CONSULTATION PAPER

ON RISK MANAGEMENT AND INTERNAL CONTROL: REVIEW OF THE CORPORATE GOVERNANCE CODE AND CORPORATE GOVERNANCE REPORT

June 2014

Hong Kong Exchanges and Clearing Limited
香港交易及結算所有限公司

CONTENTS

Page No.

EXECUTIVE SUMMARY

1. This paper seeks comments on proposed changes to the Corporate Governance Code and Corporate Governance Report (the "**Code**") relating to internal controls (Sections C.2 and C.3).

2. The *Consultation Paper on Review of the Code on Corporate Governance Practices and Associated Listing Rules* published in December 2010 proposed substantive changes to the then Code on Corporate Governance Practices and related Rules. However, the review did not include the internal controls section of the Code as this was to be the subject of a separate consultation exercise in due course.

3. Since the introduction of the Code in 2005, corporate governance codes, rules and regulations in overseas jurisdictions have evolved and now place greater emphasis on risk management, rather than just on internal controls. The existing Code does not properly reflect this emphasis. The Code may also be improved to better delineate the roles and responsibilities of the board, the management and the internal audit function, as well as to set out the minimum specific disclosures that issuers should make so as to enhance transparency.

4. The proposals set out in this consultation paper are intended to:

   (a) emphasise that internal controls are an integrated part of risk management;

   (b) enhance accountability of the board, board committees and management by clearly defining their roles and responsibilities in risk management and internal controls;

   (c) improve transparency of the issuer's risk management and internal controls by upgrading the recommendation for issuers to disclose their policies, process, and details of the annual review carried out in respect of the effectiveness of the risk management and internal control systems; and

   (d) strengthen oversight of the risk management and internal control systems by upgrading the recommendation for issuers to have an internal audit function.

Risk management as an integral part of internal control

5. To place greater emphasis on the integration of risk management and internal control, we propose to add "risk management" to the title of Section C.2 of the Code and throughout Sections C.2 and C.3 of the Code where appropriate.

Responsibilities of the board and management

6. We propose to amend Principle C.2 to strengthen the role of risk management, while at the same time delineating the responsibilities of the board and management to enhance accountability.

7. We also propose to introduce a new Recommended Best Practice ("**RBP**", i.e. voluntary) to state that the board may disclose in the Corporate Governance Report that it has received assurance from management on the effectiveness of the issuer's risk management and internal control systems.

Annual review and disclosure in the Corporate Governance Report

8. We propose to amend an existing Code Provision ("**CP**", i.e. subject to "comply or explain") to clarify that, in addition to carrying out a review of the effectiveness of an issuer's risk management and internal control systems at least annually, the board should also oversee the issuer's systems on an ongoing basis. The aim is to emphasise that the board has an ongoing responsibility to oversee the issuer's risk management and internal control systems, and that this responsibility is not discharged by a one-off annual review.

9. We propose to upgrade to a CP a current RBP, which sets out the matters that the board's annual review should consider. The purpose is to highlight the importance of this provision and focus issuers' attention on the particular matters specified.

10. We also propose to upgrade to a CP a current RBP, which sets out the particular disclosures that issuers should make in their Corporate Governance Reports following the annual review (or more frequent reviews). The aim is to encourage more substantive, meaningful disclosure of issuers' risk management and internal control systems and the substance of their reviews. It also aims to facilitate comparability across issuers' Corporate Governance Reports by setting out the minimum information that issuers should disclose in relation to their risk management and internal control systems.

11. Further, we propose to amend the wording of this CP to streamline the requirements, remove ambiguous language, and clarify that the risk management and internal control systems are designed to manage rather than eliminate risks. We also propose to incorporate in this CP the existing recommendation that issuers disclose their procedures and internal controls for handling and disseminating inside information.

12. We propose to simplify and upgrade a number of the existing Recommended Disclosures relating to internal controls to Mandatory Disclosure Requirements. We also propose to remove some Recommended Disclosures on the basis that they are ambiguous.

13. Lastly, we propose to remove the RBP that "*issuers should ensure that their disclosures provide meaningful information and do not give a misleading impression*", as it seems obvious, redundant and oddly misplaced as an RBP.

Internal audit

14. We propose to upgrade to a CP the existing RBP for issuers without an internal audit function to review the need for one on an annual basis, and amend it to state that issuers should have an internal audit function.

15. We also propose introducing new Notes to this provision to clarify that:

    (a) the role of the internal audit function is to carry out the analysis and independent appraisal of the adequacy and effectiveness of an issuer's risk management and internal control systems; and

    (b) a group with multiple listed issuers may share group resources of the holding company to carry out the internal audit function for members of the group.

16. In connection with our proposals relating to the internal audit function, we also propose to amend an existing CP to state that the board's annual review should ensure the adequacy of resources, staff qualifications and experience, training programmes and budget of the issuer's internal audit function (in addition to its accounting and financial reporting functions).

Proposed amendments to the Code

17. The proposed amendments to the Code are set out in **Appendix I**.

18. We conducted a stakeholder consultation to solicit views from interested groups of practitioners and issuers on our proposals and the issues involved. We thank them for sharing with us their views and suggestions.

Next Step

19. Responses to this consultation paper and any other comments on related matters that might have an impact upon the changes proposed in this paper should be submitted to us by 31 August 2014. The Exchange, after reviewing and taking into account all the responses and comments submitted by 31 August 2014, will develop the consultation conclusions paper and work with the Securities and Futures Commission ("**SFC**") for any amendments to the Code.

HOW TO RESPOND TO THIS CONSULTATION PAPER

The Exchange, a wholly-owned subsidiary of HKEx, invites written comments on the changes proposed in this paper, or comments on related matters that might have an impact upon the changes proposed in this paper, on or before 31 August 2014. You can respond by completing the questionnaire which is available at: **http://www.hkex.com.hk/eng/newsconsul/mktconsul/Documents/cp201406q.doc**

Written comments may be sent:

By mail or hand delivery to

Corporate and Investor Communications Department
Hong Kong Exchanges and Clearing Limited
12/F, One International Finance Centre
1 Harbour View Street
Central
Hong Kong

Re: Consultation Paper on Risk Management and Internal Control: Review of the Corporate Governance Code and Corporate Governance Report

By fax to

(852) 2524-0149

By e-mail to

response@hkex.com.hk

Please mark in the subject line:

Re: CP on CG Review relating to Risk Management and Internal Control

Our submission enquiry number is (852) 2840-3844.

Respondents are reminded that the Exchange will publish responses on a named basis in the intended consultation conclusions. If you do not wish your name to be disclosed to members of the public, please state so when responding to this paper. Our policy on handling personal data is set out in **Appendix II**.

Submissions received during the consultation period by 31 August 2014 will be taken into account before the Exchange decides upon any appropriate further action. The Exchange will develop a consultation conclusions paper which will be published in due course and work with the SFC for any amendments to the Code.

DISCLAIMER

CHAPTER 1: INTRODUCTION

20. The Code was introduced in January 2005 and underwent substantive changes following the publication in December 2010 of the *Consultation Paper on Review of the Code on Corporate Governance Practices and Associated Listing Rules* and the resulting consultation conclusions. However, the consultation paper did not propose changes to the internal controls section of the Code as it was considered an area that warranted a separate review.

21. Internal control has been defined as: "*A process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance.*" [1]

22. We note from a review of global developments in this area that, since 2005, focus has shifted from internal control as a separate concept to internal control as an integrated part of risk management. Corporate governance codes, rules and regulations across overseas jurisdictions now generally put greater emphasis on risk management, rather than just on internal control.[2]

23. Many surveys conducted after the 2008 financial crisis have revealed that companies are placing increasing importance on the identification, understanding and management of risk.[3] Research indicates that, when properly implemented, risk management functions can effectively lower the risk levels of an organisation.[4] According to a survey conducted by an accountancy firm, more than 80% of institutional investors responded that they were willing to pay a premium for companies with good risk-management practices. Similarly, a majority of respondents to the same survey said that they had passed up the opportunity to invest in a company because they believed risk management was insufficient.[5]

24. It seems to be broadly recognised, not only abroad but also domestically, that internal control is most effective when it is integrated with risk management, and both are embedded in the governance processes of an organisation. Discussions during stakeholder consultation indicate that this is a commonly held view amongst groups of practitioners and issuers in Hong Kong. The concept of internal control as an

---

1 The Committee of Sponsoring Organizations of the Treadway Commission ("**COSO**") defines internal control in its "Internal Control – Integrated Framework" (known as the "**COSO Framework**").

2 Two of the most internationally recognised guidelines on internal control incorporate a risk management-based approach. These are the UK Financial Reporting Council's ("**UK FRC**") "Internal Control: Revised Guidance for Directors on the Combined Code" (often referred to as the "**Turnbull Guidance**") and the COSO Framework.

3 Ernst & Young, "Progress in financial services risk management-A survey of major financial institutions", (2012).

4 Andrew Ellul and Vijay Yerramilli, in "Stronger Risk Controls, Lower Risk: Evidence from US Bank Holding Companies", (2012), found that bank holding companies with strong risk management functions had lower enterprise risk. Gaizka Ormazabal Sanchez, in "Essays on Corporate Risk Governance", (2011), found that firms with an observable risk management function, chief risk officer, risk management policies, or other organisational structure related to risk oversight had less volatility during the financial crisis.

5 Ernst & Young, "Investors on risk. The need for transparency", (2006).

integrated part of risk management is not new to Hong Kong and the proposed amendments to the Code should bring the internal control section in line with existing market practices.

25. At the same time, we recognise that issuers vary significantly in their individual characteristics, size and complexity of operations, and the nature of the risks and challenges they face. In keeping with the philosophy behind the Code that one size does not fit all, the current proposals continue to give issuers flexibility by way of CPs and RBPs.

26. The changes proposed in this paper only relate to the Code. We would like to reiterate that CPs and RBPs are not Rules. To avoid "box-ticking", issuers must consider their own individual circumstances, the size and complexity of their operations and the nature of the risks and challenges they face. Deviations from the Code are acceptable if the issuer considers there are more suitable ways for it to comply with the Principles.

27. We examined the internal control practice of a number of other jurisdictions including the UK, Australia, Singapore, the US and Mainland China. The UK, Australia and Singapore have corporate governance codes that follow a similar "comply or explain" approach as our Code. The internal control practice in the US and Mainland China is quite different from ours, however. In the US, this area is mainly governed by the Sarbanes-Oxley Act ("**SOX**") (Section 404) and the rules implemented by the Securities and Exchange Commission ("**SEC**").[6] Mainland China's approach is more in line with the US model. The most important regulation in this area is the Basic Standard for Enterprise Internal Control ("**Basic Standard**"), often referred to as "China SOX" due to its similarities to the US SOX.

28. Chapter 2 of this paper discusses and seeks views on the proposals. We also seek views on a range of implementation dates for the proposed amendments.

29. While this consultation paper focuses on the Main Board Listing Rules, it applies equally to the GEM Listing Rules.

30. After reviewing and taking into account all the responses to this consultation paper submitted by 31 August 2014, the Exchange will develop a consultation conclusions paper and work with the SFC for any amendments to the Code. Revisions reflecting comments will be incorporated into the draft amendments of the Code.

[6] SEC Exchange Act of 1934 rule 13a-15 or rule 15d-15 (and item 308 of Regulation S-K).

CHAPTER 2: PROPOSALS

1. Risk management and internal control

Current requirement

31. The existing title of Section C.2 of the Code is simply "Internal controls".

Issue

32. One of the principal drivers behind the proposals in this paper is to emphasise that internal control is an integrated part of risk management. This should be reflected in the title of the internal controls section of the Code.

Requirements in other jurisdictions

33. Overseas jurisdictions such as the UK, Australia and Singapore incorporated "risk management" in the titles to internal controls section of their codes.

Consultation proposal

34. In light of the broader aim of our proposals to reflect the integration of risk management and internal control and the similar approach of other jurisdictions, we propose to amend the title of Section C.2 of our Code to "Risk management and internal control".

Consultation question

Question 1: Do you agree with our proposal to amend the title of Section C.2 of the Code to "Risk management and internal control"?

2. Responsibilities of the board and management

Current requirements

35. Principle C.2 states that the board should ensure that the issuer maintains sound and effective internal controls to safeguard shareholders' investment and the issuer's assets.

Issues

36. The Principle does not give sufficient weight to risks and risk management in relation to internal control. Nor does it set out the relationships between the issuer's objectives, the risks involved in achieving those objectives, and the internal control systems that mitigate those risks.

37. Further, both the board and management of an issuer have important roles to play in respect of an issuer's risk management and internal control systems. The delineation of their respective responsibilities is essential for ensuring the effectiveness of these systems.

38. Some of the shortcomings of risk management and internal control failures seen during the global financial crisis were attributed to risk not managed on an enterprise basis and not adjusted to corporate strategy. Risk managers were often separated from management and not regarded as an essential part of implementing the company's strategy. In some cases, boards were ignorant of the risk facing the company.[7] The Principle does not address these issues.

39. Another issue may be that the Principle – in specifying that internal controls are for the purpose of safeguarding shareholders' investment and the issuer's assets – is too narrow in scope. Effective risk management and internal control systems are fundamental to supporting the achievement of an issuer's objectives and creating, enhancing, and protecting stakeholder value. They enable an issuer to capitalise on opportunities while offsetting threats, and create a competitive advantage, as an issuer with effective controls can take on additional risk.[8] The broader purpose of risk management and internal control therefore goes beyond safeguarding shareholders' investment and the issuer's assets.

Requirements in other jurisdictions

40. The principles in this area vary across the corporate governance codes in the UK, Australia and Singapore.

41. The UK code[9] states that the board is responsible for determining the nature and extent of the significant risks[10] it is willing to take in achieving its strategic objectives, and that the board should maintain sound risk management and internal control systems.

42. Although the principle in the UK code does not address the role of management, the Turnbull Guidance (which provides guidance to issuers on how to comply with the risk management and internal control provisions of the UK code) does. It states that the role of management is to implement board policies on risk and control. In fulfilling its responsibilities, management should identify and evaluate the risks faced by the company for consideration by the board and design, operate and monitor a suitable system of internal control which implements the policies adopted by the board.[11]

---

7 Organisation for Economic Co-operation and Development, "Corporate Governance and the Financial Crisis – Conclusions and emerging good practices to enhance implementation of the principles", (2010).

8 International Federation of Accountants, "Evaluating and Improving Internal Control in Organizations", (2012), pages 4-5.

9 Principle C.2.

10 In November 2013, the UK FRC published a consultation paper entitled "Risk management, Internal Control and the Going Concern Basis of Accounting" ("**November 2013 consultation paper**"). It proposed to amend "significant risks" to "principal risks", to be consistent with the wording of the UK Companies Act. In April 2014, the UK FRC published a further consultation paper entitled "Proposed Revisions to the UK Corporate Governance Code", in which it proposed to proceed with this amendment ("**April 2014 consultation paper**").

11 Turnbull Guidance, paragraph 17. The UK FRC's November 2013 consultation paper proposed to amend this to state that it is the role of management, not the board, to implement and take day-to-day responsibility for board policies on risk and control. But the board needs to satisfy itself that management have understood the risks, implemented and monitored appropriate policies and controls, and are providing the board with timely information so that it can discharge its own responsibilities. In turn, management should

43. The Australian code states that a listed entity should establish a sound risk management framework and periodically review the effectiveness of that framework. Under the Australian code, the commentary to the principle delineates the respective responsibilities of an issuer's board and management.

44. The Singapore code states that the board is responsible for the governance of risk; further, the board should ensure that management maintains a sound system of risk management and internal controls to safeguard shareholders' interests and the company's assets, and should determine the nature and extent of the significant risks which it is willing to take in achieving its strategic objectives.

45. The Singapore code addresses in the principle the role of both the board and management. It elaborates further on the respective responsibilities of the board and management in a "comply or explain" provision, which states that the board should determine the company's levels of risk tolerance and risk policies, and oversee management in the design, implementation and monitoring of the risk management and internal control systems.[12] In addition, the board should (on a "comply or explain" basis) comment in the annual report on whether it has received assurance from the issuer's CEO and CFO regarding the effectiveness of the company's risk management and internal control systems.[13]

Consultation proposals

46. During discussions with stakeholder groups, a widely held view which emerged was that the respective responsibilities of the various bodies within an issuer, particularly the board, management and internal audit, should be clearly delineated.

47. To address the issues in paragraphs 36 to 38, we propose to amend the Principle to state that:

(a) the board is responsible for evaluating the risks it is willing to take in achieving the issuer's objectives and ensuring the establishment and maintenance of effective risk management and internal control systems; and

(b) the management is responsible for designing, implementing and monitoring the risk management and internal control systems. The management should also provide assurance to the board on the effectiveness of the systems.

48. The internal audit function (which is discussed in greater detail in section 4 below) provides support to the board and management, and the risk management and internal control systems by carrying out analysis and independent appraisal of the systems. The internal audit function is often referred to as the "third line of defence".[14]

---

ensure responsibilities are clearly established at all levels of the organisation (paragraph 21 of the proposed new guidance).

12 Singapore code, Guideline 11.1.

13 Singapore code, Guideline 11.3(b).

14 This is based on the Institute of Internal Auditors' Position Paper, "The Three Lines of Defense in Effective Risk Management and Control", (2013).

49. We also propose to remove from the Principle the wording "*to safeguard shareholders' investment and the issuer's assets*" to address the issue in paragraph 39. The scope of the amended Principle is wider and therefore encompasses the fact that this is a purpose of the risk management and internal control systems.

50. In connection with our proposal in paragraph 47(b) above, we propose to introduce a new RBP to state that the board may disclose in the Corporate Governance Report that it has received assurance from management on the effectiveness of the issuer's risk management and internal control systems.

Consultation questions

Question 2: *Do you agree with the proposed amendments to Principle C.2 to define the roles of the board and the management, and state that the management should provide assurance to the board on the effectiveness of the risk management systems*? *Is the intention of the proposed wording sufficiently clear?*

Question 3: *Do you agree with our proposal to introduce an amended RBP (C.2.6) to provide that the board may disclose in the Corporate Governance Report that it has received assurance from management on the effectiveness of the issuer's risk management and internal control systems? Is the intention of the proposed wording sufficiently clear?*

3. Annual review and disclosure in the Corporate Governance Report

Current requirements

51. CP C.2.1 states that the directors of an issuer should at least annually conduct a review of the effectiveness of the issuer's and its subsidiaries' internal control systems and report to shareholders that they have done so in their Corporate Governance Report. The review should cover all material controls, including financial, operational and compliance controls and risk management functions.

52. RBP C.2.3 sets out the particular matters that the board's annual review should consider:

(a) the changes since the last annual review in the nature and extent of significant risks;

(b) the scope and quality of management's ongoing monitoring of risks and the internal control system, and where applicable, the work of the internal audit function;

(c) the extent and frequency of communication of monitoring results to the board;

(d) significant control failings or weaknesses that have been identified during the period; and

(e) the effectiveness of the issuer's processes for financial reporting and Listing Rule compliance.

53. RBP C.2.4 states that issuers should disclose, in the Corporate Governance Report, a narrative statement on how they have complied with the internal control code provisions during the reporting period. It also sets out the particular disclosures that issuers should make, including:

(a) the process used to identify, evaluate and manage significant risks;

(b) additional information to explain the main features of the risk management and internal control systems;

(c) an acknowledgement by the board that it is responsible for the internal control system and reviewing its effectiveness;

(d) the process used to review the effectiveness of the internal control system; and

(e) the process used to resolve material internal control defects.

54. Section S. of the Code sets out additional Recommended Disclosures that issuers are encouraged to make in their Corporate Governance Reports in respect of their internal controls.

Issues

Inadequate disclosure relating to annual review

55. The internal control provisions of the Code have been criticised as being ineffective, in that it is voluntary for issuers to disclose details of their annual reviews. Critics question the value of having a CP (CP C.2.1) that requires the issuer (on a "comply or explain" basis) to report to shareholders in the Corporate Governance Report that it has undertaken such a review, when it is voluntary for the issuer to provide details (such as the specific matters under RBP C.2.4 and the Recommended Disclosures under Section S.). Without this information, it is difficult for investors and other stakeholders to assess whether the issuer's management and board have properly discharged their duties to maintain a sound internal control system. It also fails to encourage or exert pressure on issuers to adopt a reasonably sound internal control system.

Matters to be considered at annual review

56. RBP C.2.3 contains important and helpful guidance on the risk management and internal control matters issuers should consider in their annual review. However, as an RBP, this provision lacks authority and issuers therefore might not give them sufficient consideration when conducting their annual review.

Ongoing process as opposed to one-off review

57. Also in relation to CP C.2.1, some stakeholders commented that the board does not simply discharge its duties relating to an issuer's risk management and internal

control systems by way of a one-off annual review. They suggested that emphasis be placed on the ongoing nature of the board's responsibilities in this regard.

Requirements in other jurisdictions

Disclosure relating to annual review and matters to be considered

58. The corporate governance codes in the UK, Australia and Singapore all require the board (on a "comply or explain" basis) to at least annually conduct a review of the effectiveness of the company's risk management and internal control systems, and report to shareholders that they have done so.[15]

59. In the UK, the Turnbull Guidance provides guidance on the particular matters to be considered in the board's annual review.[16] It also provides additional direction on the disclosures the board should include in its narrative statement in the annual report on how it has complied with the risk management and internal control provisions of the UK code.[17] This should include, among other disclosures, a summary of the process the board has applied in conducting its annual review and a confirmation that necessary actions have been taken to remedy any failings or weaknesses identified from the review.[18]

60. Also, the UK's Disclosure and Transparency Rules ("**DTR**") require the corporate governance statement in the annual report to include a description of the main features of the company's internal control and risk management systems in relation to the financial reporting process.[19] They also require an entity which must prepare a group directors' report[20] to include in that report a description of the main features of the group's internal control and risk management systems in relation to the process for preparing consolidated accounts. [21]

61. Further, the UK FRC's November 2013 consultation paper proposed a new CP in the UK code, which would require the board (on a "comply or explain" basis) to carry out a robust assessment of the principal risks facing the issuer, confirm in the annual report that it has carried out such an assessment and explain how the principal risks are being managed or mitigated. [22]

---

15 UK code, CP C.2.1. This will become CP C.2.3, if the proposals in the UK FRC's April 2014 consultation paper are adopted. Australian code, Recommendation 7.2 and Singapore code, Guidelines 11.2 and 11.3.

16 Turnbull Guidance, paragraph 31. Under the revised guidance proposed in the UK FRC's November 2013 consultation paper, this guidance is retained under paragraph 40.

17 Turnbull Guidance, paragraphs 33 to 38. Under the revised guidance proposed in the UK FRC's November 2013 consultation paper, these disclosure guidelines are retained under paragraphs 54 to 59.

18 Turnbull Guidance, paragraph 36 (paragraph 58 under the revised guidance proposed in the UK FRC's November 2013 consultation paper).

19 DTR 7.2.5 R.

20 As required under section 415(2) of the UK Companies Act 2006, for a financial year in which: (a) the company is a parent company; and (b) the directors of the company prepare group accounts, the directors' report must be a consolidated report relating to the undertakings included in the consolidation.

21 DTR 7.2.10 R.

22 The UK FRC in its April 2014 consultation paper proposed to adopt this as new CP C.2.1.

62. The new edition of the Australian code adopts a similar provision[23] to CP C.2.1 in our Code. In the commentary, the new Australian code provides that the issuer should also disclose any insights it has gained from the review and any changes it has made to its risk management framework as a result.

63. The Singapore code requires (on a "comply or explain" basis) the board to comment on the adequacy and effectiveness of the internal controls (including financial, operational, compliance and information technology controls) and risk management systems in the company's annual report. The provision goes on to say that the board's commentary should include information needed by stakeholders to make an informed assessment of the company's internal control and risk management systems.[24]

64. Under the US rules, each annual report must contain an internal control report, which must include an assessment by management of the effectiveness of the company's internal control structure and procedures for financial reporting. Further, the accounting firm that prepares the company's audit report must issue an attestation report to express an opinion directly on the effectiveness of the company's internal control over financial reporting.[25]

65. Mainland China's Basic Standard requires Chinese enterprises[26] to establish, evaluate and assess the effectiveness of their internal controls, following which they must disclose their conclusions in an annual self-assessment report. Companies are also required to undergo an external audit review of their internal control systems and disclose the results of that review in addition to their self-assessment reports.[27]

Ongoing process as opposed to one-off review

66. The UK FRC proposed in its November 2013 consultation paper amendments to its existing CP C.2.1 to clarify that the board has a responsibility to monitor the risk management and internal control systems on an ongoing basis, and should not rely solely on an annual review.[28] This was considered uncontentious by the respondents to the UK FRC's consultation, who considered it a useful clarification of the intent underlying the current wording of the UK code. [29]

---

23 Recommendation 7.2 under the third edition of the Australian code.

24 Singapore code, Guidelines 11.2 and 11.3.

25 The requirement for the auditor's attestation report does not apply to "non-accelerated" filers (i.e. companies with an aggregate worldwide market value of the voting and non-voting common equity held by non-affiliates under US$75 million (HK$582 million)).

26 All listed companies are required to comply with the Basic Standard, while unlisted large and medium-sized Chinese enterprises are encouraged to adopt it.

27 Article 46 of the Basic Standard and the "Application Guidelines for Enterprise Internal Control", "Guidelines for Assessment of Enterprise internal Control" and "Guidelines for Audit of Enterprise Internal Control" (collectively referred to as the "**Implementation Guidelines**").

28 The existing CP C.2.1 states that "the board should, at least annually, conduct a review of the effectiveness of the company's risk management and internal control systems and should report to shareholders that they have done so."

29 The UK FRC proposed in its April 2014 consultation paper to proceed with this amendment to the UK code. Assuming the proposal is adopted, the existing CP C.2.1 will become CP C.2.3 of the UK code and be amended to state that "the board should monitor the company's risk management and internal control systems and, at least annually, carry out a review of their effectiveness, and report on that review in the annual report. The monitoring and review should cover all material controls, including financial,

67. Moreover, the COSO Framework states that "monitoring activities" should form an integrated component of internal control. Monitoring activities include ongoing evaluations or separate evaluations conducted periodically (or a combination of the two) to ascertain whether the company's internal controls are present and functioning.[30]

Consultation proposals

Disclosure relating to annual review and matters to be considered

68. We propose to upgrade to a CP the existing RBP C.2.3, which sets out the matters that the board's annual review should consider. The purpose of this proposal is to highlight the importance of this provision and focus issuers' attention on the particular matters specified therein.

69. We also propose to upgrade RBP C.2.4 to a CP, which sets out the particular disclosures that issuers should make in their Corporate Governance Reports in relation to how they have complied with the internal control CPs during the reporting period. Under the existing Code, the board is only obliged (on a "comply or explain" basis) to disclose in the Corporate Governance Report that it has conducted an annual review of the issuer's internal control systems (in accordance with CP C.2.1). However, our findings in our *Analysis of Corporate Governance Practice Disclosure in 2012 Annual Reports* indicate that issuers' compliance with RBPs generally tends to be low.[31] This proposal aims to encourage more substantive, meaningful disclosure of issuers' risk management and internal control systems and the substance of their annual reviews. It also aims to facilitate comparability across issuers' Corporate Governance Reports by setting out the minimum information that issuers should disclose in relation to their risk management and internal control systems.

70. Further, we propose to amend the wording of proposed CP C.2.4 to incorporate risk management where appropriate, to simplify the requirements and remove ambiguous language, and to make clear that the risk management and internal control systems are designed to manage rather than eliminate risks. Further, we propose to upgrade the existing recommendation that issuers disclose their procedures and internal controls for handling and disseminating inside information (existing Section S., paragraph (a)(ii)), amend it to include the handling of "other regulatory compliance risks", and move it into a new sub-paragraph under proposed CP C.2.4 (CP C.2.4(e)).

71. Consequent to the proposal to upgrade RBP C.2.4, we propose to upgrade to Mandatory Disclosures most of the existing Recommended Disclosures in relation to internal controls (Section S.) and amend the title of this section to incorporate "risk management". In summary, this will require issuers to disclose:

    (a) whether they have an internal audit function;

---

operational and compliance controls."

30 See COSO Framework Executive Summary.

31 We found that only 2.2% of the 1,083 issuers whose annual reports we reviewed disclosed whether they had complied with the RBPs in the Code.

(b) how often the risk management and internal control systems are reviewed, the period covered, and where an issuer has not conducted a review during the year, an explanation why not;

(c) a statement that a review of the effectiveness of the risk management and internal control systems has been conducted and whether the issuer considers them effective and adequate; and

(d) significant views or proposals put forward by the audit committee.

Ongoing process as opposed to one-off review

72. We propose to amend the existing CP C.2.1 to add that the board should oversee the issuer's risk management and internal control systems on an ongoing basis. It aims to emphasise that the board has an ongoing responsibility to oversee the issuer's risk management and internal control systems, and that this responsibility is not discharged by a one-off annual review.

73. The proposed amendment does not seek to impose any additional obligation on issuers. Rather, it aims to clarify the intent underlying the existing wording of CP C.2.1. This approach is also consistent with that of the UK (see paragraph 66 above).

Other amendments

74. We propose amending CP C.2.1 to state that the board, rather than the directors, is responsible for overseeing the issuer's risk management and internal control systems, etc. This proposal does not represent a change in policy direction or intention. The board, as before, remains collectively responsible. The proposed change is only to make the language of this CP consistent with that of the other provisions in this section of the Code.

75. We propose to move the existing recommendation that issuers disclose details of any significant areas of concern (Section S., paragraph (a)(ix)) to a new RBP C.2.7. We also propose to amend the wording of this provision to widen its application so that it no longer restricts disclosure to significant areas of concerns "which may affect shareholders". Compliance with this provision will continue to be voluntary.

76. In addition, we propose to remove the RBP that issuers should ensure their disclosures provide meaningful information and do not give a misleading impression (RBP C.2.5), as it seems obvious, redundant and oddly misplaced as an RBP. Our proposals to upgrade the provisions relating to disclosure in the Corporate Governance Report should help to ensure that issuers provide meaningful information on their risk management and internal control systems.

77. On the basis that they are ambiguous, we propose to remove a couple of items under the "Recommended Disclosures".[32]

[32] Section S., paragraphs (a)(i) (an explanation of how the internal control system has been defined for the issuer) and (a)(vii) (the directors' criteria for assessing the effectiveness of the internal control system).

Consultation questions

Question 4: *Do you agree with the proposed amendments to CP C.2.1 to state that the board should oversee the issuer's risk management and internal control systems on an ongoing basis? Is the intention of the proposed wording sufficiently clear?*

Question 5: *Do you agree with our proposal to upgrade to a CP the existing RBP C.2.3, which sets out the matters that the board's annual review should consider?*

Question 6: *Do you agree with our proposal to upgrade to a CP the existing RBP C.2.4, which sets out the particular disclosures that issuers should make in their Corporate Governance Reports in relation to how they have complied with the internal control CPs during the reporting period?*

Question 7: *Do you agree with our proposal to amend the wording of proposed CP C.2.4 to simplify the requirements and remove ambiguous language, and to make clear that the risk management and internal control systems are designed to manage rather than eliminate risks? Is the intention of the proposed wording sufficiently clear?*

Question 8: *In relation to proposed CP C.2.4, do you agree with our proposal to upgrade the existing recommendation that issuers disclose their procedures and internal controls for handling and disseminating inside information (Section S., paragraph (a)(ii)), and amend it to include the handling of "other regulatory compliance risks"?*

Question 9: *Do you agree with our proposal to upgrade to Mandatory Disclosures most of the existing Recommended Disclosures in relation to internal controls (Section S.), as described in paragraph 71 of this paper?*

Question 10: *Do you agree with our proposal to move the existing recommendation that issuers disclose details of any significant areas of concern (Section S., paragraph (a)(ix)) to a new RBP C.2.7, and to amend the provision to widen its application by removing the reference to areas of concern "which may affect shareholders"?*

Question 11: *Do you agree with our proposal to remove RBP C.2.5, which states that issuers should ensure their disclosures provide meaningful information and do not give a misleading impression?*

Question 12: *Do you agree with our proposals to remove the recommendations that issuers include in their Corporate Governance Reports:*

(a) *an explanation of how the internal control system has been defined for them (Section S., paragraph (a)(i)); and*

(b) the directors' criteria for assessing the effectiveness of the internal control system (Section S., paragraph (a)(vii))?

4. Internal audit

Current requirements

78. Under the existing Code, it is an RBP for issuers without an internal audit function to review the need for one on an annual basis and disclose the outcome of this review in the Corporate Governance Report (RBP C.2.6).

Issues

79. Currently, it is voluntary for issuers to have an internal audit function. However, the internal audit function plays an important role in ensuring the effectiveness of an issuer's risk management and internal control systems. As discussed in paragraph 48 above, it is often seen as the third line of defence. It helps the issuer to carry out an analysis and independent appraisal of the adequacy and effectiveness of the issuer's systems and functions, and it may serve as a check on the first and second lines of defence. Some have suggested that it may be impossible to have an effective internal control system without an internal audit function.

80. While the internal audit function was broadly recognised during stakeholder consultation as an important aspect of an issuer's risk management and internal control systems, there were concerns that there may be a limited supply of qualified, experienced internal audit personnel. In addition, some issuers might face resource constraints and may struggle to hire new staff to carry out the internal audit function. In this connection, there may be concerns around the independence of the internal audit function, as some issuers may utilise existing staff involved with preparing the issuer's financial statements to conduct the internal audit as well.

Requirements in other jurisdictions

81. Each of the UK, Australia and Singapore codes contains a provision that requires issuers (on a "comply or explain" basis) to maintain an internal audit function.

82. The UK code requires that if the issuer does not have an internal audit function, the audit committee should consider annually whether there is a need for one and make a recommendation to the board, and the reasons for the absence of such a function should be explained in the annual report.[33]

83. Under the Australian code, the issuer should disclose how the internal audit function is structured and what role it performs; or, if it does not have such a function, it should disclose the processes it employs for evaluating and continually improving the effectiveness of its risk management and internal control processes.[34]

---

[33] UK code, CP C.3.6.

[34] Australian code, Recommendation 7.3. Note that the internal audit provision was only upgraded to a "comply or explain" level of obligation in the most recent (third) edition of the Australian code.

84. The Singapore code states that issuers should establish an effective internal audit function that is adequately resourced and independent of the activities it audits.[35]

85. In the US, under the New York Stock Exchange ("**NYSE**") Corporate Governance Standards,[36] it is mandatory for issuers to maintain an internal audit function to provide management and the audit committee with ongoing assessments of their risk management processes and system of internal control.[37]

86. Under the Code of Corporate Governance issued by the China Securities Regulatory Commission ("**PRC code**"), the internal audit function is addressed only in relation to the main duties of the audit committee, which include reviewing the internal audit system and its execution, and overseeing the interaction between the issuer's internal and external auditing institutions.[38]

Consultation proposals

87. To address the issues set out in paragraph 79, we propose to upgrade RBP C.2.6 to a CP and amend it to state that issuers should have an internal audit function, and those without an internal audit function should review the need for one on an annual basis and disclose the reasons for the absence of such function in the Corporate Governance Report.

88. In respect of the issue set out in paragraph 80, we understand that in practice it is common for issuers to engage external service providers to perform the internal audit function. Discussions with practitioners indicate that in most overseas jurisdictions (including the UK, Australia, Singapore and the US) issuers are considered to be in compliance with the relevant code provision or rule if they opt to outsource their internal audit functions. As such, we are of the view that compliance with the proposed CP may be achieved either by way of an in-house internal audit function or an outsourced one.

89. We also propose introducing new Notes to this provision to clarify that:

(a) the role of the internal audit function is to carry out the analysis and independent appraisal of the adequacy and effectiveness of an issuer's risk management and internal control systems; and

(b) a group with multiple listed issuers may share group resources of the holding company to carry out the internal audit function for members of the group.

90. In connection with our proposals relating to the internal audit function, we also propose to amend the existing CP C.2.2 to state that the board's annual review should ensure the adequacy of resources, staff qualifications and experience, training

---

35 Singapore code, Principle 13 and Guidelines 13.1 to 13.5.

36 The NYSE Corporate Governance Standards are set out in the NYSE Listed Company Manual, Section 303A.00.

37 NYSE Listed Company Manual, Section 303A.07(c) and related commentary.

38 The provisions of the PRC Code must be incorporated in listed issuers' articles of association or rules of governance.

programmes and budget of the issuer's internal audit function (in addition to its accounting and financial reporting functions).

91. Our findings indicate that many of our issuers already have an internal audit function. According to our *Analysis of Corporate Governance Practice Disclosure in 2012 Annual Reports*, 51% of issuers disclosed they had one. This is likely an underestimation of the actual percentage of issuers with an internal audit function, as it is only an RBP for them to disclose this in their Corporate Governance Reports. Compared to the overall RBP compliance rate of 2.2% (see Note 31), this 51% compliance rate is very high and indicates that issuers are likely ready for this provision to be upgraded to a CP.

Consultation questions

Question 13: Do you agree with our proposal to upgrade RBP C.2.6 to a CP (re-numbered C.2.5) and amend it to state that an issuer should have an internal audit function, and issuers without an internal audit function should review the need for one on an annual basis and disclose the reasons for the absence of such function in the Corporate Governance Report? Is the intention of the proposed wording sufficiently clear?

Question 14: Do you agree with our proposal to introduce the new Notes as described in paragraph 89 of this paper? Is the intention of the proposed wording sufficiently clear?

Question 15: Do you agree with our proposal to amend the existing CP C.2.2 to state that the board's annual review should ensure the adequacy of resources, staff qualifications and experience, training programmes and budget of the issuer's internal audit function (in addition to its accounting and financial reporting functions)?

5. Audit Committee's role

Current requirements

92. Under the current provisions of the Code, the audit committee already has certain risk management and internal control responsibilities. For example, under CP C.3.3 (the audit committee's terms of reference), it is responsible for overseeing the issuer's financial reporting system and internal control procedures. This includes the responsibility to review the issuer's financial controls, internal control and risk management systems (CP C.3.3(f)).

93. Also, where an internal audit function exists, the audit committee is responsible for:

(a) ensuring co-ordination between the internal and external auditors;

(b) ensuring that the internal audit function is adequately resourced and has appropriate standing within the issuer; and

(c) reviewing and monitoring its effectiveness (CP C.3.3(i)).

Issues

94. Our existing approach is consistent with that of most overseas jurisdictions that we have examined. However, there are concerns in the market that the audit committee's duties are already quite extensive. Some have suggested that risk management should not be put under the remit of the audit committee, as this could stretch its resources and divert its focus.

95. A separate board risk committee could be an effective way to focus issuers on risk management and internal control matters, while at the same time addressing the concern that the audit committee is over-burdened. However, during soft consultation, it became evident that this should perhaps be a matter left to issuers to decide for themselves. For some issuers, it may be appropriate to establish a risk committee. But for others (particularly smaller issuers with fewer directors), establishing another board committee may be a strain on their resources and, in any event, the committee would likely comprise the same directors that sit on all the other board committees.

Requirements in other jurisdictions

96. As noted above, most jurisdictions assign risk management and internal control related duties to the audit committee. Under the UK code, the audit committee is responsible for reviewing the issuer's internal control and risk management systems, and monitoring and reviewing the effectiveness of the issuer's internal audit function. However, the UK code acknowledges that issuers may have a separate board committee to review their internal control and risk management systems.[39]

97. The Australian code contains a new "comply or explain" provision which states that issuers should establish a risk committee (which may be part of the audit committee), or disclose the processes they employ for identifying, measuring, monitoring and managing risks if they do not have such a committee.[40]

98. The Singapore code provides that the audit committee is responsible for:

(a) reviewing and reporting to the board on the adequacy and effectiveness of the company's internal controls, including financial, operational, compliance and information technology controls; and

(b) reviewing the effectiveness of the company's internal audit function.[41]

99. The Singapore code also contains a voluntary provision which states that the board may establish a separate risk committee, or otherwise assess appropriate means to assist it in carrying out its responsibility of overseeing the company's risk management framework and policies.[42]

---

39 UK code, CP C.3.2.

40 Australian code, Recommendation 7.1. Note that the risk committee provision was only upgraded to a "comply or explain" level of obligation in the most recent (third) edition of the Australian code.

41 Singapore code, Guideline 12.4(b) and (c).

42 Singapore code, Guideline 11.4.

100. Under the NYSE Corporate Governance Standards,[43] the duties and responsibilities of the audit committee include discussing policies relating to risk assessment and risk management. In addition, the audit committee must review major issues regarding accounting principles and financial statement presentations, including issues relating to the adequacy of the issuer's internal controls and any special audit steps adopted in light of material control deficiencies.[44]

101. In Mainland China, the PRC code addresses internal control only in the context of the audit committee's duties. These include reviewing the issuer's internal audit system and its execution (as noted in paragraph 86 above), and monitoring the company's internal control system.[45]

Consultation proposals

102. We propose to amend the audit committee Principle (Principle C.3) and CP C.3.3 to also incorporate risk management, where appropriate. This will ensure consistency throughout the internal controls and audit committee sections of the Code.

103. We do not, however, propose to amend the Code to provide for the establishment of a separate board risk committee, as we are of the view that this matter should be left to issuers to decide for themselves.

Consultation questions

Question 16: Do you agree with our proposal to amend Principle C.3 in respect of audit committees and CP C.3.3 in respect of their terms of reference to incorporate "risk management" where appropriate?

Question 17: Do you agree that the matter of establishing a separate board risk committee should be left to issuers to decide in accordance with their own circumstances?

Implementation Date

Question 18: What would be an appropriate period of time between the publication of the consultation conclusions and the implementation of the amendments set out in this paper?

(a) Six months;

(b) nine months;

(c) 12 months; or

(d) others (please specify).

---

43 NYSE Listed Company Manual, Section 303A.00 (see Note 36 above).

44 NYSE Listed Company Manual, Section 303A.07(b)(iii)(D) and General Commentary to Section 303A.07(b).

45 PRC code, Article 54.

APPENDIX I: PROPOSED AMENDMENTS TO THE CORPORATE GOVERNANCE CODE AND CORPORATE GOVERNANCE REPORT

(Unless otherwise specified, set out below are the draft Main Board Rule amendments. The Exchange proposes to make equivalent amendments to the GEM Rules.)

The marked-up parts represent the proposed amendments to the Main Board Rules.

Appendix 14

CORPORATE GOVERNANCE CODE AND CORPORATE GOVERNANCE REPORT

…

PRINCIPLES OF GOOD GOVERNANCE, CODE PROVISIONS AND RECOMMENDED BEST PRACTICES

…

C. ACCOUNTABILITY AND AUDIT

…

C.2 Risk management and internal controls

Principle

The board ~~should ensure~~ is responsible for evaluating the nature and extent of the risks it is willing to take in achieving the issuer's strategic objectives, and ensuring that the issuer establishes and maintains ~~sound~~ appropriate and effective risk management and internal control~~s~~ systems ~~to safeguard shareholders' investment and the issuer's assets~~. The board should oversee management in the design, implementation and monitoring of the risk management and internal control systems, and management should provide assurance to the board on the effectiveness of these systems.

Code Provisions

C.2.1 The ~~directors~~ board should oversee the issuer's risk management and internal control systems on an ongoing basis, ensure that ~~at least annually conduct~~ a review of the effectiveness of the ~~issuers'~~ issuer's and its subsidiaries' risk management and internal control systems has been conducted at least annually and report to shareholders that ~~they~~ it

~~have~~ has done so in ~~their~~ its Corporate Governance Report. The review should cover all material controls, including financial, operational and compliance controls ~~and risk management functions~~.

C.2.2 The board's annual review should, in particular, ~~consider~~ ensure the adequacy of resources, staff qualifications and experience, training programmes and budget of the issuer's accounting, internal audit and financial reporting functions.

~~**Recommended Best Practices**~~

C.2.3 The board's annual review should, in particular, consider:

(a) the changes, since the last annual review, in the nature and extent of significant risks, and the issuer's ability to respond to changes in its business and the external environment;

(b) the scope and quality of management's ongoing monitoring of risks and of the internal control systems, and where applicable, the work of its internal audit function and other assurance providers;

(c) the extent and frequency of communication of monitoring results to the board (or board committee(s)) which enables it to assess control of the issuer and the effectiveness of risk management;

(d) significant control failings or weaknesses that have been identified during the period. Also, the extent to which they have resulted in unforeseen outcomes or contingencies that have had, could have had, or may in the future have, a material impact on the issuer's financial performance or condition; and

(e) the effectiveness of the issuer's processes for financial reporting and Listing Rule compliance.

C.2.4 Issuers should disclose, in the Corporate Governance Report, a narrative statement on how they have complied with the risk management and internal control code provisions during the reporting period. ~~The disclosures should also include~~ In particular, they should disclose:

(a) the process used to identify, evaluate and manage significant risks;

(b) ~~additional information to explain~~ the main features of ~~its~~ the risk management ~~processes~~ and internal control systems;

(c) an acknowledgement by the board that it is responsible for the risk management and internal control systems and reviewing ~~its~~

their effectiveness. It should also explain that such systems are designed to manage rather than eliminate the risk of failure to achieve business objectives, and can only provide reasonable and not absolute assurance against material misstatement or loss;

(d) the process used to review the effectiveness of the risk management and internal control systems~~;~~ and

~~(e) the process used~~ to resolve material internal control defects ~~for any significant problems disclosed in its annual reports and accounts.~~; and

(e) the procedures and internal controls for the handling and dissemination of inside information, and for the handling of other regulatory compliance risks. *[Moved from Recommended Disclosures Section S., paragraph (a)(ii).]*

C.2.5 ~~Issuers should ensure that their disclosures provide meaningful information and do not give a misleading impression.~~ The issuer should have an internal audit function. Issuers without an internal audit function should review the need for one on an annual basis and should disclose the reasons for the absence of such a function in the Corporate Governance Report.

Notes:

1 An internal audit function generally carries out the analysis and independent appraisal of the adequacy and effectiveness of the issuer's risk management and internal control systems.

2 A group with multiple listed issuers may share group resources of the holding company to carry out the internal audit function for members of the group.

Recommended Best Practices

~~C.2.6 Issuers without an internal audit function should review the need for one on an annual basis and should disclose the outcome of this review in the Corporate Governance Report.~~ *[Moved to proposed CP C.2.5.]*

C.2.6 The board may disclose in the Corporate Governance Report that it has received assurance from management on the effectiveness of the issuer's risk management and internal control systems.

C.2.7 The board may disclose in the Corporate Governance Report details of any significant areas of concern. *[Moved from Recommended Disclosures Section S., paragraph (a)(ix).]*

C.3 Audit Committee

Principle

The board should establish formal and transparent arrangements to consider how it will apply financial reporting, risk management and internal control principles and maintain an appropriate relationship with the issuer's auditors. The audit committee established under the Listing Rules should have clear terms of reference.

Code Provisions

…

C.3.3 The audit committee's terms of reference should include at least:

Relationship with the issuer's auditors

(a) …

…

(e) …

…

Oversight of the issuer's financial reporting system, risk management and internal control systems ~~procedures~~

(f) to review the issuer's financial controls, and risk management and internal control ~~and risk management~~ systems;

(g) to discuss the risk management and internal control systems with management to ensure that management has performed its duty to have ~~an~~ effective ~~internal control~~ systems. This discussion should include the adequacy of resources, staff qualifications and experience, training programmes and budget of the issuer's accounting and financial reporting function;

(h) to consider major investigation findings on risk management and internal control matters as delegated by the board or on its own initiative and management's response to these findings;

(i) where an internal audit function exists, to ensure co-ordination between the internal and external auditors, and to ensure that the internal audit function is adequately resourced and has appropriate standing within the issuer, and to review and monitor its effectiveness;

…

CORPORATE GOVERNANCE REPORT

MANDATORY DISCLOSURE REQUIREMENTS

…

P. INVESTOR RELATIONS

Any significant changes in the issuer's constitutional documents during the year.

~~RECOMMENDED DISCLOSURES~~

~~S.~~Q. RISK MANAGEMENT AND INTERNAL CONTROL~~S~~

~~(a)~~ Where an issuer includes a directors' statement that ~~they have~~ it has conducted a review of its risk management and internal control systems in the annual report under ~~paragraph~~ code provision C.2.1, it ~~is encouraged to~~ must disclose the following:

(a) ~~(i) an explanation of how the internal control system has been defined for the issuer;~~

~~(ii) procedures and internal controls for the handling and dissemination of inside information;~~ *[Moved to proposed CP C.2.4(e).]*

~~(iii)~~ whether the issuer has an internal audit function;

~~(iv) the outcome of the review of the need for an internal audit function conducted, on an annual basis, by an issuer without one (C.2.6 of the Code);~~ *[Duplicates proposed CP C.2.5.]*

(b) ~~(v)~~ how often the risk management and internal control~~s~~ systems are reviewed, the period covered, and where an issuer has not conducted a review during the year, an explanation why not;

(c) ~~(vi)~~ a statement that a ~~the directors have reviewed~~ review of the effectiveness of the risk management and internal control systems has been conducted and whether ~~they~~ the issuer considers them effective and adequate; and

~~(vii) directors' criteria for assessing the effectiveness of the internal control system;~~

~~(viii) the period covered by the review;~~

~~(ix) details of any significant areas of concern which may affect shareholders;~~ *[Moved to proposed RBP C.2.7.]*

(d) ~~(x)~~ significant views or proposals put forward by the audit committee.

~~(xi) where an issuer has not conducted a review of its internal control system during the year, an explanation why not; and~~ *[Moved to proposed Mandatory Disclosure Requirements, Section Q., paragraph (b).]*

~~(b) a narrative statement explaining how the issuer has complied with the code provisions on internal control during the reporting period.~~ *[Duplicates proposed CP C.2.4.]*

RECOMMENDED DISCLOSURES

…

~~Q.~~R. SHARE INTERESTS OF SENIOR MANAGEMENT

…

~~R.~~S. INVESTOR RELATIONS

…

~~S. INTERNAL CONTROLS~~

~~…~~

[Moved to proposed Mandatory Disclosure Requirements, Section Q.]

T. MANAGEMENT FUNCTIONS

…

APPENDIX II: PERSONAL INFORMATION COLLECTION AND PRIVACY POLICY STATEMENT

Hong Kong Exchanges and Clearing Limited and from time to time, its subsidiaries, affiliated companies controlling it or under common control with it and its joint ventures (each such entity, from time to time, being "**HKEx**", "**we**", "**us**" or an "**affiliate**" for the purposes of this Privacy Policy Statement as appropriate) recognises its responsibilities in relation to the collection, holding, processing, use and/or transfer of personal data under the Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**"). Personal data will be collected only for lawful and relevant purposes and all practicable steps will be taken to ensure that personal data held by HKEx is accurate. HKEx will use your personal data in accordance with this Privacy Policy Statement.

We regularly review this Privacy Policy Statement and may from time to time revise it or add specific instructions, policies and terms. Where any changes to this Privacy Policy Statement are material, we will notify you using the contact details you have provided us with and, as required by the PDPO, give you the opportunity to opt out of these changes by means notified to you at that time. Otherwise, in relation to personal data supplied to us through the HKEx website, continued use by you of the HKEx website shall be deemed to be your acceptance of and consent to this Privacy Policy Statement.

If you have any questions about this Privacy Policy Statement or how we use your personal data, please contact us through one of the communication channels below.

HKEx will take all practicable steps to ensure the security of the personal data and to avoid unauthorised or accidental access, erasure or other use. This includes physical, technical and procedural security methods, where appropriate, to ensure that the personal data may only be accessed by authorised personnel.

Please note that if you do not provide us with your personal data (or relevant personal data relating to persons appointed by you to act on your behalf) we may not be able to provide the information, products or services you have asked for or process your request.

Purpose

From time to time we may collect your personal data such as your name, mailing address, telephone number, email address and login name for the following purposes:

1. to process your applications, subscriptions and registration for our products and services;

2. to perform or discharge the functions of HKEx and any company of which HKEx is the recognised exchange controller (as defined in the Securities and Futures Ordinance (Cap. 571));

3. to provide you with our products and services and administer your account in relation to such products and services;

4. to conduct research and statistical analysis; and

5. other purposes directly relating to any of the above.

Direct marketing

Except to the extent you have already opted out or in future opt out, we may also use your name, mailing address, telephone number and email address to send promotional materials to you and conduct direct marketing activities in relation to our financial services and information services, and related financial services and information services offered by our affiliates.

If you do not wish to receive any promotional and direct marketing materials from HKEx or do not wish to receive particular types of promotional and direct marketing materials or do not wish to receive such materials through any particular means of communication, please contact us through one of the communication channels below.

Identity Card Number

We may also collect your identity card number and process this as required under applicable law or regulation, as required by any regulator having authority over us and, subject to the PDPO, for the purpose of identifying you where it is reasonable for your identity card number to be used for this purpose.

Transfers of personal data for direct marketing purposes

Except to the extent you have already opted out or in future opt out, we may transfer your name, mailing address, telephone number and email address to our affiliates for the purpose of enabling our affiliates to send promotional materials to you and conduct direct marketing activities in relation to their financial services and information services.

Other transfers of personal data

For one or more of the purposes specified above, the personal data may be:

1. transferred to our affiliates and made available to appropriate persons in our affiliates, in Hong Kong or elsewhere and in this regard you consent to the transfer of your data outside of Hong Kong; and

2. supplied to any agent, contractor or third party who provides administrative or other services to HKEx and/or any of our affiliates in Hong Kong or elsewhere.

How we use cookies

If you access our information or services through the HKEx website, you should be aware that cookies are used. Cookies are data files stored on your browser. The HKEx website automatically installs and uses cookies on your browser when you access it. Two kinds of cookies are used on the HKEx website:
Session Cookies*:* temporary cookies that only remain in your browser until the time you leave the HKEx website, which are used to obtain and store configuration information and administer the HKEx website, including carrying information from one page to another as you browse the site so as to, for example, avoid you having to re-enter information on each page that you visit. Session cookies are also used to compile anonymous statistics about the use of the HKEx website.

Persistent Cookies: cookies that remain in your browser for a longer period of time for the purpose of compiling anonymous statistics about the use of the HKEx website or to track and record user preferences.

The cookies used in connection with the HKEx website do not contain personal data. You may refuse to accept cookies on your browser by modifying the settings in your browser or internet security software. However, if you do so you may not be able to utilise or activate certain functions available on the HKEx website.

Compliance with laws and regulations

You agree that HKEx and its affiliates may be required to retain, process and/or disclose your personal data in order to comply with applicable laws and regulations, or in order to comply with a court order, subpoena or other legal process, or to comply with a request by a government authority, law enforcement agency or similar body (whether situated in Hong Kong or elsewhere). You also agree that HKEx and its affiliates may need to disclose your personal data in order to enforce any agreement with you, protect our rights, property or safety, or the rights, property or safety of our affiliates and employees.

Corporate reorganisation

As HKEx continues to develop its business, we may reorganise our group structure, undergo a change of control or business combination. In these circumstances it may be the case that your personal data is transferred to a third party who will continue to operate our business or a similar service under either this Privacy Policy Statement or a different privacy policy statement which will be notified to you. Such a third party may be located, and use of your personal data may be made, outside of Hong Kong in connection with such acquisition or reorganisation.

Access and correction of personal data

Under the PDPO, you have the right to ascertain whether HKEx holds your personal data, to obtain a copy of the data, and to correct any data that is inaccurate. You may also request HKEx to inform you of the type of personal data held by it. All data access requests shall be made using the form prescribed by the Privacy Commissioner for Personal Data ("**Privacy Commissioner**") which may be found on the official website of the Office of the Privacy Commissioner.

Requests for access and correction or for information regarding policies and practices and kinds of data held by HKEx should be addressed in writing and sent by post to us (see contact details below).

A reasonable fee may be charged to offset HKEx's administrative and actual costs incurred in complying with your data access requests.

Termination or cancellation

Should your account with us be cancelled or terminated at any time, we shall cease processing your personal data as soon as reasonably practicable following such cancellation or termination, provided that we may keep copies of your data as is reasonably required for archival purposes, for use in relation to any actual or potential dispute, for the purpose of compliance with applicable laws and regulations and for the purpose of enforcing any agreement we have with you, for protecting our rights, property or safety, or the rights, property or safety of our affiliates and employees.

Contact us

By Post:
Personal Data Privacy Officer
Hong Kong Exchanges and Clearing Limited
12/F., One International Finance Centre
1 Harbour View Street
Central
Hong Kong

By Email:
pdpo@hkex.com.hk