2012 年亞洲區內部稽核協會年會

出國報告

出國人員：廖繼寬、劉玉珠、戴慧萍、郭博文

報告日期：民國 102 年 2 月 7 日

2012 年亞洲區內部稽核協會年會出國報告

摘要

2012 年亞洲區國際內部稽核協會年會於民國 101 年 11 月 8 日至 10 日一連 3 天假泰國曼谷詩麗吉皇后國際會議中心（Queen Sirikit National Convention Center）舉行。年會主題為「沙拉泰（Sala-Thai）」，意指有效之公司治理、風險管理、內部控制與內部稽核，以維護組織生存及價值發展。本屆年會，共有來自 16 個會員國約 500 多人參加，計安排 6 場專題演講(General Session)，及 20 場同步研討(Concurrent Session)。同步研討部分，分為「舞弊偵測與預防」、「資訊科技」、「公司治理、風險與遵循」、「風險管理」、「內部稽核技術與能力」等 5 項議題（track），各 4 場，共計 20 場主題。茲就參加年會經過、專題演講摘要、重要研討主題、研討心得及建議意見提出報告。研提建議意見如下：

一、審計人員應對環境風險保持高度警覺，並堅持獨立性，以回應民眾之期待。

二、審計機關應加強跨領域專業合作，俾利舞弊查核作業之進行。

三、審核意見須表達合宜，適時溝通確保意見能正確傳達予利害關係人，並持續追蹤辦理情形。

四、建構政府審計人力資本彈性化策略，加強人才留任管理。

五、辨識關鍵或潛在風險，加強辦理施政策略及計畫之審計，俾對民眾生活產生正面影響。

六、推廣應用資訊技術控管架構稽核資訊環境，加強資訊技術風險管理，掌握最新資訊科技發展趨勢，承擔稽核新興科技之工作挑戰。

七、加強運用電腦軟體輔助審計，善用持續性稽核工具與地理資訊系統，推廣電腦稽核師認證機制，促進審計工作品質進步與創新。

八、因應個人資料保護法新制實施，研擬個人資料保護之配套措施，強化安全維護管理策略。


BANGKOK 2012

目　錄

壹、前言 1
貳、參加年會過程 3
叁、專題演講摘要 6
一、精準的表達與溝通 6
二、最佳公司治理之人力風險評估 10
三、高標準的專業倫理與職業道德：內部稽核之必備要素 13
四、價值性風險管理 18
五、企業營運持續性計畫與災難復原審計 26
肆、重要研討主題 33
一、舞弊偵測技術 33
二、確認性服務黑洞－董事會及審計委員會如何發覺公司黑天鵝的存在？ 40
三、規劃一個新時代的風險管理制度 46
四、資訊科技風險與控制之最新發展 52
五、內部稽核：提升組織治理、風險與遵循之能力 58
六、企業策略稽核 63
七、資訊科技稽核人員如何能跟上最新科技趨勢 70
伍、研討心得及建議意見 78
一、審計人員應對環境風險保持高度警覺，並堅持獨立性，以回應民眾之期待 78
二、審計機關應加強跨領域專業合作，俾利舞弊查核作業之進行 83
三、審核意見須表達合宜，適時溝通確保意見能正確傳達予利害關係人，並持續追蹤辦理情形 85
四、建構政府審計人力資本彈性化策略，加強人才留任管理 86
五、辨識關鍵或潛在風險，加強辦理施政策略及計畫之審計， 91

俾對民眾生活產生正面影響
六、推廣應用資訊技術控管架構稽核資訊環境，加強資訊技術風險管理，掌握最新資訊科技發展趨勢，承擔稽核新興科技之工作挑戰 94
七、加強運用電腦軟體輔助審計，善用持續性稽核工具與地理資訊系統，推廣電腦稽核師認證機制，促進審計工作品質進步與創新 96
八、因應個人資料保護法新制實施，研擬個人資料保護之配套措施，強化安全維護管理策略 100
參考資料 104

表　目　錄

表 1	年會專題演講場次及主題	4
表 2	年會同步研討場次及主題	5
表 3	內部稽核功能之滿意度調查	9
表 4	全球企業十大風險調查結果	23
表 5	職業舞弊的初期偵知統計表	36
表 6	電腦輔助查核工具與技術類型表	57
表 7	亞洲各國公司治理分數：2007 至 2012 年	59
表 8	嘉特納公司（Gartner）提出 2012 年 10 大科技趨勢	73
表 9	美國有線電視公司（CNN）提出 2012 年 10 大科技趨勢	74
表 10	舞弊犯罪型態、平均每案損失及比例統計表	79

圖　目　錄

圖 1	溝通工具的轉變	7
圖 2	安永企業風險雷達	20
圖 3	安永風險熱圖	21
圖 4	全球企業十大風險雷達	22
圖 5	營運持續性管理生命週期圖	29
圖 6	舞弊預防計畫元素圖	39
圖 7	公司治理的四大支柱	44
圖 8	董事會風險確認架構圖	45
圖 9	風險應變彈性連續體圖	48
圖 10	風險管理階段圖	50
圖 11	內部稽核工作效能圖	51
圖 12	實施 GRC 模型之目前與未來狀態	61
圖 13	策略稽核流程	66
圖 14	最高審計機關價值與意義架構圖	92

2012 年亞洲區內部稽核協會年會出國報告

壹、前言

2012 年亞洲區內部稽核協會年會（以下稱年會），於民國 101 年 11 月 8 日至 10 日一連 3 天假泰國曼谷詩麗吉皇后國際會議中心(Queen Sirikit National Convention Center）舉行。年會主題為「沙拉泰（Sala-Thai）」或稱「泰式涼亭」。Sala 係泰文 ศาลา 的發音，指的是開放式的涼亭，該涼亭廣設於泰國之佛寺及相關宗教勝地，供人遮陽避雨之用，因此「沙拉泰」引申意為一處可供信眾休憩並保護信眾之所在，可謂為「泰國人的智慧」。本屆年會延伸此概念，邀請各國專業人士齊聚，共同探討保護組織之所在，及促進組織永續發展最有智慧之道。年會探討之議題涵蓋有效之公司治理、風險管理、內部控制與內部稽核及組織之永續發展等。本屆年會除地主國泰國外，並有來自台灣、日本、新加坡、香港、韓國、中國、印度、澳洲、紐西蘭、馬來西亞、菲律賓、印尼等國，約 500 多名內部稽核人員、會計師、專家

學者等參與。本部為鼓勵同仁積極參與國際性稽核專業研討活動，培養審計人員的國際觀，本次年會經簽奉核定遴派本部第四廳廖廳長繼寬、臺北市審計處劉科長玉珠、屏東縣審計室戴審計慧萍及本部業研會郭審計員博文等 4 人前往與會，謹將參加年會過程、專題演講摘要、重要研討主題、本次研討心得及建議意見等，報告如后。

貳、參加年會過程

2012 年亞洲區內部稽核協會年會係由泰國內部稽核協會（IIA, Thailand）主辦，泰國觀光局（Tourism Authority of Thailand）協辦。有關本屆議程，除開幕典禮與閉幕典禮外，主辦單位計安排 6 場專題演講（General Session；專題演講場次及主題詳如表 1），及 20 場同步研討（Concurrent Session）。同步研討部分，分為「舞弊偵測與預防」、「資訊科技」、「公司治理、風險與遵循」、「風險管理」、「內部稽核技術與能力」等 5 項議題（track），各 4 場，共計 20 場主題（同步研討場次及主題詳如表 2）。

本次會議主講人及與會人員皆樂於分享許多觀念與寶貴之實務經驗，各場次主講人亦熱烈回應來賓及與會者之提問，而本次受邀主講的來賓，大部分皆具有產業界之實務背景，或為組織中負責風險管理及內部稽核等經驗豐富之專業人員，深深瞭解公司治理、內部控制與風險管理之重要，與如何促進組織之永續經營，找到能為組織提供永續保護的「沙拉泰」。

最特別的是來自臺灣的中華民國內部稽核協會代表，於大會期間之尾聲，與泰國內部稽核協會代表進行交接，所有成員皆上台預告及宣傳下一屆（2013 年）將於臺北舉辦之亞洲區內部稽核協會年會。現場並反覆播放「臺灣感動您的心」（Taiwan will touch your heart）之宣傳影片，尤其是影片當中的宣傳歌曲，一聽就令人印象深刻、琅琅上口，更引起與會人員廣大的迴響。

表 1　年會專題演講場次及主題

場次	專題演講主題	主講人
GS1	精準的表達與溝通（Say it Right）	Phil D. Tarling 全球 IIA 主席暨華為技術公司（英國）內部稽核卓越中心副總裁
GS2	最佳公司治理之人力風險評估（Human Risk Assessment for the Best Corporate Governance）	John Jungsuk Pyun 韓國內部控制協會理事長
GS3	高標準的專業倫理與職業道德：內部稽核之必備要素（A Strong Ethical Compass: Essential for Internal Auditing）	Mr. David Polansky 全球 IIA 高級副總裁兼財務長
GS4	價值性風險管理(Managing Risk for Value）	Stanley Chang 中國大陸安永會計師事務所合夥人
GS5	企業營運持續計畫與災難復原審計（Auditing BCP and Disaster Recovery）	Ms. Yasumi Taniguchi 日本甫瀚諮詢公司總經理
GS6	改善泰國資本市場公司治理與內部稽核之要務（Mission to Improve Corporate Governance and Internal Audit in the Thai Capital Market）	Dr. Vorapol Socatiyanurak 泰國證券交易所主任秘書

表 2　年會同步研討場次及主題

場次	A	B	C	D	E
	舞弊偵測與預防	資訊科技	公司治理、風險與遵循	風險管理	內部稽核技術與能力
CS1	舞弊偵測技術	社會媒體風險管理	確認性服務黑洞－董事會及審計委員會如何發掘公司黑天鵝的存在？	規劃一個新時代的風險管理制度	面對未來趨勢與挑戰你是否準備好了？
CS2	內部稽核與舞弊	資訊科技風險與控制之最新發展	內部稽核：提升組織治理、風險與遵循之能力	內部控制與企業風險管理之整合	執行連續性控制監督
CS3	發展與實施舞弊風險確認地圖	評估組織之未來資訊科技、資訊安全趨勢及威脅	澳洲之公司治理	企業策略稽核	執行內部稽核工作所需之重要特質：勇氣觀點
CS4	偵測舞弊、浪費及濫用之實務工具	資訊科技稽核人員如何能跟上最新科技趨勢	公司治理、風險與遵循	如何正確執行風險導向之內部稽核？	合併確認性服務之成功因素

叁、專題演講摘要

本次年會邀請了英國華為副總裁、韓國內部控制協會理事長、全球 IIA 高級副總裁兼財務長等多位知名的專家學者進行專題演講，主題包括「精準的表達與溝通」、「最佳公司治理之人力風險評估」、「高標準的專業倫理與職業道德：內部稽核之必備要素」、「價值性風險管理」、「企業營運持續計畫與災難復原審計」及「改善泰國資本市場公司治理與內部稽核之要務」等 6 場，茲就其中 5 場專題演講內容，摘述如次：

一、精準的表達與溝通

本專題主講人為菲爾塔林（Phil D.Tarling）先生，塔林先生係英國華為（Huawei）技術公司內部稽核卓越中心副總裁，並於 2012 年開始擔任全球 IIA 主席。國際內部稽核協會（IIA）係全球性的專業協會和標準制定機構，目前會員人數約 175,000 人，來自 165 個國家。塔林先生主要負責監督及策略領導，以提升全球 IIA 之內部稽核專業價值。塔林擁有超過 25 年的內部稽核、金融、商業和公部門預算領域之經驗，主要工作經驗係對世界各國的 IIA、政府和公司行號，提供諮詢和培訓服務。

（一）十年來溝通工具的變化

人與人之間的溝通工具，因為科技的進步而產生變化。伴隨著網際網路的盛行、無線通訊用戶的增多，以及電腦、手機及各

項通訊設備的日漸豐富，溝通方法與工具在人們日常生活中所扮演的角色也發生著變化，進而亦影響溝通工具的管理方法。溝通工具由傳統上的書面溝通、手寫板、檢核表等逐漸演變為平版電腦、觸控手機、連網直接對話、視訊、臉書等溝通媒介。下圖顯示近年來溝通工具的改變。

塔林先生認為表達與溝通對於今日的內部稽核人員是一項相當重要的能力，隨著全世界溝通工具的改變，人與人的溝通方式變得更加多元且迅速，只要一瞬間訊息便已傳達。內部稽核人員需要因應這些變化，除了培養聽別人說的能力外，更應加強正確表達與溝通之能力，精準的表達自己想說的，以確保利害關係人能正確地接受稽核人員所欲表達之內容。

圖 1　溝通工具的轉變

（二）內部稽核人員如何達到有效的溝通？

內部稽核之工作關係著多數人的權利，具有舉足輕重之地位，按國際內部稽核協會對內部稽核之定義為：「一種獨立、

客觀的確認及諮詢活動，用以創造價值及改善組織的營運…透過系統化及紀律化的方法，評估及改善風險管理、控制及治理過程的效果，以達成組織的目標。」故如何溝通，原本係為內部稽核人員已經發展，透過報告風格並且傾聽的一項柔軟的技能。但在早期，內部稽核人員並未重視並妥善溝通，致大多數人對內部稽核人員印象極差。隨著溝通工具的演進，內部稽核人員更要努力改善溝通的效能以落實其角色定位，以獨立、客觀的角度執行確認與諮詢活動，增加企業營運的附加價值。

如何達到有效的溝通，首先應用同理心的立場，聆聽、瞭解對方之想法、確認問題之所在、給予適當回應及取得共識等，就如同塔林先生所述：「溝通現在是內部稽核的一項關鍵業務，其做法為：1.集中於風險；2.決定建議的解決方案；3.公正客觀而獨立；4.避免持觀望態度；5.主動積極參與組織的成功或失敗。」塔林先生亦提醒我們，在溝通同時，我們須確保我們在說之時，不僅僅有觀眾在聆聽，還要確保我們能精準地表達。

（三）如何提升內部稽核的整體滿意度？

溝通係提升內部稽核整體滿意度之最佳作法。內部稽核工作範圍常要跨越文化的藩籬，最重要的是互相尊重，聆聽不同的聲音、接受不同的方法，要知道沒有一種方法是絕對正確的，但仍須確保審計團隊之工作有共同的標準，這要定

期舉行會議、研習並妥善溝通始能達成。惟除此之外，如果現今來調查內部稽核是否能滿足利害相關人的需求和期望，審計委員會及高階管理者所評價的整體滿意度為何？IIA 在 2011 年分別對各公司審計委員會及高階管理者所進行的滿意度調查結果，如下表所示。表中顯示雖然審計委員會及高階管理者認為內部稽核的表現達到「好」的比率高達五成；惟認為達到「傑出」的比率，分別僅為 25.9%及 14%，問題出在於審計委員會及高階管理當局認為內部稽核應能提供之洞察力仍有不足之處，塔林先生認為原因在於內部稽核人員缺乏良好的溝通能力。為了使內部稽核之功能精益求精，提升良好的溝通能力，是相當重要的。

表 3　內部稽核功能之滿意度調查

	審計委員會	高階管理者
無法接受	0.0%	0.4%
差	0.4%	1.9%
尚可接受	16.1%	25.9%
好	57.6%	57.8%
傑出	25.9%	14.0%

（四）稽核長可執行的管理方式

要增加稽核人員溝通的能力，提升內部稽核的功能，塔

林先生提出以下幾點建議：

1. 與董事會直接對話，並透過審計委員會；

2. 理解高層管理人員所說的；

3. 正確解讀傳達的訊息；

4. 確保訊息回應給正確的人；

5. 要確保溝通能明確，採用平實的語言，簡潔的報告；

6. 身為顧問，隨時向董事會和審計委員會提供業務諮詢；

7. 與審計委員會成員及主席經常有非正式的互動；

8. 不只報告審計結果，亦能與業務之高層管理者討論業務問題；

9. 定期向高級管理層和董事會溝通：如新興企業所面臨的風險、從審計結果中獲知的風險和控制之趨勢等；

10. 加強內部稽核團隊間所需要的各項溝通技能。

二、最佳公司治理之人力風險評估

本專題主講人約翰·姜薩克·平恩博士（John Jungsuk Pyun），是會計師、內部稽核師、國際金融稽核師，擔任韓國內部稽核協會副理事長，與內部控制協會理事長，之前曾任韓國銀行聯合會高級管理職務與稽核工作，及數家大公司審計委員會委員，主講內容

是韓國的人力風險評估，以及韓國模式的良善公司治理。他認為人力風險評估，有助於做為創造不同性格員工更佳績效表現之重要工具，人格類型意味著公司的領導風格，人格評估分為 3 類：人格的完整性、決策過程的信心，和社會責任。

（一）最佳公司治理

治理本身指的是內部控制，內部控制的另一個說法就是治理。還有治理是以人事管理為基礎，我們必須發展及改變稽核實務，從系統的基礎，轉變到以人為基礎，人的風險比系統風險還大很多，必須更專注於人格特質評估的模式。經濟合作與發展組織（OECD）指出治理是一種關係，指的是人與人的關係、企業的關係、政治的關係與社會的關係，公司治理是公司管理階層、董事會、股東和其他利害關係人之關係，提供目標設定、實現和管理績效所需之架構。

最佳治理的決定因素，包含揭露、稽核、董事會、股東、紅利、誠信和道德價值觀、管理哲學和經營風格、組織治理、權力與責任分配、人力資源政策和程序、人員能力等等。韓國的公司治理服務中心，1 年進行 2 次公司治理調查，評估 17 個韓國家族企業集團結果，最佳治理依序是杜尚（Dusan）、鮮京（SK）、三星（Sumsung）、樂金（LG）、樂天（Lotte）、現代（Hyundai）等集團，研究團隊也選擇美國的通用和谷歌公司、德國的西門子和海德堡公司、日本的松下和住友等為最佳企業治理典範，該等企

業治理最出色部分，是具有誠正哲學和公民文化、增進人員效率的智慧工作環境、由下而上的人力行為評估。谷歌轉化韓國三星經驗，採取從基層向上的人事評估方法；西門子是德國最大且古老的公司，從三星那裡採用四眼決策過程[1]，這些人坐在一起共同合作，共識的決策模式，也有很成功的經驗，又如韓國樂天集團，採取從上到下的做法，在內部控制中，進行人格特質評估，做為一位執行長候選人，他的人格特質必須被評估，現在三星和現代等企業也採用人格評量測驗，來招募新員工。

（二）治理是內部控制

治理就是內部控制，內部控制的意思是自我控制。自我控制也是人的風險評估的指導，包含自我覺察、自我假設。以個人為基礎的思考控制，掌控情緒、掌控身體，然後你可以掌控心靈，就有希望，亦即當一個人能掌控自己的身體，他就能控制情緒與認知，這也造成了一個基礎，能夠掌控道德層面，而以團隊為基礎而言，控制改變，控制道德，進一步掌控想法。我們必須提高內在的正直度，才能獲得更好的能量。

（三）人力風險評估

以人的風險而言，當人的能力提高時，企業的風險就降低了，我們必須投資在人力資源方面。人的風險因素，會影響員工之工作表現，我們能夠透過員工訓練，掌握有關誠實、道德、倫

[1] 「四眼原則」，是指所有重大業務決策都必須由 2 個人（技術主管和商務主管）共同完成，若不能達成一致意見，則由高一級人員進行裁決，以保證經營策略能平衡商業、技術和銷售等各方面的風險。

理等因素，人的風險或人格特質評量一樣，是最強力的工具，來強化管理高層的正直及信賴度。管理財務報告風險之關鍵，往往較少在系統與過程，而較多是在其背後的人。當能力下降，風險就會上升。你可以設計控制並促進組織成功，將員工的無形資產，責任心、承諾、倫理和道德、誠信，均予以評估，任何一項都有可能助於一個更強大的控制環境，或使其惡化，內部稽核人員應挑戰組織內各階層員工之素質、誠正、動機。人格風險評估得到的結論是，性格評估是強化高階管理人員誠正與課責之最有效工具。

（四）人格評估模型

人格特質評估有很多模式，例如 DISC 行為模式之評量分析、MBTI 模式、弗洛依德心智論、榮格的人格特質論、安奈爾格蘭的九型人格識人術等，可供判讀個人行為、建立團隊與領導統御、組織管理、人際溝通及衝突解決之用。不要擔心自己的背景，找出你的類型加以修正，你會發現很實用，且表現會更好。

三、高標準的專業倫理與職業道德：內部稽核之必備要素

本專題主講人大衛．波蘭斯基先生（Mr. David Polansky），是國際內部稽核協會（IIA）財務長，服務於佛羅里達奧蘭多總部，也是 IIA 全球營運長，他的全球性團隊與世界 105 個分支機構共同提供專業指導、學習機會和知識評估認證。他認為內部稽

核人員傳統上在組織內往往被自己和他人視為「誠正堡壘」(bastions of integrity)和「倫理道德的光明信標」(beacons of ethical light)。我們總是可以信賴內部稽核人員做正確的事；然而，他們也是人，同樣受到來自文化、政治及組織的壓力。本演講探討內部稽核人員每日在導引倫理困境所面臨之挑戰，除了實際案例研究獲取之經驗教訓外，並探討國際內部稽核協會的倫理守則，與導引內部稽核人員通過「倫理道德流沙」(ethical quick sand)之有效策略。

大衛擔任 IIA 財務長、營運長各有 15 年、8 年之久，有很多深度經驗，他說由於 IIA 在全世界有很強的財務基礎與控制機制，他並不擔心倫理風險，讓他比較擔心的，是某地區內部稽核可能違反專業倫理，涉及欺騙或醜聞，可能會對專業聲譽造成重大打擊之風險。如何面對這些風險？首先必須接受並承認這些風險是存在的，認清每個人都有「盲點」，瞭解盲點的源頭，它們在組織中可能存在的地方，才能戰勝盲點。你的倫理羅盤有多可靠，是否成為自己盲點的犧牲品？他以麥特貝捷蒙（Max H. Bazerman)、安坦佛朗斯(Ann E. Tenbrunsel)合撰「盲點」(Blind Spots）這本書做報告腳本，推薦該書除了談到倫理盲點外，也是稽核作業很好的參考。

內部稽核人員盲點所在，明顯之倫理失誤，已無法避免被鎂

光燈關注。過去 10 年來，一些倫理失誤案例，還有醜聞事件，共同點就是欺騙、藏住資訊，對內部稽核來說是不道德的，例如美國有個州大學校長亂用特別費，州稽核人員發現後未予揭發，後來州政府把整個大學系統稽核部門主管全換掉，全世界有那麼多內部稽核人員和部門組織，少數害群之馬雖不至重創稽核聲譽，但人們會開始把點和點之間作連結，質疑這些人的價值，所以我們必須被看成是好人才行。他談到倫理守則，倫理守則是道德行為的藍圖，不過，有守則並不足夠，試看安隆（Enron）案，他們也有守則，必須能遵守守則，才能發揮作用。

（一）國際內部稽核協會的倫理守則（The IIA’s Code of Ethics）

這項守則是內部稽核人員行為藍圖，有關是與非之規範，包含道德責任和義務，是有價值的倫理原則。IIA 倫理守則之目的，在於提升內部稽核專業倫理文化，包含 4 大原則，這些原則更進一步由規範來加以定義：

1. 廉正：內部稽核的廉正性建立了信任感，且提供對其判斷之信賴基礎，組織信賴我們，我們必須提出正確資訊。其規範是內部稽核人員應：(1) 誠實、勤勉、負責；(2) 瞭解法律並且進行揭露；(3) 不得進行非法或不名譽的行為；有些事雖合法，但可能是不道德的，就不該做；(4) 尊重並努力達成合法且符合倫理目標。

2. 客觀：內部稽核人員必須展現最高程度的專業客觀性，在

進行檢驗某項行動或過程中，從蒐集、評估、和報告資料時都一樣。內部稽核人員必須對所有相關情事，進行平衡的評估判斷，不應受到自己立場或他人影響。其規範是：(1) 內部稽核人員不應參與任何會造成偏見的活動；(2) 不接受任何會削弱專業判斷的事；(3) 揭露一切重要事實。

3. 保密：內部稽核尊重其所獲得之資訊的價值與所有權，在未經適當授權下，不應揭露任何資訊，除非因法律或專業要求而必須如此。內部稽核人員應：(1) 審慎使用並保護所有的資訊；(2) 不違法使用資訊或用來獲取利益。

4. 勝任能力：內部稽核不應在缺乏知識、技能或經驗的情況下進行，內部稽核人員應：(1) 不參與其缺乏知識、技能和經驗之服務；(2) 遵循標準；(3) 持續改善精進效果和品質。

(二) 內部稽核人員的「盲點」

大衛先生不認為稽核人員會故意違反專業倫理，倫理的違背通常是因「盲點」而起，大部分問題發生在灰色地帶。內部稽核人員把自己當成組織中信任的保護者，期待的作為是揭露不道德行為，而自己不會進行違背倫理的事，然而實際上，我們的思想容易受到倫理規範的限制，或認知的侷限，因而可能沒有覺察到所做決策的倫理層面。當遇到真實情況時，行為可能突然改變，當下想要的，和認為會做的不一樣；專業人員傾向於把利益衝突，看成刻意墮落的問題，不過既得利益者會有完全不同的看

法，他們已經無法再客觀了。不要認為你不可能做出糟糕的決策，我們都是不完美的，必須防衛自己抵抗誘惑，記得合法和符合倫理可能是 2 件事。現實中，我們的盲點每天被暴露出來，因為各種因素，而把倫理的衝突合理化。案例情境如下：

情境 1：你的內部稽核團隊發現，在國際商業部門，可能有賄賂情形發生，法律顧問建議你不必擔心--這些只是使作業順暢完全合法的付款，把這件事公開，只會讓一般人困惑，卻傷害公司聲譽或罰款。你可能合理化想，反正顧問說沒問題，就先擱著吧。

情境 2：你剛完成某領域的稽核作業，這部門是你幾年前工作過的，假設你是這個公司的稽核長，你發現重大的管理缺失，當時你是負責這個領域的，你知道揭露出來會影響你的表現成果，會不會合理化的想，經過這麼多年，這不重要了，如果我提出報告，會讓我受到埋沒，你會提出報告嗎？或者你剛稽核 1 個你一直很想進入的部門，你有關鍵性的發現，而揭露出來可能終結任何你進去工作的機會，你會報告嗎?

情境 3：你稽核某個領域，其中你的家人或好友必須負關鍵責任，你發現應該可以預防的重大問題，揭露出來可能會影響親人或朋友，甚至讓他們失業，直覺上你想這是工作，當然要報告，不過如果和你最好的朋友或者岳父及親人有關，你可以瞭解這些因素會讓你改變，給你很好的理由不揭露。

（三）省思

強化倫理羅盤之策略，在於認識並解決盲點。想想哪些策略，可以強化倫理，首先必須理解，為了生存、滿足利益做出行為選擇，完全是人性所趨，在做決策時，必須冷靜想一想，為何這麼做、盲點在哪裡、將有哪些影響，應用一些管控方法，強迫自己深思熟慮，有的組織在稽查人員參與查核事件之前，要求填寫有沒有朋友或家人在所稽查領域工作之問卷，提出各式問題，強迫冷靜仔細思考，以發現可能的倫理衝突盲點。

四、價值性風險管理

本專題主講人為張翌軒先生（Stanley Chang），張先生係北京安永（Ernst & Young）管理顧問公司之合夥人。他曾對亞洲國家的主要大企業、政府機關、中央銀行及地方、省政府之國營企業，及多國之非營利組織等提供有關內部稽核、風險管理、內部控制覆核及公司治理等服務，有非常資深的內部稽核實務經驗。

（一）安永的全球企業十大風險與機會調查

今日的企業面臨許多前所未有的挑戰，市場波動性、定價壓力、市場績效變異、利害關係人之需求等因素，促使企業間的競爭愈來愈激烈。安永於過去幾年皆針對全球各大企業進行風險調

查，並出版年度企業風險報告（Business Risk Report），由於風險與機會往往是一體兩面，如何能將危機轉化為轉機，取決於企業領導人之智慧與企業之風險管理機制。安永本次報告除比照往年針對全球企業之風險進行調查外，並擴展研究範圍，將機會納入調查，同時探討全球企業之十大風險與十大機會。

本年度（2012）在 ACIIA 專題演講所提出之報告，係安永針對 2011 年度進行之調查研究，並對 2013 年度提出預測。惟因為本場次時間的限制，張先生僅對全球十大風險進行討論。為了辨認當前及未來企業可能面臨的風險與策略挑戰，本調查首先對專家學者進行訪談，訪談對象包括各產業的企業高階主管（策略規劃及風險管理主管、內部稽核主管、業務單位主管等）、企管顧問、分析師、安永的實務專家等，受訪人數超過 75 人，並涵蓋金融、政府與公部門、健康照料、生命科學、石油與天然氣、能源與電力及零售與批發等 7 個產業。

為瞭解已辨認出的策略挑戰之重要性，並對各項風險進行排序及對未來進行預測，安永於本年度特別進行第 2 階段的大規模調查，不同於第 1 階段之專家訪談，本階段主要係調查 15 個國家的政府與企業，針對其自身之組織狀況進行回應，每個國家約有 50 至 52 個組織接受調查。7 個產業中，最少的產業有 82 個組織接受調查，最多的產業則達 142 個組織，本階段共計調查 733 個政府與企業組織。

（二）安永的企業風險雷達與風險熱圖

依據安永所發展出的安永風險通用模型(Ernst & Young Risk Universe™ model)，企業之風險可區分為財務、遵循、營運及策略 4 個構面，並可以雷達圖加以表示，稱為安永風險雷達，如下圖。遵循風險源於政治、法律、管制規範或公司治理；財務風險源於市場和實體經濟的波動性；策略風險與顧客、競爭對手及投資者有關；營運風險則影響到企業的流程、系統、人員及企業整體價值鏈。落點愈接近雷達的中心，代表企業高階主管認為該風險之挑戰愈大。

圖 2　安永企業風險雷達

安永風險熱圖（Ernst & Young Risk Heat Map）呈現另一種觀點的風險分布，此工具能使我們從調查結果中瞭解到企業高階主管用於減緩風險的策略。右上角的部份是最受到企業所關注

的風險，代表受訪者普遍認為這些風險對其企業產生的影響相對較大。同時，較多受訪者表示，需要採取更多措施以有效管理這些風險，但企業仍未採取有效措施進行管理。

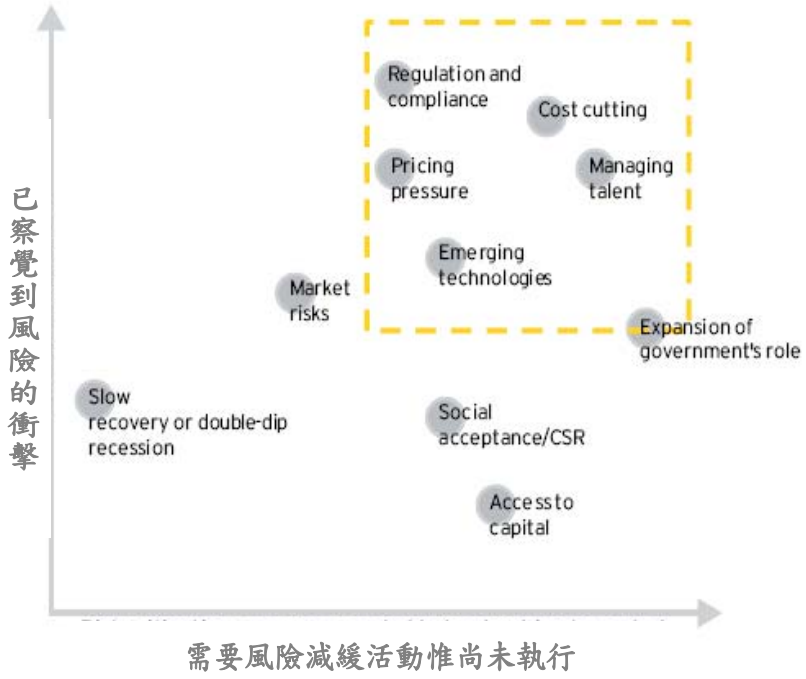


圖 3　安永風險熱圖

儘管圖中各風險的位置並非總是基於調查統計的顯著差異設定，但在考慮減緩風險因素的情況下，該圖針對可能被認為是最重要的風險提出了一種不同觀點，以該圖（2011 年調查結果）為例，企業應重視降低成本和人才管理這兩項風險。

（三）全球企業十大風險

下圖顯示本次全球十大企業風險之調查結果。安永企業風險雷達是一個簡單明瞭的工具，可以清楚地顯示研究所涵蓋的 7 個

產業之十大風險。位於雷達中心的風險係受調查的 700 多位企業高階主管，所普遍認為未來數年內可能對其企業構成最大挑戰的風險。箭頭表示這些高階主管對 2013 年該風險的重要性是上升還是下降的預測。

圖 4　全球企業十大風險雷達

2011 年全球企業的 10 大風險依序為：法規與遵循、削減成本、人才管理、定價壓力、新興科技、市場風險、政府職能之擴張、經濟復甦緩慢或二次蕭條、社會可接受風險（企業社會責任）及取得貸款。下表列出十大風險、2010 年之排名及 2013 年之預測。

表 4　全球企業十大風險調查結果

風險	2011 排名	2010 排名	2013 預測
法規與遵循	1	1	◎
削減成本	2	6	—
人才管理	3	4	+
定價壓力	4	15	—
新興科技	5	13	+
市場風險	6	新進	+
政府職能之擴張	7	新進	+
經濟復甦緩慢或二次蕭條	8	3	—
社會可接受風險	9	9	+
取得貸款	10	2	+

註：「＋」：排名上升；「－」：排名下降；「◎」：排名維持不變。

1. 法規與遵循

與 2010 年報告相較，排名仍居首位。在所調查的 7 個行業中，有 4 個行業排在首位。把該風險排在第一的 2 個行業（銀行、生命科學）對 2013 年的風險均持看漲態度。預測 2013 年，將與當前排名一樣，仍維持在十大風險之首。

2. 削減成本

與 2010 年報告相較，排名上升 4 名。企業普遍認為促使削減成本排名上升的原因，來自於政府的財政緊縮政策。預測 2013 年排名將有所下降。

3. 人才管理

與 2010 年報告相較，排名上升 1 名。儘管未高居榜首，但幾

乎所有行業都將人力資源風險列為前四大挑戰之一。企業普遍認為應該加強對人才管理的重視，並研訂人才管理的流程，此外新興市場國家對此風險的關注程度最高。預測 2013 年之排名將有所上升。

4. 定價壓力

與 2010 年報告相較，排名上升 11 名（2010 年該風險排在第 15 名，並未上榜）。許多行業的企業正面臨市場成熟和成長率減緩的挑戰，這對價格構成壓力。此外，與削減成本一樣，國家財政緊縮政策顯然也是促成此風險上升的原因之一。預測 2013 年之排名將有所下降。

5. 新興科技

與 2010 年報告相較，排名上升 8 名。提及該風險最多的原因在於企業在建立創新文化中面臨的困境和未經驗證技術帶來的不確定性。預測 2013 年之排名將有所上升。

6. 市場風險

新進入前十大風險之一。市場風險是一個新近上榜的風險，主要原因在商品價格震盪和房地產市場波動。預測 2013 年之排名將有所上升。

7. 政府職能之擴張

另一個新進前十大風險是政府職強之擴張，該風險是全球兩個最大經濟體—美國和中國的受訪者最關注的四大問題之

一。預測 2013 年排名將有所上升。

8. 經濟復甦緩慢或二次蕭條

與 2010 年報告相較，排名下降 5 名。由於社會預期經濟日漸復甦，經濟風險有所下降，但仍有 50%的德國受訪者表現出對財政緊縮等問題的擔憂，同時有 50%的美國受訪者表示個人需求依然疲軟。預測 2013 年該排名將有所下降。

9. 社會可接受風險（企業社會責任）

與 2010 年報告排名相同，仍為第 9 名。石油天然氣、生命科學和公共管理行業提及來自公眾壓力上升的受訪者最多。提及最多的應對措施是在企業經營策略中融入企業社會責任。預測 2013 年之排名將有所上升。

10. 取得貸款

與 2010 年相較，排名下降 8 名。企業對獲取信貸的擔憂總體上有所消除，但全球四分之一的企業仍然表示難以取得貸款。預測 2013 年之排名將有所上升。

研究調查的結果發現，法規與遵循目前仍是企業面臨的最大風險，係銀行業與生命科學產業最為關注的風險，在 7 個行業中，有 4 個行業都將法規與遵循列為第一大風險。且所有行業均將該風險列為四大風險之一，預測 2013 年仍為首要風險。目前企業建議之因應策略為，透過風險長的設置來管理該風險，並加強與政府部門的關係及提升法規遵循的職能。

政府職能之擴張係 2011 年又一新增之風險。在調查的 7 個產業中有 6 個產業的受訪者認為 2013 年該風險的重要性會持續上升。未來國家與私營企業之間的關係將與現在大不一樣，政府在處理其與私營企業關係時，將會扮演更主動的角色。雖然許多受訪者都表示已為削減成本及定價壓力採取了相對有效的措施，但在所有行業中，這兩項風險的排名亦大幅上升。

（四）結語

如何面對風險並做好風險管理，是企業創造商機的重要課題。報告中提及的企業十大風險之排序係經過定性的研究及持續資料之蒐集所得出，目的係幫助企業辨認 2011 年及以後年度所面臨的主要風險。然而，不同的產業、不同的企業對風險的定義皆有所不同，這取決於企業的目標和許多其他因素。因此，安永希望透過此十大風險的研究報告引起討論，並有機會再對此進行更深入之探索。

五、企業營運持續性計畫與災難復原審計

本專題主講人為谷口保實（Yasumi Taniguchi）女士，谷口女士目前擔任日本甫瀚顧問公司董事總經理，亦是日本安達信的風險諮詢組的成員，在美國和日本擁有超過 15 年內部審計和風險諮詢服務經驗。她向日本介紹 CSA，並率先成為日本內部稽核人員第一個通過認證

之 CSA。谷口女士在日本風險與控制自我評估會議中，亦是一個經驗豐富的主持人。會議中，谷口女士指出在 2011 年 3 月 11 日，日本北部發生大地震，引發的巨大海嘯淹沒了宮城縣部分經濟區域，其破壞性影響及供應鏈連鎖性反應，不僅重挫日本各大企業，亦波及全球。本場演講係討論關於從地震、海嘯以及其他近期發生的災害事件帶給日本公司的教訓及經驗，會議內容涵蓋基礎知識、營運持續性計畫到內部稽核人員的角色和價值。

（一）日本地震和自然災害的經驗教訓

2011 年 3 月 11 日，在日本發生芮氏規模 9.0 級大地震，隨後而來的巨大海嘯（滑坡長度 450 公里，寬度 150 公里、40.5 公尺）毫不留情的侵入了宮城縣。強震令日本福島縣核電廠發生故障，廠內多個核電機組相繼發生爆炸引致輻射外洩，通信、電力線路停擺，輻射的不斷釋放，折損當地的設施、污染鄰近海域及重挫各地商業行為，持鑽的電力短缺、輻射問題蔓延各地，全球相關供應鏈同受其損害波及，損失經日本估計超過 3,000 億美元。另最近發生的災害和直接經濟成本，如下分述：

1.2011 年日本東北大地震和海嘯，日本損失估計超過 3,000 億美元。

2.2008 年四川大地震，中國損失估計超過：148 億美元。

3.2011 年泰國水災：損失估計 457 億美元（世界銀行估計）。

4.2001 年美國 911 恐怖襲擊事件：損失估計 207 億美元。

5.2005 年美國卡特里娜颶風保險賠償 450 億美元。

從上揭災害的經驗學到的教訓與經驗，有：

1.肇因於自然災害或其他事故致業務中斷之影響力會漸形擴大。

2.現在全球供應鏈係多層次的，只要一有國家發生災難，連鎖反應將波及全球。

3.如果災難一定會發生，應事先預計將是何時生。

4.災難準備和危機應對計畫應依據最壞的情況下妥為規劃。

（二）深入瞭解營運持續性

企業營運持續性是指企業有應對風險、自動調整和快速反應的能力，以保證企業能持續運作，分為危機管理計畫、災難復原計畫（IT）、業務復原計畫等。現在各國已訂立營運續性架構和指導方針者包括：英國標準協會（BSI）所訂之 BS 25999－Business Continuity、新加坡標準 SS540、澳大利亞和新西蘭 BCM 標準 AS/NZS5050:2010…等；另國際組織 ISO 在 2012 年 5 月亦公布了新的標準－ISO22301:2012 社會安全，營運持續性管理系統，可供各行業參照應用。營運持續性管理生命週期，圖示如下：

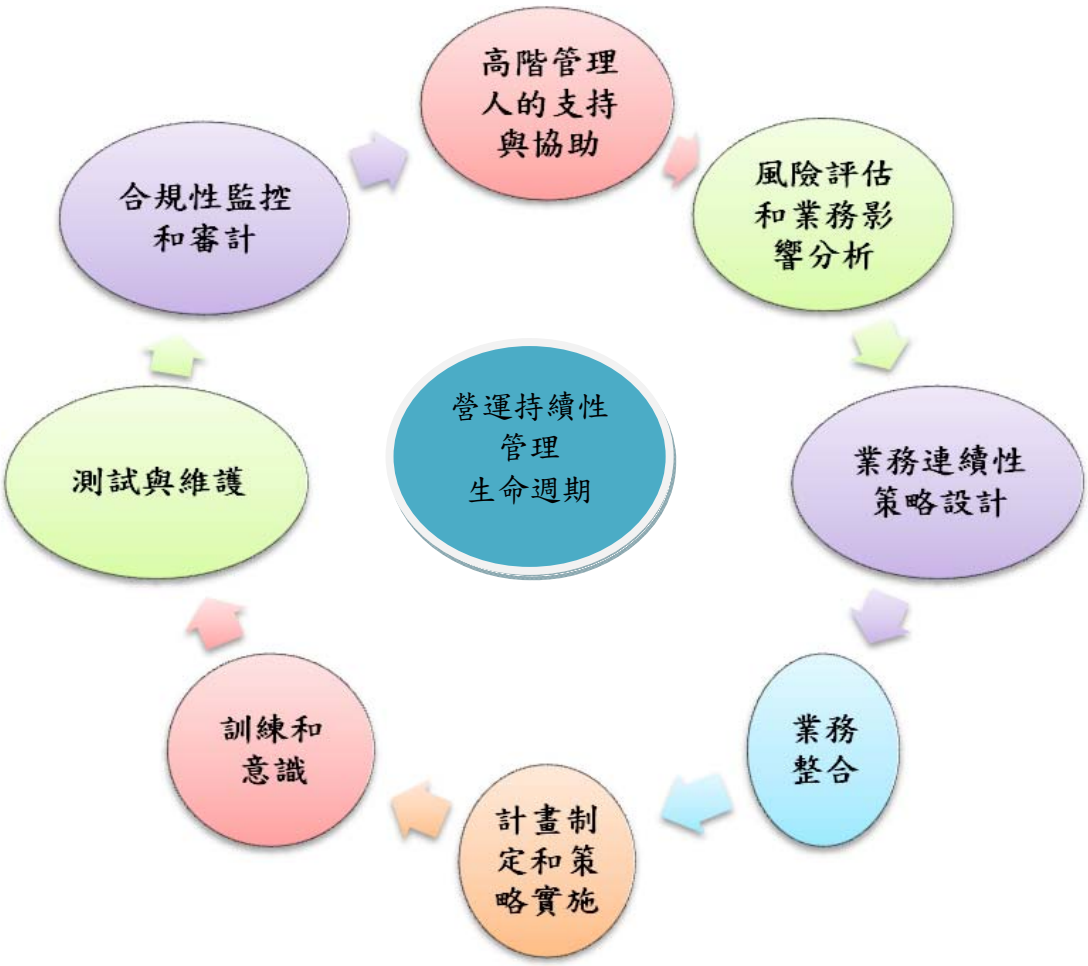


圖 5　營運持續性管理生命週期圖

當資訊網路一有危機，應納入營運持續性計畫的不應只是資訊科技，該計畫既強調營運持續性，就必須涵蓋整個組織範圍、部門和業務，要有效恢復網絡或業務連結免於中斷，需要的技術人員除 IT 部門的主要成員外，還有為該公司提供的服務的任何廠商，且更要共同仔細研究各項業務流程，落實顧客服務精神，有效並優先為客戶提供服務。

（三）內部稽核在營運持續性中擔任的角色

1.須事先得到執行營運持續性管理者的支持

（1）監管要求；

（2）審計結果；

（3）客戶的特殊需求；

（4）從風險評估和業務影響分析結果（BIA）；

（5）內部稽核人員應隨時評估組織的營運持續性過程；

（6）內部稽核的功能—應定期評估組織的營運持續性過程，事先做好營運持續性準備供高階管理人員隨時參考。

2.發揮內部稽核在營運持續性計畫中的作用

（1）組織的規劃方面—內部稽核活動可以協助評估組織的內、外在環境。

（2）在評估 BCP / DRP 設計過程方面—內部審計人員對企業、個人的功能和關係能有透徹了解；審查擬定之營運持續性及災難復原計畫的設計、完整性、和整體性有否充足。

3.在審查營運持續性計畫中，內部稽核人員應考慮的方向，為：

（1）所有的計畫為最新的嗎？（有否過時？）

（2）是否涵蓋所有關鍵業務功能和系統？

（3）計畫設計之基礎上已包含業務中斷風險及潛在後果？

（4）計畫已完整記錄了嗎？

（5）職能和責任分配為何？

（6）是組織能夠且預備實施的計畫嗎？

（7）測試和修訂計畫是建立在成果的基礎上嗎？

（8）計畫檔案是否正確和安全地儲存，並確知儲存位置。

（9）員工全然熟知備用設施的位置。

（10）計畫能向當地的緊急服務求助並協調？

4.執行營運持續性及災難復原計畫後回饋期，內部稽核人員的角色：

（1）監督計畫的成果和控制的有效性。

（2）對 BCP 提出建議改善意見。

（3）在災難復原計畫過程中提供支持。

（4）協助確定災難中汲取的經驗、教訓和恢復之操作事宜。

5.定期審計組織的 BCPs/DRPs 及相關問題

（1）不利的情況發生後，充分保證已及時恢復操作和處理。

（2）反映當前企業的經營環境。

（四）結語

谷口女士認為，日本經歷了大地震、海嘯等天然災難的洗禮，已從中汲取教訓，深知只有透過營業持續性業務之管理和內部稽核的功能及運作，妥予建立危機管理機制，來支持公司營運持續性管理，才能有效減輕突如其來災難之損害，就如同美國國土安全部（The Department of Homeland Security）有言：「今日投

資於計畫，不僅有助於保護您公司的投資和生活，同時也支持了您的員工、客戶、利益相關者、社會、當地經濟，乃至於全國。」

肆、重要研討主題

一、舞弊偵測技術

本場次係由澳大利亞企業破產重組公司（KordaMentha）執行董事羅伯特‧科克雷爾（Mr. Robert Cockerell）先生主講。科克雷爾為一擁有專業證照且逾 30 年專業服務經驗之調查學者，主要從事複雜的犯罪調查工作及舞弊偵知預防。自 2010 年 9 月起任職墨爾本辦事處之舞弊調查小組，協助各企業組織進行偵防及再審查作業。

他首先敘明舞弊的定義:「蓄意以欺騙或其他手段獲取不當利益」。公司內部員工或外部的人竊取公司金錢或財產，這些蓄意欺騙之行為將對個人或組織造成實質或潛在的財務損失，亦衍生後續不良效應，身為審計人員必須學習前衛的面談技巧以提高聆聽技能、發掘問題及有效分析，瞭解不合理行為相關線索，以檢測舞弊是否確實存在。

（一）典型欺詐舞弊犯之共同特徵

羅伯特先生指出，澳大利亞犯罪學研究所在 2003 年之研究[2]，有關典型舞弊犯之共同特徵，可供我們檢視參考，如下：

1. 平均年齡約 40 歲（女性約 42 歲，男性約 43 歲）。

[2]資料來源：2003 年，澳大利亞和紐西蘭的嚴重欺詐案，AIC 研究和公共政策系列第 48 號，AIC，澳大利亞澳大利亞犯罪學研究所。

2.被指控者約 80%為男性，20%的女性。

3.大部分為完成中學教育或擁有大學以上之高學歷人士。

4.約 44%的人握有相關犯罪訊息。

6.約 27%的人有詐欺前科。

7.超過 50%的人沒有犯罪記錄。

8.最常見的動機是貪婪和賭博，20%的動機是從事與業務相關工作。

9.大部分舞弊犯是會計主管、高階經理人或主管。

根據美國舞弊查核師協會的報告指出，公司負責人及行政主管涉及舞弊的比例僅 23.3%，不過一旦涉及舞弊，竊占金額高達 834,000 美元；經理人次之，涉及舞弊比例占 37.1%，竊占金額平均為 150,000 美元；基層員工為主嫌比例占 39.7%，造成企業損失平均僅約 70,000 美元，而該研究亦指出，儘管男性犯罪者比例頻率最高，占舞弊案件 40.9%，但女性往往是主謀，經統計，受害者蒙受之損失會隨主謀年齡及學歷攀升。

（二）舞弊之趨勢及統計數據

近年來，舞弊案之數量、及因舞弊案耗費成本有漸趨增加趨勢，羅伯特先生指出於2009年畢馬威會計師事務所舞弊調查結果及舞弊查核師協會在 2008 年報告（Nation on Occupational Fraud and Abuse）等文獻、相關統計數據中，即可得知最成功的企業往往是商業舞弊的主要受害者。以下分述：

（1）從 2008 年 1 月起每 6 個月間，澳洲法庭起訴的較大宗的舞弊案金額已經超過 1 億美元。

（2）2006 年至 2008 年期間，馬來西亞調查舞弊訪談費用約人民幣 63,500,000 元。

（3)澳大利亞企業估計員工舞弊損失每年約耗費 18 億美元。

（4）最成功的企業常是商業欺詐的主要受害者。

（5）舞弊查核師估計，典型的美國組織因舞弊失去了 7%的年度收入（相當於 994 億美元)。

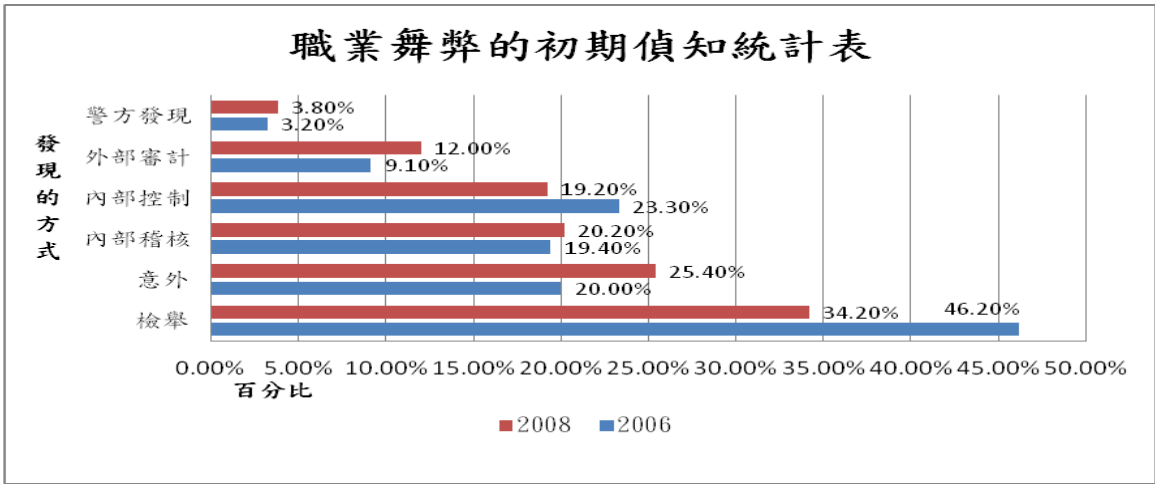
（6）英國一年的舞弊成本耗費約 300 億英鎊 ，這遠遠超過先前舞弊查核師之預期。

另 2008 年美國舞弊查核師協會(ACFE)指出[3]，幾乎一半以上的案例研究中，舞弊最常被發現的方式是檢舉（占 46.2%)，意外發現僅占 20.0%，研究調查證明，企業仍要更積極做好偵查舞弊的工作，亦說明了良好的控制環境，在舞弊偵測各環節中的重要性。

根據調查，目前公認反詐騙最有用的方法依序為：1.設置舉發專線；2.匿名檢舉信函；3.道德規範。而要讓密告檢舉者能暢所欲言、提供更完整詳盡的證據，就需要一個感覺安全又可靠的環境，如果整體環境讓所有員工認知舞弊及不道德是可恥的、不被接受的，在這氛圍中，上列方式更容易成功。

[3]資料來源：2008 年美國舞弊查核師協會(ACFE)國家會報。

表 5　職業舞弊的初期偵知統計表



（三）舞弊的影響與案例研究

舞弊不僅會導致社會的財務報告會計訊息失真，危害社會經濟的健康發展，而且對相關的機構和人員也會造成嚴重的經濟後果，近年發生不少企業經理人涉及淘空、舞弊之情事，使得投資人對公司經營高層以及外部查核人員產生嚴重懷疑，重創投資大眾信心，茲列舉羅伯特先生所指出舞弊的影響：1.損失收入；2.危害商譽；3.不良宣傳；4.員工士氣低迷；5.股價驟跌；6.合約減損；7.徒增訴訟成本；8.人力資源成本增加…等。

科克雷爾認為我們可由霸菱銀行（Barings bank）舞弊案[4]的經驗及教訓得知，如及早注意並對下列既存缺失提出質疑當可及時防範舞弊，包括：

1.收入是否確實已列借項；

[4]霸菱銀行(Barings bank)李森(Nick Lesson)事件，年僅 28 歲高級期貨交易員短短 2 年半時間，使具有 232 年歷史的霸菱銀行最後以 1 英磅象徵性價格被荷蘭國際銀行(ING)所收購。

2.現金流入或流出的業務被轉移理由；

3.是否明確記載所有員工的職能組織結構圖；

4.是否確實執行適當的職責分工；

5.辦公室的工作人員是否專業經驗足夠嗎；

6.經由隨機的毒品和酒精測試後，依舊有未檢出惡習的員工被錄用；

7.政策未臻一致，隨著不同的客戶改變；

8.永遠記住，無論從事何種業務，現金是一個關鍵的控制；

9.密碼有否確實控制,未經授權的員工是否能任意改變密碼;

10.有否審慎審查或核閱報告，仔細評斷問題根源；

11.新的總帳帳戶是否有足夠的控制。

羅伯特先生亦認為，各企業若能對上述 11 項做出適當控制，則可避免大部份舞弊案的發生。

（四）舞弊風險的識別—警示訊號(Red Flag)

對於舞弊風險警訊或其徵兆，稽核人員應發揮專業懷疑之精神，實事求是，質疑取得資訊偏差，力求真確。羅伯特先生認為主要的舞弊風險警示訊號（red flag）可從以下三個方面來探討：

1.銷售與收入面（僅列舉部分項目）

（1）與客戶間不尋常關係

（2）缺乏壞帳政策，沒有監測舊債

（3）逾期應收帳款的增加

（4）不合理且未經授權之逾期債務核銷

（5）異常的交易對象及受益人

（6）不切實際的激進的銷售及盈利激勵計畫。

（7）高度複雜的銷售交易

（8）異常的高額代理佣金或折扣

（9）過多的銷貨退回

（10）與銷售記錄未相應的銷售佣金及其他銷售費用

2.採購，負債及支付面（列舉部分項目）

（1）與供應商有不尋常的關係

（2）未具合適的供應商選擇策略（如透明的招標程序）

（3）偏愛特定供應商

（4）供應商的業務地址僅為郵政信箱號碼

（5）超額費用

（6）趁景氣好購置較多設備

（7）異常費用的核銷

3.其他警示訊號（列舉部分項目）

（1）僱員有不誠實行為的歷史

（2）對員工和管理者有財政方面的壓力

（3）個人擔保債務管理不佳

（4）關於員工和管理者的生活方式存在些許謠言

（5）拒絕休假

（6）主管經常承擔下屬的職責

（7）不採取適當的管理行動糾正偏離既定政策行為

（8）頻繁的客戶投訴或告密者匿名指控

（9）常存在重大關係人交易

（10）特定的工作人員處理特定的客戶

(五)舞弊預防計畫應具備之元素

舞弊對於企業帶來的商譽與金錢傷害不容小覷，企業應有相應的策略，以降低舞弊風險或舞弊發生後帶來的損失，企業應建立舞弊預防計畫，舞弊預防計畫雖不提供防止舞弊行為之絕對保證，但它可以有效減輕舞弊的影響。有效的舞弊預防計畫應包括如下圖之元素：

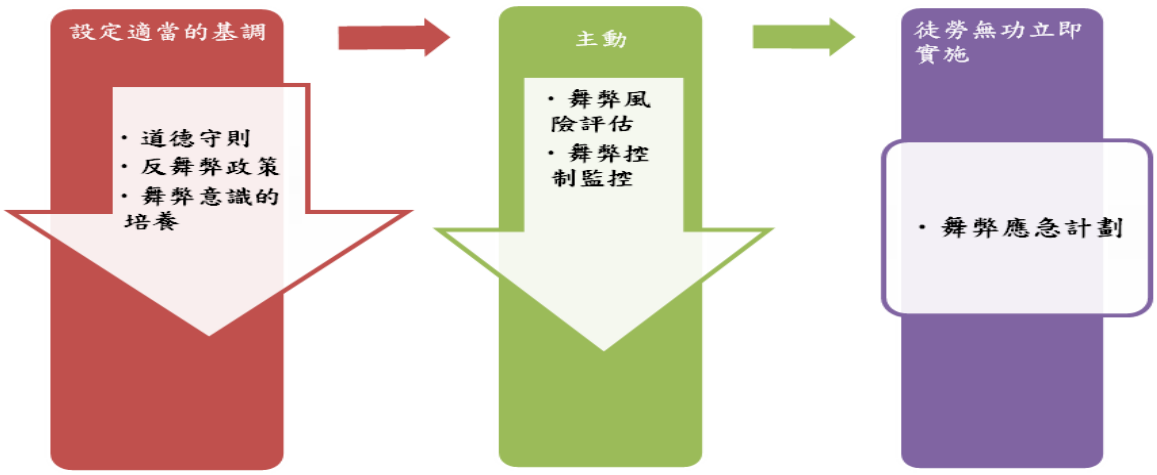


圖 6　舞弊預防計畫元素圖

(六)結語

不管企業或組織，只有透過持續不懈的努力才能保護自身不

受重大舞弊的影響。主動建立有效管理舞弊風險的環境才能有效防患未然，關鍵原則包括：1.應在組織管理結構建立舞弊風險管理程序，確實傳達董事會和高級管理層對於舞弊風險管理期望的書面政策；2.定期進行舞弊暴險評估，確定需要應對的風險或事件；3.建立預防技術，有效避免潛在關鍵舞弊事件及減輕舞弊對組織帶來的影響；4.建立檢測技術，如預防策略失效或風險發生時及時揭露舞弊事件；5.潛在舞弊中應具備報告機制，協調各種調查與糾正策略，確保舞弊能得到適當和及時的解決。

二、確認性服務黑洞－董事會及審計委員會如何發覺公司黑天鵝的存在？

本專題主講人為來自馬來西亞的黃福基（Wee Hock Kee；音譯）先生，黃先生係馬來西亞吉隆坡之企業管治委員會亞太私人有限公司之常務董事，並擔任馬來西亞捷卡有限公司（馬來西亞證券交易所上市公司）之獨立董事，在 MACD（馬來西亞公司主管聯盟）擔任常務職，他曾擔任 2011 年 IIA 國際內部稽核協會年會組織委員會之主席。

（一）黑天鵝與企業舞弊

股神華倫巴菲特（Warren Buffet）曾說：「我們花 20 年所建立之聲譽，往往僅需 5 分鐘的時間就能毀滅它。」納西姆・塔雷

伯（Nassim Taleb）在其暢銷書「黑天鵝效應（The Black Swan）」[5]中，提出所謂的黑天鵝觀念。17 世紀以前的人，在還沒有發現澳洲之前，相信所有天鵝都是白色的，這個想法無懈可擊，因為看起來，這和實證現象完全吻合。直到有人在澳洲發現了黑色的天鵝後，瞬間把人類過去的經驗全部推翻。這個故事顯示，我們從觀察或經驗所學到的東西有嚴重的侷限，以及我們的知識不堪一擊。一個單一觀察、單一事件或單一要素，就能讓千萬次確認看到數百萬隻白天鵝所得到的普遍化推論失效。所謂黑天鵝事件是指一種看似極不可能發生的事件，它具備：

1. 難以預料，出現在平常的期望範圍之外；

2. 它帶來極大的衝擊及嚴重後果；

3. 雖然發生可能性很低，但是一旦發生之後，我們會做出某種解釋，讓該事件成為可解釋及可預測的。

當難以預料且產生嚴重衝擊的事件發生，我們先前所學的知識似乎將難以派上用場。而黑天鵝事件最佳的實例包括 911 的恐怖攻擊、安隆案、全球經濟危機及近年來的企業舞弊醜聞等。而企業舞弊就是發生於組織內部的黑天鵝。

（二）舞弊與風險管理

黑天鵝確實存在於組織內部，從對野鳥的觀察中，可以瞭解企業內部人員從事舞弊交易的心態，黃先生提出一個有趣的研

[5] 完整書名為「黑天鵝效應：如何及早發現最不可能發生但總是發生的事（The Black Swan: The Impact of the Highly Improbable）」。

究。30 年前，有 3 位生物學家針對生長在美國南部及墨西哥一代的黃眼麻雀（yellow-eyed junco）設計了一個實驗，他們捕捉了 7 隻在美國東南部的黃眼麻雀，然後先讓牠們挨餓 1 小時，第一個實驗讓牠們從 2 個碟子中選擇牠們的食物，第一個碟子中總是固定放 2 顆穀粒，另一個碟子則有一半的時間完全沒有東西，一半的時間為 4 顆穀粒。黃眼麻雀只要飛到第一個碟子就可以確定吃到 2 顆穀粒，飛到第二個碟子則不一定。每 30 秒補充一次，實驗結果發現有 76%（二十五分之十九）的情況，麻雀會選擇第一個碟子。之後進行第二個實驗，讓牠們挨餓 4 小時，同樣 2 個碟子，然後每分鐘才補充一次食物，由於選擇第一個碟子，黃眼麻雀將可能面臨無法吃飽甚至無法繁殖的情況，這時候選擇第二個碟子的麻雀變多了。這個實驗告訴了我們，當面臨生存及繁殖的壓力時，麻雀會開始進行賭注，選擇有可能有最多食物的碟子。此實驗可用來解釋財務舞弊者的心態，在面臨壓力時，這些人往往會從風險規避（risk aversion）者變成損失規避（loss aversion）者，且會愈賭愈大。

2011 年針對全球舞弊型態的分析（KPMG Analysis of Global Patterns of Fraud）發現多數舞弊者為男性、介於 36 至 45 歲之間、多半從事財務部門或財務相關職務、在該公司年資超過 10 年，並擔任高階管理職務。原因多半來自於個人的貪婪與壓力所致。

為使企業在難以預料的事件發生時能有所因應，許多企業皆

導入風險管理機制，惟根據近年來許多企業的案例分析，當前之風險管理機制仍可能無法找出黑天鵝的主要原因包括：

1.風險管理並非建立於整體企業基礎之上；

2.風險管理並未隨組織策略進行調整；

3.風險管理人員通常與公司管理人員各自為政；

4.大部分案例中董事會皆不重視公司所面臨的風險。

（三）GRC 與確認性服務

GRC 係治理(Governance)、風險(Risk)與遵循(Compliance) 3 個英文字母首字之縮寫，公司治理、風險管理與法規遵循係近年來受到廣泛討論之重要議題。根據 OCEG（Open Compliance & Ethics Group）之定義，GRC 係由人、流程、及科技所構成的一個系統，使組織能夠：

- 瞭解利害關係人的期望並能按照其重要程度依序處理；
- 設定企業目標並能同時考慮風險及創造價值；
- 將風險組合最佳化並維護價值以完成目標；
- 遵循法令、合約、內部、社會及道德之規範；
- 提供可靠、攸關與即時之資訊予利害關係人；
- 促使系統的績效與效得以衡量。

為了發覺黑天鵝，黃先生提出公司治理的四大支柱包括：董事會（審計委員會）、管理當局（執行長及財務長等）、外部審計及內部稽核；而其中的關鍵要素為：董事會必須包括獨立的資深

董事，管理當局必須正直、外部審計必須獨立且客觀、內部稽核必須有勇氣，詳如下圖。

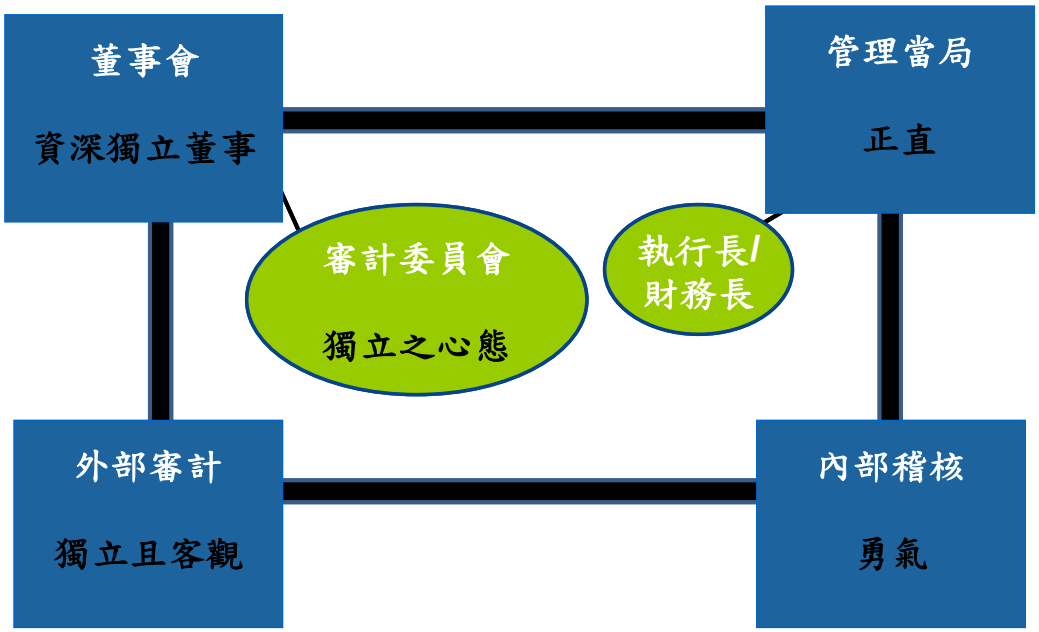


圖 7　公司治理的四大支柱

國際內部稽核協會（IIA）定義了確認性服務提供者的三個層級，該三個層級係依據利害關係人之不同、執行確認性活動的獨立性程度、及確認性服務的強度（robustness）來分類，包括：

1. 向管理當局報告者，或者係隸屬於管理當局的一部分（管理確認性服務），包括執行自我評估控制的個人、品質稽核人員、環境稽核及其他管理指派的稽核人員。

2. 向董事會報告者，包括內部稽核與合規遵循部門。

3. 向外部利害關係人報告者（外部審計確認性服務），傳統上此功能係經由獨立或法定之會計師完成。

組織各階層所面臨之各項風險不盡相同，可由董事會風險確

認架構圖（Board Assurance Framework）看出。該圖由下往上依序分為 4 個層級（L1-L4），最下方之第 1 層級為企業營運功能，主要面臨的風險為一般性及實務風險，第 2 層級為監督功能，包括風險管理、財務、法務、遵循、策略等部門，面臨企業政策之制定與監督等風險，內部稽核則屬於第 3 層級，主要面臨的風險為獨立性，第 4 層級為董事會，詳如下圖。

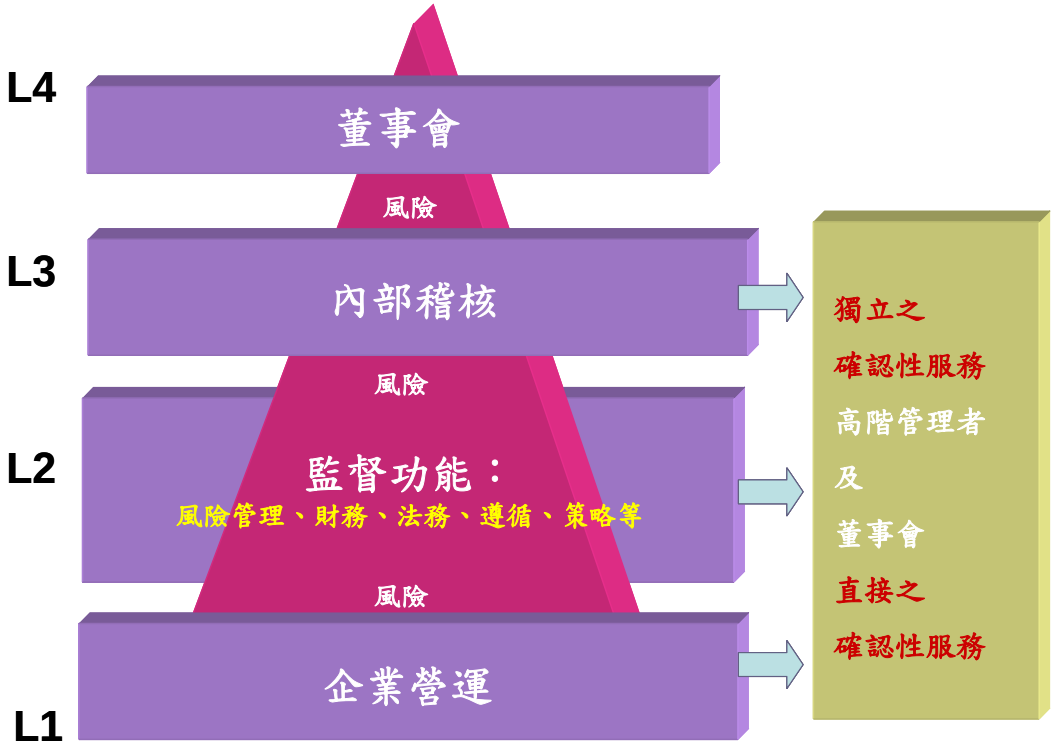


圖 8　董事會風險確認架構圖

黃先生強調為發覺組織內部的黑天鵝，企業必須增加對風險的重視程度，讓所有主管皆瞭解公司所面臨的各項風險，風險胃納中應考量各項因數，建立專責的風險管理委員會等機制，考慮聘用風險專家等。我們必須體認到黑天鵝永遠存在於組織之中。此外，有一些訊息我們必須留意，例如主管人員的離職、外部審

計人員的離任，內部稽核長的離職等，皆有可能是黑天鵝存在的警訊。

三、規劃一個新時代的風險管理制度

本專題主講人魏若妮·普瑞丹諾蒂小姐(Varunee Pridanonda)，是會計師、內部稽核師、國際內控自評師、國際風險管理確認師、舞弊查核師，泰國普華永道會計師事務所(PWC)合夥人，提供治理、風險、遵循與內部稽核服務。

她認為現今複雜的風險形勢，內部稽核部門每天面對不同的風險，不能只作年度稽核計畫，更要協助公司評估風險。首先，從風險複雜性來說，現有傳統式風險管理方法在這個多變的環境，已無法提供足夠保障，它只能管理一部分風險。第 2，速度和廣度，風險的變化速度非常快，可能每天面對的不一樣，這個風險有可能影響到下個風險，讓風險管理更加複雜。第 3，一個公司通常花多少財力和時間來做風險管理？這 3 點告訴我們要正確作風險管理是很複雜的過程，面對每天多變的不同風險，現有制度可能不夠有效達到目的和結果，所以重點要修正現有制度讓它更有效率。

(一) 企業風險管理之外的 3 個步驟

大多數公司有一個風險管理大綱，單單只有這個大綱是不夠

的，需要的是 3 個重點：

1.形塑公司文化：如何評估公司是否已有嵌入式的風險管理，如果這個制度已成為公司的一個傳統，應該每日例行會議上都要討論到風險管理作業，要協助公司把風險管理的執行，變成例行作業一部分。

2.建立風險胃納：要對公司做深度瞭解，以決定公司承受風險程度，並對高階主管提出計畫做統合管理，避免各部門不曉得公司風險胃納，不論事情風險大小都得詢問高級主管，這樣會讓公司沒有競爭力和效率。

3.風險和策略整合：每個部門也許有不同的想法，但有一個共識是很重要的，內部稽核單位應協助公司超越風險。公司董事會要負風險管理最終責任，應確保高階管理人員負管理所有風險之責，不論是財務上、制度上或執行上，內部稽核單位要確定公司主管們清楚瞭解各項策略所有可能風險，以及董事們在例行會議討論風險管理作業。

（二）風險管理之連續性

把風險評估制度變成公司文化一部分之後，要進行下一步，就是對風險之應變能力。以前有傳統式風險管理方法，新的方法叫做「抗風險能力」，就是不論遭遇什麼困難，都有馬上回歸原點，能夠捲土重來之能力。下圖有 3 個步驟，最左邊的是「生存」，過去幾年遇到嚴重天災，你的公司早有防禦準備，而沒有受到嚴重

虧損還能繼續營業運作，這就是所謂生存。傳統式風險管理也許可以幫助渡過生存這一部分，但這樣還不夠，一個企業還要能發光發亮，必須進行到「適應」的步驟，要能夠適時調整政策以面對多變的市場環境和風險，最終目的能夠有「轉變」的能力，成功例子是 APPLE，它成功地電腦硬體轉換成人人生活上不可或缺的伴侶，他的定位不再只是一個電腦公司，從這些例子學習在多變的市場，不但作調整還更進一步地將企業轉變成更成功的商業形態。

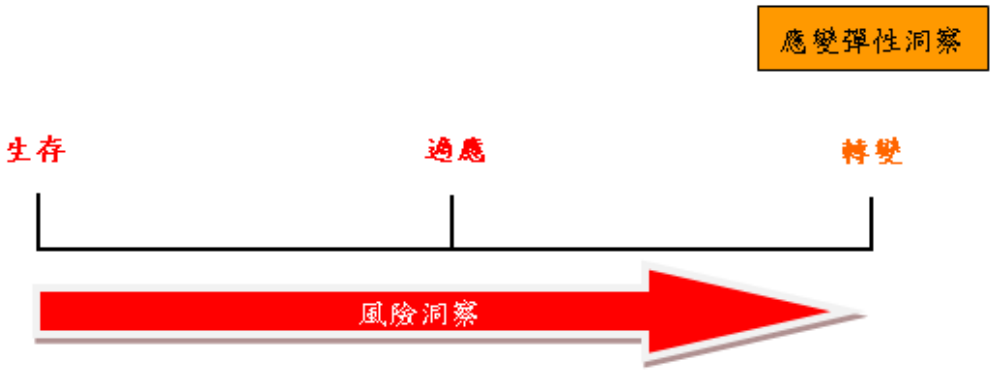


圖 9　風險應變彈性連續體圖

要能成功地從「生存」到「適應」，到最後的「轉變」，必須遵守 4 個步驟（4A）：

1. **整合**（Alignment）：策略和風險管理結合，兩者必須相輔相成，還有公司領導方式與獎勵間之結合、在市場上和其他企業公司合作等，所以必須做好溝通，在風險管理上不僅要跟合作伙伴溝通清楚，更要跟董事會說明清楚。

2. **意識**(Awareness)：企業該清楚自己在風險管理上的定位，

風險接受度高低，並讓公司員工知道，在政策上才能清楚一致。公司也要意識到任何外在的危機或機會，包含天災人禍，市場上的危機或新商機，以及顧客和員工的認知，要確定價值觀成功地嵌入公司變成公司文化一部分。

3.能力（Ability）：從經驗中學習和應變，將專業多元化，應用在不同的風險管理策略中。

4.靈活性（Agility）：任何事情簡單化比複雜化好，公司應嵌入繼續進步的文化，以及一致性和透明化，對於察覺到的風險，勇於討論，而非視而不見。

下圖可供評估自己的公司是在風險管理連貫性的哪一個階段，共有 4 個階段，圖中間的線代表一個公司從注重過程的形態進入到重視文化的形態；圖下方注重過程的公司，在所謂第 1 階段，此時企業通常還是用傳統風險管理法，這類公司未定期討論風險管理，只在有問題發生時匆忙緊急處理，而且只有能力處理一部分問題，無法全方位面對，它的風險管理報告資料不全，沒辦法真的使用。第 2 階段形態的公司，有比較好的風險管理報告，可以執行，但也無法作為建立政策使用。第 3 階段公司開始將風險管理觀念和策略灌輸到公司文化裡，變成公司的一部分，前 2 階段的公司只能夠看到已發生的風險，無法預測可能發生的風險，第 3 階段開始，公司開始考慮到未來會發生的事，有比較強的抗風險能力，他們會從經驗中學習，參考過去的風險來預測未

來的危機，能夠使用他們報告的資訊幫助管理階層作政策之輔助。第 4 階段形態的公司，人人會將風險管理當作辦理每個策略前都應討論的事項，這樣的意念已經深深嵌入公司文化裡。以上所述，對於內部稽核部門的意義，在於風險管理綱要需要修正，要從傳統式慢慢走出來，一直進步到第 4 階段，最終目標是將公司轉變成可以從危機和風險裡走出來的企業。

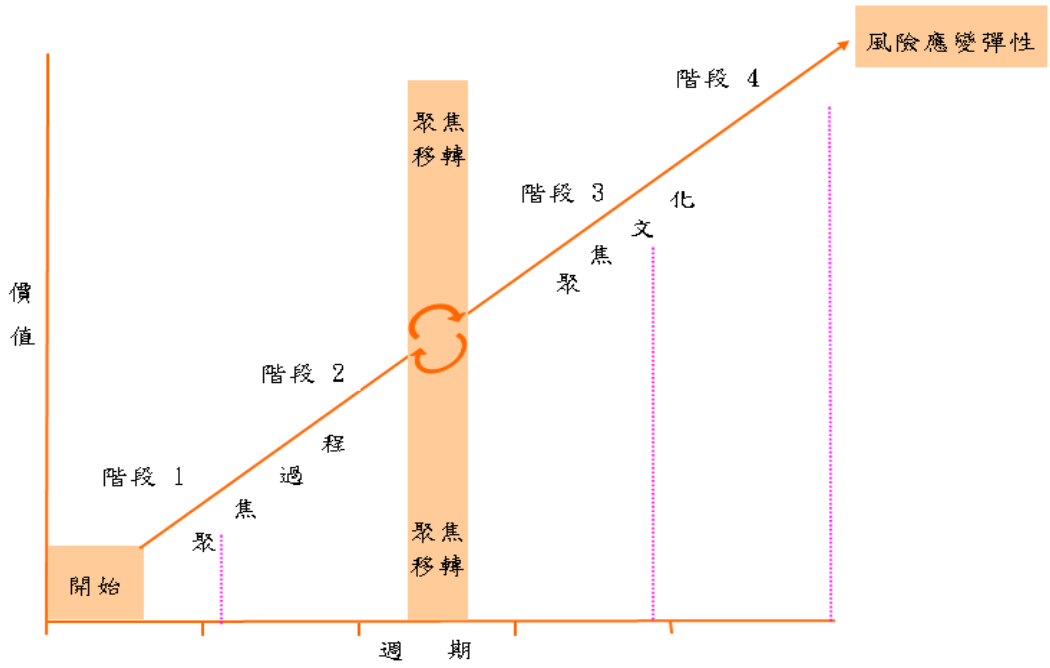


圖 10　風險管理階段圖

（三）業務環境與內部稽核必須連結

不同時候有不同風險產生，股東們對公司的期待也會隨時改變，內部稽核的功課就是要一直進步，從基層一直往上前進，下圖顯示基層部分基本工作，包括：1. 詳細瞭解所有重要的風險和難題；2. 確保公司利益達到股東的期待；3. 培養稽核部門人才的模式必須跟公司利益一致，包含是否需要增加人員、需要哪方面

的專才；4. 管理股東的期望，好好經營股東的關係；5. 維持服務至上的公司文化和態度，瞭解顧客需求及如何滿足其需求；6. 提供符合成本效益的服務，與其每年請更多人來做一樣的工作，內部稽核部門更要協助公司有效率工作；7. 有效運用科技，達到更大的工作效益；8. 促進品質進步和創新。

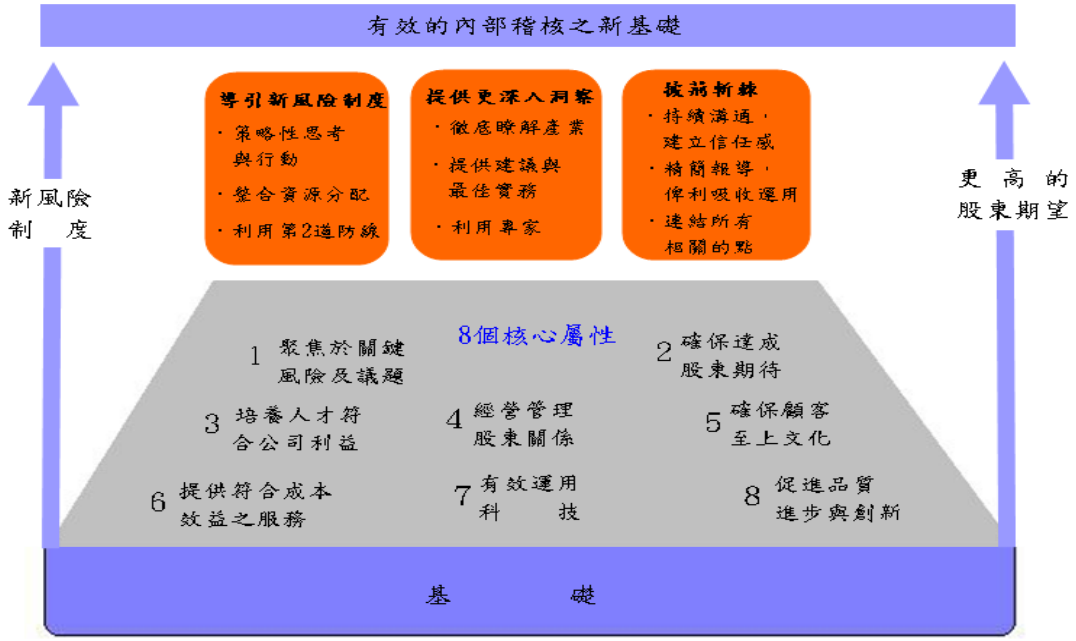


圖 11　內部稽核工作效能圖

這個圖最上方的 3 點就是內部稽核部門需要做到的，也進一步達到股東的期望。第 1 點，導引新風險制度，必須有能力及智慧來作策略性的思考與判斷，除了判斷可能的風險外，也要知道如何分配資源提供公司協助，並利用第 2 防線，公司的第 1 防線是管理階層，第 2 道防線是風險管理人員，內部稽核部門是第 3 防線，要好好跟風險管理部門合作，以增進整體工作效率。第 2 點，提供更深入的洞察，要徹底地瞭解自己公司的產業及運作方

式，內部稽核部門應該跟管理階層爭取參加固定會議。第 3 點，披荊斬棘，持續不斷地溝通以建立信任感，每個部門彼此間要互相合作，只有靠不斷溝通才能達到最高效率；幫忙把所有東西連結起來，協助所有部門，包括對外對內所有相關人士和部門，把每個步驟作連接，讓大家都有一個清楚的畫面，不要忘了要常常和股東們溝通並瞭解他們的期望是什麼。

四、資訊科技風險與控制之最新發展

本專題主講人任家明先生（Frank Yam），是香港科信集團（Focus Strategic Group）總裁，經常在國際內部稽核協會、國際電腦稽核協會各組織機構演說，也是中國南京審計學院兼任教授和香港內部稽核協會理事。他認為資訊科技（Intellectual Technology, IT）變化太快了，身為一個內部稽核人員，必須跟上變化的腳步，並分享當前 IT 環境趨勢與風險，及內部稽核人員面臨之挑戰，建議採用相關策略。

（一）網路犯罪年代新興的資訊科技風險與趨勢

當今 IT 發達的網路時代，風險是什麼，就是有關資訊之保密性、完整性、可用性、聲譽和公眾的信賴、系統生產率。通常審計委員會憂慮 IT 的 5 個主要風險，包含：1. 遵循與控制：能否依賴資訊的完整性；2. 企業永續性：能否讓企業永續經營；3. 安全風險：能否趕走壞人；4. 外包風險：能否依賴合夥人及賣方；5.

計畫交付與複雜性：由資訊科技所獲得的是否物有所值，是否極大化 IT 投資之價值。

我們如果丟了手機，遲早會發現它不見，但電腦資料被偷，可能永遠不會發現，這就是科技世界不同的地方。通常網路安全課程第 1 課是 CIA，代表的是資訊科技之保密性、完整性和可用性（Confidentiality, Integrity, Availability），但公司董事會、審計主管和高階管理人員往往只在意資訊正確性，關於資訊安全呢？如果你是在會計部門，你知道大部分資料都是下載到 Excel 來，慢慢修正變成可用報表，這個過程可能出現人為誤差實在太大，這就是科技環境風險；上面幾點措辭雖然不同，意思大致相同，倒數第 2 點風險外包，是有關雲端科技，下面會予探討。至於第 5 點計畫交付和複雜性，20 年前的公司大概只有 40%的高科技作業計畫可以成功完成，另外 60%不易成功，意思是可能沒有達到預算，所需時間太長或是整體品質不良。高失敗率原因之一是沒有好用的軟體，現在大部分軟體公司已修正應用程式，讓客戶易於使用，成功率進步到 65～70%，但仍然不夠，稽核人員須注意 IT 投資價值是否極大化；另在經濟壽命屆期報廢電腦，很多公司以為把檔案清除就安全，實則不然，最好的方法是把硬碟拿掉。

（二）稽核人員必須知道的挑戰

關於 IT 新風險圖象，包含：1.網路安全、2.行動應用程式及設施與 e 化商務、3.社群網絡、4.災難復原計畫、5.巨量資訊、6.雲端運算、7.持續產生差距的合作關係。摘述如次：

1.網路安全：常聽到有人攻入某家公司電腦，他們採用一種

社會工程的方法，例如使用他人姓名、照片與職位名稱，變成另一個人，開一個 Gmail 帳戶，接下來寄發信件，大家會接受及相信，Facebook 也是一樣道理，假扮他人很簡單，只要幾分鐘時間，就變成另一個人。

2.行動應用程式及設施與 e 化商務：現在幾乎每個人都有手機，我們有太多密碼要記，因為記不住，只好把密碼存在手機裡，網路安全問題越來越多。

3.社群網絡：Z 世代年輕人，做事方法不一樣，必須瞭解他們的行為和心態，才能進一步適當規範，簡單講，Z 世代值得注意的是：(1) 資訊超載、(2) 是否相信資訊、(3) 影響力、(4) 身份危機。基本上就是有太多資訊，且不知資訊是否正確，連資訊來源可能都不能信任；很多人在網路世界小有名氣，也有一定影響力，利用社群網路放消息，短短幾分鐘就可以傳到幾千人，不要小看網路力量，要觀察誰是這些有影響力的人，多花心思管理，另上面已談過冒用他人之身份危機。

4.災難復原計畫：大部分人有 Yahoo、Gmail 或 Hotmail 帳戶，但多數人不會做備份，以為 Yahoo、Google 這種大公司不會倒，5 年前如果問雷曼兄弟控股公司會不會倒，你會說不可能，今天都知道正確答案了，所以如果裡面有重要東西，不僅要備份，也要確定有很好的災難復原計畫。

5.巨量資訊：過去公司存放的資訊多是書面的，現在打電話交易，很多以錄音存檔處理，公司存有大量資訊數據，要有一套系統方法整理資訊，做好備份工作，以便日後能隨時調閱，而且

一定要做「恢復測試」，亦即隨便選個文件，刪除後將之恢復，然後點進去確認所有的內容和資料都還是完整的。

6. 雲端運算：包含服務與契約風險、科技風險，前者譬如鎖定供應商，就不能說換就換，另服務協議書之撰擬，重點包含權責歸屬、購買之軟體有哪些應用程式，關於第三者使用權，因為所有資訊都存在雲端，誰可以調閱這些資料，你可能只跟 1 個供應商簽協議書，但這個供應商可能有好幾個供應商，這些供應商可能又有自己的外包商，其中有許多層，也就是許多人可以隨時調閱我們的資料庫，這裡面藏有危機。另科技風險，例如整合及寬頻，部分國家頻寬較差，如果從雲端資料庫調閱資料，速度比較慢；又如編碼和解碼的管理，如果選擇編碼，就須考慮額外的費用，而且必須提供供應商編碼用之密碼，如此他們也會有你的密碼，所以要考慮是否要這樣做；另有關雲端運算之測試與監控，提供者可能不允許你進行雲端資料庫滲透測試稽核，而要透過供應商，也要慎重考慮。雲端科技越來越普遍，稽核人員第 1 步要「風險評估」，決定公司之風險承受能力，然後有 3 種選擇：(1) 不做雲端資料庫、(2) 做獨立的雲端資料庫、(3) 做公開的雲端資料庫；每一個選擇有它的風險。

7. 持續產生差距之合作關係：科技一直進步，稽核人員的責任改變，企業不僅希望協助評估風險，提出適當建議，更要求協助執行，但資訊部門預算不會跟著科技進步速度而增加，如果要提供高品質資料庫，就不能慢慢作系統改進，要採取大幅度的機器或軟體更新。由於企業對增進經營能力之要求很高，但資訊科

技預算下滑，及因系統複雜性，導致生產力及交付能力下滑，乃持續產生差距之合作關係。

（三）對稽核人員建議之策略

稽核人員需要多少控制權？要確定控制權有效率地用在對的地方而不是越多越好，在策略方面有幾個重點：

做正確的事，勝過以正確方法做事：大家常忙著遵循公司程序，那只是在對的時間點做事，而不是做對的事，稽核人員必須瞭解企業環境，對症下藥，提出正確解決方案。

注重人力資源：內部控制是由人來完成，要持續吸引並保有人才，予以培訓及提供晉升機會，教導商業道德也是很重要的一環。IT 稽核面臨之挑戰，應該僱用稽核人員訓練他們 IT 知識，還是僱用 IT 專家訓練他們為稽核師？僱用全時 IT 稽核人員或外包、或是成立 1 個獨立部門？這是複雜的問題，要視公司財力而定，建議至少要培訓內部稽核人員瞭解 IT 可能有的問題，這樣跟 IT 部門合作也會更順利。

把業務環境與 IT 做連結：基本上，讓 IT 部門與使用者兩方面互相瞭解彼此作業內容，以業務語言來溝通，協助每個人瞭解 IT 風險；IT 部門要注意報表使用者是誰，可以有好幾份不同形態的同一份報告，針對不同部門需求作調整，將科技專業用語改成一般用語，讓報表更簡單易懂。

（四）稽核人員的新工具

現今的稽核人員可以利用之工具有：

1. 內控自評(Control Self Assessment, CSA)：組織為實現

目標、控制風險而對內部控制系統的有效性和恰當性實施自我評估的方法；為增進對風險控管與自行檢查的能力，內部稽核協會有提供這方面的認證服務(CCSA)。

2.電腦輔助查核工具與技術(Computer Assisted Auditing Tools and Techniques，CAATs)：多數人會想到通用套裝稽核軟體（ACL/IDEA），但還有很多建議用的軟體，像是 CaseWare、TeamMate、Securac、EnCase、AutoAudit…等等。

表 6　電腦輔助查核工具與技術類型表

類　　型	常 見 軟 體 名 稱
通用稽核軟體	ACL / IDEA
工作底稿軟體	CaseWare
風險評估軟體	Securac
鑑識軟體	EnCase, FTK, X-Ways
混合型軟體	TeamMate, AutoAudit
其他	—

資料來源：演講者提供，本文整理繪表。

3.IT 保證架構：有個工具可謂稽核師聖經，即 COBIT（資訊系統及相關技術控制目標，Control Objectives for Information & related Technology, COBIT[6]），美國資訊系統稽核與控制協會(Information Systems Audit and Control Association, ISACA)於 2012 年 4 月才剛發布全新之第 5 版。保證架構有很多個，最重要的 2 點是：1.大部分的公司都會使用很多個不同的 IT 架構，所

[6] COBIT，國際上公認 IT 管理與控制標準，最早發布於 1996 年，是一系列關於 IT 管理框架的集合，為管理者、稽核人員和用戶提供一套通用的 IT 控制目標及控制慣例，以便決定系統的安全性，及透過 IT 監管以保護資訊資產。

以要去瞭解各個架構間如何運作；2.可以利用 COBIT 做為總架構，因為 COBIT 會討論到所有可能碰到的問題。

（五）結語

稽核人員如何提供加值服務？首先必須瞭解公司面臨之風險和整個商業環境，建立有效率之 IT 管理方法，擔任 IT 稽核人員要多學習，去上一些課程，才能把工作做得更好，提供加值服務。最後提供幾個想法：1.把內部稽核人員培訓為 IT 稽核師，以確保所有稽核師 10 年後還是有工作；2.解決方案必須與企業策略一致，如果不能瞭解企業策略，便無法生存；如果只是一昧地遵守公司程序就可能沒有對症下藥，記得要做對的事；3.注重人才和公司文化，確保公司有好的工作文化是很重要的。

五、內部稽核：提升組織治理、風險與遵循之能力

本專題主講人為來自泰國的 Suphamit Techamontrikul 博士與 Weerapong Krisadawat 先生。Techamontrikul 博士係泰國曼谷德勤（Deloitte Touche Tohmatsu Jaiyos Co., Ltd.）審計與諮詢服務部之合夥人，對各產業的私人企業與上市公司提供顧問及審計服務已有 21 年之經驗。目前擔任會計準則制定委員會之委員，亦擔任泰國 IIA 之副主席。Krisadawat 先生為曼谷德勤企業風險服務部之合夥人，曾在泰國外商銀行擔任過高階主管，他

的專長在公司治理、風險管理、內部稽核、能源與資源，銀行與金融機構及公部門等領域。

（一）泰國的 GRC

GRC 係公司治理、風險管理與法規遵循，近年來受到廣泛討論。根據亞洲公司治理協會（Asian Corporate Governance Association）的調查，2012 年亞洲各國公司治理之分數如下表所示。

表 7　亞洲各國公司治理分數：2007 至 2012 年

	2007	2010	2012	分數增減（2010-2012）
新加坡	65	67	69	+2
香港	67	65	66	+1
泰國	47	55	58	+3
日本	52	57	55	-2
馬來西亞	49	52	55	+3
臺灣	54	55	53	-2
印度	56	48	51	+3
韓國	49	45	49	+4
中國	45	49	45	-4
菲律賓	41	37	41	+4
印尼	37	40	37	-3

泰國從 2007 年至 2012 年，公司治理分數雖呈現進步之趨勢，但是亞洲公司治理協會指出，貪污的情況仍是泰國主要待解決之課題。泰國證券交易所與市場投資機構（Market for Alternative

Investment，MAI）針對泰國上市公司有關公司治理實務進行全面的調查，並將調查結果呈現於 GRC 國家報告之中，該報告內容主要包括：

1. 泰國公司治理實務與上市公司之改善情形。

2. 公司治理績效表現。

3. 泰國上市公司公司治理的優勢與劣勢。

4. 分析主要公司治理實務與公司治理績效的關係。

5. 分析公司治理績效與企業價值。

在泰國發生經濟危機後，泰國政府更加重視公營事業的經營效能。泰國政府於 2002 年 10 月 3 日成立公營事業政策管理辦公室（State Enterprise Policy Office），監督公營事業的績效。目前泰國共有 55 家公營事業，包括能源、通訊、運輸、農業、自然資源、社會科技、銀行等產業。

（二）GRC 能力模型

GRC 能力模型(GRC Capability Model)主要可參考 OCEG(Open Compliance & Ethics Group）的紅皮書（Red Book)。OCEG 係一非營利組織，主要協助企業透過企業文化，並整合治理、風險管理及遵循程序，達到「原則績效」(Principled Performance)。OCEG 提供與 GRC 相關之指引與準則、實務社群(線上空間、工具、資源及論壇等）及評估標準與標竿等。

原則績效係一經註冊的專有名詞，定義為：在考量不確定性

的運作下，完善的達到可靠的目標。亦即治理、管理與確認等三個功能，除了達到傳統績效外，更應滿足風險管理與法規之遵循，如此所達成的績效始可稱為原則績效。

下圖旨在表達，目前企業的公司治理、風險管理、法規遵循等各項方案通常過於分散，且往往疊床架屋、無一制性，因此必須將此三項功能予以整合，將分散管理轉化為企業整體管理，化被動為主動，採用系統觀點，以增加企業附加價值，導入 GRC 能力模型，如此才能夠化危機為轉機。

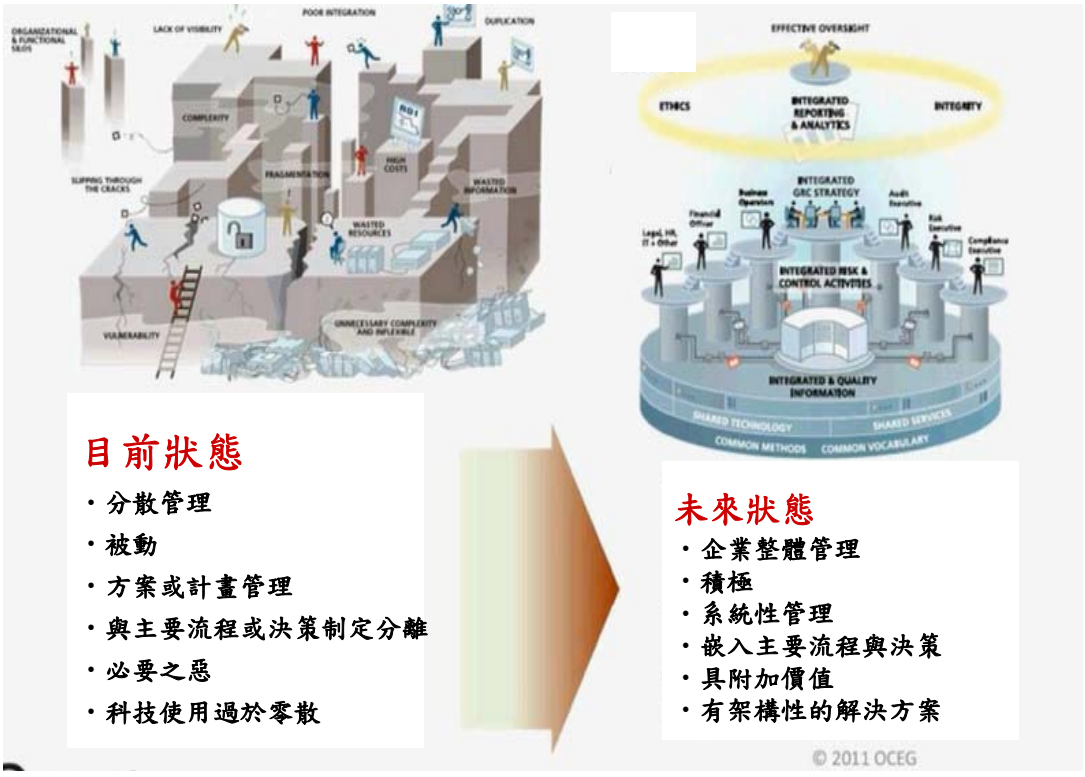


圖 12　實施 GRC 模型之目前與未來狀態

（三）內部稽核與 GRC 能力模型之整合

OCEG 之紅皮書將 GRC 能力模型分為 8 個要素，包括脈絡（Context）、組織（Organize）、衡量（Measure）、評估（Assess）、回應（Respond）、前瞻（Proact）、偵測（Detect）。其中確認（Assurance）系在衡量要素下的第 4 個子要素，在 GRC 能力模型下之定義為：提供管理當局及董事會 GRC 系統係可靠的、有效果的、有效率的且具回應力的，包括以下原則：

1.管理當局及董事會需對 GRC 制度之有效性，獲得獨立且合理之確信。

2.管理當局及董事會應對 GRC 制度之有效性，獲得獨立且合理之確信，以偵測及預防與組織決策不一制的行為。

3.此項確認性服務可由內部稽核、外部審計或評估人員進行。

4.不同時點與不同目的之情況下，所需之確認性服務程度亦可能有所不同。

5.評估者的獨立性及能力有所改變，則需要增加確信的程度，並須藉由獨立與客觀之程序來覆核，以進一步加強該程度。

企業亦須定期評估 GRC 管理活動，包括：1.GRC 管理是否有效設計？2.GRC 管理是否有效執行？組織應監督管理當局的控制活動是否持續的執行，以達到效能。持續的監督應建立在組織日常的營運活動中，並且即時的執行。評估時須考量以下要素：

1.對企業文化的影響；

2.範圍及策略；

3.結構與資源；

4.管理政策與訓練；

5. 內部執行流程；

6. 持續改善之成果。

（四）關鍵成功因素

內部稽核之關鍵成功因素可分為：

1. 個人的專業與職責，包括設計與執行評估時，應具備適當的技術與資格。

2. 高階管理者能從董事會監督的角度，負起適當之注意義務，並瞭解或參與內部稽核的各項業務及流程。

3. 建立有效的文件管理程序及適當的文件保留政策。

傳統內部稽核的角色為提供確認性服務、評估並給予建議、協助公司內部控制及進行顧問諮詢服務等，而現今內部稽核則必須基於利害關係人與管理者的期望，並因應環境變化而持續不斷地演變。有效的內部稽核應幫助組織完成公司目標，並提升組織在公司治理、風險管理與法規遵循的能力。

六、企業策略稽核

本專題主講人招信江先生（Pont Chiu），是香港交易及結算所有限公司資深副總裁兼內部稽核部門主管。他一直是香港內部稽核協會活躍成員，曾在 2008 年至 2011 年間擔任該協會主席，目前是監事；在此之前，他擔任香港金融管理局內部稽核主管，及高盛國際有限公司內部稽核部門副主管。他認為策略是企業成功的關

鍵因素之一，如果採取不適當策略，可能導致災難，即便制訂一個正確的經營策略，如果執行方式錯誤也會導致策略失敗，因此，內部稽核人員如何確信管理階層已採取適當經營策略並適當執行，可否發揮更加積極作用，他從下列面向來探討。

（一）什麼是策略風險？

策略風險就是由於錯誤或不當策略導致之損失。產生策略風險原因，包含：1.錯誤假設；2.缺乏資訊，例如市場趨勢、經濟、新技術發展、競爭者活動；3.在規劃企業策略時採用了不正確的資料或資訊做分析；4.管理階層的薪酬與投資報酬有直接連結關係，導致高風險等。很多案例說明組織失敗，並非沒有好的策略，而是因為執行方式錯誤。策略風險之負面影響，例如：2012 年摩根大通公司（JP Morgan）投資策略導致虧損近 58 億美元，該公司執行長承認這是一個非常糟的計畫策略，糟糕的審查、執行及監控；2007 年美國匯豐融資公司（HSBC Finance Corporation）收購家居用品國際公司（Household International），造成 172 億美元呆帳，這是該公司史上最糟糕之決策；時代華納企業（Time Warner）2000 年併購美國線上公司（America Online），9 年後解併，市場資本額由 3,500 億美元下跌至 657 億美元。還有英國發生出名的胡佛公司（Hoover）行銷策略失敗案例，胡佛原本是英國最有名的吸塵器品牌，1992 年英國經濟衰退，執行長決定採用行銷策略消除庫存，宣布購買超過 100 英鎊產品，就會得到歐洲

任一城市來回機票各1張，但是接著有無法拿到機票的生氣顧客，電視新聞拿它做文章，客戶組成抗議團體，鬧上法院，法院判決公司必須全額賠償，最後它被一家電器廠商收購，整個經營團隊全部失業。這些案例，顯然的，是因錯誤的假設，缺乏資訊或使用不精確資訊，或是有利益衝突，管理階層僅想推銷產品完成目標，蒙蔽自己並試圖操弄他人，這就是為什麼需要內部稽核。

（二）策略稽核之目標

為什麼策略會錯誤，須先瞭解策略是如何形成的。首先，在策略規劃過程，基本上，詳細規劃、分析、評估、審批、執行，是一個企業策略規劃典型的處理流程。但並非每個企業都有明確的流程，因為多數策略是由大人物決定，公司裡鮮少有人敢挑戰，更多時候，是沒有被告知全部過程，直到事情出錯。因此，在策略規劃過程，評估管理階層是否採行適當的策略規劃流程，其流程是否經過定義，及是否採用適當的分析方法與資料及程序，以識別、分析和管理策略相關之影響與風險，及時提供管理的風險評估結果與內部控制意見，就是策略稽核之目標。

在策略執行過程，需要考慮許多因素，人員、財務、專業能力、客戶、資訊、溝通等；貫徹執行，聽來容易，但人們總是忽略某些必須放入流程的考量，公司面臨一個大策略或計畫轉變，必須檢討是否有執行能力。為減輕策略之風險，要注意內部控制是否有效實施，或與業務流程整合，已確定之策略是否可由公司

資源支持，並清楚地傳達給相關部門，對於敏感之策略，驗證是否施予保密安排。

（三）如何執行策略稽核

多數重大的商業想法，是由公司所有者或主要決策者做出的，他有了概念與願景，與經營團隊共同構思策略，得出一個基本的策略藍圖，再詳細分析規劃，設定策略目標，確認風險，以風險評估結果，確認控制活動，辨認什麼是需要做的或可能出錯的，記錄下來，再根據形勢變化檢討及改變策略，據以執行及控管，以確保達成。如下圖所示。

圖 13　策略稽核流程

謹就策略稽核執行步驟，摘要說明如下：

1.瞭解公司在當前市場或產業中的位置

包含內部評估、外部評估，如果有多個策略發展架構，必須有更多正式步驟，必須懂法律、規範、環境、運籌、財務，蒐集資料並做假設，這些評估須要被小心規劃並且嚴格檢視，此項風險管理程序有助於整個程序之記錄。在內部和外部評估之後，稽核人員應該瞭解公司在市場及產業間之地位，並提供管理階層風險評估結果之建議意見。

（1）內部評估：以 SWOT 工具做分析，分析公司之優勢、弱點、機會和威脅。包含公司之技能、產品和服務、顧客、供應商；可支援策略的組織文化與結構、業務流程；從市場、經濟和財務觀點，分析策略可行性和健全性；辨識策略相關風險，其影響和可能性；對所有部門來說，策略是否透明清楚；是否有充足時間與資源等。

（2）外部評估：是一種量化分析，分析瞭解經營環境，與產業及競爭者之比較。任何安全的企業策略，必須有數字基礎，瞭解整個環境，市場有多大、客戶在哪、產業及市場成長速度、每年銷售成長百分比、競爭者數量、競爭者的策略及優勢，事關風險，須請管理階層在紙上寫下，做個徹底的風險分析。當然，數據不是全部，還有很多的評斷，但是評斷是由因素去支持的，策略也是，須評估管理階層主要假設與經營計畫是否合理。

2.評估與策略相關之風險與控制

- 策略風險之評估

內部稽核人員要檢討管理階層策略風險評估過程與結果，包含：(1)有無明確流程，以規劃、核可、執行和審查策略計畫；(2)既定的程序是否定期檢討；(3)是否適當地遵循程序；(4)有無遺漏任何關鍵風險，或不適當的控制；(5)關鍵假設和預測是否合理；(6)假設和預測可能隨時間變更，對於需要長時間執行之策略（例如 3 年），管理階層是否具有更新與追蹤關鍵假設和預測

的程序；(7) 是否確認適當的內部控制；(8) 是否實施有效的內部控制；(9) 是否有確認管理控制系統及模型；(10) 關鍵風險在整個執行過程有無予以追蹤；(11) 關鍵流程、資訊科技和財務系統能否處理公司之必要改變。

- 策略風險管理控制

好的策略規劃，必須適當被定義，必須有成本控制的時間、適當的治理架構、品質控管等，策略發展計畫實施過程，從上到下，每一個關鍵部門及關鍵領域都必須有一個風險登記冊，並維護風險登記冊，它真的協助辨識出許多的風險，另組織須有適當溝通管道讓內部稽核人員表達意見，發生任何錯誤，內部稽核可以追蹤並跟團隊分享，正確界定和登記主要的風險因素。內部稽核人員可以協助的策略風險管理控制關鍵因素，包含：(1) 範圍、時間計畫表、成本規劃；(2) 風險記錄；(3) 人力資源規劃；(4) 角色和責任分配；(5) 品質規劃與控制；(6) 溝通管理；(7) 公司財務系統或控制是否可支援該類型業務或交易。

3. 發展策略稽核工作計畫進行稽核

除了上述風險評估及管理控制外，策略稽核工作計畫也要考慮下列事項：(1) 高階管理人員的支持與積極治理；(2) 公司達成策略目標的成本和效益；(3) 公司內部參與和溝通，及經營流程改變的管理；(4) 計畫表和流程、品質管制計畫或程序；(5) 追蹤經驗教訓。例如，一個金融機構要興建資訊大樓，建構資訊

中心是個高度專業的建築，如何執行這個專案？必須做很多不同分析，正式的策略發展應遵循許多相同模式與流程，並定期檢討，確實分析與控管風險，將風險記錄在紙上。在規劃階段必須考慮：（1）建築、資料中心和專案管理方面，是否有足夠的內部專業技術；(2) 專案治理架構；(3) 成本估算和業務預測的假設；(4) 需求是否清楚確認；(5) 專案和成本控制；(6) 品質保證計畫。在執行階段要考慮：(1) 專案管理控制；(2) 管理階層監控之關鍵風險；(3) 執行關鍵控制；(4) 人員安全程式；(5) 事故處理和上報。在專案後，必須記取經驗教訓。

（四）策略稽核面臨之挑戰

內部稽核人員必須有效率的，在對的時間用對的方式提供正確建議。策略稽核之挑戰是：1. 策略稽核對大多數公司而言是個新觀念，內部稽核人員需要董事會的全力支援；2. 缺乏執行策略稽核之知識與稽核資源；3. 每個策略可能有許多活動與目標，內部稽核人員難以參與所有活動；4. 有時難以充分瞭解市場、趨勢和競爭者之策略及活動；5. 並非所有資料都是現成可用的，而且選擇用來支持策略所使用之資料是主觀的；6. 太多主觀因素，許多策略行動沒有明確的對錯答案。組織內越大的計畫越困難，內部稽核人員沒有資源、經驗、系統去控管那樣一個系統，不知它的重點在哪，如何去解決它，具有挑戰性，因此無法直接介入一個很複雜的策略專案，由小型策略做起比較容易，一定有我們可

以貢獻之空間，再循序漸進，建立系統式架構方法，做回顧性分析，將經驗傳承。

七、資訊科技稽核人員如何能跟上最新科技趨勢

本專題主講人威莉蓬・突優帕屯女士（Vilaiporn Taweelappontong），是資訊安全系統專家、資訊安全管理系統稽核人員，泰國普華永道會計事務所（PWC）合夥人，帶領資訊科技（Information Technology, 簡稱 IT）顧問作業，對於系統安全和技術擁有豐富經驗，協助許多大型跨國公司設計資訊安全體系架構與策略，及評估實施自動化安全操作遵循與風險管理技術。她與大家分享擔任 IT 稽核人員面臨之挑戰，及瞭解科技趨勢與跟上時代的秘訣。

科技隨時在變，稽核人員必須發展基本的科技知識，掌握最新趨勢和技術，與時俱進，才能做出詳細審核。隨著科技在組織監控扮演更重要角色，組織在管理新且具特定風險的新興技術時，會轉向稽核顧問請求協助，稽核人員如何針對最新趨勢 IT 進行稽核，將面臨挑戰。這些擴大的角色、技能和專業，解決方法是，要有大格局的科技觀點，關注最新最熱門的議題，有很多管道提供最新商業和科技趨勢，稽核人員要讓自己保持在時代尖端，隨時得知最新技術及趨勢，才能提供公司更好的科技建議。

（一）追蹤重要科技網站

前幾名重要科技網站，結合商業和科技，改善人類的生活。第 1 名是 WIRED 科技新聞網站，有許多新科技新聞報導，關於科技如何影響商業、文化，有時也影響政治，記者和科技作家都很推薦的網站。第 2 個是 CNN 網站，它是第 1 個 24 小時提供新聞的電視台，裡面也有科技類，例如你會看到歐巴馬如何贏得選舉，民主黨有很多資料庫，他們僱用數據分析顧問，把眾多資料庫結合成 1 個資料庫，發展出程式，進行詳細的投票行為分析。第 3 個是 ZDNet，剛創立時關注一般科技，後來專注於企業和財金科技，例如行動運算技術、電子商務還有科技資源等等。

（二）追蹤重要科技趨勢預測

另一個要推薦 IT 稽核人員閱讀的領域是科技趨勢，通常出版社、研究公司會推出下一年度 IT 新趨勢。世界知名 IT 研究機構嘉特納（Gartner）公司列出 2012 年 10 大策略性科技，並分成 3 個領域：科技改善人類生活、科技改善商業、科技改善 IT 經驗（詳表 1）。第 1 項是媒體平板，平板在 2012 年十分熱門；第 2 項行動應用程式及介面，我們可以看到手機有很大商機，不只是電子商務（e-commerce），更是行動商務（m-commerce）；第 3 項情境與社群使用者經驗，是關於使用社群媒體創造使用者經驗，社群媒體不只 Facebook，它是一種組織策略，可以透過社群媒體推出新產品，改善顧客經驗，改善內部合作，像是資誠（PWC）也有自己的社群媒體計畫，全球 170 個辦公處就算用 e-mail 也不方便溝

通，所以發展自己的社群媒體策略，設計創造自己的工具版本，結合 Facebook、twitter 和維基百科的特徵，當需要任何協助，只要把問題發佈上去，就可以傳送到網絡上每個人，許多公司發展社群媒體策略，它運用在許多領域，不只是內部，也可以用在顧客上，稽核人員未來可能也要稽核社群媒體運用情形。

另一個是美國有線電視公司(CNN)推出的 2012 年 10 大熱門科技趨勢，其中結合了觸控裝置、社群互動、近距離無線通訊(NFC)、行動電視、聲控、第二螢幕體驗等（詳表 2)。富比士公司（Forbes）也提出 10 大科技趨勢，其中它提出很有趣的科技運用「事物遊戲化（The Gamification of Everything)」，使用它來改變人類行為，例如，當你要搭地鐵時，會選擇走樓梯還是坐電梯？一般人不會選擇走樓梯，但是如果在樓梯上裝置電子設備，爬樓梯時發出音樂，變得好玩，大家就會選擇爬樓梯，這是一個教育技術，藉著趣味性改變人們行為，遊戲化(Gamification)可以運用在組織或大眾身上、用在任何地方或事情。

表 8　嘉特納公司（Gartner）提出 2012 年 10 大科技趨勢

人類經驗	1. 平板媒體與未來產品（Media tablets and beyond）
	2. 行動為主的應用程式與介面（Mobile-centric applications and interfaces）
	3. 情境與社群使用經驗（Contextual and social user experience）
商業經驗	4. 物聯網（Internet of things）
	5. 應用程式商店與市集（App stores and marketplaces）
	6. 次世代分析技術（Next-generation analytics）
	7. 巨量資料（Big data）
資訊科技部門經驗	8. 記憶體內運算（In-memory computing）
	9. 超低耗能伺服器（Extreme low-energy servers）
	10. 雲端運算（Cloud computing）

太多新趨勢了，要小心科技超載，這裡提供一些指導方針，有 4 個問題是 IT 稽核人員需要注意的：

1. 它對你的公司影響是什麼；

2. 必需瞭解安全和控制；

3. 公司可以從這項趨勢獲得什麼好處；

4. 如果公司要運用這項趨勢，IT 稽核人員如何協助達成。

表 9　美國有線電視公司（CNN）提出 2012 年 10 大科技趨勢

1.觸控電腦（Touch computing）
2.社群互動（Social gestures）
3.近場通訊及移動支付（NFC and mobile payments）[7]
4.iPad 之外（Beyond the iPad）
5.電視無所不在（TV Everywhere）
6.聲音控制（Voice control）
7.體感手勢（Spatial gestures）
8.第二螢幕體驗（Second-screen experiences）
9.可彎曲螢幕（Flexible screens）
10.第 5 代超文字標記語言（HTML5，Hyper Text Markup Language）[8]

（三）跟上科技潮流的秘訣

1.閱讀：不斷閱讀，使自己保持在時代潮流尖端，善加利用新聞彙集軟體（News Aggregator），它是工具，也是網站，整合來自眾多網站的標題，從標題中找有興趣的再深入閱讀。

2.加入社群網站：twitter 或 facebook 裡面有很多連結，可以連結到新聞，就像新聞彙集軟體，可以獲得最新消息。

3.參加研討會：有很多資訊安全、IT 方面的研討會或線上研討會，通常是免費的，提供一些關鍵議題。

4.與科技人保持聯繫：與科技人及 IT 稽核人員保持良好關

[7] NFC(Near Field Communication)，可以讓手機當成信用卡，只要在商店的信用卡機器上感應，消費金額就可自動由帳戶中扣除。

[8] HTML，超文字標記語言 ，利用純文字進行幕後版排，網頁的原始碼呈現方式之一，HTML 檔案是由一些標記標籤(Markup tags)組成，標記標籤用來告訴瀏覽器如何顯示網頁，HTML 檔案的副檔名為.htm 或.html。

係，建立人際網路，當遭遇到問題時，可以得到很多有用想法和資訊。

5.建構訂閱軟體（Establish RSS Feeds）:「訂閱軟體」（RSS Feeds） 是一個建立新聞的程式，可以幫忙建立標題，下載到行動裝置 iPhone、iPad、筆電或電腦使用，獲得最新趨勢和科技資訊。

6.參與內部稽核或電腦稽核協會,與其他 IT 稽核人員建立網絡：跟同儕緊密連結，進行交流，是跟上科技潮流的方法。

7.加入科技郵件群組（Participate in selected technology mailing Groups）：推薦 2 個方式加入科技郵件群組，1 個是 Computerworld，它會摘要標題然後寄 e-mail 到你的信箱，打開信箱就能閱讀，另 1 個是 iapp，也是跟上潮流好方法。

（四）內部稽核承擔新興科技挑戰

這裡提供 1 份資誠（PWC）對新興科技的報告，它不是寫新興科技的內容，而是它對內部稽核的威脅，談論雲端運算、網路安全、社群媒體、電腦使用人口和智慧型裝置，針對各該領域提出容易出錯的地方，及其對 IT 稽核人員的威脅與機會。

1.雲端運算（Cloud Computing）：雲端運算，使用電腦資源提供服務，資訊彷彿在雲端，可能在不同國家的某處，可能在不同建築物裡，它是很好的概念，很多公司這麼做，但有一些出問題的例子，索尼遊戲平台（Sony PlayStation Network ）由於駭

客入侵，造成當機及 7 千 7 百萬用戶個資遭竊；亞馬遜公司（Amazon）雲端服務當機事件，客戶網站被迫中斷達 36 小時，過度依賴雲端，可能對企業造成損害。身為 IT 稽核人員，要注意查核關鍵領域：(1) 合約協議，查核合約、提供者、領域、執行程序、安全控制、公司簽名、提供者簽名；(2) 存取控制；(3) 是否有證明及第三者審查；(4) 遵循要求；(5) 可用性、可靠性和彈性；(6) 備份和還原；(7) 可攜性。

2. 網路安全 (Cyber Security)：關於公司的網路安全，在查核過程，你可以問一些基本安全問題：有哪些資訊資產、哪些風險、哪些網路、哪些系統、哪些資料？

3. 社群媒體 (Social Media)：社群媒體是一種傾聽的技術，傾聽人們對公司的意見，是一個熱門風潮，要注意公司使用何種社群媒體策略架構、方針及控制，由於任何人都可以張貼消息在社群媒體上，有人張貼錯誤消息，傳播速度很快，影響公司形象，是否增加風險，是否有資料損失等。

4. 電腦使用人口 (Computer Usage/Demographics)：這是關於人口資料摘要的新興科技，就像上述歐巴馬的例子，他有很好的資料庫團隊，發展人口選戰策略。有許多策略能幫助你解讀人口資料，上面提到索尼遊戲平台駭客入侵的例子，身為 IT 稽核人員，審查人口資料庫系統或程序時，要查目前及未來的風險。

5. 智慧型裝置 (Smart Devices/Technology)：這可以是任何

裝置，像是 iPhone, iPad, Blackberry，你無法阻止員工連上網路，有一個著名例子，蘋果公司（Apple）員工將 iPhone 原型機外洩。公司是否允許使用智慧型裝置，是否有控制的政策，是否允許連上網路下載資訊，有些公司允許員工使用 iPhone 和 iPad，但只能看不能下載資訊，如果下載並儲存，公司機密就可能外洩，因此 IT 稽核人員須查核智慧型裝置策略、程序、安全控制。

伍、研討心得及建議意見

綜上，本次研討會議題安排，包含人力資源評估、舞弊偵防、公司治理、風險管理、法規遵循、內部稽核技能等，除治理、風險與遵循外，並安排 4 場關於資訊科技系列研討會，顯示資訊科技對稽核工作具深遠影響。謹就與會研習結果提出心得及建議意見如下：

一、審計人員應對環境風險保持高度警覺，並堅持獨立性，以回應民眾之期待

本屆年會同步會議之其中一項重要主題為 GRC，GRC 係治理（Governance）、風險（Risk）與遵循（Compliance），主要希望企業應將公司治理、風險管理及法規遵循予以整合，以發揮最大綜效。在專題演講中，安永亦提出最新調查的全球十大風險報告，顯見風險對稽核人員的重要；而同步會議中，泰國曼谷德勤（Deloitte Touche Tohmatsu Jaiyos Co., Ltd.）之合夥人亦指出，未來稽核人員將演變為「滿足利害關係人期望」的角色。國際最高審計機關組織（INTOSAI）第 20 屆會員代表大會提出之報告，要求最高審計機關在不違反獨立性的情況下，應扮演主動評估環境風險及辨認利害關係人期望的角色，因此評估風險與滿足利害關係人期待，係未來公、私部門審計之重點。

根據安侯國際財務顧問股份有限公司（KPMG）美國鑑識會計團隊 2009 年度舞弊調查問卷報告（KPMG US 2009 Fraud Survey

Report）顯示，約有 65%的回覆者認為舞弊及不當行為係目前所處產業的重大風險之一。所有組織都受舞弊風險影響，嚴重的舞弊會導致整個組織的瓦解、大規模投資損失、鉅額的法律費用、公司重要人物被監禁，以及對資本市場的信心的潰散。IIA、AICPA 及美國舞弊查核師協會（Association of Certified Fraud Examiner，ACFE）對舞弊的定義皆為：「有意或故意欺騙他人，而導致善意的一方遭受損失或意圖不軌之人獲得利益」。根據 2010 年 ACFE 全球舞弊研究報告統計，舞弊詐欺事件造成的損失佔企業組織年營收 5%，對照 2009 年世界產值估計，總損失超過 2 兆 9 千億美元，平均每件職場舞弊所造成的損失在 16 萬美元，四分之一的舞弊事件損失金額超過 100 萬美元，而舞弊事件平均持續約 18 個月才被發現。其犯罪型態、平均每案損失及次數比例如下表。

表 10　舞弊犯罪型態、平均每案損失及比例統計表

犯罪型態	平均每案損失（美元）	比例
侵占	13.5 萬	90%
貪瀆	25 萬	30%
財務報表舞弊	400 萬	5%

2007 年企業舞弊監督系統報告(Oversight System Report on Corporate Fraud）指出舞弊發生的原因，以「有進行舞弊的壓力」（81%）為最高，其次為「獲得個人利益」(72%）等，可見壓力係造成企業舞弊主要原因之一。因此企業必須有必要去發覺公司內

部黑天鵝的存在，並設法找出方法，以紓解人員舞弊之壓力，預防及偵測舞弊之發生。

最近，聯合晚報（2012 年 11 月 28 日）刊載前「消防署長黃季敏被控任內涉及採購案收受回扣」；自由時報（2012 年 11 月 30 日）刊載「災修工程涉收回扣，南投縣長李朝卿聲押」；聯合新聞網（2012 年 12 月 4 日）刊載「消防署特種搜救隊訓練補給科長、台中市消防局災害搶救科員，涉嫌辦理採購案綁標、圖利特定廠商」…等，面對與日俱增的政府高官貪污舞弊行為，重挫政府威信，臺灣已於 100 年 4 月 20 日公布制定「法務部廉政署組織法」，並於 100 年 7 月 20 日成立法務部廉政署，但為何仍有為數不少之政府高官鋌而走險，漠視道德輿論，浪費公共資源和資金，令公眾對政府失去信任。政府如何偵防，以確實防貪、反貪、肅貪，並遏止舞弊行為，此係法務部職掌；審計機關之願景為「實踐優質審計服務，創造最大審計價值」、「提升政府施政績效，促進政府廉能政治」，身為審計人員，在促進政府廉能政治上，亦有責任促其導向正軌，且不法舞弊行為多源於內部控制欠佳，審計人員如能積極主動查核，對及時遏止舞弊亦能發揮相當成效並減少損失對道德風險保持高度警覺。

根據研究發現，超過 85%的舞弊源自於內部人員，超過 55%的舞弊犯罪者多為管理階層，顯見環境的管理基調決定舞弊案發生的可能性，所以可先評估：

1.業務單位行為規範、道德政策及舞弊政策的管理基調；

2.是否重視道德舉發熱線提供的警訊；

3.員工雇用與升遷有無明確指引及做好背景調查；

4.檢舉人的身份保全措施是否適當；

5.對檢舉案的重視程度，是否有確實偵查並及時補救系統性措施。

有關審計機關之獨立性，在 2011 年第 66 屆聯合國大會決議文(A/RES/66/209)中已明確宣示，該決議要求世界各國應致力強化其審計機關之職能，以促進公共行政之效率、課責、效能及透明度。該決議除強調提升審計機關之職能外，並鼓勵各會員國參採國際最高審計機關組織(INTOSAI)所頒布之利瑪宣言(Lima Declaration)及墨西哥宣言(Mexico Declaration)，以維繫國家最高審計機關之獨立性。另在審計人員方面，我國審計準則公報第 1 號指出，審計人員執行查核工作時，應保持嚴謹公正之態度及超然獨立之精神並盡專業上應有之注意。因此，為善盡專業上應有之注意，審計人員平時蒐集輿論媒體等與受查單位相關資訊，評估舞弊風險及控制活動之設計有效性，協助受查單位導入風險管理：

1.評估舞弊風險：經由評核業務單位重大施政計畫重點所在，透過績效審計或財務報表審計等方式，協助受查單位確認舞弊風險癥結，防止不實財務報導、資產挪用、不當收入及支出或

公務人員不當財務行為。

2.評估業務單位的控制活動：業務單位，建立有效的內部控制制度，包含確認業務人員已瞭解內部控制流程及預防業務主管逾越控制程序應採取的行動。

3.評估舞弊有關控制之設計和運作有效性，運用平時蒐集的輿論媒體等與受查單位相關資訊導入風險管理，配合當下時空背景，協助業務單位隨時修正稽核計畫和程式，確保舞弊查核計畫隨時有效。

安侯全球舞弊型態分析報告（KPMG Analysis of Global Patterns of Fraud）指出利用內部控制的漏洞進行舞弊者由 2007 年的 49%上升至 2011 年的 74%，可見公司要能夠持續的維持內控機制的正常運作，時時填補漏洞。審計機關亦應敦促行政機關，不僅要建立起適當的內部控制及風險管理機制，更應隨時對各部門之內控缺失及可能漏洞進行評估，以降低舞弊之情形。

美國會計師協會查核準則第 99 號公報:財務報表查核舞弊之考量(SAS No. 99: Consideration of Fraud in a Financial Statement Audit)，提醒審計人員舞弊發生的三大要件：誘因與壓力（Incentive）、機會（Opportunity）、不當行為之合理化（Rationalization）。因此內部稽核人員及外部審計人員執行審計稽核業務時，應落實專業懷疑態度，秉持追根究底的精神及公正的評估審計證據，才能預防、偵測舞弊之發生。根據 Kroll

2011/2012 全球舞弊查核報告，企業舞弊案朝向高複雜度方向發展，企業普遍感覺威脅提高。國際內部稽核協會（IIA）前理事長丹尼・拜倫（Dennis Beran）提出，稽核人員應該成為風險與內部控制專家。因此，內部稽核及外部審計人員除可藉由參加 CFE 考試，獲得舞弊查核專業肯定及認證資格外，執行審計稽核業務時能瞭解預防性、偵測性及回應性等各項舞弊風險管理策略，對舞弊及道德風險保持高度警覺，並能從不同角度分析資料，善用資料分析及資訊科技技術，來進行舞弊偵測與預防，有效提升稽核效率及效果，且能積極地與利害關係人溝通、建立良好關係，最重要的要能夠不忘記秉持客觀與獨立，以提升審計及稽核之價值。

二、審計機關應加強跨領域專業合作，俾利舞弊查核作業之進行

舞弊查核及財務鑑識除應具備會計、審計之專業知識外，尚需俱備法律、心理學、社會學、犯罪學、證據法則、資訊系統和電腦鑑識、其他鑑識科學領域等相關專業及技術，才能有效還原舞弊事件原貌，提高偵防率，並及時挖掘各機關存在的貪污舞弊案。大多數審計人員係以核對文件與數字等方式查看財務面存在及適當性，較之舞弊查核人員除確認文件的存在外，對鑑識文件係真實抑或偽造性等專業能力仍有所不足，故審計人員除應自我充實相關專業知識外，須精進審計證據的蒐集方法與技術，加強違失案件之查核能力，並培養觀察、分析、溝通、整合等能力外，

建議走出自我框架，多汲取鑑識審計先進偵查技能，善用資訊科技及資料分析技術，或延請專家學者、檢調人員傳授偵測舞弊的新知技術，加強跨領域專業合作與聯繫，共謀舉發不法。

審計機關設置舉發熱線，須同步考量人力運用以發揮查核績效：目前審計機關對檢舉熱線已訂有「審計機關人民陳情案件處理作業要點」之規範，大部分檢舉人都相當信任審計機關的公正獨立而妥予運用期舉發不法，惟仍不乏有檢舉人未掌握確實證據、或圖個人私利、或報仇怨…等濫用檢舉信箱。審計機關人力一向吃緊，在既定工作之餘仍須查證檢舉案，復依上開規定須於30 日內辦結情形下，有時難免有分身乏術之嘆，當然遇有舉發事項明確、牽涉層級高且影響金額龐大，為求時效則須立即簽辦或需增加人力、時間，惟為使審計人力及時間運用更為精準，建議落實審計機關人民陳情案件處理作業要點第 17 條規定「審計機關受理人民陳情案件有下列情形之一者，得不予處理：(一) 無具體內容，且未具真實姓名或聯絡方式者。」對於匿名案件且檢舉內容不具體者，不予處理。另檢舉內容尚稱具體惟未具真實姓名及聯絡方式者且影響財務效益金額未達標準（例如 10 萬元)，建請不須強制規定須於 30 日內辦復，輔以審計人員列管提高受查單位控制風險值並列入下期財務收支抽查併抽查重點辦理等程序辦理即可，如此或可稍事減輕審計人員工作負擔及壓力，期能有效運用有限人力以提升實質查核效益。

此外，應落實檢舉人身份保防作業。舞弊案件犯罪行為人對於從事違法行為存有高度警戒心，為保護自己極盡能事，使得線索發掘不易，而檢舉人對各受理機關身分保密作業信任程度低，為使生命安全不受威脅，擇選匿名方式舉發不法，而匿名舉發意味著調查人員無法與陳情人聯絡以獲取更多事證，同時也會提升調查行動的困難度。所以審計機關為能確實舉發不法，除了落實執行「政風機構協助機關落實檢舉(陳情)人身分保密實施要項」、「審計機關受理檢舉（陳情）案件專責人員處理檢舉（陳情）人身查證作業程序」等身份保防規定，確保檢舉人身份受到保護外，建請在審計部全球資訊網廉政園地內宣導上揭身份保防規定及承諾不會揭露身分以安檢舉人之心，俾能使其勇於揭示不法，並鼓勵檢舉人留下真實姓名及聯絡方式，以利後續查證、舉證聯繫事宜。在香港，廉政專員公署 ICAC（The Independent Commission Against Corruption）在其資訊網頁刊載並鼓勵民眾舉報貪污舞弊行為，且該地區訂頒之「證人保護條例」已有事實證明確能鼓舞公眾的信心，讓證人勇於挺身而出舉報公務人員貪污舞弊行為。

三、審核意見須表達合宜，適時溝通確保意見能正確傳達予利害關係人，並持續追蹤辦理情形

本屆年會全球 IIA 主席塔林先生在專題演講中強調審計人員溝通能力的重要性，並建議審計人員應熟析各項新的溝通工具，包括 iPad、智慧型手機、Facebook、Youtube 等溝通媒介或網站，

以精確表達意見予利害關係人，其中也包括審計報告的發布。

隨著科技技術演進，人與人之間的溝通工具不再是傳統的實體書信、報表紙張等，資訊傳播科技改變社會事務的管理模式，資訊傳播科技將資訊數位化後，資訊之蒐集、分享與研析應用更形便利，同時提供我們掌握更多更精確的資訊以評估現在、規劃未來，進而供我們應用在審計事務上，迅速提出專業性的建議意見供被審核機關參採。惟近來在審核意見傳達方面，仍有無法詳實傳達到被審核機關內心並令其真心接受情形，如依審計部審計業務研究委員會先前據「審計機關策略管理與績效評估推動試辦計畫」辦理被審核機關滿意度調查，其中「審計機關意見是持平客觀」、「審計機關之審計意見是可行的或具參考價值」、「審計人員在查核過程能向機關學校適時溝通重要審核意見（績效性意見）」、「審計人員能說明執行詢問、觀察、盤點、函證其技術之目的及必要性」等項之滿意度經評核有不足情形，顯示審計人員提出的審核意見或有未盡合宜之處，身為審計機關一員，應檢討改進，如審計意見立基應有充分證據以資佐證、用詞遣字須嚴謹避免主觀論斷、持平提出審核意見、以同理心立場傾聽被審核機關執行現況及窒礙難行之處、多角度研析法令面與執行面落差並加強溝通，以顧客服務精神提出有價值、富創新的策略計畫與策略地圖供被審核機關參考，期共同努力改善現在、策進未來，以創造能感動人心的審計機關形象，發揮、實踐優質審計服務，創造

最大審計價值。

四、建構政府審計人力資本彈性化策略，加強人才留任管理

人力資本管理與績效管理是現代公務人力管理最主要課題，人力資本管理也是組織管理之基礎，攸關組織策略能否順暢推動，包含人力進用策略、人力運用以至人力留用等多元化管理範疇，不僅須反應當前工作需要，也須籌劃因應未來挑戰。

本次年會之專題演講，安永合夥人張先生，提出了安永 2011 年全球企業十大風險報告，其中「人才管理」與 2010 年之報告相較，風險排名上升 1 名，且幾乎所有行業都將人力資源風險列為前四名，企業普遍認為應該加強對人才的重視，並研訂人才管理的流程，且預測 2013 年該風險會再度上升，顯見人才管理的重要性與日俱增。現今審計機關人力資本核心管理工作在確保能吸引、延攬、留任具有適當技能與經驗之人才，尤其面對複雜詭譎的社會經濟環境等外在挑戰與機關本身業務革新，必須針對整體人力資本進行衡量分析，充分掌握人力狀況，即時調整因應。近年來審計機關為配合國際審計新趨勢，積極推動辦理各種新興業務，例如：審計機關策略管理與績效評估機制、審計工作財務效益統計等，雖獲致豐碩成果，但不少審計人員因業務壓力或內部誘因不足，離開審計工作崗位，實宜盡速妥為因應處理。謹分述如次：

（一）前瞻規劃審計人力制度，建構審計機關人力彈性化策略

80 年代以來，各國為提升施政績效，以效率化為目標，追求新治理模式，「彈性導向」成為管理核心議題之一，歐美各國蓬勃發展的彈性人力觀念與做法，藉由提高人力數量的調度力、工作流程及薪資結構設計等做法，以多樣化的方式管理人力資本。美國於 2004 年在「聯邦審計署人力資源改革法」(GAO Human Capital Reform Act of 2004) 中，授權審計長得自行設計該署組織架構及運作模式，提供審計人員待遇調整及各項福利措施等誘因，以招募各界專才進入審計機關，期能提升審計服務品質；此項重大變革內容，包含：薪資彈性、離退與進用彈性、獎勵績優輪調人員、休假更加彈性、公私部門人力交流等。對於優秀及認真工作之審計人員，不吝給予加薪及升遷。該署員工待遇之給付以績效為導向，確實依照員工努力程度予以績效考核，對於自願離退人員有更高核定權，並賦予該署更多權限聘請部分工時之兼職人員，以應尖峰工作量之需求；對於調派全國各地人員之福利有更大之補償彈性，得應實際需要核給搬遷費，另對某些特定職位之員工提供休假保障，即使服務年資未滿 3 年仍可獲得較多之年休假日。他山之石可以攻錯，我政府審計部門原已人少事繁，加諸近年大力推動辦理績效性審計，仍須兼顧合法性審計工作，彈性化人力管理實屬必要，美國聯邦審計署人事制度變革，可供我國借鏡，建構審計機關人力彈性化策略，以避免留不住好的人才。

（二）因應內外環境變化，加強人才延攬與留任管理

國際最高審計機關組織（INTOSAI）於公部門審計人員倫理規範與審計準則中，建議不同審計工作需要不同學術背景的審計人員，個別審計人員不需具備履行各項審計職掌之全方位能力，審計工作應指派有勝任能力之工作團隊辦理。我審計機關職司監督各級政府財務收支，任務艱鉅，加以現今加強辦理績效審計，惟未有專業之績效審計工作團隊，審計人員多被訓練要求成為全方位之查核人員，然績效審計與財務報表審計或遵循審計工作，有極大之差異，且皆需投入許多時間及精力辦理。審計人員在面對各式各樣受查部門及專業、合法性與績效性審計工作要求之下，為了辨識風險所在而加以查核，有賴事前充份準備，惟因工作龐雜，往往準備時間不足，且審計工作常需依賴受查機關提供資料，在機關資料提供不足或延遲提供情形下，審計人員同時面臨查核報告到期、工作太雜無法專心撰寫報告、長官期許報告內容創新及具深度與良好品質、審計績效評比等情境，身在此種須有多元能力及時間緊迫與機關內外雙重壓力下，造成審計人員知識焦慮、競爭焦慮，身體或心理健康產生問題，導致人員流動率頗高。除了上述審計工作本身之問題外，近年來審計機關女性人員大幅增加且占審計人員之多數，一般來說，女性仍被賦予照顧家庭與小孩之大部分責任，女性員工的管理在人力資本管理領域，其角色異於往昔。為扮演好稱職之審計人員，審計人員常兢兢業業戮力從公，留在辦公室加班或將工作帶回家撰寫查核報告，難能兼

顧家庭與小孩需求，長久下來，造成家人之不諒解，以致審計人員對機關的承諾降低，無法堅持對審計工作之熱忱；兼以外部環境變化，近 2 年來，五都及桃園升格準直轄市，人員擴增，大幅釋放會計人力職缺，審計機關同仁紛紛轉而求去，加速審計人才流失。為利同仁兼顧多重身份角色，更須強調彈性管理，瞭解員工遭遇之困難，因應外界變化，追求個人與業績之穩定成長。

人才的留任，必須給予誘因，誘因不外乎是升等、加薪、獎金、休假、福利等。建議首先可執行的是鼓勵休假，讓休假彈性化，放寬休假規定，例如同仁若於非上班之期間仍執行公務者，人事單位因盡可能放寬並協助審計同仁核予加班補休。而現行審計人員常因出差抽查及趕辦查核報告或總決算審核報告，時間迫促，無法依個人及家庭需求時間請假，或因人力不足，未准或延後同仁申請補休或留職時間等，應盡量避免。又現行留職停薪要件為公務員服兵役、受拘役、調派至國外或其他機關任職、全時進修或重大傷病、養育 3 足歲以下子女、直系血親尊親屬老邁或重大傷病須侍奉等[9]，以上均係公務員因外在因素須予留職停薪，至於公務員個人需求或工作壓力等因素擬留職停薪者，現行法令似未有此機制。審計機關實有必要彈性處理，俾予審計人員喘息與調適之機會，可參考大學教授每 7 年可以休假 1 年（或 3 年半休半年）之規定，給予各審計單位 1 年有 1 或 2 個優秀人員選擇

[9] 公務人員留職停薪辦法第 4 條規定參照。

數個月或 1 年中長期休假方式，訂定彈性休假辦法、放寬休假規定，以減少離職率，並吸引延攬新血。此外，也應檢討考績制度，因為考績影響獎金、薪資甚至是升等，若要避免人才外流，則考績制度及其評比程序有必要確實重新檢討。

五、辨識關鍵或潛在風險，加強辦理施政策略及計畫之審計，俾對民眾生活產生正面影響

COSO（Committee of Sponsoring Organizations of Treadway Commission）於 2004 年發表企業風險管理架構，此與其 1992 年發表內部控制整合架構，主要差異在於增加策略與目標設定項目，顯示內控發展趨勢強調對於「策略」之稽核[10]。另國際最高審計機關組織（INTOSAI）於 2012 年 9 月之最高審計機關組織國際準則 ISSAI X(草案)指出，最高審計機關之價值與意義係來自於對民眾生活產生正面影響，包括：加強政府與公部門之課責、廉正及透明度；對民眾及利害關係人展現持續之攸關性；透過以身作則成為典範機關等 3 大目標，詳如下圖。審計機關審核對象係行政部門，透過對行政部門執行各項策略及計畫提供建言，促使行政部門改善，進而對民眾生活產生正面影響。

[10] 策略是組織為達成一項或多項目標，所採取之決策與行動；策略稽核，係稽核團隊以專業技能，針對組織重大策略之制定與執行成效，提供獨立與客觀之評估方法，以協助組織高層確認關鍵風險、降低決策失誤及執行成果不彰的成本。

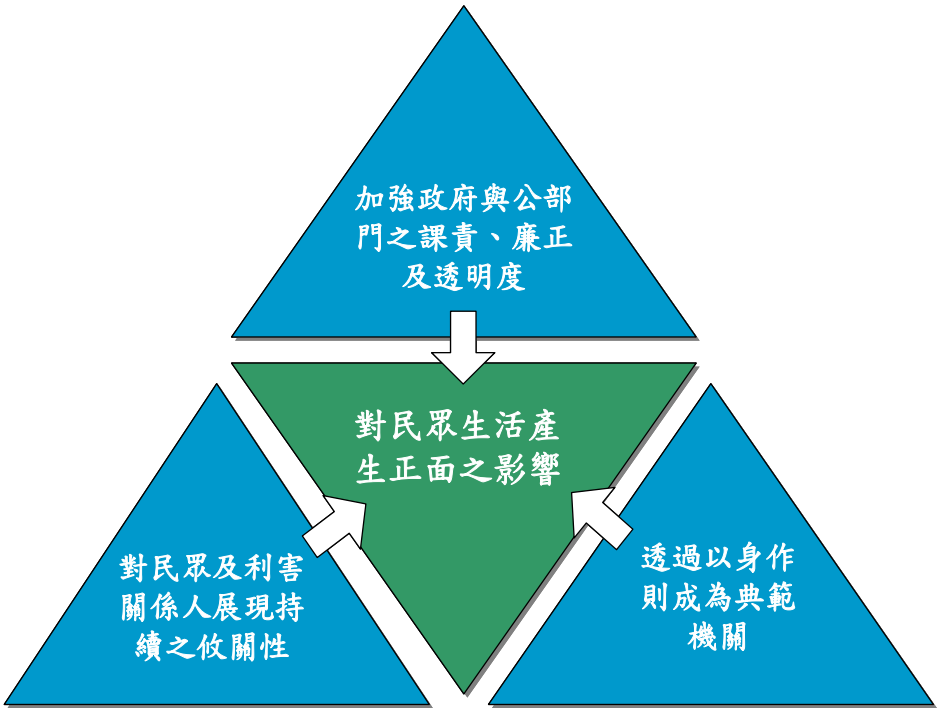


圖 14　最高審計機關價值與意義架構圖

俗云：「錯誤政策，比貪污還可怕」，政府施政績效良窳之關鍵，不全然是執政者操守或法規機制的問題，而在於有沒有正確之策略主軸，有沒有做「對的事」或有價值的事，及有無執行力，固然採取不適當策略，可能導致災難，即便制訂一個正確的策略，如果執行方式錯誤也會導致失敗。審計機關站在服務行政機關的立場，要協助機關避免錯誤或不當策略導致之損失，俾對民眾生活產生正面影響。

（一）辨識關鍵或潛在之風險，加強規劃辦理抽查

在不確定風險因素之下，策略良窳及執行過程之監督，攸關各項營運效果之成敗，依據普華永道會計師事務所（PWC）於 2008 年 10 月研究調查，發現企業所面臨之 4 大風險中，策略風險占 60

%，其餘依序為營運、財務、遵循風險各占 20%、15%及 5%，說明組織之策略風險非常高，此項調查結果值得政府機關引以為鑑，審計機關應加強辨識受查機關之關鍵或潛在風險，並審酌評估與民生福祉攸關、預算規模較大、可能存有舞弊及浪費暨不法情事、社會輿論關注、新興方案如促參或民間融資提案（PFI）等風險程度較高議題相關政策或施政計畫，規劃辦理查核工作。

（二）促請善用風險管理工具，設置風險管理登錄冊，加強控管策略風險

策略管理重視執行、控制與評估，其中均包含風險在內，風險管理是組織內每一份子必須參與的工作，須強化機關成員風險意識，及善用風險管理工具，以推動風險管理工作。現今很多機關採取督導會報、管考會議，以控管策略及計畫執行之進度，然對於風險之控管尚顯不足。策略發展計畫實施過程，應遵循相關模式與流程，尤其是長期性計畫，須有更新與追蹤關鍵假設和預測的程序，採「滾動式」管理與定期檢討，以減少策略規劃和策略執行之間落差，如能善用風險管理工具，例如風險管理登錄冊，針對特定機關與策略設計風險登錄及評估檢核表，從上到下，每一個關鍵部門及關鍵領域設置風險登記冊並予維護，確實評估分析並登記主要的風險，再就該等風險因子進行研擬削減、規避或承擔等因應措施，透過檢核表的填寫及彙整，強迫在做決策時，能夠深思熟慮。

六、推廣應用資訊技術控管架構稽核資訊環境，加強資訊技術風險管理，掌握最新資訊科技發展趨勢，承擔稽核新興科技之工作挑戰

資訊科技化的浪潮席捲全球，其對於組織管理幅度與深度的影響，不下於工業革命時期對於產業之衝擊，並催化人類工作方式、生活環境與思維觀念之巨大變化，把人類帶引至便利的數位社會；然而，資訊科技變化速度很快，在享受數位化帶來利益之時，身為審計人員，必須跟上變化的腳步，新興科技對審計工作形成了很大挑戰。

（一）培訓應用資訊科技控制架構之稽核智能，降低系統控制風險

當組織營運依賴電腦系統程度愈來愈高時，面對電腦化以及資訊化帶來之風險，成為重要課題。為加速政府會計發展，趕上國際步調，行政院主計總處於民國 96 年研訂完成普通基金普通公務會計制度，經過數年試辦，預計於民國 103 年正式實施；新普會制度變革頗大，其新版普通公務 GBA 資訊系統，配合新普會制度重新建構代碼與設定、系統管理、流程管理、電子文件管理等功能，並將憑證處理功能納入，且已建置電子發票介接介面，可直接於系統進行審查與核銷，及具備完整上傳會計報告等電子檔案功能。由於各種資訊電子化，涉及電子簽章作業、電子控制技術、審計軌跡確保等問題，以往審計工作採書面審核為主之作業型態，將面臨重大挑戰。

一般而言，系統潛藏之風險包含安全風險、控制風險、系統風險與商業風險，受到 2002 年美國制定沙賓 404 法案影響，控制風險議題持續受到專業團體重視。資訊化作業環境下，大部分的交易紀錄、控制方法與稽核軌跡皆留存於資訊系統中，一般審計人員對資訊系統架構欠缺認識，即使網絡圖表採標準程序，也會以為很複雜，以致無法進一步查核驗證資訊技術及其操作環境安全性，及其資料是否值得信賴。關於資訊科技控制架構，例如 COBIT 工具，被喻為稽核師聖經，是全球公認且運用最廣之控制架構，能有效連結組織日常營運需求，將資訊科技活動組織成一般可接受的流程模式、辨識及配置可運用資訊科技資源、定義管理控制目標等，如以公司治理說明 COSO 內部控制整合架構的關係，那 COBIT 則是 IT 治理準則及 IT 界的 COSO[11]。身處資訊化工作環境，審計人員對於 IT 管理與控制架構，宜詳加瞭解其內涵，有賴審計機關持續不斷的培訓同仁相關智能，推動查核驗證資訊系統控制環境，以落實稽核工作。

（二）掌握資訊科技發展趨勢，承擔新興科技稽核之工作挑戰

現今是資訊科技時代，有許多新興科技趨勢，例如雲端運算、社群媒體等，審計人必須承擔新興科技挑戰，掌握最新科技趨勢脈動，瞭解面臨之風險和整體環境，因應資訊科技蓬勃發展與環境變遷，研習有效率之科技查核知識，增進查核技能，方能把工

[11] 參閱周靜幸、溫大民，政府資訊科技稽核，內部稽核季刊，民國 100 年 1 月。

作做得更好，創造更多價值。關於資訊科技稽核相關議題、資訊科技稽核計畫之擬定、資訊科技專案稽核等，於「全球科技稽核指引 (GTAG)」有詳細介紹說明[12]，可供我等審計人員參考運用，審計機關要把審計人員培訓為 IT 稽核師，瞭解新興科技趨勢及內容，與其可能有的問題、風險，研議加強稽核之方法，以提升審計成果。

七、加強運用電腦軟體輔助審計，善用持續性稽核工具與地理資訊系統，推廣電腦稽核師認證機制，促進審計工作品質進步與創新

在ｅ化的營運環境下，電腦輔助審計技術(Computer Assisted Audit Techniques, CAAT）是一種因應資訊科技產生的現代審計方法，審計人員在電腦軟體輔助下，可以勾稽比對分析巨量資料，辨認異常之處及可能存在之風險，具有低成本、高成效之優點，可為組織提供比過去更為健全之監督機制。審計部自 78 年開始接觸並推廣應用 ACL 等電腦軟體輔助查核，歷經二十餘年，增加政府數十億元收入，成效斐然。宜賡續研議相關稽核策略，提升審計成效，謹摘述如下：

（一）善用「持續性稽核」工具，以監督風險

近年來，為了減輕稽核人員工作負擔，提升稽核活動效率與

[12] 全球科技稽核指引(Global Technology Audit Guide, GTAG)係由 IIA 研擬與資訊科技管理、控制及安全有關之議題，提供內部稽核主管、審計委員會成員及管理階層，對於資訊科技相關風險之瞭解與建議意見。中華民國內部稽核協會已於民國 100 年 8 月翻譯出版。

價值，持續性稽核與監控（continuous auditing/ monitoring ）技術之應用與發展，成為稽核領域的新興議題。持續性稽核係透過自動化技術，運用較高頻率方式自動執行控制及風險評估，供應即時準確之查核報告，以減輕稽核人員負擔，並將事後查核模式提前至即時偵測查核，提升稽核工作價值，其運作原理係奠基於電腦輔助稽核技術，常見的應用技術類型有內嵌稽核模組（Embedded Audit Modules）、通用稽核軟體（General Audit Software）等 2 類；內嵌稽核模組是於資訊系統內部加入測試控制有效性而設計的稽核模組程式，通用稽核軟體則是可使稽核人員獨立自行擷取各種來源資料，並內建各種查核分析功能，即可擷取資料進行分析。

部分稽核作業已成功應用「持續性稽核」技術，舉地方稅務機關運用違章車輛自動辨識系統為例，稅務機關向私人機構購置違章車輛自動辨識系統，於道路架設攝影機，自動判斷畫面中道路行駛的車輛並取像，自動辨識出車號並立即與未完稅、已註銷及離島免稅車輛資料庫（由稅捐稽徵單位事先轉檔存放在系統中）比對該車號如為違章車輛，系統即儲存相關的資料和照片供車輛檢查人員事後確認，並提供舉發單列印功能，節省人工手動開單人力成本。此項技術，取代傳統由稅務、警察單位派員於路口攔檢，查核違章車輛欠稅與使用情形，節省大量人力，並大幅提升查核效率。依審計部彙整地方政府購置違章車輛自動辨識系統情

形及相關財務效益資料，截至民國 101 年 6 月底止，計有新北市等 17 市縣購置該系統，計採購 48 套，平均每套成本約 41 萬餘元，該系統民國 100 及 101 年度 6 月底止查緝違章車輛計 54,703 輛，補徵使用牌照稅及罰鍰高達 9 億 5,991 萬餘元，即每套系統在此 1 年半時間辨識補稅將近 2 千萬元，顯示系統費用不高，稽徵稅款及罰鍰數額龐鉅，強化並健全稅捐稽徵作業，成效頗佳。類此，持續性稽核技術工具運用經驗，確實可以有效降低監督風險與成本，值得推廣參採。

（二）賡續研析可供提升審計作業品質之通用稽核軟體，推廣運用

通用稽核軟體（General Audit Software, GAS）可將不同資料格式及種類的檔案匯入做分析應用，目前使用率最高的稽核軟體，有 ACL、EXCEL、ACCESS、IDEA 等，審計機關近年來加強推廣使用，已有很多應用之經驗，審計人員使用技術亦漸臻成熟；此外，專家建議還有很多可採用之軟體，像是 CaseWare、TeamMate、Securac、EnCase、AutoAudit…等等，關於這些軟體內容，是否適合審計機關運用，其功能效益如何，尚待研析推廣使用。

（三）運用地理資訊系統及加值利用衍生之資料，強化查核技術方法

地理資訊系統（Geographic Information System, GIS），是一個邁向現代化國家所應具備之基礎建設，亦為我國現階段發展之重要建設，結合各種具有空間分布特性之地理資料，利用空間圖層資料庫技術，進行資料之建立、編輯、查詢、分析、儲存和

顯示圖形，用途廣泛。我政府發展國土資訊系統起源甚早，行政院早於民國 78 年核定「國土資訊系統綱要計畫」、內政部繼於 81 年訂頒「國土資訊系統實施方案」，各級政府陸續開發地理資訊系統，例如路網與休閒旅遊系統、都市計畫使用分區管理系統，或消防勤務派遣系統等等，然皆為各單位各自委外開發建置，投資建置不同規格之共用性資料，缺乏統籌整合協調機制，發生相同資料重複建置或整體資源浪費。迨至 96 年 3 月公布施行國土測繪法，主管機關內政部為建置基本圖資，於同年 7 月報經行政院核定「國家地理資訊系統建置及推動 10 年計畫」[13]，近年來陸續辦理完成「國家基本測量發展計畫」、「高精度及高解析度數值地形模型建置計畫」及「基本圖及地形圖修測計畫」等，並訂頒作業要點補助地方政府推動，政府始整合地理資訊資料庫，提供單一窗口供機關業務推動及民間加值應用。

透過地理資訊系統整合套疊數值地籍圖，可真實的將地上物使用現況直接呈現地籍圖線並連結實地照片，使人一目了然，並可依需求縮放適當之圖籍比例尺，減少實地勘查人力及時間之耗費。部分機關單位運用圖資協助處理公務，例如地方稅務機關為查核加蓋違章建物影響稅收情形，利用 Google Earth 或地理資訊 e 點通等系統，先行查核瞭解房屋建物概況，獲悉各處建物基本概況後，再赴現場實地查證，收事半功倍之效；審計機關運用航照

[13] 該項 10 年計畫，涵蓋 9 大資料庫，包含：地形圖、土地、城鄉規劃、社會經濟、自然環境、行政區界、環境品質、交通運輸、公共管線及工程等項。

圖查核造林獎勵金發放，獲致良好審計效益等。另上述 10 年計畫執行成果之流通供應、加值利用等，亦將衍生不同型態之運用內涵，審計人員可研究廣為運用相關圖資查核，以提升審計成效。

（四）鼓勵審計同仁取得電腦稽核師證照，獲取專業能力證明

美國資訊系統稽核與控制協會（Information Systems Audit and Control Association, ISACA） 除了上述制訂完成實用之資訊系統稽核與控制標準架構 COBIT 外，並推動國際電腦稽核師（Certified Information Systems Auditor, CISA）及國際資訊安全管理師（Certified Information Security Manager, CISM）的證照制度，該協會公正獨立的形象，獲得美國政府課責總署（GAO）認可，要求查核美國政府單位資訊系統相關人員，必須具有 CISA 資格。近年來審計部每年開設電腦審計課程積極培訓同仁，多數審計人員已具備電腦稽核之專業技能，惟未參與認證取得電腦稽核師證照，有待鼓勵同仁參加認證，獲取專業能力證明。

八、因應個人資料保護法新制實施，研擬個人資料保護之配套措施，強化安全維護管理策略

政府為與國際社會接軌，積極引入歐美先進國家隱私權保護之制度與作法，以符合國際公約與條約之要求。安侯建業會計師事務所（KPMG）於 2012 年 7 月公布「企業舞弊及不當行為問卷調查報告」，內容指出，超過 6 成上市櫃公司主管認為，舞弊及不當行為是目前台灣經營環境須關注的一大問題；竊取機密資訊與違

反個資法，是現今較擔心的舞弊風險。調查報告指出，有 4 成回覆者認為現今最讓企業擔心的舞弊是「竊取機密資訊」與「違反個人資料保護法」等挪用資產類風險，與 2009 年調查相比，增加近 1 倍。

民國 99 年 5 月 26 日總統公布並於 101 年 10 月 1 日施行「個人資料保護法」，該法係修正自「電腦處理個人資料保護法」，名稱有所不同，新法拿掉了電腦處理，個人資料不再限制於電腦檔案之形式，擴大保護客體為所有個人資料[14]，除電腦處理外，尚包含紙本等書面文件。關於個人資料之資訊安全管理作業，新法明定公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，以防止個人資料被竊取、竄改、毀損、滅失或洩漏[15]；另對於個人資料安全維護方式，要求「個人資料蒐集、處理及利用之內部管理程序」與「個人資料安全維護之整體持續改善」[16]，均屬全新之要求，若因外洩個人資料，侵害被使用人權利，最高賠償總額達 2 億元，且被使用人不需擔負舉證責任，而需由機關證明已盡一切可能保護資料。準此，新法施行，影響頗鉅，所有涉及蒐集、處理及利用個人資料者，面臨更高管理風險，宜妥為因應。

(一)檢討研修審計機關個人資料安全保護規定，以資周延

[14] 依個人資料保護法第 2 條規定：「個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。」

[15] 個人資料保護法第 18 條規定參照。

[16] 個人資料保護法施行細則第 12 條規定參照。

個人資料保護法明定公務機關保有個人資料檔案者，應訂定個人資料安全維護規定[17]。完善之管理制度，能降低資訊安全風險，審計機關原已訂頒「審計部及所屬各審計處室資訊安全管理作業規定」、「審計部及所屬各審計處室運用各機關電腦資料檔案管理規定」、「審計部及所屬各審計處室電腦儲存媒體管理措施」，因應新法施行，修正主軸在於擴大保護客體為所有個人資料，除電子檔案外，尚包括人工紙本等個人資料，審計機關宜全面重新檢視現行資訊安全內部規章之周延性，建立明確的政策規範與監督體系。

（二）研擬電腦報廢處理作業規範，確保資料安全

關於個人電腦已不堪使用需辦理報廢時，很多人以為把檔案清除就安全，專家建議最好的方法是把硬碟拿掉，因為現今科技進步，有心人會利用專業軟體將刪除掉之檔案予以恢復，所有的內容和資料都還保持完整的。審計機關為電腦審計作業之需，轉錄各機關之電腦資料檔案，雖已規範應採取必要之管制措施，對於轉錄之檔案及經處理衍生之檔案，應於抽（調）查案件處理完竣後，通報政風單位監視銷毀，惟電腦報廢，通常是整批交由電腦回收廠商處理，未有規範報廢電腦其硬碟之處理方式，宜研擬控管規範，將硬碟取下交由機關專責人員予以格式化等方式處理，以確保資料確實安全無外洩之虞。

[17] 個人資料保護法施行細則第 24 條規定參照。

（三）研議公文附件具機密性者之處理方式，妥設控管機制

對於含有個人資料之公文，其以附件密送處理者，實務上常以「附件抽存解密」做為解密條件，依行政院修正文書管理手冊規定，「附件抽存解密」適用於該附件已載明解密條件者，惟機關多未載明附件之解密條件，縱有載明亦記載多年後如 10 年解密等情形，附件既由承辦人抽存，未歸入機關檔案，機關未設有適當控管機制，歸由承辦人自行處理之做法，產生控管漏洞，倘若疏未注意控管，不僅難保個資外洩情事發生，陷承辦人於危機之中，並與個人資料保護法責由機關承擔資訊安全維護管理責任之規定未合，宜研謀妥為處理。

《參考資料》

2012 年亞洲區內部稽核協會年會書面資料。

CIA Review 第一科 內部稽核在治理、風險及控制之角色，中華民國內部稽核協會 2010 年 2 月 12 日第 14 版，作者：Irvin N. Gleim，譯者：周台俊，覆核：陳錦烽。

ISSAI X: The Value and Benefits of Supreme Audit Institutions – making a difference to the lives of citizens (Exposure Draft)，INTOSAI，2012。

KPMG Analysis of Global Patterns of Fraud – Who is the typical fraudster? KPMG，2011。

The 2007 Oversight Systems Report On Corporate Fraud，Oversight Systems, Inc.

周靜幸、溫大民，政府資訊科技稽核，內部稽核季刊，民國 100 年 1 月。

高登・唐諾森，公司治理--哈佛商業評論精選，2006 年 5 月，林宜賢、蔡慧菁譯，天下文化出版。

黃淙澤、林宜隆等，電腦稽核與資訊安全管理--以 COBIT 為例，電腦稽核，第 9 期，民國 92 年 7 月。

孫嘉明，如何藉由電腦輔助稽核跨至持續性稽核與監控，內部稽核季刊，民國 100 年 4 月。

審計準則公報第四十三號—查核財務報表對舞弊之考量，財團法人中華民國會計研究發展基金會出版，審計準則委員會於民國 95 年 9 月 1 日正式發布。

鑑識會計及舞弊查核，指南書局 2011 年 8 月出版，作者：Mary-Jo Kranacher、Richard Riley、Joseph T.Wells，譯者：中華民國會計師公會全國聯合會鑑識會計委員會。