基於ITIL與ISO 27001建構大學校園資訊安全治理 -以中部某大學為例

曹偉駿　　鄭植尹　　蔡欣潔
大葉大學資訊管理學系
wjtsaur@yahoo.com.tw

摘要

隨著資訊技術的進步，校園資訊系統所提供的服務也越來多元化，享受便利的同時，個人的隱私資料、組織的機密文件也逐漸暴露在安全的漏洞之下。針對提升校園資訊服務的安全等級以及加強組織成員對於資訊安全的認知等目標，政府極力推動大學校園通過資訊安全管理系統稽核，目前 ISO 27001 當屬有效的稽核工具，但其中的控制措施項目相當繁雜。因此，如何簡化 ISO 27001 的控制措施以達到安全理論與實務上的最佳化已成為政府單位日益重視的議題，本論文將針對此議題提出基於 ITIL(IT infrastructure library) 與 ISO27001 之大學校園資訊安全治理模式，並以個案研究方法探討中部某大學之資訊安全治理概況。其研究流程首先針對研究對象之相關人員進行深度訪談；其次，再以策略、技術、組織、人力及環境等構面推導出相關命題，並針對大學校園環境的資訊安全治理策略提出建議，確保大學校園資訊安全治理的永續經營。

關鍵詞：資訊安全管理、資訊技術基礎建設典範(IT infrastructure library, ITIL)、國際資訊安全標準、資訊技術治理、資訊安全治理

1. 緒論

自 1988 年第一套大學校園資訊系統誕生以來，各大專院校無不致力於開發功能更齊全、層面更廣闊的資訊系統以提供更好的資訊服務品質給更多層級的使用者。伴隨著資訊系統附加效益的提升，組織對資訊系統的依賴程度也持續的提高，導致資訊與通訊面臨安全的問題，包含駭客入侵、阻絕服務攻擊(denial of service, DOS)、病毒、內部人員攻擊/偷竊等各類問題，同樣也牽涉到組織機敏性以及使用者隱私資料的交換與儲存。因此在過去的 20 年，多數企業已經意識到資訊革命對於組織帶來的衝擊,而且對於組織存亡與否息息相關，為確保資料的機密性與完整性，保護使用者的資料以及維護組織重要公文之安全，已日漸受企業組織及民眾所重視，且逐漸影響國家安全、經濟發展與社會安定等各項之議題(Von Solms, 1996)、(李東峰，2001)、(樊國楨，林樹國，鄭東昇，2005)、(葉俊榮，2005)，根據電腦安全學會(computer security institute[CSI], 2009) 訪談各類型之企業、政府及醫學機構等從事電腦安全相關人員，所得之電腦犯罪與安全調查報告指出「有 25%受訪者認為，組織因資安事件所造成的損失中，有超過 60%導因於內部人為疏失。」且資訊事件所造成的成本曾在 2005 年時高達一億三千萬美金。大學校園環境為典型知識密集型組織，但確未曾受到與商業組織相同的重視(Doherty, Anastasakis, and Fulford, 2009) 大學校園中擁有龐大的教職員個人資料、學位論文、甚至是專利著作屬於 B 級的重要公共基礎建設。因而，國家資通安全會報第十七次工作小組會議結論，政府部會中 A、B 級單位需在民國 96 及 97 年底以前通過資訊安全管理認證(國家資通安全會報，2005)，雖然政令已頒布實施，但根據國家資訊基本建設發展協進會(NII 發展協進會)於 2008 年 11 月出版之「校園資安防護認知及法令宣導」中所提及之國內大學建置 ISMS 概況，在期限內達成的大專

院校並不多，因此，如何讓資訊技術在安全系統的要求下提升效率與效能，降低因繁複的安全控制措施所帶來的不便，即為本論文的研究動機之一。

此外，以資訊安全治理而言，有學者 Brown and Grant (2005)指出在公司治理議題上，雖然資訊技術與資訊安全一直扮演著重要的角色，但是此兩者在連接上較薄弱，而且大部份的研究都著重於資訊安全治理的觀念性架構，對於實務研究上較缺乏，無法在公司治理上有效實行，即為本論文的研究動機之二。

最後，在資測會開辦的「ITIL 結合 ISO27001 之實務課程」當中曾提及 ISO 27001 無論在導入階段或是通過驗證的後續維護，資訊部門最常面臨的，就是如何符合 ISO27001 標準中，所有要求的持續性改善、降低 IT 服務中斷、提高可用性及如何定訂 KPI，以進行有效性評量，這些都在 ITIL 的理論中，有相當多可供借鏡之處，但目前從事這兩者結合應用的研究甚少，因此，本論文將依據現有的文獻嘗試將兩者做結合應用於建構大學校園之資訊安全治理，此為本論文研究動機之三。

根據上述之研究背景與動機，由於本論文研究目的在於藉由 ITIL 與 ISO 27001 的整合來簡化資訊安全管理標準繁複的控制程序，以達到有效率的大學校園資訊安全管理。因此，必需借重 ISO 27001 詳細的規範來進行資訊安全風險的管理與查核，另外又必須導入 ITIL 的觀點將財務及需求管理納入其中，考量成本因素進而取得管理高層的支持。綜上所述，若將兩標準整併進行勢必要考慮到以下因素(黃小玲，2010)：

一、所有標準的策略目標，皆以整體組織為基礎實踐。
二、共用(含審查及改善機制等)管理架構。
三、降低執行、維護管理的資源與成本。
四、ISO 標準的流程與一致性。
五、文件與紀錄集中管理。
六、產生共通性之管理報表。

當所有條件具備之時則可達到 ITIL 與 ISO 27001 的有效整合但需考慮建置初期的整合規劃與實作成本，以避免重複投資，因此如何將 ITIL 與 ISO 27001 進行初步的整合及規劃以提供大學校園建置資訊安全治理則為本論文之主要目的。此外，現今各大專院校均積極推動校園服務 e 化。即使政府積極推動資訊安全管理認證，但仍然會因管理階層的疏忽、訊息傳達的效率不佳亦或教職員工及學生對安全的認知不足，而導致資訊安全事件的發生。因此本論文將採取個案研究，並以中部某通過 ISO 27001 資訊安全管理認證之大學為研究對象，探討以下四個項目：

一、探討大專院校資訊安全現況，以及資訊安全、資訊技術治理、資訊安全治理、ITIL 與 ISO 27001 等領域之暨有文獻。
二、了解大學校園擬定資訊安全政策所採用之資訊安全標準。
三、了解資訊安全治理在大學校園治理中所扮演的角色，以及其所帶來之效應。
四、透過個案研究的方式，探究大學校園資訊安全建置之情況，並藉此分析其安全需求。

2. 文獻探討

2.1 資訊安全管理

根據美國國家標準與技術學會(National Institute of Standards and Technology, NIST)於 2007 年指出資訊可以透過網路來互通共享，同時也將資訊暴露在多樣化之威脅(Threat)與脆弱(Vulnerability)中，部份資訊可以公開，但部份資訊屬機密，不可揭露且不可篡改，必須作保密的管制以防使用者有意或無意的讀取或更改，同時也必須確保資料的機密(Confidentiality) 、完整性(Integrity) 、可用性(Availability)以達成資訊安全之目的(NIST, 2007)。學者 Von Solms and VonSolms (2004)則認為資訊安全管理十項重要關鍵：(1)資訊安全是公司的責任；(2)資訊安全是企業議題，並非全部是技術議題；(3)資訊安全管理是項多維的紀律；(4)

資訊安全必須基於鑑定風險；(5)資訊安全管理為國際上最主要實施的重要任務；(6)組織的資訊安全政策是絕對必要的；(7)資訊安全承諾的實行與監控是絕對必要的；(8)合適的資訊安全管理架構是絕對必要的；(9)使用者意識為資訊安全重要核心；(10)透過資訊安全經理及基礎建設的支持並有效執行任務。

2.2 資訊技術治理

資訊技術治理對公司來說，是一項重要的法律，雖然這項目標已達成，但仍有多數企業未建立適當的控制。因此學者研究發現資訊技術在企業中具有驅動利益的價值，其範圍包含(1)策略整合；(2)價值傳遞；(3)風險管理；(4)資源管理；(5)績效衡量。

一、策略整合(Strategic alignment)：
為了達成企業整合，利害關係人驅動策略整合，保證資訊技術策略與企業策略一致；保證資訊技術傳遞的時間符合預算的期望，並擁有合適的功能及效益；平衡支持企業體系之間資訊技術的投資，並協助企業成長；市場決策之資訊技術資源的重點即是引導資源驅動策略及提高顧客忠誠度。

二、價值傳遞(Value Delivery)：
只要實際成本以及投資利率受到管理方能達成傳遞價值的預期效益。董事會應保證資訊技術整合致使傳遞價值以確保基礎建設，使企業成長、提升收益、顧客滿意度以及驅動競爭策略。

三、風險管理(Risk Management)：
風險管理是驅駛董事會必須向股東、管理者、員工以及顧客去證實企業治理的效益。董事會應進行風險管理，以確定組織對於重大風險以及說明承擔或規避風險的政策。堅持將風險管理納入企業的運作中，以便能快速回應變動的風險至適當的管理階層。

四、資源管理(Resource Management)：
在處理資源管理方面，董事會應確保適當的方法與足夠的能力存在於組織管理資訊技術工程中，並有益於真實且可達成目的。實際上，董事會治理資訊技術的支出可能產生無意義的成本以及落實組織有利的行動。

五、績效衡量(Performance Measurement)：
為了衡量資訊技術治理之績效，可利用平衡計分卡衡量公司績效、用戶定位、操作以及未來方向。所謂可以利用績效衡量將策略轉換達成目標的行動。透過衡量其間的關係及完成目標必要的知識資產來達成。

2.3 資訊安全治理

由於本研究著重於建立一套資訊安全治理，因此針對曹子珊、曹偉駿(2004)對資訊安全治理文獻作介紹。公司治理是一套責任與實行的做法，應由董事會及執行者提供目標與策略方向，以確保目標的實現，並確定風險能適當地管理與查核，進而證明企業的資源是可靠且低風險的(ITGI, 2007)、(Moulton and Coles, 2003)，因此 Wilson (2007)認為治理與安全是結合在一起的活動及規章。根據 Pasquinucci(2007)指出在許多情況之下遵循傳統的作法實行風險的分析與管理，是無法解決新技術所帶來的威脅，因此我們更需要發展更實際且有效的方法，這不僅是技術方面的資訊與通訊技術安全，而是整個公司的資訊安全治理過程。學者 Andersen (2001)認為資訊安全治理乃是「一種董事會及執行者的責任，屬於公司治理的部份，它包含了領導、組織結構與程序並執行資訊技術政策，以確保組織的資訊技術維持並延伸組織的政策與目標，以達到企業競爭優勢之組織能力」，也就是說建立並維持一種治理架構，以確認資訊安全政策與經營目標相一致，並同時符合現行的法律規章。學者 Johnson (2006)研究指出在資訊安全治理中，人的行為是最難控制，也是組織中最重要的資產之一，但也是最薄弱的一個環節，Relyea(2008)也認為「人」在資訊安全上所扮演的角色非常重要，必須對資訊安全負起職責。許多研究

指出在資訊安全治理模式並不是另外的管理模式，而是將管理納入一個組織性的集體控制循環模式中，其主要是由結構(structure)、控制(control)、程序(process)所組成的議題，並實際運用領導、實行、控制，以確實達到組織的目的(Prakash and Hart, 1999)、(Von Solms and Von Solms, 2006)。因此提出資訊安全治理的控制循環，其控制循環之核心原則必須符合公司之相關活動，可經由上而下之三個循環步驟，如圖 1 所示：

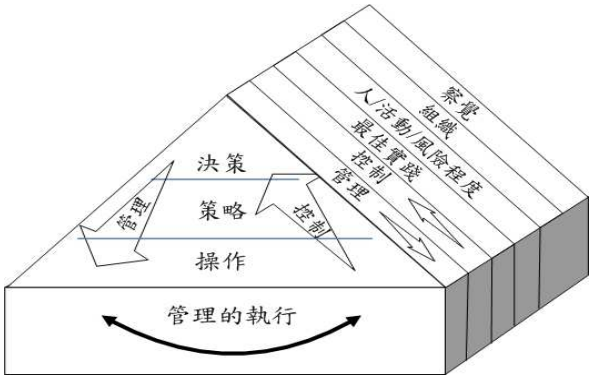

圖 1 資訊安全治理之控制循環

2.4 ITIL 與 ISO 27001

一、 ISO 27001

許多研究發現，可將 ISO 27001 所規範之資訊安全控制有 11 大管理要項區分為策略(strategy)、技術(technology)、組織(organization)、人(people)與環境(environment)五構面，其組成 STOPE 模型，以此作為發展電子政府評估之基礎，如表 1 所示(Bakry, 2004)、(ISO 27001, 2005)、(Broderick, 2006)、(Saleh, Alrabiah,and Bakry, 2007)、(Esteves and Joseph, 2008)。

二、ITIL

ITIL 是種縮寫，全名是 IT infrastructure library，取名自各單字的首位英文母集合而成，1980 中期由英國政府電腦電信局(CCTA)受委託發起專案，由學界研究學者們與各大資訊廠商(如 IBM、HP、CA 等)共襄盛舉，彙整各產業界優良資訊環境管理經驗，集結成冊，共約 40 本書，這也是命名 library 的源由。去蕪存菁，集各家之大成，理論立意適用各產業，經過時間淬練，為最佳實踐架構。 ITIL 與舊有的資訊管理方法論不同，不以功能、系統類別去個別探討，而是重視流程整合，提昇資訊效能，符合經濟效益，進而支援企業的營運。ITILv3 的結構(ITGI, 2007)如圖 2 所示。

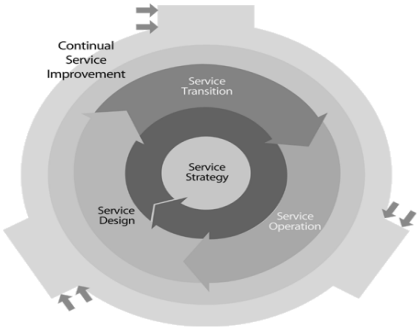

圖 2 ITILv3 基礎架構

表 1 STOPE 之 ISO 27001 控制項目

構面	ISO 27001 控制目標	構面	ISO 27001 控制目標
策略	A.5 安全政策(Security Policy)	組織	A.6 資訊安全組織(Organization of Information Security)
技術	A.10 通訊與作業管理 (Communications and Operations Management)		A.7 資產管理(Asset Management)
			A.14 企業營運持續管理(Business Continuity Management)
			A.13 資訊安全事故處理 (Information Security Incident Management)
	A.11 存取控制(Access Control)	人力	A.8 人力資源安全(Human Resources Security)
	A.12 資訊系統之獲得、開發與維護 (Information Systems Acquisition, Development and Maintenance)	環境	A.9 實體與環境之安全管理(Physical and Environmental Security)
			A.15 遵行(Compliance)

3.研究方法

資訊管理的研究方法可歸類為以下六種：個案研究、實驗研究、彙總研究、模式推導與系統展視等：前四種為歸納法，後二種為演繹法(梁定澎，1997)。本研究主要是期盼發展「健保局之資訊安全治理」。故採取參與觀察、深度訪談與文件檔案收集等方法為主的探索性研究(Yin, 2001)。個案研究法包含對現行記錄及檔案之探討，以及現象發生原因之觀察，且不具結構性之訪問，及其他資料蒐集方法之應用(謝安田，2006)。

一、研究對象

由於本論文研究設計將 ISO 27001 管理要項劃分為策略、技術、組織、人員、環境等五個構面來探討且本論文研究之目的在於建構大學校園之資訊安全技術治理模式，尤其是本論文所探討之對象已於民國 97 年成功導入 ISO 27001 資訊安全管理並取得第三方稽核認證，因此，訪談對象的選擇將從該校資訊安全政策所規範之管理人員選取策略、技術及組織層面代表性人物，另外，為得知資訊安全政策是否有效傳達以及全校教職員生對於資訊安全的認知程度，因而在使用者面亦選取資安專長教師一名及學生代表一名，一共五人，如表 2 所示，在獲得受訪人同意之後，約定時間地點對受訪人進行訪談。

表 2　受訪者資料

受訪者	學／經歷背景
學生代表 A 學生	學士／實務經歷 0 年
資安專長 B 教師	博士／實務經歷 10 年
電算中心 C 主任	博士／實務經歷 8 年
電算中心 D 組長	博士／實務經歷 5 年
電算中心 E 組長	博士／實務經歷 12 年

二、資料收集方法

為使本論文研究架構更為完整並符合大學校園之需求，本論文主要先針對 ITIL 與 ISO 27001 蒐集國內外相關文獻、研究成果，並配合行業特性，進而設計雛型模式。為避免設計的指標太偏向研究者本身的主觀看法，無法於實務上有效的應用。因此，另一項重要的補強工具，則是使用深度訪談之方式，由研究者與受測對象進行面對面的溝通與訪問，期望經由實地的訪談與研究對象取得共識，並為其發展合適的治理制度。本論文在個案研究進行的過程中採用多種資料蒐集法取得所需之相關資訊，其中資料蒐集的方法包括：

1. 文獻探討與整理：蒐集、整理、閱讀與研究主題相關文獻，如資訊安全管理、資訊技術治理、ITIL 及 ISO 27001 等。
2. 實地觀察：對研究對象進行實地觀察以瞭解其實際運作流程、組織成員對資訊安全的認知、資訊安全政策的實施等情形。
3. 深度訪談：訪談內容針對 ITIL 及 ISO 27001 之控制項目間的關聯性所設計。藉由受試者之經驗與知識，增進對大學校園之資訊安全概況及可能遭遇事項的瞭解。因此，針對研究對象之電算中心主管及相關人員進行深度訪談。本論文依 (Bakry, 2004)、(CNS 27002, 2007)、(ITGI, 2008)、(Broderick, 2006)、(Saleh, Alrabiah, and Bakry, 2007)、(Esteves and Joseph, 2008)設計訪談如表 3 所示。

4.個案描述與分析

以下各節將對本論文所研究之個案進行詳細的描述與分析。首先於 4.1 節針對研究個案之相關背景、組織與安全概況詳細描述，其次於 4.2 節進行命題推導，最後於 4.3 節針對研究結果做出分析。

4.1 研究個案之相關描述

一、研究對象之背景與組織

本論文所選取的研究對象為位於國內中部之某大學。該對象自 1990 年創校迄今，師生人數約 11000 人。其經營策略主要透過師徒傳承制和產學合作的方式達到科技結合人文以及理論與實務並重的企業夥伴型大學，並於 2009 年 12 月與國內 107 家企業簽署「企業夥伴策略聯盟」，且該研究對象也配合政府的宣導於 2009 年 2 月順利通過第三方稽核驗證，取得 ISO 27001「資訊安全管理系統(ISMS)」認證。鑒於

表 3　訪談題目

構面	ISO 27001 控制目標	ITIL v3 流程	題目大綱
策略	A5 安全政策	評估、財務管理、權限管理、資訊安全管理、服務連續性管理	貴校之資訊安全政策由誰制定?是否有法源依據?上一次修訂是合時?透過什麼樣方式公告?
技術	A10 通訊與作業管理	評估、需求管理、能力管理、變革管理、知識管理、事件管理、問題管理、權限管理、服務報告、服務測量、供應者管理、服務請求管理、制定服務策略、服務投資管理、服務級別管理、轉換規劃與支持、服務驗證與測試、廢除與部署管理、7階段改善流程、服務連續性管理、服務資產與結構管理	貴校資訊設施的使用情況如何是否有文件進行相關規範?校園資訊系統的開發是否曾委外處理?校園內是否曾發生資料外洩、遺失、誤用等資訊安全事件？
	A11 存取控制	變革管理、問題管理、權限管理、資訊安全管理、服務連續性管理、轉換規劃與支持、服務資產與結構管理	貴校所提供之資訊服務有哪些種類主要提供給哪些對象？是否對這些服務進行相關之規範?
	A12 資訊系統之獲得、開發與維護	評估、問題管理、權限管理、變革管理、供應者管理、服務級別管理、服務請求管理、資訊安全管理、服務連續性管理、轉換規劃與支持、服務驗證與測試、廢除與部署管理、服務資產與結構管理	貴校資訊系統的開發程度如何？其開發過程為何？在使用上是否合乎您需求?最近一次更新是在什麼時候?
組織	A6 資訊安全組織	服務台、權限管理、應用管理、科技管理、變革管理、能力管理、供應者管理、服務級別管理、資訊安全管理、服務連續性管理、轉換規劃與支持、服務運作法則及責任	貴校是否有專責資訊安全的單位，其組織如何形成?其組織職掌與運作情形為何?
	A7 資產管理	問題管理、科技管理、轉換規劃與支持、服務資產與結構管理	貴校之資訊資產如何分類?是否列冊管理？
	A13 資訊安全事故處理	財務管理、知識管理、事件管理、事故管理、問題管理、權限管理 服務測量、資訊安全管理、服務請求管理、服務連續性管理、發佈與部署管理	貴校是否曾接獲資訊安全事件通報?其處理情形為何?
	A14 企業營運持續管理	評估、服務台、事件管理、事故管理、可用性管理、服務連續性管理	貴校是否爲資訊相關事項成立跨部會小組？ 是否爲任何可能之危機擬定緊急應變措施?
人力	A8 人力資源安全	權限管理、資訊安全管理、供應者管理、廢除與部署管理、服務運作法則及責任	貴校對於人員的聘僱辦法為何?在資訊安全相關辦法上是否載明個人職權範圍與相關罰則？
環境	A9 實體與環境之安全管理	科技管理	貴校在人員的進出管制上有什麼樣的規定?校園內設備損壞率有多高?
	A15 遵行	問題管理、權限管理、供應者管理、服務級別管理、轉換規劃與支持、服務資產與結構管理、服務運作法則及責任	貴校在擬定資訊安全政策時是否有法源根據? 是否曾檢驗政策頒布實行後的成果?

該校對於經營策略的實踐程度及本研究需求，因而引以為本論文之探討對象，該校之詳細資訊如表 4 所示。

表 4　研究對象資料

大學校方資訊	
創立時間	1993 年 3 月
地理位置	台灣省中部地區
經營目標	企業夥伴型大學
學生人數	約 1 萬人
教職員工及行政人員人數	約 871 人
是否具有資訊系統	是
是否通過資訊安全認證	是
是否具備資訊安全政策文件	是
是否具有專職之資訊部門	是
資訊處理基礎設施	有線網路、無線區域網路及通訊相關硬體設備

負責保存與實踐該校資訊安全政策之權責單位為該校之電子計算機中心，其部門下轄三個組別，並設有主任一名、組長兩名及相關人員 15 人，專司校園內所有資訊相關作業以及相關辦法之擬定，因此，本論文也將針對此單位選取具代表性人物作為本研究之受訪對象。本論文研究對象之組織分佈如圖 3 所示。

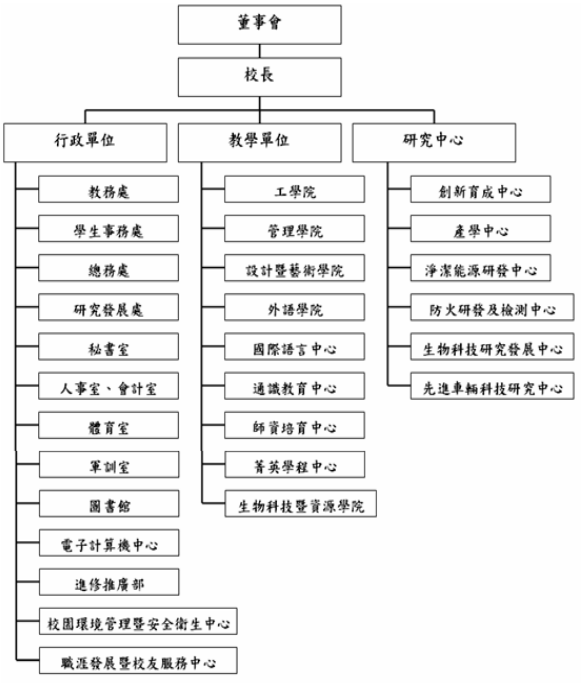

圖 3 研究對象組織分佈

二、研究對象之資訊安全概況

本節將依據實地觀察的情況與資料收集的結果，針對該研究對象之資訊安全概況分做具體的說明。說明的方式將依 STOPE（策略、技術、組織、人力、環境）等五個構面分別以該校之資訊安全組織、資訊系統、資訊安全政策、資訊安全人力及資訊安全環境等五個部份進行探討。

(一) 資訊安全組織

依據本研究對象之組織章程，凡隸屬該校之資訊及資安相關業務，均交由該校之電算中心負責承辦，其組織圖如圖 4 所示。

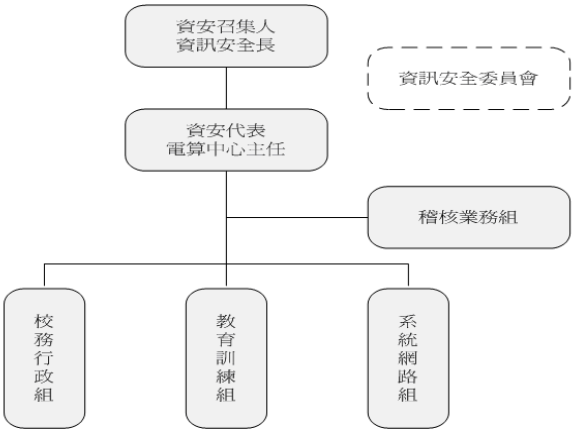

圖 4 資訊安全組織配置

依據校園組織章程規定，資安召集人主要由校長擔任並由校長所遴選之電算中心主任出任該校之資訊安全代表，其管轄範圍除原屬電算中心所屬之三個組別，另加入由各部會管理人員所組成之稽核業務組。以下將對各組別的執掌逐一進行說明。

1. 校務行政組：

   負責規劃、整合及開發校務行政資訊化之相關事宜。

2. 教育訓練組：

   負責規劃、推動人員資訊教育之相關事宜。建立全校授權軟體管理制度，以落實電腦軟體智慧財產權管理制度。加強學生對網路倫理及智慧財產權之認識宣導。

3. 系統網路組：

   負責校園網路安全及系統建置的規劃、管理及推動。定期檢視校園網路合法軟體及建立不當資訊防治機制。

4. 稽核業務組：

負責該校之資訊安全政策的維護與落實。提供明確之指示，適時修訂資訊安全政策，以確保本其政策符合現行之需求。

(二)資訊系統

若依據教育部所頒布的『教育體系資通安全管理規範』，將本研究對象之資訊系統依業務特性劃分為學術網路系統以及行政資訊統。該校對於學術網路系統的管理上為考量服務品質與安全需求，除了確實依據使用者的層級及應用範圍進行明文規定並公告辦法實施；另外，於電算中心也為學術網路的使用設立了一個組別來進行規劃、監控、維護及管理。運行至今，除了未遵守校園網路使用規定的舉報，尚無重大之資訊安全情事發生。至於行政資訊系統方面，該校對於校園 e 化的進行相當徹底，不但依各單位層級之業務需求分別為其設計專屬之行政資訊系統，此外還再電算中為其設置一個專責的組別，並分派與各組員進行維護及管理。由於使用者數量龐大，且各單位業務執掌相當繁雜，因此在運行過程中偶爾會因為系統超載而造成服務中斷，但因其分工規劃的相當詳細且皆有專員負責，因此恢復服務的速度相當迅速。

(三)資訊安全政策

該校之資訊安全政策主要目的在於維護該校電算中心電腦機房正常營運及為保護該校核心業務相關資訊資產（資訊資產包括資料、系統、設備等）之安全，防範資訊處理作業過程發生影響資訊及系統機密性、完整性及可用性之安全事件，確保該校資訊處理作業能安全有效地運作，因此制訂該資訊安全政策。本政策共分為八節來規範該校資訊安全的建置，如表 5 所示。

(四)資訊安全人力

該校配置之資訊安全人力主要如圖 4 所示、共計一名主任、兩名組長以及 15 名資訊技術人員，共計 18 名。

(五)資訊安全環境

該校之校園環境進行人員進出管制，各開放資訊設施皆有使用規定。校園內建置有線網路、以及無線區域網路環境。資訊服務提供的對象主要為學生、教師及職員。

4.2 命題推導

在進行推論時，由於同一事物可能具多重屬性，因此在評斷事物的過程中，必須同時對多個相關因素作綜合性的考量與評估。因此當本研究將 ITIL 及 ISO 27001 結合至大學校園資訊安全治理策略循環控制進行探討時，將依循(1)策略規劃，(2)技術管理，(3)組織管理，(4)人力資源安全管理，(5)資訊安全環境管理等五個構面進行命題推導 (參照表 1、表 3 所示)，期望能旁徵博引，吸取較好的管理經驗以提供更廣泛的管理範疇、進而協助大學校園資訊安全政策的制訂。

一、策略規劃

(一)命題 1.1：資訊安全政策的制訂應參考資安相關法令及施行單位業務上的需求，並經由管理階層核准，以適當方式向所有員工公佈與宣導，在必要時告知相關單位及合作廠商，以利共同遵守。

本論文研究發現，該校於制定資訊安全政策確實參考「教育體系管理規範」、「電腦處理個人資料保護法」、「教育部所屬機關及各公私立學校資通安全工作事項」等法源依據，並載明各項相關規範，惟獨在其公告實施的過程出現瑕疵。

該校電算 C 中心主任回答：「本單位在建置資訊安全策略的同時，獲得校方高層的充分授權及支持且顧及資訊安全需求及教育體系相關之資訊安全法規，因此成立了跨部會小組來共同研擬資訊安全的需求及適用範圍，並依教育部所頒布的資訊安全規範進行規劃，因此這份文件應該沒問題。」該校電算中心 D 組長表示：「早在政府推行資訊安全認證之前，我們就已經為校園內制定相關的資訊安全文件，例如：個人資料隱私權保護、各資訊系統及硬體設備的使用辦法等等」該校電算中心 E 組長表示：「本校的資訊安全政策制訂大抵上

表 5 資訊安全政策

資訊安全政策章節	欲達成之目的
1.目的	維護該校電算中心電腦機房正常營運及保護該校核心業務相關資訊資產之安全，防範資訊安全事件的發生，確保該校資訊處理作業能安全有效地運作。
2.法源依據	「教育體系管理規範」 「電腦處理個人資料保護法」 「教育部所屬機關及各公私立學校資通安全工作事項」
3.資訊安全目標	資訊服務持續不中斷 資訊保護嚴密不外洩
4.資訊安全政策期許	建立一個完整、可行、有效之資訊安全管理系統，以為該校資訊安全提供最佳之保障。
5.驗證範圍	大葉大學電算中心電腦機房
6.責任劃分	明訂該校資訊安全組織之執掌，及校內所有人員所應負起的資訊安全責任。
7.風險評鑑與管理	為達成該校資訊安全願景，符合政策目標，特制定風險評鑑與管理程序書，進行風險評鑑與管理，以有效管理資訊資產面臨之風險，降低風險至可接受範圍。
8.資訊安全政策之遵循	該校電算中心所有員工、簽約廠商未遵循本政策或相關資訊安全規定，或行使其他任何危及該校資訊安全之行為，將訴諸適當之懲罰程序或法律行動；對於資訊安全法令或技術提供改進意見，經執行確具成效者，給予適當獎勵。

是以 ISO 27001 的規範為藍本，由於公告實施的時間並不長，因此尚無更新資料。」該校 A 學生表示:「對於校內之資訊安全政策，我了解的不多。」

二、技術管理

(一)命題 2.1：施行單位應鑑別(identify，該資料機密等級與存取動作)與文件化相關之存取行為，建立存取控制政策的內容及範圍，防範非經授權存取的可能及危險，降低相關資訊或檔案遭竊取的威脅。

該校電算中心 C 主任回答:「其實早在 2008 年的 6 月，本單位就開始依服務等級，為存取控制的規定進行文件化。」; B 老師表示:「根據以規範的存取行為必須文件化且公告實施，並提供取得的管道，以利相關人員取用。」; A 學生表示:「除了資訊硬體設施的取用規定，針對文件資料的取用並不了解」。

(二)命題 2.2：系統開發與維護應納入資安方面的考量，從初始的規畫、設計、乃至測試、上線、維護等程序，針對可能的危機與錯誤採取相對的措施，在不違反各資安政策與措施的情形下，符合施行單位的要求。

該校負責系統開發的 D 組長表示:「本校資訊系統的開發，主要包含需求、更新異動與測試驗收等三個部分。除了擁有絕對必要性之系統外，系統的開發通常要得到各單位具填系統需求申請之後才開始運作，系統完成的兩週內送交需求單位驗收，通常我們會要求該單位指派一名人員專責該系統的維護及管理，若有須調整的項目本單位即以該員為橋樑進行系統的更新異動。此外，由於系統採行需求開發的方式進行，因此，除非申請單位提出相關安全需求，否則即不再建置考量之內。」; C 主任則表示:「由於本校資訊安全管理導

入的時程尚短，在日後的資訊系統的開發及更新上，本單位會主動為其考量資訊安全因素。」；根據 B 老師表示：「目前校園內使用者對於資訊安全的認知有限，在系統的建置上加入資安控制措施，反而導致使用者覺得不便的不便，因此，教育使用者對於資訊安全的認知應該優先執行。」

(三)命題 2.3：為確保正確以及安全的操作資訊處理設施，降低各種可能的風險與損害，維護資訊處理與通訊服務之完整性及可用性，必須設立通訊與作業安全之管理措施。

該校電算中心主任表示：「為確保本校資訊處理設施完整，降低人為因素之造成的損害，本中心在系統主機、網路使用以及校務行政系統等更方面皆設有相關標準作業流程，並公告於電算中心網站提供需要之使用者下載。」；該校 A 學生表示：「由於本校網路設備的管理職權傾向全權委由電算中心處理，對於相關的辦法，除非影響自身使用上的權益，否則不是很清楚。」；該校 B 老師則說道：「雖然曾上電算中心網頁瀏覽相關的辦法，但其規範的對象大都僅限於軟、硬體設施，關於人員及通訊作業的安全規範的確尚待加強。」

三、組織管理

(一)命題 3.1：為確保施行單位資產獲得適切的保護，明確的資產分類與保護層級，將有助於資產保管的執行效率，降低受危害的可能，勢必進行徹底財產清點與分類。

E 組長為負責電算中心所有軟硬體設施的最高指導人員，在本校具備十年以上的網路設備管理經驗，根據 E 組長口述表示：「資訊是無形的，但其附加價值可能高過有形的硬體資產，本單位對硬體設備等資產均有明定之管理辦法，另外所有資產街名列於財產清冊當中，並由專人負責。」；D 組長則表示：「有關資產分類與管理的規定，目前主要以資料保存的型態為主。」C 主任則表示：「資訊系統應包含軟、硬體，且應分等級管理。」

(二)命題 3.2：針對安全事件的發生，應即刻進行反應，並採取適當的處理措施，降低損害的擴大；除了忠實紀錄事件發生的經過，更需保存相關的資料紀錄作為改進的參考。

本校電算中心 C 主任表示：「本校的各單位的資訊系統皆有專人負責，因此當發生故障或中斷，專責人員可以在最短的時間內使其恢復運作，但本校尚未發生任何重大資訊安全事件。」；E 組長表示：「雖然平日對於網路上的異常行為皆有紀錄及監控，在接獲障礙通知時也趕在第一時間進行搶修，但最主要的防範方式還是必需從使用者對資訊安全的認知做起。」；A 學生表示：「學校的行政資訊系統的確會偶爾沒辦法使用，但電算中心修復的速度相當迅速。」；B 老師表示：「學校可嘗試以通識課的方式，鼓勵學生參予，以提升學生對資訊安全認知。」

(三)命題 3.3：當遭遇重大意外造成學校或單位運作中止的突發狀況發生，為使必要業務得以不受影響持續運行，將其傷害減至最低，平日應執行相關的規劃及檢測。

電算中心 D 組長表示：「後續的監督及稽核工作較難持續，主要是因為其他單位對電算中心有一定程度的依賴，加上大部分的資訊安全管理主導權在本單位，因平日業務繁忙同仁實在難以在抽身去執行這些事項。」；E 組長也表示：「平日進行準備，確實有防範於未來的效果，但也需要各部門願意抽調專責的人手與我們配合。」

(四)命題 3.4：組織內之資訊安全施行單位應指派適當權責之高層主管人員(類似資訊長的角色)，代表學校或單位落實資訊安全的決心並推動資訊安全組織，召開資安會報、訂定權責分屬、主導評估建置等相關活動，除了解各項需求外，籌備必要資源，確保資安措施正常運作，建立起一完善、安全之環境，降低組織資安面臨威脅的機率。

該校電算中心 C 主任表示：「校內行政高層對於資訊安全的階段性發展相當重視，亦全權委任本中心承辦，為落實資訊安全的目的，更是積極的通過符合 ISO 27001 的第三方認證，以此為藍本對資訊安全擬定策略，並預計逐年檢視其落實成

果。」；D 組長表示：「本校所擬定的資訊安全分定量化政策與定性化政策，為檢驗其實施程度，另外組織了跨部會稽核業務組以逐年檢視資訊安全目標的達成度。」；B 老師則認為：「資訊安全不應該只包含階段性任務，應從全面的從安全的角度來進行發展，應確實對人員進行教育，政策應彈性調整確實實施，專業人員也應定期接受教育或訓練以應付日新月異的安全挑戰。」

四、人力資源管理

(一)命題 4.1：施行單位所屬相關人員需針對其擔負的資安責任，進行管理與教育訓練，透過定期的課程訓練，確保其在職位上能執行各項相關資安措施，降低可能的資安風險。

該校電算中心 C 主任表示：「本單位雖無硬性規定人員必須定期參加教育訓練課程，但同仁仍然自行自發的參加相關資訊集會或自我進修以精進其專業技能，日後將會對其進行規劃。」；E 組長則表示：「從事資訊相關工作，必須保持知識技能的持續成長以應付時代的快速變遷，因此自我進修是不可或缺的。」B 老師則說：「在人力資源的管理上，不僅要考慮員工技能，還要考量員工本身可能帶來的資訊安全風險，因此在人員聘僱前後及日常作業都必須加以規範。」

五、資訊安全環境管理

(一)命題 5.1：為保護資訊處理設施以及所在位置的安全，除環境的管制保護措施外，軟硬體的防護措施也需徹底實行，以有效降低資安事件發生的機率。

該校電算中心 C 主任表示：「本校執行資訊設施的管制應屬相當徹底，針對每個區域皆設定開放層級及管理辦法，對於網路環境的使用辦法均清楚的載明人員之相關權責與罰則。」；E 組長則表示：「雖有明確的辦法公告實施，但違反使用規定遭舉報的案例還是相當頻繁，由此可見，使用者對於其自身在於資訊安全上所扮演的角色即可能照成的影響明顯認知不足。」；A 學生則說：「校園環境中的人員管制實施得相當徹底，相信能對校園資訊安全設施有效的進行保護。」

(二)命題 5.2：所有的 ISMS 控制措施與管理條款，除了須符合施行單位的政策外，與相關法規的符合性亦須相符，避免缺乏法源上的依據，而在於系統方面的稽核上，也需採用適當的工具進行檢測，確保運作維持不中斷。

該校電算中心 C 主任表示：「本校的資訊安全管理系統尚為建置初期，但相關的控制措施及指導皆依據 ISO 27001 國際標準、個人資料保護法及教育體系資通安全規範等法源依據來進行。」；D 組長則表示：「在系統稽核的方面也將會確保相關之資訊安全措施或規範符合現行的資訊安全管理標準、營運及相關法律與法規之要求，並每年至少查核一次。」

4.3 研究結果

根據先前所提之研究目的，本論文透過質性訪談的方式以 ITIL 與 ISO 27001 的結合來檢視該研究對象之資訊安全政策與資訊安全目標是否一致，以及瞭解大學校園之施行單位是否能有效的實施資訊安全政策。如此一來便可確保目標的實現，以及風險的有效管理與查核，使政策能達到最佳效益。本論文研究之主要成果有以下四項：

一、根據資料蒐集的結果顯示，大學校園資訊安全政策的制定大都依據 ISO 27001 資訊安全標準來制定，此外，教育部考量教育體系及相關單位的特性，在不過於耗費資源，又不暴露單位於資安危機的前提之下依據 ISO 27001 修訂了教育體系資通安全規範，並於 96 年公告各相關單位實施。

二、根據校內資訊安全目標的落實程度檢測發現，大學校園的資訊安全大部分僅是框架的實現，對於人員的教育及其中的精神尚無法徹底實行，只能著重於事後的補救無法於事先進行預防，因此，增進校內人員對其在於資訊安全的職責與角色之認知，以降低使用者不當操作造成資訊安全事件的風險，是比事後

的事件管理更能有效達到大學校園的資訊安全。

三、在 ITIL 與 ISO 27001 的整合上發現，若要有效的簡化 ISO 27001 的控制措施而又不喪失其中的精隨，勢必得先確實的對人員職掌及資產進行詳細的紀錄及劃分，將其關聯性進行文件化，並將所有文件及記錄集中由專人管理，並先導入 ITIL 中較易看見成效的服務檯功能，將相關文件及記錄進行整理，並考量使用者需求開放單一窗口對使用者進行服務。

四、本論文依專家訪談內容以及 ITIL 與 ISO 27001 的結合，針對大學校園環境資訊安全治理提出建議。

5. 結論與建議

本論文將於此節中提出結論及建議。首先，說明本論文之結論，其次針對大學校園的資訊安全治理提出建議。

5.1 結論

為達到有效的治理不光只考慮營運目標，必先了解其組織環境、業務執掌及其運作過程，因此，本研究運用個案探討的方式針對大學校園資訊安全環境、資訊安全組織與資訊安全策略的落實成果進行一個全盤的了解。進而從本論文之五位受試者的訪談資料當中，根據 ITIL 與 ISO 27001 控制項目的集合推導出符合策略、組織、技術、人力、環境等五個構面的相關命題。該個案於 2008 年間開始導入資訊安全管理系統並於近期內通過 ISO 27001 資訊安全系統認證，因此，在資訊安全的管理上應是在一定的水準之上。據研究結果顯示，其在於實體環境上落實的程度堪佳，但在於使用者的資訊安全認知上較為薄弱，造成的原因大部分為人為因素。因此，在資訊安全的落實，不僅僅是階段性目標的達成，而是應該透過妥善的教育及宣導並結合資訊安全理念於組織管理文化當中，經由全盤性的考量針對全校師生資訊安全保障需求，及內外部可能遭遇之系統威脅，進行鑑別、管理、減少才能降低資訊資產所面臨的風險，達到組織永續經營的目的。因此，在 5.2 節將對本論文所探討之個案提出建議。

5.2 建議

本論文主要透過結合 ITIL 與 ISO 27001 對大學校園的提供資訊安全治理的模式，ITIL 主要的功能在於將流程最佳化，它能將 ISO 27001 所提供的流程最佳化，以達到有效率的資訊安全治理。以下為本論文針對大學校園的資訊安全治理所提出的建議。

一、資訊安全策略的擬定

資訊安全政策的擬定除了必須通過組織管理高層的支持，此外，必須考慮到必要性、財務狀況是否許可、是否考慮到後續可能發生的情況，政策制定實施以後要定期檢視其達成效率並進行評估改進。

二、資訊技術的安全

資訊技術的部份就屬通訊及作業管理與 ITIL 的交集最廣，同時這一部份也是對作業人員進行作業規範相當重要的一個環節，在資訊安全的控制措施當中，人員是最無法控制的項目，但我們仍可就其業務相關範圍進行詳細規範，同時對於人群的管理必須針對其層級屬性的不同，詳細的分群，並針對各群集的業務特性加以詳細規範並付諸實行。

三、資訊安全組織

資訊組織的運作應依能力需求將各單位的執掌詳細區隔，且必須讓每個施行單位了解自身的職責，此外資訊設施、資訊資產也需詳細分類並列冊由專人管理，一旦發生安全事故必須在最小的影響下盡快處理，最後需將事情的經過及處理方式詳盡紀錄，以利日後相關事故處理以及策略更新作為參考。

四、資訊安全人力管理

對於施行單位以及服務對象皆必須進行清楚的權限劃分，並在開始

提供或取用服務以及結束時進行相關詳細規範，以避免人為因素所造成的資訊安全風險。

五、實體環境的控管

在實體環境的控管中必須就可能發生的問題進行探討，且須定期稽核檢驗以檢視策略是否合乎時宜，並跟據法源依據進行更新，以確保其永續運作。

參考文獻

[1]朱惠中、廖崇賢、陳惠娟，2006，「從管理層面探討當前的資訊安全問題」，2006年資訊管理學術與實務研討會論文集，161-168頁。

[2]孫淑景，2003，內控處理準則電腦資訊循環之個案研究-以BS7799資訊安全及COBIT控制目標為例，中原大學會計學系未出版之碩士論文，4-21頁。

[3]黃小玲，2010，如何整合ISMS與ITSMS，http://www.icst.org.tw/docs/Fup/6月_如何整合ISMS與ITSMS.pdf [2010, june 21]。

[4]曹子珊，曹偉駿，2004，「基於平衡計分卡架構設計適用於金融控股產業之資訊安全管理研究」，電腦稽核，11，54-69頁。

[5]葉俊榮，2005，「電子化政府資通安全發展策略與展望」，研考雙月刊，29(1)，20-34頁。

[6]樊國楨，2003，資訊安全管理系統與稽核，行政院國家科學委員會科學技術資料中心，行政院國家科學委員會。

[7]謝安田，2006，企業研究方法論(第三版)。

[8]樊國楨、林樹國、鄭東昇，2005，「資訊安全保證框架標準初探」，資通安全分析專論，中華資訊安全管理協會。

[9]梁定澎，1997，「資訊管理研究方法總論」，資訊管理學報，4(1)， 1-6頁。

[10] 李東峰，2001，企業資訊安全控制制度之研究，第三屆全國資訊管理博士生聯合研討會論文集，1-22頁。

[11] 吳琮璠，1997，「資訊管理個案研究方法」，資訊管理學報，4(1)，7-17頁。

[12] Andersen, W. P. “Information security governance.” Informati- on Security Technical Report, 6(3) 2001, pp: 60-70.

[13] Bakry, S. H. “Development of e-Government: A STOPE view.” International Journal of Network Management, 14(5) 2004, pp: 339-350.

[14] Brown, A. E. and Grant, G. G. “Framing the frameworks: a review of IT governance research.” Communications of the Association for Information Systems, 15, 2005, pp: 696-712.

[15] Broderick, J. S. “ISMS, security standards and security regulations.” Information Security Technical Report, 11(1) 2006, pp: 26-31.

[16] CNS 27002: 2007. Information technology - Information technology - Security techniques - Code of practice for information security management, Chinese national standard.

[17] Computer Security Institute. 2007 computer crime and security survey.

[18] Eloff, M. M. and Von Solms, B. “Information security management: An approach to combine process certification and product evaluation.” Computers & Security, 19(8) 2000, pp: 698-709.

[19] Esteves, J. and Joseph, R. C. “A comprehensive framework for the assessment of e-Government projects.” Government Information Quarterly, 25(1)2008, pp: 118-132.

[20] Fulford, H. and Doherty, N. F. ” The application of information security policies in large UK-based organizations.” Information Management and Computer Security, 11(3) 2003, pp: 106–114.

[21] Hardy, G. “Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges.” Information Security Technical Report, 11(1) 2006, pp:

55-61.

[22] ITGI. COBIT: Control Objectives Management Guidelines Maturity Models (4.1th ed.), United States of America, 2007.

[23] Johnson, E. C. “Security awareness: switch to a better programme.” Network Security, (2) 2006, pp: 15-18.

[24] Moulton, R. and Coles, R. S. “Applying information security governance.” Computers & Security, 22(7) 2003, pp: 580-584.

[25] National Institute of Standards and Technology, 2007 NIST Special publication 800-100, Information security handbook, A guide for managers.

[26] Organization for Economic Co-Operation and Development 1992. OECD Guidelines for the security of information systems.

[27] Organization for Economic Co-Operation and Development 2001. Guidelines for the Security of Information System.

[28] Ozier, W. “Generally accepted system security principles.” Computer Security Journal, 13(2) 1997, pp: 69-75

[29] Pasquinucci, A. “Security, risk analysis and governance: a practical approach.” Computer Fraud & Security, (7) 2007, pp: 12-14.

[30] Prakash, A., & Hart, J. A. Globalization and Governance: An Introduction. London: Routledge, 1999.

[31] Relyea, H. C. “Federal government information policy and public policy analysis: A brief overview.” Library & Information Science Research, 30(1) 2008, pp: 2-21.

[32] Saleh, M. S., Alrabiah, A. and Bakry, S. H. “Using ISO 17799: 2005 information security management: A STOPE view with six sigma approach.” International Journal of Network Management, 7(1) 2007, pp: 85-97.

[33] Von Solms, B. and Von Solms, R. „The 10 deadly sins of information security management.” Computers & Security, 23(5) 2004, pp: 371-376.

[34] Von Solms, B. “Information security - The fourth wave.” Computers & Security, 25(3) 2006, pp: 165-168.

[35] Wilson, P. “Governance and security: Side by side.” Computer Fraud & Security, 2007(4) 2007, pp: 15-16.

[36] Yin, R. K., Case study research: Design and methods. (Rev. ed.). Newburry Park, California: Sage Publications, 1989.