Part 2
Accountability and Audit:
Internal Controls - Sound and effective controls

Summary of the relevant sections of the Corporate Governance Code ("Code") (Appendix 14 Main Board and Appendix 15 Growth Enterprise Market Listing Rules)

Code Section C.2 - Internal Control: Principle
The board should ensure that the issuer **maintains sound and effective internal controls** to safeguard shareholders' investment and the issuer's assets.

- **Relevant Code Provisions** are (emphasis added):

C.2.1: **The directors** should **at least annually** conduct a **review of the effectiveness** of the issuer's and its subsidiaries' **internal control** systems and **report to the 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**.

C.2.2: The board's annual review should, in particular, consider the **adequacy** of resources, staff qualifications and experience, training programmes and budget of the issuer's **accounting and financial reporting function**...

- There are also **Recommended Best Practices ("RBPs")** (C.2.3) regarding, inter alia:
  (i) Factors that the board's **annual review** should consider, including:
    (a) the scope and quality of **management's ongoing monitoring of risks** and of the **internal control** system, and where applicable, the work of **internal audit and other assurance providers**;
    (b) the extent and frequency of **communicating monitoring results to the board** (or board committees) to enable it to **assess the issuer's controls and the effectiveness of risk management**;
    (c) **significant control failings or weaknesses identified** during the period **and their impact, or potential impact, on the issuer's financial performance or condition**.

A Guide on Better Corporate Governance Disclosure

(ii) **Corporate governance report ("CG Report")**: issuers should disclose in the CG Report **how** they have complied with the Code Provisions on internal control during the period, including (C.2.4):

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

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

(c) the **process used to review the effectiveness** of the internal control system, and

(d) the **process used to resolve internal controls defects** for any significant problems disclosed in its annual reports and accounts.

(iii) **Issuers without an internal audit function should review the need for such function, on an annual basis**, and should disclose the outcome in the CG Report.

- The above disclosures should provide **meaningful information** and should **not** give a **misleading** impression (C.2.5).

- There are also a number of other "**recommended disclosures**" in the **CG Report** regarding internal controls, including procedures and **internal controls** for the handling and **dissemination of inside information** (S.(a)(ii)) and the **criteria** used **for assessing the effectiveness of the system** (S.(a)(vii)).

1. Analysis: Key themes underlying the Code requirements

1.1 The **Code Provisions** do **not prescribe** any **internal controls system** applicable to all issuers. The intention is that issuers should have a free hand to design their systems, having regard to any special circumstances that may lead to their adopting a particular approach.

1.2 Again, the Code Provisions do **not prescribe** the **elements of the board's review** process or rigid requirements as to **disclosure**. Some **guidance** is, however, provided in the form of "**RBPs**".

1.3 Relationship between **internal controls and risk management**:

A useful summary is contained in the UK Turnbull Guidelines:

"...a company's internal controls system has a key role in the management of risks that are significant to the fulfilment of its business objectives... A company's objectives, its internal organisation and environment in which it operates are continually evolving and, as a result, the risks it faces are continually changing. A sound system of internal control therefore depends on a thorough and regular evaluation of the nature and extent of the risks..."

A Guide on Better Corporate Governance Disclosure

The RBPs reflect significant risk management disclosure considerations, e.g., disclosure of the process used to identify, evaluate, and manage significant risks.

1.4 At the invitation of the Stock Exchange, in 2005, the Hong Kong Institute of Certified Public Accountants ("Institute") published a guide entitled "*Internal Control and Risk Management – a Basic Framework*" ("**Implementation Guide**").

1.5 The guide aimed to help listed issuers **understand** and **implement** the requirements in the **Code**, and to **devise their own internal controls procedures**.

Therefore, in discussing disclosure issues in this document, where appropriate, reference will be made to the Implementation Guide as well, and to the underlying principles set out therein.

1.6 To sum up, our interpretation of the key themes underlying the Code requirements (and RBPs) are:

A. The issuer has to maintain a sound internal controls system.

B. The board is responsible for the issuer's maintaining a sound internal controls system and should acknowledge this in the CG Report.

C. The board has to review the system's effectiveness and report to the shareholders at least on an annual basis.

It should obtain the necessary assurance from other stakeholders, including management's on-going monitoring, the work of (where applicable) internal audit and other assurance providers (e.g., external auditors).

(N.B. This board review process should involve on-going monitoring, not simply a review to be conducted annually.)

1.7 Report users, including investors, would also appreciate:

D. A high-level description of key risks facing the company, their impact and the mitigating measures taken.

2. How to provide meaningful disclosure in relation to the key themes

This section considers what disclosures users of an issuer's report, including investors, would consider **"meaningful" and to offer practical value. It is possible to provide meaningful disclosures by using high-level statements**, without divulging commercially-sensitive information.

Under each principle, we have included some brief **commentary**. In some cases, there are **sub-themes** under the relevant theme. **Examples** are also provided to illustrate the relevant issues where appropriate.

(N.B. Theme B is not discussed in detail as it involves only a straightforward statement of board responsibility).

Themes A and B: The issuer has to maintain a sound internal control system. The board is responsible for the issuer's maintaining a sound internal controls system and should acknowledge this in the CG Report.

There are various key elements of a "sound internal control system", which can be described in terms of possible sub-themes.

Sub-theme (A.1): Responsibilities

Under the Code, the **board has overall responsibility** for the issuer's internal controls and risk management system. However, it is the role of **management** to implement the board's policies on risk and control, i.e., to design, operate, and monitor a suitable system. The board may also delegate detailed aspects of the review work to **board committees** (e.g., audit committee, risk management committee). Relevant **considerations** include the size and composition of the board; the scale, diversity, and complexity of the company's operations; and the nature of the significant risks it faces. If a designated committee has a special role in supporting the board in this aspect, the results of its work should be reported to the board.

Under a widely accepted model, there are **three lines of defence** below the board and senior management levels: (a) operational managers who own and practise the controls on a day-to-day basis; (b) risk, compliance and other policy setting groups which help build and monitor the first line of defence; and (c) internal audit which provides independent assurance.

So, how does the process work in your company?

Sub-theme (A.2): State the structured approach adopted

The adoption of a structured approach, i.e., a well-defined and systematic framework in applying internal control principles, will greatly assist report users to appreciate the underlying rigour of the system. It also facilitates the work of the board in reviewing it. It is useful, therefore, to state the approach adopted.

One well-known framework is that published by the Committee of Sponsoring Organisations of the Treadway Commission ("**COSO**") in the United States. This approach is the principal framework referred to in the Implementation Guide and it is consistent with the approach suggested by Hong Kong Standard on Auditing 315. The COSO framework has five key components:

A Guide on Better Corporate Governance Disclosure

- **Control environment**
- **Risk assessment**
- **Control activities**
- **Information and communication**
- **Monitoring activities**

(It should be noted that the original COSO framework, published in 1992, was updated in 2013 ("**COSO 2013**"). The revisions involved, among other things, codifying 17 principles that support the five components above. After December 15, 2014, compliance with the original framework will no longer be regarded as complying with COSO and the updated framework will be considered the sole COSO internal control mechanism).

Sub-theme (A.3): Describe key aspects of your company's own internal control system

As explained in the Implementation Guide, internal controls **should be tailored to an individual company's particular characteristics and circumstances**. This may depend upon, for example, its industry, size, and organisational structure. Therefore, report users would be interested in understanding the key aspects of your company's system in light of your own circumstances.

There are detailed discussions in the Implementation Guide on the five components under the COSO model.

Theme A: Examples – sub-theme (A.3): A company's internal controls system (risk management aspects)

Example 1

A key component of a company's internal control system is risk management. The following example describes the tools and processes used. The integration of risk in strategic development, business planning and other key business processes, is stressed. (Also see example for sub-theme (A.4) – "improvement areas and the way forward" below):

Our Risk Management Process

- **Is embedded in our strategy development, business planning, investment decisions, capital allocation and day-to-day operations.**
- **Is in line with leading industry standards and practices, including ISO 31000 : 2009 Risk Management - Principles and Guidelines.**
- **Involves establishing the context, identifying risks, assessing their consequences and likelihood, evaluating risk levels, control gaps and priorities, and developing control and mitigation plans. This is a continuous process with periodic monitoring and review in place.**

Our Quarterly Risk Review Process at Group Level	• Every quarter, our business and functional units are required to submit their material risks identified through their risk management process to Group Risk Management. • Group Risk Management, through aggregation, filtering and prioritizing processes, compiles a Quarterly Group Risk Management Report for discussion at the Group Executive Committee (GEC), chaired by the CEO. The Committee reviews and scrutinizes the material risks and ensures the appropriate controls and mitigation measures are in place or in progress. Emerging risks, which might have a material impact on the Group over a longer timeframe, are monitored and discussed at the Committee. • Following review by the GEC, the Quarterly Group Risk Management Report is submitted to the Audit Committee with a summary of the material risks circulated to the Board. "Deep dive" presentations on selected risks are given to the Audit Committee for more detailed review.
Our Risk Review Process for Investment Decisions	• All new investments must be endorsed by Management's Investment Committee, chaired by the CEO, before seeking approval from the Board or Finance & General Committee. • We require independent functional review and sign-off of any investment proposal before submission to the Investment Committee. Group Risk Management sign-off is part of the investment review process. • Group Risk Management requires that the project owner conducts a risk assessment with proper documentation. Detailed checklists and worksheets are adopted for identifying risks/mitigations and assessing risk level. Material risks and associated mitigations are highlighted and discussed at the Investment Committee.
Our Risk Management in the Business Planning Process	• In our annual business planning process, business units are required to identify all material risks that may impact their achievement of business objectives. Identified risks are evaluated based on the same set of risk criteria as the quarterly risk review process. Plans to mitigate the identified risks are developed for implementation and budget allocation purposes. The material risks set out later have been extracted from our 2012 business planning process.

(CLP Holdings Limited, Annual Report 2012)

Theme A: Examples – sub-theme (A.3): A company's internal controls system (control environment, control activities, information and communications, monitoring aspects)

Example 2

The following example illustrates a company's control procedures established pursuant to COSO standards, spanning control environment (e.g., tone at the top; a whistle blowing policy to safeguard integrity); control activities (e.g., established structure with clear segregation of duties; financial controls and IT controls); information and communications (e.g., timely communication within the organisation, as well as with its stakeholders; dissemination of inside information); and monitoring (e.g., on-going monitoring activities; internal audit):

Key control procedures

An internal control and risk management system, which is an integral part of the Group's management system, is on a par with the COSO (Committee of Sponsoring Organizations of the Treadway Commission) standards, and is designed to provide reasonable, though not absolute, assurance against material misstatement or loss and to manage rather than eliminate risks of failure to achieve business objectives. Key control procedures and measures include:

- Establishing a structure with defined authority and proper segregation of duties
  - A clear organisational structure with defined lines of responsibility to facilitate systematic delegation of authority
  - Written policies, procedures and guidelines with defined limits of delegated authority to facilitate effective segregation of duties and controls
- Monitoring the strategic plan and performance
  - A 3-year strategic plan prepared with inputs from Division/Department Heads lays down the corporate strategies, and provides guidance for the preparation of the annual operating plan
  - The relevant Divisions/Departments carry out their respective business operating plans as laid down in the strategic plan in accordance with the adopted policies and procedures
  - An annual budget with financial targets provides the foundation for the allocation of resources in accordance with prioritised business opportunities
  - Variance analyses help identify deficiencies and enables timely remedial actions to be taken
- Designing an effective accounting and information system
  - A comprehensive accounting system for providing financial and operational performance indicators to facilitate problem identification, and to ensure complete and accurate financial information for timely reporting and disclosure purpose
  - An information system for identifying, capturing and communicating pertinent information to enable employees to carry out their responsibilities
  - Regular reviews for ensuring proper and legitimate dissemination of financial information
  - System and procedures are in place to identify, assess and manage risks including legal, credit, market, concentration, operational, environmental, behavioural and systematic risks that may have an impact on the Cash and Derivatives Markets in Hong Kong. Exposure to these risks is monitored by the Management Committee, the Executive Committee, and the Risk Management Committee on a continual basis

(Hong Kong Exchanges and Clearing Limited's website, referred to in its Annual Report 2012)

Sub-theme (A.4): Improvement areas and the way forward

As discussed in the Implementation Guide, the system of control should (i) be **embedded in the operations** of the issuer and form part of its culture; (ii) be capable of **responding quickly to evolving risks** to the business arising from internal changes, as well as changes in the business environment; (iii) include procedures for **immediate reporting of significant control failings and corrective actions** taken.

Therefore, internal control and risk management should be part of **a continuing process**. A company may start off by building the relevant risk governance structure, system, processes and tools. However, the system will be most effective if it is embedded in the company's culture and business operations, in other words, a "living" system implemented by the operating units and other relevant parts of the organisation.

Theme A: Examples – sub-theme (A.4): improvement areas and the way forward

Example 3

The following company sets out its improvement actions taken during the year as well as the way forward. These include further embedding the integration of risk management into its strategy development and other business planning processes. The completion of the improvement steps is reported in the following year's report. (See example for sub-theme (3) above):

Major Initiatives in 2011	Examples of some initiatives
Process	• Enhanced our risk management framework by reinforcing risk ownerships, defining Group level risk criteria, and standardising risk languages amongst business units. • Established and implemented a quarterly reporting process of top tier risks by business and functional units, with review by the Group Executive Committee, oversight by the Audit Committee, and summary submission to the Board; deep dive presentations on selected risks are produced as required.

Outlook and Major Initiatives for 2012

- Continue to enhance our risk management framework and assist business units in roll-out and implementation of their own frameworks.
- CLP Power will roll-out an improved risk management framework with cross-functional risk management committee or similar entity established.
- Majority-owned Chinese assets to develop operational risk management frameworks.
- Embed the integration of risk management into strategy development and business planning processes.
- Facilitate efficient identification of emerging risks.
- Extend investment risk review as appropriate for projects entering commercial operations phase.

(CLP Holdings Limited, Annual Report 2011)

Theme C: The board has to review the system's effectiveness and report to the shareholders at least on an annual basis.

It should obtain the necessary assurance from other stakeholders, including management's on-going monitoring, the work of (where applicable) internal audit and other assurance providers (e.g., external auditors).

This theme flows from Theme B (the board's responsibility for the issuer's maintaining an effective internal controls system). **The board should**, therefore, **define the process to be adopted for its review** of internal control efficiencies, including the **source of "assurance" received during the year** and the **annual assessment process** itself. The source of assurance includes the scope and frequency of reports from the management, internal auditor and external auditor, if applicable. As explained earlier, the role of **board committees** in the review process, including that of the audit committee, is for the board to decide.

A Guide on Better Corporate Governance Disclosure

Report users would appreciate an **understanding of the process the board has actually gone through** for the purpose of giving the **"internal controls effectiveness" statement**.

Theme C: Example

The following international example gives a very comprehensive list of the source and frequency of various forms of assurance that the board received, including from the management, internal auditor, and external auditor:

Internal controls
During the year we have examined the key elements of the internal control processes and provided assurance to the Board on the effectiveness of the internal control environment. Set out below are a number of the activities that have been completed in our review of financial, operational and compliance controls.

- We considered the results of internal control self-assessment returns from the businesses and reviewed management responses to any identified weaknesses.
- We received a report from the external auditor which set out their key observations on the internal control environment that had arisen during their annual audit, along with management's remediation plans to strengthen further the internal controls within the Group.
- At most meetings we receive a summary of the financial control audits performed by Internal Audit, including the key recommendations. The audits include reviews of processes relating to accounting and finance, revenue, project management and contracting, capital expenditure, procurement, inventory, payroll and general computer controls. Last year we reported that particular attention had been given to ensuring a timely remediation of any audit recommendations; this rigour has continued this year with updates provided at each meeting.
- We reviewed arrangements under which employees can, on a confidential basis, raise concerns about potential irregularities in financial reporting or other matters, and the arrangements for follow-up actions.
- Significant variances between results and internal forecasts are considered and where such variances are indicative of control failings, management actions to address weaknesses are reviewed.
- We continue to focus on system tools to tighten our internal controls, for example establishing an automated ledger link between general ledgers and sub-ledgers in our ERP systems in the businesses to the Group's financial consolidation system that ensures a full audit trail and no allowance for manual entries.
- The Audit Committee receives a regular and comprehensive review of internal controls and accounting matters in advance of each results announcement.

The Board's review of the risk management process and its statement on internal control is contained on page •.

Risk management
As the Audit Committee is responsible for reviewing risk management processes and reporting systems on behalf of the Board, presentation of an update from the Chairman of the Risk Committee has become a regular cadence. A standardised approach to the completion of project risk registers has facilitated reporting to the Audit Committee and enabled more sophisticated and meaningful reports.

As well as reviewing the major risks in more detail, we monitored the mitigation actions put in place by management.

(Invensys plc, Annual Report 2013)

Theme D: A high-level disclosure of key risks facing the issuer, their impact and the mitigating measures taken.

The previous theme deals with disclosing the **process**. In terms of **substantive issues**, what are the key risks facing the company, their impact and mitigating measures that have been taken? It is also important to **link** the description with the **specific strategy** and risks **during the year**. What, for instance, are the changes during the year?

Theme D: Examples

Example 1

In this example of a public utility group, regulatory and political risk is one of the key risks it faced during the year. In the following extract, developments in this risk category during the year, risk assessment, and key risk mitigating measures are set out clearly:

Regulatory Risk across the Group
Globally, we have seen both a rise in governments' desire to intervene more directly in the privately-owned power sector, with strengthened regulatory control, and public support for such measures. The global financial crisis has brought increased public focus on the affordability of government and/or regulated services, including electricity. Pressure on electricity tariffs is affecting the financial standing and outlook of the power sector. All CLP's businesses operate under various local and national regulatory regimes and are currently facing the risk of adverse regulatory changes.

Risk Identification	Risk Assessment	Key Risk Mitigations
Regulatory and political risk of Hong Kong (HK) business	Rising costs and tariff increases have become a regulatory challenge for the HK business. We are not only encountering short-term risk with Government's difficulty in explaining the cost implications of its own policy decisions, but also long-term risk of adverse regulatory changes to the SoC. Whilst we have improved communication, explaining the link between higher tariffs and the rising cost of gas purchases, many stakeholders continue to express concern about higher tariffs.	• Implement Stakeholder Engagement Plan. • Strengthen cost justification and transparency. • Explore further stringent control over operating costs. • Enhance capital project development and prioritisation process. • Publicity and brand building to reinforce appreciation of CLP's performance and the value of its service to customers. • Help customers mitigate tariff impact. • Prepare for the discussion on future market developments with Government and the public.

(CLP Holding Limited, Annual Report 2012)

Example 2

In this example of a hotel operator, the descriptions of some key risks it faced during the year have been extracted. These include expenditure (in the light of its on-going refurbishment plans) and other risks specific to the service industry (e.g., health and safety for visitors, data privacy and damage to reputation by social media).

Inability to fund capital expenditure to maintain and renovate existing properties could reduce our profits

Risk Description	Risk Mitigation
Capital expenditure to develop, maintain and renovate our existing properties is critical to our business. If we are forced to spend larger amounts of cash from operating activities than anticipated to operate, maintain or renovate existing properties, our ability to invest in new business opportunities could be limited. In addition, we may need to postpone or cancel other planned renovations or developments to meet such cash demands, which could impact our ability to compete effectively.	• On-going regular maintenance of hardware standards • Continuous monitoring of furniture, fixture & equipment spend by operations and Head Office

Failure to address health and safety issues could result in guest or employee injuries or illness

Risk Description	Risk Mitigation
Our operations, merchandise and the properties we own and manage are subject to extensive health and safety laws and regulations of various local and national governments. Failure to timely address health and safety issues or comply with these laws and regulations could expose us to costs and liabilities.	• Professionally certified premises and staff • Policies and procedures on handling food, waste, and any hazardous materials • Robust crisis management process, ongoing risk assessment exercises, regular health consultations, etc.

Breach of data privacy could subject us to fines and costs

Risk Description	Risk Mitigation
Collection and usage of information relating to our guests, customers and employees for various business purposes, including marketing and promotional purposes, are governed by privacy laws and regulations in jurisdictions around the world. New privacy regulations could increase our operating costs, and impact our ability to market our products, properties and services to our guests. Failure to comply with applicable privacy regulations could also result in fines, and harm the value of our brand and impact our business.	• Implementation of Group-wide data privacy policy and manual and training • Assessment by data privacy teams across operations • Process for reporting and dealing with data breaches

Damage to reputation may be caused by negative comments on social media

Risk Description	Risk Mitigation
Negative comments made on social media, in the absence of a verification mechanism, including those by disgruntled staff and guests could damage our reputation. In addition, monitoring and management of social media could be costly and force us to divert our resources. Failure to maintain and protect our reputation from social media damage could tarnish our brand and impair our business.	• Implementation of Group-wide social media usage guidelines • Social media monitored by external service provider

(The Hongkong and Shanghai Hotels, Limited Annual Report 2012)