Journal of Accounting Review
會計評論，第 64 期，2017 年 1 月
第 1－38 頁

以 COBIT 5 觀點探討 ERP 系統風險管理機制

張碩毅
國立中正大學會計與資訊科技研究所

張益誠*
國立東華大學會計學系

李幸蓉
國立中正大學會計與資訊科技研究所

陳央庭
國立中正大學會計與資訊科技研究所

摘要

本研究以電腦稽核協會於 2012 年所發布的資訊科技與資訊系統控制架構－COBIT 5 為基礎，建構出一套適用於企業資源規劃系統的風險管理機制。本研究運用 Gowin's Vee (Gowin 1981)模型建立本研究流程。在理論端，本研究透過文獻探討方式，藉由蒐集與編碼相關文獻，建構出 ERP 系統風險管理機制之雛型。透過德爾菲法執行兩回合的專家問卷，進行內容效度和一致性的檢定以完成本研究機制之修正，修正後之 COBIT 5 為基礎的 ERP 系統風險管理機制具有 4 構面、52 項風險因子及針對風險因子的 125 項控制項目。在實證端本研究以個案研究，透過與個案公司的深度訪談，驗證本研究機制之有效性。本研究結果，能協助企業藉由風險辨識、評估、回應、監督與修正等完成整個風險管理的程序，快速找出潛在的風險因子並採取控制措施，提供企業一個便利且有效的 ERP 系統風險管理工具。

關鍵詞：企業資源規劃系統、COBIT、風險管理

* 通訊作者電子信箱：icc@mail.ndhu.edu.tw。地址：花蓮縣壽豐鄉大學路二段 1 號。

收稿日：2013年9月
接受日：2016年4月
三審後接受
主審領域主編：陳育成教授
DOI: 10.6552/JOAR.2017.64.1

Development of an Enterprise Resource Planning System Risk Management Mechanism Based on COBIT 5

She-I Chang
Institute of Accounting and Information Technology
National Chung Cheng University

I-Cheng Chang*
Department of Accounting
National Dong Hwa University

Hsing-Jung Li
Institute of Accounting and Information Technology
National Chung Cheng University

Yang-Ting Chen
Institute of Accounting and Information Technology
National Chung Cheng University

Abstract

The present research investigates the possible ERP system risk factors based on COBIT 5 released by ISACA for information technology and information system control architecture in 2012. Gowin's Vee (Gowin 1981) is adopted as the main research strategy in this study. First, on theoretical development , this study collects and codes relevant literatures; then, the prototype of ERP systems risk management mechanism is formed through literature review. A two-round Delphi expert questionnaire is then adopted to revise the prototype of the risk management mechanism via optimizing content validity ratio and consistency test. The finalized establishment of the Mechanism of ERP systems risk management consists of 4 dimensions, 52 risk factors, and 125 control items. Finally, this study adopts a case study method, conducting an in-depth interview with a case company and assessing the validity of the research results on the practical side. The findings of this study add to enterprise risk management process consisting of the steps of identification, assessment, response, and monitoring and revision to provide enterprises a convenient, quick, and suitable ERP system-risk management tool.

Keywords: *Enterprise resource planning (ERP), COBIT, Risk management.*

* Corresponding author, email: icc@mail.ndhu.edu.tw. Address: No. 1, Sec. 2, Da Hsueh Rd. Shoufeng, Hualien 97401, Taiwan (R.O.C.).

Submitted September 2013
Accepted Aril 2016
After 3 rounds of review
Field Editor: Professor Yu-Cheng Chen
DOI: 10.6552/JOAR.2017.64.1

壹、緒論

高度全球化和國際化促使企業廣泛的依賴於科技，管理和發展其商業業務與營運過程時，透過大量的投資資訊科技（information technology，簡稱 IT）以提高自身的競爭力。企業資源規劃（enterprise resource planning，簡稱 ERP）系統從 20 世紀 90 年代崛起成為軟體產業最為著名的企業軟體之一(Stefanou 1999; Oliver and Romm 2000)。ERP 系統為跨組織整合的軟體套件，其中包括了多重功能的應用程序（例如：財務、產銷、供應鏈、人力資源、採購庫存）之共享資料庫。幫助企業組織以最佳且有效率的方式管理其資源是 ERP 系統主要的業務(Noudoostbeni, Ismail, Jenatabadi, and Yasin 2010)。ERP 系統除了得到廣泛的應用，並提供了提高公司競爭優勢和市場占有率的有效性(Ketikidis, Koh, Dimitradis, Gunsekaran, and Kehajova 2008)。ERP 系統有利於企業徹底改善業務效率和效果，可說是任何大型的現代化企業組織的必備解決方案(Drobik and Rayner 2013)。

Wailgum (2009)調查近 400 位北美及歐洲的軟體決策者發現，在 2008 年全球經濟不景氣的情況下仍有三分之二的決策者積極投資 ERP 系統，包括從專案導入到系統擴展與升級。導入 ERP 系統雖有益於提昇競爭優勢及市場占有率，但學界與業界皆已發現 ERP 系統的導入仍存在許多問題與挑戰，例如時程延宕或預算超支等(Dezdar and Sulaiman 2009)。行動歐洲公司因其企業合作夥伴的反對，而棄置高額建置之 ERP 系統；美國應用材料公司(Applied Materials)因不堪負荷建置 ERP 系統所產生之組織變革，最後也放棄所採用之系統；北美億而富艾托化學公司(Elf Atochem North America)曾因企業併購過程中，各事業單位主要的 ERP 系統各自為政，互不相容之系統導致營運資料無法順暢傳遞，最後使得企業利害關係人無法及時做出營運決策(Davenport 1998)。另外，台灣廣運機械工程公司在導入 ERP 系統時，也曾因系統複雜性與教育訓練等問題，導致企業內部員工強烈的反彈（羅玳珊 2010）。由上述可知，導入 ERP 系統帶給企業相當顯著的益處，然而當系統為企業帶來組織效益時，相關風險亦同時存在(Poba-Nzaou, Raymond, and Fabi 2008)。因此 ERP 系統如同一把雙面刃，同時可能為組織創造價值與損失。

ERP 系統從計畫採用到實際上線維護的生命週期中，在企業流程設計、組織結構、系統、實務、文化與員工的態度等方面會引起變革(Gibson 2004)。企業中負責 ERP 系統導入的專案團隊多半缺乏此類系統的導入經驗，甚至有許多風險不是專案團隊所能控制的(Sherer and Alter 2004)。如何在 ERP 系統專案中妥善的控制風險，以符合時間、成本、品質的目標，是專案團隊與高階管理者面臨最大的挑戰。由於 ERP 系統紛紛被企業所導入，ERP 系統建置過程之相關風險因子也陸續被加以討論。以 ERP 生命週期而言，導入 ERP 系統前的主要風險包含系統選擇不當、不當的策略規劃、主要使用者參與程度低；導入中的主要風險包含無效的專案管理技術、缺乏訓練與指導、不當的變革管理；

導入後的主要風險為缺乏諮詢服務，與系統供應商之穩定性不佳(Aloini, Dulmin, and Mininno 2007)。

為了有效管理企業 ERP 系統生命週期所產生的風險，管理當局必須落實資訊治理等行動來加以因應。Van Grembergen and De Haes (2009)指出，資訊治理可視為公司治理的一部分，其治理的方式是藉由定義與建置一套合理的機制，來規範組織資訊的流程與管理架構，使管理當局與資訊人員可了解其權責，進而協助企業達到資訊策略整合與提升企業價值等目的。根據 Wilkin and Chenhall (2010)對於資訊治理的定義與分類中，風險管理是其中一項重要的類別。而資訊科技風險管理的範疇包含 IT 策略風險、資料正確性、使用者身分確認、系統安全性與災害復原等(Wilkin and Chenhall 2010)。因應資訊科技與組織變革的發展，企業需要擴展對風險管理的看法以涵蓋新的風險概念(Sherer and Alter 2004)。有效的風險管理制度可協助企業辨認及評估在日常營運過程中可能面臨的風險，並適當地回應風險（林寶珠與王敏馨 2003）。

Boockholdt (1987)認為風險分析技術的重要性建立在安全性和完整性控制。風險分析為風險識別過程，風險分析確已成為安全管理的相當重要的一環，資訊系統的安全性可避免不必要的損失和昂貴的控制措施(Baskerville 1991)。風險分析技術提供關鍵性預測經濟利益的一種投資手段，也就是說風險分析是在建立風險的貨幣價值(Gallegos, Richardson, and Borthick 1987)。相對的風險評估是暴露於風險的程度(Gallegos et al. 1987)，風險分析對於評估安全性非常有用，但它單獨不能形成一個完整的風險管理的基礎。因此本研究欲探究那些為 ERP 系統的風險因子，建構一風險管理機制，以利公司建立完整資訊安全策略之基礎。

保證安全性的有效需要實質性的確保，其中象徵性的確保(symbolic assurance)需要獲得利益關係人的信任和接受。COBIT 是資訊科技治理（information technology governance，簡稱 ITG）的架構，確保組織的政策、計劃、程序和結構設計可實現業務目標，並防止、偵測或改正非預期的事件(Wilkin and Chenhall 2010)。COBIT 為開發和評估技術密集型資訊系統的常用架構(Tuttle and Vandervelde 2007)。COBIT 亦為企業進行 IT 風險管理所採用的架構(Wilkin and Chenhall 2010; De Haes and Debreceny 2013)。此架構最初是 ISACA 的 ITGI (Information Technology Governance Institute)所開發和維護的 IT 最佳管理之實踐與基準，目前最新版本為第五版(ISACA 2012)，即為以下所稱 COBIT 5。

綜上，本研究欲探討與分析整個 ERP 系統在 COBIT 5 模式可能會在管理面上遭遇的不同構面之風險，進而評估風險項目提供管理階層選擇或制定適合的因應策略，並作為擁有 ERP 系統企業建立風險管理機制之評估參考。本研究期望從 COBIT 5 觀點建立完善的 ERP 系統風險管理機制，幫助企業及早辨認風險、評估其風險大小及優先順序並以適當的策略因應之。本研究首先透過文

獻探討，以 COBIT 5 管理領域為基礎，建構出 ERP 系統潛在的風險因子，再透過德爾菲專家問卷得到實務界的意見進行結果做修正，以建構出 ERP 系統風險管理機制。最後本研究則透過個案研究實證 ERP 系統風險管理機制的有效性。

貳、文獻探討

一、風險管理與程序

風險管理(risk management)在內部稽核協會（Institute of Internal Auditors，簡稱 IIA）網站定義為：「識別、評估、管理和控制潛在事件或情況的過程，目的是為實現組織的既定目標並提供合理保證」(IIA 2011)。風險管理認識到風險存在於所有組織中的這一個事實，因此，風險管理最大的挑戰就是將風險控制在組織偏好的範圍之內，也就是「將風險控制在組織願意接受的水平」。但擁有正確及完整的風險管理機制及收集風險資料，透過適當的風險監控作業，就能有效的降低風險發生的機率與其影響程度，讓整體組織資源的運用達到最佳化（張碩毅與吳承志 2008）。企業單位採取各種可行方法以認知、發現各種可能存在之風險，並衡量其可能發生之損失頻率與幅度，而於事先採取適當方法加以預防、控制，若已盡力預防控制仍難免發生損失時，則於事後採取財務填補措施以恢復原狀，以保持企業之生存與發展（鄭燦堂 2012）。

美國 COSO 委員會出版的企業風險管理－整合架構（enterprise risk management- integrated framework，簡稱 ERM）(COSO 2004)，將風險視為一個事項發生之可能後果，而該事項對達成企業目標會產生不利的影響。近幾年許多的風險管理機制應運而生，例如 PMI 2001、Standards Australia 1999、SAFE methodology、Risk Diagnosing Methodology，這些都是經典的循環性風險管理機制(Aloini et al. 2007; Aloini, Dulmin, and Mininno 2012a, 2012b)。表 1 彙總 Standards Australia (2004)、鄧家駒(2005)、Aloini et al. (2007, 2012a, 2012b)等可適用於 ERP 系統的風險管理程序，分別為風險辨認、風險評估、風險回應、以及監督與修正。

表 1　風險管理程序

風險管理程序	說明
1. 風險辨認	首先找出風險的來源，風險有許多不同來源如財務、技術、安全、資訊、人員、企業流程、管理、外部及成功的風險。
2. 風險評估	風險具有獨特性且無法完全消除，依據過去發生損失發生紀錄及詳細損失資料，利用機率理論或統計技術，預測發生相關風險、事故機率、幅度及對企業的影響。
3. 風險回應	依風險對企業影響大小與優先順序，透過成本與效益比較分析選定風險因應的最佳策略，以達成風險管理目標。
4. 監督與修正	風險的特性是變動，因此需定期加以評估檢討並修正風險管理策略。

風險因子、關鍵成功因素和不確定因子常被用來傳達相同的意思(Aloini et al. 2007, 2012a, 2012b)，也有很多不同的管道可以用來描述與分類風險(Baccarini, Salm, and Love 2004)，因此風險辨認對於管理階層來說是一挑戰，同時資訊人員也需要以更廣泛的角度來看待系統的潛在問題，包含流程內所有可能的人員和部門(Aloini et al. 2012a, 2012b)。以 ERP 系統生命週期而言，從導入前的 ERP 系統選用、導入 ERP 系統間的運作到 ERP 系統導入後之控管，所產生的風險包含系統選擇不當、專案團隊能力不足、高階主管參與程度不高、主要使用者參與程度低、缺乏訓練與指導、不當的企業流程再造、缺乏管理性之指引、無效的專案管理技術、不當的變革管理、缺乏諮詢服務、系統供應商之穩定性不佳與不當的策略規劃。風險評估即為辨認上述風險因素並予以分析、考量其發生之可能性及影響的過程，決定風險如何管理等(COSO 1992)。其主要目的在於透過列舉企業所面臨的潛在威脅與弱點藉以決定企業所面臨的風險值。

企業風險管理不是嚴格的順序過程，一個組成要素不只是影響下一個組成要素。它是一個多方向，且反覆進行的過程，任一個組成要素都必須存在而且運作順利，才能使其發揮作用。風險管理必須隨著時間與環境的變遷來適度修正風險管理的策略，因此在成效考核與回饋上，必須提供決策者重要的指標以作為是否修正策略的依據（鄧家駒 2005）。ERP 系統串連整個企業功能，疏於管理其風險將很可能會導致企業體損失。此外 ERP 專案失敗最常見的理由就是管理階層沒有做好其風險評估與管理 (Wright and Wright 2002; Sherer and Alter 2004)。因此 ERP 系統的風險管理實為整個企業營運的重要關鍵之一。

此外企業應該要有較為健全的 IT 內部控制以防止舞弊並且偵測錯誤，以降低企業的 IT 風險及其對企業未來可能造成的損失。COBIT 的設計用於組織管理的基準測試工具，包括相關的 IT 控制的最佳實踐。COBIT 其強大的控制促使內部和外部稽核應用 COBIT 作為財務報表稽核以及營運及遵循性稽核重點。管理階層應使用 COBIT 控制架構進行財務報表稽核，以評估其 IT 內部控制的有效性(Tuttle and Vandervelde 2007)。因此企業透過了解資訊系統的風險以及弱點，企業應進行 IT 內部控制的動作以確保其資訊系統安全具有正確的管理，使得組織擁有的資產，甚至涉及個人隱私的資料都能夠受到保護（張碩毅、黃士銘、阮金聲、洪育忠與洪新原 2005）。本研究認為透過 IT 控制的強化得以實現 ERP 系統風險管理的程序。

二、風險管理的標準與規範

風險管理相關的標準以及規範包括企業風險管理的整合架構(COSO ERM)考量企業內一般性風險管理所需要參考的環境要素；ISO/IEC 31000 風險管理的指導原則與綱要，了解風險管理的原理、架構及過程；ISO/IEC 27005 以及 ISO/IEC 27001 標準的探討，了解資訊風險管理的重要性，組織不論在建置 ISMS

時的風險管理程序或是在資訊安全方面透過 ISO/IEC 27001 得知相關的控制領域及控制目標(ISO/IEC 2005b; ISO/IEC 2011)；COBIT 5 則為一套基於企業資訊科技治理的完整性架構。另外，由於 COSO ERM 是一個高層次的概念性架構，主要著重於組織之治理面，關於 IT 控制目標和相關活動較沒有提供詳細的標準。而 COBIT 5 架構中除了包含組織治理等流程外，並提供 IT 管理之四大領域（調整、規劃與組織；建立、取得與導入；交付、服務與支援；監控、評估與衡量）的詳細流程(De Haes and Debreceny 2013)。管理領域是在治理領域監督下的運作結果，並進行管理回饋。另一方面，ISO/IEC 27000 系列標準（ISO/IEC 27001 與 ISO/IEC 27005）則強調 IT 管理面之內容，對 IT 治理面的規範則較無著墨。而 ISO/IEC 31000 雖有制訂治理面的流程，但在管理面則僅著重於調整、規劃與組織領域的流程(ISACA 2012)。綜上所述，相較於其他標準，COSO ERM 的原則性較高。但 COBIT 5 除了可補足 COSO ERM 所欠缺之詳細流程外，也強化 ISO/IEC 系列標準對於其他領域流程之內容。表 2 整理與風險管理相關的標準及規範之發表年份與主要概念及目的。

表 2　風險管理標準及規範

標準及規範	年份	概念及目的
COSO ERM	2004	幫助組織在訂定出自身的策略及目標之後，辨認出可能會對組織目標產生影響的種種情事。幫助企業衡量以及判斷這些影響組織達成目標的風險，並且評估風險所帶來的威脅，進而做出適當的回應。
ISO/IEC 27001	2005	幫助組織降低資訊安全事件所造成的傷害，並預防潛在危害，主要是組織在建置資訊安全管理系統（information security management system，簡稱 ISMS）的規範及要求。
ISO/IEC 31000	2009	目的在於提供風險管理的原則及指導綱要，予以不同類型、規模的組織管理整體或個別專案之風險」。
ISO/IEC 27005	2011	主要規範組織在制定 ISMS 時必須遵循的風險管理的程序，確保組織資訊資產遭受攻擊時，能即時維護資訊系統並保持系統正常運作及資訊系統資料合法存取，可幫助組織導入資訊科技的風險管理，有效解決資安方面問題。
COBIT 5	2012	透過應用資訊科技提供所有必要的程序和促成的因素(enablers)來幫助企業價值創造，因為不同的企業有不同的目標，企業可以透過各層級的目標(goals cascade)，自行定義 COBIT 5 以適合本身企業全景的情況，將高層次的企業目標轉化成容易管理的並特定與 IT 相關的目標將它們對應到特定的流程以及實務上。

根據 ISACA (2008)針對全球電腦稽核協會的會員所進行的線上調查結果分析，企業在日常營運中所面臨的前兩項重要問題，為企業在當地法規的遵循以及企業在 IT 管理／資訊科技治理機制的建立。ITG 是確保 IT 策略與企業策略間得以聯結，透過開發和維護一個有效率的 IT 控制與責任機制、績效管理和風險管理來最大化企業的價值。在 ITG 機制與公司治理機制同時有效率的運作下也可以強化企業管理者的責任(Kaarst-Brown and Kelly 2005)。過去文獻已有探討 ITG 的方法。Bin-Abbas and Bakry (2014)提出了 50 項 ITG 的控制項目來進行 ITG 評估。該方法可使組織發現其 ITG 的主要優勢和弱點，並找到未來治理的發展方向。

為了有效地利用 IT，很多的國家和國際組織已頒布多項 ITG 的建議文件。關鍵文件包括：ISACA 的“COBIT: Control Objectives for Information and Related Technologies” (Bakry and Alfantookh 2006; ISACA 2012); 英國的政府商務辦公室（Office of Government Commerce，簡稱 OGC）的“ITIL: Information Technology Infrastructure Library”(Alfantookh and Bakry 2009; Cabinet Office 2011)；與 IT 服務管理標準“ISO/IEC 20000” (ISO/IEC 2005a)；IT 治理的原則相關的標準“ISO/IEC 38500” (ISO/IEC 2008)；IT 治理“MIT: Massachusetts Institute of Technology” (Weill and Ross 2004)。這些對 ITG 的評估建議支持組織計劃和未來的改進成果。

在控制制度之下不可缺少的一環就是 IT 與 IS 控制的概念，為了強化 IT 與 IS 控制之遵循，其中最為廣泛使用之架構為 ISACA 所制定的 COBIT。根據 ITGI 指出：「COBIT 是唯一能夠提供 IT 投資全生命周期的一個管理框架。這個框架能支持 IT 商業目標的完成、確保商業 IT 定位、並且能夠提高 IT 效率與有效性。」這個 COBIT 流程的模型是一個完整的、綜合的模型，但是它並不是唯一可能的流程模型。ISACA 認為使用 COBIT 5 這個流程參考模型的公司須考慮到本身的情形，來定義與企業本身符合的流程集合。結合企業在 IT 活動所涉及的所有運作模式是邁向良好管理的關鍵步驟。COBIT 被倡導為以 IT 程序、IT 領域、資訊準則和 IT 資源為基礎之流程內控理論。由於 COBIT 與 IT 有關，且經過不斷的發展，其已成為組織執行 IT 控制重要的參考架構(Tuttle and Vandervelde 2007)。

強大的 IT 可提高組織績效(Melville, Kraemer, and Gurbaxani 2004)。管理階層應使用 COBIT 控制架構進行稽核，以評估其內部控制的有效性。建構 IT 控制理論有三個因素須考量：(1)資訊的可靠性、保密性和完整性以有效的方式體現資訊的品質；(2)IT 程序考量與控制高度相關，也就是有效的遵循法律、法規和契約是受到人和擁有必要的資料所影響的；(3)稽核的考慮與 IT 設計（如應用和基礎建設）相關，進而確保業務資訊的可用性(Tuttle and Vandervelde 2007)。也就是資訊的品質、資訊處理和系統設計過程直接影響內部控制的有效性。

稽核的風險可分為固有風險、控制風險和偵測風險。如果有效性內部控制的施行是可能緩解財報發生重大錯誤之風險。為了減少在 IT 環境中的稽核風險，會計師應對 IT 的控制有清晰透徹的了解(Huang, Hung, Yen, Chang, and Jiang 2011)。就查核的觀點，如資訊科技之控制可維護資訊之完整性及系統所處理資料之安全性，且包含有效之一般控制（IT general controls）及應用控制（IT application controls）；即使資訊科技之控制可能不會直接影響組織中之財務活動，或許仍將對組織中財務報導的一致性和有效性產生正面的影響。美國公開發行公司會計監督委員會（Public Company Accounting Oversight Board，簡稱 PCAOB）在審計準則第 2 號（Auditing Standard No. 2，簡稱 AS2）指出，當 ITGC 是有效時透過 IT 自動化的應用可以幫助提高稽核的效率。

企業高度依賴 IT 以確保營運可靠和可信賴。為了證明和報導企業內部控制結構和程序管理評估，對管理階層來說以遵循 COBIT 5 架構以評估自身 IT 控制的有效性。就 ERM 的本質來說，它是一個概念性的框架且沒有提供關於 IT 控制目標和相關活動的詳細標準。但是 COBIT 已被廣泛接受為一個可靠和全面的架構來管理風險和 IT 控制，並列示企業為了實現其相關控制目標時，IT 的程序應如何傳遞資訊(Coe 2005; Reghavan 2006)。

目前 ERP 系統高建置比率反映出實行 ERP 系統風險管理的重要性與必要性，本研究認為採用 COBIT 5 架構中的「管理」關鍵領域對於目前 ERP 系統可能產生的風險，相較於過去的規範及標準，能有不一樣的方式達成 ERP 系統的風險管理，甚至對於風險達到更有效的管理與控制。有別於 COBIT 5 架構中的治理領域，管理領域中的流程，包含企業層級 IT 活動的計畫、建立、營運與監督之職責。期望透過 COBIT 5 架構強化 IT 與 IS 的控制制度，更強調本研究以 COBIT 5 架構為基礎建構 ERP 系統風險管理機制的重要性。

參、研究設計與方法

本研究運用 Gowin's Vee 模型建立研究的流程(Gowin 1981; Novak and Gowin 1984)如圖 1 所呈現，在理論端透過文獻探討方式建構出衡量 ERP 系統風險管理機制之雛型；實證端則先採用德爾菲法專家問卷，為確保及提高各衡量構面與項目的內容效度(content validity)，運用發放專家問卷取得學界與業界專家意見，以 Lawshe (1975)所提出的內容效度指數（content validity ratio，簡稱 CVR[1]）方法及驗證過程，針對各衡量領域、流程與項目指標進行篩選的動作，以萃取適合衡量 ERP 系統風險管理項目，最後輔以個案研究法來確認 ERP 系統風險管理機制的有效性，建構完成以 COBIT 5 為基礎之 ERP 系統風險管理機制。

本研究運用德爾菲法的流程共包括：(1)成立專家小組、(2)設計專家問卷、(3)發放問卷給專家小組、(4)針對專家問卷進行分析歸納、(5)若各問項未達一致性，則重新發放問卷、(6)產出結論報告。德爾菲法是請求專家提供專業知識、經驗及意見，經由多回合的問卷發放與回饋意見控制，以取得一群專家對特定議題共識的一種研究方法(Dalkey and Helmer 1963; Delbecq, Van de Ven, and Gustafson 1975; Linstone and Turoff 1975; McKenna 1994)。

[1] CVR 為判定題項「符合」與「不符合」的實際專家人數與期望值之差，佔期望值的百分比數。

$$CVR = \frac{n_e - (N/2)}{N/2},$$

n_e：對於某一特定題項，評斷該題為「符合」及「不符合」的人數。

N：所有專家人數。

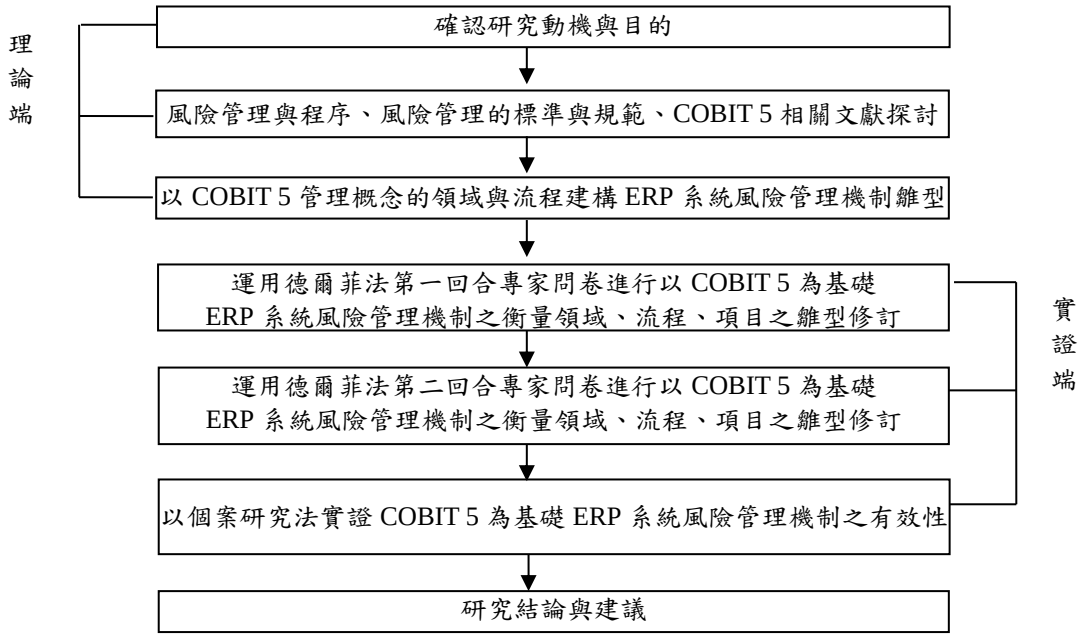

圖 1　研究流程

本研究以某個案公司為研究對象進行深度研究，訪問對象包括該公司以下人員：(1)總經理、副總經理（非必要）、(2)資訊長、ERP 系統負責人、或相關之主管、(3)負責執行 ERP 系統之專案成員。藉由在公司現場蒐集到企業實際運作的初級資料為主、次級資料為輔，進行資料之蒐集、分析與整理。初級資料方面將透過直接觀察、實際深度訪談的方式進行蒐集。次級資料將與公司產業相關之研究或資料、書面文件等予以彙整、歸納與分析，同時蒐集與本研究設計之 ERP 系統風險管理機制相關之資料。將個案公司的訪談結果與個案公司所提供的建議，在歸納整理後對本個案研究撰寫相關之結論。個案研究執行步驟如下：

- 設計本研究機制之說明手冊，在進行個案訪談前先請個案公司（多位人員）實際地檢視和使用本研究機制。
- 建置一套個案研究準則，此個案研究準則內容主要包含專訪函、資料蒐集、研究概述、COBIT 5 為基礎的 ERP 系統風險管理機制以及訪談內容共五個部分，並透過此準則與個案公司相關人員進行深度訪談。
- 研讀與個案公司產業相關之文獻與公司基本資料、組織發展情形。
- 透過與個案公司人員實際接觸，取得個案公司重大事記表、組織架構圖、業務狀況以及未來發展計畫等相關資料。
- 藉由與個案公司相關人員訪談的方式，評估本研究之風險管理機制於實務界的有效性，以及在 ERP 系統的風險管理上有何幫助。

肆、以 COBIT5 為基礎之 ERP 系統風險管理機制

本研究在文獻蒐集的過程以下列條件：(1)與內部控制或資訊安全風險管理有關之文獻；(2)內部控制或風險管理相關的議題、法規或標準有關之文獻；(3)其他對於本研究有幫助之文獻。最後以國內與國外共 10 篇文獻進行相關編碼（如表 4 之註 1 所列示）。

本研究利用德爾菲方法來檢驗由文獻歸納出之 ERP 系統的風險管理之雛形是否合理，並取得專家們的一致意見。德爾菲法專家挑選原則為工作內容與 ERP 系統的風險管理有關，本研究德爾菲專家小組為 14 位。德爾菲專家問卷主要目的在於確認適合用來衡量 ERP 系統風險管理的控制項目有哪些、以及確認控制項目是否正確歸類至 COBIT 5 應有的領域與流程內。故問卷設計以邏輯判斷為主並輔以空白處使專家能充分表達意見。

問卷將會進行反覆的詢問，直到專家們達成共識為止，目的是希望能透過專家們不斷的討論，以取得較完善的需求項目。第一回合德爾菲專家問卷將透過專家來決定問項歸類正確且適合用來當作 ERP 系統風險管理控制項目。第二回合專家問卷係為處理第一回合專家意見分歧部份，讓專家建立共識，再次確認以 COBIT 5 為基礎之 ERP 系統風險管理機制。兩回合問卷以電子郵件夾帶檔案方法與回收，問卷回收後之一致性檢定，以 CVR 值(Lawshe 1975)檢定內容效度，以及 Holden and Wedman (1993)提出之四分位差檢定專家意見離散程度，並以兩種檢定值採最嚴格之「聯集」檢定標準[2]。以下就研究雛型發展及德爾菲法之驗證過程分別說明。

一、研究雛型發展

首先依過去風險因子(risk factor)相關文獻整理與彙總出 53 項風險因子（如表 4），依照 COBIT 5 的流程參考模型中「管理」概念所包含的四個領域作為分類構面（表 3 為 COBIT 5 管理領域四大構面之介紹），分別將 53 項風險因子分類，例如風險因子：「4.安全措施的效果不佳」，符合 APO 領域下「擬定資訊環境架構」的概念，因此將此風險因子分類至「調整、規劃與組織(APO)」的構面，並給予此風險因子編號：「APO.1 安全措施的效果不佳」，其餘風險因子的分類方式，依此概念進行（如附錄 1）。

[2] CVR最小值：5人，0.99；10人，0.62；14人，0.51；15人，0.42。
四分位差(Q)：Q ≤0.6，高度一致性；0.6< Q ≤1.0，中度一致性；Q>1.0，未達一致性。

表 3　COBIT 5 管理領域四大構面之介紹

構面（構面描述）	流程
1.調整、規劃與組織（align, plan, and organize，簡稱 APO）：本構面作業程序包括：擬定策略性資訊技術規劃、擬定資訊環境架構、決定技術方向、釐定資訊組織及其關係、專業的投資管理、溝通管理目標與方向、人力資源管理、確保符合外部需求、風險評估、風險管理、專案管理及品質管理等。並提供傳送解決方案和服務的方向。	APO01 定義與管理 IT 管理標準。
	APO02 定義管理策略。
	APO03 管理企業架構。
	APO04 管理創新。
	APO05 管理投資組合。
	APO06 管理預算與成本。
	APO07 管理人力資源。
	APO08 管理關係。
	APO09 管理服務契約。
	APO10 管理供應端。
	APO11 管理品質。
	APO12 管理風險。
	APO13 管理安全。
2.建立、取得與導入（build, acquire, and implement，簡稱 BAI）：本構面作業程序包括：確認自動化解決方案、應用軟體獲得及維護、技術架構的獲得及維護、科技基礎建設的取得及維護、開發及維護資訊程序、安裝及認證系統及變更管理等。並提供解決方案並將其轉成服務 項目。	BAI01 管理計劃與專案。
	BAI02 管理需求定義。
	BAI03 管理解決方案和規劃組織。
	BAI04 管理可用性和能力。
	BAI05 管理組織變革。
	BAI06 變更管理。
	BAI07 管理變更的驗收與過程。
	BAI08 管理知識。
	BAI09 管理資產。
	BAI10 管理組態設定。
3.交付、服務與支援（deliver, service, and support，簡稱 DSS）：本構面作業程序包括：定義及管理服務層級（等級）、外包服務管理、績效及容量的管理、確保持續性的服務、確保系統安全、分析及分配成本、使用人員的教育訓練、客戶支援（協助）及諮詢、系統設定管理、問題及異常事件的管理、資料管理、硬體設施管理、知識管理、操作管理等。並接收解決方案並轉換成對終端使用者有用的活動。	DSS01 管理服務水準。
	DSS02 管理第三方服務。
	DSS03 管理問題。
	DSS04 管理持續性。
	DSS05 確保系統安全。
	DSS06 確認企業流程控制。
4.監控、評估與衡量（monitor, evaluate, and assess，簡稱 MEA）：本構面作業程序包括：監督各項資訊流程、評鑑內部控制的允當性、是否有獨立之品質保證、提供獨立的稽核、監督與評估系統內部控制、監督與評估是否有遵循外部需求、監督與評估績效與一致性。並監控所有的流程，來確保所有的程序都確實進行。	MEA01 監控、評估與衡量資產績效。
	MEA02 監控、評估與衡量系統內部的控制。
	MEA03 監控、評估與衡量外部規定的遵循。

註：資料來源：ISACA (2012)。

第二步，探討此風險因子「4.安全措施的效果不佳」可能含括在 COBIT 5 的「管理」概念(APO、BAI、DSS 及 MEA)的 32 個流程中。舉例來說：「4.安全措施的效果不佳」本研究認為可能引起此風險所涉及的流程為：「APO01 定義與管理 IT 管理標準」與「DSS05 確保系統安全」。

第三步，在 COBIT 5 的「enabling process」手冊中，為這 32 個流程之下訂定了 195 個控制目標。舉例來說：在 APO 的 APO01 流程之下，分別定了 8 個控制目標，分別為：(1)APO01.01 定義的組織結構；(2)APO01.02 建立角色和責任；(3)APO01.03 維護管理系統的實現；(4)APO01.04 溝通管理的目標和方向；(5)APO01.05 最佳化的 IT 運作的位置；(6)APO01.06 定義資訊（數據）和系統的所有權；(7)APO01.07 管理持續改進的過程；(8)APO01.08 保持遵守政策和程序。

依照本風險因子「4.安全措施的效果不佳」，與之相關流程為「APO01 定義與管理 IT 管理標準」與「DSS05 確保系統安全」，因此，在 APO01 流程下參考 COBIT 5 標準，得出控制目標為 APO01 之下的「APO01.08 保持遵守政策和程序」與 DSS05 之下的「DSS05.02 管理網絡連接的安全性」、「DSS05.03 管理端點安全性」。因此得出在「4.安全措施的效果不佳」風險之下的控制目標分別為：「APO01.08 保持遵守政策和程序」、「DSS05.02 管理網絡連接的安全性」與「DSS05.03 管理端點安全性」，本研究給予這三項控制目標編號：「APO.1.1 保持遵守政策和程序」、「APO.1.2 管理網絡連接的安全性」與「APO.1.3 管理端點安全性」。

第四步在確認此風險因子「4.安全措施的效果不佳」的分類構面以及得出相關之流程和流程的控制項目（目標）後，需找出在這些對應的控制目標下，針對組織內角色與職能給予適當的責任分配，因此，最後根據控制項目（目標）的文獻來源，參照 COBIT 5: enabling processes 分別歸屬控制項目的 26 個組織內角色和職能。著重在風險因子發生對應的流程與其控制項目（目標）；並根據控制項目（目標）的文獻來源，也可參照 COBIT 5: enabling processes 手冊，了解其控制項目的 26 個組織內角色和職能歸屬。

重複以上步驟分別將表 3 經文獻探討所得 53 個風險因子，以 COBIT 5 為基礎分析歸納影響流程及控制項目（目標）並重新編碼。附錄 1 為本研究之 COBIT 5 為基礎的 ERP 系統風險管理機制之雛形，在 APO 構面下包含 20 個風險因子、BAI 構面含 18 個風險因子、DSS 構面含 9 項風險因子與 MEA 構面的 6 項風險因子，共 53 項風險因子，其流程之控制目標共為 136 項。

表 4　ERP 系統風險因子彙整

風險因子	文獻[1]	A	B	C	D	E	F	G	H	I	J
1.	輸入錯誤或是竄改的資料	◎				◎		◎			
2.	經授權的使用者誤用	◎				◎	◎				
3.	不受管束或未經授權的系統存取	◎				◎	◎				
4.	安全措施的效果不佳	◎				◎	◎				
5.	IT 內部的程序錯誤	◎									
6.	程序與控制	◎	◎		◎	◎		◎			
7.	儲存媒體的處理	◎									
8.	程式錯誤	◎	◎			◎		◎			
9.	作業系統的瑕疵	◎			◎	◎					
10.	通訊系統或伺服器的損壞	◎			◎	◎					
11.	意外的故障	◎				◎	◎				
12.	故意的行為	◎									
13.	缺乏交易軌跡	◎					◎				
14.	職責集中化：職能有無分工	◎			◎	◎	◎	◎			◎
15.	難以整合各個部門			◎							
16.	交易由電腦自動產生或執行	◎				◎					◎
17.	人工控制依賴電腦控制							◎			
18.	缺乏持續的溝通			◎	◎				◎	◎	◎
19.	缺乏外部顧問			◎	◎				◎		◎
20.	無法將使用者需求轉換成技術需求或快速滿足使用者需求	◎		◎			◎	◎			
21.	與舊系統整合之挑戰			◎							
22.	缺乏充分的訓練規劃		◎	◎					◎		◎
23.	大範圍的組織變化				◎						
24.	技術人員的效能問題			◎	◎						
25.	喪失版本更新之控制								◎		
26.	難以衡量績效與效益								◎		
27.	難以持續評估新的技術				◎						
28.	不合邏輯的處理							◎			
29.	科技的誤用				◎			◎			
30.	使用者涉入不足		◎	◎	◎				◎	◎	◎
31.	流程再造的問題		◎		◎				◎		◎
32.	ERP 系統沒有符合營運流程		◎	◎	◎					◎	◎
33.	不適合的科技任務		◎								
34.	資料轉換				◎						
35.	缺少適當方法論				◎						◎
36.	沒有適當規劃			◎	◎						
37.	人力資源政策未改變			◎	◎						
38.	缺少有效率之專案管理技術			◎	◎						◎
39.	缺少高階管理者支持			◎	◎				◎		◎
40.	基礎建設不足			◎	◎						◎
41.	公司現有文化				◎						
42.	組織現有結構問題				◎						
43.	沒有辦法快速回應							◎			
44.	無法驗核處理過程							◎			
45.	供應商問題			◎					◎	◎	◎
46.	現有系統準備變革程度								◎		◎
47.	團隊組成不穩定			◎	◎						◎
48.	缺乏通訊基礎建設			◎	◎						◎
49.	資源不足			◎	◎						
50.	無法支援資料整合之跨組織設計			◎							
51.	缺乏資料庫基礎建設			◎	◎						◎
52.	人員任用不適當			◎							
53.	試圖與舊系統結合			◎							

註：A: Musaji (2002); B: Wright and Wright (2002); C: Huang, Chang, Li, and Lin (2004); D: Sherer and Alter (2004); E: 行政院研究發展考核委員會(2009); F: 陳錦烽(2006); G: 張碩毅等 (2005); H: Aloini et al. (2007); I: Bannerman (2008); J: Hakim and Hakim (2010)。

二、以德爾菲法修正研究雛型

本研究在初步確認以 COBIT 5 為基礎的 ERP 系統風險管理機制的雛型之後，將採用美國蘭德公司(Rand Corporation)所提出的方法及驗證過程，透過發放德爾菲問卷的方式，取得學術界與產業界等專家們的意見與共識，進行本雛型機制的篩選與修正。德爾菲法能夠透過多回合的問卷調查整理出一致的專家意見，且其匿名性可以解決面對面討論或會議方式產生的困難，讓專家可以在互不影響的狀況下提出正確的建議。修正本研究機制雛型的風險項目、控制目標，以增強本研究未來在實務上的貢獻。

本研究專家小組的成員以企業資源規劃系統領域與企業風險管理顧問的從業人員為主，亦邀請於大專院校之教授或研究領域於 ERP 系統及風險管理相關的學者參與。將研究機制雛型以 E-mail 夾帶檔案的形式發放，並藉由填答者直接回覆信件的方式取得填寫後資料。專家小組人數一般以 10 至 50 人為宜，最佳人數為 15 人左右(Linstone and Turoff 1975)。本研究共選取專家 14 位，其中在各中小企業及政府機構資訊相關部門專家共 6 位；資訊顧問、會計師事務所之專家共 6 位；來自學術界之專家共 2 位；其中偏向 ERP 系統使用者之專家共 8 位；偏向 ERP 系統及企業風險管理顧問之專家共 6 位，而此 14 位專家之工作年資及使用 ERP 系統年資約為 11 年。表 5 為專家之背景資訊。

表 5　專家資料

專家類別	編號	服務機構	職稱	年資
ERP 系統使用者端之專家	1.	製藥業	副部長	14
	2.	製造業	副理	12.5
	3.	光電產業	經理	9
	4.	半導體製造業	稽核室主任	10
	5.	光電產業	副理	7
	6.	政府機構	科長	10.5
	7.	教育服務業	教師	7.5
	8.	教育服務業	助理教授	3.5
ERP 系統及企業風險管理顧問端之專家	9.	會計師事務所	顧問	2
	10.	會計師事務所	協理	11
	11.	資訊顧問業	經理	32
	12.	電腦軟體服務業	資料庫管理人員	6.5
	13.	企業經營管理顧問業	顧問師	12
	14.	資訊服務業	經理	15

第一回合問卷實施時間自 2013 年 4 月 8 日開始，並於同年 5 月 3 日完成所有問卷之回收。德爾菲專家問卷目的為篩選出 ERP 系統之風險因子與 COBIT 5 管理下的四大構面之間的配適程度，及決定針對此風險因子之控制項目的重要程度。藉由專家之經驗及專業知識確認該衡量項目是否適合當作 ERP 系統風險管理衡量項目，故衡量尺度設計為「適合」或「不適合」的邏輯選項；進而確認該衡量項目對於 COBIT 5 的歸類（包括四大領域及其流程）是否合適，故衡量尺度亦為是與否之邏輯判斷，但為了能更準確將項目歸類，另設計文字欄位，提供專家做建議模組、建議流程等意見交流。

第一回合的德爾菲法問卷分成三段階段檢視其結果，首先第一階段專家內容效度部分，根據第一回合德爾菲專家問卷在「適合程度」上的填答結果，共 53 個題項所計算出來的 CVR 值，除了「APO.3 故意的行為」此一題項未達標準值 0.51 以上之外，其餘題項皆在標準 0.51 以上，即專家對於 ERP 系統環境下的風險因子歸類至 COBIT 5 的四大構面的適合程度表達高度同意。

第二階段篩選該項目是否適合當作衡量 ERP 系統風險管理之項目，結果顯示共有 18 個控制項目未符合四分位差小於 0.6 或標準差小於 1 的標準（如附錄 1）；四分位差皆大於 0.6 分別為：「APO.3.2 建立一個測試的環境」、「APO.3.3 監測與安全相關事件的基礎設施」、「APO.4.2 執行控制的自我評估」、「APO.10.1 定義組織結構」、「APO.10.2 了解企業的發展方向」、「APO.13.1 了解企業的發展方向」與「APO.15.1 定義一個可參考的架構」、「BAI.2.1 定義和維持業務功能和技術要求」、「BAI.6.2 管理關鍵的資產」、「BAI.7.2 建立和維護一個如何配置的知識庫和基準」、「BAI.11.3 加入控制活動至業務流程中以符合企業目標」與「BAI.14.1 建立組織變革的意願」、「DSS.3.2 定義業務連續性的政策、目標與範圍」；標準差大於 1 分別為「APO.10.2 了解企業的發展方向」、「APO.12.2 培育並促進知識共享的文化」、「APO.13.1 了解企業的發展方向」、「APO.15.1 定義一個可參考的架構」、「APO.15.2 建立一個有利於創新的環境」與「APO.19.2 識別和記錄目前的資產」、「DSS.4.1 設備的管理」、「MEA.1.1 確認和評估供應商關係和合約」，將於第二回合問卷提出討論。

最後一階段其他專家於空白處填寫之意見（如下表 6）也將於第二回合專家問卷提出討論。因專家提出對於該項目的建議內容可能會影響其他專家之判斷，或其它專家提出應加入之衡量項目，故將請專家閱讀其他專家之意見進行再次確認。

第二回合專家問卷的「詳加敘述風險因子，並且重新分類至本構面之項目」、「詳加敘述風險因子，並再次確認之項目」、「類似概念的風險因子合併後，再次確認之項目」三大部分。本次專家問卷目的乃針對專家於第一回合提出之建議與統計彙總成果，再次確認專家之意見。第二回合共發出 14 份問卷收回 14 份，回覆率 100%。預計刪除項目之部分，針對在第一回合未達專家內容效度檢定的項目「APO.3 故意的行為」，第二回合專家意見相當一致，皆認為此

一題項不適合作為以 COBIT 5 為基礎的 ERP 系統風險管理機制下的風險因子項目，因此予以刪除。

表 6　專家意見彙整

項目	專家意見
APO.1	●資安措施非 ERP 的管理範圍。
APO.3	●風險控制無法考慮舞弊項目，其中故意的行為就是一種舞弊的行為。任何控制目標無法以防弊為目的，因為舞弊行為無可預期。 ●故意的行為沒辦法預先規劃。雖可預先防犯，但無法全面事先規劃完善。 ●故意的行為此風險名稱不夠明確。 ●通常風險不會故意發生。
APO.4	●此風險因子的定義不清，不了解何謂職責集中化之職能有無分工？會造成何種風險？
APO.8	●效能是較屬於評估方面的問題，組織可規劃、調整人才需求，但效能的發揮與否要再評估後才可了解。
APO.10	●與 APO.16 組織現有結構的問題重覆。
APO.11	●在規劃階段就已經評定不適合，對於科技任務的定義是否不夠客觀？ ●風險因子敘述與控制項目不明確。
APO.12	●當選定某 ERP 系統時就會運用該產品所推薦的方法論。
APO.13	●此風險因子名稱不夠明確。 ●公司沒能力也會找顧問公司來規劃。
APO.15	●公司文化是由經營階層所建立，若非經營階層主動提出，實務上應該不會在 ERP 系統導入專案來討論改變公司文化問題。
APO.17	●風險因子敘述與控制項目不明確。 ●供應商關係管理屬管理議題，與 ERP 無關。
APO.18	●風險因子敘述與控制項目不明確。
APO.19	●此風險因子名稱不夠明確。 ●風險因子敘述與控制項目不明確，資產與資源區別為何?
APO.20	●與 APO.14 人力資源政策未改變重覆。
BAI.1	●一般錯誤皆可回復後改正。
BAI.2	●內部程序是組織內部規劃的問題？還是當 IT 的部份就內部程序而言是建立的問題？
BAI.3	●此風險因子名稱不夠明確。 ●內部程序是組織內部規劃的問題？還是當 IT 的部份就內部程序而言是建立的問題？
BAI.5	●屬於控制環境的項目。 ●作業系統與 ERP 系統內容無關。 ●風險因子敘述與控制項目不明確。
BAI.6	●風險因子敘述與控制項目不明確。 ●非關 ERP。
BAI.7	●風險因子敘述與控制項目不明確。 ●非關 ERP。
BAI.8	●比較類似是組織的變更管理是嗎？ ●風險因子敘述與控制項目不明確。
BAI.9	●題意不清。 ●風險因子敘述與控制項目不匹配。 ●無 ERP 維護合約不影響 ERP 運作，除非該公司沒有聘顧適當的 IT 人員。
BAI.11	●比較類似是組織的變更管理是嗎？
BAI.12	●比較類似是組織的變更管理是嗎？
BAI.15	●風險因子敘述與控制項目不明確。
BAI.17	●風險因子敘述與控制項目不匹配。
BAI.18	●ERP 導入應捨棄舊系統。
DSS.1	●不影響 ERP 導入。
DSS.2	●授權是經規劃與建立的。
DSS.3	●交易的軌跡是經規劃與建立的。
DSS.4	●交易由電腦自動產生時，風險何在？
DSS.5	●定義不清。 ●理論上人工的錯誤應高於電腦（除非在規劃階段設定錯誤），不理解此風險因子的意義。
DSS.7	●風險因子敘述與控制項目不明確。
DSS.8	●資料轉換此名稱不像是風險因子。
MEA.2	●不相關。
MEA.3	●績效衡量為 ERP 導入後議題, 非關 ERP 本身風險。

第二回合結果顯示修正過後風險因子的編號「作業系統的瑕疵而影響 ERP 系統運作」，此風險因子之 CVR 值為 0.43，未達此最低標準。表 7 彙總「作業系統的瑕疵而影響 ERP 系統運作」不適合之專家意見。

表 7 「作業系統的瑕疵而影響 ERP 系統運作」風險不適合之專家意見

專家編號	專家意見或建議	本研究處理方式
2.	目前作業系統的成熟性都很高，不覺得是風險項目。	彙總四位專家之意見，認為作業系統的問題需在 ERP 系統取得前就須確認，且目前作業系統成熟性夠高，因此本研究採用專家意見，將此風險因子及其控制項目剔除。
3.	ERP 廠商在產品出貨前就應確認相容性。	
5.	BUG 可修正。	
7.	取得 ERP 系統前，本就應先考慮自身原有的作業系統。	

在第二回合德爾菲問卷針對風險因子所對應的控制項目進行一致性的檢定，共 7 項控制項目，其四分位差大於 0.6 僅為中度一致性或是其標準差大於 1 而未達專家的一致共識，針對這些控制項目，各專家之意見及本研究處理方式整理如表 8，使本機制成為具有表面效度與內容效度之以 COBIT 5 為基礎之 ERP 系統風險管理機制。

表 8 專家之意見及本研究處理方式

專家編號	控制項目	專家意見或建議	本研究處理方式
5.	APO.15.2 建立一個利於創新的環境。	公司文化非一朝一夕可改變，ERP 導入不需將「人」的問題納入考慮，請企業指派適當人選即可。	認同該專家之看法，修正控制項目為：需基於企業之文化建立一個利於創新之環境，繼續採用此控制項目。
3.	APO.19.1 優先考慮資源的分配。	硬體資源在規劃階段就應該非常清楚。	認同該兩位專家之看法，將此兩項控制項目修正為一項：於規劃時考慮資源的分配並定期識別及記錄資產。
5.	APO.19.2 識別並記錄目前的資產。	ERP 購買時相關資源便會一併購入。	
5.	APO.10.2 了解企業未來的發展方向。	在 ERP 導入時的 BPR 中處理。	認同該專家之看法，將此控制項修正為：以企業流程再造的角度了解企業未來的發展方向。
5.	BAI.5.3 建立和維護一個如何配置的知識庫和基準。	無法預知何時損壞。	認同此專家之看法，且此控制項已達中度一致性，因此採用原始之控制項目以控制無法預知之損壞。
7.	BAI.11.1 持續不斷的變革。 BAI.11.2 追踪和報告變更狀態。	新舊結合上有問題，不可能導入。	認同該專家之看法，並將此兩項控制項目修正為：持續追蹤新舊系統結合時變革的狀態。

經過文獻探討彙整出之機制雛型及兩回合德爾菲問卷修正雛型之後，第一回合符合專家內容效度檢定之風險因子共 18 項，達成專家一致共識之控制項目共 45 項。將第一回合未達內容效度而預計刪除之風險因子共 1 項；需再次確認之風險因子共 32 項、控制項目 85 項。第二回合德爾菲問卷回收後，確認刪除 1 項風險因子，並整併第二回合最初之 85 項控制項目至 80 項。因此，本研究利用德爾菲法兩回合之過程，產出已達成專家共識之 COBIT 5 為基礎之

ERP 系統風險管理的機制，本機制涵蓋 4 大領域構面、52 項風險因子及針對風險因子所對應的 125 項控制項目。

伍、以個案實證 ERP 系統風險管理機制之有效性

本研究擬採用單一個案為研究對象，以獲得較高的研究深度。首先了個案公司進行 ERP 系統風險管理的概況，及在執行 ERP 系統風險管理時所遭遇的困難和挑戰來了解個案公司的實務做法；再者對個案公司有效性之評估，採本研究之 ERP 系統風險管理程序為基礎，分別為風險辨識、風險評估、風險回應與控制三大步驟，藉由訪談前給予受訪者試用本研究機制後，評估本機制在此風險管理的三個階段的動作對於個案公司在 ERP 系統風險管理上的有效性來作探討，並瞭解本機制對個案公司之貢獻、缺點與需要加強的部分以及個案公司的其他看法與建議。

一、汽車產業與個案公司簡介

台灣汽車工業及其零組件工業構成一典型的中衛體系，中心車廠將零組件外包給一級衛星廠，一級衛星廠再將細部零件、半成品或製程轉包給第二級、第三級衛星廠，形成多層次的金字塔型分工結構。目前台灣 10 家汽車廠旗下的 OEM 供應商約有 400 家左右，若加上第二級、第三級衛星廠，以及供應售後維修體系的零組件供應廠商，台灣汽車零組件供應廠商約有 2,300 餘家。近年來在政府及廠商積極拓展外銷下，汽車零組件出口值逐漸成長，帶動我國汽車零組件產值提升。2009 年雖遭受全球金融海嘯影響，整體產業值跌落谷底，但自 2010 年起，受國內經濟復甦及車市成長利多拉抬下，產值連三年突破新台幣 2,000 億元，更於 2012 年達到新台幣 2,263 億元。

個案公司於民國 74 年成立於嘉義資本額為 9 億台幣，是台灣兩千大之民營企業，員工人數約 480 人，現今分別在台灣嘉義及大陸無錫兩地設置生產據點，係專業之汽車關鍵零組件製造商，主要以北美供給整車廠裝車零件、售後維修市場為主，客戶為美國通用汽車公司(GM Motor Group)及美國五大汽車維修市場零組件經銷商產品，93%外銷全球世界各地。個案公司之資訊系統建置為 Oracle ERP (R11i)系統，包含三大模組：配銷模組、製造模組及財務模組。配銷模組內容包含有庫存管理、採購管理、訂單出貨管理；製造模組則包含有產品結構管理、工單管理、物料需求規劃、產能需求規劃、預測主生產計畫以及成本管理；財務模組方面包含有總帳、應收帳款、應付帳款、現金管理、固定資產等功能。此外，近年加強品質管理，也透過 ERP 系統的品質管制系統，有效蒐集個階段之品質資訊，以作為分析改善之依據。對於製程管制，也引進 SPC 電腦軟體，以作為製程管制之即時分析，並減少人員統計之時間，提高即時監測之效率。

二、以個案研究驗證本研究機制有效性

驗證本研究機制以個案研究方式進行，在訪談過程中以錄音方式記錄完整的訪談內容，並整理訪談內容。訪談對象為個案公司的管理部副理與資訊課課長，兩位皆為執行 ERP 系統之專案成員及負責人。訪談結束後若有資料不足或遺漏的部分，則以 Email 或電話方式洽詢，並整理出訪談之會議紀錄。

（一）ERP 系統運行的過程所遭遇的風險

個案公司主要將 ERP 系統分成導入與維護兩階段，導入會用專案的方式進行，專案控管清楚地定義專案的時間、成本、目標與範圍；而維護的部分，個案公司每一年都會進行後續調整的專案，加上系統平常的維護運作，都會有相關的辦法去定義。若要細分可能發生的風險則可根據本研究的主要構面的分類方式進行說明如表 9。

表 9　個案公司 ERP 系統運行上依四構面所發生的風險

調整、規劃與組織(APO)	本研究所彙整之風險因子
管理部副理表示	
◆ 在規劃階段風險發生的可能是最大的。因為 ERP 系統是全公司人員在使用的系統，所以跨部門整合上的難度可說是最高的。	●APO.5 難以整合各個部門。
◆ 受訪者也表示當初規劃時除了考慮功能面上的問題之外，因為 ERP 系統是根據所有資料為基礎建立而成的一個系統平台，一般導入 ERP 系統的公司，未來也很有可能導入所謂的商業智慧 business intelligence (BI)或是競爭智慧 competitive intelligence (CI)等等，所以規劃階段不能只考慮到功能面上的問題。	●APO.13 未尋求顧問公司進行適當的規劃。
◆ 受訪者也提到除了在規劃時整合上的問題之外，高階及管理人員的需求也是需要考量的，若是在此階段沒有釐清，在 ERP 系統後續的維護上可能也會發生問題。	●APO.20 人力資源上的政策未改變而造成人員任用上的錯誤。
◆ *關鍵人員*：因為系統的導入並不是公司所有人員皆參與，一定是每個作業單位下的關鍵人員，這位關鍵人員能不能代表那個單位並且需考慮他的經驗。若缺少在導入時的關鍵角色，則這也可能成為在這個階段上的風險來源。	●APO.20 人力資源上的政策未改變而造成人員任用上的錯誤。
◆ 導入顧問：在公司導入系統時所尋求的導入顧問，若他們只具備軟體背景而不具備公司產業的背景這就可能發生問題。因為像是公司這種中大型企業，將近 1,000 名員工，其實現場的人員是不會使用電腦的，所以導入顧問的關鍵就在於要如何將他們在現場人員的作業導入至系統這是很關鍵的，而其實在這之間，彼此的協調和溝通也是佔了很重要的部分。	●APO.17 系統供應商端上在系統的取得、開發及維護上的問題。
◆ 專案經理：在使用者端與顧問端專案經理，負責管理的導入的所有事項。	●APO.4 角色職權未適當分工，造成權力過度集中的問題。
◆ 公司在完成規劃及建立階段，並向使用者端的人員進行功能上的說明和相關的教育訓練後，系統實際運作上，使用者可能去嘗試一些在系統規劃時未被定義的執行動作，因為在使用者直覺的認知上就是去試功能，這種結果可能產生一些異常的狀況發生，或是造成異常的資料或是資料錯亂的風險。	●APO.7 缺乏充分的訓練規劃。

表 9　個案公司 ERP 系統運行上依四構面所發生的風險（續）

建立、取得與導入(BAI)	本研究所彙整之風險因子
資訊課長表示	
◆在建立的階段上，使用者與顧問端理解上的差異是個很大的問題可能初期規劃時顧問團隊已有想到使用者的某種需求，系統上線後使用者一開始覺得這是他想要的，但漸漸的使用者的想法與系統執行的觀念上開始有落差，這是因為系統的架構存在著它的商業邏輯(business logic)。個案公司表示這種問題在導入的一開始無法很容易地去發現，當實際運行時使用者才會發現結果怎麼跟他想像的不一樣，以公司來說，在當初 ERP 系統由鼎新轉為 Oracle 時，員工在操作費用的分攤動作時，就發生使用者的想法與系統執行結果有落差的問題。	●BAI.3 流程與控制制度建立上的問題。
監控、評估與衡量(MEA)	本研究所彙整之風險因子
管理部副理表示	
◆在監督階段，最大的風險在於界定監督上的相關標準，因為這些相關的標準，會隨著公司的發展而變化。	●MEA.1 缺乏持續的溝通。

（二）處理或回應 ERP 系統的風險

個案公司在處理及回應 ERP 系統的風險上主要分為導入前的規範及導入後運作上的管理（如表 10）。

表 10　個案公司於導入前後處理風險之程序

導入前的規範面	本研究所彙整之風險因子
資訊課長	
◆個案公司的做法是在導入階段上會有相關的規範和宣導，以防止在實際運作時有其他問題的發生。	●APO.7 缺乏充分的訓練規劃。
◆也會根據過去相關的問題來進行教育訓練。例如：剛開始導入時，作業面的運作一定有相關的教育訓練以及嚴格的規範，並也有系統的操作使用手冊的產生。	●APO.7 缺乏充分的訓練規劃。
導入後的運作面	本研究所彙整之風險因子
資訊課長	
◆實際運作時，一定會有異常的發生，而這些異常可能是在導入階段沒有發現而且是偏作業面上的問題，例如：會針對這些異常狀況，訂定強制規範的動作，明確指出這個作業不能進行什麼動作，並告知使用者雖然系統具有這功能，但並不能進行這些動作，若執行一定會有異常的狀況發生。而這就是在執行面上的規範。	●BAI.3 流程與控制制度建立上的問題。

而公司在導入之後是有對 ERP 系統運作過程產生的風險進行風險管理的動作，大致包含四個步驟：風險項目之提出、列管、追蹤、檢視。最初由專案中各小組提出其所面臨最迫切之問題，並提出對應之解決方案；將所提出之項目與本專案之風險項目表比較，可直接列入項目表中或是修改原有之項目，使其涵蓋範圍擴大，之後，將其餘項目作一分析，區分其是否屬於正進行中之工作，例如某些已導入之項目因變更關係而重新實施，但這些項目不影響專案整體時程、成本，倘若判斷為真正風險項目，則將其列入風險項目表中；接續各專案小組負責追蹤其個別之風險項目，將結果與進度向專案管理辦公室報告。此追蹤之工作包括移除非屬風險之項目、修改控管風險之方法及增加新的項

目。若有必要，則由專案管理辦公室導入新的資源以協助風險控管；最後，此風險項目表可視其需要，於例行之專案管理計劃檢視會議中進行修改工作。除此之外，受訪者之（管理部副理）也針對公司的風險管理提出補充說明，公司風險管理之階段包括(1)導入前，在導入階段會針對系統權限或是備援的動作做相關的規劃；(2)導入後，正式導入之後，針對實際執行上發生的異常，會有一些改善的機制；(3)年度稽核，分為內部稽核和外部稽核，而在內稽的過程中也使個案公司再次地重新檢視目前現有的風險。

（三）研究機制有效性評估

個案訪談前給予受訪者檢視並使用本研究機制修訂後的結果，進行本研究機制有效性評估，本研究將依照 ERP 系統的風險管理程序之四大步驟：「風險辨認」、「風險評估」、「風險回應」及「監督與修正」進行訪談。

首先在風險辨認的程序將四大領域構面中 52 項風險因子，請訪談人員判斷此 52 項風險在個案公司中發生的有無。在受訪者檢視及使用過後，結果顯示，在 APO 構面下共有 23 項可能發生之風險因子，而受訪者判斷有 16 項(16/23=70%)是會發生於個案公司的；在 BAI 構面下共有 16 項可能發生之風險，而受訪者認為有 8 項(50%)是會發生的；在 DSS 構面下具有 7 項風險因子，受訪者認為有 6 項(86%)是會發生在此構面之下的風險；最後在 MEA 構面下，本機制具有 6 項風險因子，受訪者認為只有 2 項(33%)是會發生的。綜合四個構面的 52 項風險因子，受訪者檢視過後認為其中有 32 項(62%)風險因子是會發生在公司的 ERP 系統運作上，顯示出本研究機制在風險辨識階段的有效程度，可知本機制在風險辨識的運作上對於公司是有效的。

Al-Shehab, Hughes, and Winstanley (2004)認為風險因子本身其實並沒有辨認出風險，需透過風險評估的模式，才能找到最為重大的風險因子，並且排列風險的大小。因此本研究透過受訪者以風險因子的影響程度高、中或低評估四領域中的風險因子。評估結果在 APO 領域中有 5 項受訪者評估其重要性為「高」的項目； BAI 領域中 8 項會發生在公司的風險因子，其中共有 2 項受訪者評估為「高」影響程度的風險項目；在 DSS 領域且發生在公司的風險因子中僅 1 項受訪者評估為高影響程度的風險因子；而在 MEA 領域中，2 項會發生在公司的風險因子，其中有 1 項受訪者評估為「高」影響程度的風險項目。經過風險評估後可知在個案公司會發生的風險因子且影響程度為「高」的風險項目共 9 項，影響程度為「中」的風險項目共 13 項，而影響程度為「低」的風險項目共 10 項，公司可根據此結果選擇優先處理這些影響程度為「高」的風險項目。

在風險回應步驟方面，評估過後的風險可透過控制措施來控制該風險（張碩毅與吳承志 2008）。四個領域構面共有 9 項為「高」影響程度的風險因子，且根據這 9 項風險因子列出受訪者認為控制效果為「高」和「中」的控制項目，這 16 項控制項可作為公司在遇到這些「高」影響程度的風險因子時，能優先採取的控制與回應動作（如表 11）。

表 11 「高」影響程度風險因子以及控制效果為「高」和「中」的控制項目

「高」影響程度之風險因子	控制效果為「高」和「中」的控制項
未尋求顧問公司進行適當的規劃。	確實了解企業的發展方向。
經營階層所提出之可能影響系統運作的公司文化問題。	定義一個可供參考的架構。
	需基於企業之文化建立一個利於創新之環境。
難以整合各個部門。	協調和溝通。
缺乏充分的訓練規劃。	確定關鍵的 IT 人員。
	能組織和理解資訊，將其轉化為知識。
團隊組成不穩定。	定義架構的實施。
流程與控制制度建立上的問題。	追踪和報告變更狀態。
	加入控制活動至業務流程中以符合企業目標。
	監督內部控制。
因通訊系統或伺服器的損壞而影響 ERP 系統的運作。	確認和記錄目前資產。
	管理與系統有關的關鍵性資產。
	建立和維護一個如何配置的知識庫和基準。
不合邏輯的操作，造成錯誤發生。	定義策略性的計劃。
缺乏持續的溝通。	加入控制活動至業務流程中以符合企業目標。
	確定外部需求的遵循性。

最後在監督與修正步驟部分，根據了解個案公司 ERP 系統風險管理實施狀況，公司最主要目前只將作業分為 ERP 導入前的規範及導入後針對作業面上之異常進行管理，而受訪者表示本研究對於個案公司的有效程度及幫助，在於將風險因子項目，除了較清楚地評估其重要程度，並將所對應的 COBIT 控制項目列出並整理，這種做法就專案導入時可以很快速地來進行評估及計畫，透過本研究機制可以考慮得更為周詳。因此本研究之 ERP 系統風險管理機制的確有其建構的價值，並且經由個案公司的實際應用印證了本機制具可行之有效性。

陸、結論與建議

本研究利用 ISACA 最新公布的資訊科技治理及資訊系統控制的架構－COBIT 5 為基礎，提供企業與資訊人員一個便利、迅速、正確的辨識、評估、回應與控制之 ERP 系統風險管理的機制，探討 ERP 系統可能發生的風險因子、類別與特質，進一步評估各個風險對企業的影響，並探討企業應該採取哪些方式來回應與控制風險。

本研究經由文獻探討歸納出 ERP 系統風險管理的程序以及雛形，並運用德爾菲專家問卷，以專家在實務上的角度，補充理論端上文獻的不足，並進行 ERP 系統風險管理機制上的修正，最終修正後之成果得出本研究提出該管理機制共具有 4 大領域構面、52 項風險因子以及針對風險因子的控制項目共125 項，最後並以個案研究進行實務上驗證本研究提出之管理機制之有效性。

過去針對資訊科技風險管理的研究，多以探討風險因子與評量、分析風險作為研究目的，而本研究與其差異之處在於主要將新提出應用於資訊科技／資

訊系統的控制架構：COBIT 5，結合屬於資訊科技其中一部分的 ERP 系統風險管理上，藉由本研究之結果可幫助企業組織重視 ERP 系統的風險管理，以快速的方式辨識出風險並進行回應與改善的動作，進而發揮整個風險管理效果，本研究之結果也可做為未來欲針對 COBIT 架構之研究人員進行相關研究時的參考。未來研究方向應加強根據控制項目定義明確、增設治理領域流程、完整的職能分配，更能達成對於風險因子的有效控制，使整個 ERP 系統的風險管理程序更臻完善。另一方面，由於不可掌握的 ERP 系統風險於未來將可能產生，本研究所彙整之 ERP 系統風險將無法全部涵蓋，此為本文之研究限制。

附錄 1　COBIT 5 為基礎的 ERP 系統風險管理機制雛形及德爾菲法專家問卷結果

領域	風險因子	CVR	影響流程	控制項目(目標)	第一回合專家問卷結果					第二回合專家問卷結果		
					四分位差	標準差	平均數	修正風險因子	重新分類	四分位差	標準差	平均數
APO 構面	APO.1 安全措施的效果不佳	0.86	APO01 DSS05	APO.1.1 保持遵守政策和程序。	0.5	0.75	4.31	ERP 系統上資訊安全保護措施不佳。		0.5	0.51	4.38
				APO.1.2 管理網絡連接的安全性。	0.5	0.60	4.23			0.5	0.83	4.23
				APO.1.3 管理端點安全性。	0.5	0.73	4.23			0.5	0.65	4.38
	APO.2 經授權的使用者誤用	1.00	APO01 DSS05, DSS06	APO.2.1 定義資訊（數據）和系統的所有權。	0.5	0.73	4.29					
				APO.2.2 監測基礎設施與安全相關的事件。	0.5	0.80	4.21					
				APO.2.3 管理角色，職責，存取權限和級別的權限。	0.5	0.52	4.50					
	APO.3 故意的行為	0.43	APO13 BAI07 DSS05 MEA01	APO.3.1 監督和審查。	0.375	0.88	4.10	（預計刪除風險因子）。				
				APO.3.2 建立一個測試環境。	0.875	0.88	4.10					
				APO.3.3 監測的基礎設施與安全相關的事件。	0.875	0.88	3.90					
				APO.3.4 建立一個監控的方法。	0.375	0.74	3.90					
	APO.4 職責集中化：職能有無分工	0.86	APO12 MEA02	APO.4.1 闡述風險。	0.5	0.75	4.31	角色職權未適當分工，造成權力過度集中的問題。		0	0.58	4.00
				APO.4.2 執行控制的自我評估。	1	0.82	4.00			0.5	0.69	4.15
	APO.5 難以整合各個部門	1.00	APO08	APO.5.1 協調和溝通。	0.5	0.65	4.43					
	APO.6 與舊系統整合之挑戰	1.00	APO01 BAI05 DSS01	APO.6.1 維護管理系統的實現。	0.5	0.50	4.36					
				APO.6.2 形成有效的執行團隊。	0.5	0.63	4.36					
				APO.6.3 管理環境。	0.375	0.66	4.14					
	APO.7 缺乏充分的訓練規劃	1.00	APO07 BAI08	APO.7.1 確定關鍵的 IT 人員。	0.375	0.77	4.14					
				APO.7.2 組織信息轉化為知識。	0.5	0.77	4.14					
	APO.8 技術人員的效能問題	0.86	APO07	APO.8.1 保持足夠且適當的人力資源。	0.5	0.60	4.23					
				APO.8.2 維護人員的技能和能力。	0.5	0.60	4.23					
				APO.8.3 評估員工的工作績效。	0.5	0.51	3.62					
	APO.9 使用者涉入不足	1.00	APO08 APO09 BAI02	APO.9.1 協調和溝通。	0.5	0.76	4.50					
				APO.9.2 確定 IT 服務。	0	0.62	3.93					
				APO.9.3 定義和維持業務功能和技術要求。	0	0.62	4.07					
				APO.9.4 進行有效性研究。	0.375	0.66	4.14					

附錄 1　COBIT 5 為基礎的 ERP 系統風險管理機制雛形及德爾菲法專家問卷結果（續 1）

領域	風險因子	CVR	影響流程	控制項目(目標)	第一回合專家問卷結果				第二回合專家問卷結果			
					四分位差	標準差	平均數	修正風險因子	重新分類	四分位差	標準差	平均數
APO構面	APO.9 使用者涉入不足	1.00	APO08 APO09 BAI02	APO.9.1 協調和溝通。	0.5	0.76	4.50					
				APO.9.2 確定 IT 服務。	0	0.62	3.93					
				APO.9.3 定義和維持業務功能和技術要求。	0	0.62	4.07					
				APO.9.4 進行有效性研究。	0.375	0.66	4.14					
	APO.10 ERP 系統沒有符合營運流程	0.86	APO01 APO02 BAI02	APO.10.1 定義的組織結構。	1	0.86	4.08	ERP 系統因組織結構的問題而未符合其營運流程。		0	0.64	3.92
				APO.10.2 了解企業方向發展。[c]	1	1.24	3.77			1	0.86	3.92
				APO.10.3 定義和維護業務功能和技術要求。	0	0.71	4.00			0.5	0.69	3.85
	APO.11 不適合的科技任務	0.71	APO02 APO03 APO04 BAI02	APO.11.1 溝通 IT 策略及方向。	0.125	0.67	3.92	規劃階段時評定不適當的科技技術任務，造成 ERP 系統運作上的錯誤。		0	0.55	3.85
				APO.11.2 選擇機會和解決方案。	0.125	0.67	3.92			0	0.64	3.92
				APO.11.3 監控和掃描技術環境。	0	0.79	3.92			0.5	0.76	4.08
				APO.11.4 評估潛在的新興技術和創新理念。	0.125	0.83	3.83			0.5	0.76	3.92
				APO.11.5 定義和維護業務功能和技術要求。	0.125	0.58	3.83			0.5	0.65	3.62
	APO.12 缺少適當方法論	0.86	APO02 BAI08	APO.12.1 定義策略性計劃和路線圖。	0.5	0.95	3.69	未有與 ERP 系統配合的方法論。		0.5	0.78	3.54
				APO.12.2 培育並促進知識共享的文化。	0.5	1.04	3.62			0.5	0.80	3.85
	APO.13 沒有適當規劃	0.71	APO02 BAI01	APO.13.1 了解企業方向發展。	1	1.00	3.92	未尋求顧問公司進行適當的規劃。		0	0.58	4.00
				APO.13.2 監督及控制專案。	0.125	0.67	3.92			0.5	0.69	4.15
	APO.14 人力資源政策未改變	1.00	APO07	APO.14.1 計劃和追蹤 IT 企業人力資源的使用。	0.5	0.70	4.21					
	APO.15 公司現有文化問題	0.86	APO03 APO04	APO.15.1 定義的參考架構。	1	1.19	3.62	經營階層所提出之可能影響系統運作的公司文化問題。		0.5	0.69	3.85
				APO.15.2 建立一個有利於創新的環境[d]。	0.5	1.12	3.62			1	0.82	4.00
	APO.16 組織現有結構問題	1.00	APO01 APO03 BAI05	APO.16.1 定義的組織結構。	0.5	0.85	3.50					
				APO.16.2 開發企業架構的願景。	0.5	0.84	3.64					
	APO.17 供應商問題	0.71	APO08 APO10	APO.17.1 管理業務關係。	0.5	0.89	3.67	系統供應商端上在系統的取得、開發及維護上的問題。	BAI	0.5	0.77	3.62
				APO.17.2 識別和評估供應商的關係和合約。	0.125	0.85	4.00			0.5	0.60	4.23

附錄 1　COBIT 5 為基礎的 ERP 系統風險管理機制雛形及德爾菲法專家問卷結果（續 2）

領域	風險因子	CVR	影響流程	控制項目(目標)	第一回合專家問卷結果				第二回合專家問卷結果			
					四分位差	標準差	平均數	修正風險因子	重新分類	四分位差	標準差	平均數
APO 構面	APO.18 團隊組成不穩定	0.86	APO03 BAI05	APO.18.1 定義所實施的架構。	0.5	0.77	3.38					
				APO.18.2 提供企業基礎架構服務。	0.5	0.52	3.54					
				APO.18.3 維持的變化。	0	0.64	3.92					
	APO.19 資源不足	0.71	APO06 BAI09	***APO.19.1 優先考慮資源的分配***[b]。	0.5	0.52	4.50	ERP 系統所需之資源不足，例如：硬體設備。		0.625	0.79	4.08
				APO.19.2 識別和記錄目前的資產[b]。	0.5	1.07	3.33			0.625	0.79	3.92
	APO.20 人員任用不適當	0.86	APO07	APO.20.1 保持足夠的和適當的人力資源。	0.5	0.63	4.31	人力資源上的政策未改變而造成人員任用上的錯誤。		0.5	0.76	4.08
BAI 構面	BAI.1 輸入錯誤或是竄改的資料	0.86	BAI03 BAI06 DSS01	BAI.1.1 構建解決方案。	0.5	0.51	4.62	輸入錯誤或是竄改過的資料（可回復改正）。		0.5	0.65	4.33
				BAI.1.2 追踪和報告變更狀態。	0.5	0.48	4.69			0.5	0.79	4.42
				BAI.1.3 監控 IT 基礎設施。	0.5	0.66	4.54			0.125	0.67	4.08
	BAI.2 IT 內部的程序錯誤	0.86	BAI02 BAI03 MEA02	BAI.2.1 定義和維護業務功能和技術要求。	1	0.82	4.00	系統於規劃時內部的程序錯誤。	APO	0	0.53	4.14
				BAI.2.2 設計詳細的解決方案元件。	0.5	0.52	4.46			0.375	0.58	4.21
				BAI.2.3 執行控制的自我評估。	0	0.55	4.15			0	0.53	4.14
	BAI.3 程序與控制	0.71	BAI06 DSS06 MEA02	BAI.3.1 追踪和報告變更狀態。	0.5	0.51	4.42	流程與控制制度建立上的問題。		0.5	0.78	4.33
				BAI.3.2 調整控制嵌入業務流程中的活動與企業目標。	0.5	0.65	4.33			0.125	0.58	4.17
				BAI.3.3 監督內部控制。	0.5	0.67	4.42			0.5	0.67	4.42
	BAI.4 程式錯誤	1.00	DSS02	BAI.4.1 驗證批准，並滿足服務請求。	0.5	0.84	4.36					
	BAI.5 作業系統的瑕疵	0.57	APO01 BAI09 DSS01	BAI.5.1 優化的 IT 運作的位置。	0	0.63	4.00	作業系統的瑕疵而影響 ERP 系統運作。		0.5	0.67	4.30
				BAI.5.2 管理關鍵資產。	0.5	0.65	3.73			0	0.57	3.90
				BAI.5.3 監控 IT 基礎設施。	0.5	0.50	3.64			0.375	0.63	3.80
	BAI.6 通訊系統或伺服器的損壞	0.71	BAI09 BAI10 DSS04	BAI.6.1 確認和記錄目前資產。	0.125	0.85	4.00	因通訊系統或伺服器的損壞而影響 ERP 系統的運作。		0.5	0.72	3.83
				BAI.6.2 管理關鍵資產。	0.625	0.95	4.00			0.125	0.58	4.17
				BAI.6.3 建立和維護的結構資源庫和基準線。	0.125	0.58	3.83			0.625	0.79	3.92
				BAI.6.4 制定和實施業務連續性反應。	0.25	0.74	4.00			0	0.60	4.00
	BAI.7 意外的故障	0.71	APO01 BAI10 DSS01	BAI.7.1 優化的 IT 運作的位置。	0.125	0.67	4.08	硬體或軟體意外的故障而影響 ERP 系統的運作。		0	0.41	4.00
				BAI.7.2 建立和維護的結構資源庫和基準線。	0.625	0.79	4.08			0.5	0.76	4.08
				BAI.7.3 監控 IT 基礎設施。	0.5	0.72	4.17			0	0.58	4.00

附錄 1　COBIT 5 為基礎的 ERP 系統風險管理機制雛形及德爾菲法專家問卷結果（續 3）

領域	風險因子	CVR	影響流程	控制項目(目標)	第一回合專家問卷結果					第二回合專家問卷結果		
					四分位差	標準差	平均數	修正風險因子	重新分類	四分位差	標準差	平均數
BAI 構面	BAI.8 大範圍的組織變化	0.71	APO03 BAI05 MEA02	BAI.8.1 定義的參考架構。	0.5	0.78	3.67	大範圍的組織變化而未進行完善的變更管理作業。		0.5	0.77	4.00
				BAI.8.2 嵌入新方法。	0.5	0.79	3.58			0.5	0.69	3.45
				BAI.8.3 計劃保證措施。	0.5	0.90	3.50			0.5	0.69	3.45
	BAI.9 喪失版本更新之控制	0.71	BAI06 BAI07	BAI.9.1 追踪和報告變更狀態。	0.125	0.58	4.17	因未有適當的 IT 人員而喪失版本更新之控制。	APO	0.125	0.45	4.25
				BAI.9.2 計劃的業務流程，系統和數據轉換。	0	0.60	4.00			0.5	0.67	4.42
	BAI.10 科技的誤用	0.86	BAI04	BAI.10.1 評估目前的可用性，性能和容量，並建立一個基準。	0	0.64	4.08					
	BAI.11 流程再造的問題	0.71	BAI06 BAI07 DSS06	BAI.11.1 追踪和報告變更狀態。	0.25	0.90	3.92	因流程的再造而未進行變更管理。		0.5	0.60	3.77
				BAI.11.2 計劃的業務流程，系統和數據轉換。	0.125	0.67	4.08			0	0.64	4.08
				BAI.11.3 調整控制嵌入業務流程中的活動與企業目標。	0.625	0.79	4.08			0.5	0.60	4.23
	BAI.12 缺少有效率之專案管理技術	0.86	BAI01	BAI.12.1 維護計劃和項目管理的標準方法。	0.5	0.65	4.38	缺少有效率之專案管理技術而未達成變更管理。	APO	0.5	0.63	4.31
	BAI.13 基礎建設不足	1.00	APO06 BAI09	BAI.13.1 創建和維護的預算。	0.375	0.73	4.07					
				BAI.13.2 管理關鍵資產。	0.5	0.77	3.86					
	BAI.14 現有系統準備變革程度	1.00	BAI05 BAI07 DSS04	BAI.14.1 建立希望改變。	0.875	0.83	3.93					
				BAI.14.2 評估，優先考慮和批准變更請求。	0.375	0.73	4.07					
				BAI.14.3 進行恢復後檢討。	0.375	0.73	3.93					
	BAI.15 缺乏通訊基礎建設	0.86	BAI09 BAI10	BAI.15.1 識別和記錄流動資產。	0.5	0.87	3.62	缺乏通訊基礎建設，例如：防火牆、無線網路設備等。		0.5	0.60	3.77
				BAI.15.2 建立和維護的結構模型。	0.5	0.78	3.46			0.5	0.78	3.46
	BAI.16 無法支援資料整合之跨組織設計	1.00	APO03 APO04 BAI05 BAI08	BAI.16.1 定義架構是如何實施。	0.375	0.86	3.86					
				BAI.16.2 建立一個有利於創新的環境。	0.5	0.94	3.57					
				BAI.16.3 啟用操作和使用。	0.375	0.58	3.79					
				BAI.16.4 評估和退休資訊。	0	0.77	3.86					
	BAI.17 缺乏資料庫基礎建設	0.86	APO03 BAI09	BAI.17.1 提供企業基礎架構服務。	0	0.80	3.85	缺乏資料庫等基礎建設而影響 ERP 系統運作。		0.5	0.63	3.69
				BAI.17.2 識別和記錄目前資產。	0.5	0.93	3.77			0.5	0.65	3.62
	BAI.18 試圖與舊系統結合	0.86	BAI05 BAI07 DSS01	***BAI.18.1 維持的變化***[d]。	0.5	0.80	4.15	與舊系統結合時未捨棄舊有系統而造成的問題。		0	1.01	3.77
				BAI.18.2 追踪和報告變更狀態[d]。	0.5	0.52	4.46			0	1.07	3.85
				BAI.18.3 計劃的業務流程，系統和數據轉換。	0.5	0.66	4.46			0.5	0.65	4.38
				BAI.18.4 執行操作的程序。	0.5	0.60	4.23			0.5	0.60	4.23

附錄 1　COBIT 5 為基礎的 ERP 系統風險管理機制雛形及德爾菲法專家問卷結果（續 4）

領域	風險因子	CVR	影響流程	控制項目(目標)	第一回合專家問卷結果					第二回合專家問卷結果		
					四分位差	標準差	平均數	修正風險因子	重新分類	四分位差	標準差	平均數
DSS 構面	DSS.1 儲存媒體的處理	0.86	DSS05	DSS.1.1 管理 IT 資產的存取。	0.5	0.85	4.31	儲存媒介未做適當的管理而造成的問題。		0.125	0.58	4.17
			DSS06	DSS.1.2 保護資訊資產的安全。	0.5	0.65	4.62			0.5	0.67	4.50
	DSS.2 不受管束或未經授權的系統存取	0.86	DSS05	DSS.2.1 管理用戶身份和邏輯存取。	0.5	0.66	4.46	不受管束或未經授權的系統存取。	APO	0.5	0.66	4.46
			DSS06	DSS.2.2 管理角色，職責，存取權限和級別的權限。	0.5	0.65	4.38			0.5	0.52	4.46
	DSS.3 缺乏交易軌跡	0.86	BAI07	DSS.3.1 計劃的業務流程，系統和數據轉換。	0.5	0.86	4.08	缺乏經由規劃與建立的交易軌跡。	APO	0.5	0.48	4.31
			DSS04	DSS.3.2 定義業務連續性政策、目標與範圍。	1	0.95	3.92			0	0.55	4.15
			DSS06	DSS.3.3 確保資訊事件和責任的可追溯性。	0.5	0.66	4.54			0.5	0.66	4.54
			MEA01	DSS.3.4 建立一個監控方法。	0.5	0.87	4.38			0.5	0.51	4.38
	DSS.4 交易由電腦自動產生或執行	0.86	DSS01	DSS.4.1 管理設備。	0	1.17	3.77	電腦自動產生交易，未經過覆核。		1	0.86	3.92
			DSS06	DSS.4.2 確保資訊事件和責任的可追溯性。	0.5	0.80	4.15			0.5	0.75	4.31
			MEA02	DSS.4.3 執行控制的自我評估。	0	0.76	4.08			0.5	0.73	4.23
	DSS.5 人工控制依賴電腦控制	0.71	APO13	DSS.5.1 定義和管理資訊安全風險處理計劃。	0.5	0.62	4.25	人工控制過度依賴電腦控制，造成舞弊發生的可能。		0.5	0.67	4.36
			DSS01	DSS.5.2 監控 IT 基礎設施。	0.125	0.85	4.00			0.25	0.60	3.82
			DSS06	DSS.5.3 管理錯誤和異常。	0.5	0.67	4.42			0.5	0.67	4.36
			MEA02	DSS.5.4 執行控制的自我評估。	0.125	0.67	4.08			0	0.54	3.91
	DSS.6 無法將使用者需求轉換成技術需求或快速滿足使用者需求	1.00	APO08	DSS.6.1 協調和溝通。	0.5	0.76	4.43					
			BAI08	DSS.6.2 使用和分享知識。	0.375	0.73	3.93					
	DSS.7 不合邏輯的處理	0.86	APO02	DSS.7.1 定義策略性計劃和路線圖。	0.5	0.76	4.08	不合邏輯的操作，造成錯誤發生。		0	0.64	4.08
			BAI08	DSS.7.2 識別和分類資訊來源。	0	0.86	3.92			0.5	0.69	4.15
			DSS02	DSS.7.3 定義事件和服務請求分類方案。	0.5	0.76	3.92			0.5	0.80	4.15
	DSS.8 資料轉換	0.86	BAI06	DSS.8.1 跟踪和報告變更狀態。	0.5	0.76	3.92	資料轉換時發生錯誤而影響系統。		0.5	0.69	4.15
			DSS01	DSS.8.2 執行作業程序。	0.5	0.77	4.38			0.5	0.80	4.15
	DSS.9 沒有辦法快速回應	1.00	BAI03	DSS.9.1 設計詳細的解決方案元件。	0	0.64	4.08					
			DSS02	DSS.9.2 驗證批准，並滿足服務請求。	0.375	0.58	4.21					
			DSS03	DSS.9.3 確定和分類問題。	0	0.55	4.00					

附錄 1　COBIT 5 為基礎的 ERP 系統風險管理機制雛形及德爾菲法專家問卷結果（續 5）

領域	風險因子	CVR	影響流程	控制項目(目標)	第一回合專家問卷結果					第二回合專家問卷結果		
					四分位差	標準差	平均數	修正風險因子	重新分類	四分位差	標準差	平均數
MEA 構面	MEA.1 缺乏持續的溝通	1.00	APO10 DSS06 MEA03	MEA.1.1 管理供應商關係和合約。	0.5	1.07	4.07					
				MEA.1.2 調整控制嵌入業務流程中的活動與企業目標。	0	0.53	4.14					
				MEA.1.3 確定外部的遵從性要求。	0.375	0.47	4.29					
	MEA.2 缺乏外部顧問	0.86	APO02 BAI01 MEA03	MEA.2.1 了解企業方向發展。	0	0.71	4.00	缺乏顧問以監督、評估系統內控允當性。		0	0.55	4.15
				MEA.2.2 管理利益相關者的參與。	0	0.86	3.92			0.5	0.69	3.85
				MEA.2.3 最佳化外部要求的回應。	0	0.64	4.08			0	0.82	4.00
	MEA.3 難以衡量績效與效益	0.86	MEA01	MEA.3.1 設置性能和一致性的目標。	0.5	0.73	4.23	難以衡量 ERP 的績效，以確保程序確實進行。		0.5	0.75	4.31
	MEA.4 難以持續評估新的技術	1.00	MEA01 MEA03	MEA.4.1 收集和處理性能和一致性數據。	0.375	0.86	3.86					
				MEA.4.2 確定外部的遵從性要求。	0.5	0.61	3.71					
	MEA.5 缺少高階管理者支持	1.00	MEA01	MEA.5.1 建立一個監測的方法。	0.5	0.77	4.14					
				MEA.5.2 分析和報告性能。	0.5	0.63	4.36					
	MEA.6 無法驗核處理過程	1.00	BAI07 MEA01 MEA03	MEA.6.1 規劃驗收測試。	0.5	0.77	4.14					
				MEA.6.2 分析和報告性能。	0.375	0.58	4.21					
				MEA.6.3 外部合規性確認。	0	0.62	3.93					

註：第二回合專家問卷控制項目修訂結果為：

[a] ***APO.15.2 建立一個有利於創新的環境***　修訂為 需基於企業之文化建立一個利於創新之環境。

[b] ***APO.12.1 優先考慮資源的分配、APO.12.2 識別並記錄目前的資產*** 此兩項控制項目修正為一項 於規劃時考慮資源的分配並定期識別及記錄資產。

[c] ***APO.10.2 了解企業方向發展*** 修訂為 以企業流程再造(BPR)的角度了解企業未來的發展方向。

[d] ***BAI.18.1 維持的變化、BAI.18.2 追踪和報告變更狀態*** 此兩項控制項目修正為一項**持續追蹤新舊系統結合時變革的狀態**。

參考文獻

行政院研究發展考核委員會，2009，風險管理及危機處理作業手冊，網址：http://www.rdec.gov.tw/ct.asp?xItem=3854955andCtNode=12944andmp=100，搜尋日期：2011 年 7 月 31 日。(Research, Development and Evaluation Commission, Executive Yuan. 2009. The guidance of risk management. Available at: http://www.rdec.gov.tw/ct.asp?xItem=3854955andCt Node= 12944andmp=100. Accessed: July 31, 2011.)

林寶珠與王敏馨，2003，21 世紀的企業風險管理制度，會計研究月刊，第 210 期（5 月）：51-58。(Lin, B. Z., and M. H. Wang. 2003. Enterprise risk management in 21st century. *Accounting Research Monthly* 210 (May): 51-58.)

張碩毅、黃士銘、阮金聲、洪育忠與洪新原，2005，企業資源規劃，臺北：全華科技圖書股份有限公司。(Chang, S. I., S. M. Huang, J. S. Roan, Y. C. Hung, and S. Y. Hung. 2005. *Enterprise Resource Planning*. 1st edition. Taipei, R.O.C.: Chuan Hwa Book Company)

張碩毅與吳承志，2008，企業資源規劃系統建置與管理，臺北：碁峰資訊。(Chang, S. I., and C. C. Wu. 2008. *The Implementation and Management of Enterprise Resource Planning*. 1st edition. Taipei, R.O.C.: GOTOP Information Incorporation)

陳錦烽，2006，整合性企業風險管理，內部稽核，第 53 期（1 月）：19-24。(Chen, J. F. 2006. Integrated enterprise risk management. *Internal Auditor* 53 (January): 19-24.)

鄧家駒，2005，風險管理，臺北：華泰文化事業股份有限公司。(Teng, C. C. 2005. *Risk Management*. 1st edition. Taipei, R.O.C.: Hwa Tai Publishing Company.)

鄭燦堂，2012，風險管理：理論與實務，臺北：五南圖書出版股份有限公司。(Cheng, T. T. 2012. *Risk Management: Theory and Practice*. 1st edition. Taipei, R.O.C.: Wu-Nan Book Incorporation)

羅玳珊，2010，數據加速成長腳步，哈佛商業評論，第 46 期（6 月）：72-76。(Lo, T. S. 2010. Information speed up growth. *Harvard Business Review* 46 (June): 72-76.)

Alfantookh, A., and S. H. Bakry. 2009. IT governance practices: ITIL. *Saudi Computer Journal: Applied Computing and Informatics* 7: 56-65.

Aloini, D., R. Dulmin, and V. Mininno. 2007. Risk management in ERP project introduction: Review of the literature. *Information and Management* 44 (September): 547-567. (DOI:10.1016/j.im.2007.05.004)

Aloini, D., R. Dulmin, and V. Mininno. 2012a. Risk assessment in ERP projects.

Information Systems 37 (May): 183-199. (DOI:10.1016/j.is.2011.10.001)

Aloini, D., R. Dulmin, and V. Mininno. 2012b. Modelling and assessing ERP project risks: A Petri Net approach. *European Journal of Operational Research* 220 (July): 484-495. (DOI: 10.1016/j.ejor.2012.01.062)

Al-Shehab, A. J., R. T. Hughes, and G. Winstanley. 2004. Using causal mapping methods to identify and analyse risk in information system projects as a post-evaluation process. Paper presented at the 11th European Conference on Information Technology Evaluation, Netherlands.

Baccarini, D., G. S. Salm, and P. E. D. Love. 2004. Management of risk in information technology projects. *Industrial Management and Data Systems* 104: 286-295. (DOI: 10.1108/02635570410530702)

Bakry, S. H., and A. Alfantookh. 2006. IT governance practices: COBIT. *Saudi Computer Journal: Applied Computing and Informatics* 5: 53-61.

Bannerman, P. L. 2008. Risk and risk management in software projects: A reassessment. *Journal of Systems and Software* 81 (December): 2118-2133. (DOI: 10.1016/j.jss.2008.03.059)

Baskerville, R. 1991. Risk analysis: An interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems* 1 (March): 121-130. (DOI: 10.1057/ejis.1991.20)

Bin-Abbas, H., and S. H. Bakry. 2014. Assessment of IT governance in organizations: A simple integrated approach. *Computers in Human Behavior* 32 (March): 261-267. (DOI:10.1016/j.chb.2013.12.019)

Boockholdt, J. L. 1987. Security and integrity controls for microcomputers: A summary analysis. *Information and Management* 13 (August): 33-41. (DOI:10.1016/0378-7206(87)90028-0)

Cabinet Office. 2011. *ITIL Lifecycle Suite*. 2nd edition. London, U.K.: The Stationery Office.

Coe, M. J. 2005. Trust services: A better way to evaluate I.T. controls. *Journal of Accountancy* 199: 69-75.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 1992. *Internal Control - Integrated Framework*. New York, N.Y.: Committee of Sponsoring Organizations of the Treadway Commission.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2004. *Enterprise Risk Management - Integrated Framework*. New York, N.Y.:

Committee of Sponsoring Organizations of the Treadway Commission.

Dalkey, N., and O. Helmer. 1963. Delphi technique: Characteristics and sequence model to the use of experts. *Management Science* 9 (April): 458-467.

Davenport, T. H. 1998. Putting the enterprise into the enterprise system. *Harvard Business Review* 76 (July-August): 121-131.

De Haes, S., and R. S. Debreceny. 2013. COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems* 27 (Spring): 307-324. (DOI:10.2308/isys-50422)

Delbecq, A. L., A. H. Van de Ven, and D. H. Gustafson. 1975. *Group Techniques for Program Planning: A Guide to Nominal and Delphi Processes*. Glenview, I.L.: Scott, Foresman & Company.

Dezdar, S., and A. Sulaiman. 2009. Successful enterprise resource planning implementation: Taxonomy of critical factors. *Industrial Management and Data Systems* 109: 1037-1052. (DOI:10.1108/02635570910991283)

Drobik, A., and N. Rayner. 2013. Develop a strategic road map for postmodern ERP in 2013 and beyond. Available at: https://www.gartner.com/doc/2566015/ develop-strategic-road-map-postmodern. Accessed: May 9, 2014.

Gallegos, F., D. R. Richardson, and A. F. Borthick. 1987. *Audit and Control of Information Systems*. Cincinnati, O.H.: Thomson Corporation-South-Western Publishers.

Gibson, C. F. 2004. IT-enabled business change: An approach to understanding and managing risk. Available at: ftp://public.dhe.ibm.com/la/documents/imc/la/pe/ news/events/mit_2010/6a_mit_cisrwp346_itenabledbuschange.pdf. Accessed: March 19, 2014.

Gowin, D. B. 1981. *Educating*. New York, N.Y.: Cornell University Press.

Hakim, A., and H. Hakim. 2010. A practical model on controlling the ERP implementation risks. *Information Systems* 35 (April): 204-214. (DOI: 10.1016/j.is.2009.06.002)

Holden, M. C., and J. F. Wedman. 1993. Future issues of computer-mediated communication: The results of a Delphi study. *Educational Technology Research and Development* 41 (December): 5-24. (DOI: 10.1007/BF02297509)

Huang, S. M., I. C. Chang, S. H. Li, and M. T. Lin. 2004. Assessing risk in ERP projects: Identify and prioritize the factors. *Industrial Management and Data Systems* 104: 681-688. (DOI: 10.1108/02635570410561672)

Huang, S. M., W. H. Hung, D. C. Yen, I. C. Chang, and D. Jiang. 2011. Building the evaluation model of the IT general control for CPAs under enterprise risk management. *Decision Support Systems* 50 (March): 692-701. (DOI:10.1016/j. dss.2010.08.015)

Institute of Internal Auditors (IIA). 2011. Risk management. Available at: https://www.iia.org.uk/resources/risk-management/. Accessed: May 27, 2014.

International Standards Organization/International Electrotechnical Commission (ISO/IEC). 2005a. *ISO/IEC 20000 Information Technology - Service Management*. Geneva, Switzerland: International Organization for Standardization/International Electrotechnical Commission.

International Standards Organization/International Electrotechnical Commission (ISO/IEC). 2005b. *ISO/IEC 27001 Information Technology - Security Techniques - Information Security Management Systems-Requirements*. Geneva, Switzerland: International Organization for Standardization / International Electrotechnical Commission.

International Standards Organization/International Electrotechnical Commission (ISO/IEC). 2008. *ISO/IEC 38500 Corporate Governance of Information Technology.* Geneva, Switzerland: International Organization for Standardization/International Electrotechnical Commission.

International Standards Organization/International Electrotechnical Commission (ISO/IEC). 2011. *ISO/IEC 27005 Information Technology-Security Techniques - Information Security Risk Management*. Geneva, Switzerland: International Organization for Standardization/International Electrotechnical Commission.

ISACA. 2008. Top business/technology issues survey results. Available at: http://www.isaca.org/Template. cfm?Section=Home &template= /Content Management/Content Display.cfm&ContentID=43978. Accessed: May 16, 2014.

ISACA. 2012. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows, I.L.: ISACA.

Kaarst-Brown, M. L., and S. Kelly. 2005. IT governance and Sarbanes-Oxley: The latest sales pitch or real challenges for the IT Function? Paper presented at the 38th Annual Hawaii International Conference on System Sciences, Hawaii.

Ketikidis, P., S. L. Koh, N. Dimitradis, A. Gunsekaran, and M. Kehajova. 2008. The use of information systems for logistics and supply chain management in south east Europe: Current status and future direction. *Omega* 36 (August): 592-599.

(DOI: 10.1016/j.omega.2006.11.010)

Lawshe, C. H. 1975. A quantitative approach to content validity. *Personnel Psychology* 28 (December): 563-575. (DOI:10.1111/j.1744-6570.1975.tb01393.x)

Linstone, H. A., and M. Turoff. 1975. *The Delphi Method: Techniques and Applications*. Massachusetts, M.A.: Addison-Wesley.

McKenna, H. P. 1994. The Delphi technique: A worthwhile approach for nursing? *Journal of Advanced Nursing* 19 (June): 1221-1225. (DOI:10.1111/j.1365-2648.1994.tb01207.x)

Melville, N., K. Kraemer, and V. Gurbaxani. 2004. Review: Information technology and organizational performance: An integrative model of IT business value. *MIS Quarterly* 28 (June): 283-322.

Musaji, Y. F. 2002. *Integrated Auditing of ERP Systems*. New York, N.Y.: John Wiley and Sons Incorporation.

Noudoostbeni, A., N. A. Ismail, H. S. Jenatabadi, and N. M. Yasin. 2010. An effective end-user knowledge concern training method in enterprise resource planning (ERP) based on critical factors (CFs) in Malaysian SMEs. *International Journal of Business and Management* 5: 63-76.

Novak, J. D., and D. B. Gowin. 1984. *Learning How to Learn*. 1st edition. England: Cambridge University Press.

Oliver, D., and C. Romm. 2000. Enterprise resource planning systems: An outline model of adoption. Paper presented at the GITM World Conference, Memphis.

Poba-Nzaou, P. L. Raymond, and B. Fabi. 2008. Adoption and risk of ERP systems in manufacturing SMEs: A positivist case study. *Business Process Management Journal* 14: 530-550. (DOI: 10.1108/14637150810888064)

Reghavan, K. R. 2006. Internal control and operational risk: FDICIA, Sarbanes-Oxley and Basel II. *Bank Accounting and Finance* 19: 3-9.

Sherer, S. A., and S. Alter. 2004. Information system risks and risks factors: Are they mostly about information systems? *Communications of Association for Information Systems* 14: 29-64.

Standards Australia. 2004. *AS/NZS 4360: 2004 Risk Management*. Sydney, Australia: Standards Australia.

Stefanou, C. J. 1999. Supply chain management (SCM) and organisational key factors for successful implementation of enterprise resource planning (ERP)

systems. Paper presented at the annual Americas Conference on Information Systems, Milwaukee.

Tuttle, B., and S. D. Vandervelde. 2007. An empirical examination of CobiT as an internal control. *International Journal of Accounting Information Systems* 8 (December): 240-263. (DOI: 10.1016/j.accinf.2007.09.001)

Van Grembergen, W., and S. De Haes. 2009. *Enterprise Governance of Information Technology: Achieving Strategic Alignment and Value*. New York, N.Y.: Springer.

Wailgum, T. 2009. ERP investments still top the list for corporate IT spending. Available at: http://www.cio.com/article/507663/ERP Investments Still Top the List for Corporate IT Spending. Accessed: May 10, 2013.

Weill, P., and J. W. Ross. 2004. *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Boston, M.A.: Harvard Business School Press.

Wilkin, C. L., and R. H. Chenhall. 2010. A review of IT governance: A taxonomy to inform accounting information systems. *Journal of Information Systems* 24 (Fall): 107-146. (DOI: 10.2308/jis.2010.24.2.107)

Wright, S., and A. M. Wright. 2002. Information system assurance for enterprise resource planning systems: Unique risk considerations. *Journal of Information Systems* 16: 99-113. (DOI: 10.2308/jis.2002.16.s-1.99)

Development of an Enterprise Resource Planning System Risk Management Mechanism Based on COBIT 5

In an age of intensified globalization and internationalization, enterprises invest heavily in information technology to enhance their competitiveness in the process of managing and developing their commercial business and operation. Enterprise resource planning (ERP) emerged in the 1990s as one of the most widely known categories of corporate software in the software industry. The ERP system is a suite of inter-organizational integrated software that includes a shared database of multi-functional applications (e.g., finance, production, marketing, supply chain, human resources, purchase and inventory). The ERP system brings enterprises considerable organizational benefits but coincidentally introduces related risks.

This study explores and analyzes the multi-faceted risks that the entire ERP system may encounter in terms of management in the COBIT 5 framework. It then assesses the risky projects for the management team to choose or formulate coping strategies, and provides reference for enterprises equipped with the ERP system to establish a risk management mechanism. It aims, from the COBIT 5 point of view, to build a risk management mechanism targeted at the ERP system, helping enterprises identify risks in time, evaluate risk scale and significances, and respond with appropriate strategies.

This paper first, through literature analysis and based on the management-oriented COBIT 5, constructs potential risk factors of the ERP system. Then it obtains practical opinions by using the expert-dependent Delphi questionnaire to modify the results and thereby generate the ERP risk management mechanism. This management mechanism involves 4 main dimensions, 52 risk factors, and 125 control items targeted at risk factors. Finally, it verifies empirically through a case study the effectiveness of this ERP risk management mechanism. A case study is presented for greater depth of analysis. First of all, an investigation is conducted on the subject company's ERP risk management as well as on the difficulties and challenges that confront it. Next, to evaluate the target company's effectiveness, this study adopts a three-step ERP risk management program as its basis – identification, risk assessment, response, and control of risk. Before the interview, the interviewees try out the mechanism presented by this study. Afterwards, this study evaluates how this mechanism is effective in the above-mentioned three steps with respect to the target company's ERP risk management, and probes into this mechanism's contribution to the case company, its defects and whatever improvements are deemed necessary. The case company's opinions and suggestions are also collected.

Previous studies on IT risk management mostly aim to explore risk factors, and evaluate and analyze those risks. Differently, this study proposes a broad-based control framework applied to the information technology/ information system, COBIT 5, and combines it with ERP risk management corresponding with each individual field of information technology. The results of this study serve to enhance the awareness of enterprises and organizations of ERP risk management, and help them identify and respond to risks timely, make adjustments as needed, and eventually maximize the overall effects of risk management. Moreover, these results can serve as a reference for researchers who intend to delve into the COBIT framework. The future research direction is to control risk factors more effectively and further improve the whole ERP risk management program by more specific definition of risk items, addition of governance processes and complete function allocation. Nevertheless, the research limitation lies in that the ERP risks summarized in this study cannot fully cover all unpredictable ERP risks.