GOVERNANCE

The Manager prioritises ethical conduct and compliance with relevant laws and regulations to safeguard its sustainability goals by adopting a zero-tolerance stance against corruption and unethical practices. This approach ensures transparency, fairness, and stakeholder trust, which are vital for MIT's long-term success and generate positive impact on the society and the economy. This pillar focuses on two key topics – **Ethical Business Conduct and Regulatory Compliance** and **Cybersecurity and Data Privacy**.

Ethical Business Conduct and Regulatory Compliance

Zero
incidents of non-compliance with anti-corruption laws and regulations

Zero
material incidents of non-compliance with relevant laws and regulations

Cybersecurity and Data Privacy

Zero
cybersecurity incidents resulting in material business interruption or data leaks

Group-wide
cybersecurity training
for employees

ETHICAL BUSINESS CONDUCT AND REGULATORY COMPLIANCE

Why is this important? 3-3

Corruption undermines MIT's sustainability efforts by compromising transparency, fairness, and accountability. It hinders opportunities for deserving individuals, stifles economic growth, and leads to negative environmental and social outcomes over time.

To address this, the Manager is committed to upholding the highest standards of ethical business conduct and integrity. This commitment includes a zero-tolerance policy towards unethical practices such as corruption, bribery, fraud, and anti-competitive behaviour. Maintaining these standards is essential for preserving stakeholder trust, which is crucial for the long-term sustainability of MIT's business operations.

Management approach 3-3 205-1

The Manager is committed to conducting business ethically and in compliance with relevant laws and regulations, such as the Securities and Futures Act, the Listing Manual of SGX-ST, the Code on Collective Investment Schemes, the Singapore Code on Takeovers and Mergers, and the Trust Deed.

The Manager is vigilant against the risk of corruption. To mitigate this risk effectively, the Mapletree Group has in place a comprehensive framework of policies and procedures. These measures include stringent guidelines on procurement practices, gift giving and entertainment, securities trading, code of conduct, whistle-blowing, contract review, and anti-money laundering checks on tenants. It also has in place training and communication protocols to ensure employees remain well-informed about the latest developments and updates in relevant laws and regulations. These policies and procedures are communicated to employees and made accessible via the Mapletree Group's intranet.

Code of conduct and discipline

Ensuring a safe work environment free from discrimination, harassment, and abusive behaviour is a priority for the Manager. This commitment is codified in the Code of Conduct and Discipline in the Employee Handbook, which outlines the rules for all employees to perform their responsibilities to the highest standards of personal and corporate integrity in the workplace. The Manager strives to create a safe and healthy work environment not only for its employees but also for tenants, business partners, and visitors. The Code of Conduct and Discipline is accessible to all employees via the Sponsor's intranet.

Anti-corruption 205-1 205-2 205-3

Fraud and corruption are among the key risks assessed across all operations in MIT's Enterprise Risk Management Framework. The Mapletree Group adopts a zero-tolerance stance against bribery and corruption as it recognises that such risks could lead to significant financial and reputational implications to the organisation.

Employees are required to comply with the Sponsor's anti-corruption policies and procedures as outlined in the Employee Handbook. It also includes specific guidance on anti-corruption practices, including prohibitions on bribery and the acceptance or offering of extravagant gifts and entertainment. Failure to comply with these policies may result in disciplinary action.

The Sponsor organises training courses to foster a culture of strong business ethics and governance. These sessions aim to educate employees about the risks and consequences associated with non-compliance and corruption. They cover essential ethical policies, including gift exchange, anti-corruption measures, whistle-blowing, and insider trading. All employees and the Board of Directors are required to complete anti-corruption training during their onboarding process. During the financial year, the Mapletree Group also launched three mandatory e-learning modules on "Anti-Bribery and Corruption", "Introduction to Compliance, Whistle-blowing and Market Misconduct" and "Anti-money Laundering and Countering of Terrorism Financing and Sanctions" for all employees. Directors were encouraged to receive refresher training on anti-corruption, with 100% of directors completing the "Anti-Bribery and Corruption" e-learning module in FY24/25.

In FY24/25, 100% of new hires received communication and training on anti-corruption knowledge. 99% of the employees of the Manager and Property Manager attended trainings on anti-corruption in FY24/25. Material updates on policies and procedures relating to anti-corruption were promptly communicated to the Board of Directors and employees.

Employees must also declare any potential conflicts of interest arising from outside directorship appointments, participation in external engagements, and personal relationships among employees. The Mapletree Group will review and determine whether a conflict of interest exists and redeploy any employees where necessary. These are emphasised under the Code of Conduct and Discipline, which is accessible to all employees via the Sponsor's intranet. Anti-corruption policies and procedures are also communicated to business partners across all regions of operations. The Sponsor also has anti-bribery provisions in its General Terms and Conditions of Purchase (available on its website) as well as its Supplier Code of Conduct, which is being progressively rolled out across the Mapletree Group.

In FY24/25, there were no incidents of non-compliance with anti-corruption laws and regulations.

Whistle-blowing 2-16 2-25 2-26

The Manager has a whistle-blowing policy that allows internal and external stakeholders to report illegal, unethical, or inappropriate behaviour in the workplace. This policy protects whistle-blowers from reprisals and victimisation. Rigorous confidentiality protocols have been put in place to guarantee anonymity and protect whistle-blowers from any form of retaliation or victimisation. Reports can be made via a dedicated email address (reporting@mapletree.com.sg). All reported cases are escalated to the AC Chairman of the Sponsor and the AC Chairman of the Manager for investigation. The findings are reported to the AC of the Manager for deliberation. Employees found guilty of fraud, dishonesty, or criminal conduct in relation to their employment will face appropriate disciplinary action.

Please refer to page 97 in the Corporate Governance section of the Annual Report for further information.

Compliance with laws and regulations 2-27 416-2 417-3 418-1

The Mapletree Group is committed to complying with the applicable laws and regulations in all jurisdictions where it operates. It recognises the significant risks associated with non-compliance to legislations, including potential operational disruptions, legal disputes, revocation of license to operate, financial penalties, and reputational damage. To this end, the Manager prioritises compliance with relevant laws and regulations in conducting its business, ensuring that negative environmental impacts are reduced, and human rights are respected.

The Manager upholds high standards of corporate governance through a comprehensive group-wide Corporate Governance Framework, which provides clear guidance on regulatory compliance, anti-corruption measures, and risk management for all employees.

In response to the MAS Guidelines on Environmental Risk Management for Asset Managers, the Manager integrates environmental risk considerations into its investment decision-making process. This approach helps enhance sustainability performance and strengthen the climate resilience of MIT's portfolio.

Directors and employees are kept informed about relevant legal and regulatory updates through regular training and communication. In the event of any threatened or pending litigation, the CEO of the Manager and the Mapletree Group CCO are notified immediately to facilitate a prompt resolution.

For more details on the Manager's control measures for the assessment and management of its financial, operational and compliance risks, please refer to the Corporate Governance Framework and Enterprise Risk Management Framework, found in the following sections in the Annual Report:

- Corporate Governance, pages 83 to 104
- Risk Management, pages 105 to 107

In FY24/25, there were no material breaches of applicable local laws and regulations, including anti-corruption, health and safety impact of products and services, marketing communications, customer privacy and data and socio-economic and environmental laws and regulations.

Responsible marketing and communication 417-3

Transparent and responsible marketing and communication are key to establishing trust between stakeholders and MIT. All marketing and investor relations materials are reviewed to ensure accuracy, consistency, and legal compliance. These materials are guided by the Singapore Code of Advertising Practice and adhered to the Personal Data Protection Act. Tenants are also required to abide by relevant laws and regulations governing marketing communications and advertisement placements within MIT's properties.

The Manager prioritises timely and transparent communication with MIT's Unitholders. Public announcements are promptly published via SGXNET and MIT's website. The Manager maintains regular engagement with Unitholders through various channels, such as annual general meetings, bi-annual results webcasts, and investor presentation slides.

Anti-money laundering and countering the financing of terrorism

As a holder of a Capital Markets Services License issued by MAS, the Manager adheres to MAS guidelines on the prevention of money laundering and countering the financing of terrorism. The Mapletree Group has in place an anti-money laundering policy that guides employees in conducting anti-money laundering checks on upcoming acquisitions and prospective tenant leases exceeding a specified monetary threshold.

All necessary steps are duly carried out prior to the signing of a new lease and upon lease renewals. Refresher checks are conducted every two years for all existing leases. In addition, all suspicious transactions are reported to the Suspicious Transaction Reporting Office of the Commercial Affairs Department.

CYBERSECURITY AND DATA PRIVACY

Why is this important? 3-3

Digital technology plays a vital role in the Manager's daily operations, especially when handling extensive data relating to employees, tenants, and financial matters. This data is susceptible to cyberattacks, and any breach could lead to significant financial losses, reputational harm, legal challenges, and operational disruptions. Therefore, robust security measures are critical to safeguard sensitive information, protect individuals' privacy, and preserve stakeholder trust.

Management approach 3-3 418-1

The Mapletree Group has implemented robust Information Technology ("IT") policies and procedures to strengthen data protection. These measures include an annual IT disaster recovery plan, vulnerability and penetration tests by external specialists, and internal audits of IT controls. All software and systems are regularly updated with the latest security patches to protect against known vulnerabilities. To minimise the risk of unauthorised access to sensitive data and maintain system security, strict access controls are enforced. The Mapletree Group also regularly reviews its cybersecurity policies and data protection measures to ensure their effectiveness and relevance. The organisation also invests in the latest cybersecurity technologies to enhance its defence against cyber threats. By conducting these activities, the Mapletree Group can identify cyber risks and apply effective mitigation strategies.

To enhance awareness of phishing and malware threats, the Mapletree Group rolled out a series of communications to educate employees on the risk of cyberattacks. Furthermore, all employees were required to complete an online phishing security awareness course during the financial year. Company-wide email phishing exercises were conducted in May 2024, August 2024, January 2025, and March 2025 to assess response capabilities and enhance overall email security.

The Mapletree Group maintains a comprehensive Privacy Statement governing the responsible collection, use and disclosure and safeguarding of personal data across all touchpoints. Personal data is collected only when voluntarily provided and is used solely for specified purposes such as customer service and marketing communications. The Mapletree Group does not disclose personal data to unrelated third parties unless required by law or expressly consented to by the individual. Individuals have the right to access or amend their personal data and may withdraw their consent at any time. These requests are handled by a designated Data Protection Officer. Access to personal data is restricted to authorised personnel who are bound by strict confidentiality obligations. The Mapletree Group implements robust technical and organisational measures to safeguard personal data against unauthorised access, loss, misuse, or alteration.

The Manager ensures strict compliance with the Personal Data Protection Act and regularly reviews its policies to align with evolving legal and regulatory requirements. The full Privacy Statement is available on MIT's corporate website, and stakeholders may contact a Data Protection Officer via the dedicated emaill address provided online.

In FY24/25, there were no cybersecurity incidents resulting in material business interruption or data leaks.

Vendor risk management

The Mapletree Group has a structured approach to vendor risk management, which is crucial given the reliance on third-party service providers who have access to the organisation's systems and data.

Onboarding

- Undertake rigorous assessment on potential risks associated with vendors before granting them access to systems and data
- Include evaluation of vendor qualifications, criticality of service and contractual agreements as well as setting of security and compliance requirements

Oversight

- Continuous monitoring and regular review of vendor services
- Include performance evaluations and periodic audits to ensure compliance with industry regulations and organisational policies

Offboarding

- Ensure a secure and smooth termination while minimising risks
- Include revoking all vendor access to systems, data and resources, and ensuring proper data handling

Cybersecurity incident management

The Mapletree Group has a systematic approach to effectively detect, respond to, and recover from cyber threats.

1

Preparation

- Institute roles, responsibilities, communication protocols and escalation paths for handling incidents
- Establish an Incident Response Team to respond to cybersecurity incidents effectively
- Implement advanced monitoring and detection systems to identify threats early

2

Detection and Analysis

- Use network, application and security monitoring tools to identify unusual activities
- Notifications from systems and users to detect anomalies in user behaviour or network traffic
- Establish clear reporting channels and ensure thorough incident documentation
- Determine the extent and reach of the damage caused by the incident

3

Containment and Eradication

- Immediately disconnect compromised systems from the network and stop malicious process or unauthorised activities on affected devices (short-term containment)
- Apply temporary solutions to restore functionality while ensuring the threat is neutralised (long-term containment)
- Run security checks to verify complete eradication of threat and monitor systems for recurrence or lingering issues

4

Resolution and Recovery

- Restore affected systems and recover lost or corrupted data
- Implement additional security security measures and update security protocols to address gaps
- Inform stakeholders of the resolution status

5

Post-incident Activity

- Maintain a register of incidents to help identify patterns and apply effective solutions from past experiences
- Identify areas for improvement and verify the effectiveness of newly implemented measures
- Communicate with stakeholders to demonstrate accountability and commitment to security improvements

Business continuity plan

To mitigate the effects of unforeseen events on MIT's business and operations, the Manager has established a comprehensive business continuity plan alongside a crisis communication plan. These plans offer structured responses to various situations, such as crisis management, property damage, and IT disaster recovery. In light of growing cyber threats, the Manager performs annual tests of the IT disaster recovery plans and mandates all employees to complete all compulsory online IT security trainings.