

## Responsible behaviour

- 163 Policy overview
- 164 Business ethics and integrity
- 166 Bribery and corruption
- 166 Prevention of money laundering and combating the financing of terrorism
- 168 Fraud
- 169 Whistleblowing
- 170 Customer privacy and information security
- 172 Tax responsibility
- 173 Customer complaints
- 174 Protecting human rights






We recognise that responsible behaviour is central to safeguarding our reputation, earning stakeholder trust and sustaining our long-term success. Our commitment to business ethics and integrity underpins how we work, make decisions and deliver on our purpose.

We embed comprehensive policies and procedures across the Group to ensure compliance with applicable laws, rules and regulations while fostering a culture of professionalism and accountability. We reinforce responsible behaviour through continuous employee training and awareness to help embed ethical considerations into our long-term strategy and day-to-day operations.

Beyond our internal focus, we engage with our customers and communities to promote a broader ecosystem of ethical conduct and resilience. This includes ongoing fraud awareness campaigns as well as providing accessible whistleblowing and complaints-handling channels to uphold transparency and deliver positive outcomes for our stakeholders.

Link to strategic pillars

-  Lead in our Home Markets
-  Build a top-tier African Corporate Investment Banking (CIB) and Private Banking (PB) Institution
-  Win in the Workplace

Principle 10



Principle 3



Alignment with the SDGs, UNGC and UNEP FI PRB



Responsible behaviour

Policy overview

We are committed to conducting business ethically, responsibly and in compliance with all applicable legislation, regulations, adopted industry codes and standards, and adhering to all internal policies and sound corporate governance principles.

Policies applicable to MCB Group		 Read more
 Code of Ethics and Business Conduct embodies our commitment to ethical behaviour, integrity and accountability in all aspects of our business operations.		Page 165
 Whistleblowing Policy provides the framework for stakeholders to raise concerns about potential breaches of laws, rules, regulations or compliance without risk of victimisation, discrimination or disadvantage.		Page 169
 Data Privacy Policy outlines our approach to managing data privacy risk in accordance with the Mauritius Data Protection Act 2017 and the European Union General Data Protection Regulation.		Page 170
 Group Internal Controls Policy establishes a framework to address and mitigate risks, ensure regulatory compliance, and promote operational efficiency within the Group while maintaining a robust system of its internal controls.		Available internally
 Outside Business Activities Policy outlines a detailed approach to the handling of cases where employees engage in outside business activities and establishing a proper mechanism to identify and manage any conflict of interest that this engagement may give rise to.		Available internally
 Anti-Bribery and Corruption Policy outlines our commitment to prohibiting bribery and corruption and confirms our zero-tolerance approach to bribery and corruption.		Page 166
Policies applicable to MCB Ltd		 Read more
 Conflicts of Interest and Related Party Transactions Policy ensures that the personal interests of a director or persons closely associated with a director do not take precedence over those of MCB or its stakeholders, protecting MCB and individuals involved from any impropriety.		Available internally
 Information Security Policy covers information security, information systems, the administration of logical and physical access to information processed and stored, as well as information transmission; it is regularly updated to reflect regulatory requirements and best practices.		Page 170
 Handling of Confidential Information Policy outlines a suitable, effective and sustainable approach to the proper management and use of confidential information and aims to comply with the statutory/regulatory requirements and best practices within the industry. It establishes a common understanding of the appropriate conduct expected of the personnel in respect of the way in which confidential information is to be dealt with at MCB Ltd.		Available internally
 Customer Acceptance Policy sets out the criteria for customer acceptance, with the objective of managing money laundering, terrorist financing and proliferation financing (ML/TF/PF) risk.		Page 166
 Anti-Money Laundering Policy outlines the process of identifying, preventing and managing the risk of ML/TF/PF when providing financial services or products to customers or performing any other activities within the Group.		Page 166
 Financial Promotions Policy ensures that the Bank acts in the best interest of its customers and the general public when advertising its products and services.		Available internally
 Environmental and Social Risk Policy outlines our approach to ensure our exposure to environmental and social risks through our financing activities is identified and managed through adequate risk management framework and standards.		Page 174
 Fraud Policy has been established to facilitate the development of controls to enhance the detection and prevention of fraud against the Bank. This Policy is intended to promote consistent organisational behaviour by providing guidelines and assigning responsibility for the development of controls and the conduct of investigations.		Page 168

Our policies





Policy review and approval process

To uphold business ethics and compliance, we ensure that all required policies are regularly reviewed, approved and effectively communicated to the relevant internal and external stakeholders. Our policies undergo a thorough review process to ensure they

align with current best practices, legal requirements and our strategic and reputational objectives. The review process occurs at various levels depending on the policy's scope and impact:



Internal and external communication

We believe in transparent communication and take required steps to ensure all employees and relevant external stakeholders are informed about our policies.

For our **employees and internal stakeholders**, we use various channels to communicate our policies, such as the company's intranet, internal communication platforms, awareness campaigns and training sessions. Policies relevant to external

stakeholders are shared through public channels such as our corporate website. Where appropriate, we also engage directly with affected parties via dedicated communication channels.

Consistent with this approach, the retirement of policies is communicated internally through the same dedicated channels to ensure clarity and alignment.

Business ethics and integrity

At MCB Group, we recognise that upholding the trust and confidence of our shareholders, customers, employees and communities is a fundamental pillar to our continued success. We foster shared responsibility for business ethics and integrity, ensuring a workplace built on trust, transparency and continuous improvement.



In FY25, the Group made no political donations. The Group received no fines, settlements or penalties relating to ESG incidents or breaches. The Group received no compliance notices or warnings and was not involved in any investigations.

Our Code of Ethics and Business Conduct

Our approach to business ethics and integrity is outlined in our **Code of Ethics and Business Conduct** (the Code), which sets out the principles and standards of conduct we expect from all directors, officers and employees of MCB Group and its subsidiaries, locally and internationally<sup>1</sup>.

The conduct and behaviours outlined in the Code align with our Values and Shared Ways of Working. The Code provides clear guidance on key employee principles, such as compliance with laws and regulations, customer data protection and preventing or managing conflicts of interest. It further sets out our responsibilities towards our clients, shareholders, communities and suppliers, with a view to upholding the organisation's long-term business sustainability.

We reviewed our Code of Ethics and Business Conduct to ensure it remained fit-for-purpose and supported engagement towards the highest levels of fair, lawful and ethical business conduct. We published the revised Code in September 2024.

 Read more about our Values and Shared Ways of Working on page 129



Our Code of Ethics and Business Conduct

Training, monitoring and reinforcement

The Code is reviewed and approved at a minimum on an annual basis by the Board of Directors and published on all Group entity websites. We ensure ongoing awareness of the Code and other associated policies through induction training for new recruits as well as regular tailored sessions for employees, senior management and directors. These sessions are followed by assessments to monitor training effectiveness.

**This year, we strengthened adherence to the Code through targeted awareness campaigns and mandatory training programmes.**

We updated our induction and refresher training e-learning modules on confidentiality to promote ethical behaviour. Confidentiality is a key principle in the Code, and training outlines the legal and ethical standards governing the protection of sensitive information and our duty to safeguard client confidentiality at all times. In FY25, refresher training was assigned to targeted account officers, team leaders, managers and analysts. The induction model was assigned to all new recruits.

**In FY25, 1,062 employees underwent ethics training (FY24: 231 employees).**

**We also introduced indicators to assess the effectiveness of our training programmes and monitor ethical breaches, such as violations of our duty of confidentiality.**


Where breaches are identified, we take appropriate and timely remedial action, including targeted refresher training to reinforce ethical conduct. Our performance indicators are presented to senior management quarterly, along with the corresponding remedial measures.

Consequences of violating the Code

Non-compliance with the Code may have severe consequences for MCB Group and all employees and directors. Where the Group deems it appropriate, disciplinary or preventive actions may be taken to address existing or potential Code violations.

Reporting channels

Open communication of issues and concerns by all without fear of retribution is crucial. Internal and external stakeholders may report concerns to MCB Group's respective subsidiaries via dedicated channels. Concerns may be reported confidentially and anonymously. MCB Group prohibits retaliation for reports or complaints regarding misconduct when made in good faith.

 Read more about our approach to whistleblowing on page 169.

**To deliver on Vision 2030, we embed ethics into decision-making and promoting an ethics-driven culture.**

In FY26, we will conduct an Ethics Awareness Month to promote ethical business practices across the Group and reinforce adherence to the Code. The campaign will include an e-learning module as well as various activities to encourage ongoing reflections on ethical behaviour. Beyond the campaign, we will reinforce data ethics as a key lever for responsible innovation.



Bribery and corruption

MCB has a zero-tolerance approach towards bribery and corruption.

Our **Anti-Bribery and Corruption Policy** strictly prohibits employees from soliciting, accepting or obtaining any form of gratification in the course of business, particularly where this may conflict with the Group's duties to clients, shareholders, business partners, staff or other stakeholders. The policy also expressly forbids any payments or advantages to public officials, including gifts, rewards, discounts or premiums.

The policy sets out clear expectations for integrity-based business practices to prevent improper or illegal conduct and to promote honest and ethical behaviour in the delivery of financial services and other activities across the Group. In addition, the policy provides practical guidance to help staff assess the appropriateness of specific situations and ensure continued compliance with the Group's ethical standards.

Every year, we require our leadership team, designated employees, BU Managers and SBU Heads to submit a gift declaration form. At the same time, we require these employees to confirm that they have read and abide by our Anti-Bribery and Corruption Policy.

No material incidents of bribery or corruption were recorded in FY25.

This year, training on our Anti-Bribery and Corruption Policy formed part of our Anti-Money Laundering / Combating the Financing of Terrorism and Proliferation (AML/CFT) induction module, which was assigned to all new recruits across the Group.

[Read more about our approach to AML/CFT below](#)

In FY26, we will continue to enhance employee awareness and embed anti-bribery and corruption control measures through a dedicated training module for all employees.

Prevention of money laundering and combating the financing of terrorism

We are committed to preventing money laundering and combating the financing of terrorism.

Our **Anti-Money Laundering Policy** is a foundational element of our strategy to combat money laundering, terrorism financing, sanctions evasion and proliferation financing. The policy affirms that the Bank's products and services cannot be used by criminals to launder their illicit proceeds and outlines structured procedures to identify, assess, mitigate and report risks associated with money laundering and related threats. The policy further ensures that the law on money laundering and terrorist financing is met in full, based upon the guidelines issued by the Bank of Mauritius and international regulatory standards, fortifying the Bank's long-term institutional integrity and sustainability.

We periodically review our Anti-Money Laundering Policy to ensure it remains responsive to evolving risks.

Our **Customer Acceptance Policy** sets out the criteria for accepting customers, with the primary objective of managing ML/TF risk that the Group's local and overseas banking subsidiaries may be exposed to when providing banking services. The policy aims to ensure that the Bank and its subsidiaries are not intentionally or unintentionally used for ML/TF. It also helps to identify customers who are likely to pose a high or higher-than-standard ML/TF risk.

Training, monitoring and reinforcement

We regularly review our training material to ensure it reflects relevant regulatory changes as well as emerging risks. The training covers key principles and provisions outlined in our Anti-Money Laundering and Customer Acceptance policies. Training is mandatory and is assigned to all employees, tailored to their specific roles.

This year, we launched AML/CFT training for all Group entities to ensure consistent understanding and application of our AML/CFT policies and procedures. Aligned with global best practices, the training aimed to minimise regulatory risk, strengthen our risk mitigation framework and foster a uniform compliance culture across the Group. Going forward, AML/CFT training for MCB Group employees will be conducted annually, in line with applicable regulatory requirements.

Training undertaken in FY25:

Training programme	Training scope
<b>AML/CFT and Proliferation Financing:</b> introduced employees to the concepts of money laundering, terrorism and proliferation financing and set out essential procedures and controls to mitigate relevant risks.	<i>E-learning module; all MCB Group employees.</i>
<b>Proliferation Financing:</b> covered the legal and regulatory frameworks in place to combat proliferation financing, countries of concern and associated red flags and necessary due diligence.	<i>E-learning module; frontline employees and Compliance, Legal, Internal Audit and Trade Finance Operations teams.</i>
<b>Financial Crime Risk Management (FCRM) alerts:</b> equipped new and existing staff with tools to understand and manage FCRM alerts, including alert definitions and related assessments.	<i>Face-to-face training; account officers.</i>
<b>Suspicious Transactions Reporting:</b> educated employees on how to identify, manage and report suspicious activities that may be linked to money laundering, terrorism financing or other criminal activities.	<i>Face-to-face training; account officers.</i>
<b>Compliance Reviews:</b> provided an overview of the risk-based due diligence required for different customer types and the KYC (Know Your Customer) triggers and expectations when periodically reviewing customer profiles.	<i>Face-to-face training; account officers.</i>
<b>Compliance Risk Management:</b> equipped new and existing staff with tools to understand and manage FCRM alerts (including alert definitions and related assessments) and suspicious transaction reports, as well as how to conduct periodic risk reviews as part of customer due diligence.	<i>Face-to-face training; newly appointed account officers.</i>
<b>Customer Due Diligence/KYC:</b> immersed frontline staff in realistic situations to enhance practical skills and decision-making relative to account opening, customer due diligence and KYC best practices.	<i>E-learning module; customer service representatives.</i>
<b>Compliance and AML/CFT:</b> provided new employees with a comprehensive understanding of MCB's policies and procedures related to preventing and detecting money laundering and terrorist financing. The course covered the scope of AML/CFT regulations, the importance of compliance and the specific roles and responsibilities of employees within the framework.	<i>E-learning module; all MCB Group employees.</i>

In line with Vision 2030, MCB aims to build a top-tier African CIB and PB institution. This includes positioning the Group as a partner for Africa's just transition while delivering bespoke, integrated and competitive solutions for regional clients.

To support this strategy in the year ahead, we will enhance our AML/CFT risk assessment and monitoring procedures to reflect our growth and financing ambitions while reinforcing existing controls. We will also pursue continuous capacity building and awareness to manage increased onboarding requests and transaction monitoring alerts.

Fraud


As we navigate an increasingly complex and evolving digital landscape, fraud prevention is critical to protect the Group’s assets and safeguard the trust and financial well-being of our customers.

Complying with relevant rules and standards in personal and business conduct is the responsibility of every employee. Our **Fraud Policy** outlines our approach to managing compliance risk, defines the responsibilities of employees and management and sets out the controls to enhance fraud detection and prevention. We provide our employees with training and tools to identify, report and prevent all forms of fraud.

We review and update our Fraud Policy annually to ensure it remains appropriate, responsive to prevailing legislation and in line with organisational best practices. This year, we postponed our annual review to FY26 given the leadership change in the Head of Internal Audit, which impacted the validation process.

As outlined in the policy, management is responsible for detecting and preventing fraud, misappropriation and other irregularities. If any internal or external irregularity is suspected or detected, our Fraud Prevention BU investigates and escalates to Executives or other designated personnel, as relevant. We encourage our employees to report any suspected irregularities to our Fraud Prevention BU via our whistleblower mechanism, as affirmed in our Fraud Policy and Whistleblowing Policy.

**In FY25, we investigated 3,634 fraud cases – down from 4,281 cases last year.**


 Read more about our Whistleblowing Policy and reports received via our whistleblower mechanism on the following page.

Training, monitoring and reinforcement

Aligned with **International Fraud Awareness Week**, our Fraud Prevention BU organised a series of events this year to deepen our employees’ collective knowledge and equip our teams with tools to combat fraud effectively.

We hosted **exclusive training sessions with Professor Mario DiFiore**, Assistant Dean at the Gabelli School of Business, with experience at New York’s Federal Reserve Bank and as the Director of Compliance and Risk Training at Deutsche Bank AG. These sessions provided valuable insights into how to detect and mitigate fraud.

Our Fraud Prevention BU also conducted a **targeted awareness campaign** to empower our employees to act responsibly in the face of heightened fraud risks. We conducted the campaign via our online learning platform Percipio – reaching 2,797 employees across Mauritius, Rodrigues, Maldives and Seychelles. To boost accessibility, we also conducted a campaign in French for MCB Madagascar and reached a further 243 employees.

 Read more about our online learning platforms on page 135.

Our Fraud Prevention BU conducted a **Fraud Awareness Roadshow**, targeting employees from our retail network. The initiative aimed to improve knowledge and understanding of fraud prevention and equip our teams with the latest fraud prevention strategies. Our Fraud Prevention BU hosted six in-person awareness sessions between July 2024 and February 2025, reaching employees from MCB Madagascar, MCB Rodrigues and representatives from Business Banking and our Security and Payment Operations Business Unit SBUs – significantly enhancing our collective fraud prevention capabilities.

We published articles to raise awareness about **fraud among our customers and the wider community**, focusing on the different types of fraud, how to detect and prevent fraud and the steps to take if they suspect they may be a victim.

In addition, we continued to regularly advise our clients on fraud prevention via a **dedicated Security Centre** on the Group’s website. This resource helps customers understand common threats, including cybercrime. It provides tips to detect scams as well as clear guidance on how to report suspected fraud. We continue to closely monitor any applications or requests associated with or suspected of fraudulent activity.



Additional information is available at

For more information, follow us on TikTok



**In FY25, we conducted a total of 11 training sessions focusing on anti-bribery and anti-corruption, fraud prevention and anti-money laundering, reaching 5,721 employees (FY24: 10 sessions, reaching 389 employees).**

Whistleblowing

We strive to maintain the highest standards of professionalism and ethical conduct across all our operations.

Our **Whistleblowing Policy** establishes a framework to ensure that employees and other relevant stakeholders can report concerns safely and securely, without fear of victimisation, retaliation, discrimination or any form of disadvantage.

The policy is supported by an online reporting mechanism, which is managed by the Compliance SBU. We encourage individuals to raise genuine concerns via this mechanism.

We continue to strengthen protection for whistleblowers to ensure that employees who raise concerns in good faith face no adverse consequences. Where necessary, an independent panel investigates reported incidents and escalates findings to the Audit Committee for appropriate remedial action.



**Speak Up! We will listen to you.**

**Our whistleblower mechanism is available at**



Training, monitoring and reinforcement

In line with the requirements of our Whistleblowing Policy, we conduct periodic employee training and awareness on the policy’s provisions and procedures. This year, training on our Whistleblowing Policy formed part of our AML/CFT induction module, which was assigned to all new recruits across the Group.

Reports received

For the year ending 30 June 2025:



**In FY26, we will implement a dedicated training module for all employees to strengthen employee awareness on our Whistleblowing policy and reinforce the importance of relevant reporting and control measures.**

<sup>a</sup> The number includes transactions whose investigations started in FY24 but were concluded and filed in FY25 due to an extended review timeline.

<sup>b</sup> Corresponds to the number of transactions received through our main channels: Internet Banking, Juice and e-commerce.

Customer privacy and information security

Customer privacy is a material topic for MCB Group due to the highly sensitive nature of the personal and financial data that we handle in our role as a banking and financial services institution.

MCB Group places utmost priority on the confidentiality, integrity and availability of information. We are committed to protecting the privacy and security of personal and financial data belonging to our customers, employees and stakeholders. As a leader in the banking and financial services industry, we acknowledge that data privacy is fundamental to maintaining trust and complying with evolving legal and regulatory standards.

Data Privacy Policy and Framework

We are committed to maintaining a consistent data privacy framework across the organisation. We updated our **Data Privacy Policy** in March 2025 during the Group’s annual policy review to reflect current regulatory requirements, align with best practices and extend the policy to MCB Group Ltd and all its subsidiaries. This overarching policy is accessible internally to all employees. Our approach to governing data protection and processing is available on our website.

Our Data Privacy Policy is aligned with the **Mauritius Data Protection Act 2017 (DPA) and the European Union General Data Protection Regulation (GDPR)**. It applies to all MCB employees and contractors who handle personal data in any form – paper or electronic. The policy covers data related to past, present and prospective employees, customers, suppliers, business partners, contractors, sub-contractors and any third parties.



Our approach is clearly outlined on our website:

Data subject rights

MCB is committed to safeguarding customer data and upholding their rights under the DPA and GDPR, including:

- **Right to be Informed:** Individuals are notified through clear and concise privacy notices regarding the purpose, use, processing and retention of their personal data.
- **Right of Access:** Individuals can request access to their personal data and related information. Requests must be addressed within one month, extendable by an additional month based on complexity. All requests follow MCB’s established Right to Access procedure. The Data Protection Officer (DPO) may reject excessive or unfounded requests.
- **Right to Rectification:** Inaccurate or incomplete personal data must be corrected without delay. This is integrated into MCB’s routine business processes.
- **Right to Erasure** (“Right to be Forgotten”): Under specific conditions, individuals can request data deletion. These include cases where the data is no longer needed, has been processed unlawfully or where retention is no longer legally required.
- **Right to Restrict Processing:** Individuals may request restriction of processing under circumstances such as:
  - Unlawful processing, where the individual prefers restriction over deletion.
  - Data no longer needed by MCB but retained for legal reasons.
  - Ongoing objections.
  - Accuracy disputes.
- **Right to Object:** Individuals may object to the processing of their personal data for:
  - Legitimate interests purposes.
  - Direct marketing purposes.
  - Scientific, historical, or statistical purposes.
- **Rights Related to Automated Decision-Making:** Where decisions are made solely by automated means that significantly impact individuals, MCB provides data subjects with the right to challenge the decision and provide a mechanism to obtain human intervention.

An internal procedure is in place to ensure all these rights are supported and upheld, with oversight from the DPO.

Governance and oversight

A **Cyber and Technology Risk Committee (CTRC)** has been established, with the mandate to, amongst other things, ensure compliance with all applicable laws and regulations relevant to cyber, information and technology risks, including, but not limited to, the Data Protection Act (2017) and the Guideline on Cyber and Technology Risk Management issued by the Bank of Mauritius.

The CTRC is a joint committee comprising of the Board of Directors of MCB Ltd and MCB Group Ltd. The committee’s responsibilities and governance framework are outlined in the ‘Cyber and Technology Risk Committee Charter’ that is publicly available on MCB’s website.



Access the Cyber and Technology Risk Committee Charter at

Data breach management

MCB has a formal **Data Breach Management Process** to identify, respond to and monitor breaches promptly within the timeframe prescribed. This includes escalation protocols, notification procedures to supervisory authorities and affected data subjects. The process includes proactive and reactive measures and follows the personal data breach guidelines specified in the DPA 2017.

During FY25, three breaches were reported to the Data Protection Office. These incidents were promptly contained and eliminated and had minimal to no adverse effects on data subject rights.

MCB’s Three Lines of Defence for data privacy and cybersecurity

Our cybersecurity and data privacy framework is supported by a robust governance model consisting of three lines of defence:

- **First Line:** Our **Information Security BU** is responsible for our security operations, incident response, threat intelligence and disaster recovery.
- **Second Line:** The **Cyber and Information Security (CIS) BU** is responsible for risk management, setting policies and security governance principles and providing oversight of the activities of our Information Security BU (including ensuring compliance with security practices, requirements and regulations).
- **Third Line:** Independent audits are conducted by both MCB’s **Internal Audit** team and an **external assurance** provider, who assess the resilience and effectiveness of our policies and systems annually.

MCB Group continuously enhances its cybersecurity controls and maintains robust incident response plans.

The following plans are in place, regularly tested and adjusted (including simulation testing):

- Cyber Incident Response Plan
- Disaster Recovery Plan
- Business Continuity Plan
- Crisis Management Plan

We ensure that our customers have clear access, control and protection over their personal data.

In addition to a secure login password, we provide additional security measures to limit unauthorised account access. These measures include, for example, a highly secure automatically-generated one-time password (OTP). In addition, our security measures are underpinned by secure technology such as encryption, firewall mechanisms, temporary access denial and automatic timeouts.



We provide a detailed breakdown of the security mechanisms we have in place for our customers on our website:

We do not rent, sell or provide personal data to third parties for any purpose other than completing required transactions and/or services.

We actively minimise our data collection and retention.

At MCB Ltd, we follow the principle of deleting (or anonymising) personal information after the stated periods defined in associated policies. Our approach aligns with the requirements of the Mauritius Data Protection Act 2017 and the European Union General Data Protection Regulation. MCB adheres to the principle of data minimisation and ensures that only the personal data necessary for the stated purposes is collected, used and retained only as long as necessary.



Employee training and awareness

We conduct regular employee training and awareness sessions on data privacy and security issues.

Ongoing employee training is a key component of our data privacy culture. Training is delivered via the KnowBe4 platform, which offers more than 600 courses on cybersecurity, compliance and fraud prevention, amongst others. Training is mandatory for specific employees and business units. The CIS BU is responsible for ensuring that employees remain informed and compliant with current data privacy practices and regulations.

The security awareness training undertaken during FY25 covered a wide range of topics, including cybersecurity hygiene, data privacy and protection, policy awareness, as well as practices to detect and respond to social engineering attempts. All Group employees (including directors) received training.

Tax responsibility

Our approach to tax emphasises ethical and responsible behaviour, and we continue to uphold a consistent tax framework grounded in transparency, compliance and effective risk management.

We comply with all local legislations by continuously reinforcing existing controls, processes and reporting. The Group's risk management and internal control framework ensures we adequately manage tax risks while ensuring compliance with established internal policies and procedures and relevant laws and regulations. We promptly handle any assessments raised by tax authorities with due escalation to the Board via the Audit Committee.

To support this, the relevant teams across our organisation regularly attend trainings and seminars on tax and participate in various tax forums. We also seek assistance from independent local and international tax advisers to address complex or high-risk tax matters.

The Bank's external auditors review our tax computations and tax disclosures, during which we provide supplementary information or clarification as required.

We keep up to date with any developments in tax legislation and integrate these changes into our tax strategy while ensuring tax optimisation.

Tax paid by the Group banking subsidiaries for the year ended 30 June 2025:

	FY23	FY24	FY25
MCB Ltd <sup>a</sup>	Rs 2,277 m	Rs 4,890 m	Rs 5,247 m
MCB Madagascar	Rs 84 m	Rs 87 m	Rs 112 m
MCB Maldives	Rs 64 m	Rs 91 m	Rs 113 m
MCB Seychelles <sup>b</sup>	Rs 184 m	Rs 419 m <sup>4</sup>	Rs 250 m

Responding to evolving tax and regulatory requirements

In the Budget 2025-2026, the Mauritian government introduced a series of significant tax measures impacting the financial services sector, particularly banks.

These measures included new contributions on chargeable income and Segment A profits, adjustments to levy payable by banks previously capped, the withdrawal of certain longstanding tax incentives and an expansion of VAT obligations related to foreign digital service providers. Other measures included a requirement to settle certain income taxes in foreign currency for transactions with non-residents and Global Business Companies<sup>1</sup> (as far as banks are concerned), as well as the implementation of the OECD Pillar Two framework through a Qualified Domestic Minimum Top-Up Tax<sup>2</sup>, which further aligns Mauritius with international tax standards.

Looking ahead to FY26 and beyond, we will continue to strengthen our approach to tax, ensuring robust governance, transparency and alignment with international best practices.

We will enhance our tax risk management frameworks to address increasing complexity and evolving regulatory developments, including the implementation of the OECD Pillar Two framework in Mauritius. In parallel, we are further evaluating the digitalisation of our tax processes to further improve compliance efficiency, data accuracy and reporting capabilities.

<sup>a</sup> Tax paid for MCB Ltd in FY 2025 includes corporate income tax, corporate climate responsibility levy, corporate social responsibility, VAT, and special levy.  
<sup>b</sup> Figures have been restated for MCB Seychelles.  
<sup>1</sup> Global Business Companies (GBCs) are a form of business entity that are incorporated in Mauritius but specifically designed for international trade and investment.  
<sup>2</sup> The OECD Pillar Two framework introduced a global minimum effective tax rate of 15%, with the Qualified Domestic Minimum Top-up Tax allowing countries to collect additional taxes locally to meet this threshold. The OECD Pillar Two framework was formally agreed upon by OECD/G20 countries in October 2021 and began to take effect in various jurisdictions around the world in 2024.

Customer complaints

We are committed to maintaining a robust complaints management process as a cornerstone of our efforts to elevate service quality and deliver an exceptional customer experience.

Our dedicated complaints management team works closely with all stakeholders to ensure our framework remains fair, transparent and aligned with industry best practices. Key focus areas include:

- 1. Strengthening strategies to design and deliver intuitive, adaptable and tailored customer service solutions across multiple channels to improve employee and customer experience.
- 2. Enhancing our existing feedback channels, sharing trend analysis insights and providing targeted technical and interpersonal skills training.
- 3. Embedding a consultative complaints handling approach across the Group, including reviewing and refining the complaints handling framework to ensure ongoing effectiveness and regulatory compliance.

We provide multiple online, traditional and in-person channels for receiving and handling customer complaints. These include our Contact Centre, our extensive branch network and our Group website, which offers clear guidance on filing a complaint as well as transparency on the complaints escalation process.



More information is available at:

This year, to enhance customer complaints management, we launched a comprehensive, Group-wide complaints training programme through our online learning platform. Additionally, we assessed a new complaints management system to further strengthen our customer complaints handling process and implemented several automation initiatives to enhance operational efficiency and enable seamless service delivery.

For the year ending 30 June 2025:



In FY25, the Group continued to proactively reduce complaint volumes by driving continuous process improvements and elevating service delivery standards. We recorded a slight decrease in the share of complaints resolved within 5 days or less for MCB Ltd due to an increase in complex complaints (e.g. fraud cases, card issues and payment recalls), where investigations typically take longer.




In FY26, we will focus on reducing complaint resolution times and complaint volumes to uphold customer excellence. We will also explore opportunities to strengthen collaboration with our internal partners to promptly address issues, streamline processes and ensure efficient workflows.

Protecting human rights

We are committed to protecting human rights throughout our value chain by integrating potential business-related human rights risks into our operational and business activities.


These human rights risks include, among others, forced labour, freedom of association and collective bargaining, fair remuneration, equality and non-discrimination, data privacy, health and safety and environmental and social sustainability. To strengthen our approach, we comply with the Ten Principles of the UNGC<sup>30</sup>, demonstrating

our commitment to safeguarding human rights in our labour practices, business partnerships and supply chain practices. To mitigate potential human rights risks, we also engage with key stakeholders at all levels, including employees, customers, suppliers and the communities we serve.

Our people	<ul style="list-style-type: none"><li>• We provide a <b>healthy and safe working environment</b> and ensure compliance with internal policies, rules and applicable regulations, such as the Workers’ Rights Act 2019 (Mauritius).</li><li>• Our <b>Code of Ethics and Business Conduct</b> guides our approach to labour relations, including ensuring respect for the right to freedom of association and collective bargaining.</li><li>• We promote <b>diversity and inclusion</b>, including gender equality, and implement a <b>fair and robust</b> remuneration philosophy to reward employees.</li><li>• As outlined in our Grievance Policy, employees have the right to make use of our <b>grievance procedure</b> to ensure all grievances are settled quickly and fairly.</li></ul> <p> Read more about our approach to supporting individual and collective well-being on page 126.</p>
Our customers	<ul style="list-style-type: none"><li>• Our <b>Environmental and Social Risk Policy</b> provides guidance to identify and manage human rights risks in our financing activities, including outlining our commitment to avoid any risk of being associated with any form of forced labour, including modern slavery and human trafficking, through our business activities.</li><li>• As a signatory to the <b>Equator Principles</b>, we evaluate our portfolio against criteria relating to human rights. We further apply leading international environmental and social risk management practices in line with the <b>IFC Performance Standards</b> and the <b>World Bank’s Environment, Health and Safety Guidelines</b>.</li></ul> <p> Read more about our approach to managing environmental and social risks on page 50.</p>
Our suppliers	<ul style="list-style-type: none"><li>• When selecting and working with suppliers, we consider human rights aspects, and we also undertake <b>supplier due diligence</b> according to applicable regulations.</li></ul> <p> Read more about our approach to procurement and supplier engagement on page 86.</p>

To further reinforce our commitment to protecting human rights, our whistleblower mechanism provides internal and external stakeholders with a confidential platform to report human rights risks, concerns or incidents. This system safeguards the identities of whistleblowers and all involved parties.

In FY25, no reports or incidents were identified concerning human trafficking, child labour, forced labour or violations of the right to freedom of association or collective bargaining, either within our operations or our supply chain.

 Read more about our approach to whistleblowing on page 169.

<sup>30</sup> The UNGC principles were founded on the Universal Declaration of Human Rights, the International Labour Organisation’s Declaration on Fundamental Principles and Rights at Work, the Rio Declaration on Environment and Development, and the United Nations Convention Against Corruption.

Our overseas banking subsidiaries undertook various actions to strengthen their internal controls and embed business ethics and integrity

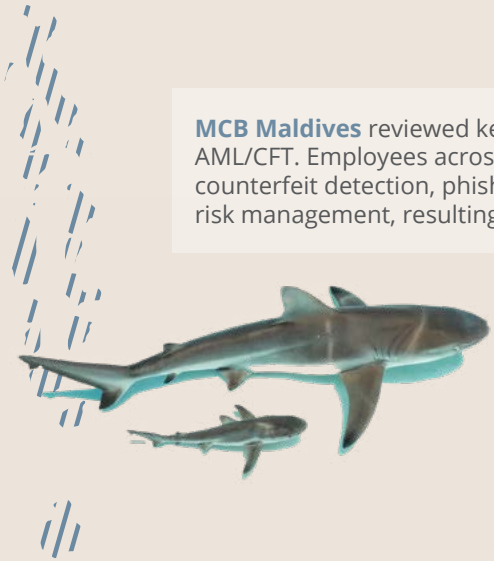
Our overseas banking subsidiaries reinforced responsible behaviour through employee training and awareness and engaged with customers and communities to promote fraud awareness



**MCB Seychelles** provided all employees with training on AML/CFT, focusing on best practice prevention and detection to counter AML/ CFT, bribery and corruption. In addition, all new recruits participated in introductory AML/CFT training. Leveraging our KnowBe4 platform, the Bank also launched complaint-handling awareness training and AI security awareness training.

MCB Seychelles remains a member of the Seychelles Bankers Association and plays an active role in promoting community fraud awareness. This year, the Bank’s senior management team led campaigns with schools, elderly groups and customers on fraud awareness and financial management. Initiatives included media sensitisation sessions to improve public information on fraud, district-level awareness programmes for the elderly, and the launch of a national School Scams and Fraud Poster Competition with the Central Bank of Seychelles and the Ministry of Education, aimed at primary school students. The Bank also broadened its public outreach through social media campaigns and radio announcements, raising awareness on fraud and providing guidance on the steps to take if they have been victims of fraud.

**MCB Madagascar** reviewed its Anti-Corruption, Fraud, AML/CFT and Whistleblowing policies, alongside targeted awareness campaigns and training. Employees were reminded of their obligations on gift declarations, suspicious transaction reporting, adherence to the Code of Conduct and the procedures and controls related to whistleblowing. Awareness sessions and e-learning modules on AML/CFT achieved full participation, helping staff strengthen vigilance and apply best practices in their day-to-day responsibilities. In addition, the Bank enhanced its risk management tools and processes, tailored to the local context. Awareness initiatives at the Bank’s head office and various branches contributed to increased incident reporting and a stronger risk culture. Fraud prevention and detection were reinforced through fraud scenarios and risk assessments.



**MCB Maldives** reviewed key compliance policies, including anti-bribery, fraud prevention and AML/CFT. Employees across the Bank benefited from targeted programmes on topics such as counterfeit detection, phishing awareness, AI, account-opening due diligence and financial crime risk management, resulting in stronger internal controls and employee awareness.