Hong Kong Institute of
Certified Public Accountants
香港會計師公會
The Success Ingredient

內部監控與風險管理的基本架構

序言

香港會計師公會於一九九五年成立企業管治委員會至今，一直為提高香港的企業管治意識及水平扮演領導角色，公會引以為豪。公會認為，優良的企業管治對吸引外資、刺激經濟增長及減低資金成本極其重要，此外，對香港作為全球主要金融中心之一及中國大陸和區內的主要國際資本市場的地位也是必不可少。

因此，公會支持香港聯合交易所有限公司(「聯交所」)最近對《上市規則》作出的修訂，以及推出《企業管治常規守則》(《守則》)及《企業管治報告》的有關規定。該等修訂將加強對香港上市公司企業管治實務及資料披露的要求。

這本內部監控與風險管理**指引**是應聯交所邀請而制訂，其主要目的是就內部監控與風險管理的基本架構提供一般指引及建議。這本**指引**引用了外國在這課題上的重要研究作為依據，這些研究都是良好實務的公認基準，這本**指引**同時又顧及了香港市場的現況。公會認為，這本指引內所載的原則及建議應有助上市公司了解及實施《守則》內有關內部監控的規定，並就其業務的具體情況和特點制訂本身的內部監控程序。

加強企業管治不單是執行法規，也是為了樹立及培養合乎道德規範和健康的企業文化。我希望本**指引**非常清楚地說明，設立完善的內部監控系統與評估其有效性並非是為了遵守不必要和繁複的監管規定，而是要實施機制以幫助公司達致其企業目標及符合股東和利益相關者的期望。在基本層面上，本**指引**強調，有效監控的首要條件，是公司必須確保擁有清晰的、經董事會同意而高級管理層及僱員清楚了解的目標。公司接著應對可能妨礙其達致上述目標的風險進行識別、評估及按優先次序排列，然後制訂程序，進行有效管理。公司也應設立預警指標，當有事情發生，便可盡快確認有關情況並通知適當人士採取行動。在實踐方面，必須同時對內和對外(例如：核數師及監管機關)進行坦誠的溝通和保持有效的資訊流通。最後，鑒於營商環境和情況不斷改變，因此必須對系統進行持續的監察和檢討。

可惜，很多公司一直缺少上述部分或全部要素。事實上，有些公司理論上雖然有光明的業務前景，但由於缺少這些要素，最後仍然失敗。有些公司因發展太快而超越其內部監控與風險管理機制的處理能力；其他公司卻因沒有制訂內部制衡機制而未能洞識問題的先兆；有些公司還屈服於主要董事及控股股東不符合市場期望及公眾利益的道德價值的影響。我們都熟悉一些典型例子，故應引以為鑑。雖然內部監控系統並非是能解決各種企業問題的靈丹妙藥，它卻有助提供合理保証，以確保由擁有智慧和判斷力的決策者所管理而運作良好的企業能達致其既定目標。

本人希望讀者清楚明白，這本**指引**在注重為如何遵守法規提供指引的同時，也同樣關注如何保障企業及營造一個讓企業茁壯成長及使股東價值增加的環境。健全的道德管治包括優良的企業管治，而有效的企業管治系統應可以使企業遵守法規及達致預計的業績表現，以符合股東及利益相關者的合理期望。這就解釋為何有效的內部監控系統與風險管理機制應被納入公司的日常管理和管治程序內，並應構成公司問責制架構和定期向股東匯報的一環。

這本**指引**與《守則》同樣是為上市公司及其附屬公司和集團內的其他公司而編製。然而，本人希望這本**指引**亦為沒有(還未)上市的企業及其他有興趣人士提供有用的參考資料。

香港會計師公會會長 兼
內部監控與風險管理專責小組主席

周光暉

二零零五年六月

香港會計師公會二零零五年企業管治委員會成員名單

主席：	周福安	佳亞有限公司
副主席：	陳記煊	南順(香港)有限公司
	Richard George	德勤 • 關黃陳方會計師行
成員：	聶雅倫	羅兵咸永道會計師事務所
	鄭國衛	國衛會計師事務所
	鍾悟思	公司註冊處
	羅義坤	九龍倉集團有限公司
	李開賢	畢馬威會計師事務所
	文禮信	摩斯倫 • 馬賽會計師事務所
	倪弼德	Potential Associates Ltd.(潛能)
	Keith Pogson	安永會計師事務所
	蕭啟鎏	利豐集團
	譚學林	樂聲電子(集團)有限公司
	謝秀玲	醫院管理局
	詹華達	浩華企業顧問有限公司
秘書：	戴尚文	香港會計師公會專項發展總監
	林淑文	香港會計師公會專項發展助理總監

內部監控與風險管理專責小組成員名單

主席：	周光暉	中國基建集團控股有限公司
成員：	周福安	佳亞有限公司
	陳記煊	南順(香港)有限公司
	Richard George	德勤 • 關黃陳方會計師行
	李開賢	畢馬威會計師事務所
	陸階	莎莎國際控股有限公司
	倪弼德	Potential Associates Ltd.(潛能)
	蕭啟鎏	利豐集團
秘書：	戴尚文	香港會計師公會專項發展總監
	林淑文	香港會計師公會專項發展助理總監

目錄

A. 目標

1.0 背景

1.1 香港聯合交易所有限公司(「聯交所」)於二零零四年十一月公布《企業管治常規守則》(《守則》)及《企業管治報告》,期後分別納入《主版上市規則》附錄十四和附錄二十三及《創業版上市規則》附錄十五和附錄十六。《守則》於二零零五年一月一日或以後開始的會計期生效,唯一例外是《守則》第C.2條有關內部監控的條文,以及建議在《企業管治報告》中披露上市公司內部監控資料的規定。該例外條文於二零零五年七月一日或以後開始的會計期生效。

1.2 聯交所邀請香港會計師公會(「公會」)制訂進一步指引,以協助上市公司了解及實施《守則》內有關內部監控的規定,並制訂其內部監控程序。

1.3 公會接受聯交所的邀請,在企業管治委員會名下成立了一個專責小組進行該項計劃。專責小組的成員亦有核數與核證準則委員會和商界專業會計師委員會的代表。

2.0 《上市規則》有關內部監控的規定

2.1 《守則》原則C.2列明:*「董事會應確保發行人的內部監控系統穩健妥善而且有效,以保障股東的投資及發行人的資產。」*

2.2 「內部監控」的《守則》條文第C.2.1條列明:*「董事應最少每年檢討一次發行人及其附屬公司的內部監控系統是否有效,並在《企業管治報告》中向股東匯報已經完成有關檢討。有關檢討應涵蓋所有重要的監控方面,包括財務監控、運作監控及合規監控以及風險管理功能。」*

2.3 《守則》第C.2.2至C.2.5段列出檢討內部監控系統及相關披露事項的「建議最佳常規」。我們鼓勵上市公司採納該等建議。

2.4 《主版上市規則》附錄二十三及《創業版上市規則》附錄十六第二段註釋,列明期望上市公司根據《守則》條文在其《企業管治報告》中作出若干具體的披露。以下是有關「內部監控」的披露要求:

「(3) 說明董事會經已檢討發行人及其附屬公司的內部監控系統是否有效(《守則》第C.2.1條)」。

2.5 倘若上市公司根據《守則》條文第C.2.1條在年報內對檢討其內部監控系統作出披露，我們鼓勵該上市公司披露《主版上市規則》附錄二十三及《創業版上市規則》附錄十六第三段(d)列明的詳細資料。

(《上市規則》內有關內部監控的《守則》條文及建議最佳常規，以及《企業管治報告》內所要求及建議披露的資料的更詳盡摘錄載於附錄I。)

3.0 指引的目標

3.1 編製這本指引的主要目的是提供內部監控基本架構的一般指引及建議。這應有助上市公司了解及實施《守則》內有關內部監控的規定，並根據其本身業務及營運的具體情況及特點而制訂適用的內部監控程序。這本指引並非巨細無遺或詳列硬性規定，但仍然對公司內負責監控的董事、經理及其他人士有所幫助。

3.2 這本指引同時擬 —

(i) 有助增加對內部監控及風險管理概念性架構的認識；

(ii) 有助提供一個可以用作發展及評估公司內部監控系統有效性的架構／基礎；及

(iii) 反映完善的企業實務，藉此公司將內部監控嵌入其業務及管理程序中，從而追求其目標。

3.3 聯交所表示，在制訂《守則》時，已經特別參考英國財務匯報委員會 (Financial Reporting Council) 於二零零三年七月公布經修訂的《企業管治綜合守則》(Combined Code on Corporate Governance)(《綜合守則》)所載的原則及指引。《綜合守則》之序言詳列如何遵守《綜合守則》個別部分的具體指引。*《內部監控：綜合守則的董事指引》*(《Turnbull 指引》)[1]是有關如何遵守內部監控條文的指引。公會在編製本指引時參考了《Turnbull 指引》。

3.4 公會認為，美國Committee of Sponsoring Organizations of the Treadway Commission (COSO)於一九九二年發表的題為*《內部監控 — 綜合架構》(Internal Control — Integrated Framework)*的報告，確立了內部監控的定義及概念性架構，是有建設性和有重要意義的。因此，如合適時，本指引採納了COSO報告所提的模式。

[1] 英格蘭及威爾斯特許會計師公會於一九九九年九月在英國出版的《內部監控：綜合守則的董事指引》(Internal Control: Guidance for Directors on the Combined Code)。

3.5 我們鼓勵上市公司的董事會在進行下列事項時參考本指引：

- 評估公司遵守《守則》原則 C.2的情況；
- 實施《守則》條文第C.2.1條的規定；及
- 在《企業管治報告》中向股東匯報該等事宜。

3.6 董事就檢討公司如何實施《守則》內有關內部監控的規定及向股東匯報實施情況時應作出判斷。

3.7 公司應從企業管治的角度，把本文件內關於設立完善的內部監控系統及檢討其有效性的指引，納入公司日常管理及管治的程序內，作為公司董事會及管理層向股東問責的一環，而不應把指引視為要符合證券市場監管機構所頒布並執行的監管規定而實行的一項措施。

4.0 指引的應用性

4.1 本指引的主要對象是《守則》條文第C.2.1條所指的上市公司及其附屬公司，然而，上市公司的性質各有不同。內部監控系統應按照個別公司的具體特點和情況，例如：根據其行業、規模及組織結構而度身制訂。因此，不適合採用「放諸四海皆準」(one size fits all) 的模式。

4.2 雖然本指引所載的原則及建議可能需要根據公司的個別情況而作出調整，但我們相信這些原則及建議會為大部分的上市公司提供有用的參考資料。我們鼓勵所有屬上市集團成員的公司採納這些原則及建議，同時，我們亦希望本指引能為擬實施或加強內部監控的公司提供有用的參考資料。

4.3 在本指引內，倘若提述「公司」，如適用者，應指其申報公司為母公司的集團。對集團公司而言，在檢討內部監控的有效性及向股東作出的有關匯報時，應從集團整體角度出發，例如：集團公司應檢討所有重要地區的所有重要監控系統是否有效。

4.4 就應用本指引而言，倘若有重大的合營企業及聯營公司並未被納入為集團成員而得以處理，我們鼓勵公司應作出有關披露。若有應用於這些實體的風險管理及內部監控保證的其他資源，也應予以披露。

B. 實施內部監控及風險管理

1.0 內部監控的架構及範疇

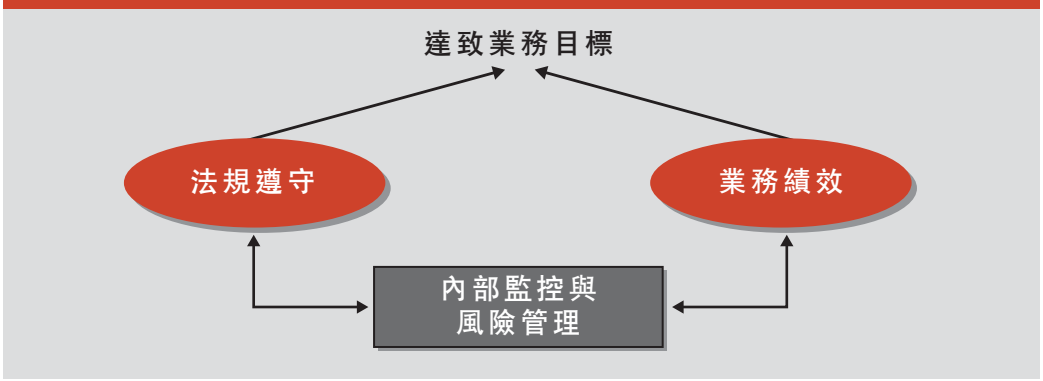
1.1 「內部監控」並無簡單定義。然而，誠如上文A.3.4 段所述，公會認為COSO報告提供了有用的模式，所以本指引在適合時採用了COSO報告所述的定義及概念性架構。（見附錄 II）。

1.2 COSO報告所述的內部監控系統的定義，是指為達致以下目標而提供合理保證的程序：

- *營運的效益及效率*
- *財務匯報的可靠性*
- *遵守適用的法律規則*

1.3 內部監控對業務的有效營運及日常運作極為重要，並有助公司達致其業務目標。誠如上文所述，內部監控的範疇非常廣泛，它包含納入策略性、管治及管理程序內的所有監控，涵蓋公司全面的業務及營運，而不單只是直接涉及財務營運及匯報的監控。內部監控的範疇並不局限於業務中一般被視為法規遵守事宜的層面，同時也延伸至業務的績效層面。（見圖1）。

圖1：內部監控架構



1.4 內部監控必須針對業務的具體性質及需要。因此，它們應反映出完善的企業實務，並在持續轉變的營商環境中經常保持適切性，讓公司對業務或行業的具體需要能夠作出反應。

1.5 不應視監控為業務的一項負擔，反之應視它為一種途徑，藉以增加業務發展的機會及減低由不速事件造成的潛在損失。此外，成功的公司不應自滿或被本身的成就所蒙蔽。有許多例子，都是由於缺乏內部監控或內部監控出現缺點而危及公司的成功。

1.6 同時，成本／效益方程式亦與內部監控系統有關。在整體系統的設計及在風險識別、評估和釐定風險的優先次序方面，必須考慮成本／效益的因素。

內部監控的功能

1.7 然而，監控並不等同管理，而且並不構成與公司管理有關的事宜。雖然它的目的是支持公司達致業務目標，並可作為對可能阻礙達致目標的障礙的預警系統，但另一方面，內部監控並不說明要訂立哪些目標。雖然它有助確保為決策、執行及監察工作提供可靠資料，亦能幫助管理層對所採取行動的後果作出評估及匯報，但並不能取代管理層作出策略及營運決定。此外，應否採取行動及應採取甚麼行動的決定屬內部監控範疇以外的事。

1.8 隨之而言，監控系統存在一些固有的限制。設計完善的內部監控系統能減少但不能消除決策判斷失誤、人為錯誤、監控活動及程序受僱員或其他人士串謀破壞、管理層逾越監控及其他不可預見的情況。

1.9 因此，完善的內部監控系統有助提供合理但並非絕對的保證，以確保公司避免在達致其業務目標或在合法進行業務過程中，被可以合理地預見的情況所妨礙。然而，完善的內部監控系統並不能對公司提供百份百保障，避免其業務目標無法達致或避免出現所有重大錯誤、損失、欺詐或違反法規的情況。

1.10 誠如上文A.4.1段所指，沒有兩間公司會有或應該有相同的內部監控系統。公司及其監控系統會因行業、規模和組織結構，以及公司文化和管理哲學不同而有所分別。因此，雖然所有公司都需要下文B.2.2段所述的每個元素，確保其業務活動有足夠的監控，但每間公司應有一個獨特的、配合本身的情況而度身制訂的內部監控系統。管理層須根據公司的需要而作出判斷，設訂所需監控系統的性質及了解這些監控系統的運作是否有效，以達致公司的目標。

2.0 完善的內部監控系統的要素

2.1 內部監控系統包括公司的政策、程序、工作、行為及其他方面，當集合一起時則可：

- 透過讓公司能夠對與達致公司目標有關的重要業務、營運、財務、法規遵守及其他風險作出適當反應，從而促進公司的營運成效及效率。這包括保障資產，避免誤用或流失及欺詐，並確保負債得到確認及控制；
- 有助確保對內、對外匯報的質素。這需要維持適當的記錄及程序，從而使機構內外產生適時、相關及可靠的資訊；及
- 有助確保遵守適用的法律和條例，以及遵守業務操守的內部政策。

2.2 內部監控可分成五個互相關連的元素。就配合達致個別而又重疊的營運、財務匯報及法規遵守的目標時，這些元素也作為評估內部監控系統有效性的標準，圖2內已有說明。這些元素是：

(i) 監控環境 — 是其他內部監控元素的根基，並提供紀律及結構。監控環境因素包括人員的道德價值及勝任能力(素質)、董事會提供的指示及管理的效率。

(ii) 風險評估 — 識別及分析影響達致目標的風險(包括與監管及營運環境不斷轉變有關的風險)，以此作為釐定應如何降低及管理這些風險的依據。

(iii) 監控活動 — 幫助確保管理層的指示得以執行，以及用於處理風險以達致公司目標的任何行動得以採取的各種政策及程序。

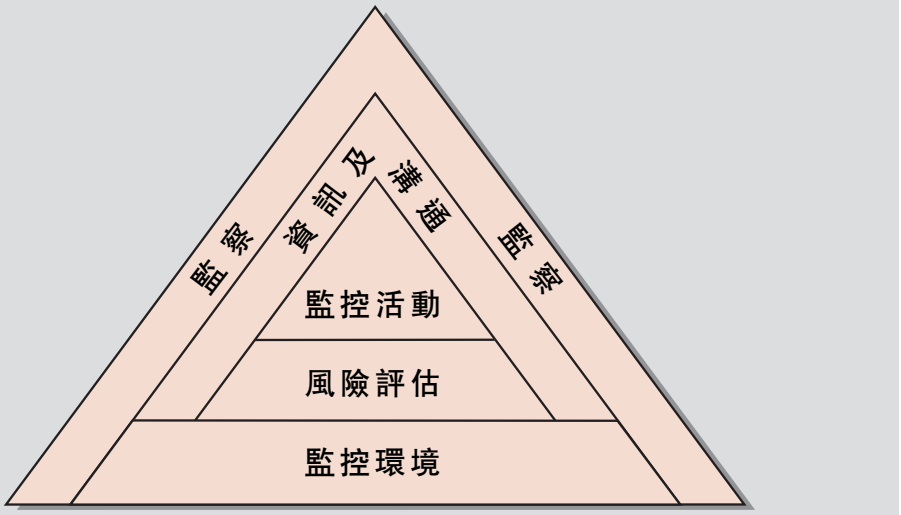
(iv) 資訊及溝通 — 在人員能夠履行職責的方式及時間範圍內，識別、取得及匯報營運、財務及法規遵守的相關資訊的有效程序及系統。

(v) 監察 — 持續評估內部監控系統是否充足及其表現素質的程序。內部監控不善之處應向適當的上級管理層滙報。適當的上級可以是高級管理層、審核委員會或董事會。

以上五個元素的更詳盡說明和分析以及其關係載於附錄III。

2.3 公司的內部監控系統會反映其監控環境，而監控環境則包含其組織結構。

圖 2: 內部監控元素



改編自COSO的*《內部監控 — 綜合架構》*

2.4 內部監控系統應：

- 嵌入公司的營運內，並構成公司文化的一部分；
- 能夠對由公司內在因素所產生的業務風險及對營商環境的改變迅速作出反應；及
- 包括向適當的管理層即時滙報經確認的任何重大監控失誤或弱項，及所採取的糾正行動細節的程序。

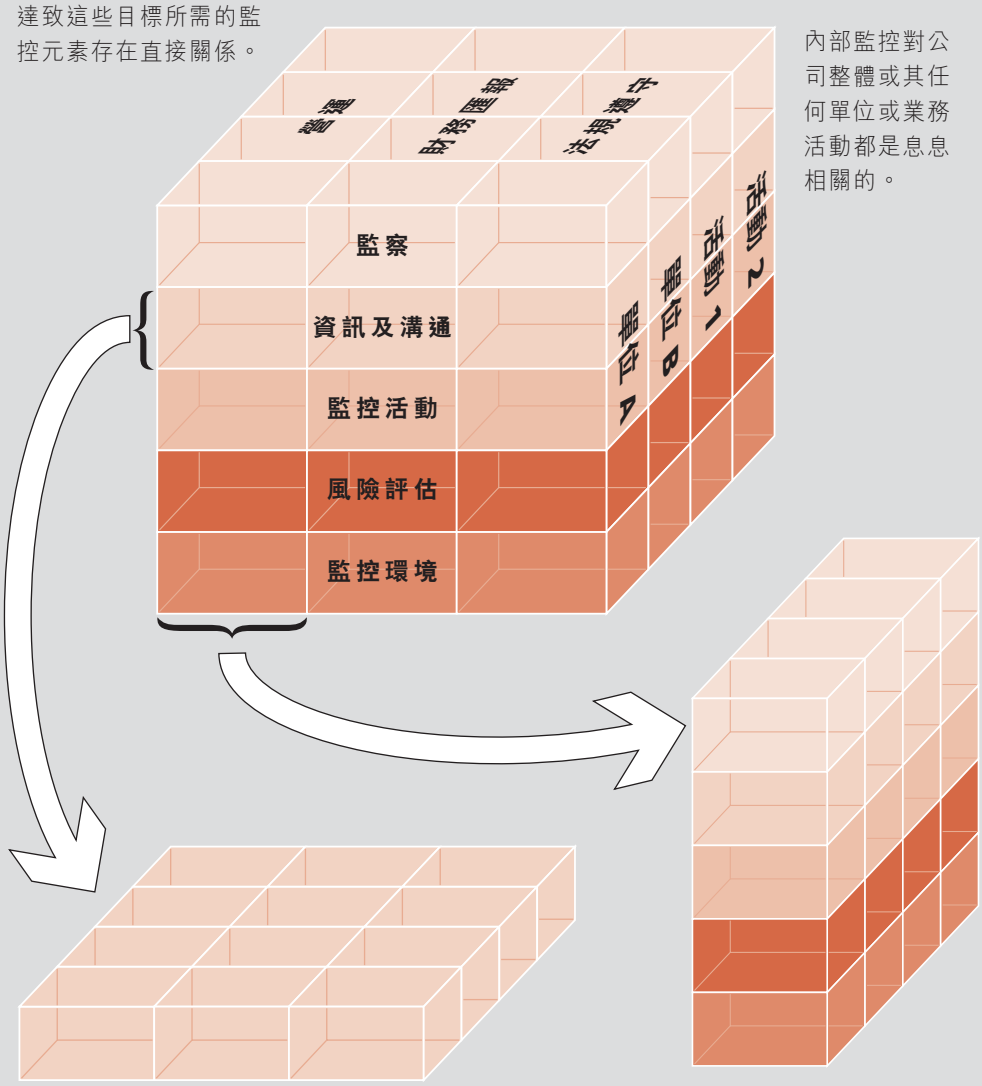
2.5 雖然個別公司有不同的特質，但內部監控程序一般應盡可能保持簡單直接，同時應謹記需要確保(a)成本沒有超過效益及(b)各級職員能夠了解維持足夠監控的重要性，而不會在實施監控時，因遇到不必要的複雜情況而對此產生不滿。

2.6 公司的目標與達致這些目標所需的內部監控元素存在直接關係。這種關係於圖3以圖像表述。所有元素適用於上文B.1.2段所提及的三個目標類別。圖3內的第三個立體面代表附屬公司、部門或其他業務單位，以及功能上或其他業務上的活動，例如：採購、生產及市場推廣。這反映出內部監控不單對公司整體，而且對該公司的各個部分都是息息相關的。

圖 3: 目標與元素的關係

公司力求達致的目標與達致這些目標所需的監控元素存在直接關係。

內部監控對公司整體或其任何單位或業務活動都是息息相關的。



三個目標類別均需要資訊，使公司可以有效地管理業務營運、編制可靠的財務報表及釐定法規遵守。

五個元素均適用於達致營運目標，並對達致營運目標十分重要。

摘自COSO的《*內部監控 — 綜合架構*》

3.0 培訓的需要

3.1 公司應給予董事及管理層適當的培訓，讓他們正確認識內部監控、其職能及範疇，包括申報事項。這樣一方面有助公司遵守內部監控的監管規定，同時也能為達致業務目標提供更大的保證。培訓課程可以由公司內部提供，亦可以透過培訓機構或專業團體提供。

4.0 風險管理

4.1 風險管理的程序包括：

- 認識公司的目標；
- 識別在達致或不能達致目標的過程中出現的風險，以及對個別風險出現的可能性和它們帶來的影響作出評估；
- 擬訂應對風險的計劃；及
- 監察及評估風險及現存應對風險的安排。

4.2 風險可以影響很多範疇，例如：策略、運作、財務、科技及環境。較明確之風險包括：重要員工的流失，財務及其他資源大幅度被削減，發生嚴重阻礙訊息傳播的事故，火災或其他災難，以致業務被干擾及／或記錄遺失。更概括地說，風險亦包括各種問題，例如：欺詐、浪廢、濫用及管理不善。

4.3 附錄IV列舉了可能需要考慮的若干風險種類，但該清單不應被視為巨細無遺，也不是為個別行業而度身制訂的。任何一間公司所面對的實際風險，可能包括個別行業獨特的風險種類，亦與該公司的具體情況有關。

4.4 風險管理對減低企業目標受不可預見事件影響的可能性極為重要。董事會應釐定公司可接受的風險種類及程度，並致力把風險維持在這些範圍內。內部監控是管理風險其中一個主要途徑。

4.5 在商業世界中，公司的目標及公司營運的環境持續轉變，導致公司所面對的風險也不斷改變。完善的內部監控系統有賴於對公司所承擔的風險的性質及程度進行全面及定期評估。內部監控系統要有足夠的靈活性，以便在環境、公司組織及目標與活動有所變更時，能作出相應改變及調整。

4.6 因為利潤及股東價值的增加，部分是由於公司能夠成功地承擔了業務風險的回報，因此，內部監控的目的是要幫助適當地管理及監控風險，而不是杜絕風險。

4.7 完善的風險管理和內部監控的基本因素，以及有效的風險管理和內部監控所顯示的一些潛在優點於下面圖4及圖5內分別說明。

內部財務監控

4.8 有效的財務監控是內部監控的要素。財務監控有助識別及管理債務，確保公司不會面對本可避免的財務風險(例如：由衍生產品及金融工具導致的損失)，以及確保用於公司業務中及公司所公布的財務訊息的可靠性。財務監控亦有助保障資產不被挪用或流失，包括防止及偵察欺詐。

4.9 內部財務監控亦是完善的風險管理基本因素的重要一環，是支持更廣泛的業務風險管理的基礎。它必須向董事會及高級管理層提供具足夠素質的資訊，使他們能作出良好的商業決定，並遵守法規所訂之責任。內部財務監控重要的範疇包括保存正確的財務記錄，以支援財政預算、預測、其他管理訊息(例如：每月管理帳目及報告、財政預算與實際業績表現的比較)及可靠的中期和年終報告。

業務計劃及財政預算

4.10 財政預算是業務計劃中重要的管理工具及主要的監控程序。有效率及有成效的財政預算系統應與業務計劃掛鈎，結合可量度的公司目標、政策及事件優先次序的說明、達致目標的策略及資源架構。這樣能促進公司訂立更清晰的遠景、促使公司制訂適當的前瞻性計劃及有助於善用資源。因此，在制訂及監察階段，風險評估亦與財政預算及業務策劃程序有關。定期檢討業務計劃及財政預算的持續相關性，並監察財政預算的表現和進度，是至為重要的。

圖4：完善的風險管理和內部監控的基本因素

改編自英格蘭及威爾斯特許會計師公會的 *Implementing Turnbull — A Boardroom Briefing*

圖5：有效的風險管理和內部監控的潛在優點

改編自英格蘭及威爾斯特許會計師公會的 *Implementing Turnbull — A Boardroom Briefing*

5.0 將程序加以嵌入

5.1 許多僱員可能負上內部監控的部分職責，作為其達致目標的問責制度的一環。某些主要人員的責任在下文C.5.0 內有所提及，但其他人士也有各自的角色。他們整體必須擁有適當的知識、技能和訊息，以及擁有設立、操作和監察內部監控系統的職權，亦必須要了解公司、公司目標、公司身處運作的行業和市場及公司所要面對的風險。

5.2 監控系統必須嵌入公司藉以追求其目標的業務程序中。隨之而言，與其發展另一套風險報告系統，不如把預警機制納入現有的管理資訊系統內。過份繁複的風險管理程序會使其偏離重點，而這個重點就是通過把監控系統結合於現存的流程內，使公司內各人能更加專注於達致業務目標，並管理好與各人工作有關的重大風險。

5.3 透過把風險管理嵌入於公司業務程序中，公司有機會消除重複或不必要的監控及創造一個環境，在完善的風險管理實務規範下，賦予公司內各人更大的權力，以滿足顧客的需要。

5.4 要解決的其中一個主要問題，就是行政管理層如何把重要的風險管理問題列入其議程中。倘若設有風險委員會，它應避免取代行政管理層的作用。它可以促使公司制訂良好的風險管理措施及提高公司的風險管理意識，但不應取替行政管理層在風險管理方面的角色。

5.5 高級管理層及董事會需自問是否有足夠而適時、相關及可靠的報告，讓他們清楚業務目標及重要風險管理的進度。舉例說，他們是否掌握足夠的、具質量的關於僱客滿意程度及僱員態度的資訊？同時當風險改變時，他們是否掌握必須的商業訊息，從而使他們能有效地作出回應？

C. 內部監控及風險管理的職責以及檢討的程序

1.0 董事會

1.1 大致而言，內部監控系統的目的是使公司能達致其業績表現和盈利之目標，與及達致公司的整體使命。在這方面，董事會認同一套清楚界定的目標是至為重要的。這些目標應在全公司內廣泛傳達。誠如先前所述，內部監控系統的直接目的是有助提供合理程度的保證，確保公司達致既定目標。就管理對完成業務目標至為重要的風險而言，內部監控扮演一個重要角色。

1.2 《守則》原則C.2說明，董事會的職責是確保公司的內部監控系統一直穩健妥善而且有效，以保障股東的投資及公司的資產。為履行此職責，董事應最少每年檢討一次公司及其附屬公司的內部監控系統是否有效，並在《企業管治報告》中向股東匯報已經完成有關檢討。有關檢討應涵蓋所有重要的監控方面，包括財務監控、運作監控及合規監控以及風險管理功能(《守則》條文第C.2.1條)。

1.3 董事會於每份中期報告日前評估公司於報告期內發生而對公司已有重大影響，或在合理程度上可能有重大影響的內部監控系統的任何轉變，是一項良好實務。在中期報告內，公司亦應考慮是否披露內部監控系統任何重大失誤或弱項及其對公司的影響，讓投資者及公眾人士評估公司的狀況。

檢討內部監控及風險管理的有效性

1.4 雖然管理層須就設計、運作及監察內部監控系統向董事會負責，並向董事會保證已經完成有關工作，但檢討內部監控系統是否有效屬董事會職責的重要部分。董事會需要根據管理層所提供的資訊及保證，作出適當及仔細的查詢後，就內部監控是否有效發表意見。

1.5 董事會可以委派董事會委員會，例如：審核委員會(亦見下文C.4.0)、風險管理委員會等，處理檢討工作的細節。該等委員會的檢討工作範疇是經董事會考慮各種因素而釐定，例如：董事會的人數及結構、公司業務規模、業務多元性及公司運作的複雜程度，以及公司所面對重大風險的性質。

1.6 若董事會委派董事會委員會進行本指引內屬於董事會的工作，有關委員會的工作結果應予匯報給董事會，由董事會審閱。考慮到董事會負上在《企業管治報告》內有關內部監控披露事宜的最終責任，全體董事須經適當及仔細查詢後，對有關檢討工作是否足夠發表意見。

檢討程序

1.7 持續有效的監控是完善的內部監控系統的要素。然而，董事會不應是被動，並且不應只依據公司內的嵌入監察程序以履行其職責。董事會應定期收取及審閱內部監控報告。

1.8 此外，董事會須對公司及其附屬公司的內部監控系統的有效性進行每年評估，以便在《企業管治報告》內作出內部監控系統的公開聲明。有關評估必須涵蓋財務報表所涉及的期間，以及(在適當情況下)直至有關年報及財務報表批准日止的非常重大事項。

1.9 董事會應規定其檢討內部監控之有效性所擬採用的程序。這應包括在年度內呈交董事會審閱的報告的範疇及頻次，以及年度評估的程序，從而使董事會擁有可靠及適當的文件，以支持其在《企業管治報告》內所作的內部監控聲明。

1.10 被委派對內部監控系統提供意見的管理層或其他人士(例如：內部核數師)，應不時向董事會或指定的董事會委員會提交工作報告，匯報公司現時最新的監控情況。事實上，這是一個持續評估程序，以確保所有重要業務均已納入評估的範疇。

1.11 就報告所涵蓋的範疇，董事會應明確表示希望報告能夠對重要風險及內部監控系統能否有效地管理該等風險作出中肯的評估。已經識別的任何重大監控失誤或弱項，包括這些監控失誤或弱項已經、或可能已經或可能將會對公司產生的影響，以及糾正這些失誤或弱項所採取的行動，應在報告內加以討論。管理層與董事會就風險及監控事宜進行坦誠的溝通是至為重要的。

1.12 關鍵風險指標及嵌入的監察措施所產生的結果，應持續地向董事會及指定的委員會匯報，而董事會主席應鼓勵在每次董事會會議上討論風險管理及內部監控事項，並把該等事項列入董事會一般會議議程內。其他委員會(例如：行政及審核委員會)作出的報告，也提供了討論風險及監控問題的機會。

1.13 於年度內審閱報告時，董事會應：

- 考慮哪些是重要風險及評估如何識別、衡量及管理該等風險；
- 特別就已經匯報的任何內部監控失誤或弱項，評估有關內部監控系統在管理重大風險方面的有效性；
- 考慮是否即時採取必要的行動，以糾正內部監控的任何重大失誤或弱點；及
- 考慮評估結果是否表示有需要進一步擴大內部監控系統的監察範圍。

1.14 在《企業管治報告》中就對公司內部監控系統作出公開聲明所進行的年度評估工作，董事會應考慮其於年度內所審閱的有關報告中所處理過的任何問題，以及其他額外的必須資料，以確保於檢討年度內及直至有關年報及財務報表批准日止，董事會已經考慮過公司內部監控系統的各重要方面，包括財務、運作和合規監控以及風險管理之功能。

1.15 進行年度評估時，我們也鼓勵董事會考慮《守則》C.2.2段內列明為「建議最佳常規」的各事項。

1.16 倘若董事會於任何時間知悉內部監控系統有任何重大失誤或弱項，應決定這些失誤或弱項是如何產生，及應重新評估管理層對內部監控系統的設計、運作及監察的持續程序是否有效。董事會可能需要考慮是否應及時披露內部監控系統的任何重大失誤或弱項及其對公司的影響，特別是有關資料可以被視為價格敏感的資料，讓投資者及公眾人士能夠衡量公司的狀況。

1.17 為對內部監控的有效性進行客觀評估，董事及管理層應制訂一套標準，作為判斷的基礎。

匯報內部監控及風險管理

1.18 在敍述公司如何應用《守則》原則 C.2的聲明中，在適用時，董事會至少應披露：

- 公司設有識別、評估及管理公司所面對而威脅其達致業務目標的重大風險的持續程序；
- 公司於檢討年度內及直至有關年報和財務報表批准日止已經設有內部監控系統；及
- 內部監控系統於檢討年度內已經由董事會進行檢討。

1.19 董事會亦可考慮披露公司的內部監控系統是否符合本指引內列明的原則。

1.20 董事會可考慮在《企業管治報告》內提供額外資料，以幫助投資者了解公司的風險管理程序及內部監控系統。

1.21 關於應用《守則》原則C.2 的披露事宜，應包括董事會作出的確認聲明，說明董事會負責確保公司維持一個完善、有效的內部監控系統及檢討該系統的有效性。

1.22 董事會也應解釋該系統是用作管理風險，以達致公司的業務目標，而不是杜絕失誤風險，而該系統只能對這方面提供合理但不是絕對的保證。此外，該系統不能保證不會發生重大錯報或損失。

1.23 根據《守則》條文第C.2.1 條，董事會應概述其(如適用，透過其委員會)檢討內部監控系統的有效性所採用的程序。董事會也應披露其處理在年報及財務報表內所披露的有關重要內部監控的任何重大問題的程序。

1.24 《主板上市規則》附錄二十三及《創業板上市規則》附錄十六第三段列明在《企業管治報告》中建議披露的內部監控資料。這些就是我們鼓勵上市公司在其《企業管治報告》中評述的範疇，但其所需的詳盡程度，則視乎上市公司業務活動的性質及複雜性而可能有所不同。

1.25 倘若董事會不能作出上文C.1.18及 C.1.23段所述的一項或多項披露資料，也應考慮說明事實並給予解釋。《守則》規定，倘若董事會未能對公司及其附屬公司的內部監控系統或其任何一部分是否有效進行檢討，應作出披露並提供經過深思熟慮得出的理由。

1.26 董事會應確保所披露的資料為有意義的資料，而且並無給人有誤導的感覺。董事會應參考《主板上市規則》第2.13(2) 條，說明上市公司及其董事於披露資料時所應採用的一般性原則。

2.0 董事會政策

2.1 內部監控系統由不同人士執行，而公司內的許多人士都會承擔內部監控的部分角色及職責，作為其對達致目標的問責的一環。

2.2 如上文所述(見C.1.2段)，董事會是最終負責公司內部監控系統的。董事會應制訂適當的內部監控政策，並應索要、取得及評估由行政管理人員、公司核數師和其他有關人士(如適用者)對內部監控結構的每個元素(見上文B.2.2段)所編製的有關資料，讓董事會滿意該系統及程序是有效地運作的。

2.3 董事會應進一步確保內部監控系統有效地把風險經已批准的方式監控，及維持在已批准的範圍內。

2.4 在釐定內部監控政策，及藉此評估在公司的獨特情況下構成完善的內部監控系統的元素時，董事會應詳細考慮以下因素：

- 公司面對的風險的性質及程度；
- 董事會認為公司可以承受的風險的程度及種類；
- 風險實現的可能性；
- 公司減低風險實現的能力及減低這些風險實現時對業務產生影響的能力；及
- 把特定監控系統的運作成本與管理有關風險所獲得的益處相對比。

2.5 董事會首要採取正確的態度及傳遞一個清楚的信息，說明各人應認真地負上監控職責，這是至為重要的。為達致這目標，董事會可自問，例如：**公司對風險管理及內部監控抱有正確的態度嗎？**一些事項會顯示出有需要改變對風險管理及內部監控的行為和心態。這些事項包括：

- 董事會認為風險管理「不是他們的問題」；
- 公司只關注內部財務監控方面而不是更廣濶層面的內部監控；
- 董事會對業務目標缺乏共識；
- 檢討內部監控系統只被視為是為了遵守規例及作出公開聲明而進行的工作，而不是業務的一部分；
- 風險管理被視為某項功能的責任，例如：審核或保險；
- 缺乏已確定的關鍵風險指標；及
- 僱員缺乏風險意識的培訓或經驗。

2.6 許多公司的董事會都是透過功能委員會(例如：審核、薪酬及提名委員會)履行其職責。不同的委員會可以從不同的觀點分別為內部監控元素提供意見，亦可以在有關政策事項上向董事會提供協助。

3.0 內部審核功能

3.1 《守則》C.2.5段說明，沒有內部審核功能的公司，應每年檢討是否需要增設此項功能，然後在其《企業管治報告》內披露檢討結果。

3.2 公司設有內部審核功能，定期監察關鍵監控及程序，是一項良好實務。該等定期監察是公司內部監控系統的組成部分，有助確保監控系統的有效性。

3.3 內部審核可以透過以下途徑對公司作出重大和有價值的貢獻：

- 對風險管理，特別是環繞內部監控系統的設計、執行及運作方面提供建議；
- 藉着識別節省監控成本的機會，與及減低運作上及有關的損失，從而加強風險管理和監控管理的效率及成效；及
- 提升公司內的風險及監控概念，例如：透過舉辦或推行自我評估監控計劃。

3.4 內部審核功能可以提供各方面的收益。倘若有適當資源，它應可以：

(a) 就公司的風險管理及內部監控的架構是否足夠及有效向董事會及管理層提供客觀保証；

(b) 幫助管理層改善用以識別及管理風險的程序；及

(c) 協助董事會履行其加強及改善風險管理和內部監控架構的職責。

3.5 然而，是否需要設有內部審核功能則要視乎個別公司之特性。這些特性包括公司業務活動的規模、結構、多元化程度和複雜性、僱員數目、公司的企業文化以及成本／效益等。高級管理層及董事會可能希望取得風險及監控的客觀保証及建議。獲足夠資源分配的內部審核功能(或具有其相同性質的功能，例如：合資格的獨立第三方受僱進行一部分或全部有關工作)可提供這類保証及建議。公司內可能有其他功能，同樣提供涵蓋專門範疇(例如：健康與安全、規則與法例的遵守及環保問題)的保証及建議。

3.6 倘若缺乏內部審核功能，管理層需應用其他監察程序，向本身及董事會保證內部監控系統按既定方針運作。在這些情況下，董事會需要評估該等監察程序能否提供足夠及客觀的保証。

3.7 董事會在評估是否有需要設置內部審核功能時，應考慮是否存在與公司業務活動、市場或公司其他方面相關的外在環境的任何趨勢或當前因素，而這些趨勢或因素已增加或預期會增加公司所面對的風險。風險增加也可能由內在因素導致，例如：機構重組、滙報程序或相關資訊系統的改變。其他要考慮的事項包括由內部監控系統的監察工作或意外事件發生的次數增加所顯示的不利趨勢。

3.8 我們鼓勵未有設立內部審核功能的公司的董事會，在其每年評估是否有需要增設此項功能時，應考慮上文C.3.5及C.3.7段所述之因素。

3.9 倘若公司已設有內部審核功能，我們建議董事會在每年檢討內部審核之工作範疇、職權及資源時，亦須考慮包括上文C.3.5及C.3.7段所述之因素。

4.0 審核委員會

4.1. 審核委員會在公司的監控及風險管理架構上(包括在檢討程序中)擔當重要角色。《主板上市規則》第3.21條及《創業板上市規則》第5.28條規定每間上市公司須設立審核委員會。

4.2 審核委員會的職權範圍至少應包括《守則》條文第C.3.3條所載的職責，當中包括以下與監管上市公司財務申報制度及內部監控程序有關的職責：

- 檢討公司的財務監控、內部監控及風險管理制度；
- 與管理層討論內部監控系統，確保管理層已履行職責，建立有效的內部監控系統；
- 主動或應董事會的委派，就有關內部監控事宜的重要調查結果及管理層對該等結果的回應進行研究；
- 如公司設有內部審核功能，須確保內部和外聘核數師的工作得到協調；也須確保內部審核功能在公司內部有足夠資源運作，並且有適當的地位；以及檢討及監察內部審核功能是否有效；
- 檢討集團的財務及會計政策及實務；及
- 檢查外聘核數師給予管理層的《審核情況說明函件》、核數師就會計記錄、財務帳目或監控系統向管理層提出的任何重大疑問及管理層作出的回應。

(有關審核委員會角色及職責的更詳盡指引，請參考公會於二零零二年二月出版的*《審核委員會有效運作指引》*。)

5.0 系統中的其他各方

行政管理層

5.1 行政管理層是直接負責執行董事會制定的整體策略及政策，以及負責公司的一切活動，包括內部監控系統的運作。然而，各級管理層有不同的內部監控職責，這取決於公司的特性。

高級行政人員

5.2 行政總裁專責行政管理的一切事宜，並就公司的表現和董事會策略及政策(包括風險及監控政策)的執行方面向董事會負責。

5.3 行政總裁應聯同其他高級行政人員，認定及評估公司面對的風險，匯報予董事會作考慮。他們同時負責設計、操作及監察適當的內部監控系統，以執行董事會制訂的政策。他們須確保存在正面的監控環境，以及內部監控的所有組成部分均設置得當。他們亦須領導及指導其他負責主要功能範疇的高級經理，定期檢討他們的職責及他們監控業務的方式。

5.4 《主板上市規則》第3.24條及《創業板上市規則》第5.15條規定，每間上市公司必須聘有一名全職「合資格會計師」，該名人士須屬高級管理人員，其職責*「必須包括監督發行人及其附屬公司的財務匯報程序及內部監控，以及遵守《上市規則》有關財務匯報及其他涉及會計事宜的規定」*。因此，根據上市規則，合資格會計師有責任監督與財務功能有關的內部監控。

5.5 財務總監亦可能是合資格會計師，一般擔當重要的監察角色。財務總監通常參與制訂及編製全公司的預算及計劃，有關工作須追蹤及分析整間公司的表現，不僅在財務方面，還要從運作及合規的方面着眼，範圍涵蓋各業務部門、附屬公司及其他業務單位的一切活動。因此，財務總監一般是管理監控的中心點。

5.6 就其職務而言，財務總監應參與以下有關程序，例如：確立公司目標及確定策略，分析風險及就如何管理影響公司的轉變／風險而作出決定。財務總監可就以上事宜提供寶貴意見及指示，並處於適當位置以專注於監察及跟進已決定採取的行動。

監察總監

5.7 監察總監(若設立此職位)的職責至少應包括以下各項：

(i) 確保董事會完全知悉董事會採用的運作框架；

(ii) 確保董事會依照既定程序運作；及

(iii) 協助董事會執行為確保公司符合所有適用的法律規章與最佳實務的程序，並向董事會提供相關建議。

運作人員

5.8 負責組織單位(即個別部門／分部)的高級經理，可能獲指派負責制訂及執行針對其屬下單位目標的內部監控政策及程序，並確保它們與全公司的目標保持一致。

5.9 單位經理在為單位職能制訂及執行特定之內部監控程序上，通常擔當更親力親為的角色。他們可能被要求就監控作出建議、監察其運作及向上級經理匯報有關監控的執行情況。

5.10 監督人員直接參與詳細執行監控政策及程序的具體工作。他們可能被要求就例外情況及出現的其他問題採取行動，並向上級管理層匯報任何重要的事情，不論該等事情是關於某一項交易或顯示有更廣泛的影響的迹象。

附錄 I

摘錄自《上市規則》有關「內部監控」的規定

《企業管治常規守則》

C.2 內部監控

原則

董事會應確保發行人的內部監控系統穩健妥善而且有效，以保障股東的投資及發行人的資產。

守則條文

C.2.1 董事應最少每年檢討一次發行人及其附屬公司的內部監控系統是否有效，並在《企業管治報告》中向股東匯報已經完成有關檢討。有關檢討應涵蓋所有重要的監控方面，包括財務監控、運作監控及合規監控以及風險管理功能。

建議最佳常規

C.2.2 董事會每年檢討的事項應特別包括下列各項：

(a) 自上年檢討後，重大風險的性質及嚴重程度的轉變、以及發行人應付其業務轉變及外在環境轉變的能力；

(b) 管理層持續監察風險及內部監控系統的工作範疇及素質，及(如適用)內部核數功能及其他保證提供者的工作；

(c) 向董事會(或旗下委員會)傳達監控結果的詳盡程度及次數；透過有關傳達，董事會得以對發行人的監控情況及風險管理的有效程度建立累積的評審結果；

(d) 期內任何時候發生重大監控失誤或發現重大監控弱項的次數，及因此導致未能預見的後果或緊急情況的嚴重程度，而該等後果或情況對發行人的財務表現或情況已產生、可能已產生或將來可能會產生的重大影響；及

(e) 發行人有關財務報告及遵守《上市規則》規定的程序是否有效。

C.2.3 作為《企業管治報告》的部分內容，發行人應以述形式披露其如何在報告期內遵守有關內部監控的守則條文。有關披露內容也應包括下列事項：

(a) 發行人賴以辨認、評估及管理所面對的重大風險所採取的程序；

(b) 任何有助了解發行人風險管理程序及內部監控系統的額外資料；

(c) 董事會承認其須對發行人的內部監控系統負責，並有責任檢討該制度的有效性；

(d) 發行人檢討內部監控系統是否有效所採取的程序；及

(e) 發行人就處理於年度報告及賬目內所披露的有關重要內部監控事項的重大問題所採取的程序。

C.2.4 發行人應確保所披露的是有意義的資料，而且沒有給人有誤導的感覺。

C.2.5 沒有內部核數功能的發行人應每年檢討是否需要增設此項功能，然後在其《企業管治報告》內披露檢討結果。

《企業管治報告》

強制披露要求

2. 上市發行人須列載其年報所涵蓋會計期間的以下資料，以及在切實可行的情況下盡量包括於刊發年報當日之前期間任何關於以下資料的重大事項：

註：除上述披露責任外，載於《守則》內的守則條文預期發行人於其《企業管治報告》中作出若干具體披露。發行人若選擇不作有關的預期披露，必須按第2(a)(iii)段規定，就其偏離行為提供經過深思熟慮得出的理由。為方便發行人參考起見，以下列出守則條文所預期的具體披露內容：

3 說明董事會經已檢討發行人及其附屬公司的內部監控系統是否有效（《守則》第C.2.1條）；

建議披露的資料

3. 本段所載列有關企業管治的披露資料，只供上市發行人參考，但其內容並非巨細無遺亦毋須作強制遵守。有關資料傾向列載上市發行人可於其《企業管治報告》評述的範疇。其所需的詳盡程度，視乎上市發行人業務活動的性質及複雜性而有所不同。本交易所鼓勵上市發行人在其《企業管治報告》中包括以下資料：

(d) 內部監控

(i) 若上市發行人根據《守則》第C.2.1條，在年報內附載董事聲明，說明董事已經作出有關內部監控系統的檢討，則本交易所亦鼓勵上市發行人在該報告中披露以下詳情：

(aa) 闡釋如何為發行人釐定內部監控系統；

(bb) 處理及發布股價敏感資料的程序和內部監控措施；

(cc) 上市發行人是否設有內部核數功能；或當上市發行人並未設有內部核數的功能時，檢討是否須要設有這功能的結果；

(dd) 內部監控檢討的頻次；

(ee) 表示董事會已檢討內部監控系統有效性的聲明，並說明他們認為內部監控系統是否有效及足夠；

(ff) 董事評估內部監控系統的效用時所採用的準則；

(gg) 檢討所涵蓋的期間；

(hh) 任何對股東構成影響的重要關注事項的詳情；

(ii) 審核委員會提出的任何重要意見或建議；及

(jj) 如上市發行人並未於年內檢討其內部監控，須就此作出解釋；

(ii) 就上市發行人如何在報告期內遵守有關內部監控守則條文的敘述聲明（包括根據《守則》第C.2.3 段所載事項）(《守則》第C.2.3段）；及

(iii) 沒有內部核數功能的發行人每年就是否需要增設此項功能而進行檢討的結果（《守則》第C.2.5段）。

附錄 II

內部監控的概念及範圍

1. **《坎特伯里報告》(Cadbury Report)**[2] 說明董事要履行保留足夠會計記錄的職責，實際上須就公司的財務管理維持一個內部監控系統，包括設有將欺詐風險減至最低的程序。

2. **Rutteman 指引**[3] 把「內部財務監控」定義為對保護資產、保留適當會計記錄及企業內部所使用或用作發表的財務資料的可靠性進行內部監控。Rutteman 指引亦鼓勵董事檢討及匯報內部監控的一切事宜，包括為確保具效益及效率的業務運作和符合法律規章而進行的監控。

3. **Committee of Sponsoring Organizations of the Treadway Commission (COSO)**[4] 於一九九二年發表題為*《內部監控 — 綜合架構》*的報告，把內部監控定義為*「機構的董事會、管理層及其他人士為達致以下目標提供合理保證而實施的程序：*

   - *營運的效益及效率*
   - *財務匯報的可靠性*
   - *遵守適用的法律規則」*

4. COSO 以上定義對內部監控的基本概念提供了一些深入的見解，特別是：

   - 內部監控是一個達致目標的***程序***及方法，而其本身並非目標。
   - 內部監控預期***只可提供合理保證***，而非絕對保證。
   - 內部監控由公司各級***人員實施***及配合***達致目標***。

2 英國研究企業管治財務範疇委員會於一九九二年十二月在英國發表的報告。

3 英國Rutteman工作小組於一九九四年十二月在英國發表的《內部監控及財務匯報： 英國註冊上市公司董事指引》。成立該工作小組的目的，是就內部監控匯報制訂評估效益的標準，並為董事擬訂指引。

4 COSO 是於一九八五年設立的一項私營計劃，由美國五間財務專業團體共同贊助 — 美國會計協會(American Accounting Association)、美國執業會計師公會 (American Institute of Certified Public Accountants)、財經行政人員協會(Financial Executives Institute)、內部核數師協會(Institute of Internal Auditors)及美國會計人員協會(National Association of Accountants)(現稱美國管理會計師協會(Institute of Management Accountants))。COSO的目標是透過專注於企業管治、道德操守及內部監控，以改善財務匯報的素質。

5. **加拿大特許會計師公會監控標準委員會(CoCo)[5]發表的《*監控指引*》**，以COSO報告中所載的概念作為基礎，把監控定義為包含「*公司的組成元素（包括其資源、系統、程序、文化、結構及任務），而這些元素合起來支持員工達致機構的目標*」。CoCo 報告亦從另一個角度對此作出闡述：「*只要機構未能達致其目標的剩餘（不受控制）風險被認為可接受，那麼監控便屬有效*」。

5 加拿大特許會計師公會監控標準委員會（現稱風險管理及管治委員會）於一九九五年十一月在加拿大發表的《*監控指引*》。

附錄III

內部監控系統組成部分的詳情

(1) 監控環境

誠如上文B.2.2段所述，監控環境是內部監控其他元素的根基，並提供紀律及結構。監控環境因素包括人員的道德價值及勝任能力(素質)、董事會提供的指示及管理的效率。

監控環境應包括堅守誠信及高尚的道德價值。就此而言，高級管理層必須把公司的價值及行為標準向僱員明確傳達，例如透過正式的行為守則，以及高級管理層以身作則，從而鼓勵其他僱員遵守。對違反行為守則的人員作出適當懲處，亦是確保他們遵循及把行為守則融入企業文化的重要一環。

獎勵及誘惑是可能破壞深厚道德文化的陷阱。前者包括施加壓力以達致不切實際的業績目標，特別是短期業績及與業績掛鈎的豐厚報酬。後者包括無效的監控，例如在敏感的範疇職責劃分不清，予人有盜用資產或隱瞞欠佳表現的機會；薄弱的內部審核功能，未能察覺及匯報不當行為；及低效率的董事會，無法對高級管理層進行客觀的監督。

監控環境的其他方面包括：

- *堅守用人唯才的承諾*：管理層應明確說明每項工作所需的才能水平，並將其具體化為必需的知識及技巧。
- *積極投入的董事會及審核委員會*：董事會必須具備適當水平的管理、專門及其他知識，還必須擁有履行其策略及監督功能的才幹及思維。董事會成員必須保持客觀及積極詢問管理層的活動。審核委員會亦應擁有具備適當經驗、合資格、獨立及積極的成員。
- *分配權力及責任，以及行動問責性*：這包括確立匯報關係及授權協定。其中主要的挑戰是下放權責並限於達致目標所需的程度，且要確保風險的接受是基於識別風險及盡量減低風險的合理措施。另一項重要挑戰是確保所有僱員明白公司的目標。監控環境在很大程度上取決於個人對他們將負有多大責任的了解。
- *組織架構*：公司的架構須加以組織、使制訂的策略得以最有效的貫徹施行，從而達致特定目標，並提供所需的資訊流，以致可適當地管理公司的活動。
- *人力資源政策及實務*：持續教育及訓練(例如在道德操守、職務、職責、科技及市場發展等方面的訓練)是十分重要的，同樣重要的是表現反饋及評估、以及提供具競爭力的薪酬福利招攬有才之士。

(2) 風險評估

如上文所述(見B.2.2段)，*風險評估*涉及識別及分析達致目標可能遇上的風險，包括與監管和營運環境轉變及業務策略有關的風險，以此作為釐定應如何減低及管理風險的依據。

確立目標

風險影響公司生存及成功競爭的能力。董事會及管理層必須審慎決定可承擔的風險，並力求把風險維持於這一水平之內。確立目標是風險評估及管理的前提條件， 儘管它不是內部監控的組成部分，但卻是確保內部監控得以執行的先決條件。

因此，確立清晰的業務目標是十分重要的。這些應是未來的目標而非過去或現在的目標，同時亦應注意該等是可達致的目標。董事會應考慮現有目標是否至少能應付未來兩至三年其可能面對的挑戰。

通過在公司層面確立遠大的目標，以及在活動層面確立更具體的目標，機構便可確定達致目標的關鍵因素。

雖然不同類別的個別目標可能出現重疊，但仍可根據以下廣泛類別加以界定：

- *營運目標*：這些目標與完成公司的基本使命和處理公司的營運效益及效率有關，包括表現及盈利目標和防止資源流失。
- *財務匯報目標*：這些目標與編製可靠的公開財務報表有關，包括中期報告及財務摘要報告等資料。它們主要是因應外在的規定而制訂。
- *合規目標*：這些目標與公司遵守適用的法律、規則及規例有關，此等規定涉及市場(包括持續上市責任及專門的行業規例)、定價、稅務、環境、僱員福利及國際貿易。

公司的整體目標應分拆成較明細的目標，與整體策略保持一致並與整間公司的活動保持聯繫。活動目標亦需清晰及易於被負責有關活動的員工所理解，並應可以衡量。

風險識別及評估

識別風險可運用不同的技術，包括：由外聘及內部核數師為界定公司的活動範圍而開發的技術、定期檢討影響公司的經濟行業因素、高級管理層會議及與業內分析員會面。不論採取甚麼方法，管理層須仔細考慮促成或增加風險的因素，包括以往未能達致目標的教訓；僱員素質；競爭加劇等重大轉變；立法、監管及人事方面的變更；市場發展；特定活動對公司的重要性及其複雜性。

風險亦應在活動層面上加以識別，這有助把風險評估集中於主要業務單位或功能上，同時也有助把公司層面的風險保持於可接受的水平。

對公司達致目標所面對的重大風險作出初步識別後，就以下問題在公司內進行廣泛諮詢可能有所幫助：

- 對公司業務目標、業務策略及有關重大風險的認知；
- 公司的風險管理政策；
- 採納的監控策略是否有效及實施這些策略的方法；
- 良好風險管理及內部監控的基礎；
- 為減低影響公司達致其業務目標的能力的重大風險而作出改善的途徑；及
- 不斷轉變的行為。

這樣的諮詢有助確定高級管理層是否已識別所有與目標有關的重大風險，同時亦為董事會檢討內部監控的有效性及向股東匯報監控情況奠定穩固的基礎。

繼識別公司及活動層面的風險後，應進行風險分析。風險的重要性及可能性一經評估，管理層需考慮如何管理風險。視乎風險的性質，減低風險出現的重要性或可能性而可以採取的行動包括：確定後補供應商、獲取更適用的營運報告及改善培訓方案等。識別已轉變的環境及按需要採取行動的程序對風險評估十分重要，有關轉變可包括如下事宜：

- *營運環境改變*：例如由於撤銷監管、定價受到的公眾壓力增加等因素導致改變。
- *新入職人員*：要員更替；員工流失率高，加大培訓及監察的壓力。
- *新資訊系統*：在開發新系統時，尤其在時間緊迫的情況下，未能實施有效的監控。
- *業務出乎意料迅速地增長*：當業務大幅地增長及迅速地擴充時，現有的監控系統可能不勝負荷。
- *新產品系列或活動*：當公司從事其不熟悉的業務或進行不熟悉的交易，現有的監控可能有所不足。
- *公司重組*：重組及削減成本的計劃可能導致員工流失及對僱員缺乏充分的監察及／或缺乏明確的職責劃分。
- *擴充海外業務*：由於市場環境及地方文化等方面的差異，把業務擴展至外國市場可能招致獨特的風險。

確定相關及重要轉變的機制應盡可能具前瞻性，而早期預警系統應準備妥當，以識別數據傳輸的新風險。

區分風險的優先次序

風險可根據其影響及可能性而區分優先次序，例如：

A. 需立即採取行動

B. 考慮採取行動及制訂應急計劃

C. 考慮採取行動

D. 定期檢討

公司不應只從財務角度考慮風險的影響，更重要的是考慮其對達致公司目標的潛在影響。並非所有風險均被界定為重大風險。公司對非重大風險亦應定期加以檢討，尤其在外界環境轉變時，以查證這些風險是否仍屬非重大風險。

識別全部重大風險並區分其優先次序後，確定以下各項要點會有所幫助：(a) 董事是否願意承擔此風險，(b) 甚麼監控策略可避免或減低全部風險，(c) 誰人負責管理風險和維持及監察監控，(d) 有甚麼剩餘風險，亦即實施監控程序後剩餘的風險，及(e) 有甚麼早期預警機制？

以下逐一列出這些要點：

(a) 每一項風險都應從其對公司目標的影響方面作出考慮。董事會應決定經識別的風險是否超過達致目標所獲得的收益，亦即風險若超過回報，是否值得為完成該特定目標而繼續努力？假如決定繼續下去，董事會必須採取具體的監控策略，以決定如何應對風險。

(b) 監控策略包括：

- 承擔風險；
- 轉移風險（例如通過更改合約條款把風險轉移至另一方）；
- 消除風險（通過採取退出策略）；

- 監控風險(例如：通過把監控納入運作程序中，加強品質控制，委任最佳的員工負責管理)；
- 與另一方共同承擔風險；及
- 為部分或所有風險購買保險。

(c) 不應委派一人承擔管理全部風險的責任，理想的做法是由管理不同業務活動的人員分別承擔。

(d) 實施監控策略後，公司可考慮釐定剩餘的風險水平。如上文所述，有一要點要注意，要完全杜絕風險並不可能。公司須知道其面對的風險水平及如何對此進行管理。假如存在風險，它們必須是合理的風險，而非未受注意或未被充分考慮的風險。董事會須釐定其風險承受力，亦即願意承擔的風險水平，而公司的業務目標必須配合董事會的風險承受力。就重大風險而言，則須考慮風險／回報比率是否適當。

(e) 早期預警機制是在問題演變成為重大事故前，以及在可採取行動減輕或解決問題的階段，提醒董事會及高級管理層保持警覺的匯報程序。公司可訂立「主要風險指標」(作為早期預警機制的一種形式)，以及早顯示潛在問題，從而迅速採取補救措施。

應當注意的是，儘管風險評估屬內部監控系統的一部分，但處理風險的計劃、方案及需要採取的行動均屬整體管理程序的重要部分，而非內部監控系統的元素。

(3) 監控活動

如上文所述(見B.2.2段)，*監控活動*包括多種政策及程序，有助確保有關管理指示得以執行，以及處理風險以達致公司目標所需的行動得以進行。這可能包括批准及查證、檢討、保護資產及劃分職責。監控活動可區分為營運、財務匯報及符合法例規則三個類別，然而它們之間有時可能出現若干重疊。公司各級人員進行的常見監控活動如下：

- *最高層檢討*：例如把實際表現與預算、預測、先前期間的表現及競爭對手的表現進行比較及檢討。
- *直接功能或作業管理*：負責管理功能或作業的經理審閱表現報告。
- *資料處理*： 採取多種監控措施檢查交易的準確性、完整性及授權，例如例外情況報告。

- *實物監控*： 確保設備、存貨、證券及其他資產受到保護並定期接受檢查。
- *表現指標*： 分析不同組合的數據，如營運或財務數據及兩者之間的關係，並進行調查及／或採取補救行動。通過調查未預期的結果或不尋常的趨勢，管理層可識別可能無法達致基本活動目標的情況。
- *職責劃分*：劃定及區分不同人員之間的職責，以加強檢查及把出現錯誤或弊端的風險減至最低。

儘管規模較小公司的內部監控程序一般不太正規及較具靈活性，但仔細、認真及一貫地執行內部監控的有關政策及程序乃是十分重要。

評估風險只是整個監控程序的一部分，除風險評估外，管理層須確定處理風險所需的行動，並將之付諸實行。這些行動亦帶出把注意力集中於監控活動的作用，目的是確保所需的行動得以有效及適時的執行。

由於財務及其他數據非常依賴資訊系統，因此須對資訊系統進行監控。這些包括COSO報告所指的(a)「一般監控」，亦即確保系統維持正常運作的監控，例如備份及復原程序、應急或災難復原計劃，以及系統保安；及(b)「應用監控」，包括監控處理不同類別交易的應用軟件及相關人工程序的步驟。

(4) 資訊及溝通

如上文所述(見B.2.2段)，*資訊及溝通*是指讓僱員能夠在履行職責的範圍及時間內，識別、取得及匯報營運、財務及法規遵守的相關訊息的有效程序及系統。從廣義方面來說，這包括由最高管理層把與監控有關事宜的重要性及個人擔當的角色向下傳達、向上級滙報重要訊息的渠道，以及與外界利益相關者保持有效的溝通。

資訊

有關資訊必須以適當的形式，並在適當的時限內加以識別、收集及傳達，從而使管理層能據此作決策及採取適當的行動。

資訊系統提供營運、財務及與法規遵守有關的資料(包括由內部產生及外界提供的資料)，這些資料有助運作及監控業務，亦是決策及對外匯報所必需的根據。

當面對重大的行業轉變時，特別是對富於創新精神及快速流轉的行業而言，此等系統必須能夠配合支持新的機構目標的需要。

資訊系統可以是正式或非正式的。後者包括與客戶、供應商、監管機構及僱員進行商討，可為協助識別風險及商機提供有用資料。出席商務講座和加入貿易、專業及其他團體成為會員亦是提供相關資料的來源。

系統產生的資訊的素質會影響管理層作出適當決定的能力。報告中載有足夠的相關資料以支持有效的監控是十分重要，而系統的設計應針對這方面。就資訊素質而言，須確定以下問題的答案：

- *內容：* 內容是否適當？
- *時限：* 在需要時是否可以即時取得？
- *更新性：* 是否最新資訊？
- *準確性／可靠性：* 是否正確及可靠？
- *容易取得：* 是否各有關人士都可輕易取得？

溝通

總體而言，有效溝通必須在公司內以全方位方式進行。高級管理層應向僱員傳達清晰的訊息，使他們了解監控責任必須認真履行。他們必須明白本身在內部監控系統中擔當的角色，以及個人活動如何跟其他人的工作有所關連。他們亦須清楚把重要資訊向上級滙報的方法，公司就此需要設立公開的溝通渠道，而上級人員亦需採取樂意傾聽的態度。一個讓僱員懼怕因匯報有關資訊而遭受報復的環境，將令目標功敗垂成。

僱員必須獲告知每當有無法預計的事情發生，不僅要注意事件本身，還要注意確定事件的起因。他們須知道其活動如何跟其他人的工作有所關連，以及甚麼行為會被認為是合理或可被接受，而甚麼行動是不會被接受的。

管理層與董事會及董事會轄下各委員會之間的溝通尤為重要。管理層必須就公司的業績、發展、重大風險，主要計劃及其他有關事項不斷向董事會提供最新消息。董事會則應向管理層明確表示需要甚麼資料，並應向管理層提供指示及意見。

此外，公司亦需與外界各方(例如股東、客戶、供應商及監管機構)保持有效溝通。客戶及供應商可在產品及服務的設計及素質方面，提供非常有用的意見，而跟外聘核數師及監管人員等保持溝通，則可對公司內部監控系統運作情況提供十分寶貴的意見。與股東及財務分析師等進行坦誠溝通，從而提供他們所需要的資料。

(5) 監察

內部監控系統須接受監察。如上文所述(見B.2.2段)，*監察*是不斷評估內部監控系統表現素質的程序，包括持續的監察活動及單獨的評價。內部監控如有缺陷，應向適當的上級管理層匯報，例如高級管理人員、審核委員會或董事會。

監察可確保內部監控保持有效的運作，當中包括由適當人員評估監控的設計及運作情況，以及採取適當的跟進行動。監察除可應用於公司內的活動，亦可應用於為公司提供相關服務的外界承包商。

管理層為對內部監控系統的有效性取得合理保證而需對內部監控系統進行獨立評價的頻次，屬於判斷性質問題。在作出有關判斷時要考慮的因素包括：所發生轉變的性質及程度和伴隨的風險、執行監控人員的才能及經驗，以及持續監察的結果。由於持續監察程序為公司經常性營運活動的組成部分，且實時執行及可因應轉變作出調整，因此，原則上它們應較單獨評價所執行的程序更加有效。

由誰進行評價？

評價許多時是採取自我評估的方式進行，由負責特定單位或職能的僱員決定監控對其活動的有效性。業務部門的行政主管可率先作出評價，並可親自評估監控環境因素。業務經理可專注於運作及合規目標，而部門主管可專注於財務匯報目標。公司管理層負責檢討部門所作之評估，以及其他業務部所作出的評價。

內部核數師通常以評價內部監控作為其日常職責的一部分，他們亦會應董事會或高級管理層的要求而執行該項工作。外聘核數師的工作亦可用於考慮內部監控的有效性。

文件記錄

內部監控系統的文件記錄，隨公司的規模及複雜性等而有所不同。大型機構多半備有書面政策手冊、正規的組織架構圖、書面職務說明、操作指示及資訊系統流程圖等等。規模較小的公司可能備有較少的文件記錄，但這並不必然表示它們的內部監控沒那麼有效。然而，適量的文件記錄能令評價變得更具效率， 亦有助僱員了解系統如何發揮作用及他們在其中所擔當的角色，同時在有需要修改系統時令工作變得更加輕鬆暢順。

匯報缺陷

所有可影響公司達致目標的內部監控缺陷，應向能採取必需行動者匯報。

僱員從事經常性營運活動所產生的資料，通常透過正常渠道向他們的上級匯報，再由後者向其上級或同級人員(視乎適當情況)匯報。此外，還應有另一渠道供匯報非常敏感的資料，例如非法或不當舉動。在通常情況下，有關缺陷的調查結果不僅應向負責有關職能或活動的個人匯報，使其得以採取補救行動，還應向較其至少高一級的管理層匯報。此程序讓較高級的人員可監督及支援採取補救行動，同時有助把訊息傳達予公司內活動亦可能受到影響的其他人士。

向適當人士提供有關內部監控缺陷的資料，對保持系統的有效性尤其重要。公司可訂立規則，以確定某一職級人員作決策時所需的資料。獲傳達有關內部監控缺陷資料的人士可就須匯報的資料給予明確指示。舉例來說，董事會或審核委員會可要求管理層或內部或外聘核數師只匯報其所發現的，而又達到一定程度嚴重性或重要性的內部監控缺陷的調查結果。

附錄IV

公司可能面對的風險

業務風險

- 錯誤的業務策略
- 價格／市場佔有率受到的競爭壓力
- 全球／區域經濟問題
- 行業衰退
- 政治風險
- 不利的政府政策
- 忽視策略及實施方面的資訊科技層面
- 技術過時
- 替代產品
- 成為收購目標
- 無法獲取更多資本
- 不利的收購
- 改革及再造的步伐過慢
- 回應市場及客戶需求過慢

財務風險

- 市場風險
- 信貸風險
- 利息風險
- 貨幣風險
- 金融風險
- 流動資金風險
- 過度交易
- 高昂的資本成本
- 財務資源不當使用
- 持續經營問題
- 出現對業務敏感的欺詐
- 有關公布失實財務資料的風險
- 會計系統故障
- 不可靠的會計記錄

- 未記錄的負債
- 資訊科技系統受黑客入侵及攻擊
- 根據不完整或錯誤資料作出決定
- 資料太多但分析不足
- 向投資者作出無法履行的承諾／保證

合規風險

- 違反《上市規則》
- 違反財務法規
- 違反《公司條例》規定
- 違反競爭法規
- 違反其他規例及法律
- 訴訟風險
- 稅務問題
- 健康及安全風險
- 環境問題

營運及其他風險

- 缺乏效率／效益的管理程序
- 業務程序未能配合客戶／市場需求及策略性目標
- 喪失企業家精神
- 錯失或忽視商機
- 其他商業誠信問題
- 導致影響信譽的其他問題
- 品牌管理欠佳
- 主要改革計劃失敗
- 無法實施改革
- 原料缺貨
- 缺乏技巧
- 自然災害(例如火災及爆炸)
- 電腦病毒或其他系統故障
- 未能創造及利用無形資產
- 損失無形資產
- 損失有形資產
- 損失要員

- 損失主要合約
- 缺乏訂單
- 業務無法持續
- 繼任問題
- 無法降低成本基礎
- 過度依賴主要供應商或客戶
- 主要客戶施加嚴苛的合約責任
- 新產品或服務不合格
- 未能滿足客戶
- 服務水平欠佳
- 品質問題
- 產品責任
- 主要項目失敗
- 與科技有關的大型項目失敗
- 外包供應商未能交貨
- 僱員缺乏動力或效率
- 工業行動
- 發展中國家剝削僱員所引起的問題
- 文件的處理缺乏效率／效益
- 違反保密原則

改編自英格蘭及威爾斯特許會計師公會的 *Implementing Turnbull — A Boardroom Briefing*

附錄V

參考書目

1. *審核委員會有效運作指引(2002年)*
香港會計師公會

2. *香港聯合交易所有限公司證券上市規則(《主板上市規則》)*
香港聯合交易所有限公司

3. *香港聯合交易所有限公司創業板證券上市規則(《創業板上市規則》)*
香港聯合交易所有限公司

4. *研究企業管治財務範疇委員會報告(Report of the Committee on the Financial Aspects of Corporate Governance)(又稱"坎特伯里報告(Cadbury Report)")(1992年)*
企業管治財務範疇委員會(又稱"坎特伯里委員會(Cadbury Committee)"), 英國

5. *內部監控及財務匯報:英國註冊上市公司董事指引(Internal Control and Financial Reporting: Guidance for directors of listed companies registered in the UK)(1994年)*
Rutteman Working Group, 英國

6. *企業管治委員會:最後報告(Committee on Corporate Governance: Final Report)(又稱"Hampel報告")(1998年)*
企業管治委員會, 英國

7. *內部監控:綜合守則的董事指引(Internal Control: Guidance for Directors on the Combined Code)(又稱"Turnbull指引")(1999年)*
英格蘭及威爾斯特許會計師公會

8. *Implementing Turnbull — A Boardroom Briefing*
英格蘭及威爾斯特許會計師公會

9. *內部監控 — 綜合架構(Internal Control — Integrated Framework)(1992年)*
Committee of Sponsoring Organizations of the Treadway Commission, 美國

10. *Board Briefing on IT Governance, 2nd Edition(2003年)*
IT Governance Institute, 美國

11. *企業風險管理 — 綜合架構 (Enterprise Risk Management — Integrated Framework)(2004年)*
Committee of Sponsoring Organizations of the Treadway Commission, 美國

12. *Internal Control Reporting — Implementing Sarbanes-Oxley Section 404 (2004年)*
美國執業會計師公會

13. *Management's Report on Internal Control over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports — Frequently Asked Questions (2004年)*
Office of the Chief Accountant Division of Corporation Finance, U.S. Securities and Exchange Commission

14. *監控指引 (Guidance on Control) (1995年)*
風險管理及管治委員會 (前稱監控標準委員會) , 加拿大特許會計師公會

15. *International Standards for the Professional Practice of Internal Auditing*
內部核數師協會

香港會計師公會
電話：(852) 2287 7228
傳真：(852) 2865 6603
電郵：hkicpa@hkicpa.org.hk
網址：www.hkicpa.org.hk