資訊安全多準則評估之研究－捷運等相關個案

洪國興[1]　季延平[2]　趙榮耀[3]

摘　要

層出不窮的資訊安全事件不停的上演，駭客入侵、資訊外洩也時有所聞，在 e 化聲中，從政府到民間無不驚覺到資訊安全的重要。身負大眾運輸重任的捷運相關組織，無論係運輸營運，或是工程營建，其資訊系統對組織的重要程度正與日俱增，甚至是營運管理的命脈所繫，因此，資訊安全事件一旦發生，將立即衝擊組織的營運與服務。組織如何評估其資訊安全的程度？確實爲管理當局及社會所關注的議題，本研究係以資訊安全管理之「整合系統理論」爲基礎，以「資訊安全評估之總體指標」爲基本架構，建立「資訊安全多準則評估模式」，再以捷運等相關個案爲例，進行個案資訊安全評估，可作爲該等組織制定資訊安全管理策略之參考。

關鍵字：資訊安全、整合系統理論、多準則評估、資訊安全評估模式

Research on Multi-criteria Evaluation of Information Security

–Case Studies Regarding Rapid Transit System

Kwo-shing Hong　Yen-ping Chi　Louis R. Chao

Abstract

Various accidents of information security emerge in an endless stream. The hacker’s invading and information revealing also happen frequently. In the voice of electronic trend, the importance of information security is being aware by both the public and private sectors. Since the Rapid Transit System is responsible for public transportation, its information system is more and more important to the organization day by day either in the operation or construction. The information system is even the key element and lifeline of its operation management. Accordingly, once the information security accident happens, the operation and service of the Rapid Transit System will be affected immediately. How does the organization evaluate the degree of information security? It is really an important subject concerned by the management authority and the society. Basing on the “integrated system theory” of information security management, the research establishes the “information security multicriteria evaluation model” by the basic construct “overall indicator of information security evaluation”. It furthermore takes case studies of Rapid Transit System for example to evaluate the information security of cases. Its result is a useful reference for the organization to make information security management policy.

Keyword: information security, integrated system theory, multicriteria evaluation, information security evaluation model

1監察院綜合規劃室主任 ksh@ms.cy.gov.tw

2 國立政治大學資訊管理學系副教授 ypchi@mis.nccu.edu.tw

3 淡江大學管理科學研究所教授 chaory@ms.cy.gov.tw

一、緒論

層出不窮的資訊安全事件，無孔不入的網路入侵與組織內部的人謀不臧等，不斷地在世界各地上演，確實喚醒各界更加的重視資訊安全。組織期望可藉助研究的成果，作爲制定資訊安全策略的參考，但似無法令人滿意，所顯示的現象是：(1) 資訊安全技術面的研究多，管理面的研究少，更缺乏實證的研究（李東峰與林子銘，2001）；(2) 縱然有少數涉及資訊安全管理的研究，也是片面者多，整體性者少，且像瞎子摸象一樣只摸到一小塊，缺乏較完整的圖像，究竟是其中的那一塊呢？(3) 實務界出現一些錯誤的觀念，例如：防火牆即是資訊安全，資訊安全只有技術的問題等等……不一而足（黃承聖，2000）；(4) 直到 1995 年英國國家標準協會（British Standards Institution, BSI）制定 BS7799-1「資訊安全管理實務準則」第一部分（Information Security Management – Part 1：Code of Practice for Information Security Management），始出現較完整的資訊安全管理架構（林鈴玉，2001）。

由於資訊技術快速的進步，資訊處理架構不斷創新的情況下，資訊安全威脅的型態也千變萬化，資訊安全的技術與產品亦不斷的更新。而企業的產業別不同，所處的環境不同，組織目標更是有極大的差異，因此，不可能所有的組織都採用完全相同的資訊安全技術，建構一個與技術無關（Technical Independent）的資訊安全管理系統（Information Security Management System），以適用於不同資訊技術之組織，而如何評估此一系統的有效可行，則爲本研究之動機。

無論從學術研究的角度來看或實務面觀察，組織都需要有資訊安全管理的評估模式，使組織可以檢視其資訊安全的防衛能力，及爲資訊安全的策略管理提供一個可以參考的模式，這樣的評估模式相信是資訊安全的學術研究所要努力的方向，也是實務界所期盼的。當然資訊安全評估模式的建立是極度困難的工程，但總是要踏出困難的第一步，未來才能在現有的基礎上修正、發展，始能建構可長可久的評估模式，此亦是本研究的動機。

建立資訊安全多準則評估模式，爲組織之資訊安全評估提供策略性的參考架構。透過對資訊安全管理實務的調查，進行個案研究，以印證資訊安全管理「整合系統理論」的適合性，並發展有關資訊安全管理的研究命題，爲資訊安全管理的研究範圍與方向，開拓新的空間，則爲本研究的目的。

在捷運之工程建設與營運管理中，資訊技術（Information Technology）與知識管理（Knowledge Management）一向是捷運相關組織的核心能力，更爲其競爭利基，在善用 IT 與 KM 的過程中，資訊安全日益重要，因此，評估組織資訊安全的能力亦相對受到重視。捷運相關組織不只自身要擁有資訊安全及其評估能力，更應期許未來能以知識擴散的作法，創造組織的新利基，則亦是本研究的目的。

二、文獻探討

本研究先從文獻中探討資訊安全之定義，進而了解資訊安全管理理論之發展，並探討多準則評估與評估準則層級結構等。

2.1 資訊安全

「資訊安全」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；吳瑞明，1994；陳同孝，1996；林鈴玉，2001；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」。

「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）。

百分之百的資訊安全是難以做到的，爲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，其功能性典範（Functional Paradigm）採取下列措施（樊國楨等，2001；Panda & Giordano, 1999；樊國楨與時崇德，2000；Ellison, 1999；國家安全局，2000）：

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，關閉入侵者爲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。

宋振華與楊子劍（2001）指出：資訊安全是由一系列的安全機制所構成，每一個環節都是非常重要，一旦其中一個環境未能妥善的考慮到，即可能造成整體資訊安全體系的瓦解。因此，要建立一個完整的資訊安全體系，則需要有完整的思考，通盤的規劃，站在組織的立場，從各個層面思考不同的安全防護機制。

整體資訊安全架構的技術項目，係以安全需求爲中心，包含不同層次的資訊安全技術：

1. 安全需求：依據組織的目標、資訊政策及風險情況，研擬資訊安全需求。
2. 密碼演算法：包括密碼分析與技術。
3. 資訊系統：包括系統安全、網路安全及通信安全。
4. 應用環境：包括應用系統安全與資訊安全基礎建設。
5. 實體安全：資訊系統運作與環境之安全控管，如：機房進出管制、媒體管理、異地備援等。

資訊安全的目標在確保資訊的機密性、完整性與可用性等，即所謂的 CIA（Confidentiality、Integrity、Availability），係多數學者與專業人士可接受的定義。資訊安全可區分爲兩個層面，即技術與管理，技術層面的資訊安全發展較早，加密（Encryption）是典型的例子（陳彥學，2000；賴溪松與葉育斌，2001；劉國昌與劉國興，2001），防毒（Anti-Virus）、防火牆（Firewall）則是後起之秀；管理層面的資訊安全，在一些國際組織，諸如：BSI（British Standards Institution）、ISO 的推動下，始受到世界各國的重視，資訊安全相關國際標準的制定，如：BS7799、COBIT、橘皮書、紅皮書等對資訊安全由技術層面融入管理層面，邁向整體性、全方位架構，有極大的貢獻。一個整合資訊政策、標準、程序、資訊組織與資源、風險管理、安全意識與教育訓練、內部控制、資訊稽核的資訊安全架構，漸漸被浮現，其規劃與建置的範圍，不僅是實體面、技術面而已，更擴及政策、資源、管理與控制等，並爲因應組織環境的變化，作適當的檢討修正，形成一個循環週期。因此，資訊安全不再僅僅是技術的問題，或是安全產品與工具運用的問題，更是程序與管理的問題（洪國興，2003）。

2.2　資訊安全管理理論

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，更成爲組織的競爭策略，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，也將關係到組織資訊安全策略之建構。由資訊安全文獻探討，並從實務面觀察，可知資訊安全管理理論有（Hong 等，2003）：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。其資訊安全的決定則形成下列的函數關係（Hong 等，2003；洪國興與趙榮耀，2003）：

1.安全政策理論（Security Policy Theory, SPT）：

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）

2.風險管理理論（Risk Management Theory, RMT）：

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（制定控制制度，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）

3.控制與稽核理論（Control and Auditing Theory, CAT）：

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）

4.管理系統理論（Management System Theory, MST）：

資訊安全=f（資訊安全政策，資訊安全範圍，風險管理，實施控制制度）

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）

5.權變理論（Contingency Theory, CT）：

資訊安全＝f（資訊安全策略）

資訊安全策略=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，技術）

由於上開任何一種資訊安全管理理論，均僅能適用於部分資訊安全管理活動或機制，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，因此，整合既有的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，而另有「整合系統理論」（Integrated System Theory, IST）之提出。此一理論係由（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）爲基礎，並符合組織目標需求，形成一個整合性之資

訊安全管理模式，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，軟體管理，業務持續運作管理控制）

權變管理=f（組織內外部環境，資訊管理，資訊技術）

2.3　多準則評估與層級結構

同一事物具有多重屬性，受多重因素的影響，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價（闕頌廉，1994；劉永森，1991），即是多準則決策。多準則之群體決策（Group Decision Making）是單一決策者的延續（David & Rivett, 1978），其分析更加的複雜，必須考慮不同偏好的群體之間的衝突（Conflict），但由於群體決策可以增加決策的知識領域，擴大取得資訊的範圍，其決策亦較能得到群體的認同，使得群體參與作決策，成爲增進組織效能的一種趨勢，因此，多準則評估方法也受到管理者的重視（Huber, 1980；Hwang & Lin, 1987；謝玲芬，1989）。

在決策問題的建構步驟中，先要提出可行方案，再分析其多重目標與屬性，亦即建立決策的多重準則（Multiple Criteria）。接著決定各準則之權重，客觀地決定權重，才能使決策的結果具有相當的可信度，也是多準則決策過程中極具關鍵的程序（謝玲芬，1989）。本研究採用層級分析法（Analytic Hierarchy Process, AHP）作爲決定相對權重的方法，AHP 法的運用先要匯集專家學者的意見，將錯綜複雜的評估問題，予以層級（或網路）結構化，也就是先確定評估的主要準則，再將這些準則逐步細分，而形成一層級（或網路）結構，其最底層即爲決策者在評估時眞正的衡量項目（謝玲芬，1989）。

多重準則可採用網狀結構或層級結構分析。網狀結構之理論較爲艱澀，計算過程繁複，且在準則評估程序中，受到人類有限心智能力（比較心理原則）的限制，而容易產生混淆不清的現象，致對一般管理者而言，適用性較低。層級結構在評估的程序上，則顯得較爲清晰，且容易被人們所了解掌握，但如結構不清晰的複雜系統，卻有建構上的困難（葉牧青，1989）。本研究之「資訊安全管理」已有適當的理論基礎，即引用「整合系統理論」，其結構已近似層級關係，故其評估準則採用層級結構應頗爲適合。

「層級結構」是系統的一種特殊型態，當人類面對一個龐大而複雜的系統時，必然會將一個龐大的系統區分爲數個較小且彼此相關的系統，而層級結構合乎人們解決問題所採取的思考方式，適合用於敘述系統間的關係（王國明等，1998）。

此種結構乃是將問題系統所認定之「要件」（Entities）組合（Group）成幾個「互斥的集合」（Disjoint Sets），而形成上下「隸屬」（Dominated）的層級關係。並假設（Saaty, 1980）：

1.每一層的任一集合僅受上一層集合的影響。

2.同層中的集合彼此互斥。

3.集合中元素與元素之間相互獨立。

一個好的評估準則必須是：（1）每一個準則均與成功的目標有關；（2）評估準則必須形成一組完整、可掌握的評估條件，不應有重要的評估準則被遺漏（Rackham & Richard, 1995）。

三、研究模式

組織的資訊安全管理需要整合所有的管理政策與管理方法，乃是高層管理者所應考量到

的（Hinde,2003）。因此，組織之資訊安全管理活動，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）等資訊安全管理策略，以權變管理（Contingency Management）爲基礎的資訊安全管理架構，其中內部控制，又包含人員安全、實體安全、系統與網路、存取控制、軟體管理、業務持續運作管理等安全控制（Hong 等，2003；洪國興與趙榮耀，2003），示意如圖 1、圖 2 所示。

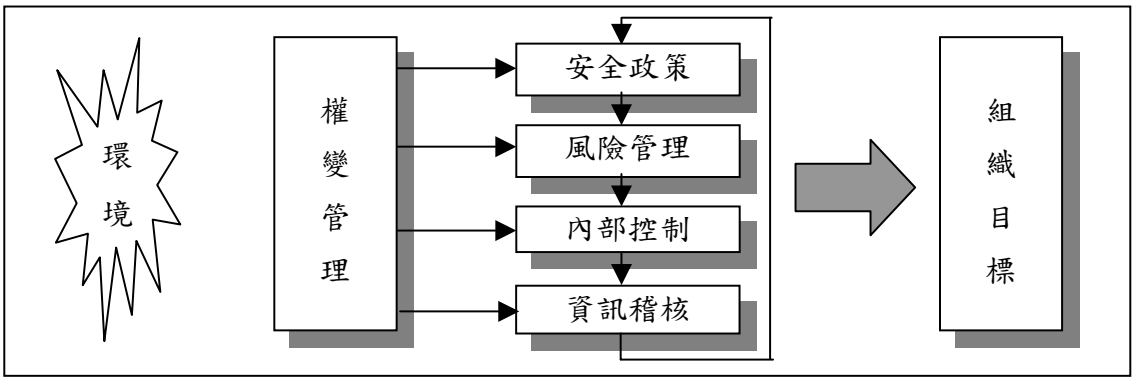

圖 1　資訊安全管理「整合系統理論」示意圖
（資料來源：Hong 等，2003；洪國興與趙榮耀，2003）

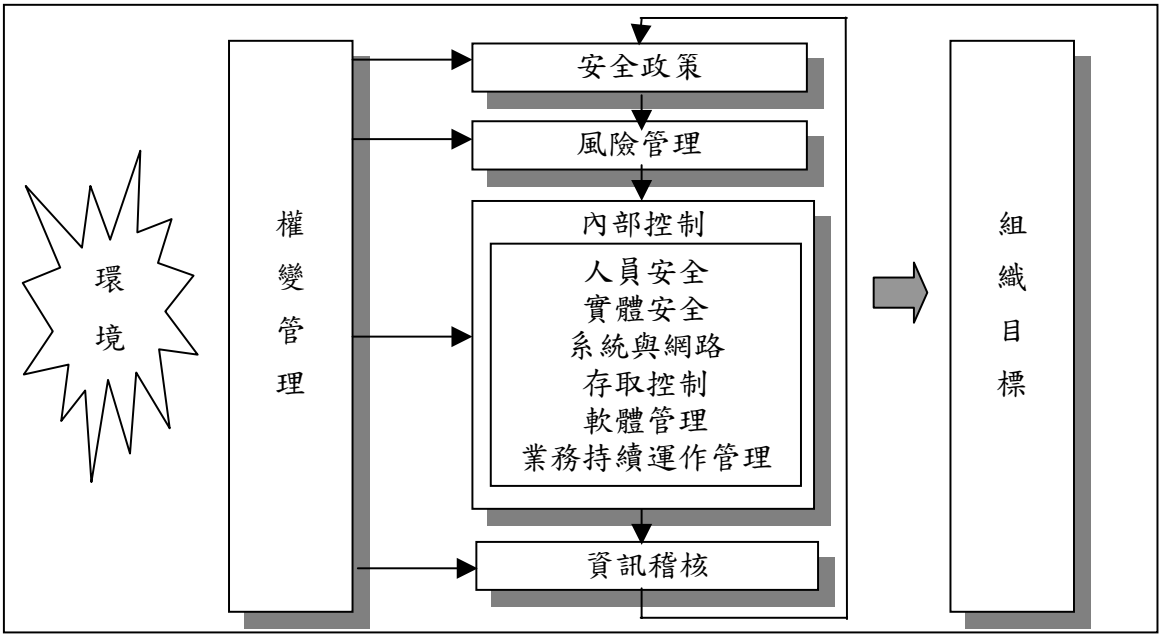

圖 2　資訊安全管理「整合系統理論」示意圖（續）
（資料來源：Hong 等，2003；洪國興與趙榮耀，2003）

以「整合系統理論」爲基礎，參考資訊安全各種文獻及國際標準，初擬資訊安全影響因素，經以名目群組技術（Nominal Group Technique, NGT），修正整理後，據以進行問卷調查，運用因素分析（Factor Analysis），萃取關鍵因素構面及因素，再發展資訊安全多準則評估指標，其指標之層級結構，如圖 3 所示。

縱然有評估指標，但若每一項指標等量齊觀，顯然並不符合組織管理策略之所需，組織對各項管理與技術的工具各有輕重緩急，而應給予不同的重視程度及優先順序（Priority），換言之，單憑以評估指標，而未賦予不同權重，是難以評估組織的資訊安全程度，因此，本研究之研究模式爲：以「整合系統理論」爲基礎，並以其據以發展的「資訊安全評估之總體指標」爲基本架構，進而建立可顯示各個評估指標不同權重的資訊安全多準則評估模式。

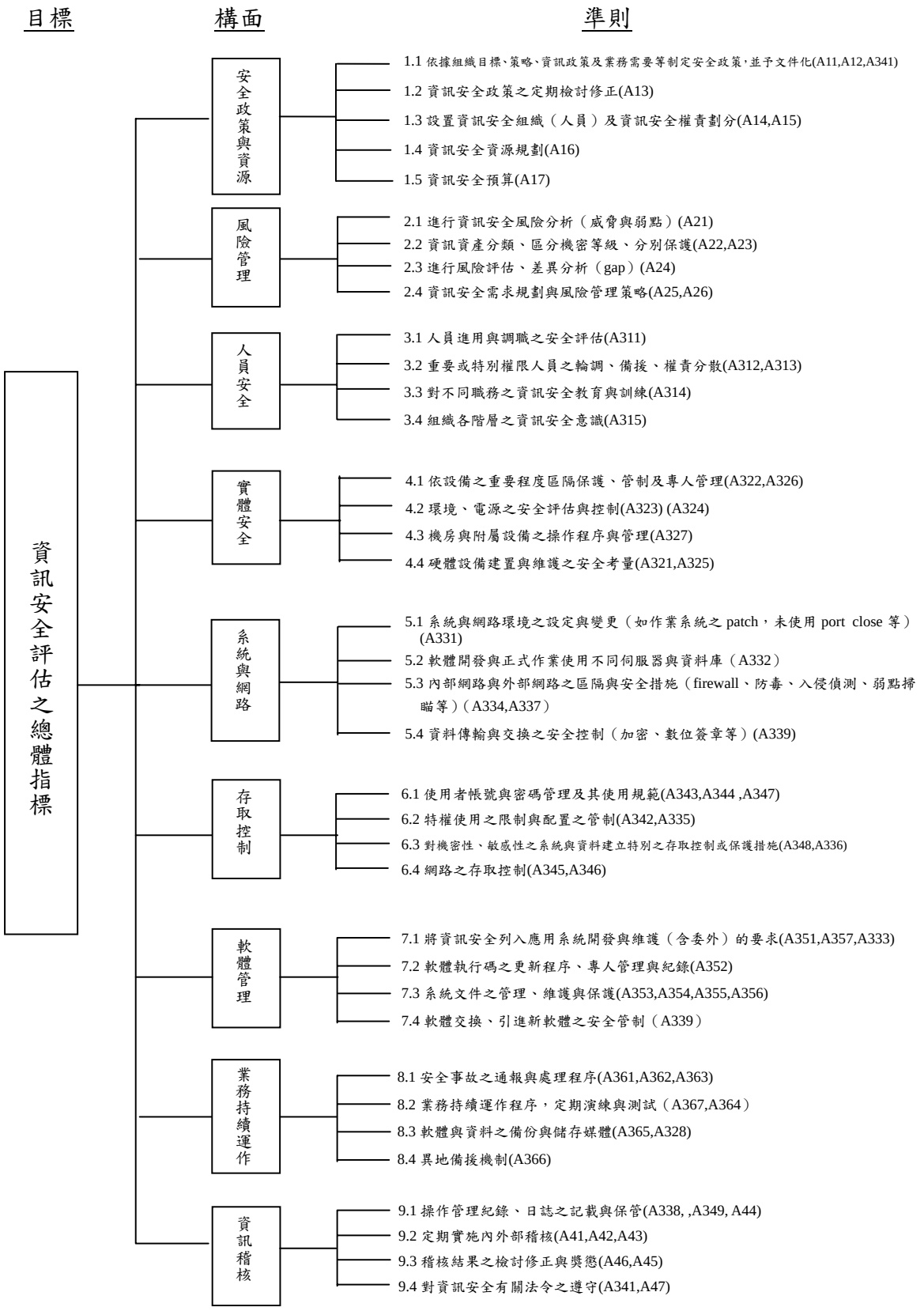

圖 3　資訊安全評估之階層體系圖

（資料來源：洪國興等，2003）

四、研究方法

本研究係以資訊安全「整合系統理論」爲基礎，並以其據以發展之「資訊安全評估之總體指標」爲基本架構，經由專家對各項評估指標重要程度的調查，透過層級分析法（Analytic Hierarchy Process, AHP），以「客觀的決定其權重」，而建立資訊安全的多準則評估模式，再以捷運等相關個案爲例，進行個案資訊安全評估。

4.1 研究流程，如圖4所示。

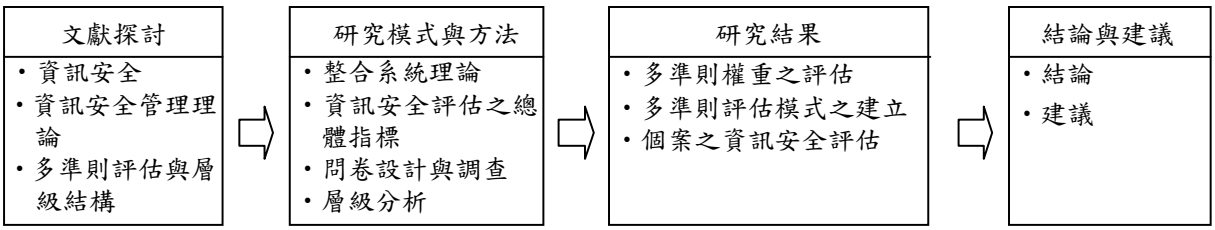

圖 4 研究流程圖（資料來源：本研究）

4.2 問卷設計與調查

問卷之設計，係依據「資訊安全評估之總體指標」，設計爲成對比較之評估問卷。分爲三個部分：

1. 第一部份：爲填答範例，由於本研究之多準則評估方法係採用層級分析法（AHP），在問卷調查時要進行成對比較，若違反邏輯一致性，將成爲無效問卷，因此，需有詳盡的填答範例，以提高問卷品質。
2. 第二部分：爲衡量指標的成對比較之問題，爲本問卷核心部分，共有10題。
3. 第三部分：爲基本資料，以作爲分群之基礎，並請受訪者填載姓名、電話等資料，當不一致性太高時，可再追蹤確認。

此問卷主要目的，在建立資訊安全多準則評估模式，因此調查對象，必須對資訊安全有相當了解，所以調查對象係選定組織之資訊主管或擔任資訊安全的工作者，故對下列專家進行調查：

1. 以組織性質分爲：政府機關、公民營企業與學校或研究機構等。
2. 以職務性質區分爲：資訊主管與非資訊主管，其非資訊主管均訪問在組織內負責或從事資訊安全工作之人員。

調查問卷 138 份，其中有效數爲 107 份，無效數爲 31 份。本研究經以「Expert Choice for Windows」決策支援軟體檢定其一致性，並逐一計算 AHP 問卷各層級之一致性。本研究以 C.R.（Consistency Ratio）爲一致性篩選標準，C.R.≦0.1 者始符合標準；C.R.＞0.1 者，則予以剔除，列爲無效問卷，其問卷回收統計如表 1、表 2 所示。

表 1 AHP 問卷回收情形

區分	政府機關	公民營企業	學校或研究機構	合計
回收數	52	71	15	138
有效數	42	54	11	107
無效數	10	17	4	31

資料來源：本研究

表 2　AHP 有效問卷之統計

區分	政府機關	公民營企業	學校或研究機構	合計
資訊主管	20	22	2	44
非資訊主管	22	32	9	63
合計	42	54	11	107

資料來源：本研究

4.3　層級分析法

本研究係爲建立資訊安全之多準則評估模式，其核心在於如何「客觀的決定權重」，因此，本研究之研究方法採用層級分析法（Analytic Hierarchy Process, AHP）。

層級分析法（Analytic Hierarchy Process, AHP）係 Thomas L. Saaty 於 1971 年開始發展。AHP 是一種多目標（多準則）的決策方法，主要應用在不確定（Uncertainty）情況下及多個評估準則的決策問題。Saaty 於 1971 年正在美國國防部從事應變規劃問題（Contingency Planning Problem）的研究工作，於 1972 年在美國國家科學基金會（National Science Foundation）的贊助下，進行產業電子合理分配的研究。1973 年 AHP 應用在 Saaty 主持的蘇丹運輸系統研究案，其理論始漸趨成熟。1974 至 1978 年間，亦不斷將 AHP 應用在其所主持的醫療優先排序分配資源衝突之研究案，並一再應用、修正及證明後，使 AHP 理論更臻完備（Saaty, 1980；Saaty & Vargas, 1980, 1982；Saaty & Bennett, 1977；葉牧青，1989；鄧振源與曾國雄，1989）。直到 1982 年爲止，AHP 已應用在下列十二種類型之問題：決定優先次序（Setting Priorities）、產生替代方案（Generating a Set of Alternatives）、選擇最佳政策或方案（Choosing a Best Policy/Alternatives）、決定需求（Determining Requirements）、資源分配（Allocating Resources）、預測結果或風險評估（Predicting Outcomes or Risk Assessment）、衡量績效（Measuring Performance）、系統設計（Designing a System）、確保系統穩定（Ensuring System Stability）、最適化（Optimizing）規劃（Planning）、衝突的解決（Conflict Resolution）（Saaty, 1980；葉牧青，1989；鄧振源與曾國雄，1989）。

之後 AHP 應用的領域除多目標決策（Multiple Criteria Decision Making；MCDM）、規劃及資源配置（Planning and Resource Allocation）、公共政策（Public Policy）外，更擴大到：供應商選擇評估（Supplier Selection Criteria）、資訊服務提供者評估（Information Service Provider Evaluation）、Intranet 採用評估（Evaluation of Intranet Adopted）與資訊委外評選等（謝玲芬，1989；黃智偉，2000；施穎偉，2000；杜鴻業，1998；盧彥旭，2001）。

應用 AHP 來處理複雜的決策問題，其進行的步驟與程序如下（鄧振源與曾國雄，1989；謝玲芬，1989；黃智偉，2000；葉牧青，1989；杜鴻業，1998；翁俊興，1983；謝育文，1985；方溪泉，1994；周冠中，1995；唐印星，1999）：

1. 問題界定
2. 構建層級結構

羅列要素或準則（Elements /Criteria），建立層級架構，要素或準則數目（最好不超過7個）。

3. 問卷設計與調查
4. 各層級要素/準則間權重的計算

建立成對比較矩陣，計算特徵值與特徵向量，一致性的檢定。

5. 整體層級一致性的檢定
6. 替代方案的選擇

整個AHP進行的步驟與程序如圖5所示：

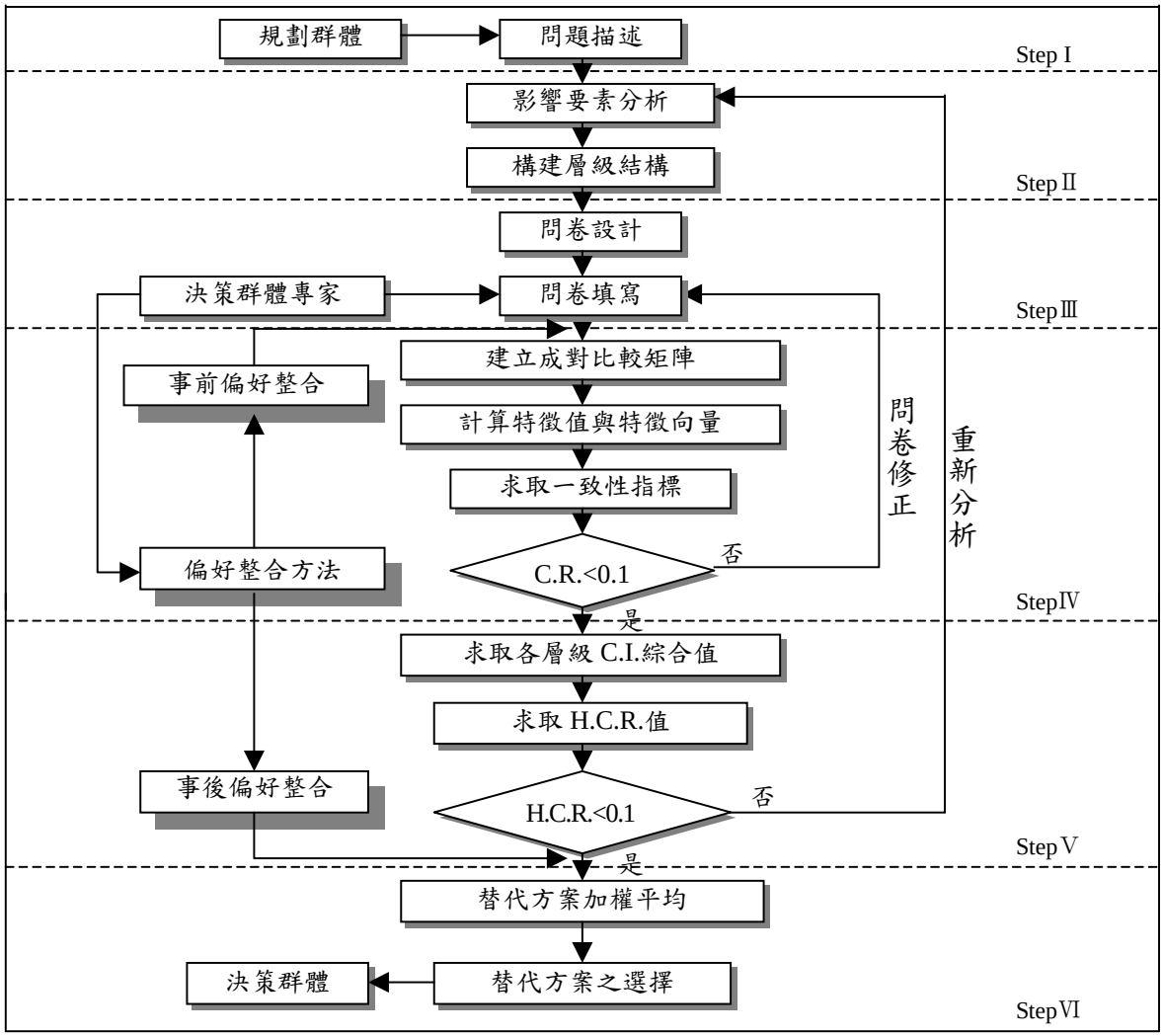

圖 5 應用 AHP 流程圖（資料來源：鄧振源與曾國雄，1989；鄧振源，2002）

五、資料分析與研究結果

5.1多準則評估模式之建立

資訊安全多準則評估模式的建構，開始於評估準則層級結構的建立，再經由資訊安全專家對評估準則之權重進行評估。本研究所建立的多準則評估模式，其評估準則之層級可區分爲三階層與四階層：

1. 三階層之多準則評估模式，其評估構面只有一層級，主要理由係較易被權重評估的專家公平看待，避免其相對權重評估失眞。其評估構面共有九個：安全政策與資源（0.1918）、風險管理（0.1100）、人員安全（0.1355）、實體安全（0.1009）、系統與網路安全（0.1241）、存取控制（0.1280）、軟體管理（0.0528）、業務持續運作（0.0952）、資訊稽核（0.0618）等，下一階層各評估準則共分爲37個，其權重等如圖6所示。

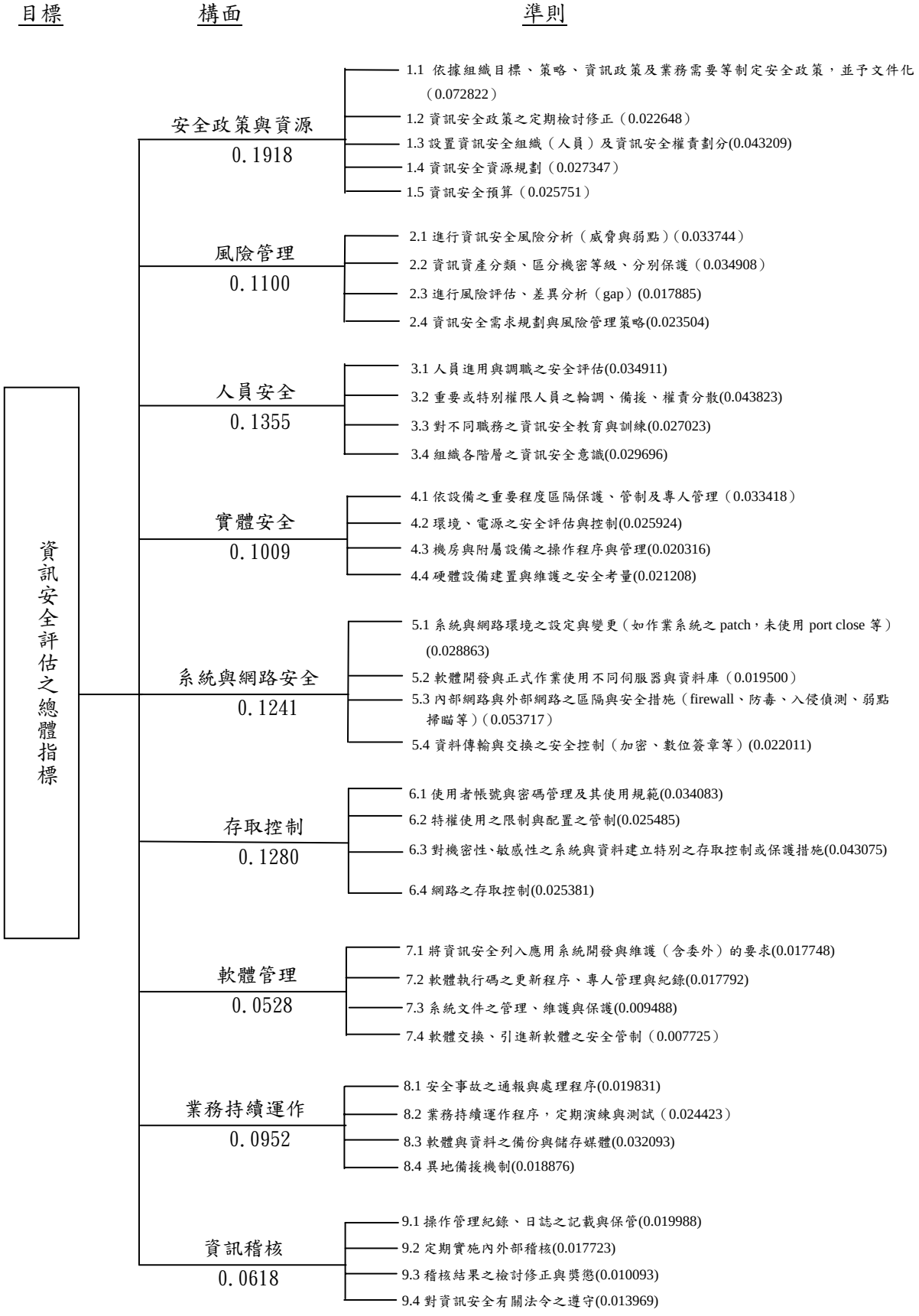

圖 6　資訊安全多準則評估模式（三階層）（資料來源：本研究）

2. 四階層之多準則評估模式，其評估構面分爲兩層級，主要理由係較符合本研究所依據的「整合系統理論」(Integrated System Theory)，且層級結構清楚。其評估構面第一層共分爲四個：安全政策與資源（0.1918）、風險管理（0.1100）、內部控制（0.6364）、資訊稽核（0.0618），其中內部控制之下一階層，爲評估構面之第二層級，共分爲六個：人員安全（0.1355）、實體安全（0.1009）、系統與網路（0.1241）、存取控制（0.1280）、軟體管理（0.0528）、業務持續運作（0.0952），如圖7所示。其最底層評估準則亦分爲37項及其權重等，均與三階層之多準則評估模式相同。第一層評估構面的權重，以內部控制最高（0.6238），而從文獻探討或理論的分析，均可知內部控制是受到各家理論的重視。再者資訊安全的威脅75％至80％來自組織內部（林傳敏，2000；Van Duyn, 1985），因此內部控制被認爲係解決資訊安全重要的策略，而本研究在分析理論時亦說明，內部控制受到各家理論所重視，係組織達成資訊安全目標的重要手段，足見與本研究所評估之權重爲各評估構面最高者，自是不謀而合。

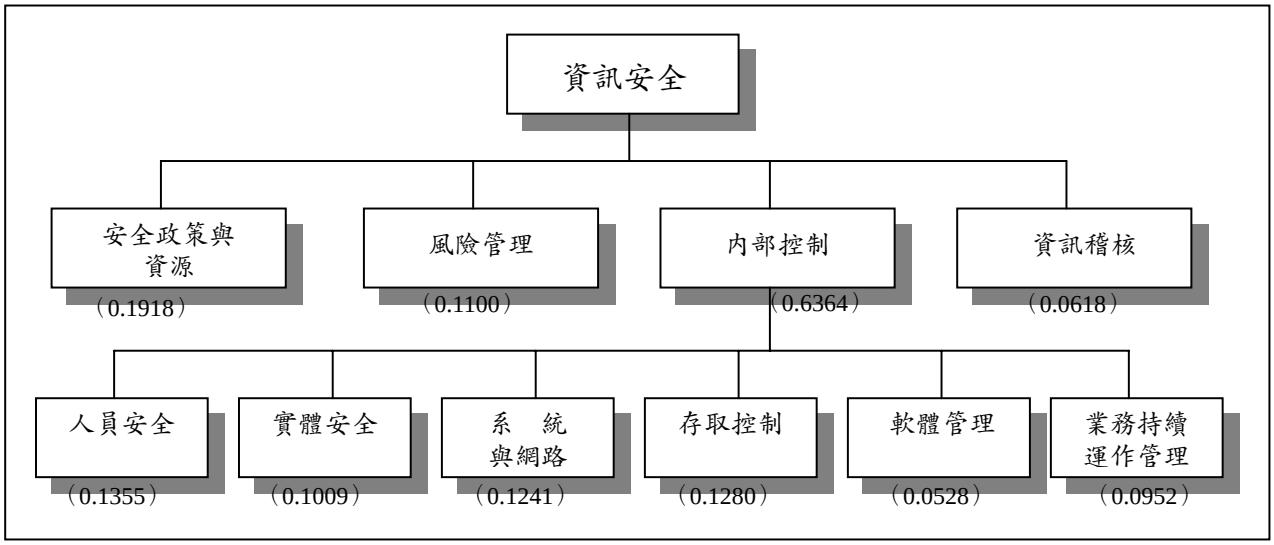

圖 7　資訊安全多準則評估模式（四階層）（資料來源：本研究）

資訊安全多準則評估模式雖有三階層與四階層之分，但實質內涵應屬相同，如以四階層表達係爲顧慮權重評估時，恐「內部控制」之權重可能有被低估之虞，故以三階層表達，但以四階層表達則較符合「整合系統理論」所發展的研究架構。在研究階段經徵詢學者專家意見，在兼顧權重評估的眞實性與符合理論基礎的考量下，一致主張區分三階層與四階層兩模式，對模式的表達更清楚，又無礙於模式之應用。因此，可在「資訊安全多準則評估模式」的建立過程中，使用三階層架構，以簡化評估構面與評估準則權重的評估，避免「內部控制」評估構面之權重可能被低估；而當權重評估完成，其評估模式建立後，應再依「整合系統理論」轉化成四階層架構，從「整合系統理論」觀點加以解釋，以使研究理論與實證研究得以兼疇並顧。

5.3 捷運等個案之資訊安全評估

本研究的主要目的在建構「資訊安全多準則評估模式」，並以此模式進行捷運等六個案之資訊安全評估。其個案係我國軌道車輛有關的組織，亦即捷運相關的組織，包括：政府機關、公營企業、民營企業；有的負責工程建設，有的負責營運，有的先負責工程建設，俟完工後，又負責營運，可說國內主要軌道相關的組織均已涵蓋在內。其軌道車輛之工程建設規模龐大，工程經費達數新台幣數千億元，其營運更負起台灣主要長程陸路運輸，或都會區主要大眾運輸之重任，對國計民生均有極大的影響，其資訊安全能否具體落實，將直接影響到該組織的

營運，也間接影響到社會大眾「行」的便利，因此，「資訊安全」難謂其不重要，這是選擇以作爲個案研究的主要理由。由於資訊安全評估結果公開有其敏感性，避免因而爲該等組織帶來困擾，因此，不公開其組織名稱，其基本資料如表 3 所示。

表 3　捷運等個案之基本資料

背景資料	個案 A	個案 B	個案 C	個案 D	個案 E	個案 F
員工人數	347 人	1600 人	1700 人	3016 人	141 人	14842 人
應用資訊系統的歷史	9 年	5 年	16 年	7 年	10 年	31 年
資訊部門設置時間	6 年	4 年	16 年	11 年	9 年	31 年
資訊部門層級	一級單位	一級單位	一級單位	一級單位	一級單位	二級單位
資訊人員人數	7 人	35 人	35 人	70 人	9 人	58 人
主要資訊科技架構與平台	分散式	非集中式 分散式 網路式	網路式	非集中式 分散式	非集中式 分散式 網路式	集中式
網際網路連線	已建置	已建置	已建置	已建置	已建置	已建置

資料來源：本研究

其評估步驟爲：

1.設計資訊安全評估表，將評估構面或評估準則之權重列入表中。

2.評分，評分方式可分爲直接評分與成對比較評分。

（1）直接評分法（黃智偉，2000；陳重光，2001），其評分標準爲：

傑出（Outstanding）86-100

滿意（Satisfactory）71-85

需改善（Needs Improvement）41-70

重大缺陷（Significant Deficiency）21-40

完全沒有（No System）0-20

（2）成對比較評分法，即按層級分析法（AHP）之兩兩比較方式，評估相對權重，亦即將兩個個案之某評估構面或評估準則兩兩比較，評估其權重，作爲評分（Saaty, 1980；刀根薰，1993）。

3.計算個案評估構面或評估準則之加權分。

4.計算個案各評估構面或評估準則之加權總分。

5.依據加權總分評定等級，其等級範圍如表4所示。

表 4　資訊安全評估等級表

等級	加權總分	等級細分範圍		代表意義
		＋	－	
A	86-100	>96	<90	A、A+：安全極佳 A-：安全佳
B	71-85	>80	<75	B+：安全普通 B　：安全尚可 B-：安全待改善
C	41-70	>60	<50	安全有缺陷
D	21-40	>33	<27	安全頗爲嚴重
E	0-20	>13	<7	安全極度嚴重

資料來源：本研究

由於成對比較評分之加權總分之高低會隨個案之多寡產生變化，當個案少時，每一個案之加權總分較高，當個案多時，每一個案之加權總分較低，因全部個案之加權總分之和爲 1，因此，無法訂定一個可以適用於不同個案數的等級評估標準，但得視個案數確定後，訂定其標準，唯仍有可能欠客觀。如每次評估，其個案數均固定，則可訂定其等級評估標準，否則以採用直接評分法爲宜。因爲層級分析法（AHP），其主要功能在排序，以挑選最佳方案或個案，而非評估等級。因此，若欲評估等級，則宜採直接評分法；若係對方案或個案之優劣排序，選取最佳方案或個案，則直接評分法與成對評分法均無不可。

由於個案評估資料取得不易，且無資訊安全評估之權力，爲簡化起見，本研究採資訊安全評估構面，以直接評分法進行評估。經上述步驟評估結果如表 5 所示。

表 5 資訊安全評估表

評估模式		個案 A		個案 B		個案 C		個案 D		個案 E		個案 F	
評估構面	權重	評分	加權分	評分	加權分	評分	加權分	評分	加權分	評分	加權分	評分	加權分
1 安全政策與資源	0.1918	88	16.88	94	18.03	90	17.26	96	18.41	85	16.30	87	16.69
2 風險管理	0.1100	85	9.35	93	10.23	75	8.25	94	10.34	20	2.20	50	5.50
3 人員安全	0.1355	85	11.52	92	12.47	89	12.06	89	12.06	60	8.13	88	11.92
4 實體安全	0.1009	88	8.88	94	9.48	94	9.48	95	9.59	80	8.07	93	9.38
5 系統與網路	0.1241	95	11.79	94	11.67	95	11.79	95	11.79	86	10.67	70	8.69
6 存取控制	0.1280	90	11.52	93	11.90	88	11.26	88	11.26	86	11.01	88	11.26
7 軟體管理	0.0528	93	4.91	94	4.96	93	4.91	92	4.86	50	2.64	75	3.96
8 業務持續運作	0.0952	88	8.38	90	8.57	93	8.85	90	8.57	88	8.38	89	8.47
9 資訊稽核	0.0618	89	5.50	95	5.87	88	5.44	92	5.69	87	5.38	87	5.38
加權總分		88.730		93.180		89.300		92.570		72.780		81.250	
序位		**4**		**1**		**3**		**2**		**6**		**5**	
等級		**A-**		**A**		**A-**		**A**		**B-**		**B+**	

資料來源：本研究

六個研究個案之加權總分最高之個案 B 與最低之個案 E，相差達 20.4，距離頗大，顯示組織「資訊安全」之個別差異甚大，列爲等級 A 的個案 B 與個案 D，亦即序位分別列第 1 與 2 者，兩組織均爲公民營企業，而其各個評估構面的評分均甚高，尤其個案 B 評分均在 90 分以上，高低分相差只有 5 分；個案 D 評分均在 88 分以上，高低分相差 8 分，顯示，欲達到較高的資訊安全水準，對於資訊安全各個構面均應加以重視。列爲等級 B-的個案 E，亦即序位爲第 6 者，係一政府機關，其評分最低的評估構面爲「風險管理」，僅評爲 20 分，其餘政府機關的個案 A 與 C，其「風險管理」，也分別爲該個案評分最低的評估構面，顯示政府機關的個案對「風險管理」似較未能受到重視，至少，重視程度不如公民營企業的個案，而個案 E 評分高低相差達 68 分，個案 F 高低相差達 43 分，而且個案 E 與個案 F 均以「風險管理」評分爲最低，而其與「資訊安全多準則評估模式」中，「風險管理」評估構面的權重之排序爲第 5 名的重要程度（如表 3、表 4 所示）相較，顯示「風險管理」未受到應有的重視。因此，當組織資訊安全資源無法照顧到全部的安全構面或評估準則時，應將資訊安全資源重點投資於其權重較高，即排序在前者，才能使資訊安全資源發揮最大的效用，以較少的投資獲得相對較多的資訊安全，換言之，組織可將「資訊安全多準則評估模式」運用在資訊安全資源的規劃、分配及建置之策略上，如此將會爲組織帶來更好的資訊安全效果。

六、結論與建議

6.1　結論

就多準則評估模式之研究而言：其目的在發展資訊安全評估之多準則決策（Multiple Criteria Decision of Information Security Evaluation）體系，經實證研究結果：

1. 發展「資訊安全評估總體指標」之層級結構，建立九大評估構面；包括：「安全政策與資源」、「風險管理」、「人員安全」、「實體安全」、「系統與網路」、「存取控制」、「軟體管理」、「業務持續運作」、「資訊稽核」等。下一層之評估準則共37項。
2. 對資訊安全評估構面權重之評估，其重要程度依序爲：「安全政策與資源」、「人員安全」、「存取控制」、「系統與網路」、「風險管理」、「實體安全」、「業務持續運作」、「資訊稽核」、「軟體管理」等。
3. 全部評估準則不分評估構面之權重，經全體專家對全部37項評估準則之評估，其權重高低之排序前十名依序爲：「1.1依據組織目標、策略、資訊政策及業務需要等制定安全政策，並予文件化」、「5.3內部網路與外部網路之區隔與安全措施（firewall、防毒、入侵偵測、弱點掃瞄等）」、「3.2重要或特別權限人員之輪調、備援、權責分散」、「1.3設置資訊安全組織（人員）及資訊安全權責劃分」、「6.3對機密性、敏感性之系統與資料建立特別之存取控制或保護措施」、「3.1人員進用與調職之安全評估」、「2.2資訊資產分類、區分機密等級、分別保護」、「6.1使用者帳號與密碼管理，及其使用規範」、「2.1進行資訊安全風險分析（威脅與弱點）」、「4.1依設備之重要程度區隔保護、管制及專人管理」等。
4. 將「資訊安全多準則評估模式」應用於研究個案之資訊安全評估，其評分方法可區分爲直接評分與成對比較評分，爲簡化起見，採資訊安全評估模式第二層之評估構面，以直接評估法進行評估，其中個案Ｂ的序位最高，各構面加權分之排序與評估模式之排序完全相同，顯見評估模式具有標竿作用。

6.2　建議

1. 對評估準則的建立，可否採用專家訪問法，或德菲法（Delphic），亦是未來可進行的研究。
2. 多準則評估的方法甚多，對於資訊安全評估，亦可採用其他的評估方法，如德菲層級分析法（Delphic Hierarchy Process）、等級固有向量法（Graded Eigenvector Method）、幾何最小平方法（Geometric Least Square）或直接加權法等，對層級分析法（AHP）亦可改採模糊積分法，以建構更切合需要的資訊安全多準則評估模式。
3. 個案研究可以提供研究結果的印証，因此，在個案的選擇上可以按不同性質選取，甚至若能找到適當的個案，以一個單一的個案作深入而具體的研究，相信亦具有極高的研究價值與貢獻。
4. 就實務探討所發展的命題，對於學術研究或實務上制定決策（Decision Making）均有其重要意義，值得未來進行後續的實證研究，將可累積更大的貢獻。
5. 本文各項研究的結果，均可作爲組織對資訊安全規劃與建置策略之參考。對一個新的組織，可按「整合系統理論」之循序程序，進行規劃與建置；而對於一有歷史的組織，已有部分的資訊安全建設時，整合性的規劃可能是必要的途徑；但無論任何組織當發生嚴重的資訊安全事故，或組織之資訊技術環境有重大變革時，應採取權變管理，速謀因應對策。在建置過程中，可依本研究所建構之「資訊安全多準則評估模式」中之評估構面或評估準則，按其權重高低，依序規劃建置，換言之，本文各評估構面或評估準則之權

重表所列之排序均可作爲規劃建置的順序，當組織資訊安全資源未盡充裕時，可集中少數安全資源，以建置最重要的部分，亦即選擇權重較高或排序在前的評估構面或評估準則建置之，將可獲得較高的成本效益。

6.3 結語

捷運工程之規劃在國內已有數十年的歷史，台北都會區的捷運工程建設計畫，自民國七十五年開始推動，迄今也將近二十年，身負其規劃、設計、施工，並籌辦營運等重責大任的台北市政府捷運工程局，已累積了無數的專業知識與經驗，這些極爲珍貴的智慧資產（Intelligent Capital）應予有效的利用。其中資訊技術（Information Technology）在整個捷運建設中扮演著極爲重要的角色，如：資訊系統開發與管理，系統整合，工程管理資訊應用，足爲國內的典範。資訊安全在捷運建設的初期即受到重視，IT 的內部控制與管理制度已行之有年，具有深厚的基礎。

本文所研究之資訊安全多準則評估模式，除了可作爲捷運等相關組織制定資訊安全策略的參考之外，也可在豐富的捷運建設智慧資產上錦上添花。

【本文感謝台北捷運工程局技術發展處丁立邁處長審查】

參考文獻

1. 刀根薰著（1993），陳名揚譯，競賽式決策制定法－AHP 入門，建宏書局。
2. 方溪泉（1994），AHP 與 AHP 實例應用比較－以高架橋下使用方案評估爲例，國立中興大學都市計劃研究所碩士論文。
3. 王國明、顧志遠與洪振創（1998），服務業績效評估模式建立理論與應用研究，國家科學委員會專題研究計畫成果報告（NSC87-2213-E-155-006）。
4. 吳琮璠（1996），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，PP.21-40。
5. 吳瑞明（1994），系統安全問題與防護措施，資訊與教育，40 期。
6. 宋振華、楊子劍（2001），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，PP.114-125。
7. 李東峰、林子銘（2001），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。
8. 杜鴻業（1998），台灣地區企業採用 Intranet 的評估因素與應用模式之研究，國立交通大學管理科學研究所碩士論文。
9. 周冠中（1995），外包決策評估模式之研究，以金融產業資訊系統爲例，國立政治大學資訊管理研究所碩士論文。
10. 林傳敏（2000），電腦稽核－網路世代不能沒有電腦稽核觀念（上、下），企銀報導，第 199、200 期。
11. 林鈴玉（2001），國內網路銀行現況發展及交易安全之研究，國立交通大學管理學院（資訊管理學程）碩士論文。
12. 施穎偉（2000），電子商務環境供應鍊供需互動模式之研究，國立政治大學資訊管理學系博士論文。
13. 洪國興（2003），資訊安全「影響因素與評估模式」之研究，國立政治大學資訊管理學系博士論文。
14. 洪國興、趙榮耀（2003），資訊安全管理理論之探討，資管評論，第十二期，PP.17-47。
15. 唐印星（1999），採購績效衡量關鍵因素之研究－以台灣電子汽車、鋼鐵、機械等產業

爲例，國立雲林科技大學工業工程與管理研究所碩士論文。
16. 翁俊興（1983），分析層級程序應用在投資計劃評估之研究，國立政治大學企業管理研究所碩士論文。
17. 國家安全局（2000），建立我國通資訊基礎建設安全機制研究報告書（本文），國家安全局。
18. 陳同孝（1996），資訊安全中道德教育問題之研究，勤益學報，13 期。
19. 陳彥學（2000），資訊安全理論與實務，文魁資訊公司。
20. 陳重光（2001），考量網路經濟特性下影響台灣地區商業銀行分行設立地點區位因素研究，雲林科技大學工業工程與管理研究所碩士論文。
21. 黃承聖（2000），企業資訊安全的起點－資訊安全政策，網路通訊，8 月。
22. 黃智偉（2000），供應鍊管理下供應商選擇評估之研究－以台灣地區中衛體系之汽機車業與電腦資訊業爲例，國立雲林科技大學工業工程與管理研究所碩士論文。
23. 葉牧青（1989），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。
24. 劉永森（1991），層級分析法（AHP）中機率性判斷之研究，國立中山大學資訊管理研究所碩士論文。
25. 劉國昌、劉國興（2001），資訊安全，儒林出版社。
26. 樊國楨、方仁威與徐士坦（2001），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，PP.1-52。
27. 樊國楨、時崇德（2000），一般認同系統安全原則與通資系統的永續經營計畫初探，建立我國通資訊基礎建設安全機制研究報告書（參考資料），國家安全局，PP.256-300。
28. 鄭信一（1999），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。
29. 鄧振源（2002），計畫評估方法與應用，海洋大學運籌規劃與管理研究中心。
30. 鄧振源、曾國雄（1989），層級分析法（AHP）的內涵特性與應用（下），中國統計學報，第 27 卷，第 7 期，PP 13767-13786。
31. 盧彥旭（2001），資訊系統委外選商評選準則及權重之建立，世新大學資訊管理學系碩士論文。
32. 賴溪松、葉育斌（2001），資訊安全入門，全華科技圖書公司。
33. 謝育文（1985），分析層級程序法（AHP）應用在我國個人電腦用印表機開發之研究，國立台灣商學研究所碩士論文。
34. 謝玲芬（1989），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。
35. 謝清佳、吳琮璠（1999），資訊管理－理論與實務，資訊管理智勝文化事業。
36. 闕頌廉（1994），應用模糊數學，3 版，科技圖書公司，PP.143-67。
37. Anderson, J. M. (2003), Why we Need a New Definition of Information Security, Computers & Security, Vol.22, No.4, PP.308-313.
38. Chapman, D. B. & Zwicky, E. D. (1995), Building Internet Firewalls, O'Reilly & Associates.
39. David, C. & Rivett, B. H. P. (1978), A Structural Mapping Approach to Complex Decision Making, Journal of Operational Society, Vol.29, No.2, PP.113-128.
40. Dhillon, G. & Backhouse, J. (2000), Information System Security Management in the New Millennium, Communication of the ACM, Vol.43, No.7, July 2000, PP.125-128.
41. Ellison, R. J. etal. (1999), Survivable Network System Analysis : A Case Study, IEEE Software, PP.70-77.

42. Ettinger, J. E. (1993), Key Issues in Information Security, Information Security, Chapman & Hall, London, PP.1-10.
43. Finne, T. (2000), Information Systems Risk Management : Key Concepts and Business Processes, Computers & Security, Vol.19, No.3, PP.234-242.
44. Gehrke, M. , Pfitzmann, A. & Rannenberg, K. (1992), Information Technology Security Evaluation Criteria (ITSEC)-A Contribution to Vulnerability?, INFORMATION PROCESSING 92-Proc. IFIP 12th World Computer Congress Madrld, Spain, Sept, PP.7-11.
45. Hinde, S. (2003) The law, Cybercrime, Risk Assessment and Cyber Protection, Computer & Security, Vol.22, No.2, PP.90-95.
46. Hong, K.S., Chi, Y.P., Chao, L.R. & Tang, J.H. (2003), An Integrated System Theory of Information Security Management, Information Management & Computer Security, Vol ,11,No.5,PP.243-248.
47. Huber, G.P. (1980), Managerial Decision Making, Scott Foresman and Company.
48. Hwang, C.L. & Lin, M.J. (1987), Group Decision Making Under Multiple Criteria : Methods and Application, Lecture Notes in Economics and Mathematical Systems 281.
49. ISO / IEC 17799 (2000), Information technology-code of practice for information security management.
50. Panda, B. & Giordano, J. (1999), Defensive Information Warfare, Communications of the ACM, Vol.42, No.7, PP.31-32.
51. Rackham, L. F. & Richard, R. (1995), Getting Partnering Right : How Market Leaders Are Creating Long-term Competitive Advantage, by McGraw-Hill Int'l Enterprises Inc.
52. Saaty, T. L. (1980), The Analytic Hierarchical Process, New York : McGraw-Hill.
53. Saaty, T. L. & Bennett, J. P. (1977), A Theory of Analytical Hierarchies Applied to Political Candidacy, Behavioral Science, 22, PP.237-245.
54. Saaty, T. L. & Vargas, L.G. (1980), Hierarchical Analysis of Behavior in Competition : Prediction in Chess, Behavioral Science, 25, PP.180-191.
55. Saaty, T. L. & Vargas, L.G. (1982), The Logic of Priorities, Boston : Kluwer- Nijhoff.
56. Schneider, E. C. & Gregory, W. T. (1990), How Secure Are Your System? Avenues to Automation, Nov.
57. Schultz, E. E., Proctor, R. W., Lien, M. C. & Salvendy, G. (2001), Usability and Security An Appraisal of Usability Issues in Information Security Methods, Computer & Security, Vol.20, No.7, PP.620-634.
58. Smith, M. (1989), Computer Security-Threats, Vulnerabilities and Countermeasures, Information Age, October, PP.205-210.
59. Van Duyn, J. (1985), The Human Factor in Computer Crime, Petrocelli Books, Inc., Princeton, NJ.