企業風險管理的指引 － ISO 31000(風險管理系統)

彭金玉*
開南大學風險管理系 助理教授
趙家民
南華大學環境管理研究所 助理教授

摘 要

2007 年美國次級房貸與 2008 年雷曼兄弟銀行倒閉等重大事件爆發後，引發全球性的金融危機，對全球之經貿與企業經營環境帶來空前的嚴重衝擊。此刻，企業經營者面對各種的風險，應妥善規劃與處理。因此，企業如何建構一個完整且能符合企業需求的風險管理系統，乃爲迫切且重要的課題。但現行國際間已公告的風險管理系統與標準，版本及類別甚多，使得企業在選擇適合組織本身所需之風險管理系統時，缺乏評選準則。本文利用文獻分析法；針對風險管理系統的內涵、原則、實施指引、管理架構、管理流程與策略等，作深入的分析與探討。研究結果顯示；ISO 31000 風險管理系統標準之理論、管理架構及策略，比較符合企業與未來風險管控發展趨勢所需。除可提供學術領域之研究；以及作爲企業建構風險管理系統與實施之參考外，亦可降低企業的經營風險，進而可提升企業的競爭力，達到企業永續經營的目標。

關鍵字：風險、風險管理、ISO/DIS 31000、企業風險管理、文獻分析法

---

*通訊作者：彭金玉
Email：Robert@mail.knu.edu.tw

Enterprise risk management guidelines

－ ISO 31000(Risk management system)

Jin-Yei Peng
Assistant Professor，Department of Risk Management，Kainan University
Chia-Min Chao
Assistant Professor，Institute of Environmental Management，Nan Hua University

Abstract

In 2007 the United States and 2008 with the subprime mortgage bank Lehman Brothers closed down after the outbreak of major events such as the rise of the global financial crisis on Taiwan's economic and business environment brought about by unprecedented deal a serious impacted. At the moment，the world's managers In the face of various risks，and planning should be properly dealt with. As a result，enterprises can build a complete line with the needs of enterprise risk management system，and it is thus an urgent and important issue .ISO / DIS 31000 (risk management standard) has been in 2008 Sept. 1 to complete the voting committee，is expected to be in the near future version of the ISO international standards and notice
implementation.

This paper uses literature review method to analyze ISO / DIS 31000 risk management standard of content，in principle，the implementation of the guidelines，management structure，processes and management strategies for in-depth evaluation research. In addition to the provision of enterprise risk management system construction and implementation of reference，but also to reduce business risk and thus enhance the competitiveness of enterprises，and enterprises to meet objective Continued to operated.

Keywords：risk、risk management、ISO/DIS 31000、enterprise risk management、literature review method.

壹、緒論

人類自從進入 20 世紀後半以來，企業營運環境的變遷趨勢轉向加遽。因此，產能需不斷擴充，技術亦需持續提升，加以產品創新設計與行銷模式的推陳新出，正逐漸爲企業帶來「風險」(Risk)。而在現今相互依存與連結的經營模式中，企業隨著非核心產品及服務紛紛委外生產後，顧客、供應商、合作伙伴及競爭者間之關係將越趨複雜。現行的企業可謂是金融風險、產品風險、市場風險、環境、安全、衛生及工程等風險的集合體，亦即整合性風險 (Integrated risk)，使得傳統的經營與風險管理模式已明顯不足。

在科技蓬勃發展下，企業要如何把風險管理科技及其基礎建設融入企業的內部文化；便是首當其衝的難題。再者，風險管理科技及其基礎建設須具備何種重要條件，始有助於風險管理規劃的推廣，基於必要性與經濟復甦的刺激，企業對風險管理科技與其基礎建設的需求已很明顯。無奈，國際上迄今尚未找能到適合企業建構完整的風險管理系統標準及工具以供參考。

尤以近日全球金融風暴的演變，以及三聚氰胺毒奶事件的衝擊，我國企業經營者對風險管理的理念與融入企業文化，已漸有所認知及共識。因此，本文將利用文獻分析法；針對國際間現行之風險管理系統或標準，其原則、實施指引、管理架構及管理流程等，進行深入的分析與探討，以提供學界學術研究，亦可作爲企業建構風險管理系統與實施的參考。

貳、文獻探討

風險管理(Risk Management)根據文獻記載，風險管理的起源大致可區分爲歐洲系統，以德國爲溯源地；另一是北美系統，以美國爲發源地(陳繼堯，1999)。德國的風險管理源自於第一次世界大戰後的「風險政策」(Risikopolitik)論。第一次世界大戰，德國戰敗，企業爲求生存，紛紛開始研究因應之道。而風險對策咸認爲是經營上之重要課題，其因應的方法即所謂的「風險政策」，內容包括：風險控制、風險分散、風險補償、風險防止及風險隔絕等措施。

美國的風險管理，則可追溯至 1930 年的美國經濟大蕭條。1931 年美國成立經營者協會(American Management Association，AMA)保險部門，直到 1957 年，美國保險管理學會(The American Society of Insurance Management)才開始重視風險管理的觀念，並成立教育委員會協助美國各大學推廣風險管理教育。爲因應風險管理的發展，美國保險管理學會復於 1975 年改名爲「風險暨保險管理學會」(The Risk and Insurance Management Society，RIMS)，使風險管理的領域，由單國性業務跨入了多國籍企業。

雖然我國風險管理教育早在 60 年代即已萌芽，但成效僅止於保險相關之學校或企業之中低階幹部。1985 年 7 月因臺灣電力公司恆春核能三廠火災及巨額損失，促使政府與公民營企業對風險管理的重視。1997 年亞洲金融風暴發生後，短短幾個月，造成東亞國家發生貨幣貶值競賽，亦使日、韓等國某些知名之證券公司及人壽保險公司倒閉。

隨著全球氣候異常、科技快速發展、國際間交流往來頻繁、媒體發達及人民對政府期許提高等自然與人文環境變遷，導致社會充滿不確定性，政府施政所面臨之挑戰日增。爲確保民眾權益，降低風險發生之可能性與衝擊，行政院於 2005 年 8 月函頒「行政機關風險管理推動方案」(行政院研考會，2006)，以培養行政院所屬各機關的風險管理意識，促使各部會清楚瞭解與管理施政之主要風險，以形塑風險管理文化，提升風險管理能量，有效降低風險發生之可能性與衝擊，能如期如質達成組織目標。

吳宗鎧、賴麗華，利用蒙地卡羅法模擬 TFT-LCD 產業供應鏈報酬率與風險之研究(2006，吳宗鎧、賴麗華)，結果顯示；TFT-LCD 產業供應鏈的廠商其上中下游的平均報酬率水準屬性與其效果受影響，且供應鏈間的風險有顯著的差異。

彭金玉、許如碩，結合安全衛生管理、風險管理及防災應變技術等參數，對大專院校校園安全風險管理進行探討，其結合影響圖與模糊理論的風險量化觀念及 PDCA 循環管理機制，成功建置一套適合我國大專院校實驗(試驗)室的安全風險管理系統，以降低校園風險(2006，彭金玉、許如碩)。

張啓昌、廖國雄等，以 BS 7799 資訊安全管理規範建構資訊安全風險管理模式之研究(2006，張啓昌、廖國雄等)，以 BS 7799 資訊安全管理標準之 10 個控制要項與 127 個控制目標作爲風險評估標的，實際針對新竹某醫院加以評量、分析，建立符合該醫院之資訊安全管理模式，提升醫療品質。

劉馨隆、蔡敦仁，引入作業成本制與風險分析於營建專案成本與進度管理之應用(2007，劉馨隆、蔡敦仁)。其以引入作業成本制作爲營建專案成本分析的基礎，並以現金流量之分析爲架構，建構一合理又符合營造工程專案特性成本與進度整合管理模式，以作爲工程專案財務管理之參考及準備專案資金調度計畫的依據。

彭金玉，針對高科技產業的風險管理與策略，其環境與安衛風險管理之研究(2007，彭金玉)。依據高科技光電產業之製造與管理流程，進行環境與安衛風險失效模式分析(Failure Mode and Effects Analysis，FMEA)。研究顯示；蝕刻單元爲光電科技產業之環境與安衛風險管理的核心。

行政院勞工委員會透過國內外工程相關文獻整理與實例分析，就工程生命週期各階段之安全防範，制定公共工程施工安全風險管理防災手冊(行政院勞研所，2008)，探討國際上各先進國家於公共工程建設，在執行安全管理之制度與法令規範上，對如何確保工程作業安全等防範措施，以降低職業災害及工程風險。

參、研究方法

一、風險管理系統(ISO/DIS 31000)分析

企業風險管理系統與標準一直是學術界期待突破的研究領域，但因其涵括的學理、管理流程及控管策略，迄今尚未建立一套客觀的評選準則；可供選擇真正符合企業需求之管理系統與標準，並經企業之實務運作經驗加以驗證。因此本文利用文獻分析法，針對現行國際間所公告之風險管理標準的原則、實施指引、管理架構及管理流程等，進行深入的分析與探討。

本研究係針對現行國際間已公告之風險管理系統或相關標準，如 ISO/DIS 31000 (風險管理系統)、BS 31100 Code of practice for RiskManagement (英國風險管理標準草案)、CAN/CSA-Q850-97(加拿大風險管理標準草案)、AS/NZS 4360：2004(澳紐風險管理標準)、General Guidelines for Principles and Implementation of Risk Management (2005)，Japan(日本的風險管理標準草案)，Risk Management Program Standard (1996)等文獻資料，並依風險管理系統、風險管理架構、風險管理流程、公告版本、系統完整性及實用性等構面進行分析比較，以評選較符合企業需求之風險管理系統與標準。

1996 年 9 月美國石油與氣體研究委員會，爲使油氣相關企業在管路設計、施工及維修過程中，能事先提出有效的風險管理計畫與建議書，最主要的目的是要降低管路企業的經營風險。

2004 年 Dr Dale F Cooper 聯合澳洲與紐西蘭技術委員會(OB-007)，發展爲澳洲與紐西蘭風險管理標準(AS/NZS 4360：2004)，並結合相關的風險管理手冊(Risk Management Guidelines，2004)，廣泛應用於政府公共部門與區域部門。同時本標準亦提供政府機關作爲風險管理的指引(NSW Public Works Department，1993)，並建立標準方法，現已爲澳洲政府採用(MAB/MIAC Report 22，AGPS，Canberra、AGPS，Canberra. ISBN 0644362952，AGPS，Canberra. ISBN 0642268037)。

2004 年英國國家標準學會(BSI)爲使企業在經營過程中，能深切瞭解、發展、執行及維持風險管理，以降低組織之風險，成功的達成組織之績效目標，建立 BS 31100 Code of practice for Risk Management (英國風險管理標準草案)。本標準共包含六大部分：

1.範疇；
2.風險管理原理；
3.風險管理模式；
4.風險管理架構；
5.風險管理流程；
6.執行風險管理。

本標準可適用於任何行業、規模及性質，以及政府機構之各公共部門。

2005 年日本參照澳洲、紐西蘭、英國及 ISO/IEC Guide 73 等資訊，完成 New work item proposal (General Guidelines for Principles and Implementation of Risk Management (2005，草案)。其採行查檢表(checklist)方式，並與國際上所公告之品質、風險管理、職業安全衛生等文獻，如 ISO 10006、ISO 14971、IEC 60300-3-9 、ONR 49000、AS HB205：2004 等相關標準或指引相容。本標準共包含六大部分：

1.範疇；
2.參考標準；
3.定義；

4.風險管理的原理；

5.組織風險管理流程之執行；

6.執行風險管理融入組織文化。

2008 年 4 月國際標準組織(ISO)公佈之 ISO/DIS 31000 (風險管理系統 DIS 版)，業於 2008 年 9 月 1 日完成委員會投票，預期將於近期內公告成爲 ISO 國際版本，爲目前國際上最快速且較完整之風險管理系統與標準。ISO/DIS 31000 之管理原理、架構、管理流程及控管策略，分述如下：

企業風險管理之目標與組織活動的範圍有密切的關係，從活動的策略至運作、流程及計畫開始，且能反映這類活動對運作、財務及組織聲望的影響。風險管理可協助對未來可能發生活動的不確定性與衝擊提供決策，並評估應採行的因應措施。因此，風險管理的方法與邏輯可包含下列：

- 溝通與諮議的過程；
- 建構風險管理的相關內含；
- 辨識、分析、評價以及處理與組織活動有關之流程、功能、計畫、產品、服務或資產等風險；
- 監督與量測風險；以及
- 適當地紀錄與報告風險的結果。

風險管理常運用於安全、人類健康、環境及強制性法規等領域，並利用其管理方法以協助及確定此標準如何被定義與使用。ISO/DIS 31000 亦可幫助組織符合法規、相關要求事項及管理績效的提升。ISO/DIS 31000 風險管理之原理、架構及管理程序間的關係，如圖 1 所示。

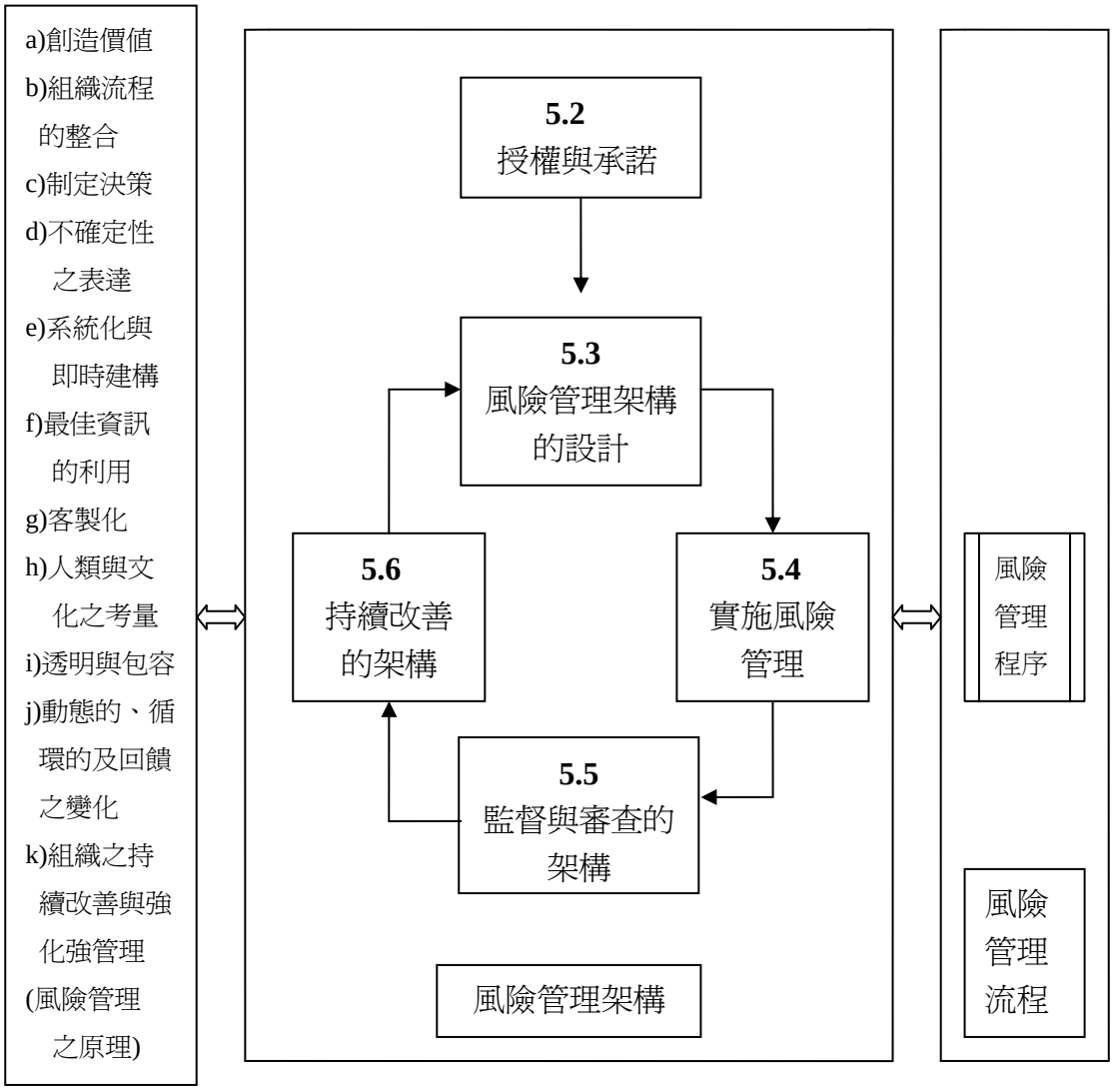

圖 1 ISO/DIS 31000 風險管理之原理、架構及程序的關係

二、風險管理架構 (Framework for managing risk) 分析

風險管理的架構可協助組織進行有效的風險管控，且風險管理的程序應運用於組織的各個階層(部門)及特定的情況。本架構應確保所有組織的各部門之風險資訊均能適當地報告，並可提供決策者制定決策時的參考。風險管理架構的組成要件，如圖 2 所示。

ISO/DIS 31000 風險管理的架構，係透過 P-D-C-A 管理循環之模式。企業於開始設計與完成風險管理架構前，須瞭解組織之內外部環境因素，訂定風險管理政策，並建立風險管理溝通的模式，將角色、責任、計畫標的、績效量測、資源及風險管理指標等進行溝通與宣導。同時擬定風險發展執行計畫與程序，經由監督與審查機制，使組織之風險管理達到持續改善的終極目標。

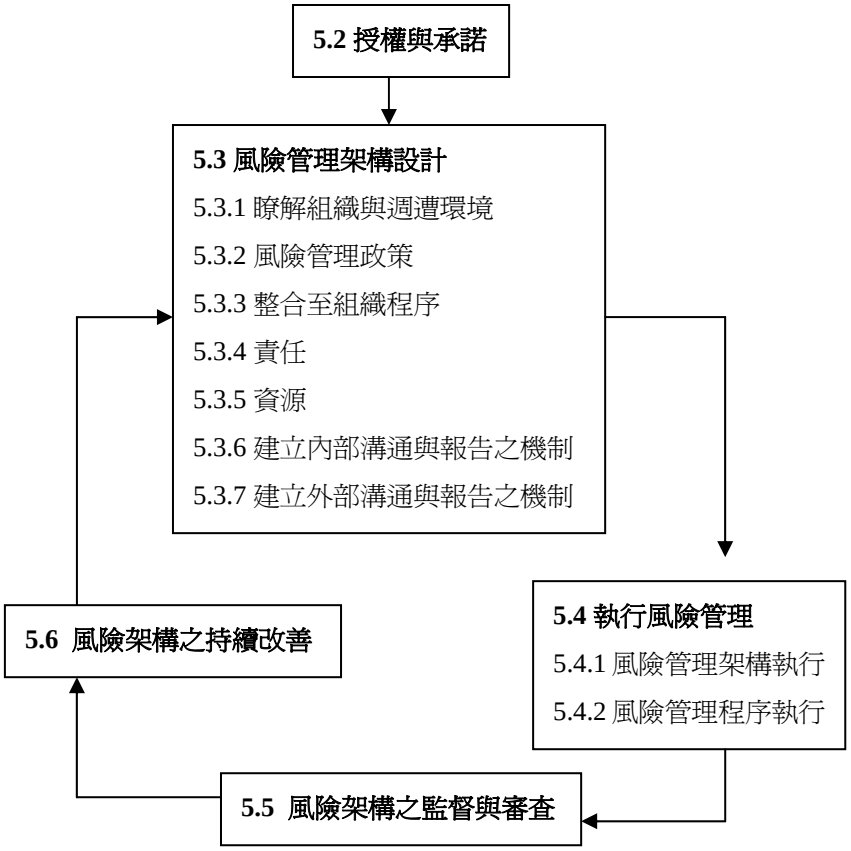

圖 2　ISO/DIS 31000 風險管理架構的組成要件

三、風險管理流程 (Process for management risk) 分析

風險管理流程所描述的相關活動，如圖 3 所示。其包括溝通與諮詢、建立環境狀況、風險評估(含風險辯識、風險分析及風險評價等步驟)、風險處理及監測與審查等要項。

6.3. 建立環境狀況 (Establishing the context)

組織應在每一個風險管理流程之範疇與風險準則界定時，應儘可能與內、外部利害相關者進行溝通與諮詢。因此在風險管理系統發展階段初期，即應建立與內、外部利害相關者的溝通與諮詢計畫，且其風險管理流程應與組織的文化、程序及架構一致。環境狀況包含組織相關的內部與外部參數，當此參數與風險管理架構設計的考量要項近似時，組織須更周詳且特別地考量如何與特殊的風險管理程序的領域相互結合，包括：

6.3.2 建立外部的環境狀況。

6.3.3 建立內部的環境狀況。

6.3.4 風險管理流程環境狀況的建立。

6.3.5 發展風險評估準則。

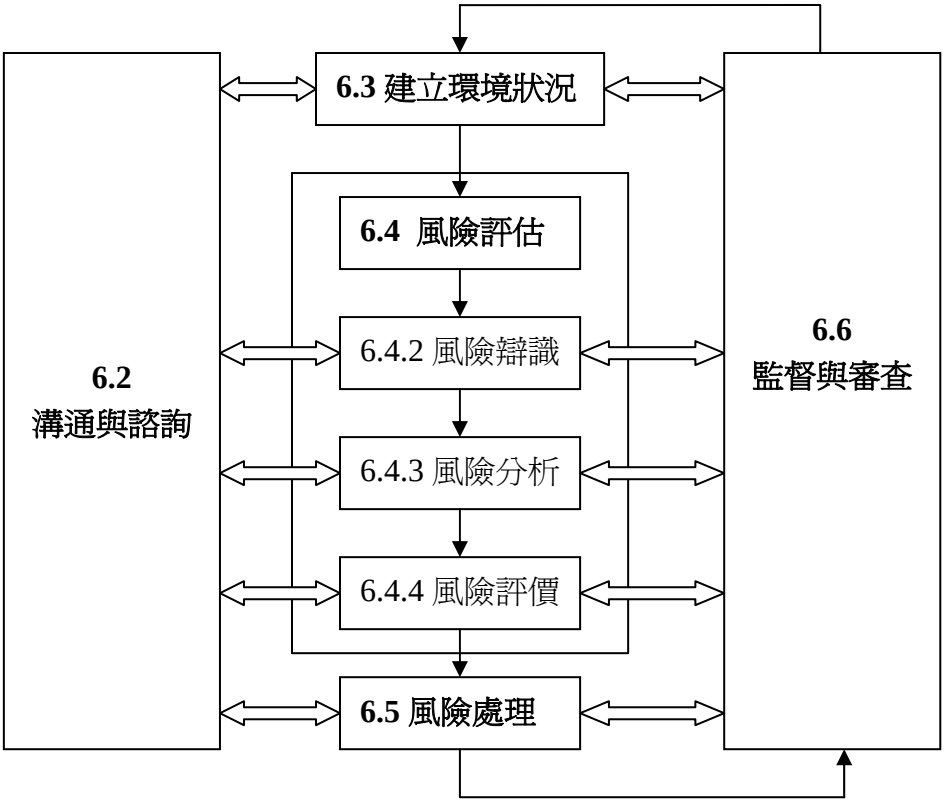

圖 3　ISO/DIS 31000 風險管理流程

6.4 風險評估 (Risk assessment)

6.4.1 一般要求事項 (general)

風險評估係指全面性的風險辯識、風險分析及風險評價的過程。

6.4.2 風險辯識 (Risk identification)

組織應辨識其風險的來源、衝擊的範圍、事件所引起原因及其潛在的後果，以達成其風險管理目標。辨識過程中；應針對組織之整體性風險進行辨識，辯識時亦應掌握相關且最新的資訊，包括適當的背景資訊與資料之更新。且須經由擁有適當風險管理專業知識的人員，辨識其可能發生的原因、情境及後果，並對風險與機會之取捨作進一步的考量。

6.4.3 風險分析 (Risk analysis)

風險分析是瞭解風險發展的過程。風險分析係作爲風險評價的輸入，以提供決策者是否採行最適當的策略與方法，並進一步處理風險。一般可藉由判定其後果、發生之可能性及風險屬性以分析風險。一個事故或一系列的事件可能導致多重的後果且可能影響其多重目標。故在執行風險分析過程中，須考量組織現行的風險控制系統及其效力。

進行風險分析時可從風險之細部變化程度、分析目的、可獲得的資訊及資源等方面著手。風險分析可採定性、半定量或定量，或上述之組合等方式進行，需視事件之需求作決定。通常可優先使用定性分析以獲得風險等級及

辨識主要的風險。當其可行且適當時，應進行特定與定量的風險分析。有時亦可利用數學模式進行模擬分析，模擬結果可提供決策者參考。

6.4.4 風險評價 (Risk evaluation)

風險評價的目的係協助組織，依據風險分析結果以判定需優先執行的風險。風險評價需包含風險等級的比較，且決策制定時應考量更廣泛的風險狀況，包含組織可承受的風險容忍度(tolerance)，法律及其他要求事項等。

6.5 風險處理 (Risk treatment)

風險處理是包括選擇一個或多個風險管控的建議，並執行此建議事項。風險處理係一個循環評估的流程，可作爲組織判斷其殘餘的風險是否可容忍，否則需產生新的風險處理方案，並評估與處理直到符合組織的風險政策爲止，而風險處理方式的選擇，不需在所有情境下彼此排擠或並列。風險處理包括風險處理方式的選擇、準備及執行風險處理計畫等要項。

6.6 監督與審查 (Monitoring and review)

監督與審查的目的爲：

- 事件、變更及趨勢以作爲組織分析與學習的經驗；
- 可偵測外部與內部環境狀況的改變，包括需修訂的風險處理及其優先事項的變更；
- 確保風險控制與處理方式在設計和運作上是有效的；以及
- 辨識額外的風險。

監督與審查應包含定期與特殊的規劃，其職責應明確訂定，監督與審查結果亦應記錄，並在適當時機向內部與外部相關者提出報告，該報告可作爲風險管理架構審查程序之資訊。

6.7 風險管理流程的紀錄 (Recording the risk management process)

風險管理的活動應是可追蹤的。在風險管理程序中，文件紀錄可提供組織作爲改善方法、使用工具及整個程序之改善基礎。

肆、結果與討論

風險管理於 1950 年代在美國崛起後，於理論與實務方面，均有長足之進展與普及，現已成爲世界公認的一項新穎管理科學。此一管理科學，不僅可協助企業藉由成本與效率的分析，對所面對的各種風險，作客觀且科學之決策，以降低經營成本與風險，進而使企業獲得更大的安全保障。

直到 1970 年代，風險管理的概念、原理及施行，已漸漸從美國遠播至加拿大、澳洲、英國、歐洲及日本等國家和地區。1999 年 9 月臺灣發生了令人震驚的 921 大地震(中央災害防救會報，2007)，2001 年 9 月美國世貿中心的恐怖攻擊事件(大紀元報，2006)，2003 年春天爆發的 SRAS 事件(工商時報，2001)，以及 2007 年美國引爆的次級房貸金融危機，造成全球經濟衰退、物價飛漲，使世人再次陷入『現代風險社會』的焦慮與不

安中，已嚴重威脅著每個國家、每個行業及每一個人。

本文利用文獻分析法；針對現行國際間所公告之風險管理標準的原則、實施指引、管理架構及管理流程等，進行深入的分析與探討。分析結果如附表所示；從風險管理系統標準之理論、管理架構、管理流程及控管策略等觀點而言，ISO 31000 風險管理系統標準，是比較符合現行企業與未來風險管控發展趨勢所需。

風險管理系統與標準文獻分析法結果一覽表

標　準 分析項目	ISO/DIS 31000	BS 31100	AN/NZS 4360	New work item proposal	Risk Management Program Standard
風險管理架構	◎	◎	◎	○	○
風險管理流程	◎	◎	◎	○	◎
系統完整性	◎	◎	○	○	○
實用性	◎	◎	○	◎	○
現行版本(CD/DIS)	DIS	CD	CD	CD	CD

符號說明：◎ 優　○ 好

伍、結論與建議

歷經美國次級房貸與雷曼兄弟銀行倒閉等重大金融風暴的衝擊後，對全球企業經營環境帶來更嚴峻的考驗。就現代組織管理者而言，如何建構一個符合企業需求之風險管理系統與控管策略，是企業訂定施政目標與計畫時，不可或缺的一環。尤其我國產業結構；與歐美各國相較，中小企業所佔比率明顯偏高，且對企業風險管理之概念與管理，尚處於萌芽與學習階段。經文獻分析法結果顯示；從風險管理系統標準之理論、管理架構及控管策略等觀點而言，ISO 31000 風險管理系統，是比較符合企業與未來風險管控發展趨勢之所需。且 ISO/DIS 31000 風險管理系統與標準，即將成爲 ISO 國際標準，不失爲企業參考的寶典。

因此；建議我國經濟部標準檢驗局，應持續追蹤 ISO/DIS 31000 風險管理系統標準的後續發展，並及早因應與制定(CNS 31000 風險管理系統)國家標準公告施行。除可提供企業建構風險管理系統選擇之參考外，且可透過第三者稽核的客觀驗證，以降低企業之經營風險，進而可提昇企業的競爭力。

參考文獻

1. New South Wales Government (1993) Risk Management Guidelines. NSW Public Works Department，Sydney，Nov. ISBN 0 731027041 .
2. Commonwealth of Australia (1996) Managing Risk in Procurement- a Handbook . AGPS，Canberra .ISBN 0 6443 6295 2 .
3. Risk Management Program Standard (1996)，The Office of Pipeline Safety，The Joint Risk Management Program Standard Team.
4. Common wealth of Australia (1996) Guidelines for Managing Risk in the Australian Public Service. MAB/MIAC Report 22，AGPS，Canberra.
5. Cooper，DF (1997) Applying Risk Management Techniques to Complex Procurement. Purchasing Australia，AGPS，Canberra .ISBN 0 6422 6803 7 . Public Works Department，Sydney，Nov. ISBN 0 7310 27041 .
6. An Integrated Risk Management Framework for Small Agencies (2004)，Consulting and Audit Canada.
7. Standards Australia and Standards New Zealand (2004) HB 436：2004，Risk Management Guidelines：Companion to AS/NZS 4360：2004，Sydney，NSW. ISBN 0 7337 5960 2 .
8. General Guidelines for Principles and Implementation of Risk Management (2005)，Japan.
9. The Australian and New Zealand Standard on Risk Management，AN/NZS 4360：2004，Broadleaf Capital International Pty Ltd, 2007.
10. BS 31100 Code of Practice for Risk Management Consultation (2007)，British Standards Institution，U.K.
11. Risk management – Principles and guidelines on implementation，Draft International Standard ISO/DIS 31000，International Organization for Standardization 2008.
12.陳繼堯，1999 年 8 月，風險管理的回顧與將來，風險管理管理雜誌第 2 期，9~12.
13.行政院研考會，2006 年 11 月，前言，風險管理作業手冊，1.
14.吳宗鎧、賴麗華，2006 年 5 月，策略聯盟廠商供應鏈風險之研究 - 以臺灣 TFT-LCD 產業爲例，風險管理與決策研究學術研討會，23~29.
15.彭金玉、許如碩，2006 年 8 月，大專院校校園安全風險管理之探討，2006 年大學基礎教育國際學術研討會，20~28.
16.張啓昌、廖國雄等，2006 年 5 月，以 BS7799 資訊安全管理規範建構醫院資訊安全風險管理模式之研究 - 以新竹某私立醫院爲例，風險管理與決策研究學術研討會，111~120.
17.劉馨隆、蔡敦仁，2007 年 5 月，作業成本制與風險分析於營建專案成本與進度管理之應用，風險與安全管理國際學術研討會，35~42.

18.彭金玉，2007 年 5 月，高科技產業的風險管理與策略 - W 光電公司的環安衛風險管理研究，風險與安全管理國際學術研討會，19~28.
19.鄭燦堂，2007 年 10 月，風險管理理論與實務，五南出版圖書有限公司， 再版，7- 8.
20.行政院勞工委員會勞工安全衛生研究所，2008 年 5 月，公共工程施工安全風險管理防災手冊.