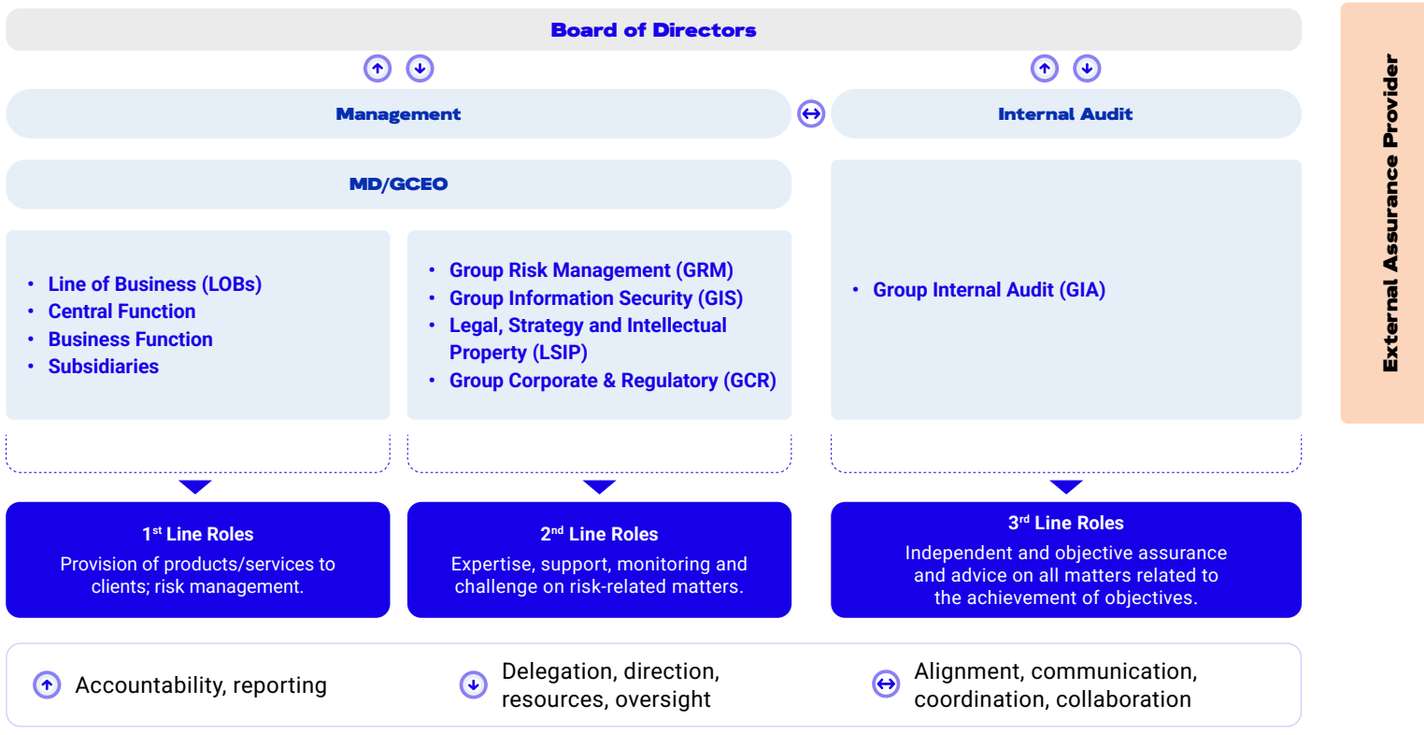
DIRECTORS' STATEMENT ON RISK MANAGEMENT & INTERNAL CONTROLS (DSORMIC)

Under Paragraph 15.26(b) of the Main Market Listing Requirements of Bursa Malaysia Securities Berhad (Bursa Securities), the Board of Directors of a listed issuer is required to include in its annual report a statement on the state of risk management and internal control of the issuer as a group. In fulfilling this requirement, TM's Board of Directors ("Board") presents this Statement on Risk Management and Internal Control in accordance with the Statement on Risk Management and Internal Control: Guidelines for Directors of Listed Issuers endorsed by Bursa Securities. This statement outlines the nature and scope of risk management and internal control within TM Group for the financial year under review and is jointly endorsed by the Board Risk and Investment Committee (BRIC) and the Board Audit Committee (BAC).



The Group adopts the Three Lines Model issued by the Institute of Internal Auditors (IIA) to delineate clearly the roles and responsibilities for risk management and internal control across TM. This model establishes a structured basis for accountability, segregation of duties and independent assurance and supports a consistent approach to risk governance throughout the Group.

Under this model, responsibilities are allocated across three (3) distinct lines. The First Line, comprising Business and Operations, is accountable for owning and managing risks within their respective areas. This includes implementing and maintaining effective internal controls, complying with approved policies and delegated authorities and promptly escalating control weaknesses or incidents.

The Second Line, represented by the Risk and Compliance functions, provides oversight and challenge to the First Line. Its role includes establishing risk management frameworks, policies and risk appetite parameters, monitoring compliance with regulatory and internal requirements and consolidating enterprise-wide risk information for Management and the BAC.

The Third Line, comprising Internal Audit, provides independent assurance on the adequacy and effectiveness of governance, risk management and internal control systems. To preserve independence and objectivity, Internal Audit reports directly to the BAC.

Together, the three (3) lines promote management accountability while preserving independent oversight and assurance, in line with Bursa Malaysia's Statement on Risk Management and Internal Control expectations. To enable this structure to operate cohesively, TM maintains a structured Enterprise Risk Management (ERM) governance process to support coordination and information flow on risk matters. Risk information identified by the First Line is consolidated and reviewed by the Second Line (Risk Management), which provides challenge, oversight and escalation of key risks to Management and the BRIC. In parallel, the Third Line (Internal Audit) delivers independent assurance on governance, risk management and internal control processes.

DIRECTORS' STATEMENT ON RISK MANAGEMENT & INTERNAL CONTROLS (DSORMIC)

Internal Audit aligns its audit planning with key Second Line functions and draws on risk assessments and monitoring outputs in determining audit priorities. Audit results and thematic issues are reported to Management and the Board Audit Committee, enabling appropriate deliberation and follow-up actions.

During the financial year, the Group continued to maintain and support the role of the Second Line (Risk) within the existing ERM framework through established governance, reporting and escalation arrangements. Ongoing efforts focused on promoting clarity of responsibilities and maintaining adequate capability to support effective risk oversight.

Enhancements to the Third Line (Internal Audit) were undertaken to further strengthen assurance capabilities. These included the adoption of the 2024 IIA Global Internal Audit Standards to improve independence, objectivity and audit methodology, as well as capability development in sustainability assurance, digital auditing, data analytics and cyber risk. In addition, ongoing Quality Assurance and Improvement Programme (QAIP) monitoring was carried out to support continued conformance with updated auditing standards. Greater use of data-driven and continuous auditing techniques were introduced to expand audit coverage and shorten audit cycles.

RESPONSIBILITY AND ACCOUNTABILITY

The Board

The Board is committed to establishing and overseeing the Group's risk management framework and internal control systems. Guided by the Group's risk appetite, the Board ensures that these systems operate within acceptable tolerance levels to support the achievement of the Group's goals and objectives in a dynamic and challenging business environment.

In fulfilling this role, the Board regularly reviews the effectiveness and adequacy of the framework by identifying, assessing and monitoring key risks to safeguard shareholder investments and protect the Group's assets. Oversight of risk management and internal control is carried out through the BRIC and the BAC, to which specific responsibilities have been delegated.

Board Risk and Investment Committee (BRIC)

The primary role of the BRIC is to support the Board in maintaining a robust Enterprise Risk Management (ERM) framework and ensuring its effective implementation, thereby strengthening the Group's corporate governance. Its focus is on the identification, assessment and monitoring of key business and investment risks.

The BRIC serves as the principal platform for deliberating on these risks and the related controls. During the financial year, it reviewed the outcomes of the Corporate Risk Assessment, assessed movements in key risks and evaluated the effectiveness of mitigation measures and controls. The BRIC also examined the quality and consistency of risk reporting and recommended enhancements where appropriate to ensure the ERM framework remains fit for purpose for TM Group.

BRIC undertake ongoing risk management training to support effective oversight of the Group's risk profile.

The Terms of Reference (ToR) and primary responsibilities of the BRIC in relation to risk management are incorporated in the Board Charter, which is available on the Company's official website at www.tm.com.my.

Board Audit Committee (BAC)

The BAC assists the Board in assessing the effectiveness of the Group's internal control structure and in reviewing financial reporting. In carrying out these responsibilities, the BAC reviews the adequacy and integrity of the Group's internal control systems and management information systems, including compliance with applicable laws, rules, directives and guidelines, through the Group Internal Audit (GIA) function.

In addition, the BAC provides oversight of the Group's management of investigations and prosecutions, fraud and disciplinary matters, ethics and integrity principles and whistleblowing processes through the Group Integrity & Governance (GIG) function. Both GIA and GIG report directly to the BAC, supporting its ability to exercise independent oversight.

The BAC's Terms of Reference are stipulated in the Board Charter and are accessible on the Company's website. Its primary duties in assessing the adequacy and effectiveness of internal control systems implemented within the Group are further elaborated on pages 273 to 276.

While specific functions are delegated to its committees, the Board acknowledges that it remains responsible for all actions taken by these committees in carrying out their respective roles, including the outcomes of reviews and the disclosure of key risks and internal control systems in this Integrated Annual Report.

To support this responsibility, the BAC assessed the integrity of TM's internal control environment through a multiple-assurance and advisory approach. This typically included reviews of Internal Audit results, with emphasis on high- and medium-risk findings, thematic issues, repeat observations and progress of action plans. The BAC also considered External Auditor reports, including audit opinions, management letters and assessments of financial reporting controls, together with Integrity and Governance updates on integrity-related cases and fraud incidences.

Further assurance was derived from Management control self-assessments, comprising annual certifications on entity-level and key process controls, as well as financial reporting assurance, which covered accounting policy updates, key judgements and estimates, any restatements and the quality of financial disclosures. This integrated view enabled the BAC to assess the internal control environment in a holistic manner and provided confidence that it was effective, reliable and aligned with governance expectations.

Management

Management is accountable to the Board and is responsible for adopting a proactive approach in implementing processes to identify, evaluate, monitor and report risks, as well as for assessing the effectiveness of internal control systems. Management ensures that timely and appropriate corrective actions are taken and provides assurance to the Board that the Group's risk management and internal control systems operate adequately and effectively in all material aspects, based on the ERM framework and internal control systems adopted by the Group.

In relation to risk management, Management has implemented processes to identify and analyse the risk appetite relevant to the Corporate Risk and to determine the level of risk tolerance. Management is also responsible for implementing and monitoring the ERM framework in line with TM Group's strategic direction and relevant risk appetite. To address changes in risk exposures or emerging risks, appropriate actions are taken and matters are brought to the attention of Management and the Board in a timely manner.

The ERM is aligned with the strategic planning process through the incorporation of risk assessments, risk appetite and key risk indicators. Performance is monitored through regular reporting to Management and the Board to support alignment with relevant risk appetite and strategic objectives, while continuous assessment of key areas are undertaken to identify emerging risks.

Improvements in risk ownership and accountability at divisional and subsidiary levels were driven through continuous engagement on ERM processes and governance. This included regular communication with risk owners and coordinators to reinforce their roles in identifying and assessing risks. Accountability was further enhanced through defined escalation and reporting lines, strengthened tracking of mitigation actions and timelines and periodic management reviews of residual risk movements, supporting more consistent and effective risk management across TM Berhad.

ENTERPRISE RISK MANAGEMENT

ERM Framework

ERM forms an integral part of the Group's governance framework and supports the systematic assessment, mitigation and monitoring of inherent and emerging risks to safeguard the Group's interests.

TM has adopted the ISO 31000:2018 Risk Management Standard as the basis of its ERM framework. This provides a structured approach to risk identification, assessment, treatment, monitoring and reporting and integrates risk management into governance, strategy, planning and operational activities across the Group. Clear risk ownership, escalation mechanisms and oversight arrangements support effective implementation at both business unit and subsidiary levels.

Throughout the year, ERM practices continued to be applied across the organisation and its subsidiaries to support business strategies and operations. During FY2025, enhancements focused on improving consistency and effectiveness through refined risk identification and assessment guidance, clearer articulation of risk causes, impacts and controls, closer monitoring of residual risk movements and trends and strengthened tracking and reporting of mitigation actions. These measures supported more consistent application of the ERM framework and improved oversight of key risks across TM Group.

Consistency in risk rating and prioritisation is achieved through a standardised ERM methodology, including common assessment criteria, uniform rating scales and aligned definitions of likelihood and impact across the Group.

In 2025, TM has expanded our governance to incorporate Third Party Risk Management Framework.

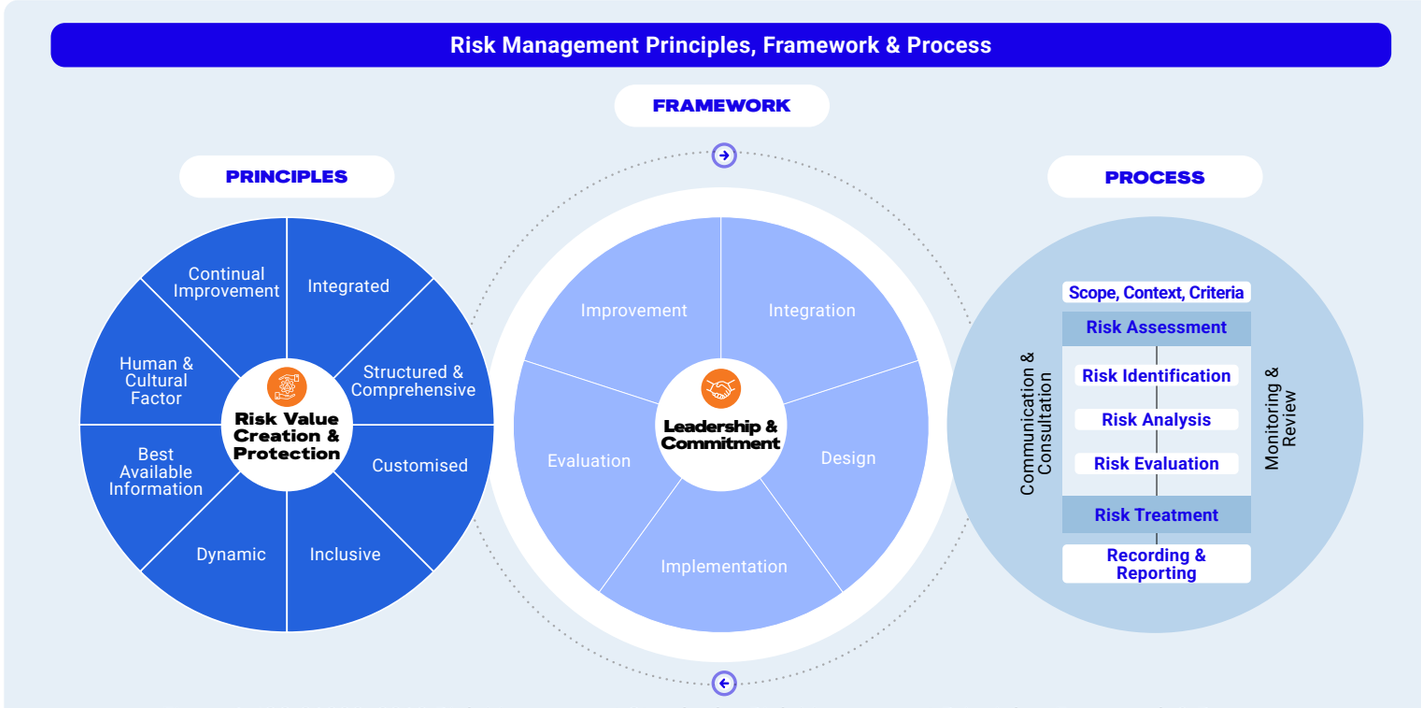


Figure 1: ISO 31000: 2018 Risk Management Standard – Risk Management Principles, Framework & Process

DIRECTORS' STATEMENT ON RISK MANAGEMENT & INTERNAL CONTROLS (DSORMIC)

TM Group Risk Governance Structure

TM Group's risk governance structure extends across the organisation, from the Board to all operational levels, providing comprehensive oversight and supporting proactive risk management.

Corporate risks identified across divisions are consolidated at Management level and tabled to the Management Committee (MC) for reviewed prior to reporting to the BRIC and the Board. Through this structured Group-wide process, senior leadership evaluates, endorses and approves the Corporate Risks, ensuring consistent prioritisation, governance and accountability at Board level.

To ensure effective implementation across the organisation, Risk Coordinators are appointed within each Line of Business (LOB), Central Function, Business Function and subsidiary. They are responsible for coordinating risk management activities and controls within their respective areas, including regional and state operations, for ensuring consistent application of risk management practices. Through this structured network, risk information is consolidated, communicated and embedded into business processes, enabling informed, timely and risk-aware decision-making across the Group

Heads of Divisions play a pivotal role within this structure by embedding and enforcing ERM practices within their respective areas. They are accountable for driving risk ownership, ensuring disciplined risk management practices and integrating risk considerations into day-to-day operations and decision-making.

Throughout the year, structured risk management training programmes were conducted for Risk Coordinators and key risk management personnel across business units and subsidiaries to enhance accountability, reinforce risk ownership and promote the consistent implementation of the Group's Enterprise Risk Management (ERM) framework. TM is committed to integrate ERM into the organisation's performance management framework.

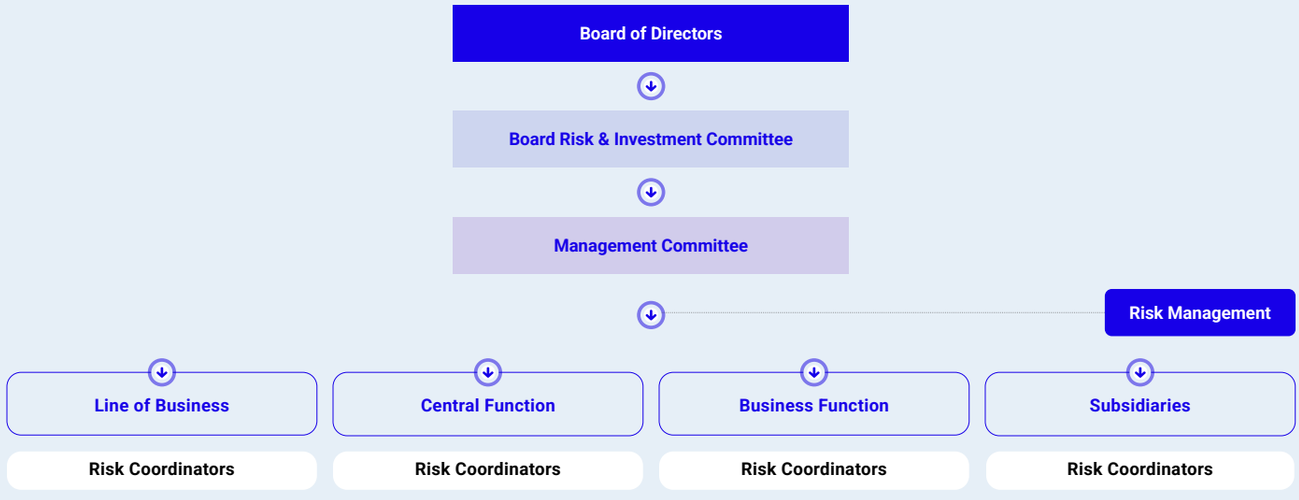


Figure 2: TM Group Governance Structure

TM Corporate Risk Management Policy and Risk Appetite Statement

TM Group applies a risk-based internal control system to provide reasonable assurance in achieving its strategic goals, including sustainable growth, resilience and alignment with the PWR 2030 vision of becoming a Digital Powerhouse.

Risk management operates within the Board-approved risk appetite through the incorporation of risk appetite thresholds into the ERM framework and decision-making processes, supported by regular monitoring of key risks and implementation of mitigation actions. Risk appetite considerations are reflected in policies, delegated authorities and approval workflows. Where risk exposures approach or exceed approved thresholds, matters are escalated through the relevant governance channels for review and direction, supporting disciplined risk management aligned with the Group's strategic objectives.

TM's Corporate Risk Appetite is communicated and applied at operational levels to guide risk assessment and management based on evaluations of likelihood and impact.

As part of its responsibility to establish and oversee the risk management framework and internal control systems, the Board reaffirmed TM Corporate risk appetite and tolerance levels. Guided by the approved Risk Appetite Statement, the Board ensured that risk-taking activities and the control environment operated within acceptable tolerance levels in support of the Group's objectives in a challenging business environment.

Through regular reviews, the Board assessed the adequacy and effectiveness of the framework by identifying, assessing and monitoring key risks, taking into account the Group's Corporate Risk Profile, key risk indicators and management's mitigation actions. Oversight of risk management and internal control matters was delegated to the BRIC and the BAC, which provided focused review and challenge before matters were escalated to the Board for consideration and reaffirmation.

During FY2025, the Board, through the BRIC, reviewed and reaffirmed the Corporate Risk's appetite and tolerance levels as part of its oversight of significant risk exposures. These reviews enabled the Board to assess whether residual risks were managed and monitored in line with management-defined thresholds and risk oversight practices. GIA presented high-risk audit findings arising from planned, ad hoc and follow-up audits, together with key control weaknesses and the status of management action plans, to the BAC on a quarterly basis. The closure of high-risk audit issues are closely monitored and closed based on validation of evidences ensuring risks are adequately mitigated.

Emerging Risks

The Board receives quarterly reports on Corporate Risks through the BRIC, with material incidents and significant changes in risk exposure escalated on timely basis.

Emerging risks are identified through continuous monitoring of relevant internal and external developments in key areas. These risks are assessed at a high level to determine their potential relevance and impact on the Group's overall risk profile and, where appropriate, are incorporated into BRIC reporting for oversight and ongoing monitoring at TM Group.

During FY2025, enhancements to risk reporting focused on strengthening risk analysis, improving visibility of residual risk movements and implementing forward-looking and structured tracking of mitigation actions.

Sustainability Integration into the ERM Framework

The Board ensures that sustainability-related risks, including climate, cybersecurity, supply chain and labour risks, are integrated into the Group's enterprise risk management framework. These risks are identified, assessed, prioritised and monitored as part of the Group's Corporate Risk Profile.

Oversight of sustainability-related risk considerations is exercised through the BRIC as part of the Board's broader enterprise risk oversight. This approach supports consistent monitoring of evolving sustainability-related risk exposures and aligns with relevant disclosure considerations under ISSB Standards.

Internal Control

The Board acknowledges that the Group's internal control systems are established to manage and reduce risks that may hinder the achievement of the Group's goals and objectives. These systems provide reasonable assurance against material misstatements and losses, including those relating to financial information, business operations, environmental matters, compliance obligations and fraud. Internal controls are embedded within the Group's operations and form part of core business processes.

These systems are designed to manage risks rather than eliminate the possibility of failure to achieve business objectives. Accordingly, they provide reasonable, but not absolute, assurance against material misstatement or losses.

The internal control framework is developed based on the Committee of Sponsoring Organisations of the Treadway Commission (COSO) Internal Control–Integrated Framework. The Board conducts regular reviews of the adequacy and integrity of these controls, taking into account changes in laws, regulations and the business environment.

Governance

- **Group Organisation Structure**

  The Group maintains clearly defined lines of responsibility and authority to support timely decision-making in a dynamic business environment, effective supervision of daily operations, prompt resolution of audit issues and accountability for internal controls. This is supported by a formal organisational structure and an established Limit of Authority (LoA) matrix that sets out approval thresholds for the Board and Management across key processes. The LoA is approved by the Board and subject to periodic review and enhancement to reflect changes in accountability and the Group's risk appetite.

- **Annual Business Plan and Performance Monitoring**

  Annual business plans are prepared by TM's Lines of Business and major operating subsidiaries and are presented to the Board for approval. Performance is reviewed against approved targets on a monthly basis, enabling timely corrective actions to mitigate risks. The Board also receives regular reports from Management on key operating statistics, as well as legal and regulatory matters, supporting informed oversight of business performance and compliance.

- **Strategic Theme and Business Direction**

  TM has set its aspiration to become a Digital Powerhouse by 2030 under the PWR strategy. This direction focuses on defending and growing its core business while expanding beyond connectivity through the development of platform ecosystems for future growth. Leveraging next-generation infrastructure, AI-powered data centres, sovereign cloud capabilities and robust cybersecurity, TM is progressing towards building a platform ecosystem that enables customers to host applications and services, supporting Malaysia's ambition to develop as a regional digital hub.

- **Product Governance Framework**

  A Product Governance Framework has been established to govern and oversee value creation arising from product development and management. This framework supports alignment between product initiatives and TM's strategic direction and business objectives. Risk considerations are embedded throughout the product development lifecycle and integrated with the Group's Enterprise Risk Management (ERM) framework.

- **Procurement Policy**

  TM's procurement policies and processes govern the full procurement value chain and define authority limits and accountability for TM employees and business partners. Aligned with ISO 37001 (Anti-Bribery Management System), these policies promote ethical, transparent and sustainable practices

DIRECTORS' STATEMENT ON RISK MANAGEMENT & INTERNAL CONTROLS (DSORMIC)

while leveraging digital transformation to enhance efficiency. Procurement activities are guided by three (3) principles: value creation, sustainability and ESG integration and digital transformation.

- **Policies, Manuals and Procedures**

  TM's Business Policy & Governance (BPG) framework sets out key policies and governance requirements, with designated process owners responsible for policy development, periodic review and compliance. Detailed procedures and guidelines support effective implementation, operational consistency and alignment with regulatory requirements and recognised practices.

- **Insurance and Physical Safeguards**

  The Group maintains appropriate insurance coverage and physical safeguards to protect significant assets and to reduce the risk of material loss arising from unforeseen events.

- **Corporate Committees**

  Three Corporate Committees — the Management Committee (MC), Business Operations Council (BOC) and Technology Committee (TechCom) — provide guidance and decision-making within their respective mandates. Roles and authority levels are defined to support effective business execution with appropriate controls. MC focuses on strategic and policy matters, while BOC and TechCom oversee operational performance, execution and deployment in business and technology areas.

- **Best Practice Committee (BPC)**

  The BPC which reports to the Board Audit Committee, reviews updates on financial performance and completeness, listed issuer compliance, policies and governance practices, as well as developments in statutory and regulatory requirements.

- **Recording to Reporting (R2R) Framework**

  The R2R Framework supports financial reporting integrity and transparency through systematic monitoring and escalation of non-compliance matters. It promotes a culture of compliance and supports the reliability and completeness of financial reporting in line with applicable standards.

- **Procurement Compliance Committee (PCC)**

  The PCC oversees the implementation of procurement consequence management to support compliance with policies, procedures and authority limits. Procurement personnel are required to report non-compliance, while the PCC addresses such matters and determines appropriate actions.

- **TM Sponsorship Management Guidelines**

  These guidelines set out requirements for sponsorships, donations, gifts and hospitality to support the achievement of intended objectives while reducing associated risks. Sponsorship activities aim to contribute to business growth, technology advancement, people development and nation-building and, where relevant, support brand outcomes.

- **Management Information Systems**

  Key information systems support the Group's operations and communication with stakeholders. These systems are governed by the TM IT Policy and Enterprise Architecture Standard, which control access and monitor usage. Business processes guide IT services and align with recognised standards and practices. Continuous training ensures compliance and Legacy Mission Critical (MC) & Business Critical (BC) application risks are proactively managed and updated quarterly to the BRIC while monitoring the availability and performance of IT systems.

- **TM Cyber Security Management**

  Information Security Governance and Certifications

  Telekom Malaysia (TM) continues to strengthen its cybersecurity governance framework to safeguard Mission Critical (MC) and Business Critical (BC) services, particularly systems handling personally identifiable information (PII) and public-facing digital platforms, in alignment with regulatory requirements, including the MCMC Information Network Security Guidelines (INSG) and NACSA Cyber Security Act (CSA 2024).

  TM maintains internationally recognised certifications, including ISO/IEC 27001 (Information Security Management Systems), Business Continuity Management Systems (BCMS) and the Payment Card Industry Data Security Standard (PCI DSS) across cloud infrastructure, network operations and enterprise IT systems. A comprehensive cybersecurity risk assessments for new projects and major changes to existing systems and applications continue to be conducted to identify and mitigate potential threats to digital infrastructure.

  Technology Uplift

  TM continues to enhance its cybersecurity posture through risk-based and compliance-driven initiatives across critical systems and digital assets. Key initiatives include strengthening External Attack Surface Management (ASM), enhancing Identity and Access Control through role-based access enforcement and secure access mechanisms and implementing Data Protection controls across the information lifecycle to reduce attack surfaces and minimise exposure of PII data. A comprehensive cybersecurity risk assessment is conducted through Cybersecurity Control Assessments (CCAs), leveraging the NIST CSF 2.0 methodology to identify gaps and reinforce operational resilience across TM's digital infrastructure.

  Cybersecurity-Focused People Development

  TM fosters a cyber-aware culture through ongoing awareness and capability development programmes. These initiatives include enhanced cybersecurity e-learning programmes for TM's employees, quarterly phishing simulation exercises and cybersecurity awareness sessions for employees and business partners. Internal engagement initiatives such as TM Cyber Day, webinars and cyber talks further reinforce cybersecurity awareness across the Line of Business.

To strengthen crisis management, TM conducted a comprehensive Tabletop Simulation and Cyber Drill Exercise involving TM's C-Suite management and members of the Board of Directors (BOD) to validate executive decision-making, crisis coordination and incident response readiness.

Third Party Information Security Requirements for Suppliers

Security requirements are embedded across TM's third-party engagements to strengthen supply chain resilience. Supplier onboarding processes require fulfilment of defined cybersecurity criteria prior to engagement and vendors are required to meet the Vendor Security Index (VSI) in order to assess and measure their cybersecurity posture.

Vendors are classified using a risk-based tiering framework, with enhanced cybersecurity assurance, remediation tracking and periodic reviews applied to top-tier vendors supporting critical application services, ensuring continuous improvement and supply chain resilience.

INTERNAL AUDIT

TM Group's internal audit function is carried out by GIA, which delivers independent assurance and advisory services to strengthen governance, risk management and internal control practices. Through a structured and disciplined methodology, GIA evaluates business processes and control environments to support the achievement of organisational objectives and safeguard long-term value creation. The mandate, sufficient standing, authority and responsibilities of internal auditors, which enable them to discharge their functions effectively, are set out in the Internal Audit Charter approved by the BAC.

Leadership of GIA sits with the Chief Internal Auditor (CIA), who reports functionally to the BAC. This reporting arrangement protects independence and objectivity while preventing situations that could influence professional judgement. An administrative reporting line to the Group Chief Executive Officer (GCEO) provides the necessary standing for the CIA to carry out responsibilities effectively. Further details on the CIA's professional background are available in the "Profile of Senior Leadership" section of this Integrated Report.

Oversight of the internal audit function is exercised by the BAC, which reviews and approves the appointment of internal auditors and manpower requirements, annual audit plan including the scope of work, performance evaluation and budget for the internal audit function. This oversight confirms that GIA is supported by the appropriate skills and capacity to deliver its mandate. The CIA provides periodic updates to the BAC on audit progress, key observations and emerging control matters. The BAC also reviews the performance of both GIA and the CIA to assess progress and outcomes achieved during year.

PRACTICES AND FRAMEWORK

GIA conducts its work in line with established internal policies, procedures and frameworks, supported by the COSO and Control Objectives for Information and Related Technology (COBIT). These references guide the evaluation of the Group's internal control environment, governance practices and risk management processes.

Audit engagements adopt the 2024 Global Internal Audit Standard (GIAS), International Professional Practices Framework (IPPF®), including the Core Principles for the Professional Practice of Internal Auditing, International Standards, the Definition of Internal Auditing and the Code of Ethics. This ensures consistency, quality and professional conduct across all assignments.

SCOPE AND COVERAGE

The annual audit plan is developed using a risk-based methodology that considers TM's strategic priorities, enterprise risk profile and input from the BAC and Senior Management. This approach enables the Board to receive independent assurance that audit activities focus on areas of higher exposure and strategic importance.

During FY2025, audit coverage focused on several key risk areas:

- **Product Strategy and Management**
  Evaluating the strategy, planning, development and management of key products such as Unifi Mobile, cloud services and data centres monetisation.

- **Project and Service Delivery**
  Monitoring and managing TM's major projects, services and systems, encompassing processes, IT systems, network infrastructure and people capabilities.

- **Procurement and Operational Controls**
  Reviews identified opportunities to strengthen procurement oversight and controls, including process transparency and monitoring.

- **Cybersecurity and IT Readiness**
  Observations included the need to enhance cybersecurity awareness and capabilities across relevant functions, as well as to ensure IT solutions support business objectives effectively.

- **Data Governance and Privacy**
  GIA highlighted the criticality of centralized oversight for data-related functions to improve visibility, management and protection of personal and sensitive data.

- **Network and System Security**
  Reviews identified opportunities to reinforce access controls, authentication mechanisms and adherence to network security policies.

DIRECTORS' STATEMENT ON RISK MANAGEMENT & INTERNAL CONTROLS (DSORMIC)

- **Policy Adherence and Consequence Management**
  Findings emphasized the need to strengthen enforcement of policies, monitoring of compliance and timely implementation of fraud and risk management systems across the LOBs and Enablers.

Audit reports highlighting significant improvement areas were tabled to the BAC for deliberation, while other reports were presented through quarterly updates. Each observation was supported by practical recommendations, with Management responses obtained to facilitate timely resolution. Progress on agreed actions is tracked through monthly monitoring and validation exercises conducted by GIA.

INTERNAL AUDIT QUALITY

Quality oversight within GIA is driven through a structured Quality Assurance and Improvement Programme (QAIP) developed and overseen by the CIA. This programme covers all aspects of internal audit activities and serves as a benchmark for assessing audit practices against the standards issued by the Institute of Internal Auditors (IIA).

An internal quality assessment is conducted annually by an independent internal review team under the CIA's direct supervision. The outcomes of these assessments are presented to the BAC for review. In line with professional standards, an external quality assessment is carried out at least once every five (5) years by a suitably qualified and independent assessor.

To further strengthen assurance, GIA applies a three (3)-tier quality review mechanism that incorporates subject matter experts as peer reviewers. This process provides an additional layer of scrutiny to confirm that audit conclusions are supported by relevant, reliable and sufficient evidence. The review framework also confirms that all significant risk areas are adequately assessed before final engagement outcomes are communicated to Management and the BAC.

GIA has enhanced audit delivery through continuous optimisation of its Audit Management System. A dedicated Data Analytics Team supports auditors by expanding data coverage and strengthening validation procedures. Continuous auditing initiatives are being explored to complement the traditional audit approach and provide earlier insight into potential risk exposures. These initiatives enable GIA to maintain sound governance practices through risk-based audit planning, periodic plan reviews, robust policies and procedures, effective use of audit technology, structured supervision, timely reporting, systematic follow-ups on audit findings and regular updates to the BAC on implementation status. Adherence to the IIA Code of Ethics is applied and declared across all audit engagements.

RESOURCES

Audit activities during the year were carried out by a team of 45 internal auditors with diverse academic and professional backgrounds, including Engineering and Network disciplines, Accounting and Finance, Information Technology and Business Administration. This multidisciplinary composition enables GIA to deliver well-rounded audit coverage across the Group's operations.

PROFESSIONAL QUALIFICATION & CONTINUOUS COMPETENCY DEVELOPMENT

Capability building within GIA is shaped around developing a future-ready internal audit function while serving as a platform to nurture talents and potential business leaders. In line with the Internal Audit Charter, GIA commits to continuously strive to improve the proficiency and effectiveness of its service. Continuous learning remains a priority to keep pace with evolving business, digital and risk landscapes. To support this, a competency assessment survey was conducted in November 2025, benchmarking each auditor against the IIA Audit Competency Framework. The results identified individual capability gaps, which were addressed through targeted development programs.

Beyond technical audit skills, auditors are also exposed to broader business areas including entrepreneurship, strategic management, innovation and operational excellence. This broader exposure strengthens the business acumen, commercial awareness and supports more insightful audit engagements.

GIA comprises professionally accredited auditors and the pursuit of professional certification is actively encouraged across the function. The audit team holds a diverse range of core auditing and functional professional certifications, including the Certified Internal Auditor and Certified Information Systems Auditor, as well as other specialised qualifications. These credentials strengthen the technical expertise and enhance the professional credibility of the audit function.

GIA actively develops auditor capabilities through involvement in strategic initiatives and leadership programmes, complemented by exposure to emerging risks, evolving tools and technologies and professional developments within the audit community. In addressing future challenges, GIA has further strengthened and broadened its audit coverage to assess emerging risks associated with digitalisation and automation, data analytics, sustainability, IT and digital and cybersecurity

Overall, GIA continues to enhance its operating model through workforce realignment and continuous capability building. Its portfolio-based organisational structure supports talent rotation and skills diversification, enabling auditors to gain broad exposure across TM's value chain while strengthening audit coverage across business functions.

BUSINESS CONTINUITY AND RESILIENCY

Business Continuity Management (BCM)

TM Group's BCM framework supports operational resilience by promoting preparedness, continuity of critical services and coordinated crisis response across the Group. The framework is governed through defined roles and oversight responsibilities and is supported by structured processes across the BCM lifecycle to anticipate, respond to and recover from disruptions affecting customers, operations and essential network and services.

The BCM approach is reinforced through Group-wide governance and accountability, ensuring continuity requirements are embedded at business and operational levels. Business Impact Analysis (BIA) is conducted to identify critical processes, recovery priorities and required recovery capabilities. Documented response and recovery plans are maintained for key disruption scenarios and are supported by escalation procedures and crisis communication arrangements. Periodic reviews, drills and validation exercises are conducted to keep plans current and usable during actual incidents.

Internal Audit provides independent assurance over the BCM framework through reviews of lifecycle implementation and operational readiness, including the adequacy of continuity arrangements. Audit coverage also considers maturity and control effectiveness based on the Group's risk profile and Board priorities, including technology risks relating to Digital and IT, cybersecurity, ESG-related matters and third-party dependencies. Follow-up monitoring is performed to track the closure of identified gaps and improvement actions within agreed timelines.

Integration of Macro Trends and Corporate Risks into Resilience Planning

Forward-looking considerations of macro trends and emerging risks are incorporated into ERM and BCM processes to maintain the relevance of continuity strategies in a changing environment. Key focus areas include increasing dependence on digital connectivity, a rising cyber threat landscape, climate-related physical risks to network and mobile infrastructure, third-party concentration and supply chain constraints and regulatory and sustainability-driven requirements affecting preparedness and disclosure.

These considerations are integrated into BCM and resilience planning through refreshed risk inputs from Group-level risk assessments and operational BIAs. Continuity plans, crisis response strategies and escalation thresholds are updated accordingly and cross-functional readiness is enhanced for converging risk scenarios such as extreme weather events, prolonged power outages, network and service disruptions and cyber incidents. Insights from these activities are used to update BCM inputs, including BIAs, continuity strategies such as BCPs and DRPs, scenario testing and response plans.

Scenario Analysis and Stress Testing

Scenario analysis and stress testing are applied to assess the Group's ability to sustain operations under adverse and uncertain conditions. These exercises evaluate vulnerabilities across critical processes and enabling systems, network and service recovery capabilities and resource readiness and the effectiveness of responses under constrained recovery environments such as limited site access, vendor support challenges and concurrent incidents.

TM applies these approaches through Table-Top Exercises and Field Test Exercises to test its ability to sustain critical services under severe yet plausible disruption scenarios. Events examined include technology outages, cyber incidents, security threats, facility unavailability and workforce impacts. Recovery capabilities are validated against defined recovery time objectives and impact tolerances.

Findings from scenario analysis and stress testing are systematically applied to improve continuity plans, technology resilience measures and crisis management procedures. This supports stronger preparedness and the ability to sustain critical services during adverse and unexpected conditions, including climate-related disruptions where applicable.

Crisis Simulations and Resilience Exercise

During FY2025, crisis simulations and resilience exercises were conducted to enhance incident preparedness and organisational response. These simulations were designed to validate crisis management activation and decision-making processes, cross-functional coordination and escalation protocols, crisis communication workflows and operational recovery actions under disruption conditions.

Stress-testing themes addressed major network and service disruption scenarios, operational events affecting facilities, personnel and third-party dependencies and cyber incident simulations involving data breaches, ransomware-type disruptions and loss of system availability.

BCM Group Corporate, in collaboration with Group Information Security, conducted the "TM Comprehensive Table-Top Simulation and Cyber Drill Exercise 2025." The exercise involved the Board of Directors, Top Management and key functional leaders, with participation from Groups, Lines of Business, Divisions, Subsidiaries and States.

Outcomes from these exercises were applied to strengthen response playbooks, clarify roles and responsibilities and refine recovery strategies to reduce restoration time for critical services. The simulations also supported improvements in strategic crisis governance, escalation protocols, crisis communication processes and decision-making effectiveness under cyber and operational disruption scenarios.

DIRECTORS' STATEMENT ON RISK MANAGEMENT & INTERNAL CONTROLS (DSORMIC)

Collectively, these scenario-based evaluations provided Management and the Board with added assurance that resilience strategies adapt as risks evolve. In parallel, emerging risks are monitored to strengthen resilience through appropriate risk transfer measures and insurance coverage for loss recovery, supporting protection of assets, people, customers and key stakeholders while limiting financial and operational impacts.

TM continues to advance its BCM programmes while embedding business continuity into organisational culture. As a national connectivity provider supporting millions of Malaysians, continuity planning has become increasingly important in supporting TM's role as a Digital Orchestrator and in pursuing its aspiration to become a Digital Powerhouse by 2030. These efforts also support Malaysia's ambition to develop as an ASEAN digital hub by promoting resilient digital infrastructure and services.

ADEQUACY AND EFFECTIVENESS OF THE GROUP'S RISK MANAGEMENT AND INTERNAL CONTROL SYSTEMS

The Board evaluates the effectiveness of the Group's risk management and internal control systems using a combination of quantitative and qualitative indicators.

Quantitative indicators include Corporate key indicators, movements in residual risk levels and the timeliness of mitigation and control actions. These measures provide insight into changes in the Group's risk profile and the responsiveness of management actions. In addition, the Board considers assurance indicators presented by GIA, including the number and severity of audit findings, the ageing and status of outstanding audit actions, the timeliness of remediation of high-risk issues and the level of completion of the risk-based internal audit plan covering key risk areas.

Qualitative considerations complement these measures and include Internal Audit's assessment of the adequacy and operating effectiveness of controls, management's commitment and accountability in addressing control weaknesses and thematic insights arising from audit reviews that may signal systemic or emerging risks. Together, these indicators enable the Board to form a view on whether risk management and internal controls operate effectively and whether residual risks are managed and monitored in line with management-defined thresholds and risk oversight practices.

Oversight of this evaluation process is exercised through the BRIC and the BAC, which provide focused review and challenge to support the Board's overall assessment of system adequacy and effectiveness.

The Statement does not include the risk management and internal control systems of TM Group's joint ventures and associates. Nonetheless, TM Group's interests are served through representation on the BOD and Senior Management posting(s) to the joint venture and associate and through the review of management accounts received. These provide the Board with performance-related information to enable informed and timely decision-making on the Group's investments in such companies.

Assurance to the Board

The Group Chief Executive Officer (GCEO) and Group Chief Financial Officer (GCFO) provided formal written assurances to the Board confirming that TM Group's Risk Management and Internal Control (RMIC) systems were adequate and effective in all material aspects. These assurances were supported by Management Assurance Declarations from Divisional Heads. Based on these representations and ongoing assurance activities, the GCEO and GCFO provided the Board with reasonable assurance in accordance with SORMIC requirements.

The annual assurance statement typically covers the effectiveness of internal controls across financial reporting, operations, compliance, cybersecurity and Sales, IT and Network areas. It also addresses the accuracy of financial statements and compliance with applicable accounting standards, adherence to laws, regulations and internal policies, reporting of material control weaknesses, fraud incidents and significant breaches and confirmation that risk management processes operate as designed and within the Board-approved corporate risk appetite.

REVIEW OF THE STATEMENT BY THE EXTERNAL AUDITORS

As required by Paragraph 15.23 of the Bursa Malaysia Securities Berhad Main Market Listing Requirements, the external auditors have reviewed this Statement on Risk Management and Internal Controls. Their limited assurance review was performed following the Malaysian Approved Standard on Assurance Engagements, ISAE 3000 (Revised), Assurance Engagements Other than Audits or Reviews of Historical Financial Information and Audit and Assurance Practice Guide 3, Guidance for Auditors on Engagements to Report on the Statement on Risk Management and Internal Control included in the Annual Report issued by the Malaysian Institute of Accountants. AAPG 3 does not require the external auditors to form an opinion on the adequacy and effectiveness of the risk management and internal control systems of the Group.