STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL

FINANCIAL YEAR ENDED 31 DECEMBER 2017

INTRODUCTION

The Board of Directors is pleased to provide the Statement on Risk Management and Internal Control pursuant to the Bank Negara Malaysia Corporate Governance Policy outlining the key features of the risk management and internal control system of Maybank IB ("the Bank") during the year under review.

BOARD RESPONSIBILITY

The Board takes cognisance of its overall responsibility in establishing a sound risk management and internal control system as well as reviewing its adequacy and effectiveness. In view of the inherent limitations in any internal control system, the risk management and internal control system can only provide reasonable assurance, rather than absolute assurance, that the significant risks impacting the Bank's strategies and objectives are managed within the risk appetite set by the Board and Management. It does not in any way eliminate the risks of failure to realise the Bank's objectives and against any material financial misstatement, fraud or losses.

The Board has established a governance structure to ensure effective oversight of risk and control in the Bank. It is assisted by the Risk Management Committee (RMC) and Audit Committee of the Board (ACB) to oversee all matters with regard to risk and control.

The Board is satisfied that the Bank has implemented an ongoing process to identify, evaluate, monitor, manage and respond to significant risks faced by the Bank in its achievement of the business goals and objectives amidst the dynamic and challenging business environment and increasing regulatory scrutinisation. The outcome of this process is closely monitored and reported to the Board for deliberation and where required, the Board directs the Management to take the necessary remediation actions to address the gaps/deficiencies reported. This ongoing process has been in place for the entire financial year under review and up to the date of approval of this Statement.

MANAGEMENT RESPONSIBILITY

The Management is overall responsible to implement the Board's policies and procedures on risk and control and its roles include:

Identifying and evaluating the risks relevant to the Bank's business, and the achievement of business objectives and strategies;

Formulating relevant policies and procedures to manage these risks in accordance with the Bank's strategic vision and overall risk appetite;

Designing, implementing and monitoring the effective implementation of risk management and internal control system;

Implementing the policies approved by the Board;

Implementing the remedial actions to address the compliance deficiencies as directed by the Board; and

Reporting in a timely manner to the Board any changes to the risks and the corrective actions taken.

RISK MANAGEMENT AND INTERNAL CONTROL SYSTEM

Risk Management

Risk Management Framework

Risk management has evolved into an important driver for strategic decisions in support of business strategies while balancing the appropriate level of risk taken to the desired level of rewards. As risk management is a core discipline of the Bank, it is underpinned by a set of key principles which serve as the foundation in driving strong risk management culture, practices and processes:

01 Establish risk appetite and strategy

The risk appetite which is approved by the Board, articulates the nature, type and level of risk the Bank is willing to assume.

02 Assign adequate capital

The approach to capital management is driven by strategic objectives and accounts for the relevant regulatory, economic and commercial environments in which the Bank operates.

03 Ensure proper governance and oversight function

There is a clear, effective and robust governance structure with well-defined, transparent and consistent lines of responsibility established within the Bank.

04 Promote strong risk culture

Institutionalisation of a strong risk culture that supports and provides appropriate standards and incentives for professional and responsible behaviour.

05 Implement sound risk frameworks and policies

Implementation of integrated risk frameworks, policies and procedures to ensure that risk management practices and processes are effective at all levels.

06 Execute strong risk management practices and processes

Robust risk management processes are in place to actively identify, measure, control, monitor and report risks inherent in all products and activities undertaken by the Bank.

07 Ensure sufficient resources and system infrastructure

Ensure sufficient resources, infrastructure and techniques are in place to enable effective risk management.

Risk Appetite

The risk appetite is a critical component of a robust risk management framework which is driven by both top-down Board leadership and bottom-up involvement of management at all levels. The risk appetite enables the Board and Senior Management to communicate, understand and assess the types and levels of risk that the Bank is willing to accept in pursuit of its business objectives. The development of the risk appetite is integrated into the annual strategic planning process and is adaptable to changing business and market conditions. The articulation of the risk appetite is done through a set of risk appetite statements that define the Bank's appetite on all its material risks. The risk appetite balances the needs of all stakeholders by acting both as a governor of risk, and a driver of future and current business activities.

Risk Governance and Oversight

The risk governance model provides a transparent and effective governance structure that promotes active involvement from the Board and Senior Management in the risk management process to ensure a uniform view of risk across the Bank. The governance model aims to place accountability and ownership whilst facilitating an appropriate level of independence and segregation of duties between the three lines of defence, which include risk-taking units, risk-control units and internal audit.

Risk Management Practices and Processes

The risk management practices and processes enables systematic identification, measurement, control, monitoring and reporting of risk exposures across the Bank.

IDENTIFICATION

- Identify, understand and assess risks inherent in products, activities and business initiatives.
- Enable early detection of risk and ensure sound risk management practices are in place to manage and control product risk.
- Adopt forward looking approach in identifying emerging risk to ensure appropriate steps are taken to minimise the Bank's exposure.

MEASUREMENT

• Develop risk measurement techniques across different dimensions of risk factors to ensure continual reassessment and identification of risks.

• Measure aggregate exposure of the Bank, individual business and country, the risk types as well as the short and long run impact of the exposures.

CONTROLS

• Establish quantitative and qualitative controls including risk limits, thresholds and triggers to oversee and manage the risk exposures identified.

• Implement risk mitigation techniques aimed to minimise existing or in some instances to prevent new or emerging risks from occurring.

MONITORING & REPORTING

• Monitor forward looking key risk indicators and early warning signals to ensure that sufficient and timely action is in place to mitigate any potential risk to the Bank.

• Report the state of compliance to the Management level and Board level risk committees as well as to the Board on a regular basis.

Shariah Governance Framework

The Bank's Shariah Governance Framework sets out the expectations of the Shariah governance structures, processes and arrangements of all businesses within the Bank that execute Islamic business transactions. This is to ensure that all its operations and business activities are in accordance with Shariah principles as well as to provide comprehensive guidance to the Board, Group Shariah Committee and Management in discharging their duties in matters relating to Shariah.

The Bank's Shariah Governance Framework reflects the responsibility of the Board, Management, Group Shariah Committee and Shariah Control functions which laveraged on Maybank Islamic Berhad ("MIB") and Maybank Group ("Group"), namely, Shariah Advisory and Research, Shariah Risk, Shariah Review and Shariah Audit, as well as Business Units to ensure effective management of Shariah Non-Compliance risks.

The end-to-end Shariah compliant governance mechanism is executed through four lines of defence that cater for both pre-execution and post-execution. The four lines of defence are 1st-Management and Business Unit (The Bank), 2nd-Shariah Advisory and Research (MIB), 3rd-Shariah Risk (The Bank) and 4th-Shariah Audit (Group) and Shariah Review (MIB).

Cyber and Technology Risk Management Policy and Guideline

The Cyber Risk Management Policy is established to identify risks, build resilience, detect cyber threats and effectively respond to cyber related events. The Policy encompasses the cyber risk management strategy, governance structure and risk management enablers. It complements the Technology Risk Management Guideline and covers both Business and Technology drivers from an end to end perspective, which focus on the key layers of People, Process and Technology.

Technology Risk Management Guideline sets the standards for systematically identifying the causes of failure in the organisation's technology related functionalities, assessing the impact to the business and taking the appropriate risk remedial actions. This is established to safeguard the Group's reputation and to maintain high service levels to customers as well as business units.

INTERNAL CONTROL SYSTEM

The key elements of the internal control system established by the Board that provides effective governance and oversight of internal controls include:

- **Group Organisation Structure**

The Board has established an organisation structure with clearly defined lines of responsibility, authority limits, and accountability aligned to business and operations requirements which support the maintenance of a strong control environment.

- **Annual Business Plan and Budget**

An annual business plan and budget are submitted to the Board for approval. Performance achievements are reviewed against the targeted results on a monthly basis allowing timely responses and corrective actions to be taken to mitigate risks. The Board reviews regular reports from the Management on the key operating statistics, as well as legal and regulatory matters. The Board also approves any changes or amendments to the Bank's policies.

• **Oversight by Risk Management Committee**

The Board has delegated the risk oversight responsibility to the Risk Management Committee (RMC). The committee is responsible for formulating policies and frameworks to identify, measure, monitor, manage and control the material risk components impacting the businesses. The effectiveness of the risk management system is monitored and evaluated by the Risk Management function, on an on-going basis. Further information on the roles and responsibilities and specific duties of the RMC is included in the Statement of Corporate Governance from pages 32 to 34.

• **Compliance Culture**

The compliance culture is driven with a strong tone from the top, complemented by the action from the middle, to ingrain the expected values and principles of conduct that shape the behaviour and attitude of employees at all levels of businesses and activities across the Bank. Compliance framework and policies are clearly defined, consistently communicated and continuously reinforced throughout the Bank to embed a robust culture that cultivates active identification, assessment and mitigation of risks as part of the responsibility of all employees across the Bank.

As part of the compliance culture, the Bank has instilled a compliance culture where the Board, Senior Management and every employee of the Bank is committed to adhere to the requirement of relevant laws, rules, regulations and regulatory guidelines. This commitment is clearly demonstrated through the establishment of strong compliance policies and guidelines to ensure that non-compliance risks are effectively managed.

• **Regional Chinese Wall Policy**

The Regional Chinese Wall Policy ("RWCP") provides the mechanisms to manage inside information through the establishment of physical as well as procedural information barriers to separate and isolate individuals privy to inside information, prevent inadvertent spread and misuse of inside information, or the appearance thereof.

The offence of insider trading entails civil, criminal liability, criminal sanctions and possible disciplinary actions. In addition to the impact of an investigation and criminal charge against the Maybank IB employees, the impact and risk to the IB Group may result in serious operational and financial consequences and reputational damage. It is in IB Group's best interest to prevent insider trading and the RCWP may be used as a valid defense against insider trading allegations.

- **The Regional Whistle Blowing Policy and Procedures**

The Regional Whistle Blowing Policy and Procedures ("RWBP") is applicable to all employees and provides specific guidance on reportable concerns, avenues for reporting as well as governance, investigation and deliberation process. The RWBP promotes a culture of openness, accountability, integrity and professional responsibility among Employees whilst reassuring employees of protection against harassment, reprisals or victimization for raising genuine concerns.

The establishment of the policy provides management the opportunity to address any corrupt, dishonest or fraudulent activities by implementing mitigating or remedial actions to prevent systemic collapse; and provide reporting employees feedback on their concerns and to allow further escalation if they are not satisfied with the actions taken by Maybank IB.

- **Executive Level Management Committees**

Various Executive Level Management Committees (ELCs) are also established by Management to assist and support the various Board Committees to oversee the core areas of business operations. These ELCs include the Executive Committee, Management Risk Committee, Credit Underwriting Committee, IB Group Procurement Committee, IB Group IT Steering Committee and IB Group Internal Audit Committee.

- **Written Control Policies**

A written Management Control Policy (MCP) and Internal Control Policy (ICP) from Management are in place. The MCP outlines the specific responsibilities of the various parties, the Management, the Internal Audit Committee (IAC) and the ACB pertaining to internal control. The ICP is to create awareness among all employees with regard to the internal control components and basic control policy.

- **Management of Information Assets**

Confidentiality, integrity and availability of information forms the basis for data protection of customers and stakeholders, which is critical to day-to-day operations for management decision making. This holds true as the handling of information assets ultimately impacts the reputation of the Bank. To safeguard the information assets, the Information Risk Management Guideline is established to clearly define the processes for effective management of information assets and its associated risks. Guided by information handling rules in alignment to the information lifecycle, all information must be properly managed, controlled and protected. Additional measures include reinforcing the clear desk policy to minimise information leakage/theft and fraud.

• **Sustainability Management**

Operating in a sustainable manner is an organic part of the Bank's approach to its core business. Our long term financial success depends upon our ability to identify and address environmental, social and ethical issues that present risks or opportunities for our business. The Bank has in place a five year Sustainability Plan, a strategic document with the aim of generating long-lasting impact and value across three pillars; Community and Citizenship, Our People and Access to Products and Services, by integrating Environmental, Social and Governance practices into our 'business-as-usual' as part of our commitment to various stakeholders which is supported by relevant policies and systems.

• **Regular Updates and Communication of Risk Management Principles, Policies, Procedures and Practices**

Risk management principles, policies, procedures and practices are reviewed and updated regularly to ensure relevance to the current business environment as well as compliance with current/applicable laws and regulations. Risk frameworks, policies and procedures are applicable across the Bank.

• **Group Procurement Manual and Non-Credit Discretionary Power**

The Group Procurement Manual is designed to streamline the procurement functions within the Bank. It serves as a standard guideline on good management practices expected in the procurement process and procedures. Authority to approve any requisition against budgeted or unbudgeted expenditures shall be in accordance with relevant approving authority policies, i.e. the Non-Credit Discretionary Power (NCDP), Delegation of Authority (DOA) or any equivalent.

The NCDP defines the authority limits approved by the Board for procurement activities, acquisition & disposal of assets, operational writeoff, donations, as well as approving general and operational expenses.

• **Standard Practice Instruction**

Policies are in place to ensure compliance with internal controls and the prescribed laws and regulations. These policies are updated from time to time when required in tandem with changes to the business environment or regulatory guidelines. These policies are published in the communication portal which is made available to all employees.

• **Human Resource Policies and Guidelines**

The Maybank Group People Policies (MGPP) serves as a baseline with clarity on the philosophy and principles for People Management and Development in Maybank Group. It incorporates key principles and philosophies that support Maybank Group's Mission of Humanising Financial Services. The MGPP consists of a set of policies and guidelines that governs all aspects of human resource management, from talent acquisition and development, performance and consequence management, code of conduct to cessation of employment. A Disciplinary Policy is also established to provide for a structure where disciplinary matters are dealt with fairly, consistently and in line with the prevailing labour laws and employment regulations.

• **Core Values and Code of Ethics and Conduct**

The Maybank Group's core values, T.I.G.E.R. (Teamwork, Integrity, Growth, Excellence and Efficiency, Relationship Building) are the essential guiding principles to drive behavioural ethics. It is further complemented by the Code of Ethics and Conduct that sets out sound principles and standards of good practice to be observed by all.

• **Anti-Fraud Policy**

The Anti-Fraud Policy outlines the vision, principles and strategies for the Bank to adopt by instilling a culture of vigilance to effectively manage fraud from detection to remedy, and to deter future occurrences. Robust and comprehensive tools and programmes are employed to reinforce the Policy, with clear roles and responsibilities outlined at every level of the organisation in promoting high standards of integrity in every employee.

• **Reputational Risk Policy**

Protecting our reputation is paramount to operating as an institution that provides financial services. Upholding trust forms a vital part of our obligation as a financial institution. Hence, the way in which we conduct ourselves through engagements with markets, regulators, customers, and the communities we serve is crucial. Given the importance of reputation, the Reputational Risk Policy is established to effectively manage reputational risk and to institutionalise awareness on and the consequences of such risk. The Policy outlines the roles and responsibilities of key stakeholders and the guiding principles to protect the Bank's reputation.

INTERNAL AUDIT

INTERNAL AUDIT FUNCTION

The Internal Audit (IA) function is established by the Board to undertake continuous review and assessment on the adequacy, efficiency and effectiveness of risk management, control and governance processes implemented in the Bank. It reports directly to the Audit Committee of the Board (ACB) and is independent from the activities or operations of other operating units in the Bank. The fundamentals of the internal audit function involve identifying risks that could negatively impact the performance of the Bank and/or keep it from achieving its corporate goals, ensuring Management fully understands these risks and proactively recommending improvements to minimise the risks. The annual Group Audit Plan (GAP) is established based on the Maybank Risk Based Audit (MRBA) while COSO Framework is used to assess the adequacy and effectiveness of internal controls. The Management follows through and ensures remedial actions taken are prompt, adequate and effective. Status reporting of the remedial actions taken is also tabled to the ACB and IAC regularly for deliberation and tracking.

AUDIT COMMITTEE OF THE BOARD

Audit Committee of the Board (ACB) is a Board Committee established by the Board to assist in the execution of its governance and oversight responsibilities. The responsibilities include the assessment of the effectiveness and adequacy of the Bank's internal control system through the Internal Audit function. The ACB has active oversight over Internal Audit's independence, scope of work and resources. The ACB meets on a scheduled basis to review audit and investigation reports prepared by Internal Audit, taking into consideration the deliberation of the same report at the IAC. The ACB also deliberates on the outstanding audit findings to ensure prompt and effective remedial actions are taken by the Management. Where necessary, representatives from the parties being audited are requested to attend the ACB meeting to facilitate the deliberation of the audit reports. Minutes of the ACB meeting are then tabled to the Board. Further information on the roles and responsibilities and specific duties of the ACB is included in the Statement of Corporate Governance from pages 30 to 31.

INTERNAL AUDIT COMMITTEE

Internal Audit Committee (IAC) is a management level committee chaired by the Chief Financial Officer (CFO) to ensure adequacy of deliberation over issues/concerns raised by Internal Audit. It comprises senior level representatives from the various lines of business. It meets on a scheduled basis to deliberate on the findings highlighted in the audit and investigation reports and decide on the appropriate remedial actions required. Where necessary, representatives from the parties being audited are requested to attend the IAC meeting to enable more detailed deliberation and speedy resolution of the matter at hand. The status of the audit findings is also tabled to the IAC to ensure the committed remedial actions are

promptly and effectively implemented within the set timeline. Minutes of the IAC meeting are then tabled to the ACB together with the audit reports. The IAC also follows through on the actions required by the ACB.