香港董事學會
The Hong Kong Institute of Directors

15 September 2014

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

Dear Sirs

Re: Consultation Paper on Risk Management and Internal Control

The Hong Kong Institute of Directors ("HKIoD") is pleased to forward our response to the captioned paper.

HKIoD is Hong Kong's premier body representing directors to foster the long-term success of companies through advocacy and standards-setting in corporate governance and professional development for directors. We are committed to contributing towards the formulation of public policies that are conducive to the advancement of Hong Kong's international status.

In developing the response, we have consulted our members and organised focused discussions.

Should you require further information regarding our response, please do not hesitate to contact me on tel no. 2889 9986.

With best regards

Yours sincerely
The Hong Kong Institute of Directors

Dr Carlye Tsui
Chief Executive Officer

cc: Mr Henry Lai, Chairman of Council, HKIoD & Chairman, Corporate Governance Policies Committee

香港董事學會
The Hong Kong Institute of Directors

Issued on: 15 September 2014

Consultation Paper on Risk Management and Internal Control

In relation to the Consultation Paper on Risk Management and Internal Control: Review of the Corporate Governance Code and Corporate Governance Report (June 2014), the Hong Kong Institute of Directors ("HKIoD") wishes to present the following views and comments.

* * *

General comments

The functioning of capital markets depend on companies' ability to manage and capitalise on risk. An issuer's risk management process and internal control systems must recognise the fundamental point that business strategy and value creation are to be achieved with some tolerable risk. Managing risk is essential to the successful execution of company strategy; risk management is not to avert or avoid all risks.

HKIoD considers risk management and internal control key aspects of corporate governance. An issuer should have in place a risk management process that reflects the degree of retained risk the issuer is willing to take. Business strategy or objectives that involve taking greater risks would mean a risk management process and internal control systems with more robust checks and balances.

Responsibilities of the board and management

The Consultation Paper recognises, rightly so, that both the board and management have important roles to play in respect of an issuer's risk management and internal control.

The respective roles and responsibilities of the board and management will also manifest themselves when risk oversight is put into context. The board is not for day-to-day management of risk, but to be sure that management has implemented systems to manage, monitor and mitigate risk, and that the systems are appropriate given the issuer's business objective and strategy. The board and management should work together to define a prudent acceptable level of risk that produces the greatest opportunity for reward. In turn, management should provide assurance to the board on the effectiveness of the risk management process and the internal control systems.

Risk oversight should begin with an assessment of the issuer's strategy and the risks inherent in that strategy. This necessarily requires the issuer's board and management to understand and agree on the risk appetite, i.e., the type and amount of risks that the issuer is willing to accept and retain in pursuing corporate strategy. The development of the risk appetite is to overlay the issuer's strategy on risk. It is a fundamental strategic decision that a board will make.

With the appetite for retained risk determined, the board can move on to discuss the risk tolerances, i.e., the level of variance from the risk appetite that the issuer is willing to accept. The board and management should agree on plans to restore order when risk tolerance levels are exceeded.

To determine risk appetite and risk tolerance is, however, difficult. Risk assessment must include not just expected risks but plausible risks. "Black swans", those unquantifiable and unforeseeable events, may also pose significant threat to an issuer. The board must also be able to identify and recognise the interrelation of risks, so to guard against the ripple effect of small risk somewhere from aggregating to have a large impact on the organisation. Board members, especially the NEDs and INEDs, must be forthright in asking management some difficult questions on the assumptions underlying business and operational plans adopted by management.

Assurance on the effectiveness of risk management and internal control
As it relates to the respective role and responsibilities of board and management in risk oversight, HKIoD believes management should give assurance to the board on the effectiveness of risk management process and internal control systems. HKIoD also believes the board should disclose whether it has received such assurance from management.

A very legitimate concern among some of our members, however, is what sort of "assurance" board members should ask of management, and what sort of "assurance" should management strive to provide.

The pitfall is for issuers to respond to this requirement by rushing to adopt some "control framework" that evaluates risks and identifies control deficiencies in isolation, expending considerable sums along the way and probably more on engaging outside assistance, but still fail in the end to prevent material misstatements in financial reporting. That is in fact very plausible if the attempt to give and receive such assurance renders itself into a compliance "silo" that veers off the proper path of a risk management process.

The Exchange may want to further elaborate on what framework or approach for evaluation and assessment is deemed acceptable or suitable for the purpose of the assurance. HKIoD, however, takes the view that the framework or approach ought to be one that is truly risk-based, that links risks to issuer's end-result objectives and that is aligned with ERM methods that match up to the issuer's risk appetite framework. The assurance ought to be that the issuer has in place a risk management process and internal control systems that will provide the kind of risk information for the board to effectively oversee the entity-wide residual risk levels being accepted by management vis-à-vis the issuer's risk appetite and risk tolerance.

Directors' duties and board risk oversight
HKIoD takes the view that directors should only be liable for a failure of board risk oversight where there is sustained or systemic failure to attempt to assure that a reasonable information and reporting system exists. HKIoD also takes the view that good faith attempts to put in place a risk management process and internal control systems, and assurances on the effectiveness of such process and systems given in good faith even if subsequent events might suggest otherwise, should not in the absence of egregious red flags be the subject of second-guessing by law courts. Our company law and corporate governance rules should not be taken to require *extraordinary* efforts to uncover or prevent non-compliance. That said, HKIoD will expect and advise every issuer to not structure their risk management policies around the minimum requirements but to always adopt better-than-reasonable practices.

Risk of asymmetric information
Effective risks communication is the foundation for risk governance. The greatest barrier to effective risk management, however, may in fact be the risk of asymmetric information.

Every issuer board must beware of the gap that could arise between risk information known by management and the information presented to the board.

The board (and board-level committees handling risk oversight tasks) should consider with management the type and format of risk information required to fulfill risk oversight duties. The board (and committees) should have on-going, dynamic and constructive risk dialogue with management. The agreed upon risk appetite will also provide a useful frame structure for management to report risk information to the board to facilitate the risk dialogue between the board and management.

Risk in corporate culture, tone at the top and incentive structure
Without a proper culture towards risk, a culture that starts with the right tone at the top, the real benefit of risk management and internal control will likely be overlooked in the race to tick the box required by rules.

In setting the appropriate tone at the top, the board's vision of corporate strategy, commitment to risk oversight, and expectation on conduct should be communicated to personnel at all levels. A proper culture towards risk would also entail transparency between the issuer and shareholders.

An issuer's incentive structure, if such is not realistic and not geared for the achievement of longer term strategy, could actually pose risk to the issuer. The board (and committee with jurisdiction over compensation matters) may want to pay attention to this aspect of risk.

Annual review and disclosure in the Corporate Governance Report
Ongoing process as opposed to one-off review
Risk management and internal control is an on-going process. The board's risk oversight responsibility is not discharged by a one-off annual review. The board should periodically review its risk oversight process to be sure that it is ready and able to achieve its risk oversight objectives.

Disclosure
To facilitate transparency, directors need to take an active role and disclose the board's risk management methods and structures to shareholders. Information that would be important for shareholders and stakeholders to know would include the allocation of risk responsibility, such as which committees oversee which aspects of risks, and how the board has assessed its risk appetite and risk tolerance levels.

Internal audit
HKIoD concurs with the proposal that an issuer ought to have an internal audit function, but that the function can be achieved either with an in-house arrangement or by outsourcing. Either way, there should be sufficient resources allocated to the internal audit function.

If an in-house internal audit function is to be maintained, the board and management must insure that the function and personnel have proper status and support within the organisation. Without this status and support, the issuer will find it difficult to hire and retain the strong-minded, competent and forthright individuals to get the job done properly. There is a strong need for the internal audit function (and risk management personnel in general) to be independent both in fact and in appearance.

Whether in-house or outsourced, the internal audit function should pro-actively provide opinion on the effectiveness of the issuer's risk management process, that the issuer has in place a risk management process and internal control systems that will provide the kind of risk information for the board to effectively oversee the entity-wide residual risk levels being accepted by management vis-à-vis the issuer's risk appetite and risk tolerance.

Audit committee's role (and whether to have a separate risk committee)
The Consultation Paper pointed to the concern that the audit committee could be overburdened and that a risk committee is a way to focus issuers on risk and control matters, but in the end recommended that the matter be left to issuers to decide.

HKIoD takes the view that the full board should always have primary responsibility for risk oversight. Some issuers would find the merits of delegating to a risk committee, but having a risk committee should not be the end of and be all. A risk committee should not be the sole overseer of risk; setting up a specific risk committee does not replace the role of the full board.

The issue is really not about the full board or delegate to committees, but rather to define the role of the full board and the committees.

The full board's role is to oversee the broader picture of risks that threaten the issuer's strategy and business model. Board-level committees are to support the full board in addressing the risks inherent in their respective areas of oversight. The board has the task to organise its committee structure to ensure proper oversight of different categories of risks.

The audit committee should certainly have a role in risk management. However, the audit committee's role in risk management must properly be viewed as something outside the context of its role in reviewing financial statements and accounting compliance. It follows that, if the audit committee is also to have risk oversight function, it will have to schedule and allocate sufficient additional time to focus on risk oversight matters, so that a discussion of strategic risks and risk/reward tradeoffs can take place. This could indeed become an extra burden on the audit committee.

In handling risk oversight function, the audit committee, or the risk committee for that matter, is not likely to have the time and resources to deal with the full range of risks facing the company. Some risk issues will arise in the context of the work of other committees. As different risks may be best suited to the expertise of different committees, risk issues may well be in the purview of more than one committee. It is important that risk areas that need attention do not fall through the cracks of committee jurisdiction. In designing and organising a committee structure for risk oversight, the board must give sufficient forethought and instill practices to foster coordination and communication between the full board and the committees, and among the committees.

On the whole, HKIoD considers this a matter that should be left to issuers to decide with their own circumstances. It should remain the decision of each issuer's board (and its nomination committee) to determine the right size and mix of attributes of the full board and the right structure and composition of its committees to best suit the issuer's needs.

Whether to have a separate risk committee or to have the audit committee handle risk oversight, however, the heightened demand and expectation on board risk oversight will

inevitably mean greater demand in time and effort from directors, especially the NEDs and INEDs. It is essential that we find individuals who have the skills, knowledge and qualities to meet corporate governance demands of today to fill NED and INED positions, not just to make up the numbers. Prospective directors should have conscientiously equipped themselves to become NEDs/INEDs, but they must also be adequately remunerated for their skills and their time and effort.

* * *

Responses to consultation questions

Subject to our general comments above, we state our responses to specific questions as set out in the Consultation Paper as follows:-

Risk management and internal control

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"?

HKIoD Response:

- AGREE

Responsibilities of the board and management

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?

HKIoD Response:

- AGREE
  - To remove from the Principle the wording "to safeguard shareholders' investment and the issuer's assets" is appropriate because risk management and internal control has a broader purpose to support the achievement of an issuer's objective. See our general comments.
  - In addition to the role of the board vis-à-vis management; another aspect of the allocation of responsibilities that an issuer's board must also consider is whether to delegate the risk oversight function to a committee. See our general comments and our response to Question 16 and Question 17.
  - The Exchange may want to further elaborate on what framework or approach for evaluation and assessment is deemed acceptable or suitable for purpose of this assurance.

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?

HKIoD Response:

- DISAGREE
  - Disclosure on whether the board has received assurance from management on the effectiveness of the issuer's risk management process and internal control

systems should be made a CP rather than an RBP. If the board has not received such assurance, the reasons behind it should be important information for shareholders and stakeholders to know about.

- As we noted in our response to Question 14, we also believe that an issuer's independent internal audit function should also provide its opinion to the board on the effectiveness of the issuer's risk management process.

Annual review and disclosure in the Corporate Governance Report

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?

HKIoD Response:

- AGREE
  - The proposed wording is 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?

HKIoD Response:

- AGREE

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?

HKIoD Response:

- AGREE

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?

HKIoD Response:

- AGREE
  - The proposed wording is sufficiently clear.
  - On the notion of risk management and internal controls being there to manage and not eliminate risks, see our general comments.
  - As to C.2.4(b), we advise retaining the word "processes".

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"?

HKIoD Response:

- AGREE

Question 9: Do you agree with our proposal to upgrade to Mandatory Disclosures the following existing Recommended Disclosures in relation to internal controls (Section S):

(a) whether the issuer has an internal audit function;
(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?

HKIoD Response:

- As to (a), AGREE
- As to (b), AGREE
- As to (c), AGREE
- As to (d), AGREE, but we have the following remarks:
  - Significant views or proposals on risk management and internal control may come from not just the audit committee. Some issuers may decide to have a dedicated risk committee. Whether or not an issuer has a risk committee, some risk issues will or ought to have been handled by other committees that an issuer has or required to have. See our general comments and our response to Question 17.
  - We take the requirement in (d) to mean only that significant views and proposals stemming from a review of the risk management and internal control system (and the existence or not of an internal audit function) are being called for here. The Exchange may want to further clarify that it is views and proposals on improving or augmenting the process and system for discussing and managing risks that is the subject of the disclosure here, not particular business ideas or matters that may have come across the audit committee or the board.

Question10: 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"?

HKIoD Response:

- AGREE
  - Shareholders would not be the only audience interested in the risk management process of an issuer.

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?

HKIoD Response:

- AGREE
  - Proposed amendments elsewhere in this consultation exercise would obviate the need to retain RBP C.2.5.

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))?

HKIoD Response:

- As to (a), DISAGREE
  - We think this element should reasonably form part of the disclosure expected under the proposed new Code C.2.4 (upgrade from RBP) or the Corporate Governance Report Mandatory Disclosure Requirements.
- As to (b), DISAGREE
  - We think this element should reasonably form part of the disclosure expected under the proposed new Code C.2.4 (upgrade from RBP) or the Corporate Governance Report Mandatory Disclosure Requirements.

Internal audit

Question13: 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?

HKIoD Response:

- AGREE
  - The proposed wording is sufficiently clear.
  - HKIoD concurs with the proposal that an issuer ought to have an internal audit function, but that the function can be achieved either with an in-house arrangement or by outsourcing. Either way, there should be sufficient resources allocated to the internal audit function.

Question 14: Do you agree with our proposal to introduce new Notes to the proposed CP C.2.5 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?

HKIoD Response:

- As to (a), AGREE
  - An issuer's independent internal audit function should also provide its opinion to the board on the effectiveness of the issuer's risk management process.
- As to (b), AGREE
  - This should be fine if there are adequate resources and the internal audit personnel can maintain their independence.

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)?

HKIoD Response:

- AGREE
  - Some issuers may decide to outsource the internal audit function, and such would be regarded as having complied with the proposed CP 2.6. See Consultation Paper Paragraph 88. For these companies, they can still meet the requirement of the amended CP C.2.2 with reference to the outsourcing arrangement.
  - To the extent that an issuer may have delegated risk oversight to the audit committee or a risk committee, that committee should propose and recommend to the full board measures that will ensure adequate resources for the internal audit function.

Audit Committee's role

Question16: 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?

HKIoD Response:

- AGREE
  - Nonetheless, the Audit Committee's role in risk management must properly be viewed as something outside the context of its role reviewing financial statements and accounting compliance.
  - Risk issues will also be dealt with or handled by other (existing) committees. See our general comments.

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?

HKIoD Response:

- AGREE
  - Some of our members point out that the idea of a separate risk committee, though not without merit, may not be practical for smaller companies with fewer members on the board. One suggestion was to instill some size threshold for an issuer to be obligated to consider adopting a separate risk committee.

- On the whole, HKIoD considers this a matter that should be left to issuers to decide with their own circumstances. It should remain the decision of each issuer's board (and its nomination committee) to determine the right size and mix of attributes of the full board and the right structure and composition of its committees to best suit the issuer's needs.
- Whether to have a separate risk committee or to have the audit committee handle risk oversight, however, the heightened demand and expectation on board risk oversight will inevitably mean greater demand in time and effort from directors, especially the NEDs and INEDs. It is essential that we find individuals who have the skills, knowledge and qualities to meet corporate governance demands of today to fill NED and INED positions, not just to make up the numbers. Prospective directors should have conscientiously equipped themselves to become NEDs/INEDs, but they must also be adequately remunerated for their skills and their time and effort.

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 the Consultation Paper?

HKIoD Response:

- Of the choices (a) Six months; (b) Nine months; (c) 12 months; or (d) some other period to be specified, we believe (c) is the most appropriate. Issuers, however, should be encouraged to early adopt the amendments as soon as they practically can.

<END>