

# Statement on Internal Control and Risk Management

**The Board of Bursa Malaysia is committed to maintaining a sound internal control and risk management system. Each business unit/functional group has implemented its own control processes under the leadership of the Chief Executive Officer (CEO), who is responsible for good business and regulatory governance. The following statement outlines the nature and scope of the Group's internal control and risk management in 2013.**

## BOARD'S RESPONSIBILITY

The Board affirms its overall responsibility for the Group's system of internal control and risk management and for reviewing the adequacy and integrity of the system. The system of internal control covers governance, risk management, financial, strategy, organisational, operational, regulatory and compliance control matters. The Board recognises that this system is designed to manage, rather than eliminate, the risk of not adhering to Group's policies and achieving goals and objectives. Therefore, the system provides reasonable, but not absolute, assurance against the occurrence of any material misstatement, loss or fraud.

In 2013, the adequacy and effectiveness of internal controls were reviewed by the Audit Committee (AC) in relation to the internal audits conducted by Group Internal Audit (GIA) during the year. Audit issues as well as actions taken by Management to address the issues tabled by GIA were deliberated upon during the AC meetings. Minutes of the AC meetings which recorded these deliberations were presented to the Board.

A Risk Management Committee (RMC) was established and maintained in accordance with Section 22 of the Capital Markets and Services Act 2007 (CMSA) to provide risk oversight as well as ensure prudent risk management of Bursa Malaysia's business and operations. The RMC via its meetings held in 2013 had reviewed, deliberated upon and provided advice on matters pertaining to the key corporate risks, risk assessment of projects and programmes, operational risks and mitigation measures, as well as enterprise risk management (ERM) activities.

Internal control and risk-related matters which warrant the attention of the Board were recommended by the AC and RMC to the Board for its approval and matters or decisions made within the AC and RMC's purview were updated to the Board for its notation.

## KEY INTERNAL CONTROL PROCESSES

The Group's internal control system encompasses the following key processes:

### 1. Separation of Commercial and Regulatory Functions

- a. The Group's commercial and regulatory functions are segregated to ensure the proper discharge of Bursa Malaysia's regulatory duties.

Both these functions operate independently of each other to ensure that business units are not in a position to influence any regulatory decision made by the Regulation unit. It is Bursa Malaysia's statutory duty to always act in the public's best interest, having particular regard for the need to protect investors. Public Interest Directors (PIDs) are appointed by the Minister of Finance to Bursa Malaysia's Board to ensure decisions are made in the public interest.

Regulatory Committees which have been set up to deliberate and decide on regulatory matters comprise independent individuals with significant and relevant industry experience, apart from Board members, to further ensure Bursa Malaysia upholds its obligation to safeguard public interest.

- b. Processes are established and set out in the Guidelines for Handling Conflicts of Interest (COI) to deal with any possible COI which may arise in the course of Bursa Malaysia performing its commercial or regulatory role.

### 2. Authority and Responsibility

- a. Certain responsibilities are delegated to Board Committees through clearly defined Terms of Reference (TOR) which are reviewed annually.
- b. The Authority Limits Document is reviewed from time to time to reflect the authority and authorisation limits of Management in all aspects of Bursa Malaysia's major business operations and regulatory functions.
- c. The Group's Management Governance Framework, comprising two committees for the governance function and three committees for the business operations function, has clearly defined TOR to enable good business and regulatory governance.

### 3. Planning, Monitoring and Reporting

- a. An annual planning and budgetary exercise is undertaken requiring all divisions to prepare business plans and budgets for the forthcoming year. These are deliberated upon and approved by the Board before implementation.

## Statement on Internal Control and Risk Management

- b. The Board is updated on the Group's performance at every meeting. The Group's Business Plan and Budget performance for the year is reviewed and deliberated upon by the Board on a half-yearly basis. Financial performance variances are presented to the Board on a quarterly basis.
- c. There is a regular and comprehensive flow of information to the Board and Management on all aspects of the Group's operations to facilitate the monitoring of performance against the Group's corporate strategy, business and regulatory plans. The Board also reviews and approves the Annual Regulatory Report, aimed at reporting to the Securities Commission (SC) under Section 16 of the CMSA, the extent to which Bursa Malaysia and its subsidiaries have complied with their duties and obligations under Sections 11 and 21 of the CMSA.
- d. The Director of Corporate Services who is also the Chief Financial Officer (CFO), is required to provide assurance to the AC that adequate processes and controls are in place for an effective and efficient financial statements close process in the preparation of financial statements for every quarter. The CFO also assures that appropriate accounting policies have been adopted and applied consistently to give a true and fair view of the state of affairs of the Group in compliance with the Malaysian Financial Reporting Standards, International Financial Reporting Standards and the requirements of the Companies Act 1965 of Malaysia.
- b. Annual on-site regulatory audits are conducted by the SC on the Group's operations to ensure compliance with its duties and obligations under the CMSA, as well as its policies and procedures.
- c. The yearly certification for Information Security Malaysia Standard, MS ISO/ IEC 27001:2007 Information Security Management Systems was carried out by CyberSecurity Malaysia.
- d. The Auditor Independence Policy requires the lead audit and engagement quality reviewing partners to be subject to a five-year rotation with a five-year cooling off period. An annual plan, encompassing planned statutory audit, recurring non-audit services and other anticipated non-audit services by the External Auditors, requires prior approval by the AC. The AC's approval is also required for unplanned non-audit services obtained from the current External Auditor.
- e. The GIA team is required to conduct an assessment of the internal control system pertaining to the processes of the relevant business units/functional groups which have a bearing on the financial information of Bursa Malaysia, to ensure the reliability and integrity of such information. The Senior Executive Vice President, Group Internal Audit who is also the Head of GIA is required to confirm the effective operation of process controls which support the preparation of the financial statements.

### 4. Policies and Procedures

- a. Clear, formalised and documented internal policies, standards and procedures are in place to ensure compliance with internal controls and relevant laws and regulations. A list of identified laws and regulations applicable to Bursa Malaysia is documented and maintained to facilitate compliance. Regular reviews are performed to ensure that documentation remains current and relevant. Common Group policies are available on Bursa Malaysia's intranet for easy access by staff.
- b. For significant system development/enhancement projects, whether involving new product/service launches or not, the GIA conducts a System Readiness Review to ensure that due processes have been complied with prior to the implementation or launch of the product/service.

### 5. Audits

- a. Through its internal audits, GIA assesses compliance with policies and procedures as well as relevant laws and regulations. In addition, it examines and evaluates the effectiveness and efficiency of the Group's internal control system using the risk-based audit approach.

- f. Besides the annual audit, the External Auditors are engaged to conduct a limited review of the quarterly financial results together with the cumulative quarters in accordance with International Standard on Review Engagements 2410 (ISRE 2410), "Review of Interim Financial Reporting Information Performed by the Independent Auditor of the Entity" for the first three quarters of the year.

### 6. Risk Management

- a. The Group has in place an ERM framework for managing risks affecting its business and operations. One of the key features of our ERM framework is the risk governance structure comprising three lines of defence with established and clear functional responsibilities and accountabilities for the management of risk.
- b. Senior Management, which includes Management Committee members and Divisional Heads, are the first line of defence and are accountable for all risks assumed under their respective areas of responsibility in line with the Risk Management Policy and Guidelines. This group is also responsible for creating a risk-awareness culture, which will ensure greater understanding of the importance of risk management and ensure that its principles are embedded in key operational processes and all projects.

## Statement on Internal Control and Risk Management

- c. The second line of defence is provided by the RMC, assisted by the Corporate Risk Management (CRM) team, which is collectively responsible for overseeing the risk management activities of the Group and ensuring compliance with, as well as effective implementation of risk policies and objectives. In discharging its oversight function, the RMC through its scheduled meetings in 2013 apprised and deliberated upon the efforts taken by Management to address and mitigate the key corporate risks faced by Bursa Malaysia. The RMC also reviewed the progress and status of ERM activities, provided feedback on revisions to the risk parameters as well as raised issues of concern for Management's attention.
- d. The third line of defence is the AC, assisted by GIA. It provides independent assurance of the adequacy and reliability of the risk management processes and system of internal control, as well as compliance with risk-related regulatory requirements.
- e. Within the framework, we have an established and structured process for the identification, assessment, communication, monitoring as well as continual review of risks and effectiveness of risk mitigation strategies and controls at the divisional and corporate levels. An automated system has also been implemented to standardise and facilitate the risk documentation and reporting process in regard to divisional risks.
- f. Under our framework, our level of risk tolerance is expressed through the use of a risk impact and likelihood matrix with an established risk tolerance boundary demarcating those risks that are deemed to have "exceeded risk tolerance" and those which have not. We have clear risk treatment guidance on the actions to be taken for the relevant risks.
- g. To ensure that our ERM framework remains sound and effective, in 2013 we implemented the following: a new set of quantitative and qualitative parameters for measuring different impact dimensions; additional quantitative parameters with probability for assessing likelihood; a revised heat map to align with the risk tolerance; and revised risk treatment guidance.
- h. Our significant risks for 2013, and the management of these risks are outlined below:

Business interruption risk

- i. A comprehensive Business Continuity Plan (BCP), including a Disaster Recovery Plan which is tested annually, is in place to ensure continuity of our business and technology operations. In 2013, Bursa Malaysia did not face any major business interruption.

- ii. In conjunction with the new Bursa Trade Securities (BTS2) systems roll out in December 2013, Bursa Malaysia conducted many tests/exercises internally as well as with industry participants. There were five BCP tests conducted in the month of September and October 2013 with industry participants, including the activation of alternate site and backup systems. This is to provide assurance that in the unlikely event that Bursa Malaysia encounters major business interruption, our alternate site and backup systems can be successfully activated to resume our critical business operations.
- iii. For the derivatives market which operates on the Globex platform, in addition to two successful BCP tests with some market participants on 11 May 2013 and 15 June 2013, the team successfully conducted an industrywide BCP test with market participants and CME Group Inc. (CME) on 13 July 2013. This exercise involved simulating the recovery and resumption of the derivatives critical functions/systems following the failure of the derivatives systems during trading hours.

Talent management risk

- i. In 2013, we undertook several initiatives to ensure accelerated growth in behavioural, technical and functional competencies with an emphasis on increasing our employee value proposition and motivating our employees. These initiatives included:
- The implementation of the revised Job Grading Structure & Rewards Structure to ensure internal and external equity as well as ensure that our human resource practices are fair as we strive to be on par with the financial institutions market. The revised structure also serves as a foundation to ensure more effective implementation of strategic human resource initiatives;
  - The introduction of new Behavioural Competencies (which have been mapped to human resource practices) have provided a more uniform view while serving as a basis for defining leadership and/or managerial capabilities. The Behavioural Competencies are critical in order to ensure effective development of our leadership pipeline;
  - The enhancement of technical competencies for Middle Management to increase the capacity and productivity of the talent within the organisation. Specific "technical skills" and knowledge are charted to depict the required competencies necessary to perform specific functions;
  - Leadership programmes focused on harnessing leadership capability as well as grooming future leaders;

## Statement on Internal Control and Risk Management

- Targeted employee engagement activities to foster camaraderie as well as create a harmonious and conducive working environment; and
  - More strategic employer-visibility initiatives, aimed at building employer branding among potential entry-level and professional-level employees.
- ii. All areas of human resources are essential to mitigate talent management risks and the outcomes of all initiatives taken are measured and monitored to determine the effectiveness and adequacy to tackle any area of risk.

### Competition risk

- i. To continue reinforcing Bursa Malaysia's position as a competitive marketplace, we implemented various business initiatives in 2013 to create a more facilitative trading environment, offer more tradable alternatives, reshape our market structure and framework, and become a regional marketplace with global access.

### Counterparty credit risk

- i. Bursa Malaysia has set in place robust risk management processes and procedures to manage counterparty/settlement risks and prevent any systemic impact on the market. In the area of managing counterparty/settlement risks, Bursa Malaysia Securities Clearing Sdn Bhd and Bursa Malaysia Derivatives Clearing Berhad act as the clearing houses for equities and derivatives trades respectively. These processes and procedures include:
- Daily mark to market positions, initial and variation margin requirements and collateral management;
  - Monitoring capital requirements and adequacy;
  - Managing credit exposures via price, trading, single client, equity and position limits;
  - Monitoring the financial health of the clearing settlement banks via the Risk Weighted Capital Ratio (RWCR) and credit ratings. The concentration risk is also monitored based on the Trading Clearing Participant's (TCP) or Clearing Participant's (CP) total trade settlement with the relevant clearing settlement banks;
  - Maintenance and stress-testing adequacy of the Clearing Guarantee Fund (CGF) and the Clearing Fund for equities and derivatives trading respectively; and
  - Conducting default drills to test the effectiveness of relevant rules and procedures.

- ii. In 2013, there were no settlement defaults by any TCP or CP, and neither the CGF nor the Clearing Fund was called upon.

- iii. We will continue to review and enhance the above processes and procedures in accordance with best practices and standards to ensure they are viable and robust.

### Regulatory risk

- i. The discharge of our regulatory functions is to ensure that our market continues to operate in an orderly and fair manner with sound investor protection. In regulating the market we adopt a five-pronged approach comprising development, supervision, engagement, enforcement and education. We also adopt a risk-based approach in regulating the market and seek to ensure that the key risk areas are identified, monitored and managed effectively.

## 7. Performance Measurement

- a. Key Performance Indicators (KPIs), which are based on the Corporate and Divisional Balanced Scorecard approach, are used to track and measure staff performance.
- b. Yearly employee engagement surveys and customer satisfaction surveys are conducted to gauge feedback on the effectiveness and efficiency of stakeholder engagement for continuous improvement.

## 8. Staff Competency

- a. Hiring and termination guidelines are in place while training and development programmes are conducted to ensure that staff are competent and kept up to date with the necessary competencies to carry out their respective duties towards achieving the Group's objectives.

## 9. Conduct of Staff

- a. A Code of Ethics is established for all employees, which defines the ethical standards and conduct of work required at Bursa Malaysia.
- b. Bursa Malaysia has a stand-alone Whistleblower Policy and Procedures (WPP) to provide an avenue for staff or any external party to report any breach or suspected breach of any law or regulation, including business principles and the Group's policies and guidelines, in a safe and confidential manner.

## Statement on Internal Control and Risk Management

- c. A Securities Transaction Policy is established to govern the securities transactions of the Group's staff. The policy prohibits employees from using unpublished price sensitive information obtained during the course of their work for personal gain or for the gain of other persons. Employees (including principal officers) are also not allowed to trade in the securities of Bursa Malaysia during the closed period, which is 30 calendar days preceding the announcement of Bursa Malaysia's quarterly and annual financial results.
- d. A Corporate Fraud Policy is established to aid in the detection and prevention of fraud and to promote consistent organisational behaviour and practices.
- e. A Confidentiality Policy is established for the management, control and protection of confidential information used by the Group to avoid leakage and improper use of such information.
- f. Management and employees at Grade E6 and above are required to declare and provide an update annually on assets acquired or disposal during the year.
- g. Segregation of duties is practised whereby conflicting tasks are assigned to different members of staff to reduce the scope for error and fraud.

## 10. Insurance

- a. Sufficient insurance coverage and physical safeguards on major assets are in place to ensure the Group's assets are adequately covered against any mishap that could result in material loss. A yearly policy renewal exercise is undertaken in which Management reviews the coverage based on the current fixed asset inventory and the respective net book values and "replacement value", i.e. the prevailing market price for the same or similar item, where applicable. The underwriter also assists by conducting a risk assessment, which helps Bursa Malaysia in assessing the adequacy of the intended coverage. There is also a yearly renewal exercise to ensure adequacy of the Group's professional indemnity insurance coverage.

## REVIEW OF THIS STATEMENT

Pursuant to paragraph 15.23 of the Main Market Listing Requirements, the External Auditors have reviewed this Statement for inclusion in the 2013 Annual Report, and reported to the Board that nothing has come to their attention that causes them to believe that the Statement is inconsistent with their understanding of the process adopted by the Board in reviewing the adequacy and integrity of the system of internal control and risk management. This statement was approved by the Board on 29 January 2014. GIA has reviewed this Statement and reported to the AC that, while it has addressed individual lapses in internal control during the course of its internal audit assignments for the year, it has not identified any circumstances which suggest any fundamental deficiencies in the Group's internal control and risk management system.

## CONCLUSION

The Board is of the view that the system of internal control and risk management is in place for the year under review, and up to the date of approval of this Statement, is sound and sufficient to safeguard shareholders' investments, the interests of customers, regulators, employees and other stakeholders, as well as the Group's assets.

The Board has received assurance from the CEO and CFO that the company's internal control and risk management system is operating adequately and effectively, in all material aspects, based on the framework adopted by the Group.