

UEM Group Berhad (“UEM”) has implemented the FIGR as a strategic guide for effective risk oversight and to cultivate a risk vigilance culture across UEM. The FIGR is designed to be dynamic and adaptive to remain relevant amid evolving business environment in which UEM operates while supporting its sustainability and continuous improvement where required.

OUR VALUES

OUR VALUES, OUR CULTURE

- Our values guide our organizational behavior and shape the way we conduct our business activities. They define our culture and reflect our identity as an organization.
- We strive to foster a robust risk management culture at UEM with reinforcement of accountability and integrity embedded throughout our safeguards and operational practices.
- Our core values comprises of:
 - Enterprising
 - Teamwork
 - Integrity
 - Passion
 - Success

1st LINE OF DEFENCE

UEM COMMON POLICIES AND PROCEDURES (“P&P”)

- The P&P outline internal parameters, processes and operational guidelines, embedding appropriate internal controls and compliance measures aligned with applicable laws and standards.

CODE OF CONDUCT FOR EMPLOYEES

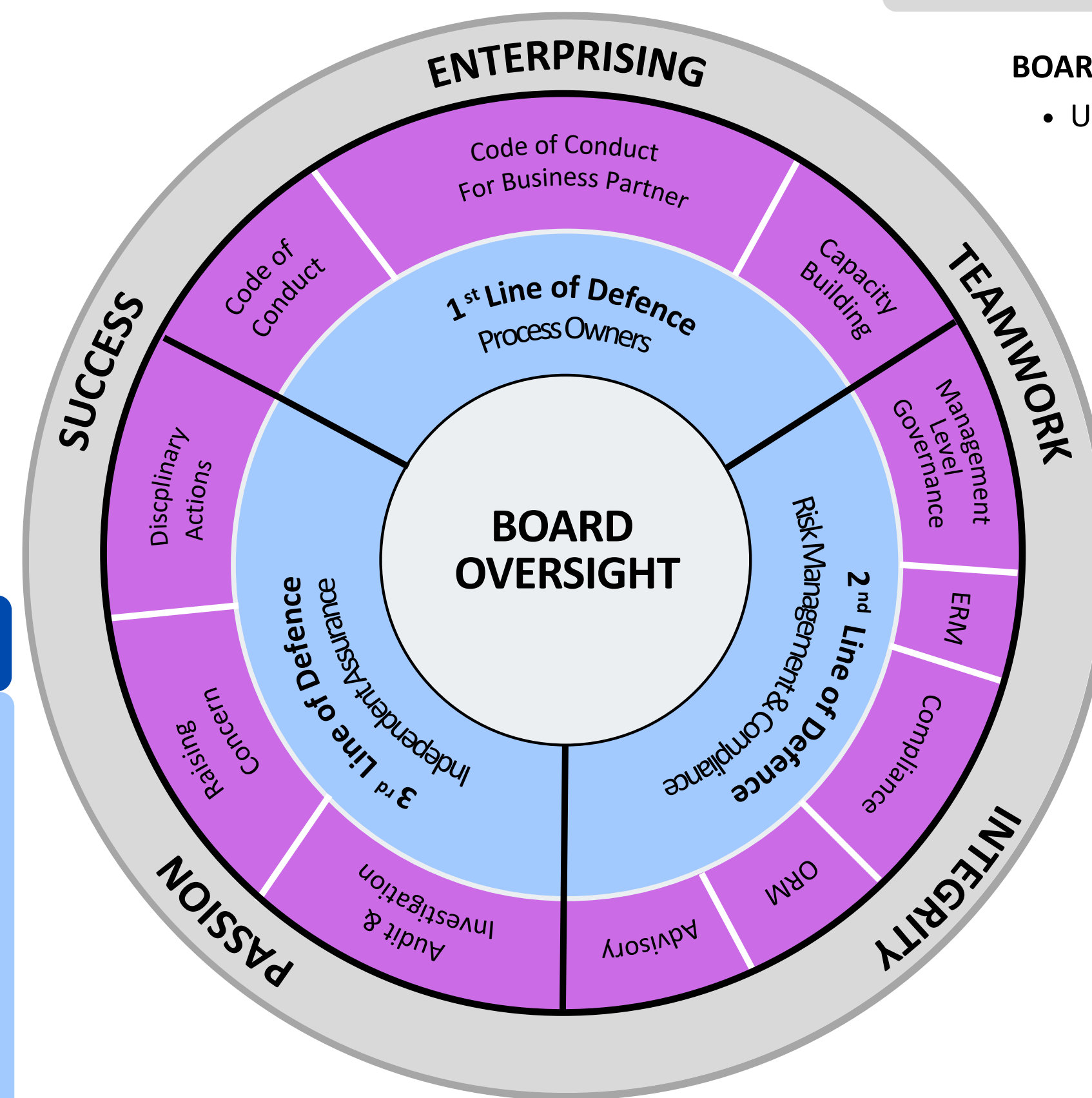
- Staff are required to comply with all relevant declaration and compliance processes, including those related to independence, interests, and gifts. They are also guided by the following key documents:
 - Code of Conduct specifies UEM’s foundational standards for ethical behavior in business and stipulates a structured approach to guide ethical decision-making.
 - Employee Handbook Serves as a comprehensive reference for all human resource-related matters for UEM staff.

CODE OF CONDUCT FOR BUSINESS PARTNER

- Provides guidance to Vendors, including Suppliers and Consultants, on the key standards and principles required to maintain a sustainable and ethical business relationship with UEM.

CAPACITY BUILDING

- Innovative and purposeful use of ICT systems and tools to enhance operational efficiencies.
- Ongoing learning and development of our people to support UEM’s operations domestically and globally.
- Comprehensive staff education and training programs that instill core values and promote a culture aligned with organizational practices.



2nd LINE OF DEFENCE

MANAGEMENT LEVEL GOVERNANCE

- MC is primarily established for consultation purposes where limits of approval under the respective approving authority shall be in accordance with the DAL, and their duties, and authorities outlines in the MC’s TOR.
- Governance, Risk and Compliance (“GRC”) reports directly to the ARC.

ENTERPRISE RISK MANAGEMENT (“ERM”)

- Strengthening organisational resilience through continuous monitoring and proactive management of both existing and emerging risks. Key focus areas include investment-related risks, strategic risks, geopolitical risks, physical and cybersecurity risks, legal and regulatory risks, as well as people-related risks.
- A risk-based approach is adopted to identify and assess risks, with prioritisation based on their likelihood and potential impact. Clear responsibilities and risk mitigation measures are outlined to effectively manage risks and protect the interests of shareholders.

COMPLIANCE

- Compliance activities including regulatory programs such as personal data protection, anti-bribery and corruption, and conflict management, alongside providing relevant training. These efforts are complemented by ongoing surveillance and monitoring of staff conduct.

BOARD OVERSIGHT

BOARD COMMITTEES

- UEM’s Board is supported by the Audit and Risk Committee (“ARC”), and Whistleblower Committee (“WC”).

GOVERNANCE FRAMEWORK

- The Board Charter and Board Committees’ Terms of References (“TOR”) outline the roles, responsibilities and authorities of the Board and its relevant committees.
- Discretionary Authority Limits (“DAL”) provide a comprehensive and effective governance framework and authority structure for the Board, Board Committees, Management Committee (“MC”) and senior management of UEM.

STRATEGIC POLICIES

- Outlines the overall strategy and guiding principles for UEM as endorsed by the Board.

3rd LINE OF DEFENCE

AUDIT & INVESTIGATIONS

- The annual internal audit plan, approved by the ARC, provides independent assurance on the effectiveness of UEM’s internal controls.
- Audits may also be conducted by GRC and/or independent internal auditor that is appointed by UEM and/or designated by relevant authorities. The audit results shall be reported directly to the ARC.
- Special reviews are initiated based on risk and exposure assessments.

RAISING CONCERNS

- Multiple channels are available for interested parties to raise issues or report concerns.
- A dedicated charter is established for Heads of Division/Department, offering guidance on how to manage and address these concerns effectively.

DISCIPLINARY ACTIONS

- Ensure consistent enforcement of our core values across all levels of the organization.

OPERATIONAL RISK MANAGEMENT

Physical and Cyber-Security Risks

- Oversight of security-related risks, including ICT and data security, email intrusions, and security breaches at premises.

UEM Business Continuity Management (“BCM”)

- The BCM Framework enhances organizational resilience, enabling UEM to effectively respond to catastrophic incidents, restore critical operations, and minimize damage and disruptions.
- Protecting our staff, reputation, and the interests of key stakeholders.

Insurance

- Risk transfer is achieved through appropriate insurance coverage, including Directors & Officers Liability, All Risks & Public Liability, and International SOS.

ADVISORY

- Provide guidance on DAL, ensuring compliance with P&P, conflict management, and the Code of Conduct.
- Offer oversight and risk input on UEM-related matters and broader national issues.