Social engineering simulations to test physical security at critical infrastructure sites such as data centres.

These exercises are integral to evaluate the Bank's detection and response capabilities, as well as reinforcing a culture of cyber vigilance across the organisation.

To ensure operational resilience, the Bank regularly conducts Business Continuity Planning (BCP) and Disaster Recovery (DR) drills. These exercises assess the Bank's ability to maintain critical business functions and minimise disruption to people, processes and infrastructure during unforeseen events. The effectiveness of the DR framework is periodically validated against defined Recovery Time Objectives (RTOs).

With rapid digitisation and the increasing sophistication of cyber threats, timely response to incidents is crucial. The Bank has established a dedicated Cybersecurity Incident Response Team (CSIRT) that operates in line with a well-defined Incident Response Plan (IRP). The CSIRT is equipped to respond swiftly and effectively to security incidents, limiting potential impact and ensuring continuity of critical services.

The Bank remains committed to safeguarding customer trust. As such, data protection is treated with the same priority as the quality of banking services delivered. Proactive awareness campaigns are regularly conducted to educate customers on secure practices when using digital channels.

There were no material incidents of security breaches or data loss during fiscal 2025.

ENVIRONMENTAL, SOCIAL AND GOVERNANCE (ESG)

During fiscal 2025, the Bank made steady progress across ESG dimensions, with targeted action towards strengthening practices and reinforcing its journey towards meeting sustainability goals. The Bank focussed on enhancing data management, and enabling more efficient tracking of key metrics, including alignment with disclosure frameworks. The focus was on aligning sustainability actions with the overall business priorities and regulatory expectations. The Risk Committee and the Board reviewed material ESG matters during fiscal 2025, and were provided updates on progress made on ESG-related initiatives at the Bank.

ESG RATINGS

The ESG practices of the Bank are evaluated by external rating agencies like Sustainalytics and MSCI. The ESG score by Sustainalytics improved from 22.5 (Medium Risk category) to 18.9 (Low Risk category) during fiscal 2025 and the rating by MSCI was maintained at A. Based on BRSR and other public disclosures, some SEBI-approved ESG rating providers in India have also started publishing ESG scores/ratings for the Bank. The scores ranged from 69 to 76 on a scale of 100.

ESG Governance

Governance Structure

- **Board of Directors - Annual Update**
- **Risk Committee - Semi Annual Reporting**
- **ESG Steering Committee - Quarterly Meetings**
- **Dedicated Team within CFO's Office Team Tracks ESG and CSR Initiatives**

Overarching Environmental, Social and Governance Policy

- Broad Focus Areas
  - Responsible Financing
  - Environmental Sensitivity in the Bank's Operations
  - Customers
  - Employees
  - Society
  - Corporate Governance
  - Cybersecurity and Data Privacy Governance Framework
  - Stakeholder Engagement and Accountability
- Policy Available on the Bank's Website