影響資訊安全關鍵因素之研究

洪 國 興[1]　　季 延 平　　趙 榮 耀
監察院綜合規劃室
國立政治大學資訊管理學系　國立政治大學資訊管理學系　淡江大學管理科學研究所

摘 要

由於資訊安全事故層出不窮，使得組織開始察覺到資訊安全可能危及企業的生存，因此，資訊安全普遍的受到重視。資訊安全產品與技術也被廣泛的討論，常被視為解決資訊安全問題的唯一辦法，而欠缺整合的對策與貫通的管理機制。欲解決資訊安全問題，學者分別從資訊安全政策（Information Security Policy）、風險管理（Risk Management）、內部控制（Internal Control）或資訊稽核（Information Auditing）等不同觀點，提出各種理論。本研究以資訊安全「整合系統理論」（Integrated System Theory）為基礎，提出「影響資訊安全因素架構」，經由因素分析，萃取八個因素構面，修正後，建構為組織「影響資訊安全關鍵因素架構」，作為組織規範資訊安全解決方案的參考。本研究也是繼 ISO/IEC 17799 公布後，就影響資訊安全關鍵因素進行實証研究的開端，相信有助於資訊安全管理之實証研究跨出重要的一步，也可作為後續相關研究的參考。

關鍵字：資訊安全、資訊安全管理理論、整合性系統理論、影響資訊安全因素、關鍵因素

[1] 洪國興 Mail Box：ksh@ms.cy.gov.tw

A Study of Key Success Factors Affecting Information Security

Kwo-Shing Hong
Overall Planning Department, Control Yuan of Republic of China
Department of Management Information Systems, National Cheng-Chi University
Yen-ping Chi
Department of Management Information Systems, National Cheng-Chi University
Louis R. Chao
Institute of Management Science, Tamkang University

Abstract

Since various accidents of Information Security emerge in an endless stream, organizations are gradually aware that Information Security may threaten the existence of enterprises. Information Security is therefore gaining growing attention universally. Products and technologies of Information Security are widely discussed and usually regarded as the only solution to information security problems, but lack of integrated strategies and comprehensive management mechanisms. To solve information security problems, scholars reached different theory in light of Information Security Policy, Risk Management, Internal Control or Information Auditing. Basing on the Information Security "Integrated System Theory", this Study integrated different views and moreover forms the "Architecture of Factors Affecting Information Security". It extracts eight constructs through factor analysis and after amending, models the "Architecture of Key Factors Affecting Information Security of an Organization". It offers a reference for the organization to standardize the resolutions of Information Security. The Study is also an inception to conduct empirical research on key factors affecting Information Security after the announcement "ISO/IEC 17799. It is believed to be an important barometer of the empirical study for Information Security Management, and will be the reference for related studies later on.

Keyword: information security, information security management theory, integrated system theory, factors affecting information security, key factors.

壹、緒論

美國的 911 事件，台灣的汐止東科大樓火災，納莉颱風的水災，財金公司的信用卡內外碼盜賣案等，一連串的安全事故，使得許多組織的資訊系統受到前所未有的重創，營業中斷，資訊資產的損害，商業利益的損失更是難以估計。由於資訊科技的快速進步，從集中式的大型主機（Central Mainframe Computers）、分散式主從架構（Client-Server），到網路式（Web Computing）的網際網路（Internet）、企業內部網路（Intranet）與企業間網路（Extranet）等，資訊系統的使用者，從只限於組織內部的資訊技術人員，而非資訊技術人員，再到組織外部的任何人。隨著資訊科技的快速發展，使用者範圍的不斷擴大，組織對資訊系統的依賴程度日益提高，使得組織所面臨的資訊安全威脅與日俱增，資訊安全管理亦成為組織資訊管理與經營策略重要的一環（Von Solms,1996；李東峰與林子銘, 2001；Schultz 等, 2001；Eloff & Von Solms, 2000）。

由於資訊安全事故層出不窮，世界各地不斷上演各式各樣的資訊安全危害事件，因此，組織開始察覺到資訊安全可能關係到其生死存亡，資訊安全的重要性即受到普遍的重視，各種資訊安全方案與解決策略也被提出，資訊安全產品也推陳出新，但現今資訊安全的解決方案卻出現：片斷而零散的安全功能、缺乏整合的對策、欠缺相互貫通的管理機制、資訊安全專業人才的不足等現象（Clyde, 2002），而要提出整體性的解決方案，必先要瞭解影響資訊安全的因素有那些？掌握影響資訊安全的關鍵因素，實為組織邁向健全的資訊安全跨出重要的第一步，也是建構資訊安全管理策略的起點, 此為本研究之動機。

解決資訊安全的問題，從制定資訊安全政策（Information Security Policy）、風險管理（Risk Management）、內部控制（Internal Control），到資訊稽核（Information Auditing）等，均有學者提出各種理論，其所揭示的影響資訊安全因素亦各有不同，如能整合各家的觀點，提出完整的影響資訊安全因素，並萃取影響資訊安全的關鍵因素，作為組織制定資訊安全策略的準據，此為本研究之目的。

本文先對資訊安全的背景加以說明。再探討資訊安全相關文獻，包括資訊安全的意義、資訊安全管理之理論發展、成功關鍵因素等。進而說明研究模式、研究方法、提出資料分析與研究結果，包括：理論探討、資訊安全影響因素之整理、調查與統計分析等，最後為結論與建議。

貳、文獻探討

本研究先從文獻中探討資訊安全之定義與資訊安全管理，再瞭解資訊安全理論的發展，及其所包含的資訊安全因素。

一、 資訊安全

資訊安全係在處理電腦系統的使用者之非授權行為的預防與發現（Gollmann,1999)。任何資訊安全政策之廣義目標，必需能保護儲存於資訊系統中資料之機密性（Confidentiality）、完整性（Integrity）與可用性（Availability），即所謂「C.I.A.」（Smith,1989；Schultz 等, 2001；ISO/IEC 17799, 2000；Chapman & Zwicky,1995；鄭信一, 1999；Dhillon & Backhouse, 2000；Gehrke 等, 1992；Schneider & Gregory, 1990；Finne, 2000；Ettinger, 1993；Anderson, 2003）：

1.機密性（Confidentiality）：確保「資訊」只能被經過授權的人，才能存

取。

2.完整性（Integrity）：保證「資訊」和其「處理方法」的準確性與完整性。

3.可用性（Availability）：確保經過授權的使用者，能存取「資訊」，並使用相關「資訊資產」。

依賴資訊系統的使用者，其軟體系統運作的表現如其所預期，則該系統即可稱之為「安全」（Simson & Gene,1991）。資訊安全的範疇包括：資訊安全政策、風險分析、風險管理、權變規劃（Contingency Planning）及災害復原（Disaster Recovery）等（Von Solms 等，1994）。運用可施行於資訊資源（硬體、軟體及資料）上之技術性防護方法及管理程序，期使組織所擁有的資訊資產及個人隱私，均能受到保護（樊國楨與楊晉寧，1996）。

資訊安全就是保護任何與電腦有關的事務之安全，將管理程序與安全防護技術運用在硬體、軟體與資料之中（Rusell & Gangemi,1992；黃亮宇，1992）。對組織而言，資訊是一種具有價值的重要商業資產，需妥善加以保護，以免受到各種威脅的攻擊，而維持組織營運的持續性，並使其可能發生損失降至最低（ISO/IEC 17799, 2000）。「資訊系統安全」乃指一切保護資訊系統資源，包括：硬體、軟體、資料庫，以防止遭受變更、破壞及未授權使用資訊系統資源之控制措施，其範圍包括技術面與組織管理面（吳琮璠，1996）。

資訊安全管理的目的在保護電腦資源，包括：硬體、軟體、資料、程序及人員，以防止電腦資源被變更、破壞及未授權使用（謝清佳與吳琮璠；1999）。當無法百分之百防止其發生時，則要減少資訊安全事故發生的機率或頻率，或當發生時，減少其後果的嚴重程度，或使其兩者都減少（Von Solms,1996；Moulton,1991）。

美國國防部發展的可信賴電腦系統評估準則（Trusted Computer System Evaluated Criterion；TCSEC, 1985）指出：安全的系統應是藉由使用特別的安全功能，以對資訊的擷取加以控制，如：經過適當授權的個人或處理，才能讀、寫、新增或刪除資訊。美國國防部的「軍事及相關術語國防辭典」，對資訊安全定義為：「保護資訊及資訊系統；以避免在儲存、處理或傳輸中的資訊遭受未經授權的存取或更改；且避免經授權的使用者遭到服務拒絕。」由於美國將資訊基礎建設中的資訊安全防護，在 Y2K 後納入國家的範圍，亦即成為國防保護的範圍，而美國的資訊安全技術研發，一向由軍方支持，資訊戰之執行則由美軍太空司令部（SPACECOM）負責。足見美軍為負責資訊安全最重要的權責單位，其對資訊安全的定義最具權威性（虞金燕與鄭祥勝，2001）。

所有涉及到「安全」的問題，基本上在處理下列事項，以確保資訊系統軟硬體之資料、資訊的機密性（Confidentiality）、整體性（Integrity）及可用性（Availability）（Pfleeger, 1996；Gollmann, 1999）：

1.預防（Prevention）：在防止資產發生危險。

2.發現（Detection）：當安全問題發生時，要有方法可以在最短時間內發現，並知道確切的危險及其嚴重程度。

3.反應（Reaction）：要在最短時間內使傷害降至最低，損害減至最少，並在最短時間內恢復到正常的情況。

「預防」與「發現」的概念對應到資訊安全即是所謂「防禦性資訊系統安全」，其目標在於：「從確保資訊資源的合法存取，到在所有可能遭受資訊攻擊時，可提供完整（Complete）、不中斷的資訊系統運作。」百分之百的資訊安全是難以做到的，為確保資訊安全基礎建設的安全性，防禦

性資訊系統受到先進國家的重視，其目的在於：「從確保資訊資源的合法存取，到所有可能遭受攻擊的階段，提供完整（Complete）、未中斷的資訊系統運作。」其功能性典範（Functional Paradigm）採取下列措施（樊國楨等，2001a；Panda & Giordano,1999；Ellison,1999）：

1.防護（Resistance）：即防止資訊系統之硬體、軟體與資料遭受外部或內部的威脅。

2.識別（Recognition）：即快速且正確的偵測與辨識出惡意的資訊攻擊，以爭取回復的時間與機會。

3.回復（Recovery）：即評估損害程度，找出隱藏的惡意程式，關閉入侵者為再次入侵留下的後門與回復資料，快速且完整的回復系統，並維護系統的完整性與可用性。

二、 資訊安全管理之理論發展

策略管理係組織為了達成期望的績效，如何發展與建置策略的一種修練（Schendel & Hofer, 1979）。由於資訊科技的快速發展，使得組織對資訊科技的依賴日深，資訊安全的影響，正逐漸擴大中。資訊安全不只是一項防禦性策略而已，更成為組織的競爭策略，因此，資訊安全管理理論的發展，將關係到資訊安全的研究，在實務層面上，也將關係到資訊安全策略之建構。本研究經由資訊安全文獻探討，並從實務面觀察，得知資訊安全管理理論有：安全政策理論（Security Policy Theory, SPT）、風險管理理論（Risk Management Theory, RMT）、控制與稽核理論（Control and Auditing Theory, CAT）、管理系統理論（Management System Theory, MST）、權變理論（Contingency Theory, CT）等五種（Hong 等，2003）。

（一）安全政策理論（Security Policy Theory, SPT）

「安全政策理論」（Security Policy Theory）係指資訊安全係經由資訊安全政策（Security Policy）之制定、實施與維護的程序來達成，以資訊安全政策為核心，形成資訊安全管理循環，經由資訊安全政策落實執行，以實現資訊安全之目標。資訊安全政策是一個管理循環，從資訊安全之規劃（Planning）、建置（Implementation）與維護（Maintenance）等形成一個持續不斷的改善工作（Kabay, 1996；黃承聖，2000；吳琮璠，2002；Flynn, 2001）。

資訊安全政策即在規劃資訊安全需要，形成共識，制定政策，付諸實施，並定期對實施效果加以檢討修正，以滿足組織的最新安全需求，而促進資訊安全的一種管理程序。其資訊安全的決定則形成下列的函數關係：

資訊安全＝f（資訊安全政策）

資訊安全政策＝f

（資訊安全政策制定，資訊安全政策實施，資訊安全政策維護）

資訊安全政策制定＝f（安全需求）

（二）風險管理理論（Risk Management Theory, RMT）

「風險管理理論」（Risk Management Theory）係指組織透過風險分析（Risk Analysis）與風險估計（Risk Evaluation），以確認資訊安全威脅（Threats）與弱點（Vulnerabilities），並估計其發生之可能性，及對資產所造成的衝擊，即是風險評估（Risk Assessment）；再據以規劃組織資訊安全需求（Information Security Requirement），及建置降低風險之管理措施，使資訊安全風險控制在可以接受的水準，而達成組織資訊安全之目標。因此，風險管理（Risk Management）是在組織內

建立與維護資訊安全的一種程序（Process）（Wright, 1999；Reid & Floyd, 2001；樊國楨等，2001b）。

風險管理係組織以風險評估（Risk Assessment）與風險控制（Risk Control）的交互運作，使資訊安全風險（Information Security Risk）控制在組織可以接受的水準，以實現組織資訊安全的一種管理程序。其資訊安全的決定則形成下列的函數關係：

資訊安全=f
（風險評估，風險控制，檢討修正）
風險評估=f（風險分析，風險估計）
風險控制=f
（建立控制制度，實施控制制度）
風險分析=f（威脅，弱點）
風險估計=f（衝擊，資產評價）

（三）控制與稽核理論（Control and Auditing Theory, CAT）

「控制與稽核」（Control and Auditing Theory）係指組織建立有利於資訊安全的控制制度（Control System），付諸實施後，以稽核（Auditing）的程序來衡量其控制的績效（Performance），檢視控制的缺失，再修正控制制度，經由一連串對資訊安全的控制與稽核之程序，以促使組織建立符合資訊安全需求的內部控制制度（Internal Control System），經持續執行，有效稽核，而確保資訊安全之實現。「控制」（Control）是一種預防（Prevents）、偵測（Detects）與改正（Corrects）不法事件的系統，ISO/IEC 17799（2000）所規範的資訊安全控制，計有資訊安全政策等十大管理要項，127 種控制方法。COBIT 參考內部控制模式所制定的資訊技術管理控制模式，制訂 34 個高層控制目標及 318 項詳細控制目標（Weber,1999；楊金炎，2001；ISO/IEC 17799, 2000；COBIT, 1998）。

組織衡酌資訊安全策略及各種資訊安全標準，以制定資訊安全控制制度（Control System），經嚴格執行並定期進行資訊稽核（Information Auditing），以評估控制制度執行成效，及資訊安全水準，據予修正其控制度，交替運作，以確保組織資訊安全的一種管理程序。其資訊安全的決定則形成下列的函數關係：

資訊安全=f
（制定控制制度，實施控制制度，資訊稽核）
制定控制制度=f（安全策略，標準）

（四）管理系統理論（Management System Theory, MST）

「管理系統理論」（Management System Theory）係指組織應建立及維護一個文件化的資訊安全管理系統（Information Security Management System, ISMS），該系統強調需要被保護的資訊資產，採用風險管理方法、控制目標、控制方法、及所需要的安全保證程序，以促使組織達成資訊安全的目標。ISMS 分為六大步驟：（1）定義政策（Define the Policy）；（2）定義 ISMS 範圍（Define the Scope of the ISMS）；（3）進行風險評估（Undertake a Risk Assessment）；（4）風險管理（Manage the Risk）；（5）選擇要實行的控制目標及控制方法（Select Control Objective and Control to be Implemented）；（6）準備適用性聲明（Prepare a Statement of Applicability）等，形成為一個程序化的安全管理系統（Sherwood, 1996；宋振華與楊子劍，2001；BS 7799-2, 1999）。

組織對資訊安全管理，依據環境與安全標準制定資訊安全政策，定義資訊安全範圍，進行風險評估與風險控制，要求組織成員一體遵行，此程序形成一個資訊安全的管理系統。其資訊安全的決定則形成下列的函數關係：

資訊安全=f（資訊安全政策，資訊安全範圍，風險管理，實施）

風險管理=f（風險評估，風險控制）

資訊安全政策=f

（組織內外部環境，標準）

（五）權變理論（Contingency Theory, CT）

「權變理論」（Contingency Theory）指：資訊安全係組織為了預防（Prevention）、偵測（Detection）與反應（Reaction），組織內外之資訊安全威脅（Threats）、弱點（Vulnerabilities）與衝擊（Impacts）的權變管理（Contingency Management），為因應環境變化與組織的管理上需要，而採取政策導向（Policy Orientation）、風險管理導向（Risk Management Orientation）、控制與稽核導向（Control and Auditing Orientation）或管理系統導向（Management System Orientation）之其中一種或多種的資訊安全管理策略，用以達成資訊安全為目標。

所謂「權變」（Contingency），是對於環境的各種變化，所產生的認知與回應，並提出有效的策略，以因應環境的變化與組織業務的需要，而「有效的策略」即是組織的調適（Fit）與一致性（Congruence）(Robbins, 1994；Drazin & Van de Ven,1985)。「權變」係兩組變數之間的互動關係，組織為因應內外環境的快速變遷，常採行權變方式（Contingency Approach），以作為一種有效的管理方式，或概念基礎。權變管理（Contingency Management）係一組環境變數與另一組管理與技術的變數之互動關係，其功能在追求組織目標的達成（Luthans, 1976；Lee 等，1982；Hinde, 2002）。

組織資訊安全所面臨的環境變數是資訊安全威脅、弱點與衝擊；而資訊安全管理的變數，包括：資訊安全政策、風險評估、內部控制、資訊稽核等之管理與技術的變數。兩組變數的互動關係即資訊安全之權變管理，亦即在尋求兩組變數之間的適應性與一致性。因此，是一種動態關係，而非靜態關係（Von Solms 等，1994；李東峰與林子銘，2001）。其資訊安全的決定則形成下列的函數關係：

資訊安全＝f（資訊安全管理策略）

資訊安全管理策略=f

（政策導向，風險管理導向，控制與稽核導向，管理系統導向，權變管理）

權變管理=f（組織環境，管理與技術）

五種資訊安全管理理論，按其主要安全管理活動、管理程序、特性及優劣、文獻等，彙總如表一所示。

表一　資訊安全管理理論彙總表

理　論	主要管理活動	管理程序	特性及優劣	文　獻
安全政策理論 (Security Policy Theory, SPT)	·安全政策制定 ·安全政策實施 ·安全政策維護	·循序流程 ·循環週期	·以資訊安全政策為主要內涵，忽視風險管理，內部控制與資訊稽核等安全機制 ·過於重視循序與結構化，對環境的應	Kabay（1996） 黃承聖（2000） Gupta 等(2001) Flynn（2001）

理 論	主要管理活動	管理程序	特性及優劣	文 獻
			變能力較低	
風險管理理論 (Risk Management Theory, RMT)	·風險評估 －風險分析 －風險估計 ·風險控制 －建立控制制度 －實施控制制度 ·檢討修正	·循序流程 ·循環週期	·強調資訊安全環境的瞭解與應變，使控制制度可符合組織的需求 ·忽視安全政策與資訊稽核等安全機制 ·過於重視循序與結構化	Wright（1999） Reid & Floyd（2001） 樊國楨等(2001b)
控制與稽核理論 (Control and Auditing Theory, CAT)	·制定控制制度 ·實施控制制度 ·資訊稽核	·循序流程 ·循環週期	·以內部控制及資訊稽核為主要內涵，忽視安全政策與風險評估等安全機制 ·重視內部控制之澈底執行，但環境應變與需求規劃卻有不足	BS7799-2（1999） ISO/IEC 17799（2000） 楊金炎（2001） COBIT（1998）
管理系統理論 (Management System Theory, MST)	·制定安全政策 ·定義安全範圍 ·風險管理 －風險評估 －風險控制 ·實施	·循序流程	·資訊安全風險管理機制雖較上述理論完整，唯忽視資訊稽核，致控制制度之落實程度受到影響 ·欠缺循環週期 ·欠缺回饋功能	BS7799-2（1999） Sherwood（1996） 宋振華與楊子劍（2001）
權變理論 (Contingency Theory, CT)	·政策導向策略 ·風險管理導向策略 ·控制與稽核導向策略 ·管理系統導向策略	·權變流程	·可充分反應組織內外環境，選擇適當的安全策略 ·欠缺整合性與結構化	Robbins（1994） Drazin & Van de Ven（1985） Luthans（1976） Lee 等（1982） Von Solms 等（1994） 李東峰與林子銘（2001）

資料來源：本研究

以上五種理論經比較分析如下：

1. 安全政策理論、風險管理理論、控制與稽核理論均係由資訊安全的某一環節切入，亦即切入點不同，如：政策理論由資訊安全政策（information security policy）切入，風險管理理論係由風險分析（risk analysis）切入，控制與稽核理論由控制制度之建立（define the control system）切入。
2. 安全政策理論、風險管理理論、控制與稽核理論，雖切入點不同，但後續的資訊安全管理內涵部分是雷同的，尤其內部控制（internal control）幾乎是受到各家理論所重視，顯然內部控制是達成資訊安全目標的重要手段。
3. 除權變理論所強調的是因應環境變化與業務需要的權變管理之外，各家理論均係一種程序，而且是固定方向由上而下（top-down）的流程，但實際上未必都是循序程序（sequential process）。
4. 各家理論均係資訊安全管理的一個環節或部分組成（components），縱使以其環節較多的「管理系統理論」而言，亦有其欠缺之處：
   (1) 由上而下的流程與現實環境未必完全吻合。
   (2) 結構化（structure）的方法論難以因應高度動態環境的需要。
   (3) 資訊安全稽核（auditing）未受到重視，使管理系統缺乏評估（evaluation）的機制。
   (4) 權變管理雖可彌補上述的不足，但是又缺乏完整的方法與步驟。

三、 關鍵成功因素

關鍵成功因素是指一個企業為了成功必須要做得特別好的工作（Daniel, 1961）；關鍵成功因素是一些變數，而管理當局為因應這些變數所形成的決策，足以對企業在產業中的競爭地位產生實質的影響。此外，這些因素將隨產業的不同而有所改變（Hofer & Schendel, 1978）；關鍵成功因素存在於企業有限的幾個領域，在這些有限而重要的領域中做對做好，企業才能有較佳的競爭績效（Rokert, 1979）；關鍵成功因素是企業面對競爭者所必須具備的最重要的競爭能力或資產。成功的企業往往在關鍵成功因素上的表現不俗，反之，表現欠佳的企業常是缺乏一至多個關鍵因素。企業唯有掌握產業的關鍵成功因素，才能建立持久的競爭優勢（Aaker, 1984）。關鍵成功因素亦是企業經營成功所必須掌握的主要範疇，有助於引導企業制定有效的策略與執行程序，並廣泛地運用於高階決策資訊系統的設計（吳青松，1992）。Ferguson & Dickinson（1982）解釋關鍵成功因素為：

1. 係組織必須加以重視並慎重處理的因素，因為這些因素會影響組織目標的達成，甚至危及組織的生存。
2. 必須特別去注意，且有顯著影響的事件或狀況。
3. 關鍵成功因素可能是組織內在或外部的因素，而其影響亦可能是正面或反面的。
4. 必須加以特別控制措施，以避免發生不良的突發事故或錯失良機。
5. 藉由關鍵成功因素可以評估組織的策略、環境、資源與營運。

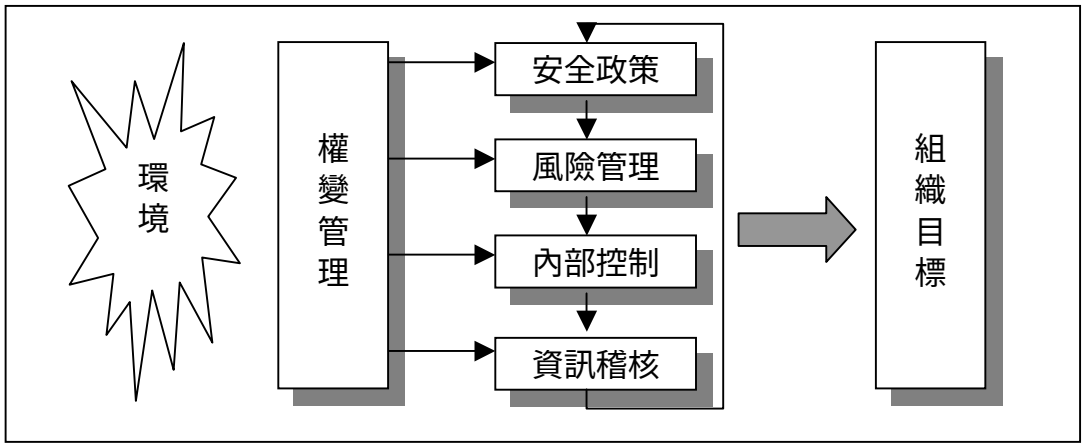
吳思華（1988）指出，關鍵成功因素就是在特定領域內與他人競爭，必須具備的技術或資產。藉由分析組織之優勢與關鍵成功因素配合之情況，即可判斷此一組織是否具有競爭力。如果組織的優勢恰好表現在領域的關鍵成功因素上，那組織就

可以取得競爭優勢。

對於萃取關鍵成功因素，其所使用的統計分析方法，國內的研究顯示，訪談、個案研究、德菲法、因素分析、層級分析等均曾運用於 KSFs 的統計分析（余幸真，2001）。因素分析是一種互依分析技術，也是縮減空間（或構面）的技術，其主要目的在以較少的維度（number of dimensions, 即構面的數目）來表示原先的資料結構，而又能保存住原有資料結構所提供的大部分資訊，換言之，也是透過資料分析的簡化或彙總來找出資料的結構（黃俊英，2000）。本研究所探討的影響資訊安全因素甚多，眾說紛紜，多到管理者不知重點在何處，本研究目的在萃取影響資訊安全的關鍵因素，故採用「探索性因素分析」（Exploratory Factor Analysis）。

參、研究模式

由於以上資訊安全管理理論僅只適用於部分資訊安全管理活動或機制，均有其侷限性，無法適用於組織全部的資訊安全活動或機制；亦無任何理論可以同時具備循序程序（Sequential process）與權變程序（Contingency Process），更難以因應高度動態的環境，並符合組織的目標。Hong 等（2003）經整合上開五種資訊安全管理理論，並觀察實務上之資訊安全管理活動，提出「整合性資訊安全管理模式」（Integrated Information Security Management Model, IISMM）。此一模式係由（1）安全政策（Security Policy）；（2）風險管理（Risk Management）；（3）內部控制（Internal Control）；（4）資訊稽核（Information Auditing）等四個資訊安全管理活動所組成，以權變管理（Contingency Management）為基礎，並與組織目標充分結合，形成一個整合性之資訊安全管理模式（Hong 等，2003），如圖一所示。



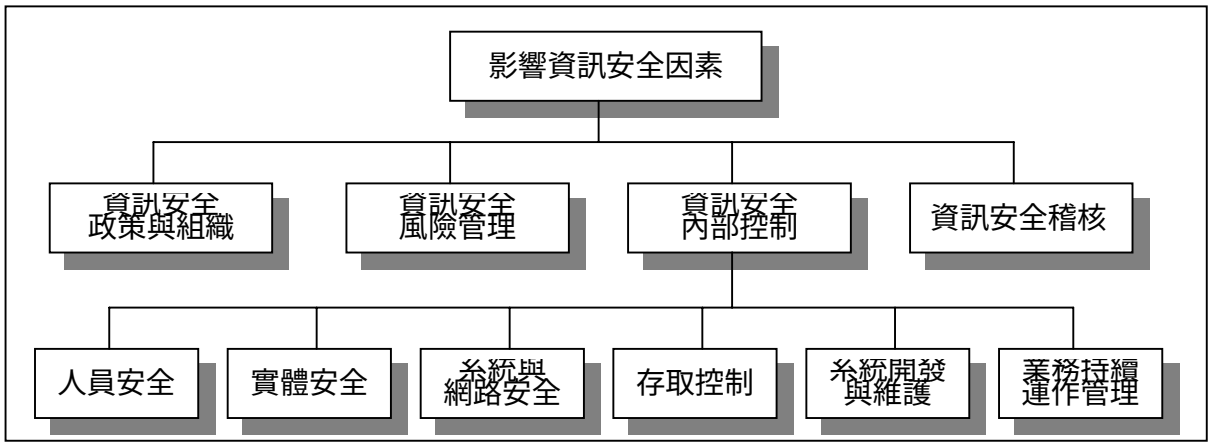
圖一 整合性資訊安全管理模式示意圖（Hong 等，2003）

組織之資訊安全管理，係整合資訊安全政策（Security Policy）、風險管理（Risk Management）、內部控制（Internal Control）、與資訊稽核（Information Auditing），以權變管理（Contingency Management）為基礎的資訊安全管理架構，其資訊安全的決定則形成下列的函數關係（Hong 等，2003）：

資訊安全=f
（安全政策，風險管理，內部控制，資訊稽核，權變管理）
內部控制=f
（人員安全控制，實體安全控制，系統與網路安全控制，存取控制，系統開發與維護控制，業務持續運作管理）
權變管理=f
（組織內外部環境，資訊管理，資訊技術）

「整合性資訊安全管理模式」（Integrated System Information Security Management Model）共有四個資訊安全管理活動：資訊安全政策（Information Security Policy）、風險管理（Risk Management）、內部控制（Internal Control）及資訊稽核（Information Auditing），以階層式展開，並參考 ISO/IEC 17799（2000）（BS7799-1）、BS7799-2（1999）、行政院資通安全訪視表、行政院及所屬各機關資訊安全管理規範、資訊安全文獻等資料，初擬資訊安全影響因素，最底層之影響資訊安全因素共 63 項，其架構如圖二所示。

本研究經採用名目群組技術（Nominal Group Technique, NGT），邀請專家學者集思廣益，匯集意見。名目群組技術係融合腦力激盪（Brainstorming）、腦力書寫（Brainwriting）及投票技術（Voting Technique）的一種匯集群體意見的方法。



圖二　影響資訊安全因素架構（資料來源：Hong 等，2003）

此方法可運用在匯集意見（Idea Generating）、問題規劃（Solution Exploration）及決定權重（Priority Setting）（David & Rivett, 1978；謝玲芬，1989）。在運用 NGT 匯集意見的過程中，以層級結構來思考，並使用「詳述化」（Specification）、「手段 - 目的」（Means-Ends）、「包括性」（Comprehensive）、「可衡量性」（Measurable）、「重要性試驗」（Test of Importance）等，作為討論檢視的指導原則（葉牧青，1989）。

1. 「詳述化」，意指將一個目標細分（Subdivide）成為幾個較低層次的次目標，以更加詳細、具體的描述目標。
2. 「手段-目的」，指從另一角度來看，

較低層次的目標，可視為達成目的的手段（Means），而較高層次的目標則是決策者所訂定的目的（Ends）；藉著不斷分析並確認（Identify）其欲達成目的，需要那些更為明確精細的中介（Intermediate）手段，而將問題系統的層級結構，由高而低的建立起來。

3. 「包括性」，在尋求屬性理論背景上（Theoretical Grounds）的「適切性」（Appropriateness），其重點在於考量所有相關資訊（Information we would like to have）。
4. 「可衡量性」，是站在實用的角度上（Practical Considerations），可否取得必要的評估標竿（Necessary Assessments）。
5. 「重要性試驗」，意指在考量增加或減少是否會影響目標的達成。

本研究所進行之 NGT，其參與之專家學者係中華民國資訊應用發展協會之會員，有政府或企業之資訊主管、資訊管理教授、系統整合（SI）廠商之高階主管、資安主管、資安人員等共 20 餘人。其經過：1.簡報影響資訊安全因素初稿。2.討論。3.共識決，未達成共識者以表決決定。經 NGT 的過程並修正整理後，最底層之影響資訊安全因素共 66 項，如表二所示。

表二 影響資訊安全因素

1	資訊安全政策與組織	3.3.6	對機密性、敏感性資料傳輸之特別保護措施（如：加密）
1.1	制定資訊安全政策並予文件化	3.3.7	網路安全之管理、硬體與軟體之建置
1.2	依據組織目標與策略、資訊政策及業務特性等因素制定資訊安全政策	3.3.8	建立操作管理之各項紀錄日誌
		3.3.9	資料及軟體交換之安全控制
1.3	資訊安全政策之定期檢討修正	3.4	存取控制
1.4	設置資訊安全組織或指派資訊安全人員	3.4.1	制定存取控制政策並符合法令規定
1.5	資訊安全權責劃分	3.4.2	對特權使用之限制與配置之管制
1.6	資訊安全資源規劃	3.4.3	多使用者系統建立使用者帳號與密碼管理程序
1.7	資訊安全預算		
1.8	對違反資訊安全規定之處置	3.4.4	遠端使用者之存取，建立驗證管制措施
2	資訊安全風險管理	3.4.5	網路管制以區隔服務、使用者與資訊系統等不同群組
2.1	進行資訊安全風險分析，包括威脅與弱點分析	3.4.6	依系統安全等級、分類、網路型態訂定適當的存取權限管理方式
2.2	建立資訊資產清冊與分類，並區分機密等級	3.4.7	使用者密碼使用、確認、登入管理之具體規範
2.3	對不同機密等級建立保護措施	3.4.8	對機密性、敏感性之系統與資料，建立特別的存取控制方式
2.4	進行資訊安全風險評估與差異分析（目前安全狀況與適當安全水準的 gap），以瞭解風險情況	3.4.9	存取控制各項紀錄的建立與保存
		3.5	系統開發與維護
2.5	依風險分析與風險評估結果進行資訊安全需求規劃	3.5.1	將資訊安全列入應用系統開發與維護的要求
2.6	資訊安全風險管理之策略規劃	3.5.2	建立應用軟體執行碼之更新程序，並由

3	資訊安全內部控制
3.1	人員安全
3.1.1	人員進用與調職時，作適當之安全評估
3.1.2	重要或須特別權限工作之適當分工，以分散權責
3.1.3	重要或特別權限工作之人員輪調與人力備援
3.1.4	對不同職務予以適當資訊安全教育與訓練
3.1.5	組織各階層之資訊安全意識
3.2	實體安全
3.2.1	硬體設備之建置先考量安全因素
3.2.2	依設備之重要程度，予以區隔保護，專人管理
3.2.3	對於危害硬體設備之環境條件（如：火、水災…）均予安全評估與控制
3.2.4	電源供應之安全評估與控制(如:備援)
3.2.5	設備維護之安全評估與控制
3.2.6	電腦機房及重要區域之進出管制
3.2.7	機房與附屬設備之操作程序與管理責任
3.2.8	儲存媒體之安全評估與管理控制
3.3	系統與網路安全
3.3.1	資訊設備與系統環境之操作與變更程序
3.3.2	軟體開發與正式作業不使用同一個伺服器與資料庫
3.3.3	將資訊安全應遵守之規定，納入委外合約條款
3.3.4	對病毒、惡意軟體入侵的預防、偵測與處理
3.3.5	對機密性、敏感性資料之管制處理程序
3.5.3	專人管理與記錄 系統文件之管理、維護及保護
3.5.4	應用軟體變更後，立即更新系統文件，兩者保持一致
3.5.5	應用軟體之處理程序與組織之內部控制程序一致
3.5.6	將資訊安全列為應用軟體變更管制程序的一部份
3.5.7	委外軟體開發與維護時，將遵守資訊安全規範列入契約條款
3.6	業務持續運作管理
3.6.1	建立弱點、威脅與故障之回應制度
3.6.2	安全事故之責任、通報與緊急處理程序
3.6.3	安全事故之檢討改進與經驗學習
3.6.4	系統中斷時，使業務持續運作之程序
3.6.5	軟體與資料之備份
3.6.6	異地備援機制
3.6.7	業務持續運作機制之定期測試與演練
4	資訊安全稽核
4.1	定期實施內部稽核
4.2	定期實施外部稽核
4.3	內部稽核人員先接受稽核訓練
4.4	與資訊安全相關紀錄檔案之記錄與保管
4.5	稽核結果之獎懲
4.6	稽核結果之後續行動（如：修正資訊安全政策、進行風險評估、修正內部控制等）
4.7	對資訊安全有關法令之遵守

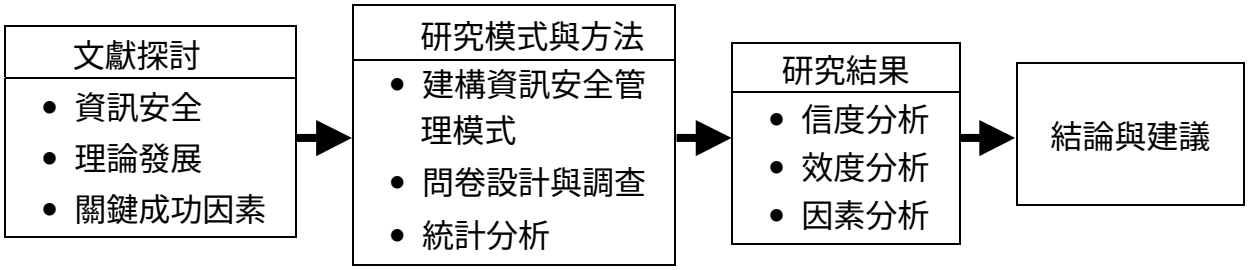
影響因素來源：Kabay,1996；黃承聖，2000；吳琮璠，2002；Flynn, 2001；Wright,1999；Reid & Floyd, 2001；樊國楨等，2001b；Weber,1999；楊金炎，2001；ISO/IEC 17799, 2000；COBIT, 1998；Sherwood, 1996；宋振華與楊子劍，2001；BS7799-2, 1999；Luthans, 1976；Lee 等，1982；Von Solms, 1994；李東峰與林子銘，2001；Gupta 等，2001。再經 NGT 後，經本研究整理而成。

肆、研究方法

本研究係以資訊安全管理理論為基礎，建構整合性資訊安全管理模式，據以發展研究設計、設計問卷、進行調查，經統計分析，提出結論與建議。

一、 研究流程

本研究之研究流程如圖三所示。



圖三 研究流程圖（資料來源：本研究）

二、 問卷設計與問卷調查

本研究之問卷設計過程詳如研究模式後段，本研究問卷調查對象為中華民國資訊經理人協會、中華民國資訊應用發展協會之會員，及政府資訊資訊主管聯席會議成員等，扣除重複部分，於 2002 年 11 月間以 E-mail 寄出問卷 650 份，填寫問卷 159 份，扣除無效問卷 5 份，有效問卷 154 份，有效填答率 23.69%。

三、 研究工具

利用 SPSS 統計工具軟體進行各項統計分析。

（一） 信度衡量：本研究以 Cronbach's α來衡量同構面所有問項之內部一致性，以測試問卷所有問項在某特定構面的一致性程度。

（二） 因素分析：進行主成份分析法（Principal Component Analysis）之因素分析，以萃取影響資訊安全之關鍵因素。

伍、資料分析與研究結果

一、信度（Reliability）分析

信度（Reliability）係指衡量結果的可靠性，即測量工具在測量某持久性特質可維持一致性（Consistency）或穩定性（Stability），也就是研究者對於相同或相似的現象進行不同的測量，其所得的結果一致的程度（張劭勳，2000）。

本研究係以 SPSS 進行問卷整體信度分析，利用 Cronbach'sα 係數檢定法，分析問卷整體之信度。分析結果整體信度之 Cronbach'sα 值為 0.9881，且所有變數之信度均在 0.9 以上，具有頗高之可靠性（Bryman & Cramer, 1997；Gay, 1992），且 Guieford（1965）認為 α 值若低於 0.35 才必須予以拒絕，因此，變數不予刪除，如表三所示。

二、效度（Validity）分析

效度係指衡量工具能夠測得所欲衡量的特質及功能的程度。內容效度（Content Validity）是指衡量工具「內容的適切性」，及衡量工具是否涵蓋所要衡量的構念，其

衡量工具的內容愈能代表研究主題，則其內容效度愈大（張紹勳，2000）。本研究量表係依據 ISO/IEC 17799-1 （2000）(BS7799-1)、BS7799-2（1999）、行政院資通安全訪視表、行政院及所屬各機關資訊安全管理規範及資訊安全文獻等資料，初擬資訊安全影響因素，再採用名目群組技術（Nominal Group Technique， NGT），邀請學者專家集思廣益，匯集意見，經修正整理後，發展成問卷，並由前測的步驟，在據予修正其內容，使問卷更為周延，因此本研究之問卷具有相當高的內容效度。

表三　問卷整體之信度分析

變數	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Alpha if Item Deleted
A11	376.4351	2405.6069	.5944	.9881
A12	376.6169	2396.7738	.6724	.9880
A13	376.6429	2405.8128	.5892	.9881
A14	376.6623	2396.8526	.6268	.9880
A15	376.6169	2394.9045	.6875	.9880
A16	376.7208	2401.2875	.6344	.9880
A17	376.8377	2385.4048	.7103	.9879
A18	376.8831	2388.1562	.7152	.9879
A21	376.8961	2387.9368	.7156	.9879
A22	376.9156	2383.2150	.7333	.9879
A23	376.9091	2374.8806	.7712	.9879
A24	377.0260	2389.6202	.6916	.9880
A25	376.9545	2402.2659	.5849	.9881
A26	376.9351	2388.1918	.7173	.9879
A311	377.0455	2385.3378	.7119	.9879
A312	376.7468	2384.2688	.7947	.9878
A313	376.8831	2379.4111	.7888	.9879
A314	376.9740	2383.9862	.7864	.9879
A315	376.8247	2391.2828	.6931	.9880
A321	376.8766	2382.7755	.7517	.9879
A322	376.8506	2379.4743	.7986	.9878
A323	376.7273	2374.6964	.8014	.9878
A324	376.6429	2382.7540	.8071	.9878
A325	376.8442	2379.0997	.8357	.9878
A326	376.5974	2385.3663	.7454	.9879
A327	376.7532	2388.4747	.7700	.9879
A328	376.6364	2391.7493	.7638	.9879
A331	376.9351	2382.4010	.8020	.9878
A332	376.8312	2400.0105	.6372	.9880
A333	376.7078	2384.4696	.7620	.9879
A334	376.4935	2386.9575	.7523	.9879
A335	376.5455	2394.6156	.7495	.9879
A336	376.5519	2398.2228	.6877	.9880
A337	376.6818	2383.2380	.7988	.9878
A338	376.9675	2380.0708	.7586	.9879
A339	376.8442	2381.1128	.8037	.9878

A341	376.9026	2384.6375	.7211	.9879
A342	376.7987	2388.0050	.7369	.9879
A343	376.6429	2382.3095	.7799	.9879
A344	376.5584	2390.0913	.7699	.9879
A345	376.7532	2389.5988	.7937	.9879
A346	376.6623	2391.5715	.7673	.9879
A347	376.5844	2393.2379	.7076	.9879
A348	376.4740	2398.6039	.6778	.9880
A349	376.8312	2395.0693	.7111	.9879
A351	376.7273	2381.8728	.7880	.9879
A352	376.8312	2386.5857	.8176	.9878
A353	377.0195	2390.4114	.7638	.9879
A354	376.8247	2390.7599	.7434	.9879
A355	376.9351	2379.2768	.8292	.9878
A356	376.8831	2383.2150	.7960	.9878
A357	376.6818	2372.9504	.8309	.9878
A361	376.9481	2380.4679	.8045	.9878
A362	376.6883	2391.5493	.7243	.9879
A363	376.8766	2393.2330	.7390	.9879
A364	376.6623	2390.3297	.7304	.9879
A365	376.3701	2397.7771	.6555	.9880
A366	376.7727	2386.4643	.6875	.9880
A367	376.9286	2391.1387	.7113	.9879
A41	376.8831	2380.4830	.7978	.9878
A42	377.0779	2373.7847	.7875	.9879
A43	376.9286	2386.9556	.8189	.9878
A44	376.9870	2381.1502	.8321	.9878
A45	377.3117	2390.6342	.6590	.9880
A46	376.8571	2388.9468	.7561	.9879
A47	376.9935	2365.1568	.8319	.9878

資料來源：本研究

三、進行因素分析

（一）適合性檢定

因素分析的目的在於以較少的因子來代表較多的變數，所以在進行因素分析之前，先確定各變數觀察值間具有共同變異的存在，如此才值得進行後續的因素分析（黃俊英，2000）。因此，本研究先進行適合性檢定，採用巴氏球形檢定（Bartlett's Test of Sphericity），p 值小於顯著水準時，即可進行後續的因子分析。

此外，另使用 KMO 係數（Kaiser Meyer Olkin Coefficient）來衡量每一個變數是否具有抽樣上的適當性，KMO 係數愈大代表資料愈適合做因素分析，其係數大於 0.9 則為「奇異」的（Marvelous）；0.8 至 0.89 為「值得稱讚」的（Meritorious）；0.7 至 0.79 為「中等」（Middling）；0.6 至 0.69 為「普通」的（Mediocre）；0.5 至 0.59 為「可憐」的（Miserable）；小於 0.5 則為「不可接受」（Unacceptable）的水準（Kaiser & Rice, 1974）。

經由 KMO 取樣的適合性檢定及 Bartlett's Test 等結果，KMO 係數為 0.947，超過 0.9 通常被認為係極佳的因素求解（Tabachnick & Fidell, 1989），且 Bartlett's Test 值 11771.853，顯著性＝0.000<α＝

0.05，顯示資料非常適合進行因素分析，如 表四所示。

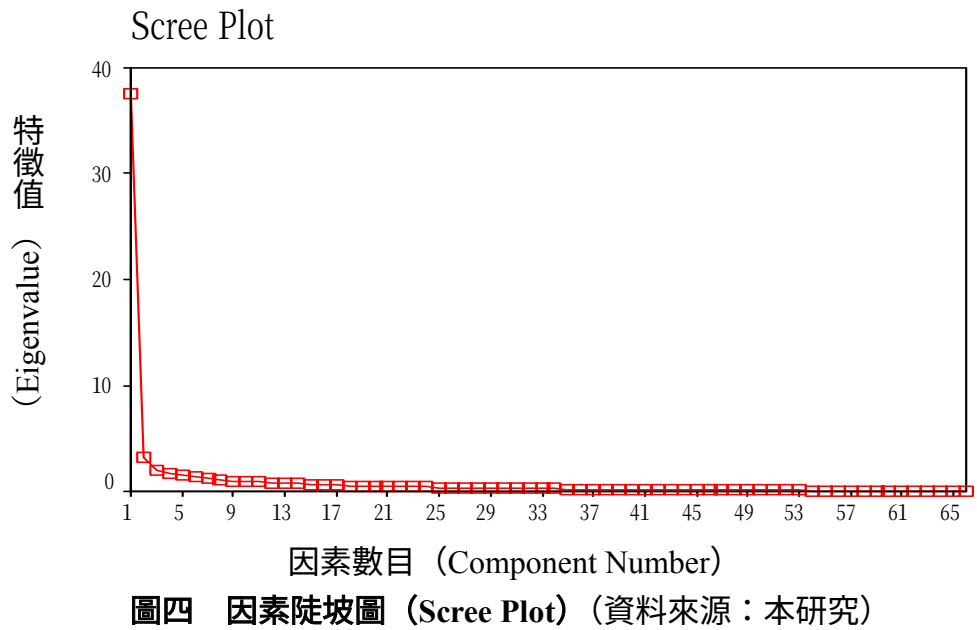
表四 KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.947
Bartlett's Test of Sphericity	Approx. Chi-Square	11771.853
	df	2145
	Sig.	.000

資料來源：本研究

（二）因素模式與因素選取

本研究之因素分析係採主成分分析法（Principal Component Analysis）來萃取相關因素。其因素的選取，係根據陡坡圖（Scree Plot），似較不易選取適當的因素數目，如圖四所示，故本研究再依據Kaiser(1958)的選取準則，將特徵值（Eigenvalue）大於 1 的因素，選取為因素個數，而以選取 8 個因素較為適當，累積解釋變異量為 75.194%，而各因素的特徵值解釋變異量與累積變異量等，如表五所示。



圖四 因素陡坡圖（Scree Plot）（資料來源：本研究）

表五 整體解釋的變異量—未轉軸前

因素構面編號	特徵值（Eigenvalue）	解釋變異量(%)	累積變異量(%)
1	37.530	56.863	56.863
2	3.235	4.901	61.765
3	2.017	3.056	64.821
4	1.625	2.462	67.284
5	1.551	2.351	69.634
6	1.420	2.151	71.786
7	1.171	1.774	73.560
8	1.079	1.634	75.194

資料來源：本研究

（三）因素轉軸

轉軸的主要目的是使因素更具有實質意涵的解釋模式，亦即達成「簡單結構」（Simple structure）（Thurston,1947）的原則，經過轉軸後的因素矩陣中每一個變數都只歸於一個或少數幾個因素上，使矩陣中零或接近於零的因素負荷量增多，以減低因素的複雜性，使因素的解釋由繁雜趨向簡單，其各個因素所代表之意義可以顯得比較清晰明顯。本研究採用 SPSS 的 Kaiser 正規化最大變量法（Varimax with Kaiser Normalization）進行轉軸，轉軸後的因素矩陣（Rotated Component Matrix）如表六所示。

表六 轉軸後的因素矩陣（Rotated Component Matrix(a)）

影響因素編號	因素構面							
	1	2	3	4	5	6	7	8
A354	.730	.190	.250	.172	.220	.251	6.786E-02	1.050E-02
A353	.703	.197	.258	.252	.169	.173	.125	.124
A356	.630	.397	.219	.247	.252	.164	8.826E-02	5.477E-02
A349	.609	.341	.167	.115	-8.093E-03	.201	.315	.192
A341	.604	.320	.333	2.301E-02	7.066E-02	1.481E-02	.370	.200
A355	.597	.363	.353	.268	.242	.180	6.450E-02	8.049E-02
A42	.586	.186	.215	.400	.280	.118	.241	.106
A352	.578	.339	.392	.343	.234	9.361E-02	3.599E-02	9.054E-02
A367	.575	.298	.106	.222	.134	.392	.141	8.716E-03
A44	.567	.264	.211	.367	.297	.196	.294	4.928E-02
A41	.566	.185	.138	.433	.299	.167	.287	.137
A351	.565	.256	.373	.200	.192	6.186E-02	.246	.267
A47	.559	.328	.308	.277	7.856E-02	.177	.314	.253
A366	.537	.186	.437	.163	7.249E-02	.255	-1.443E-02	.179
A339	.516	.400	.300	9.124E-02	.337	2.608E-02	.451	2.117E-02
A357	.507	.429	.339	.207	.183	.164	.182	.259
A331	.493	.275	.373	.384	.234	.137	.129	.116
A348	.317	.756	8.360E-02	.197	6.886E-02	.184	8.460E-02	8.696E-02
A336	9.854E-02	.724	.171	8.895E-02	.353	.201	.210	6.012E-02

A347	.356	.724	.191	.214	7.481E-02	2.833E-02	.112	.157
A335	9.737E-02	.685	.340	.228	.293	.189	.146	6.758E-02
A346	.377	.662	.272	.253	.145	-8.885E-03	.119	.229
A343	.296	.651	.325	.276	.116	.231	8.840E-02	6.781E-02
A342	.455	.605	.220	7.712E-02	.106	.194	.199	6.561E-02
A345	.343	.598	.401	.266	4.744E-02	.220	.130	6.835E-02
A344	.277	.581	.413	.353	7.348E-02	.185	6.334E-02	7.043E-02
A333	.273	.421	.300	.376	.137	.112	.235	.345
A327	.341	.336	.715	.116	5.909E-02	.163	.169	.154
A326	.268	.260	.712	.176	.135	.190	.106	.188
A323	.318	.240	.694	.256	.140	.126	.247	.176
A322	.290	.272	.595	.203	.233	.254	.250	9.965E-02
A325	.325	.278	.592	.347	.255	.173	.167	.142
A328	.289	.235	.586	.309	.173	.156	.182	.191
A324	.176	.362	.581	.368	.332	.156	.156	7.801E-02
A321	.354	.191	.536	.243	.181	.276	.244	-5.545E-03
A337	.313	.388	.525	.115	.385	.109	.306	-5.425E-03
A334	.193	.442	.445	.284	.122	.258	.289	2.176E-02
A363	.303	.194	.314	.667	.180	.106	.217	4.546E-02
A362	.288	.333	.248	.654	.117	.121	5.420E-02	.191
A364	.152	.372	.186	.640	.218	.322	8.407E-02	9.392E-02
A361	.491	.261	.245	.595	.245	5.698E-02	.132	.150
A46	.361	.226	.215	.537	.252	.156	.267	.104
A43	.399	.371	.147	.519	.226	.258	.312	2.109E-03
A332	.266	.335	.251	.466	2.169E-02	.138	.130	.157
A45	.426	2.929E-02	.255	.460	.276	.172	.292	-.165
A25	8.817E-02	.133	5.561E-02	.198	.812	.165	.178	.231
A24	.303	5.513E-02	.194	.187	.677	.318	.173	.141
A26	.243	.103	.227	.273	.644	.329	.132	.185
A21	.186	.286	.181	9.647E-02	.633	.356	.264	.113
A23	.319	.283	.289	.158	.605	.342	2.850E-02	.153
A22	.305	.355	.173	.109	.482	.303	.193	.200
A16	.213	.134	.295	5.994E-02	.345	.720	4.289E-02	1.288E-02
A14	.150	.106	9.368E-02	.325	.285	.690	6.154E-02	.253
A15	.246	.135	.218	.126	.232	.672	.190	.296
A17	.219	.259	.231	.139	.271	.592	.294	6.943E-02
A13	9.857E-02	.202	7.858E-02	6.662E-02	.254	.564	.195	.542
A365	3.691E-02	.414	.257	.440	8.516E-02	.465	7.122E-02	.126
A18	.348	.251	.122	.168	.201	.462	.419	.120
A314	.274	.246	.253	.227	.323	.271	.580	.153
A311	.255	.196	.329	.197	.265	.271	.527	-2.310E-04
A313	.249	.232	.403	.314	.193	.248	.514	.129
A315	.192	5.535E-02	.314	.276	.258	.252	.509	.316
A338	.319	.467	.219	.228	.320	-2.643E-02	.501	8.978E-02
A312	.289	.256	.390	.268	.189	.316	.431	.143
A11	.187	.128	.200	.158	.334	.224	7.402E-02	.678
A12	.195	.216	.285	.126	.280	.319	9.234E-02	.656

因素萃取方法：主成份分析法。轉軸方法：Kaiser 正規化最大變量法

資料來源：本研究

四、因素之命名與信度（Reliability）、效度（Validity）

對於任何影響資訊安全因素，其因子負荷量小於 0.5 者，先予以刪除（Hair 等，1995），經刪除 A331、A333、A334、A332、A45、A22、A365、A18、A312 等 9 個，使得影響資訊安全因素共 57 個，再經分析其信度均在 0.8 以上，如表七 所示。對探索性研究而言，大於 0.8 可謂信度頗佳（Nunnally,1978；De Vellis, 1991）。本研究就萃取之因素共 8 個，予以因素之命名，其所含之影響資訊安全因素如表八所示。而因素荷量（Factor loading）大小可判定建構效度（Construct Validity）好壞，建構效度是指「能測量理論上某概念或特質的程度」（張紹勳，2000），本研究之 8 個因素構面，其所對應的各因素之因素負荷量均大於 0.5，故可宣稱收斂（Convergent）效度頗佳，收斂效度是指「來自同一因素構面的因素，彼此相關要高」，是建構效度的一種（張紹勳，2000），顯示本研究之信度、效度均頗佳。

表七 各因素構面信度

編號	因素構面	Cronbach'sα
1	軟體與稽核	0.9694
2	存取控制	0.9538
3	實體安全	0.9570
4	業務持續運作機制	0.9325
5	風險管理	0.9242
6	安全資源	0.9040
7	人員安全	0.9020
8	資訊安全政策	0.8574

資料來源：本研究

五、因素分析結果

將因素分析所得相關資料整理如表九所示。

表八 影響組織資訊安全關鍵因素之因素負荷量表（Factor loading）

因素構面	解釋變異量%（累積變異量%）	Cronbach's α (特徵值)	影響資訊安全因素		因素負荷量
軟體與稽核	56.863 (56.863)	0.9694 (37.530)	A354	應用軟體變更後，立即更新系統文件，兩者保持一致	.730
			A353	系統文件之管理、維護及保護	.703
			A356	將資訊安全列為應用軟體變更管制程序的一部份	.630
			A349	存取控制各項紀錄的建立與保存	.609
			A341	制定存取控制政策並符合法令規定	.604
			A355	應用軟體之處理程序與組織之內部控制程序一致	.597
			A42	定期實施外部稽核	.586
			A352	建立應用軟體執行碼之更新程序，並由專人管理與記錄	.578
			A367	業務持續運作機制之定期測試與演練	.575
			A44	與資訊安全相關紀錄檔案之記錄與保管	.567
			A41	定期實施內部稽核	.566

			A351	將資訊安全列入應用系統開發與維護的要求	.565
			A47	對資訊安全有關法令之遵守	.559
			A366	異地備援機制	.537
			A339	資料及軟體交換之安全控制	.516
			A357	委外軟體開發與維護時，將遵守資訊安全規範列入契約條款	.507
存取控制	4.901 (61.763)	0.9538 (3.235)	A348	對機密性、敏感性之系統與資料，建立特別的存取控制方式	.756
			A336	對機密性、敏感性資料傳輸之特別保護措施（如：加密）	.724
			A347	使用者密碼使用、確認、登入管理之具體規範	.724
			A335	對機密性、敏感性資料之管制處理程序	.685
			A346	依系統安全等級、分類、網路型態訂定適當的存取權限管理方式	.662
			A343	多使用者系統建立使用者帳號與密碼管理程序	.651
			A342	對特權使用之限制與配置之管制	.605
			A345	網路管制以區隔服務、使用者與資訊系統等不同群組	.598
			A344	遠端使用者之存取，建立驗證管制措施	.581
實體安全	3.056 (64.821)	0.9570 (2.017)	A327	機房與附屬設備之操作程序與管理責任	.715
			A326	電腦機房及重要區域之進出管制	.712
			A323	對於危害硬體設備之環境條件（如：火、水災…）均予安全評估與控制	.694
			A322	依設備之重要程度，予以區隔保護，專人管理	.595
			A325	設備維護之安全評估與控制	.592
			A328	儲存媒體之安全評估與管理控制	.586
			A324	電源供應之安全評估與控制（如：備援）	.581
			A321	硬體設備之建置先考量安全因素	.536
			A337	網路安全之管理、硬體與軟體之建置	.525
業務持續運作機制	2.462 (67.284)	0.9325 (1.625)	A363	安全事故之檢討改進與經驗學習	.667
			A362	安全事故之責任、通報與緊急處理程序	.654
			A364	系統中斷時，使業務持續運作之程序	.640
			A361	建立弱點、威脅與故障之回應制度	.595
			A46	稽核結果之後續行動（如：修正資訊安全政策、進行風險評估、修正內部控制等）	.537
			A43	內部稽核人員先接受稽核訓練	.519
風險管理	2.351 (69.634)	0.9242 (1.551)	A25	依風險分析與風險評估結果進行資訊安全需求規劃	.812
			A24	進行資訊安全風險評估與差異分析(目前安全狀況與適當安全水準的 gap)，以瞭解風險情況	.677
			A26	資訊安全風險管理之策略規劃	.644

			A21	進行資訊安全風險分析，包括威脅與弱點分析	.633
			A23	對不同機密等級建立保護措施	.605
安全資源	2.151 (71.786)	0.9040 (1.420)	A16	資訊安全資源規劃	.720
			A14	設置資訊安全組織或指派資訊安全人員	.690
			A15	資訊安全權責劃分	.672
			A17	資訊安全預算	.592
			A13	資訊安全政策之定期檢討修正	.564
人員安全	1.774 (73.560)	0.9020 (1.171)	A314	對不同職務予以適當資訊安全教育與訓練	.580
			A311	人員進用與調職時，作適當之安全評估	.527
			A313	重要或特別權限工作之人員輪調與人力備援	.514
			A315	組織各階層之資訊安全意識	.509
			A338	建立操作管理之各項紀錄日誌	.501
資訊安全政策	1.634 (75.194)	0.8574 (1.079)	A11	制定資訊安全政策並予文件化	.678
			A12	依據組織目標與策略、資訊政策及業務特性等因素制定資訊安全政策	.656

資料來源：本研究

六、分析與討論

本研究以「整合性資訊安全管理模式」（Integrated System Information System Management Model）之四個資訊安全管理活動為基礎，經整理資訊安全有關文獻，以階層式展開，提出資訊安全影響因素 66 項，其架構如圖二所示，包括：安全政策與組織、風險管理、內部控制、安全稽核，其中內部控制又可分為：人員安全、實體安全、系統與網路安全、存取控制、系統開發與維護、業務持續運作管理等，底層全部共九個部分，經進行因素分析後，萃取八個因素構面，命名為：軟體與稽核、存取控制、實體安全、業務持續運作、風險管理、安全資源、人員安全、資訊安全政策等。其因素構面與「整合性資訊安全管理模式」所發展之「影響資訊安全因素架構」兩者對照，如表九所示。

因素構面與影響資訊安全因素架構之比較與分析：

（一）因素分析結果，其因素構面較原影響資訊安全因素架構多出「資訊安全資源」，顯示組織意識到，任何資訊安全的規劃與執行，資訊安全產品或工具的使用，無一不需要投入充分的資訊安全資源。其

表九 因素構面與影響資訊安全因素架構對照表

因素構面	影響資訊安全因素架構
軟體與稽核	系統開發與維護 資訊稽核
存取控制	存取控制
實體安全	實體安全
業務持續運作機制	業務持續運作管理
風險管理	風險管理
安全資源	
人員安全	人員安全
資訊安全政策	資訊安全政策與組織
	系統與網路安全

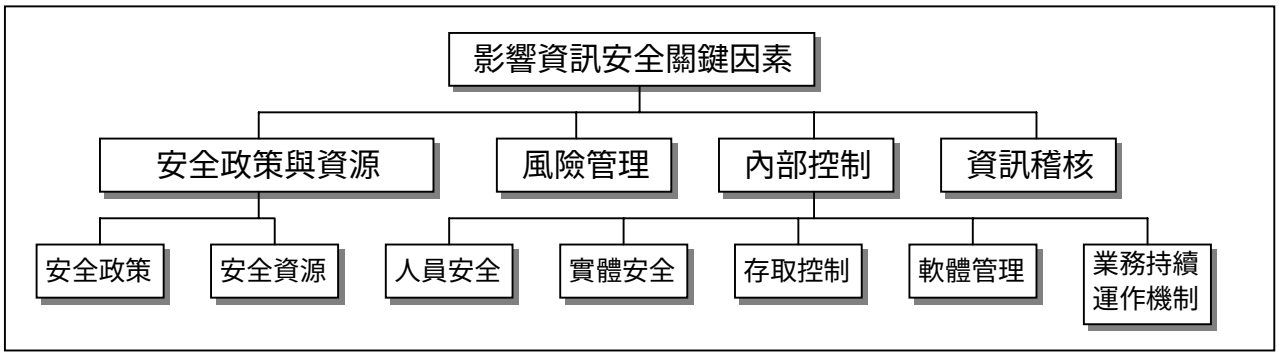
資料來源：本研究

資訊安全資源包括：資訊安全組織的設置、資訊安全人員的指派、資訊安全經費的籌措，並輔以資源規劃，藉資訊安全政策之定期檢討修正，來達成資源的有效運用。本研究亦足以顯示組織對資訊安全資源的重視，對於資訊主管（Chief Information Officer, CIO）而言，其對安全資源體驗尤深。從另一角度來看，資訊安全已從產品或技術觀點漸漸轉變到管理觀點，或策略觀點。

（二）因素構面較原影響資訊安全因素架構則減少「系統與網路安全」，原「系統與網路安全」中的變數，其中「資訊設備與系統環境之操作與變更程序」、「軟體開發與正式作業不使用同一個伺服器與資料庫」、「將資訊安全應遵守之規定，納入委外合約條款」及「對病毒、惡意軟體入侵的預防、偵測與處理」等由於因子負荷量少於 0.5 而予以刪除。其中「對機密性、敏感性資料之管制處理程序」與「對機密性、敏感性資料傳輸之特別保護措施」則歸入「存取控制」因素構面。另「網路安全之管理、硬體與軟體之建立」歸入「實體安全」因素構面，「建立操作管理之各項紀錄日誌」歸入「人員安全」因素構面，而「資料及軟體交換之安全控制」則歸入「軟體與稽核」構面，致「系統與網路安全」未能單獨成為一個因素構面，顯示「系統與網路」較傾向操作、產品、技術等特性之安全變數，由傾向策略與管理特性的安全因素構面來表現。但上開各變數之重要性平均最低者為 5.62，遠高於中間尺度的 4，且 Cronbach's α均高於 0.98，顯示各個變數均具重要性，因此，此部分尚有討論空間。

（三）無論是對「資訊安全資源」的重視或傾向操作、產品、技術等特性的變數，由傾向策略與管理特性的安全因素構面來表現，都有可能係由於本研究調查對象多數為 CIO 有關，若調查對象多數為資訊技術人員，而其結果可能有所不同，值得作為後續研究。

本研究經萃取因素構面，再以「整合性資訊安全管理模式」為基礎，經修正後，建構為「影響資訊安全關鍵因素架構」如圖五所示。



圖五　影響資訊安全關鍵因素架構（資料來源：本研究）

陸、結論與建議

本研究以「整合性資訊安全管理模式」為基礎，提出影響資訊安全因素架構，影響資訊安全因素 66 項，以問卷調查蒐集資料，經進行因素分析結果，萃取八個因素構面，提出結論與建議。

一、結論

（一） 本研究萃取八個因素構面，按解釋變異量由大而小，依序分別為：「軟體與稽核」、「存取控制」、「實體安全」、「業務持續運作機制」、「風險管理」、「安全資源」、「人員安全」與「資訊安全政策」等。

（二） 以「整合性資訊安全模式」為基礎，將「影響資訊安全因素架構」，透過因素分析所萃取之八個因素構面，轉化為「影響資訊安全關鍵因素架構」，包括「安全政策與資源」、「風險管理」、「內部控制」與「安全稽核」；其中「安全政策與資源」又可區分為：「安全政策」與「安全資源」；「內部控制」又可區分為：「人員安全」、「實體安全」、「存取控制」、「軟體管理」與「業務持續運作機制」等影響資訊安全關鍵因素。

（三） 「軟體與稽核」解釋變異量最大（56.863），顯示「軟體管理」與「資訊稽核」係組織資訊安全管理的核心，「軟體管理」尤應重視變更管理、文件管理、及與內部控制等；「資訊稽核」是組織落實資訊安全的最後把關，顯示組織實施定期的內外部資訊稽核、紀錄的保存、遵守資訊安全法令等，係對資訊安全規劃與執行的評估與檢驗，均極為重要。

（四） 「存取控制」解釋變異量次之（4.901），顯示「存取控制」制度的建立及執行，係資訊安全重要的一環。尤其在機密性維護，身分辨識機制等均頗為重要。

（五） 「實體安全」之解釋變異量再次之（3.056），「實體安全」係最早受到重視的資安因素，無論是災害的預防與控制，或是網路安全之管理、硬、軟體之建置等，都甚為重要。

（六） 解釋變異量>2, <3 的有「業務持續運作機制」與「風險管理」及「安全資源」，其重要程度較上述所列為低。對於安全事故發生後的處理，風險分析與控制，資訊安全人力與經費的籌劃等，亦是影響資訊安全的因素之一。

（七） 解釋變異量>1, <2 的有「人員安全」與「安全政策」，其重要程度又更低於上述所列。組織內部人員對資訊安全始終是威脅之一，因此，對於以安全為著眼的人力資源管理，資訊安全的教育訓練，及資訊安全政策的制定，都是影響資訊安全的因素之一。

（八） 本研究與其他相關研究或國際標準之比較：

1. ISO / IEC 17799（2000）之控制方法細目有：安全政策、安全組織、資產分類及控制、人員安全、實體及環境安全、通訊與操作管理、存取控制、系統開發及維護、業務持續性管理及符合性等，與本研究所得之因素構面比較如下：其中「人員安全」、「實體安全」、「存取控制」與「業務持續運作機制」等兩者並無不同。本研究之「資訊安全政策」對應其「安全政策」與「安全組織」；本研究之「軟體與稽核」則對應其「系統開發及維護」與「符合性」；本研究之「風險管理」除包含其「資產分類及控制」外，並增加「風險評估與控制」；本研究之「安全資源」卻係其所無，但「通訊與操作」雖係本研究所無，其原因如本研究「分

析與討論」中所述。

2. 本研究所得之資訊安全關鍵因素架構與其他資訊安全管理理論之比較：本研究之「資訊安全政策」對應安全政策理論及管理系統理論之「資訊安全政策」，及權變管理理論之「政策導向」等；本研究之「風險管理」對應風險管理理論之「風險評估」與「風險控制」、管理系統理論之「風險管理」，及權變理論之「風險管理導向」等；本研究之內部控制，包括：「人員安全」、「實體安全」、「存取控制」、「軟體管理」、「業務持續運作機制」等對應控制與稽核理論之「控制制度」、管理系統理論之「資訊安全範圍」，及權變理論之「控制與稽核導向」等；本研究之「資訊安全稽核」對應到控制與稽核理論之「資訊稽核」及權變理論之「控制稽核導向」等。但本研究之「安全資源」都是上開理論所無。
3. 張詠翔（2005）之研究所萃取之因素構面有：資訊安全政策、資訊安全風險管理、企業持續性管理、安全政策及人員管理、資訊資產管理及資訊安全防護機制等 6 個。與本研究所得之因素構面比較如下：本研究解釋變異最大的因素構面為「軟體與稽核」，而張的解釋變異量最大的因素構面為「資訊安全政策」，其中因素負荷量＞7 的因子，絕大部與「軟體管理」及「資訊稽核」有關，亦可據以命名為「軟體與稽核」。「風險管理」、「業務持續運作」、「人員安全」、「安全政策」等，兩研究並無不同。而本研究之「存取控制」、「實體安全」、「安全資源」等與上開研究之「資訊資產管理」、「資訊安全防護機制」兩者因素構面名稱雖不同，但究其所含因子，實質內容相似度則達 60%以上。但整體而言，本研究所整理的影響資訊安全因素較多，涵蓋範圍亦較廣，尤其在各家均甚為重視的「內部控制」著墨較多。

二、建議

（一） 對於影響資訊安全因素的八個關鍵因素，可作為組織資訊安全策略規劃的依據，並依據「整合性資訊安全管理模式」的程序，逐步規劃、發展與建置，值得實務界參考採行。

（二） 本研究所得之「影響資訊安全關鍵因素」，其每個因素的權重為何？如何運用以評估組織資訊安全，甚至建構資訊安全評估模式，都是未來可以研究的方向。

（三） 在「關鍵因素」的研究中，未來亦可擴大受測對象，並進行集群分析（Cluster Analysis），以了解不同受測對象，或不同組織間其影響資訊安全關鍵因素的差別為何？

參考文獻

1. Clyde, R. A., ***資安著重管理架構***，資訊傳真周刊，Nov.4, 2002, PP.46- 47。
2. TCSEC, ***可信賴系統評估準則 (Trusted Computer System Evaluation Criteria, TCSEC)***, http ://www.rdec.gov.tw/mis/standard 92/ipcs/tcsec.htm. 2003
3. 余幸真，***學習性網站關鍵因素之研究***，實踐大學企業管理研究所碩士論文，2001。
4. 吳青松，***臺灣資訊電子業關鍵成功因素之探討***，科技體制與產業發展小型研討會，1992。

5. 吳思華, ***產業政策與企業策略***, 中華經濟研究所, 台北, 1988。
6. 吳琮璠, ***國外政府機構資訊系統安全稽核制度***, 存款保險資訊季刊, 第 10 卷, 第 2 期, 1996, PP.21-40。
7. 吳琮璠, ***會計財務資訊系統***, 智勝文化事業有限公司, 台北, 2002。
8. 宋振華、楊子劍, ***組織資訊安全體系與資訊安全整體架構***, 資訊系統可信賴作業體制研討會論文集, 2001, PP.114-125。
9. 李東峰、林子銘, ***風險評估觀點的資訊安全規劃架構***, 台灣大學資訊管理學系第十二屆國際資訊管理學術研討會, 2001。
10. 張紹勳, ***研究方法***, 滄海書局, 台中, 2000。
11. 張詠翔, ***結合 BS7799 與資訊安全藍圖建構資訊安全評估機制之研究***, 銘傳大學資訊管理學系碩士論文, 2005。
12. 黃承聖, ***企業資訊安全的起點－資訊安全政策***, 網路通訊, 第 109 期, 2000, PP.100-103。
13. 黃亮宇, ***資訊安全規劃與管理***, 松崗電腦圖書公司, 台北, 1992。
14. 黃俊英, ***多變量分析***, 第七版, 中國經濟企業研究所, 台北, 2000。
15. 楊金炎, ***企業內部控制有關資訊系統與安全的個案研究***, 中原大學資訊管理學系碩士論文, 2001。
16. 葉牧青, ***AHP 層級結構設定問題之探討***, 國立交通大學管理科學研究所碩士論文, 1989。
17. 虞金燕、鄭祥勝, ***資訊安全發展趨勢與科專研發方向建議***, 財團法人資訊工業策進會, 台北, 2001。
18. 樊國楨、方仁威與徐士坦, ***建立我國通資訊基礎建設安全機制標準規範實作芻議研究報告書***, 經濟部標準檢驗局委辦計畫, 2001a , PP.1-52。
19. 樊國楨、方仁威、林勤經與徐士坦, ***資訊安全管理系統驗證作業初探***, 建立我國通資訊基礎建設安全機制標準規範實作芻議研究報告書, 經濟部標準檢驗局委辦計畫, 2001b, PP.105-125。
20. 樊國楨與楊晉寧, ***互連網（Internet）電子信息交換安全－以電子公文交換作業安全為本***, 電腦稽核, 1996, PP.14-25。
21. 鄭信一, ***現代企業資訊安全之個案研究***, 銘傳大學管理科學研究所碩士論文, 1999。
22. 謝玲芬, ***多目標（多準則）評估技術之探討及其在組織績效評估之應用***, 國立清華大學工業工程研究所碩士論文, 1989。
23. 謝清佳、吳琮璠, ***資訊管理－理論與實務***, 資訊管理智勝文化事業, 台北, 1999。
24. Aaker, D.A., ***Strategic Market Management,*** John Wiley & Sons, New York, 1984.
25. Anderson, J.M., ***Why we Need a New Definition of Information Security***, Computers & Security, Vol.22, No.4, 2003, PP.308-313.
26. Bryman, A. & Cramer, D., ***Quantitative Data Analysis With SPSS for Windows: A guide for Social Scientists***, Routledge, London, 1997.
27. BSI, ***Information Security Management Part2: Specification for Information Security Management System (BS 7799-2)***, British Standards Institution (BSI), London, 1999.
28. Chapman, B.D. & Zwicky, E.D., ***Building Internet Firewalls***, O'Reilly & Associates, Inc., 1995.
29. Daniel, D.R, ***Management Information***

Crisis, Harvard Business Review, September-October 1961, PP.111-121
30. David, C. & Rivett, B.H.P., ***A Structural Mapping Approach to Complex Decision Making***, Journal of Operational Society, Vol.29, No.2, 1978, PP.113-128.
31. De Vellis, R.F., ***Scale Development Theory and Applications,*** Sage Publications, London, 1991.
32. Dhillon, G. & Backhouse, J., ***Information System Security Management in the New Millennium***, Communication of the ACM, Vol.43, No.7, July 2000, PP.125-128.
33. Drazin, R. & Van de Ven, A.H., ***Alternative Forms of Fit in Contingency Theory,*** Administrative Science Quarterly, 30, 1985, PP.514-539.
34. Ellison, R.J. etal., ***Survivable Network System Analysis: A Case Study,*** IEEE Software, Vol.16, No.4, 1999, PP.70-77.
35. Eloff, M.M. & Von Sloms, S.H., ***Information Security Management: An Approach to Combine Process Certification And Product Evaluation***, Computers & Security, Vol.19, No.8, 2000, PP.698-709.
36. Ettinger, J.E., ***Introduction: Key Issues in Information Security***, Information Security-An Integrated Approach, Chapman & Hall, London, 1993.
37. Ferguson, C.R. & Dickinson, R., ***Critical Success Factor or Directors in the Eighties***, Business Horizons, May-June 1982, PP.14-18.
38. Finne, T., ***Information Systems Risk Management: Key Concepts and Business Processes***, Computers & Security, Vol.19, No.3, 2000, PP.234-242.
39. Flynn, N.L., ***The e Policy handbook: Designing and Implementing Effective E-Mail, Internet, and Software Policies***, American Management Association, New York, 2001.
40. Gay, L.R., ***Educational Research Competencies for Analysis and Application***, Macmillan, New York, 1992.
41. Gehrke, M., Pfitzmann, A. & Rannenberg, K., ***Information Technology Security Evaluation Criteria (ITSEC)-A Contribution to Vulnerability?*** , INFORMATION PROCESSING 92-Proceedings of the IFIP 12th World Computer Congress Madrid, Spain, September 1992, PP.7-11.
42. Gollmann, D. ***Computer Security***, John Wiley & Sons Ltd., UK, 1999.
43. Guieford, J.P., ***Fundamental Statistics in Psychology and Education***, 4th ed., McGraw-Hill, New York, 1965.
44. Gupta, M., Chaturvedi, A.R., Mehta, S. & Valeri, L., ***The Experimental Analysis of Information Security Management Issues For Online Financial Services,*** Proceedings of the 21th International Conference on Information System, 2001, PP.667-675.
45. Hair, J.F., Anderson, R.E. Tatham, R.L., & Black, W.C., ***Multivariate Date Analysis with Readings***, 4th ed., Englewood Cliffs, Prentice-Hall, New Jersey, 1995.
46. Hinde, S., ***Security Survey Spring Corp***, Computer & Security, Vol.21, No.4, 2002, PP.310-321.
47. Hofer, C.W. & Schendel, D., ***Strategy Formulation: Analytical Concepts***, St. Paul, West Publishing, MN, 1978.
48. Hong, K.S., Chi, Y.P., Chao, L.R. & Tang, J.H., ***An Integrated System Theory of Information Security Management***, Information Management & Computer Security, Vol.11, No.5,

2003, PP.243-248.
49. ISACA, ***Governance, Control and Audit for Information and Related Technology (COBIT)***, 3rd ed., Governance Institute, ISACA, 2001.
50. ISO/IEC 17799, ***Information technology-code of practice for information security management,*** 2000.
51. Kabay, M.E., ***The NCSA Guide to Enterprise Security: Protecting Information Assets***, McGraw-Hill, New York, 1996.
52. Kaiser, H.F., ***The Varimax Criterion for Analytic Rotation in Factor Analysis***, Psychometrika, 23, 1958, PP.187-200.
53. Kaiser, H.F. & Rice, J., ***Little Jiffy, MarkIV,*** Educational and Psychological Measurement, Vol.34, No.1, 1974, PP.111-117.
54. Lee, S.M., Luthans, F. & Olson, D.L., ***A Management Science Approach to Contingency Models of Organizational Structure***, Academy of Management Journal, Vol. 25, No.3, 1982, PP.553-566.
55. Luthans, F., ***Introduction to Management: A Contingency Approach***, McGraw-Hill, New York, 1976.
56. Moulton, R., ***A Strategic Framework for Information Security Management***, Proceedings of the 14th Computer Security Conference, Washington D.C., 1991.
57. Nunnally, J., ***Psychometric Theory***, 2nd ed., McGraw-Hill, New York, 1978.
58. Panda, B. & Giordano, J., ***Defensive Information Warfare***, Communications of the ACM, Vol.42, No.7, 1999, PP.31-32.
59. Pfleeger, C.P., ***Security in Computing***, 2nd ed., Englewood Cliffs, Prentice-Hall, New Jersey, 1996.
60. Reid, R.C. & Floyd, S.A., ***Extending the Risk Analysis Model to Include Market-Insurance***, Computers & Security, Vol.20, No.4, 2001, PP.331-339.
61. Robbins, S.P., ***Management***, 4th ed., Englewood Cliffs, Prentice-Hall, New Jersey, 1994.
62. Rokert, ***Chief Executives Define Their Own Data Needs***, Harvard Business Review, March-April 1979, PP.81-93.
63. Rusell, D. & Gangemi, G.T., ***Computer Security Basics***, O'Reilly & Associates Inc., California, 1992.
64. Schendel, D.E. & Hofer, C.W. (eds), ***Strategic Management: A New View of Business Policy and Planning***, Little, Brown & Company, Boston, 1979.
65. Schneider, E.C. & Gregory, W.T., ***How Secure Are Your System?*** Avenues to Automation, November 1990.
66. Schultz, E.E., Proctor, R.W., Lien, M.C. & Salvendy, G., ***Usability and Security An Appraisal of Usability Issues in Information Security Methods***, Computer & Security, Vol.20, No.7, 2001, PP.620-634.
67. Sherwood, J., ***SALSA: A Method for Developing the Enterprise Security Architecture and Strategy***, Computer & Security, Vol.15, No.6, 1996, PP.501-506.
68. Simson, G. & Gene, S., ***Practical UNIX Security***, O'Reilly & Associates, California, 1991.
69. Smith, M., ***Computer Security-Threats, Vulnerabilities and Countermeasures***, Information Age, October 1989, PP.205-210.
70. Tabachnick, B.G. & Fidell, L.S., ***Using Multivariate Statistics,*** 2nd ed., Harper & Row Publishers, New York, 1989.
71. Thurstone, L.L., ***Multiple Factor Analysis,*** University of Chicago Press,

Chicago, 1947.
72. Von Solms, R., ***Information Security Management: The Second Generation***, Computer & Security, Vol.15, No.4, 1996, PP.281-288.
73. Von Solms, R., Van Haar, H., Von Solms, S.H. & Caelli, W.J., ***A Framework for Information Security Evaluation***, Information & Management, Vol.26, No.3, 1994, PP.143-153.
74. Weber, R., ***Information System Control and Audit***, Upper Saddle River, Prentice-Hall, New Jersey, 1999.
75. Wright, M., ***Third Generation Risk Management Practices***, Computer Fraud & Security, February 1999, PP.9-12.