2009年內部稽核協會國際年會出國報告

摘 要

「2009年內部稽核協會國際年會」於今（98）年5月10日至5月13日首度假南非約翰尼斯堡舉行。主辦單位安排11場專題演講，及「最佳範例（Best Practices）」、「風險管理(Risk Management)」、「柔性技巧(Soft Skills)」、「資訊科技(IT)」、「舞弊(Fraud)」、「政府部門(Public Sector)」、「公司治理(Governance)」、「新興議題(Emerging Issues)」等8場同步舉行之研討會。

經就本次會議研討內容綜合彙整，分就「內部稽核專業之新標準」、「IFRS 介紹」、「公部門之內部稽核－能力成熟度模型」、「持續性稽核：成果及挑戰」、「COSO之內部控制監督指引」、「控制紛亂（Controls Chaos）－其他產業可從金融風暴學習什麼？」、「營運恢復力及持續性—確保資訊安全與可用性之災難復原」等7項議題提出研討內容，並擬具建議意見如下：

一、掌握會計準則未來修訂情形，避免影響未來審計業務正常推動。

二、參考企業內部稽核積極態度，妥適扮演政府管理顧問角色。

三、參考國際內部協會所推動「稽核－能力成熟度模型」(IA-CMM)方式進行自我評核，有效提升績效審計工作能力。

四、學習金融風暴之教訓，發展風險管理導向之政府經費審計。

五、順應世界潮流建立永續經營理念，強化災難復原之應變能力，以確保資訊安全。

目　錄

壹、前言 1

貳、參加年會過程 2

參、專題演講摘要 3

一、King III－內部審計之未來 4

二、內部控制制度對跨國公司資訊部門之重要性 6

三、接受風險並利用有效控制確保成功機會 7

四、企業正直 9

肆、重要研討主題 10

一、內部稽核專業之新標準 10

二、IFRS 介紹 16

三、公部門之內部稽核－能力成熟度模型 22

四、持續性稽核：成果及挑戰 26

五、COSO之內部控制監督指引 31

六、控制紛亂（Controls Chaos）－其他產業可從金融風暴學習什麼？ 37

七、營運恢復力及持續性—確保資訊安全與可用性之災難復原 43

伍、研討心得及建議意見 51

附錄 60

參考資料

表 次

表1　金融海嘯事件各方意見　9

表2　PS2100－工作性質(Nature of Work)　13

表3　IFRS修正草案(New IRFS EDs)　18

表4　新訂IFRS 討論稿 (New IFRS DPs)　19

表5　IFRS 未來排定計畫　19

表6　IFRS 已排定且辦理中之計畫　19

表7　能力成熟度層級及特徵　23

表8　IA-CMM 矩陣　24

表9　KPA：「專業人力之能力確認及召募」　25

圖 次

圖 1	IPPF組成元素及指引歸類	12
圖 2	IFRS採用或準備接軌之國家分布圖	17
圖 3	關鍵程序面（KPA）檢視程序	24
圖 4	持續性稽核之運用	29
圖 5	風險評估圖	30
圖 6	內部控制之架構	32
圖 7	COSO監督模型	35
圖 8	有效監督程序循環圖	36
圖 9	企業風險管理－COSO	42
圖 10	企業成本V.S.復原時間	45
圖 11	BIA發展圖	48
圖 12	BCM的建置及運作流程	55

國際會議講師(Peter Cheng)、IIA 理事長楊永安與本部出席代表及其他與會人員攝於會場

The Institute of Internal Auditors
2009 International Conference

2009 International Conference, Johannesburg, South Africa, 10 - 13 May 2009

2009 年內部稽核協會國際年會出國報告

貳、 前言

第 68 屆「2009 年內部稽核協會國際年會」於本（98）年 5 月 10 日至 5 月 13 日首度假南非約翰尼斯堡舉行。主辦單位為有效提升各國內部稽核人員之核心技能，並宣揚其於公司內控機制之重要性，會中邀請國際間在相關領域卓有貢獻之公司高階主管人員及學者專家們，藉演講機會分享其職場經驗或專業新知。對照目前因前歐美各大金融機構僅追求短期績效，風險意識薄弱，以致金融環境嚴重惡化，進而引發全球性金融海嘯之時空背景，更凸顯本次年會舉辦之意義。審計部為鼓勵同仁參與稽核專業研討活動，並審酌業務需要，經遴派政風室杜主任格德率第五廳曾稽察彬凱前往參加。謹就參加本次年會過程、專題演講摘要、

重要研討主題、研討心得及建議意見等提出報告。

參、 參加年會過程

本次大會於約翰尼斯堡桑德頓會議中心（Santon Convention Center）舉行，共有兩千餘位會員代表報名參加。98 年 5 月 10 日接受與會人員辦理報到手續，並在次日（11 日）大會正式開幕。在三天議程中，主辦單位共舉辦 11 場專題演講及 8 場主題同步研討會。有關專題演講部分，前兩日(11、12 日)係以內部稽核為核心議題。演講者包括：前南非最高法院法官、現為全球永續發展報告書協會(Global Reporting Initiative, GRI)主席金恩教授（Prof Mervyn King SC）；南非 ArcelorMittal 公司董事長莫黑里（Dr Khotso Mokhele）博士；全球知名企業管理軟體與解決方案供應商 SAP AG 公司副總裁克勞絲（Miriam Kraus）女士；澳洲知名連鎖超商 Woolworths 公司總經理暨前內部稽核協會理事長麥可蕾(Kathryn McLay）女士等人（演講內容詳如參、專題演講摘要）；至 5 月 13 日之演講主題，則在於介紹公司內部人員應有之觀念及技巧。包括由索羅門博士（Dr Woolf Solomon）介紹人際互動過程中，各種肢體語言所傳遞之意義；莫斯葛雷(Anton Musgrave)先生介紹企業應如何藉由業務創新，達到預期獲利目標等。此外，大會並邀請世界盃足球賽籌備委員會委員貝里先生(Gary Bailey)，以「風險管理」之角度，介紹 2010 年將於南非舉行之世界盃賽事，其籌辦過程所面臨之各項繁雜問題，以及解決方式。

有關同步研討會部分共區分為 8 項議題，由各演講人以不同角度介紹內部稽核之方式、觀念與各種新知，並作案例分享。相關議題包括：

「最佳範例（Best Practices）」、「風險管理(Risk Management)」、「柔性技巧(Soft Skills)」、「資訊科技(IT)」、「舞弊(Fraud)」、「政府部門(Public Sector)」、「公司治理(Governance)」、「新興議題(Emerging Issues)」等（各場研討會主題如附錄）。其中，與審計機關較有關聯之「政府部門」議題部分，則有：「政府對內部控制之需求」、「政府部門內部稽核人員之自我評估工具：IA-CMM」、「政府內部共享服務：何類有效？何類無效？」、「環境變異情況下之政府內部稽核單位組織調整」、「績效稽核資訊」、「內部稽核對政府部門課責機制之貢獻」等為研討主題之研討會。

明(2010)年國際稽核協會年會將於美國亞特蘭大舉行。大會安排由今年 3 月曾訪台之美國內部稽核協會副理事長保羅．索博先生（Paul J. Sobel）介紹目前會議籌備概況，並簡介明年研討主體，包括資訊科技(IT)之相關應用、透過領導技能強化審計功能（Auditing Through Leadership, ATL）等項，希望各與會人員在明年屆時能踴躍參加。

肆、 專題演講摘要

本次年會邀請進行國際間與內部稽核領域聲名卓著之公司高階主管人員或學者專家們專題演講。5 月 11、12 兩日係以內部稽核為演講之核心議題，演講者包括：全球永續發展報告書協會主席金恩教授（Mervyn King SC）；南非 ArcelorMittal 公司董事長莫黑里（Dr Khotso Mokhele）博士；全球知名企業管理軟體與解決方案供應商 SAP AG 公司副總裁克勞絲（Miriam Kraus）女士；澳洲知名連鎖超商 Woolworths 公司總經理

暨前內部稽核協會理事長麥可蕾（Kathryn McLay）女士等人。5 月 13 日演講議題則著重公司內部人員應有之觀念與技巧。如：索羅門博士（Dr Woolf Solomon）介紹人際互動過程中，各種肢體語言所傳遞之意義；莫斯葛雷(Anton Musgrave)先生介紹企業應如何藉由業務創新，以達到預期獲利目標等。謹就與內部稽核議題相關之演講內容，摘要如下：

一、 **金恩教授：King III－內部審計之未來**(King III–The Future for Internal Auditing)

前南非最高法院法官、現為全球永續發展報告書協會(Global Reporting Initiative, GRI)主席金恩教授（Prof Mervyn King SC），在本次演講中，以公司永續經營為基礎，進而討論內部稽核人員如何配合調整。首先，他談到公司所面臨之營運環境，自 18 到 20 世紀末的「工業化」、「資訊科技」...等，以迄目前 21 世紀，焦點已移轉至「能源再生」、「永續經營」等議題。在企業界，公司評價已非單純之帳面價值（book value），其他尚須包括管理階層聲譽、公司治理品質以及公司永續經營之策略等非策略因素。他以可口可樂公司為例，說明該公司之總市價較其帳面價值溢價近 20%，即係反應上開非財務性因素。為維持公司永續經營，金恩教授指出，可依循南非近期推動之公司治理準則－King III ，其中三項主要原則：公司治理、策略及永續性（Governance, Strategy, Sustainability）。

King III 準則並表彰內部稽核之功能，在於提供公司之附加性策略價值。稽核人員進行公司之內控稽核作業時，除例行之法規遵循性查核外，更應著重於風險管理（如公司營運策略、組織、財務及市場等風險），以期許本身在公司永續經營過程中，扮演不可或缺之角色。為達成該目標，內部稽核人員必須具備以下特質或能力：可靠性（Credibility）、領導技能（Leadership skills）、良好溝通（Communicator）、策略思考（Strategic mindset）、人際關係（Networker）。至於如何有效提昇內部稽核功能，可從以下層面開始著手：

- 參與公司策略決策過程：策略雖由公司管理階層研擬，並由董事會最終負責，但內部稽核必須參與公司管理階層之策略發展過程。因相較於管理階層常疏忽於如何整合風險管理與公司內控制度，內部稽核更能瞭解風險與機會之所在。
- 確認內部稽核範圍：內部稽核必須確認內控之適足性以及資訊之品質，同時要能充分辨識並及時評估阻礙公司達成目標之風險，及各種機會。
- 取得信賴：內部稽核人員對內控制度之適足性評估結果，須由董事會簽具；且因董事會之審計委員會有指派及免除總稽核之權力，故稽核單位須與董事會及上開委員會主席保持適度互動關係，俾取得其信賴。

結語

「每天工作皆可取得進展，每一步踏出后皆能獲益良多……。雖然我們竭盡所能亦無法達到至善終點，但我們不會洩氣失望，因爲在這段過程中，我們已享受到歡樂與榮耀。」

－邱吉爾爵士，英國前首相

➢ 評估之表達：評估結果或報告，須清楚表達評估之標準、範圍、期間、負責人員與其負責責項目，以及內控制度之有效性。

二、 克勞絲女士：內部控制制度對跨國公司資訊部門之重要性（The Importance of Internal Controls at a Global Company in the IT-Sector）

SAP AG 公司德國副總裁克勞絲女士演講指出，迄 2008 年底止，該公司全球員工約 51 萬 5 百餘人，共約 8 萬 2 千家公司採用該公司開發的軟體，年度總收入達 115.67 億歐元。而在全球資訊市場之市佔率中，該公司開發之企業應用系統軟體達 32.8%，相較其他資訊業者(ORACLE 17.5%、MICROSOFT3.5%)，明顯居於市場領導地位。

根據該公司之經驗，在全球化潮流之影響下，公司經營環境日趨複雜，因此經營團隊必須調適及遵守不同國家各種繁雜之法令規定，同時還要關注並防制所屬員工有行(受)賄、貪污舞弊、洩密(侵害保護資料規定與法令)等行為。在此情況下，「公司治理」、「風險管理」及「法令遵循」等三要件，為穩定控管跨國公司之不二法門，而該三要件之核心，則為持續穩定之內部控制系統。

依據 COSO 架構，有效的內部控制系統應包含持續之監督(Monitoring)、控制活動(Control Activities)、控制環境(Control Environment)、風險評估(Risk Assessment)及資訊與通信(Information and

Communication)等 5 項要素。對 SAP AG 而言，遵循法令規定以執行業務之觀念，已深植於其公司文化。該公司之內部控制系統即係依據沙賓法案(Sarbanes-Oxley Act)SOX404 之規定辦理。她並引述 KPMG(安侯建業)國際會計師事務所內部稽核總監麥克諾藍（Mike Nolan）所言：企業利用風險管理最佳化來改善經營績效，不僅可減少未來不可預知之變動，增加永續經營之條件，同時亦可提高公司聲譽，並創造股東價值。最後，克勞絲女士指出，良好之內部控制將強化公司對法規之徹底遵循，提高股東信任度、財務報告之可靠性，並減輕全球化所面臨風險，對企業永續經營更具特殊意義。

三、 亞羅紛先生：接受風險並利用有效控制確保成功機會（Embracing Risk Whilst Ensuring Success Through Effective Control）

印尼 Medco 集團公司創辦人亞羅紛先生（Arifin Panigoro，前印尼國會議員)演講指出，金融風暴並非肇始於今。數年之前，東南亞、墨西哥亦曾發生金融危機，甚至早在 1930 年代即發生所謂「大蕭條」（the Great Depression）。但為何世人永遠無法由以往慘痛經驗學會教訓？他認為，「公司治理」一直無法發揮應有功效，係類似災難不斷發生之主要原因。但要期待「公司治理」發揮功效，不應僅止於公司之法規遵循程度，更要注意管理階層是否行為不當。觀諸安隆風暴、馬多夫舞弊案等，均屬之。

亞羅紛先生另以印尼經濟情勢發展為例，說明「風險管理」之重要

性。他指出，印尼在 1997 年東南亞金融風暴中，經濟嚴重受損。主要在於該國當時經濟所以高度發展，係建立在泡沫之上，無人注意高度風險隱藏於其公司會計制度及財務報導當中。易言之，缺乏「風險管理」意識，正是導致該國於當時經濟嚴重受創之主因。所幸，印尼政府嗣後為挽救頹勢，採取積極開放之總體經濟政策，終使國家免除破產厄運，政府公債並自 90 年代占國內生產毛額(GDP)之 80%，至 2008 年已降至 30%。

該如何避免公司舞弊導致市場混亂，進而影響經濟發展？亞羅紛先生以美國國會在安隆弊案後迅速通過沙賓法案，但仍然不能杜絕馬多夫弊案為例，認為不該再侷限於思考訂定更多之公司治理有關規章，因為公司治理觀念並非透過法規準予以維繫，而必須實際融合於公司文化當中，由全體公司成員忠實遵守，方能發揮功效。

在公司各種成員當中，他特別提及內部稽核人員之角色，不應再定位於傳統數字計算，而應該期許成為公司務實經營之守護者。在作法上，內部稽核人員應充分瞭解公司本質及營運目標，並協助管理階層妥適聚焦於其目標。此外，為期公司不再侷限於公司治理之有關法規或準則等表面文字，稽核人員更應協助管理階層，建置妥適之控制環境平台，俾使全公司人員一體適用。由於這樣的任務轉換過程極為不易，並甚具挑戰性，因此稽核人員務須爭取公司最高當局支持，方能克竟其功。

最後，亞羅紛引述本次會議另一演講者－金恩教授所言：「無人比內部稽核人員更瞭解其機構所面臨之風險。」據以期許稽核人員應清楚

認知風險管理之意義，並期許自己在維護公司治理之原則上，更善盡應有職責。

四、 莫黑里先生：企業正直（Business Integrity）

南非 ArcelorMittal 公司主席莫黑里博士於演講時，將其觀察此次全球金融海嘯事件發生後之各方看法，整理如【表 1】：

【表 1】金融海嘯事件各方意見

項次	內容
1	全球財務危機事件是資本主義時代的結束，政府早該恢復實施干涉資本市場之政策（Alastair Bruce, MSN Money 雜誌編輯， 2008 年 11 月)
2	全球財務危機事件反映資本主義制度內部曾不穩定性，並顯示新古典主義試驗失敗。（Dr. Kastsuhito Iwai, 日本經濟學者, 2008 年 12 月)
3	影響近 30 年之雷根自由市場主義已經崩潰離析，接下來市場經濟該何去何從？（Financial Time.com）
4	新的資本主義形態應該是「利用資金提供服務」，而非「為資金提供服務」。（多倫多星報，2008 年 10 月 8 日）
5	21 世紀之財經架構將重新規範，如同房子原建造於砂堆者，將改建於岩石之上。(美國總統歐巴馬)

在安隆公司會計與稽核人員共同舞弊，以及馬多夫 500 億美元龐式騙局（Ponzi scheme）等案例中，凸顯現行公司治理制度已出現嚴重問題。公司高階管理人員藉職務之便，透過各種帳外融資、隱藏負債、利潤灌水、虛增現金流量等違規手段，操縱市場、銷毀重要文件、妨礙司法調查及蓄意誤導投資者，公司獲利由少數人中飽私囊，損失卻由眾人

買單；追究其原因，主要係企業道德淪喪、內控制度失靈，公司治理機制失去功能所致。為此，企業應推動「誠實」(Integrity)與「倫理」(Ethics)運動。所謂「誠實」，為面對倫理標準與價值之自發性承諾，「倫理」，則是誠實與責任。莫黑里先生並舉非洲道德哲學：Ubuntu，藉以說明之。他首先引述南非屠圖大主教之解釋：具備 Ubuntu 特質者，具開放心態，樂於助人，且具適度自信，即使他人表現優異亦不認為遭到威脅。這樣的自信來自於他（她）瞭解其身屬之大我，在遭受荼毒或壓迫時，亦無法自外其中。此外，南非前總統曼德拉亦曾舉例說明 Ubuntu 意涵：「當一位旅者停留於村落時，他不需開口向當地居民要求食物或飲水，居民即願意自動提供，這就是 Ubuntu。Ubuntu 並非提倡人們毋需滿足自己慾望，但其重點在於個人作為，可否使身處環境更為進步。」莫黑里博士藉機倡導 Ubuntu 之精神，期許企業界視之為正直經營之道德平台，並跟與會者共勉。

伍、 重要研討主題

謹就本次會議研討內容綜合彙整，分就「內部稽核專業之新標準」、「IFRS 介紹」、「公部門之內部稽核－能力成熟度模型」、「持續性稽核：成果及挑戰」、「COSO 之內部控制監督指引」、「控制紛亂(Controls Chaos)－其他產業可從金融風暴學習什麼？」、「營運恢復力及持續性—確保資訊安全與可用性之災難復原」等 7 項議題，扼述如次：

一、 內部稽核專業之新標準

本場次係由英國暨愛爾蘭內部稽核協會技術主任侃恩先生(Jackie Cain)主講，內容介紹國際內部稽核協會理事會於 2007 年通過之「國際專業實務架構」（International Professional Practices Framework, 簡稱：IPPF），包括 IPPF 之組成要素，以及與專業實務架構(PPF)之差異處。茲簡介如后：

（一）前言

國際內部稽核協會係由美國內部稽核協會於 1941 年草創，進而發展成為一個國際性機構，目前已有會員超過 16 萬 5 千名，分布於 160 餘個國家。

該協會基於內部稽核之實務所需，以往曾發布之重要作業準則，包括：職業道德規範（Code of Ethics,1967）、內部稽核執業準則（Standards for the Professional Practice of. Internal Auditing, 1978）、專業實務架構（Professional Practices Framework, 2000）等。嗣該協會理事會為提供簡單並更具彈性之稽核架構，及嚴謹、透明且值得信賴之稽核程序，讓業界共為遵循，爰以 PPF 為基礎，於 2007 年 7 月通過新版之「國際專業實務架構」（IPPF），自 2009 年 1 月開始適用，俾協助實務界人士，提供更高品質之內部稽核服務。

（二）IPPF 組成元素概述

IPPF 組成元素計有 6 項，包括：定義(Definition)、執業準則(International Standards)、職業道德規範(Code of Ethics)、立場聲明書(Position Papers)、實務諮詢(Practice Advisories)、實務指引(Practice Guides)等，並視其有效程度，分別歸類於「強制性」及「強烈建議」等兩類指引。歸類於「強制性」指引者，表示稽核人員對該元素所訂規範有強制遵循之必要；如歸類於「強烈建議」指引者，則表示 IIA 支持該元素內容係屬廣泛可行之建議方案，並強烈建議內部稽核人員遵循之。有關 IPPF 之各項組成元素及其個別歸類，詳如【圖 1】:

【圖 1】IPPF 組成元素及指引歸類

（三）IPPF 與 PPF 之基本差異說明

IPPF 係以 PPF 為基礎，刪除「發展及實務工具」，並新增闡述內

部稽核特殊角色與責任之「立場聲明書」，及與資訊科技稽核有關之「實務指引」等 2 項元素。其中「執業準則」並加入「解釋」(interpretation)，以說明各項執業準則所包含之名詞或觀念；至「實務諮詢」部分則縮小其內容範圍，並將原訂各種技術工具或流程併至「實務指引」元素。

（四）IPPF 簡介

IPPF 保留 PPF 原有之定義、職業道德規範等內容，不作更動。因此本文針對 IPPF 其餘 4 項元素說明之。

1. 執業準則(International Standards)

執業準則分為「一般準則」(Attribute Standards, AS)及「作業準則」（Performance Standards, PS）兩種。為使國際內部稽核職業準則之內容更為明確，因此在不變動準則內容之前提下更新架構，增加「解釋」部分。此外，以往 PPF 為利於讀者瞭解及應用，曾就其準則內容之特定用辭，諸如「董事會」(Board)、「內部稽核主管」（Chief Audit Executive）等，於辭彙表(Glossary)內分別釋之；IPPF 則賡續沿用既有辭彙，另考量重要性、資訊技術控制，資訊技術治理、科技基礎之稽核技術、風險胃納等因素，新增所需解釋辭彙。茲以作業準則「PS2100－工作性質」為例，說明 IPPF 修訂之處，如【表 2】。

【表 2】PS2100－工作性質(Nature of Work)

- ◆ 本準則包括：PS2110－治理(governance)、PS2120－風險管理(risk management)、PS2130－控制(control)等 3 項次準則。

◆ 準則修正重點在於強調風險基礎（risk-based），並說明內部稽核單位須以有系統、有紀律之方法，評估及協助改善治理、風險管理及其控制過程。
◆ 「解釋」(interpretation)部分，說明衡量風險管理程序有效性之所需考量因素、何者為有效且足夠之控制，及風險管理與控制程序之完整性與有效性。
◆ 「辭彙表」(glossary)部分，增加本準則內容中，有關「風險胃納」(risk appetite)1 詞之定義（風險胃納：機構願意承擔之風險）。
◆ 本準則之次準則「PS2120－風險管理」，增加「須評估風險管理之有效程度」、「改善機構績效之貢獻度」等內容。

2. 實務諮詢(Practice advisories)

實務諮詢之目的，在協助內部稽核人員於應用職業道德規範（Code of Ethics）及執業準則（International Standard）時，所需之步驟、方法或應考量因素。IPPF 針對 PPF 原有內容是否否符合上開目的（或定義）進行大幅調整，將原有 83 篇內容縮減為 41 篇，並增訂 PA 1111-1: Board interaction （董事會互動），共計 42 篇。

3. 實務指引(Practice guides)

實務指引之目的，係為執行內部稽核業務之細部指引，包含細部之流程及程序，例如各種工具及技術、工作程式、以及詳細之方法。IPPF 介紹一套以風險為基礎之 IT 一般控制評估方法(GAIT 方法)，IIA 強烈建議內部稽核人員在辨識主要之 IT 控制作業，不論是其關鍵程序或作業風險，均應參考之。

4. 立場聲明書

立場聲明書之目的，係為協助不同當事人（包含不屬內部稽核專業之人士），瞭解重要之治理、風險管理、或控制議題，並描述與內部稽核有關之角色與責任。IPPF 目前納入兩篇文章：

- 內部稽核在企業風險管理之角色（The Role of Internal Auditing in Enterprise Risk Management）
- 內部稽核在內部稽核單位資源配置之角色（The Role of Internal Auditing in Resourcing the Internal Audit Activity）

（五）內部稽核人員應扮演及避免之角色

侃恩先生於演講中，提及內部稽核人員在企業風險管理(ERM)所應扮演之角色，包括：

－由管理階層作成決定

－確認內部稽核之獨立性及客觀性

－改善企業之風險管理、控制及治理過程

此外，應避免扮演以下角色：

－對風險管理之成果負責

－代替管理階層執行風險回應

－決定如何回應風險

－確認企業風險管理架構各項元素之有效性。

（六）結語

侃恩先生最後對內部稽核未來之發展策略，提出以下方向：

1. 注意內部稽核之目標，在於協助機構達成目的

2. 內部稽核人員應由具備足夠專業能力擔任

3. 有效應用 IPPF，包括職業道德規範、執業準則等。

4. 資源運用所應考量條件，諸如：內部資源及外包資源之比例、比較優缺點、機構規模等。

二、 IFRS 介紹

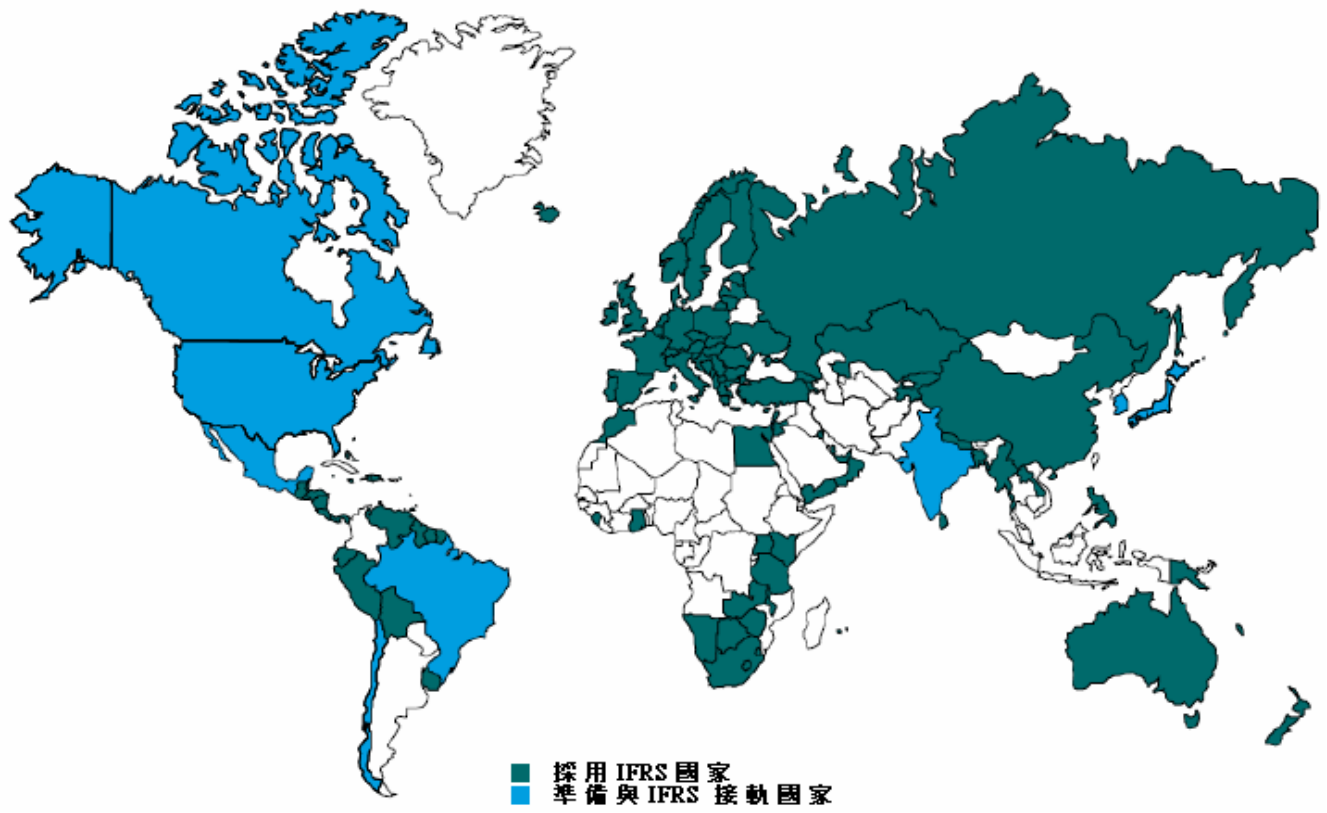
本場次係由 IFRS 委員會委員麥肯錫先生主講，摘要如下：

（一）前言

國際會計準則理事會(International Accounting Standards Board, 簡稱 IASB)於 2001 年接替國際會計準則委員會(IASC)，成為國際會計準則制定機構。IASB 並宣布，承襲 IASC 所制訂的國際會計準則；此外，國際財務報告解釋委員會(IFRIC)則於 2002 年取代常務解釋委員會(SIC)，承襲其發布之 32 個解釋函(SICs)，並陸續發布新的解釋函(IFRICs)。這些準則(IASs、IFRSs)及解釋函(SICs、IFRICs)在 IFRS 的架構下，均泛稱為 IFRSs。

目前全世界已超過 100 個國家直接採用 IFRS，或準備與 IFRS 進行接軌（如次頁【圖 2】）。至於 IFRS 可否成為國際通用之會計原則，以美國態度最為關鍵。因美國擁有全球最大資本市場，並吸納來自全球各地上市公司募集資金，如仍採用一般公認會計原則（Generally Accepted

Accounting Principle，US GAAP），將導致兩套會計原則標準並行，將增加跨國公司業務成本，影響財務透明程度，並導致 IFRS 功能因此大打折扣。事實上，美國證券交易委員會(United States Securities and Exchange Commission, SEC)於 2007 年 11 月通過之 Form-20F 修正案，規範其境外發行人(issuer)已依 IFRS 編製者，免於再調整至 US GAAP；另 SEC 於 2008 年 8 月提出「美國發行人採用 IFRS 編製財務報表之藍圖」，則規範境內發行人如何以漸進方式，分階段採用 IFRS。顯示美國會計原則對如何與 IFRS 進行完全接軌，已作好準備。



【圖 2】IFRS 採用或準備接軌之國家分布圖

雖然世界主要國家對 IFRS 多持支持態度（據統計，全球已有 64%公司以 IFRS 編製財報），但事實上，仍有甚多業者對該會計制度缺乏足夠認知。其中，34%之非美國公司業者認為其 IFRS 資訊不足，至於美

國業者感受相同者，更高達 64%，顯示諸多公司仍需接受更具體之 IFRS 訓練。應加強之處包括：提高管理階層因 IFRS 認知不足以致影響公司營運之危機意識，以及持續追蹤 IFRSs 各草案之修訂進度。

（二）IFRS 修訂草案

IASB 及 IFRIC 於承襲 IASC 及 SIC 所制定之準則及解釋函後，陸續發布新準則及解釋函，以及修訂原有準則之過程中，發現部分準則規範存有不一情事。 因此，IASB 每年均提出 IFRSs 年度改善計畫，俾使 IFRSs 之各項準則概念得以互為連貫。

2009 年以前，IASB 所發布公報（或相關解釋函）之影響範圍不大，但今(2009)年起迄年底前，預期將發布 12 至 14 則新（增）訂公報（或標準），茲列舉其中重要者，整理如【表 3】、【表 4】、【表 5】、【表 6】：

【表 3】IFRS 修正草案(New IRFS EDs)

修正公報（名稱）	修正內容
IFRS 第 7 號公報（債務工具投資）	額外揭露所有債務工具投資，但公平價值變動計入當期損益之債券投資除外。此項修訂要求企業於財務報表中，以表列方式載明該等投資之公平價值、攤銷後成本、財務狀況表上之帳面價值等
IAS 第 39 號公報（嵌入式衍生性工具）	2008 年 10 月修訂 IAS 39 時，因允許特定金融資產重分類，為防範實務應用分歧，因此再作修正。修正後，為證明嵌入式衍生性工具之會計處理，將要求所有嵌入式衍生性工具均需進行評估，包括嵌入於重分類工具，以及財務報表上之個別會計處理（如有需要）等。
IAS 第 27 號公報（合併財務報表）	本公報修訂目的，在強化及改善有關辨識公司所控制之個體，該等個體並納入合併財務報表表達之規定。由於「個體控制」之定義係採新的原則基礎（Principle-based），因此適用範圍較廣，且特殊安排者亦較難規避權責；此外，對於一般投資人而言，亦可利用本公報強化揭露公司合併報表之規定，進行投

	資評估。
IAS 第 24 號公報（與政府關係）	2003 年之前，IAS 24 規定國營企業可免除關係人揭露範圍，當年修正後廢止此項免除規定，2005 年生效後襲用至今，因此現有採用 IFRS 並以營利為目的之國營事業，均必須揭露其與其他國營事業之交易。這次公報修訂目的，即在簡化目前 IAS 24 有關國營事業之揭露規定。

【表 4】新訂 IFRS 討論稿 (New IFRS DPs)

討論稿(DP)標題	內容
收入認列 (Revenue Recognition)	IASB 委員會希望發展一個簡單收入模型，不論任何產業皆可一體適用，藉以提昇 IFRS 及美國 GAAP 現有準則之品質。在應用本項簡單收入模型後，公司如依契約規範，需完成移轉貨品及勞務給顧客之義務時，均需認列相關收入。
財務報表表達	針對 IAS 1 有關財務報表表達之議題進行討論，希望未來表達之格式中，可反應 IFRS 委員會之初始看法。

【表 5】IFRS 未來排定計畫

計畫名稱	內容
排污交易計畫	本計畫主要處理排污交易權，並預期在 2010 年底前提出 IFRS 公報
共同控制交易	說明在共同控制下之企業合併行為，IFRS 公報提出時程尚未決定。
停業及供出售持有帳戶（Hold for sale account, HFS）	增訂於 IFRS 第五號公報，增訂時程未定。

【表 6】IFRS 已排定且辦理中之計畫

計畫名稱	內容
每股盈餘	增訂於 IAS 第 33 號公報，預期於 2009 年下半年公布 IFRS 公報。

權益性質之金融工具	負債與權益分類明確化，預期於 2011 年公布 IFRS 公報
財務報表表達	績效報導，預期於 2011 年公布
課稅所得	重新檢視 IAS 第十二號公報，預期於 2010 提出最後標準。
保險合約	綜合性計畫，預期於 2011 年公布
租賃	預期於 2011 公布
離職後給付	預期於 2011 提出。
收入認列	預期於 2011 提出
公平價值衡量指引	預期於 2010 提出。

（三）我國會計制度與 IFRS 接軌作業之準備情形（補充）

我國早期公報之制定，主要係依循美國會計準則。民國 90 年經發會提出「與國際接軌」之共識，我國會計準則公報(ROC GAAP)更積極朝向 IFRS 接軌邁進。在多年努力之後，ROC GAAP 與 IFRS 之間差異已逐漸縮小，但其接軌進度相較其他國家仍屬落後，於是主管機關－金融管理委員會開始思考「直接採用」之可能性，成立「推動我國採用國際會計準則專案小組」，邀集相關單位著手進行工作分配及擬定進程之事宜。今(98)年 5 月 14 日已發布採用 IFRS。適用範圍及時程如下：

1、 第一階段：上市上櫃公司、興櫃公司及金管會主管之金融業（不含信用合作社、信用卡公司、保險經紀人及代理人）：

（1） 應自 2013 年開始依國際會計準則編製財務報告。

（2） 自願提前適用：

已發行或已向金管會申報發行海外有價證券，或總市值大於新

臺幣 100 億元之公司，於報經金管會核准後，得提前自 2012 年開始依國際會計準則增加編製合併報表，依規定無須編製合併報表者，則得依國際會計準則增加編製本身之個體財務報告(individual financial statements)。

2、 第二階段：非上市上櫃及興櫃之公開發行公司、信用合作社及信用卡公司：

(1) 應自 2015 年開始依國際會計準則編製財務報告。

(2) 得自 2013 年開始提前適用。

三、提前於財務報告附註揭露採用 IFRS 之計畫及影響（Pre-disclosure）：公司為因應採用 IFRS 編製財務報告，應訂定採用 Taiwan -IFRS 之計畫且成立專案小組負責推動，並依下列規定於採用前 2 年度財務報告揭露相關事項：

（一） 第一階段採用者：

1. 應於 2011 年度、2012 年期中及年度財務報告附註揭露採用 IFRS 之計畫及影響等事項。

2. 自願提前適用者：

(1) 應於 2010 年度及 2011 年期中及年度財務報告附註揭露採用 IFRS 之計畫及影響等事項。

(2) 如於 2011 年以後始決定自願提前採用 IFRS 編製財務報告者，應自決定日後之 2011 年期中及年度財務報告附註揭露相關事項。

（二） 第二階段採用者：比照上開方式於採用前 2 年開始辦理。

三、 公部門之內部稽核－能力成熟度模型

本場次係由國際內部稽核協會研究中心高級研究員麥可蕾女士主講，內容摘要如下：

（一）前言

內部稽核－能力成熟度模型（Internal Audit – Capability Maturity Model, IA-CMM）由國際內部稽核協會研究中心((IIA Research Foundation) 開發完成，並獲 IIA 之專業標準委員會(Professional Standards Committee, PSC)推薦，與世界銀行(World Bank)認證。IA-CMM 係內部稽核單位之自我評估架構，而在其自我評估之過程中，可透過與其所屬之機構互動溝通之機會，間接協助機構提高經營績效。

（二）IA-CMM 之建構基本原則

IA-CMM 係由內部稽核單位在下列原則之基礎上，進行自我評核：

1. 內部稽核單位係公部門有效治理(effective governance)之構成要件，並以協助機構提昇績效、建立課責制度為目標。
2. 內部稽核單位所屬機構，需設定該內部稽核單位所應達成之能力成熟度層級(level)，並確實達成目標。
3. 決定最適能力成熟度層級之影響條件有三：環境、機構本身，及該內部稽核單位。

4. 在建立 IA-CMM 模型時，由於上開 3 條件之差異，所設定能力成熟度之層級目標亦有不同，不可一體適用。

（三）IA-CMM 架構簡介

1. 能力成熟度層級

在 IA-CMM 之架構下，內部稽核單位之能力成熟度視其專業能力，依序分成 6 個層級。其個別層級名稱及其特徵，如【表 7】。

【表 7】能力成熟度層級及特徵

能力成熟度層級	層級名稱	層級特徵
1	初步	無持續及可複製之內部稽核經驗，端須仰賴個人努力。
2	基礎	具持續及可複製之內部稽核經驗及步驟
3	整合	IA 之管理及專業經驗可順利運用
4	管理	IA 藉由整合組織內部資訊，以改善組織之治理及風險管理
5	最佳	IA 藉由組織之內部或外部資訊，取得持續性之成長學習

2. 內部稽核元素

內部稽核單位係由六項元素組成：內部稽核之角色及其提供服務、構人員管理、專業實務經驗、績效管理及課責、組織關係與文化、治理架構。

3. 建構 IA-CMM 矩陣

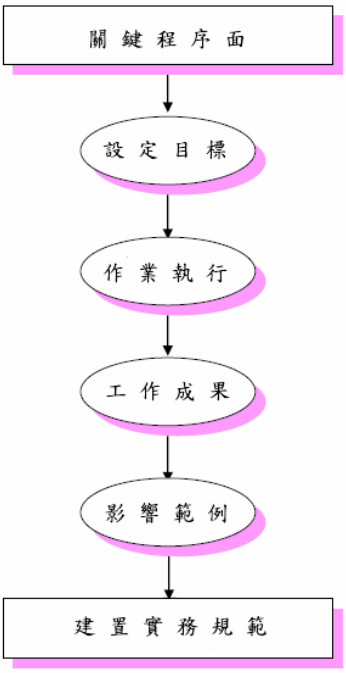
根據上開 6 項內部稽核元素及 5 個能力成熟度層級，即可完成建構內部稽核成熟度模型矩陣（IA-CMM Matrix），如【表 8】所示。該矩陣內各單元，為各內部稽核元素於該成熟度層級所需檢視之課題，另可稱之：「關鍵程序面」（Key Process Area, KPA）。

【表 8】IA-CMM 矩陣

	IA 所提供之服務及角色	人員管理	專業經驗	績效管理及課責	組織關係及文化	治理架構
Level 5-最佳化	KPA 1 KPA 2 …	KPA 1 KPA 2 …	KPA 1 KPA 2 …	KPA 1 KPA 2 …	KPA 1 KPA 2 …	KPA 1 KPA 2 …
Level 4-管理化	KPA 1 KPA 2 …	KPA 1 KPA 2 …	KPA 1 KPA 2 …	KPA 1 KPA 2 …	KPA 1 KPA 2 …	KPA 1 KPA 2 …
Level 3-整合化	KPA 1 KPA 2 …	KPA 1 KPA 2 …	KPA 1 KPA 2 …	KPA 1 KPA 2 …	KPA 1 KPA 2 …	KPA 1 KPA 2 …
Level 2-基礎化	KPA 1 KPA 2 …	KPA 1 KPA 2 …	KPA 1 KPA 2 …	KPA 1 KPA 2 …	KPA 1 KPA 2 …	KPA 1 KPA 2 …
Level 1-初步化	本階段之審計行為既屬特定且非結構化，因此結果端視該審計人員之個別能力。審計過程中，除參考外部專業組織所提供之案例外，其內部亦無案例可循。由於審計人員既無專業能力可言，因此本階段亦無所謂主要程序區塊(KPA)					

（四） KPA 檢視程序

有關關鍵程序面（KPA）檢視程序，如【圖 3】所示：



【圖 3】關鍵程序面（KPA）檢視程序

為具體說明 KPA 檢視程序，茲以【人員管理】元素於第 2 層級（基礎層級）之其中 1 項 KPA：「專業人力之能力確認及召募」為例，說明如【表 9】：

【表 9】KPA：「專業人力之能力確認及召募」

步驟	完成成果
設定目標	吸引具有足夠能力及相關技能之人員參與內部稽核作業，以提高內部稽核結果之公信力。
作業執行	一、辨識並定義將執行之稽核作業 二、辨識進行該稽核作業之所需技能（包括技巧或行為等） 三、建立該職務之工作內容 四、決定薪資條件 五、進行合理並具公信力之人員招募程序，俾選擇適合該職務之候選人。
工作成果	由適當合格人選出任該內部稽核職務
影響範圍	一、建立專業稽核制度。 二、稽核成果具公信力。（包括稽核發現、結論及所提建議意見）
建置實務規範	建置規範諸如：人員招募方針、工作內容報告、系統分類（包括設定內部稽核之能力成熟度階段）等。

（五） 自我評核步驟

內部稽核單位利用 IA-CMM 進行自我評核，步驟如下：

- ✓ 瞭解內部稽核能力成熟度模型之意涵
- ✓ 由內部稽核單位辨識需建構之關鍵程序面(KPA)
- ✓ 重新審視目前已訂定之相關文件
- ✓ 與管理階層及利害關係人進行訪談

- ✓ 確認應建構之關鍵程序面(KPA)
- ✓ 決定能力成熟度層級（第 1 至第 5 層級）
- ✓ 進行關鍵程序面(KPA)檢視程序

（六） IA-CMM 模型應用應注意原則

1.在採用 IA-CMM 模型評核機關或企業之內部稽核能力成熟度階段，並利用其關鍵程序面將實務經驗制度化之過程中，應確實利用專業判斷；同時注意，該實務經驗如無法讓後人複製學習時，即無改善可能。

2.關鍵程序面所建置規範，需融入內部稽核單位之文化，始能發揮功效。

3.選定能力能熟度階段後，包括該階段（含以下）之所有關鍵程序面皆需完成。

4.個別內部稽核單位，可視需要選定其特定之能力成熟度階段。

四、 持續性稽核：成果及挑戰

本場次由三井住友銀行內部稽核部門總稽核 Mr. Masaki Nakamura 主講。演講內容除首先概述該銀行之資產及經營規模，與市場信用評等外，主要內容在介紹該行設置於稽核部門之獨立監控小組，如何運用四大監控系統（包括舞弊交易、分行營運、分行管理、產品及服務等監控系統）推動持續性稽核。茲摘述重點如次：

（一）四大監控系統

1. 舞弊交易監控系統（Fraudulent Transactions Monitoring，FTM）

(1) 系統目的：利用資訊科技，偵測舞弊性交易之早期徵兆。如：定存客戶到期前出現鉅額現金提領、鉅額或經常性之現金提領（尤其是高齡客戶）、靜止戶之突然交易行為等。

(2) 目前監控項目計 16 項，每月調查案件數約 400 件。

(3) 作業流程：由監控小組要求分行調查可能涉及舞弊之交易活動。在分行經理完成調查並向其報告結果後，監控小組如認為仍有疑義，則再進一步由舞弊調查小組進一步調查。

2. 分行營運監控系統（Branch Operations Monitoring， BOM）

(1) 系統目的：藉由偵測分行之作業疏漏或違規事項（諸如，客戶財務報告資料輸入錯誤、未經核准之撥款行為）並提出示警，以協助分行改善。

(2) 目前監控項目計 43 項，每月調查案件數約 600 件。

(3) 作業流程：監控小組將其發現之作業疏漏事項通知相關分行並更正後，於下次實地稽核實再行檢查其更正措施之完備程度。

3. 分行管理監控系統（Branch Management Monitoring， BMM）

(1) 系統目的：監控分行有無違反人事規則或勞動法令（如強制休假、假日工作等）。

(2) 目前監控項目計 3 項，每月調查案件數約 70 件。

(3) 作業流程：監控小組將其發現可能違反人事規則之案件通知分行

經理。分行經理調查後，將真相向人事主管提出報告。

4. 產品及服務監控系統（Products & Services Monitoring， PSM）

(1) 系統目的：監控分行之銷售行為是否符合有關法規及銀行法令（如：銷售特定之財經商品或服務，有無符合交易紀錄保存規定）。

(2) 目前監控項目計 28 項，每月調查案件數約 500 件。

(3) 作業流程：監控小組將相關之違規案件通知有關分行，並在各分行視需要更正後，於下次實地稽核時再行檢查其更正措施之完備程度。

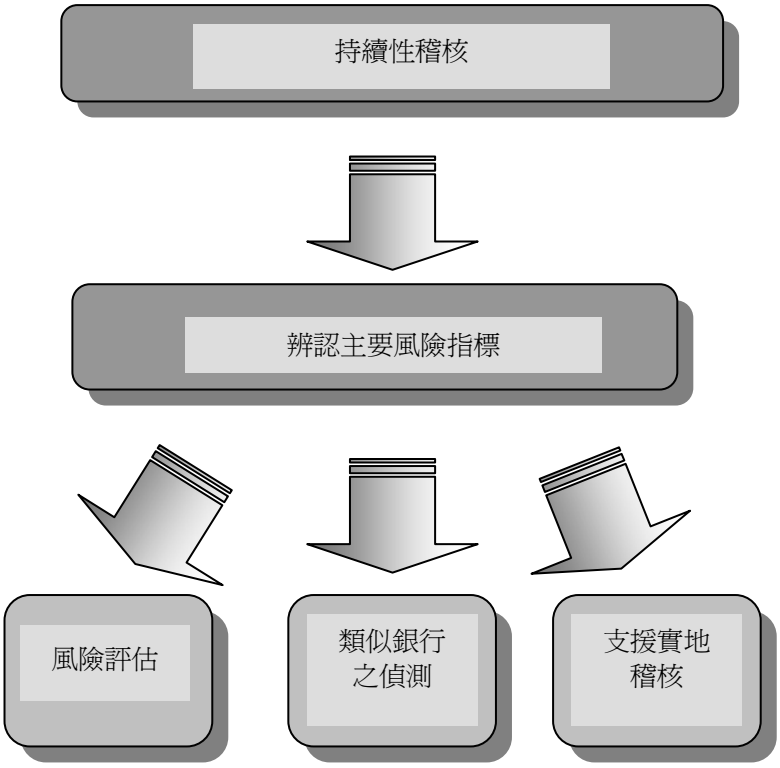
（二）持續性稽核之優缺點

■ 優點：提供稽核人員完整、有效且有力之檢查工具，尤其是對於隱身於龐大交易中之少數錯誤行為。

■ 缺點：僅能偵測較為表面之問題（諸如操作錯誤）；此外，由於難以辨認問題發生原因，因此需要佐以實地稽核。

（三）持續性稽核之運用

有關持續性稽核之運用，詳如【圖 4】，並說明如后：



【圖 4】持續性稽核之運用

1.辨認主要風險指標(Key Risk Index, KRI):

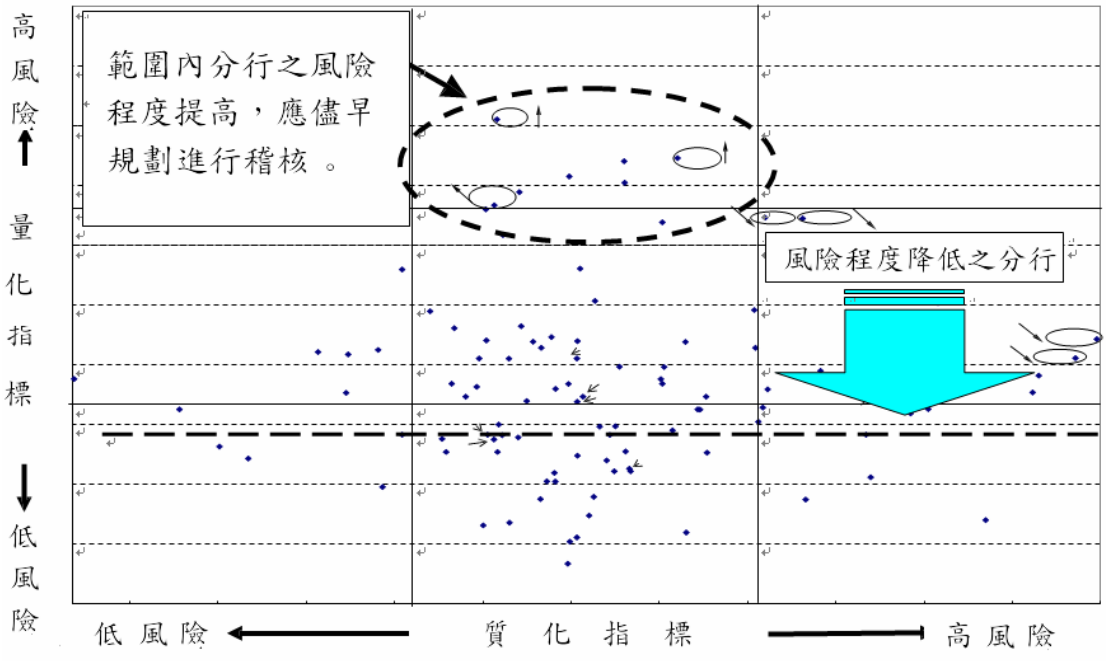
該行發現，各分行利用主要風險指標(KRI)進行風險評估之結果，並與實地稽核後所列評等檢定比較結果，發現其相關性係數（Correlation Coefficient）僅 25%。應如何改善高達 75%落差？透過持續性稽核可知，應將各分行主管之個別條件及影響分行之環境因素亦列入主要風險指標。相關 KPI 如下：

(1) 與分行主管個別條件相關之 KRI，計有：其以往接受稽核之結果、專業程度、職場背景等

(2) 與影響分行環境因素相關之 KRI，則包括客戶形態（例如資產公司、建設公司等不同性質公司之比例）、擔保不足之放款比例等。

2.風險評估

將 KPI 區分為兩類：質化指標（Qualitative measures，例如：作業疏失）及量化指標（Quantitative measures，例如：客戶形態）。各分行根據 KPI 予以質化及量化指標之評分，並據以繪入風險評估圖，如【圖 5】:



【圖 5】風險評估圖

3.類似銀行之偵測

利用 KRI 及風險評估，對於發生作業缺失之分行，可嘗試比對其指標評分相近之分行，並偵測是否發生相同之內控疏失，並利用實地查核驗證之。

4.支援實地稽核

監控小組可提供各分行稽核小組以下資料，以便即時有效辦理實地稽核，並有足夠時間與受稽核分行就其缺失討論改善之道：

(1) 近期持續性稽核及風險評估之結果－便於聚焦風險範疇及項目。

(2) 受稽核分行其內控制度薄弱之相關資料

（四）未來努力方向

未來持續性稽核之努力方向，除了須即時更新主要風險指標 KRI，以反應各分行之真正風險外，對於主要績效指標(KPI)之辨認、評估及利用，亦須運用於持續性稽核之工作上。目前三井住友銀行計畫由現行之交易檢核，提昇至部門層級之監控，未來更將擴大至公司全面性檢核，並將稽核結果及時且完整地向高階管理階層提出報告。

五、「COSO 之內部控制監督指引」簡介

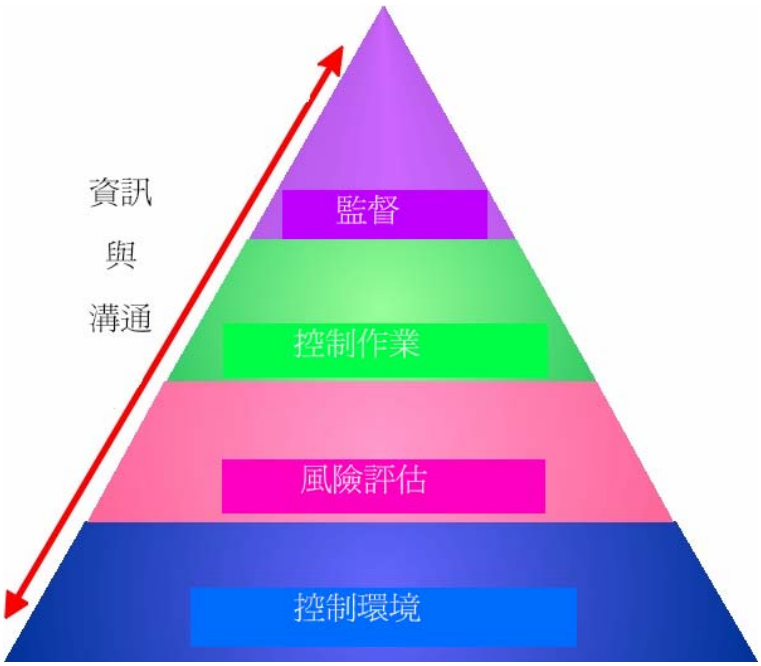
本場次係由美國政府會計協會學術委員會主席羅摩堤博士(Dr. Sridhar Ramamoorti)主講，內容分述如次：

（一）前言

COSO(Committee of Sponsoring Organizations of Treadway Commission)於 1992 年發布「內部控制：整合架構」研究報告中，揭櫫內部控制（以下簡稱：內控）之定義，同時指出，內控制度除了可因應組織內、外在環境變化外，更可提昇組織績效、降低風險、確保財務報導之可信度，以及法規遵循度，因此對組織得否順利運作，甚為重要。

根據 COSO 上開研究報告，內部控制係由：控制環境、風險評估、

控制活動、資訊與溝通、監督等五項因子所組成，其架構如圖【6】。其中，「監督」因子(Monitoring)即係基於內控制度之重要性，所建立之評核機制。



【圖 6】內部控制之架構

有效監督可確保內控機制得以有效運作，其中包括在適當期限前，由該機制之設計及運作相關成員進行評核，並採取必要步驟。但是，何謂良好之監督機制？又該如何妥適執行監督機制？根據上開研究報告（總則篇、第一章及第六章）及 2006 年 COSO 指引（COSO's 2006 Guidance，第五章），可歸納以下 2 項原則：

1. 可藉由「持續監督」(Ongoing Monitoring)及／或「獨立評核」(Separate Evaluation)等作業，協助管理階層瞭解各項內控元素是否持續運作。
2. 辨認內控制度之弱點，並及時通知有關單位採取必要作為。

（二）「COSO 監督指引」簡介：

為進一步闡明 2006 年 COSO 指引，COSO 委由 Grant Thornton LLP 會計師事務所辦理本次演講之主體－「COSO 之監督」計畫，並完成「COSO 監督指引」(Guidance on Monitoring Internal Control Systems)。茲說明影響監督成果之有效性與效率性之三項元素，如次：

1. 監督控制環境

監督之控制環境，包括：機構文化有關監督作業重要性之認知，及監督者是否具備應有之能力，並賦予足夠職權。

監督作業之重要性如欲深植於企業文化中，在於監督者對內控制度是否持續有效提出合理意見，並在內控制度之缺點在影響機構達成目標前，予以明確辨認，並改善之。至於監督者本身則應具有足夠能力，並在行使職權過程保持客觀態度。所謂足夠能力，意指熟悉內控制度之作業程序，並對辨認內控缺點具有足夠知識；至於保持客觀態度，則係不為個人利益保留監督意見。

「內部控制」定義

由公司董事會、管理當局、及其部屬，爲了合理保證達成（1）營運的效果與效率、（2）財務報導的可靠性，及（3）相關法令與規章的遵循等目標，所採行之程序。

－「Internal Control – Integrated Framework,」COSO, 1992

2. 有效排定監督程序

在 COSO 架構中，內控制度之風險評估(risk assessment)元素可辨認並評估影響組織達成其目標之風險。風險評估結果則影響監督作業範圍（諸如監督對象、監督者、監督程序與頻率等）。

當風險改變卻未調整相關控制行為，或有效之控制行為停止運作時，將使內控制度失去有效性。為避免發生上開結果，應事先排定監督

程序之順序，其架構如下

(1)建立控制基準(Control Baseline)：建立內控制度得以保持基本有效運作之基準，據以建立下一步之監督行為。

(2)識別變異程序：識別可能影響組織達成目標之風險，及其控制行為。

(3)管理變異程序：確保內控系統妥適運作，其系統範圍包括調整原有或新增之控制行為。而其結果亦可作為更新後之控制基準。

(4)控制再確認：如有需要，再透過適當之獨立評核(Separate Evaluation)作業，定期確認調整後之控制作業有效性。

有效監督包括妥適蒐集及分析具說服力之資訊(persuasive information)，據以說明內控制度之有效程度。該等資訊分成直接資訊(Direct information)及間接資訊（Indirect information）兩種：

- 直接資訊：直接資訊係指直接落實控制行為之相關作業，因此在觀察機構之控制行為時，得以一覽無疑，直接資訊除可據以建立前段所述之控制基準外，並可對內控監督過程提供查核意見所需資料。
- 間接資訊：係指在直接資訊外，其他藉以評估控制（或其元素）有無有效運作之資訊。例如：主要風險指標、主要績效指標等。

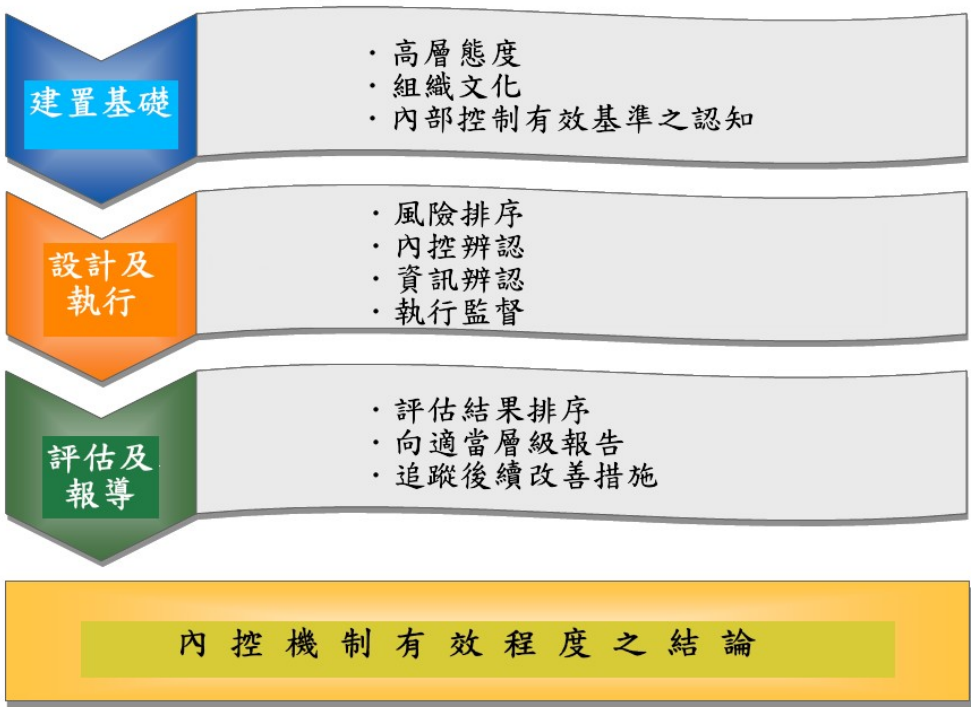
3. 監督結果報告

監督行為有效與否，須其監督結果有無向適當人選提報告，並據此採取有效改善措施。報告對象之層級，以及報告頻率，則視風險程度

及相關控制行為之重要性而定。如報告內容在於內控制度之缺失，除通知相關負責人員外，尚須告知其高一階主管，如此方能使負責人員有足夠資訊研謀改善措施，並使其主管得有機會以客觀第三者之立場，嚴謹監督其改善過程。

（三）「COSO 監督指引」之監督模型

為便於瞭解監督因子之內容，茲建立監督模型如【圖 7】，並說明如后：



【圖 7】COSO 監督模型

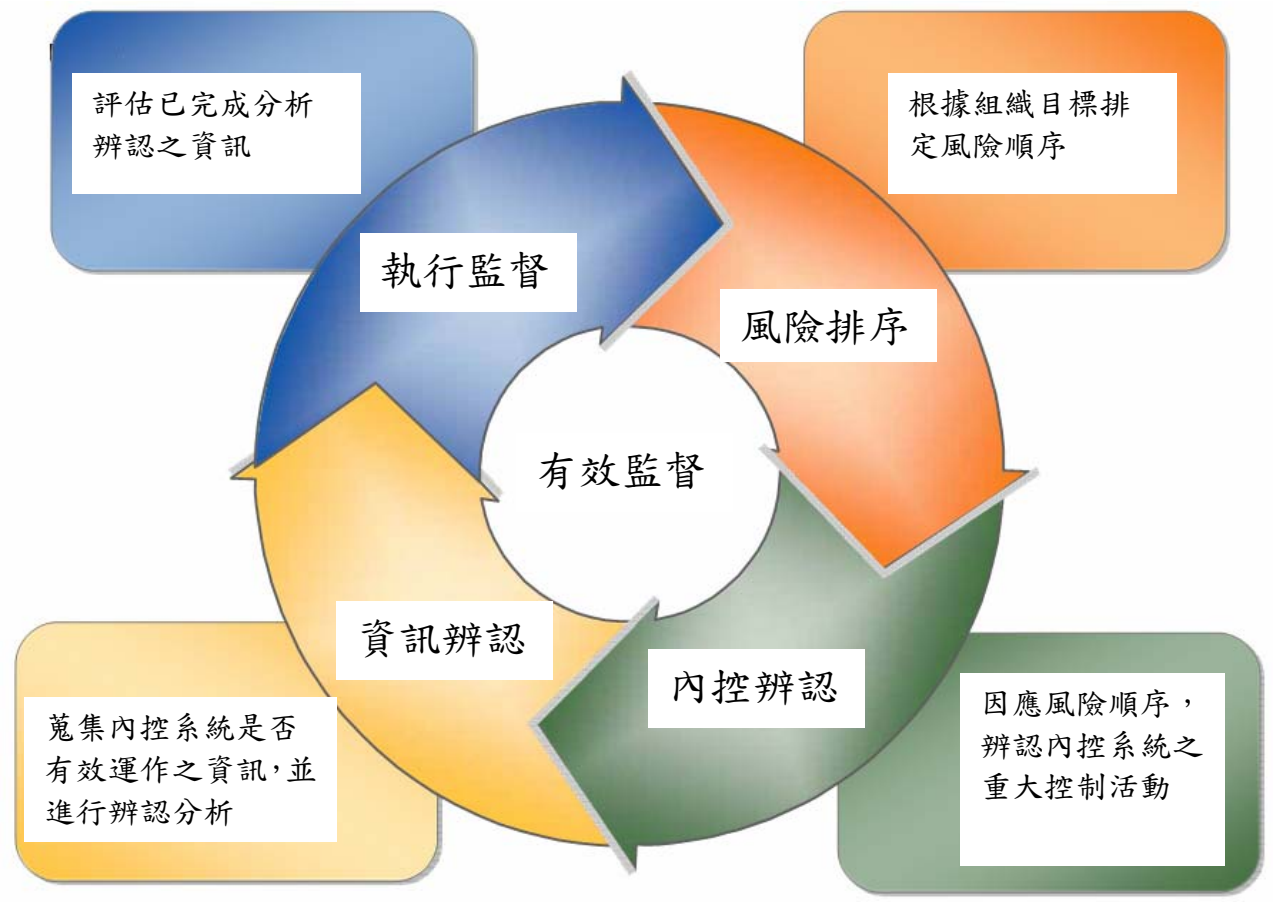
一、 建置基礎：有效執行監督行為之環境，包括：

（一） 高層對監督行為之重視程度。

（二） 公司選擇監督者時，有無考量其專業能力，並賦予權力。

二、 設計及執行

欲達到「有效監督」之目的，須根據風險之有關控制行為與重要程度，訂定並執行相關監督程序。其步驟如【圖 8】:



【圖 8】有效監督程序循環圖

「有效監督」循環之執行過程，依序分為以下步驟：風險排序、內控辨認、資訊辨認、執行監督。分別說明如下：

（一）風險排序：以風險管理導向為基礎，根據組織目標及風險程度，排定風險順序。

（二）內控辨認：因應風險順序，辨認內控系統之重大控制活動。至於所謂「重大」控制活動，如該控制行為失效時，其影響層面重大，

且無法即時偵測避免者，均可稱之。

（三）資訊辨認：即辨認前述之「直接資訊」與「間接資訊」

（四）執行監督：在完成資訊辨認之後，即開始進行監督行為。監督行為分成兩種：

1.「持續監督」(Ongoing Monitoring):即對例行性作業之有效性進行監督。由於其監督行為貼近一般作業，因此較有機會儘早辨識內控制度之缺失。

2.「獨立評核」(Separate Evaluation)：係指對特定作業或特定期間所進行之監督行為。「獨立評核」監督可運用「持續監督」之相關技巧以達成其目的，並對該作業之「持續監督」結果再次確認。但值得一提的是，由於「獨立評核」係屬特定事由所發起之監督行為，所以在其監督過程，須更注意保持客觀。

六、 控制紛亂（Controls Chaos）－其他產業可從金融風暴學習什麼？

本場次係由美國傑弗遜威爾斯管理顧問公司內部稽核與控制部門全球實務總裁 Cary Sturisky 及地區（EMEA）實務總裁 Jared Landin 共同主講，摘要如下：

（一） 金融風暴歷程

金融風暴前，外資投資美國資產以致長期利率走低、短期利率走高。投資公司利用低投資報酬搭配風險調整型年金，避險型投資則利用低成本、長期借貨以強化報酬率。此時之股市一片繁榮（美國道瓊指數

於 2006 年上揚 19%）、現金充足且具備高度流動性。但 2007 年 8 月初發生金融風暴後，全球股市下滑、四處都有物價波動及市場風險、被破壞的金融市場引發銀行業崩潰、銀行間的利率既高且不穩定（銀行害怕相互間的借貸）、銀行緊縮信用標準、在風險調整溢酬（risk-adjusted premium）取得現金，進出資本市場變得十分困難、當貸款公司離開產業時，抵押擔保市場縮小，許多超級意外事件均在同時間發生，例如雷曼兄弟（Lehman Brother）聲請破產保護、美林銀行出售、全球最大保險公司 AIG 收回國有。

金融風暴發生主因，係美國許多銀行未能建立以風險為導向之內部控制及稽核架構，一些著名銀行董事會及高階主管人員缺乏對於風險管理之認知，未能塑造重視風險管理之企業文化，又因許多職業經理人兼董事長及執行長，集決策及執行於一身，利益衝突未能迴避，其獨立監督功能啟人疑竇，復因職業經理人在董事會中作用之發揮和約束的制度安排不完善，致公司對經營性的風險及系統性風險漠不重視，形成治理機制的失靈，公司一味的追求短期卓越績效，進而衍生觸發金融風暴之基因，包括：

1. 美國次級房貸觸發全球銀行危機。
2. 空前的景氣榮景導致貸放條款過鬆，數以百萬信用紀錄不良的申請者，或許信用不合格，但卻獲得次級房貸購置房屋。
3. 隨著抵押擔保借款的增加，銀行將之發行股票，並於股市流通，銀行賺取每筆抵押擔保借款之出售費用，並提供抵押借款股票經紀商大量

的優惠措施，以增加銷售量。

4. 次級房貸如同調整型房貸利率，二年內固定付款，第一期後，利率調昇，較高的還款導致屋主付不起房貸，數以百萬的房屋被收回，問題惡化使得房價下降。

（二） 由金融危機所學習之經驗

金融危機導致全球經濟成長減緩，包括開發中國家之金融市場亦受嚴重影響，以致經濟成長衰退。影響所及，根據國際貨幣基金調查顯示，在 2009 年初期，多數已開發國家均瀕臨經濟衰退邊緣。因此，所有產業均應由此次金融危機之過程中，習得以下寶貴經驗，以避免危機再次發生：

1. 強化內部控制：

(1) 實施壓力測試（stress test）：

壓力測試係評估發生極端後果事項之後果測試，適用於可能性低且後果重大之事項，常用來評估營運事項或金融市場變動的後果，以避免意外損失發生，例如估計下列重要事項快速發生時的影響：利率上升，其影響及於固定收益投資組合之價值；能源價格上升，影響及於製造工廠之經營成本；外匯匯率變動，影響及於原料進口成本。

(2) 評估相對交易對手風險（Counterparty Risk）：

評估交易對手發生無法履行交易承諾之風險，如購買衍生性商品，對手無法交割之風險。

(3) 保持最大的流動性流出（maximum liquidity outflow）於安全水準：

公司發生財務重大危機時，短期間之最大流動性資產支出，應維持足以應付緊急危機狀況之安全水準。

2. 檢視信用評比機構：

發生金融風暴之前，許多信用評比機構給予銀行不實的信用評比（大部分給予虛偽不實的優良信用評比），而造成其浮濫的擴張授信，乃致衍生金融危機，故銀行本身內部稽核單位應加強獨立、辨識該信用評比之真實、有效性之稽核能力。

3. 嚴謹的風險管理相關事務：

(1) 提昇風險管理及治理能力：

建立 3 道風險管理防衛線（3 lines of defence），第 1 道防衛線是業務部門建立嚴謹的風險管理制度與流程，第 2 道防衛線是銀行本身內控品質之自我評估（QA），第 3 道防衛線是內部稽核協助管理階層建立監督風險管理架構，評估風險管理之有效性。

(2) 持續及系統化的檢視風險：

利用先進的電腦稽核軟體之分析（Analyze）、萃取（Extraction）、分類統計（Stratification）與差異確認（gap identification）等功能，產生異常資料並覆核異常資料以評估分析風險。

(3) 在經濟繁榮時期增加資本公積、以應付未來不確定的金融危機發生。

(4) 選任有能力、有經驗及消息靈通的管理階層：

因預防金融危機發生，以及應付已發生金融危機之處理，均需有專業能力及有相當經驗之管理階層方能勝任。

4. 審慎的業務擴張策略：

銀行對於企業的授信、投資未能訂定風險承擔限額，或對交易部位的衍生性金融商品評價作業未能確實，以及毫無風險觀念的不斷擴張業務策略，乃產生金融危機之主因，例如金融風暴前多家銀行不斷擴大信貸業務及各家投資銀行對於諸如CDO、MBS 等衍生性金融商品，追逐越來越高的槓桿比率及高利潤，擴大投資業務，最後導致他們加速滅亡。

5. 重視會計準則所能創造的透明度：

財務資訊的不透明常醞釀舞弊與策略方向錯誤的危機。

（三） 內部稽核專業所學習教訓

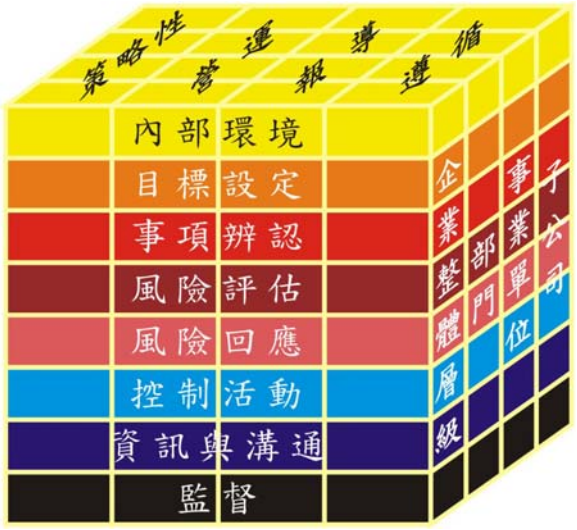
1. 公司治理：

內部稽核需對組織公司治理架構進行評估、衡量及報導，包括：企業行為及倫理、會計實務、法規機制之遵行情形；有關董事會組成的技術、經驗及獨立性；公司治理、風險管理、揭露及內部控制架構、政策及程序；審計委員會活動及財政困難之風險監督。

2. 風險管理：

內部稽核需聚焦並成為組織風險管理活動之主要參與者，包括：確保審計範圍符合風險管理架構、提供風險管理程序之確認、提供風險已正確評估之確認、評估及回饋風險管理程序、評估風險報告之正確性、檢視及監督關鍵風險之管理、瞭解企業政策及目標，及依風險之程度排定風險順序。

風險管理依 COSO 委員會 2004 年「企業風險管理—整合架構」，其追求的目標包括：策略性、營運、報導、遵循，追求的單位有企業整體層級部門、事業單位、子公司，至於進行的方式有內部環境、目標設定、事項辨認、風險評估、風險回應、控制活動、資訊與溝通，概述風險管理之定義為：企業或政府的人（內部環境）利用可靠之資訊（資訊與溝通）進行目標設定、事項辨認、風險評估、風險回應、控制活動以及監督。(如【圖 9】)



【圖 9】企業風險管理－COSO

3. 流動性審查：

內部稽核需要細心監控及執行流動性審查，特別聚焦在：

(1) 流動性架構、程序及方法。

(2) 衡量最壞情況（worse case）及其因應之程序。

(3) 處理及彙總公司數據之資訊系統及程序。

(4) 與流動性有關之資料品質（檢視資料有無虛偽、灌水情事）。

(5) 在危機中爭取時間之現金流動策略。

> 讓你陷入困境不是未知的事情，而是篤信錯誤事實。
>
> －馬克吐温，美國知名作家

4. 情境分析與壓力測試

內部稽核需審核及評估組織流動性需求是否進行有效之壓力測試及情境分析；所謂情境分析係建構在單一事件之假設性變化的組合（出售資產、地震），有價值的衡量事件對關鍵企業動因之影響，例如利息費用債券評等變化之影響，或如水災等自然災害對公司之影響；又所謂壓力測試，其定義如前述係評估發生極端後果事項之後果測試，簡言之「變化假設之百分比＝關鍵財務指標之百分比」。

七、 營運恢復力（Resilience）及持續性（Continuity）—確保資訊安全與可用性之災難復原（Disaster Recovery）

本場次係由國際內部稽核協會歐洲分會副主席—法國 COVERNIS &TEKVISIOS 公司執行長 Claude Cargou 主講，摘要如下：

（一） 當前面臨的挑戰—驅動力

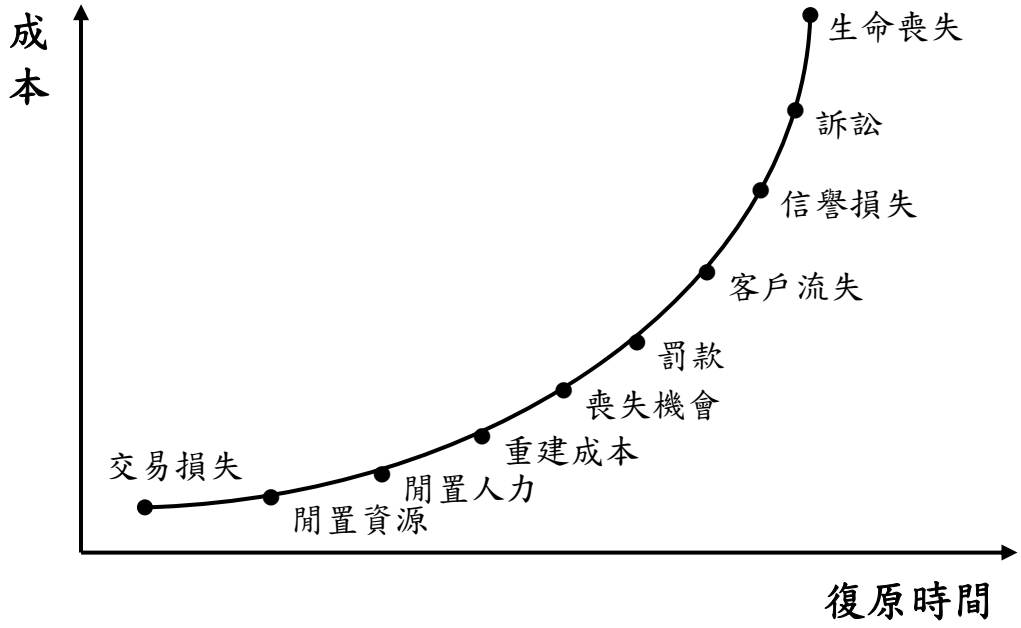
現今全球關聯密切之世界裡，資訊可謂各個企業及全球經濟之生命力，客戶隨時隨地需要獲取正確的資訊，因而許多公司必須處理有關資訊相關的重要問題，如安全威脅、服務中斷、地區性災害事件、全球化及法令規定。美國 911 意外攻擊事件破壞了許多電腦復原場所（Recovery Site），造成許多大公司數日後只能部分營運，數週後才能完全復原；規模很大的地區供電短路，證明了許多公司的復原計畫之不適當，全球化的公司一時陷入繁雜的法律規定之混亂，災變後無法迅速復原，導致公司商標、形象嚴重的損壞，因而世界各國之企業為避免災害造成的損害，紛紛加強營運持續管理（BCM），擬定營運持續計畫（BCP），實施營運衝擊分析（BIA）及風險評估（RA）。

（二） 災變復原問題探討

據 KPMG 國際會計師事務所研究結果發現，所有遭遇災害的公司，40％在二年內喪失營運能力；另據 AT＆G 公司之研究結果，在 2005 年 8 月計有 1,200 家企業在美國私部門設立災害應變計畫，惟 40％企業之持續性（Continuity）計畫並未被列為優先；2/3 的公司遭遇災害後喪失營運能力；16％的公司每日損失 100,000 至 500,000 美元；26％的公司承認他們無法估計損失多少；50％的公司在 6 個月內更新他們的災害復原計畫。

當非預期營運中斷之恢復時間愈長，企業須付出之基本成本愈高（包括：交易損失、閒置資源、閒置人力、重建成本、喪失機會、罰

款、客戶流失、信譽受損、訴訟、生命喪失。如圖 9），未能快速恢復將對公司形象產生負面影響。



【圖 10】企業成本 V.S.復原時間

（三） 恢復力（Resiliency）v.s. 復原（Recovery）

所謂恢復力（Resiliency），係指重建營運中斷服務後回復到符合營運各項需求（needs）之能力；回復（Recovery），則係指在時間範圍內回應營運災難而回復到符合營運各項要求（requirements）之能力。二者皆是 IT 導向。

（四） IT 復原與恢復力計畫之相關問題：

Claude Cargou 覆核 IT 復原與恢復力計畫之相關問題時，發現問題如下：

1. 現有「服務等級協議」（Service Level Agreements）及演練步驟未能充分反映管理階層之期望。

2. 重點所在—網路很少被測試，如有測試通常僅部分被測試而非全面，或是僅作網路連接測試而非壓力測試（Stress Test）。

3. IT 計畫很少與其營運本身之持續性相關。

4. IT 的恢復力及復原很少被稽核。

5. 公司營運的永續計畫（BCP）通常未包含 IT 恢復力及復原在內。

6. 雖將主機建置妥善，但主機回復之及時性令人質疑（災難復原如使用磁帶，是否所有磁帶來自非備援場所（off-site）之儲存設備？它能夠被讀嗎？）。

7. 設計復原計畫及實施測試時，未能於復原計畫與測試上適當的考量主機與分散式系統之之相互依賴度，因此當主機可以完全快速重建時，仍存在一些實際問題。

8. 部分組織內部備份資料中心同時設立於相同重要場所（如一些內部拷貝之備援資料中心與主要備援場所同時設立在校園裡），致共同災害復原場所之快速回復能力受限。

9. 災害復原備援場所迅速復原的能力有限，因為大部分公司「暖備援場所」（warm sites）僅佔 20 至 30％而已，其餘的「冷備援場所」（cold sites）也只處於「盡力」（best efforts）的狀態，如果有 2 個公司同時發生災害，備援之資源立即陷入吃緊（strained）狀況；又退守第二防線的備援場所計畫常不完備。

（五） 問題因應

■ 營運主管部分

1. 執行長應責成各營運主管具備 IT 恢復力及復原之相關資訊及智能。

2. 各營運主管應：

(1) 訂定 IT 恢復力及復原相關之營運衝擊分析（BIA）。

(2) 從組織內部指派一位 IT 恢復力及復原召集人，領導由各營運主管、IT 開發、IT 作業、供應商及稽核人員等所組成之治理團隊。

(3) 提供資金。

(4) 確保 IT 恢復力及復原計畫已納入營運持續計畫（BCP）。

(5) 參與測試。

■ 營運衝擊分析（BIA）（如【圖 10】），包含：

(1) 組織之各種作業流程及功能。

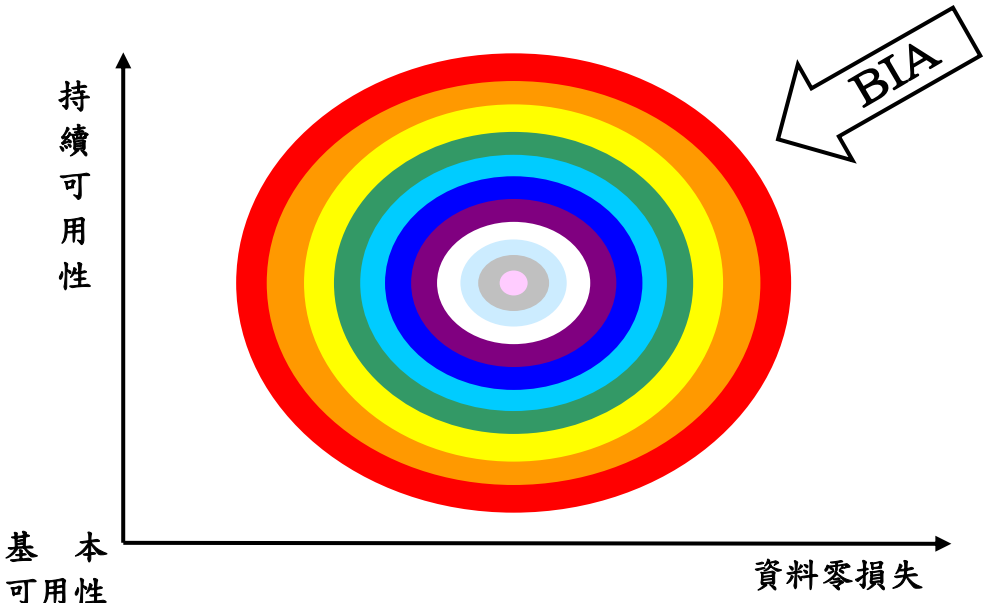
(2) 支援各種作業流程之必要資源。

(3) 各作業流程或部門間之關聯關係（包括供應商與委外廠商）。

(4) 執行某項作業流程或關鍵活動失敗之影響（評估相關衝擊及最長容忍中斷時間）。

(5) 設定每個作業流程之系統復原時間目標（recovery time objective，RTO）。

(6) 設定支持作業流程之資料復原時點目標（recovery point objective，RPO）。



【圖 11】BIA 發展圖

■ 治理團隊部分：

1. 團隊成員應包括：各營運主管、IT 開發、IT 作業、供應商及稽核人員。
2. 辨識營運恢復力及復原之相關規定。
3. 各營運主管參與測試管理—包括：恢復力之壓力測試（stress test）、點對點（point to point）恢復力及復原測試。
4. 設計方法及檢查表以利執行季節性檢查。
5. 確保 IT 恢復力及復原計畫已納入公司營運持續計畫。
6. 協助內部稽核人員檢查遵循程度
7. 向執行長及董事會審計委員會報告

■ 供應商部分：

1. 供應商協助是很重要的，其應該納入治理團隊之一，也是設計

解決方案工作團隊之一。

2. 供應商應擔任獨立覆核；驗證設計；檢查單一點失效、重要資料遺漏、互補解決方案完整性等之內部專家，並分享各種最佳實務之角色。

■ IT 恢復力：

辨識哪些關係已被辨識及包含於營運持續計畫（BCP）中。

■ IT 災難回復：

1. 恢復系統之資料備份至行政區以外或國家境外之資料中心－非同步內部備援場所；外部備援場所。並測試整體離線環境，包含復原時間。

2. 開發方法及檢查表，以確認所有復原之關係已被辨識及包含於計畫中。

（六） 策略解決方案

Claude Cargou 對上述挑戰之幾個策略解決方案如下：

A．恢復力：

1.方案一：可用性高，零資料損失

(1)同步連結 2 個內部資料中心，使重要營運系統具有高度可用性，限制距離為 100 公里以上。

(2)鏡像備援（mirrored data），零資料損失。

2.方案二：可用性高，部分資料損失

(1)非同步連結 2 個內部資料中心，使重要營運系統具有高度可用

性，無距離限制。

(2)鏡像備援（mirrored data），部分資料損失。

B．災難復原。

1. 方案三：內部復原備援點（site）

(1)非同步連結 2 個內部資料中心。

(2)鏡像備援（mirrored data）。

2. 方案四：外部復原備援點

(1)就重要營運系統簽訂充分「暖備援場所（warm site）」設備之契約。

(2)遠距儲存－磁帶或電子儲存庫（electronic vaulting）或二者皆可。（更具成本效益；復原延遲風險較高）

C．結合恢復力及復原：

1.方案五：可用性高＋內部復原備援點

(1)同步連結 2 個內部資料中心；鏡像備援，零資料損失。

(2)位於行政區以外或國家境外之非同步內部復原備援。

2.方案六：可用性高＋外部復原備援

(1)同步連結 2 個內部資料中心；鏡像備援，部分資料損失。

(2)外部復原備援點。

(3)遠距儲存－磁帶或電子儲存庫或二者皆可。

D．方案篩選：

1.各企業應視其營運需求性質及成本進行上開方案之篩選。

2.通常法令規定主導決策之制定，例如：

(1)在美國金融市場之公司，選擇兼具高度可用性及復原備援點超過 250 英里距離之方案，許多銀行適用此方案。

(2)在比利時，銀行已適用上開相關方案之要求。

3.我們強力推薦上開結合恢復力及復原之方案。

陸、 研討心得及建議意見

綜上，謹就本年國際內部稽核協會年會之專題演講內容，及同步研討會中所討論議題，提出研討心得及建議意見如次：

一、 掌握會計準則未來修訂情形，避免影響未來審計業務正常推動。

在全球化的趨勢下，世界各國之會計準則均逐步朝向與國際財務報導準則（IFRS）接軌方向邁進。而在我國，由於 IFRS 與現行的 ROC GAAP 的差異甚大，甚至有諸多 IFRS 已訂有特定公報予以規範，而我國尚無相關準則規定，諸如：合併報表、期中財務報表、金融商品之表達及揭露等。因此，我國金管單位近期陸續發布或修正許多財會公報，並密切關注國外目前的適用狀況以及相關的規定。預期在未來全面採用 IFRS 之後，各企業收入認列會和現在企業慣用方式將產生甚大差異，財務報表之編製方法亦有改變；此外，由於 IFRS 採原則基礎(Principle Based)之會計原則，企業由於在會計方法所採用空間較大，可否對其採用會計方法提供合理性說明，對查核人員將是挑戰；如企業無法提供完整佐證及說明，勢必增加審計困難度，甚至需要藉助其他專家意見，對

習於查核依 ROC GAPP 準則編製財報之審計人員而言，恐將因此增加查核時間。本部掌理公有營業、事業之審計業務，且有查核時間及人力限制，允應注意此一會計界國際趨勢，密切注意我國採用 IFRS 之預定期程及進度，並隨時掌握有關會計準則未來修訂情形，以提早研究因應之道，避免影響未來審計業務正常推動。

二、參考企業內部稽核積極態度，妥適扮演政府管理顧問角色。

風險管理係內部稽核之重要議題。以往稽核人員為協助管理階層改善機構之風險管理機制，係以提供獨立客觀之諮詢服務、協助進行管理活動，並針對特定風險及管制問題提供特殊建議。但於本次會議中，所有與會專家就內部稽核人員之權責議題莫不一再強調，內部稽核人員僅提供建議，而非代替管理階層執行工作；至管理階層接受內部稽核人員所提供意見後，如策略失效，亦不能因而免除追究課責。此外，以往內部稽核人員係針對風險管理已發生之管控缺失，以建議方式所提出之改善意見，管理階層可自行決定積極接受或消極處理；但目前觀念正逐漸改變，內部稽核單位平時即須積極與管理階層進行溝通，使其認同內部稽核人員在公司治理、風險及控制上所提意見，具系統化及客觀獨立之價值，業務部門在進行風險分析及評估之過程當中，內部稽核人員即應積極參與，而非在完成相關風險分析或評估過程後，才大肆評論尚有其他待改善之處。

上開內部稽核觀念之改變，係建立在公司有效治理之前提

上，內部稽核機制轉趨積極。此與目前審計機關期許成為「政府管理顧問」之理念，不謀而合。在作法上，審計機關可參考企業內部稽核之積極態度，在政府決策或法規修訂過程中，於謹守審計權責之前提下，視狀況提供以往審計經驗供行政部門參考，藉以加強與行政部門互動關係，並可消除其潛藏之抵制心態，對協助提升政府行政能力，恢弘審計職權，當具功效。

三、參考國際內部協會所推動「稽核－能力成熟度模型」(IA-CMM)方式進行自我評核，有效提升績效審計工作能力。

國際內部稽核協會研究中心開發完成之內部稽核－能力成熟度模型(IA-CMM)，以品質管理之角度，協助內部稽核單位進行自我評估，俾持續提昇稽核效能；此外，在自我評估過程中，內部稽核單位須與其所屬機構（或企業）之管理階層或營業單位進行互動，因此可增加彼此溝通及取得共識之機會，對於稽核業務推動，甚有幫助。另觀諸 IA-CMM 之模型架構，係由最高管理階層決定各項稽核單位關鍵要素（諸如：成員管理、專業實務、績效管理等），並視外在條件決定各該元素個別應達成之能力成熟度階段，嗣進一步討論各該階段之相關議題。其自我評核流程同時兼具廣度及深度，稽核主管亦可應外在環境，保留調整彈性，對於提升稽核能力，頗具價值。

審計機關與企業內部稽核單位之工作內容，有甚多相似之處。目前政府審計角色，已由傳統監督者，漸次轉變為提供民意

機關、監察院及受查單位加值服務之洞察者，因此績效審計之比重逐漸提高，乃必然趨勢。惟處於多元且日漸複雜之環境下，查核人員辦理績效審計工作時，須具備施政計畫及管理程序之分析能力，熟悉各種組織運作及重大施政計畫內涵，並能將查核議題提出邏輯且完整之意見[1]，因此，如何有效培訓合格之審計人力，實為審計機關必須正視課題。揆諸國際內部稽核協會刻正積極推動之IA-CMM，正可為審計機關於進行自我評核之過程中，提供有利方向，殊值更進一步深入參考及應用，俾期有效提升審計人員技能，澈底落實績效審計工作。

四、 學習金融風暴之教訓，發展風險管理導向之政府經費審計

2008 年全球金融風暴導致全球經濟成長減緩，此事件帶給企業界的教訓為：銀行在不健全的公司治理環境，缺乏嚴謹的內部控制與風險管理架構，暨無效的內部稽核與監督制度情況下，一味追求短期利潤結果，終導致企業走入「結束生命」的火坑，顯見風險管理除協助企業管理階層創造最大的價值外，尚能防止企業遭受重大損失，並維持企業永續經營的生命。

我國行政院於民國 94 年 8 月 8 日訂頒「行政機關風險管理推動方案」，規範政府推動風險管理之目標及實施策略，又於民國 97 年 4 月 1 日發布「行政院所屬各機關風險管理作業基準」，其內容包括：各部會辦理整合性風險管理之準備工作，風險管理

[1] 參考審計部「審計機關績效審計作業指引」

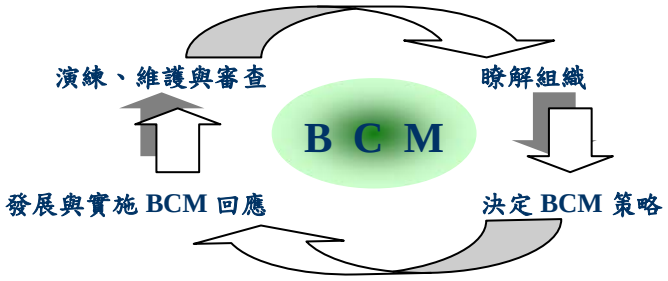
流程各階段應注意事項，提升部會組織風險管理能量及永續經營等原則性之要素，顯見行政機關風險管理乃政府重要之施政措施，政府風險管理日受重視，惟揆諸政府許多重大建設、投資及採購，發生營運後停擺、閒置、虧損、低度利用、轉投資效益不彰、採購不合用之物品，造成浪費、經費被非法挪用、貪污舞弊、施政計畫之執行未依限完成、浮編預算、盲目舉債致債台高築等事件仍屢見不鮮，足見政府常偏重於發生曝險事件後之處理，而對高風險之施政項目事前籌劃階段之辨識、評估及管理風險之能力尚待改善。政府財務收支之內部控制為政府審計之核心，而風險管理則是內部控制之延伸，惟風險管理常隨著時間之經過而有所改變，曾經有效的風險回應及控制活動，後來可能因計畫目標、組織結構、作業流程人員更替等因素之改變，而變得不再攸關，因此政府擬維持風險管理的持續有效，端賴政府管理當局之持續性監督（ongoing monitoring），及其內部稽核部門或外部稽核部門的「間斷性評估」，方能確保風險管理之有效性，進而合理保證達成施政目標，爰建議審計機關秉持監督政府機關財務收支之職責，加強審計人員有關政府風險管理專業實務訓練與能力培養，以監督政府機關落實風險管理工作，包括選擇高風險項目，從政府施政計畫開始，嚴格審核政府機關的風險管理架構是否健全、有效率及有效果，評估政府機關對風險的辨識能力及回應風險之控制活動（風險移轉分擔、抑減、規避、承受）是否有

效，並確認是否已將風險降到與其風險胃納一致之情境，進而提出有效之風險管理建議改善意見，俾達成提升審計價值及績效審計之目標。

五、 順應世界潮流建立永續經營理念，強化災難復原之應變能力，以確保資訊安全。

近年來電子資訊已成為維繫各個企業及全球經濟之生命力，惟當發生意外災難後，資訊作業的中斷對企業經營常造成重創公司的信譽與聲望、營業額降低、主要客戶流失、獲利減少、生產力降低、信用評比降低、市場競爭力降低等損害，有時嚴重到結束企業之生命，因此世界各國紛紛研擬訂定營運持續性計畫（BCP）及營運復原計畫（BRP）等相關規定，其中 ISO25999（草案）與 BS25999 有關 BCM（營運持續管理）之相關標準，其內容已發展成為可稽核的管理系統，頗值我們參考，本次南非 IIA 國際研討會 Claude 所演說的題目「營運恢復力及持續性」之內容，大部分與該標準有關 BCM 之內容相似。BCM 係一個管理流程，整合現有的風險管理、災害復原、資訊安全、緊急事件管理、危機溝通等管理制度，並鑑別威脅組織的潛在衝擊，提供一個具彈性之架構及有效反應能力之整體管理程序，以保護企業聲譽、品牌與價值，BCM 最大效益在改善組織而對關鍵目標崩潰的恢復能力，展現驗證的能力，管理業務中斷及保護組織的商譽，回復交付產品及服務的能力，並提供組織恢復能力之演練法。

BCM 的運作及發展程序為首先瞭解組織，實施營運衝擊分析（BIA），進行業務風險評估（RA），然後針對策略應考量的要素，如最大可容忍期間、成本等，暨策略應考量的資源項目，擬定策略之回應選項進而決定 BCM 策略，最後實施 BCM 之演練、維護及審查。如【圖 12】BCM 的建置及運作流程）



【圖 12】BCM 的建置及運作流程

BIA 評估分析的標的為作業流程，其目的在辨識風險及企業營運所需的資源，並評估中斷時間等潛在威脅所造成的衝擊，在衝擊與對策成本間取得平衡，建立復原的優先次序，並設定 RTO（復原時間目標）與 RPO（復原時點目標），定義關鍵活動的最長容忍中斷時間，鑑別支持關鍵活動的依存活動（包括供應商與委外廠商），定期或於組織活動有重大變化時進行營運分析；又上開 BCM 範疇中的風險評估（RA）主要目的在鑑別威脅與弱點暨風險與可接受風險水準，並針對關鍵活動選擇適當的風險處理方式，以降低中斷發生可能性，縮短中斷時間及減少其將來的衝擊。

前開 BCM 經 BIA 及 RA 運作後對已辨識之風險所實施之風險控制（回應）模式為：

（一）承受：

BCM 策略適用於組織內所接受的風險。但不適合組織可能藉由此法而調整其風險胃納。

（二）分擔（程序轉移）：

市場競爭策略協議（MCA）轉移至另一組織或主要組織的替代部分。相互協議能在某些選取服務上發揮效力，但建立此協議時應注意，該協議應具強制力，並透過服務等級協議（SLA）或正式契約方式進行測試；或購買保險商品，保險能夠提供組織財務補償，但保險本身並非完整解決方案，保險結合 BCM 可能是最整體性的解決方案。

（三）規避（終止或改變）：

欲改變或終止服務、產品、職務或程序之決定應視為 BCM 程序內程序策略的部分。此方法最常見於具有有限生命週期的產品。

（四）抑減（緩和損失）：

風險控制與行動計劃的實施與管理以減少、最小化或抵銷潛在損失。

綜上，營運持續管理 BCM 策略已成為 ISO 及 BS 之標準（25999），為世界各國普遍運用，而我國行政院為推動各機關強化資訊安全管理，建立安全可信賴之電子化政府，早於民國 88 年 9 月訂定「行政院所屬各機關資訊安全管理要點」，其中

第拾點規範業務永續運作，規定各機關應訂定業務永續運作計畫，評估各種人為天然災害對機關正常業務運作之影響、訂定緊急應變及回復作業程序及相關人員之權責並定期演練及調整更新計畫，本部亦於民國 91 年 5 月 1 日訂定「審計部及所屬各審計處室資訊安全管理作業規定」，其中第三十四點之規定內容與上開行政院資訊安全管理要點內容雷同，而近幾年來本部業研會對於本部及所屬審計處室有關資訊業務永續運作之規劃與督導不無餘力，惟因礙於備援資料貯存環境受限，致 AP 系統產生之備援資料未能貯存於一定安全距離之備援場所；另本部所屬機關亦礙於資訊人力之不足，未能定期獨立實施災害復原測試及演練；爰建議本部規劃適當的主機貯存空間，使所屬機關電腦各種 AP 系統所產生之資料（非公務機密及敏感性資料）以非同步連結本部主機方式，備份傳輸貯存於本部主機電腦，另本部各單位電腦 AP 系統產生之資料，其中機密部分經加密處理後，連同非機密資料分別貯存於一定安全距離之備援場所；建請本部業研會加強對本部所屬機關承辦資訊安全人員實施有關災害復原之測試及演練訓練，使其具有獨立實施災害復原作業之能力，或研發由本部主機經由網路直接對所屬機關電腦實施復原作業之技術，以達業務永續經營之目標。另建議本部加強審計人員有關營運持續管理（BCM）及災害復原（Recovery）的相關智能訓練，俾充實其對於各政府機關永續經營計畫之稽核能力。

《附錄 1》

一、 最佳範例（BEST PRACTICES）
（一） BP1：多重文化審計團隊群如何共同有效運作
（二） BP2：組織控制之意見表達
（三） BP3：內部控制之新標準
（四） BP4：持續審計：成果及挑戰
（五） BP5：風險管理、內部控制及公司治理之共同焦點：亞洲挑戰
（六） BP6：內部稽核師對適正計畫之加值

二、 風險管理(RISK MANAGEMENT)
（一） RM1：國際組織對舞弊風險之評估
（二） RM2：風險管理之信譽
（三） RM3：IFRS 之風險管理及內部稽核
（四） RM4：內部稽核人員對人際風險之監督
（五） RM5：新 COSO 指引中有關內控制度之監督範疇
（六） RM6：企業風險管理(ERM)之下一步

三、 柔性技巧(SOFT SKILLS)
（一）SS1：內部稽核報告之柔性面
（二）SS2：取得全球性資源
（三）SS3：強勢績效文化之發展
（四）SS4：適當之雇主角色
（五）SS5：如何將想法予以最佳落實
（六）SS6：驅動內部稽核至新階段

四、 資訊科技(IT)
（一）IT1：利用複合架構產生廣泛性之資訊科技控制環境
（二）IT2：審計軟體之心理層面
（三）IT3：資訊安全之確保
（四）IT4：如何利用部落格、維基等網路工具強化報告
（五）IT5：審計科技之策略性運用
（六）IT6：達成使用者安全有效取得資訊之 12 步驟

五、 舞弊(FRAUD)
（一）FR1：謊言偵測－終極發現
（二）FR2：專家目擊證詞
（三）FR3：政治控制環境下之舞弊及貪腐風險管理
（四）FR4：與敵人共枕－當董事會潛藏舞弊者
（五）FR5：從國際角度思考賄賂及貪腐
（六）FR6：竊取本質－國際性病根

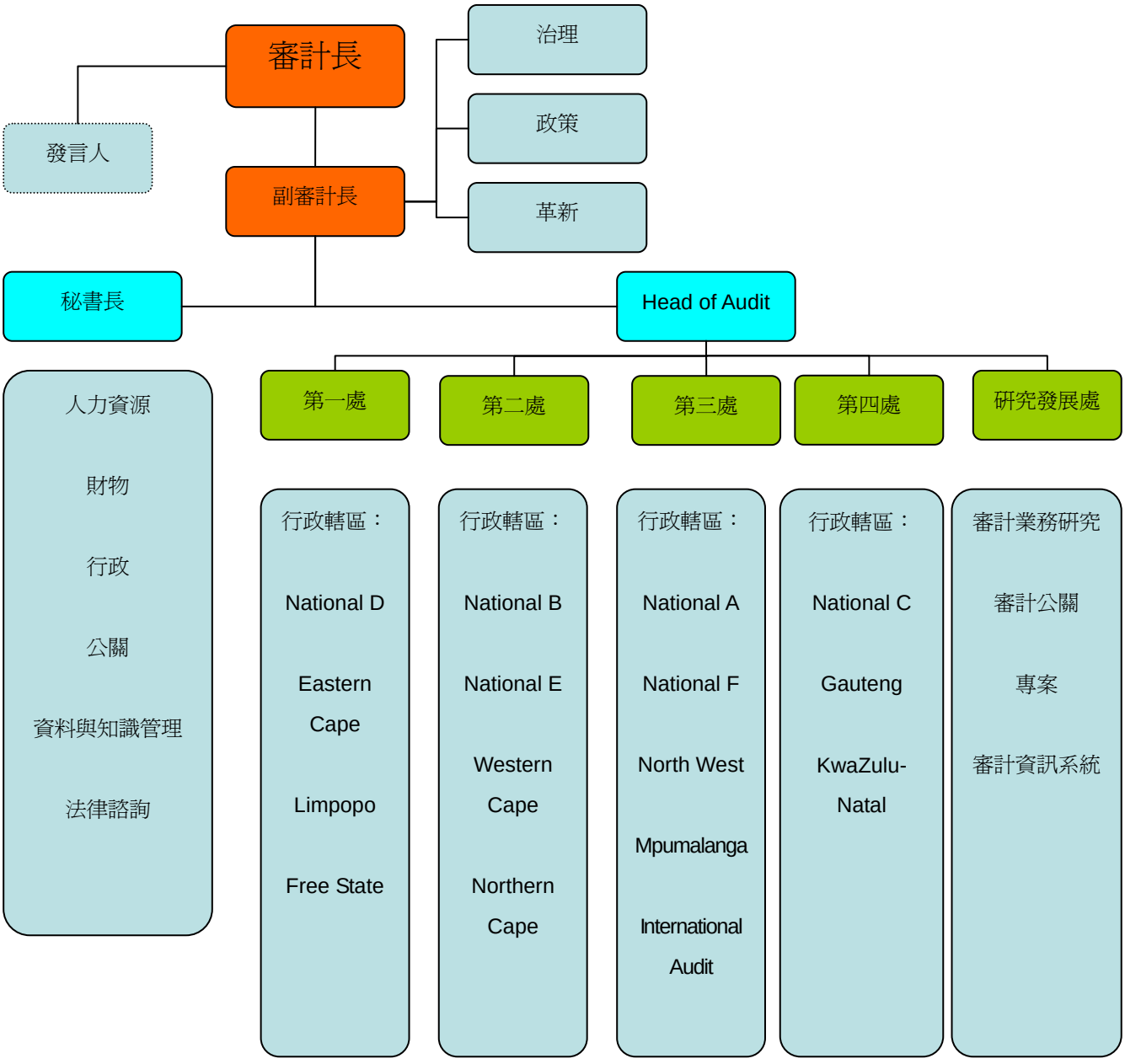
六、 政府部門(PUBLIC SECTOR)
（一）PS1：政府對內部稽核之期待
（二）PS2：IACMM 模型－內部稽核人員自我評估工具

（三）PS3：政府部門之有效及無效服務
（四）PS4：公部門內部稽核單位如何因應環境變遷
（五）PS5：審計績效資訊
（六）PS6：公部門內內部稽核人員對課責制度之貢獻

七、 公司治理(GOVERNANCE)
（一）GOV1：中國大陸之公司治理環境新形態
（二）GOV2：會議室禮儀
（三）GOV3：公司治理－內部稽核人員準備好了嗎？
（四）GOV4：由董事會角度看公司治理之價值
（五）GOV5：內部稽核係公司治理之重點－此為事實抑或迷思？
（六）GOV6：公司治理架構下之內部稽核人員角色

八、 新興議題(EMERGING ISSUES)
（一）EI1：確認性稽核之整合可否避免公司發生危機
（二）EI2：由跨領域之角度思考專業化之新興議題
（三）EI3：各產業由金融危機可學習之課題
（四）EI4：公司社會責任
（五）EI5：利用成熟性模型加強內部稽核之價值
（六）EI6：公司治理之文化因素

《附錄 2》 南非審計機關組織架構圖



我們的願景

我們係可提升公部門課責能力，且受人民（利害關係人）認同之最高審計機關

聲譽承諾／任務

審計長依憲法之規定為最高審計機關之首長，其職權為藉由對公部門審計之監督、課責與治理，而強化國家的民主，進而建立公眾的信賴。

我們的價值

- 我們受民眾信賴與尊敬
- 我們的課責性明確且嚴謹
- 我們以績效為導向
- 我們擁有良好聲譽
- 我們擁有高效率之團隊
- 我們以南非為榮

《參考資料》

1. 2009 年 IIA 國際年會書面資料。
2. An Overview: COSO's guidance on Monitoring Internal Controls，Dr. Sridhar Ramamoorti。
3. Internal Control – Integrated Framework, Guidance on Monitoring Internal Control Systems，Sep. 2007。
4. Internal Audit Capability Model(IA-CM)for the Public Sector, http://www.theiia.org/research。
5. "Is your internal audit department ready for IFRS?", Ernst & Young Global (EYG) 。
6. Structure and processes of the IPPF, http://www.theiia.org/guidance/additional-resources/ippf-project/。
7. 國際專業實務架構，財團法人中華民國內部稽核協會。
8. 單一財會準則時代即將來臨－談會計準則與國際接軌，詹靜秋，內部稽核季刊，98年3月。
9. 談英國政府風險管理內部稽核，行政院研究發展考核委員會。
10. 台灣會計準則與國際會計準則之比較，安永會計師事務所。
11. 財團法人中華民國會計研究發展基金會－TIFRS專區，最後瀏覽日：民國98年8月15日。
12. 財團法人中華民國內部稽核協會網站(http://www.iia.org.tw/)，最後瀏覽日：民國98年8月31日。
13. 企業風險管理－整合架構，馬秀如博士等譯，財團法人中華民國會計研究發展基金會。
14. 企業風險管理－整合架構應用技術，馬秀如博士等譯，財團法人中華民國會計研究發展基金會，財團法人中華民國內部稽核協會。