資訊安全管理理論之探討

A Study of Theory for Information Security Management

洪國興
Kwo-Shing Hong
監察院綜合規劃室
Overall Planning Department
Control Yuan

趙榮耀
Dr. Louis R. Chao
淡江大學管理科學研究所
Institute of Management Science,
Tamkang University

摘　要

由於資訊科技的快速進步，組織對資訊科技的依賴日深，尤其網際網路所建構的電子商務時代，組織之資訊系統的使用者，已由組織內部的人員，擴大到組織外部任何不特定的個人，使得組織的資訊安全面臨空前的挑戰，因此，資訊安全的管理與技術，亦受到研究者與實務界普遍的重視，然而「資訊安全管理」尚缺乏一貫的理論架構。本文試圖經由資訊安全管理文獻的探討與實務面的觀察，就當今組織資訊安全管理的現象歸納為：安全政策理論、風險管理理論、控制與稽核理論、管理系統理論、及權變理論等，再就這些理論衍生整合成為另一新的資訊安全管理理論，亦即建構為資訊安全管理之「整合系統理論」。資訊安全管理理論的提出將有助於後續的研究者與實務界人士，藉以了解資訊安全管理的現象，解釋資訊安全管理策略，及預測投入資訊安全管理策略與方法，預期可能的結果，並對後續的研究提供研究方向與理論基礎。

關鍵字：資訊安全、安全政策理論、風險管理理論、控制與稽核理論、整合系統理論

Abstract

With the rapid advancement of information technology, organizations put dependence on it more than ever. Especially in the era of electronic commerce, users of a certain organization's Internet system broaden from members inside to unknown individuals outside. Many organizations are facing unprecedented security challenges. Therefore, information security techniques and management tools have caught a lot of attention from both academia and practitioners. However, there is lacking a theoretical framework for information security management. This paper, through literature review and practical observations, attempts to summarize and integrate five existing theories: security policy theory, risk management theory, control and auditing theory, management system theory and contingency theory to build a comprehensive theory of information security management (ISM). It suggests that an Integrated System Theory (IST) is useful for understanding information security management, explaining information security management strategies, and predicting possible outcomes while applying those strategies. This theory may lay a solid theoretical foundation for further empirical researches and applications.

Keywords : Information Security, Information Policy Theory, Risk Management Theory, Control and Auditing Theory, Integrated System Theory

壹、緒論

「資訊」(Information)是企業的重要資產之一，對組織而言，是具有價值的，因此，必須適切的加以保護(ISO/IEC17799, 2000)。「安全」(Security)是指結合系統、運用及內部控制，來確保資料及作業程序的完整、真實及隱密（洪祥洋，2000)。

由於資訊科技的快速進步，從 60 年代的集中式大型主機（Central Mainframe Computers)，70 年代中期以後的個人電腦、部門運算(Departmental Computing)、區域網路（Local Area Networks)，到 90 年代的主從式（Client-Server)、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，也從只侷限於組織內部的資訊技術人員的存取資訊設施（Access Information Facilities)，漸漸增加到組織內部的非資訊技術人員，也需要存取資訊設施，進而擴大到跨組織的電子交易，連結不同平台的資訊設施，使用者也隨之擴大到組織外部不特定的個人。隨著資訊新科技的快速發展，使用者範圍不斷的擴大，組織對資訊系統依賴程度的提高，使得資訊安全面臨更大的挑戰(Von Solms, 1996；Schultz 等，2001；李東峰與林子銘，2001；林震岩，1996；Loch 等，1992)。

換言之，資訊安全的日愈重要，係由於資訊系統的環境大幅度的改變，在網際網路的環境中，隨時都有爲數可觀來自世界各地的非授權使用者，可能去存取或變更組織的資訊，使組織的資訊系統面臨空前的威脅；因此，資訊安全也是當今任何組織爲達成有效管理的重要關鍵之一，資訊安全也成爲每一個組織的核心業務之一（Schultz 等，2001；Eloff & Von Solms, 2000a；Trček, 2003)。

美國的 911 事件，台灣的汐止東科大樓火災等一連串大型災害發生後，確實使各界掀起對資訊安全的更加重視，組織希望藉助過去研究的結果，以作爲制定資訊安全策略的參考，但結果似無法令人滿意，其現象是：(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)。

以上的現象，顯然與資訊安全管理領域缺乏一貫性的理論有關（黃慶堂，

1999)，使得無法像資訊管理其他領域或資訊系統的研究同樣的蓬勃發展，可在既有的理論基礎上進行研究(Zmud & Boynton, 1991)，也爲實務界提供管理策略的重要來源之一。對研究者而言，理論基礎可以將前人研究所累積的知識進一步整合與連結，以發展更成熟的理論，亦可提供研究構面（Key Constructs）及構面間關係的來源，以探究其現象（Phenomenon），並提供研究之概念架構（Conceptual Framework），供作者發展其心智模式（Mental Model）等，均足以顯示理論對研究的重要性（Zmud, 1995）。

本文的目的希望對當前資訊安全管理的現象，經由文獻的探討，實務面的了解與觀察，加以整理歸納成爲資訊安全管理理論，並進而建構新的資訊安全管理理論，以有助於未來資訊安全管理的研究與實務運用，對於了解、解釋、預測資訊安全管理活動提供幫助，並爲未來的研究者提供研究方向與理論基礎，且能爲實務運用提供資訊安全管理的選擇方案。

本文先對資訊安全管理之背景加以說明，再探討理論的意義（Definition of Theory）、理論的構成（Components of Theory）及理論的功能（Functions of Theory)；進而歸納整理資訊安全管理五種理論，再將這些理論整合後，建構整合系統理論（Integrated System Theory），最後作成結論，並對未來的研究者或實務應用者提出建議。

貳、文獻探討

本研究先從文獻中瞭解資訊安全，從其定義、架構及範疇等三方面來探討資訊安全。

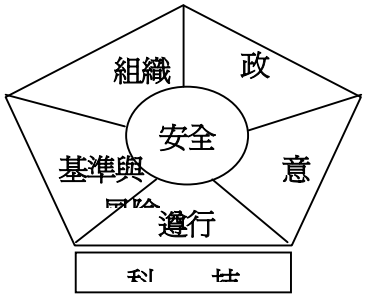
一、資訊安全定義

電腦安全的定義：電腦安全在處理電腦系統的使用者之非授權行爲的預防與發現（Gollmann, 1999）。

任何電腦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；吳瑞明，1994；陳同孝，1996；林鈴玉，2001；Ettinger, 1993；Anderson, 2003)；具體而言，三者所欲達成的目標分別爲：

1. 機密性：確保「資訊」只能被經過授權的人，才能存取。
2. 完整性：保證「資訊」和其「處理方法」的準確性與完整性。
3. 可用性：確保經過授權的使用者，當需要時就能存取「資訊」，並使用相關「資訊資產」。

依賴電腦系統的使用者，其軟體運作的表現如其所預期，則該系統即可稱之爲



圖一 資訊安全架構圖（資料來源：Tudor,

「安全」（Simson & Gene, 1991）。Von Solms 等（1994）認爲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。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（黃亮宇，1992；Rusell & Gangemi, 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，並使業務可能發生損失降至最低（ISO /IEC 17799, 2000）。

二、資訊安全架構

Tudor 指出：組織的資訊安全架構係由下列五個部分所組成（Tudor, 2001），如圖一所示：

（一）安全組織與基礎建設（Security Organization and Infrastructure）。
（二）安全政策、標準與程序（Security Policy, Standards, and Procedures）。
（三）安全基準與風險評估（Security Baselines and Risk Assessments）。
（四）安全意識與教育訓練（Security Awareness and Training Programs）。
（五）遵行（Compliance）。

（一）安全組織與基礎建設

資訊安全組織與基礎建設是資訊安全最基本的架構，對資訊安全管理之成敗，有極關鍵性的影響。

安全組織之層級及人力的配置，應視組織資訊與安全的環境而定，有設獨立之資訊安全部門者，或在職位上有設置 CISO（Chief Information Security Officer）、Security Officer、Security Coordinators / Liaisons 等，亦即視資訊安全管理之需要而定。在安全的基礎建設方面，首重資訊資源的分類（Classifying Information Resources），亦即按機密性（Confidentiality）、完整性（Integrity）與可用性（Availability）等加以區分。

（二）安全政策、標準與程序

安全政策係在表達企業所期望達成的安全政策目標。其內涵應包括：安全政策範圍、資訊安全責任分工，以及資訊安全政策之實踐的管理作爲。

安全標準係對資訊安全之作業與管理，所訂定的規則、程序或規定。標準有最低性與選擇性，亦即可以訂定最低需求，即低於此一標準將影響組織的資訊安全；亦可是選擇性，即按不同的企業特性，不同的產品與服務，不同的風險承擔能力，及成本的考量而有不同的選擇標準。

（三）安全基準與風險評估

安全風險評估，係在瞭解並評定組織資訊安全風險之高低，以作爲組織資訊安

全風險決策之依據。組織對於資訊安全計畫的控制通常係集中式，對於資訊安全的管理則通常係分散式，所以先要從中央組織對資訊安全計畫的機制，進而再逐步到企業每一項業務與管理。

（四）安全意識與教育訓練

建立資訊安全意識與教育訓練的目標，使組織成員認知其對企業資訊資產保護之責任，了解資訊資源的價值，潛在威脅在何處？

（五）遵行

資訊安全管理之遵行，包括組織內不同層次的稽核（Auditing）、監督（Monitoring）與調查（Investigating）等。

三、資訊安全管理範疇

有關資訊安全管理的文獻中，以 ISO / IEC 17799 及行政院參照 BS7799-1 制定的資訊安全管理規範，對資訊安全管理範疇的界定較爲完整，經整理如下（ISO/IEC 17799, 2000；行政院主計處電子處理資料中心, 2001；Sherwood, 1996；Eloff & Solms, 2000b；Tryfonas 等，2001；宋振華與楊子劍，2001；宋鎧等，2001）：

（一）資訊安全政策制定及評估

（二）資訊安全組織及權責

（三）人員安全管理及教育訓練

（四）系統安全管理

電腦系統作業程序及責任、系統規劃、電腦病毒及惡意軟體之防範與控制、軟體複製的控制、個人資料之保護、日常作業與媒體之安全管理、資料及軟體交換之安全管理。

（五）網路安全管理

網路安全規劃與管理、全球資訊網與電子郵件之安全管理、網路安全稽核、憑證機構之安全管理。

（六）系統存取控制

資訊系統存取控制與責任、網路存取之安全控制、電腦系統之存取控制、應用系統之存取控制、系統存取及應用之監督、組織外部人員存取資訊之安全管理、系統稽核規劃。

（七）系統發展及維護之安全管理

系統安全需求規劃、應用系統之安全、應用系統檔案之安全、系統變更及維護環境之安全。

（八）資訊資產之安全管理

（九）實體及環境安全管理

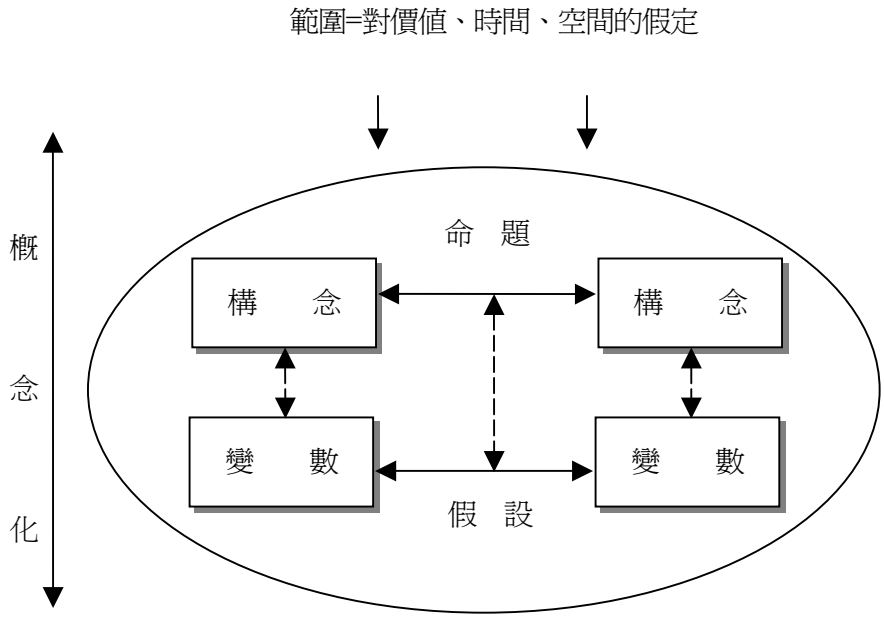
設備安全管理、周邊安全管理。

（十）業務持續運作之規劃及管理

業務持續運作之規劃、資訊安全事件緊急處理機制。

參、資訊安全管理理論之發展

理論是由構念（Constructs）和命題（Propositions）所構成。理論是一個構念與變數（Variables）的系統，構念是被賦予一組具體語意之有意義名詞，經由命題將兩個以上的構念連結關係；變數是賦予數值的符號，代表數量或數值的集合，經由假設（Hypotheses）將兩個以上的變數連結其關係（Bacharach,1989；張紹勳，2000）。



圖二　理論的構成（資料來源：Bacharach, 1989；Cheon 等，1995）

理論是一種有關的構念、定義（Definitions）、命題的組合，以設定變數之間的關係，用以表達現象的一種系統觀，其目的在解釋與預測現象（謝安田，1983；張紹勳，2000）。理論是一套概念，

以及這些概念間可能有的關係，是一種想要代表或模式化世界上某些事務的架構（高熏芳等，2001）。理論的構成如圖二所示（Bacharach, 1989；Cheon 等，1995）。

理論的功能，在於對有興趣的變數間之關係，達到預測與了解的目的（Dubin, 1976）。更具體而言，理論具有「了解」（Understanding）、「解釋」（Explanation）、「預測」（Prediction）與「指導」（Direction）的功能（Cozby, 1981；張紹勳，2000；謝安田，1983）：

1. 理論有助於「了解」現象，「了解」又有兩種情境：
   （1）預測性的了解、經濟主義的了解，係經由客觀「觀察」所獲得的了解。
   （2）同理心（Empathic）的了解、詮釋主義的了解。
2. 理論可用於「解釋」現象之間的關係。解釋的精確性（Accuracy）是衡量理論解釋能力的準則之一。
3. 理論可用來「預測」行爲。理論可描述「先前發生的事情（Antecedent）」與「結果（Consequences）」兩者之間的關係。
4. 理論可用於「指導研究」，使後繼的研究者，在既有的理論與研究的基礎上，獲得指導，繼續修正理論，建構理論，使知識能更進一步的累積。

理論模型作爲一種科學認識的成果，必須以特定的形式來表述。其表述方式有兩類：一類是借助語言、圖象、符號等工具的定性表述；另一類是借助於公式、圖表等工具的定量表述（張瓊等，1994）。本研究對於理論之表述，係使用言語、圖形與函數關係式等來表述。

策略管理係組織爲了達成期望的績效，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，更影響到資訊安全的實務層面有關資訊安全策略之擬定，顯見資訊安全理論之發展至爲重要。找尋理論的來源有二：其一是歸納法，從既有的研究上歸納整理，以持續的、累積的、有目的的來發展理論；其二是類推法，從其他相關領域的理論來發展研究模式（林東清與許孟祥，1997）。本研究經由資訊安全既有的文獻加以探討，並從實務面觀察，將資訊安全管理理論歸納整理，提出：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, CAT）、管理系統理論（Management System Theory, MST）、權變理論（Contingency Theory, CT）等五種資訊安全管理理論，就理論發展的途徑（Approach）而言，應屬前者的歸納法。

一、安全政策理論（Security Policy Theory,

SPT）

所謂「安全政策理論」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，以資訊安全政策爲核心，形成資訊安全管理循環，經由資訊安全政策之落實執行，來實現組織資訊安全之目標。

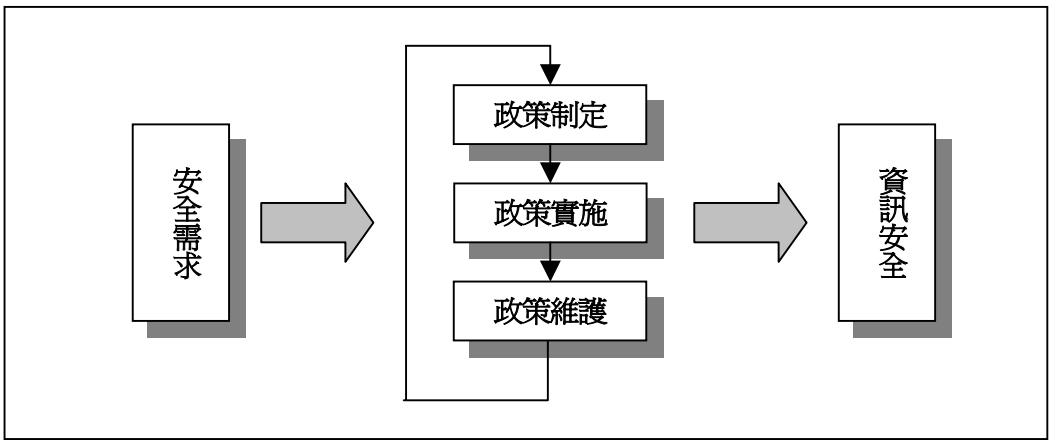
Kabay（1996）指出：資訊安全政策之制訂，應經由(1)評估與說服管理高層；（2）資訊安全需求分析；(3)形成政策與完成程序；(4）實施；(5）維護。黃承聖（2000）認爲資訊安全政策是一個管理循環，從制定、實施，到評估，是一種持續不斷的改善工作。從管理功能的觀點來看，資訊安全政策的管理循環是：規劃（Planning)、建置（Implementation）與維護（Maintenance）之循環。

資訊安全政策生命週期（Information Security Policy Life Cycle）分爲四大部分（1）評估（Assess)：政策評估（Policy Assessment）與風險評估（Risk Assessment)；(2）計畫（Plan)：政策發展（Policy Development）與需求定義（Requirement Definition）；(3）實施（Deliver）：控制之定義（Controls Definition）與控制之實施（Control Implementation)；(4）營運（Operate)：趨勢檢視與事件管理（Review Trends & Manage Events）、監督營運（Monitor Operations）(Gupta 等，2001)。

吳琮璠（2002）認爲制定資訊安全管理政策應：建立安全目標、資訊分級、評估安全風險、發展系統安全計畫、指派權責、進行測試、評估系統安全。Lindup（1995）提出資訊安全政策之發展與建置的步驟爲：(1）資訊安全政策之草擬與討論；(2）CEO 對資訊安全政策之承諾、核定與發布；(3）實施；(4）監督與稽核。

Flynn（2001）提出ｅ政策（ｅPolicy）的內涵，包括：全面性的資訊稽核（Comprehensive ｅ-Audit)、資訊安全風險管理政策（ｅ-Risk Management Policy)、電腦安全政策(Computer Security Policy)、電腦保險政策（Cyber Insurance Policy)、電子郵件政策（E-Mail Policy)、網際網路政策(Internet Policy)、軟體政策（Software Policy）等，經由資訊安全政策的文件化，強力說服員工，建立安全意識，以確保資訊安全規範的執行，並以管理高層的支持與承諾、資訊安全的教育訓練、資訊安全危機應變規劃、資訊安全政策的有效執行，及對資訊安全政策的不斷檢討修正等措施來確保組織的資訊安全。

資訊安全政策即在規劃資訊安全需求，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，而促進資訊安全的管理程序，示意如圖三所示。其資訊安全的決定則形成下列的函數關係：



圖三 資訊「安全政策理論」示意圖（資料來源:本研究）

資訊安全＝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）

所謂風險管理理論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），及估計其發生之可能性，再進行風險評估（Risk Assessment），以規劃組織資訊安全需求（Information Security Requirement），並據予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。

Wright（1999）指出：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）。風險管理的核心是風險評估（Risk Assessment），亦即經由對資訊安全風險的確認與評估，組織再據予實施適當的安全控制。其目的在確保資訊系統安全是否符合成本效益與組織的安全需求，以達成組織之目標。

Reid & Floyd（2001）提出所謂：「風險分析流程圖」（Risk Analysis Flow Chart），組織應先確認資訊資產所面臨之威脅與弱點爲何？兩者交互產生風險，組織的控制活動之目的在降低風險，使不利於資訊資產的保護活動降低至某一水準，水準以下即是剩餘風險（Residual Risk），

若決策者認爲剩餘風險的水準不能接受，即再增加控制措施，直到風險水準降低至決策者可以接受的水準，管理控制的制度即告確定。

樊國楨等（2001）亦提出：風險管理步驟，（1）風險分析（Risk Analysis）；（2）風險評估（Risk Assessment）；（3）改善計畫或管理控制（Improvement Plan or Management Control）；（4）控制績效審查（Review of Control Performance）；持續改善、週而復始，以達成降低風險、促進資訊安全的目的。風險係由威脅（Threats）、弱點（Vulnerabilities）與資產價值（Assets Value）所組成，因此，風險分析的內涵在分析組織所面臨的威脅與及存在的弱點，風險估計則在估計資產價值，及組織對資訊安全所造成的衝擊程度。

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管理程序，示意如圖四所示。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）

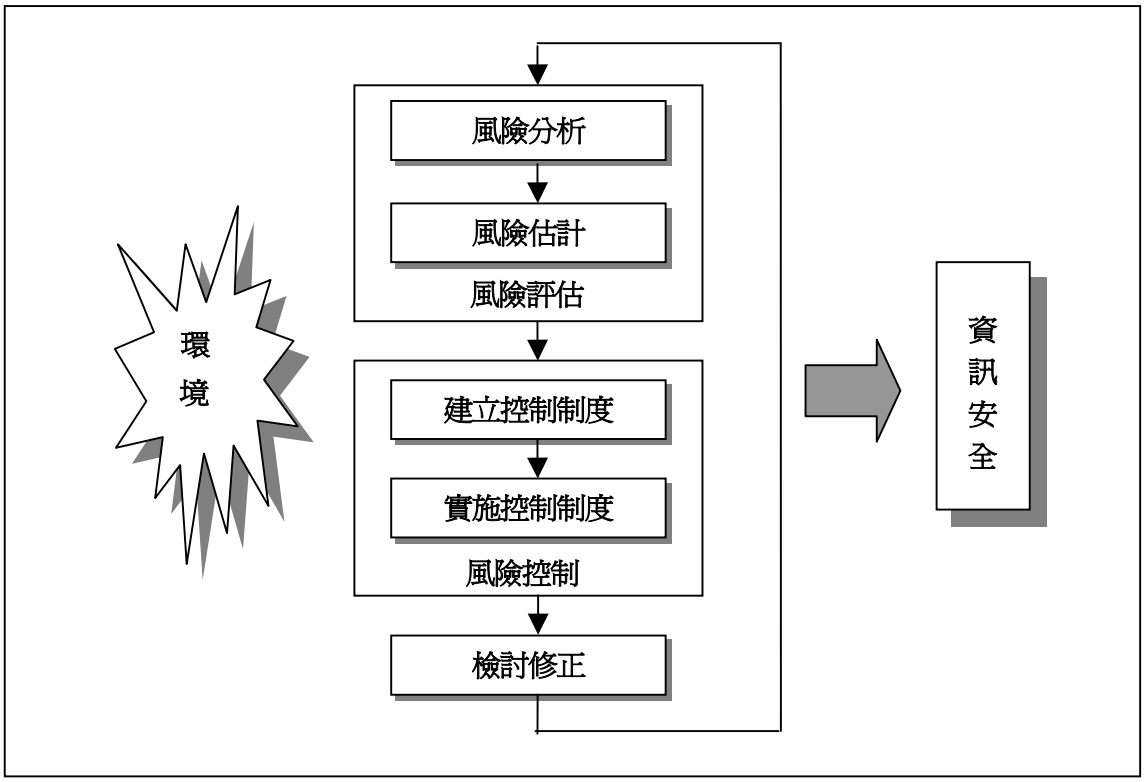
風險評估=f（風險分析，風險估計）

風險控制=f（建立控制制度，實施控制制度）

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

所謂：「控制與稽核」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。

Weber（1999）認爲「控制」（Control）是一種預防（Prevents）、偵測（Detects）與改正（Corrects）不法事件的系統；故控制方法有：預防性控制、偵測性控制與更正性控制。林勤經等（2001）認爲資訊安全的控管，考量的議題有：（1）多元系統的型態管理；（2）系統間通訊連結的建立與維護；（3）系統連結遭非法濫用的預防；（4）多層次與多點的資訊傳輸；（5）資料儲存與備援策略；（6）資訊安全防護技術的建置。



圖四 資訊安全「風險評估理論」示意圖（資料來源：本研究）

ISO/IEC 17799（2000）所規範的資訊安全管理有：（1）安全政策（Security Policy）；（2）安全組織（Security Organization）；（3）資訊資產分類與控制（Assets Classification and Control）；（4）人員安全（Personnel Security）；（5）實體及環境安全（Physical and Environment Security）；（6）通訊與操作安全（Communication and Operation Security）；（7）系統存取控制（System Access Control）；（8）系統開發及維護（System Development and Maintenance）；（9）業務持續運作規劃（Business Continuity Planning）；（10）遵行（Compliance）等十大管理要項，127種控制方法。

楊金炎（2001）提出資訊系統內部控制關係圖，其控制項目包括：（1）資訊部門之功能與職責劃分；（2）系統開發及程式修改控制;（3）編制系統文書之控制;（4）程式及資料存取之控制；（5）資料輸出入之控制；（6）資料處理之控制；（7）檔案及設備之安全控制；（8）硬體及系統軟體購置之控制；（9）系統復原計畫、制度及

測試程序之控制。

國際電腦稽核協會（ISACA）所提出的 COBIT（Control Objectives for Information and Related Technology）係參考兩種主要的內部控制模式所制定的資訊技術管理模式。其參考的內部控制模式爲「整體營運控制模式」及「專注於資訊技術控管模式」，因此，COBIT 係資訊管控的高層準則，而非技術準則，亦即對資訊技術資源，包括：資料、應用系統、技術、硬體設備、人員等，經由規劃與組織、取得與建置、交付與支援、監控等活動，藉由平衡風險、資訊技術與程序，以指導及控制組織達成目標（COBIT, 1998）。

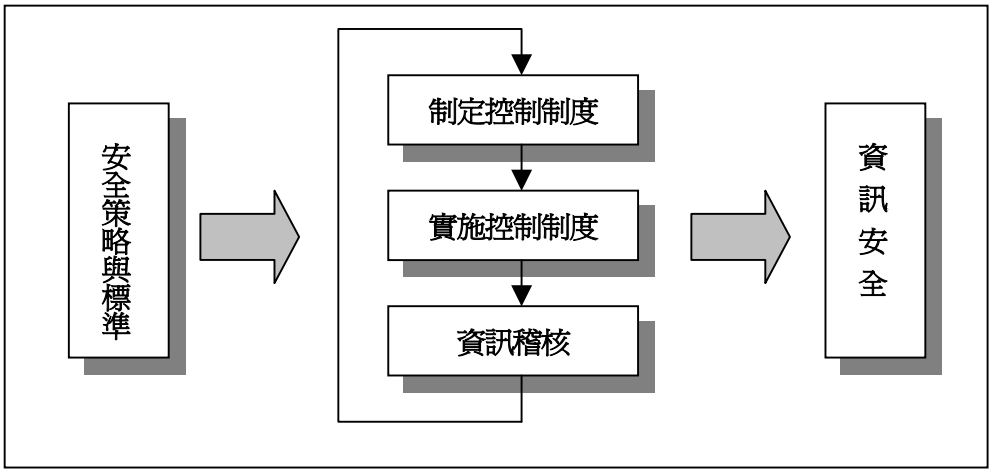
組織衡酌資訊安全策略，依據各種資訊安全標準，以制定資訊安全控制制度（Control System），嚴格執行並定期進行資訊稽核（Information Auditing），以評估控制制度執行成效，及資訊安全水準，據予修正其控制制度，交替運作，而確保資訊安全的管理程序，示意如圖五。其資訊安全的決定則形成下列的函數關係：

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）

所謂「管理系統理論」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），該系統應強調需要被保護的資訊系統資產，並採用風險管理方法、控制目標、控制方法、及所需要的安全保證程序。



圖五　資訊安全「控制與稽核理論」示意圖（資料來源:本研究）

ISMS 分爲六大步驟：（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，形成一個程序化的安全管理系統（BS7799-2；1999）。

Sherwood（1996）提出資訊安全政策架構，稱爲 SALSA（Sherwood Associated Limited Security Architecture），從組織需求與安全策略出發，建構資訊安全管理架構，分爲五層：（1）企業需求層（Business Requirements）；（2）主要安全策略層（Major Security Strategies）；（3）安全服務層（Security Service）；（4）安全機制層（Security Mechanisms）；（5） 安全產品與科技層（Security Products and Technologies），形成管理層級架構。

宋振華與楊子劍（2001）提出資訊安全體系流程：（1）現況調查訪談；（2）資訊安全檢測；（3）風險評估與管理；（4）資訊安全政策與作業程序；（5）教育訓練；（6）導入。

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，示意如附圖六。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）

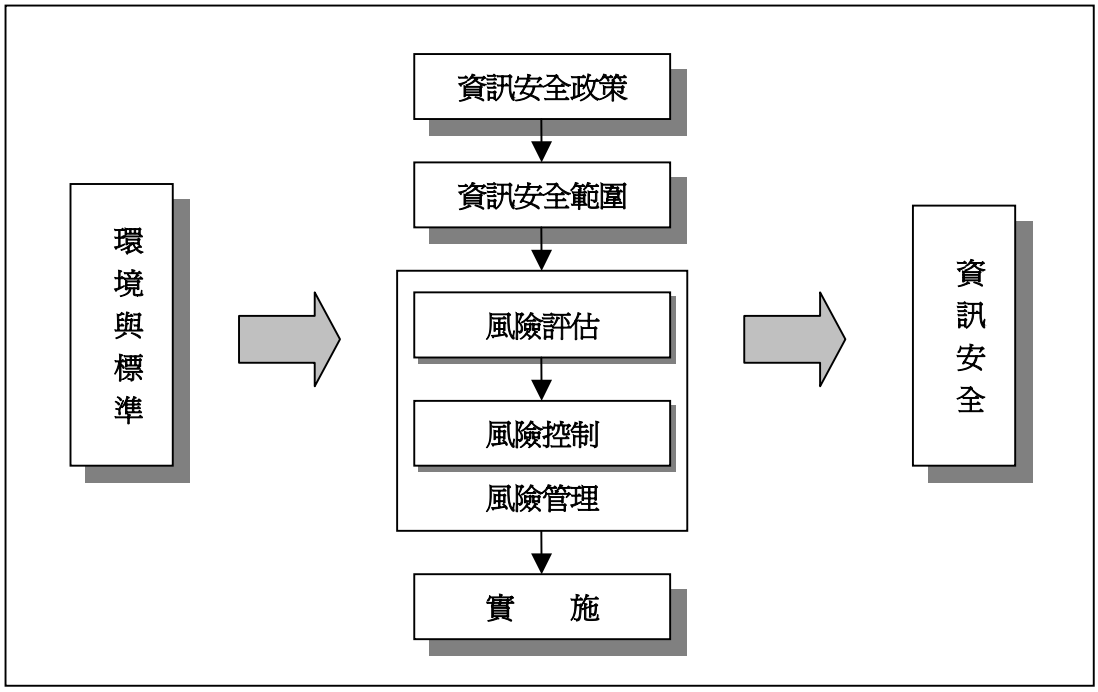
「權變理論」指：資訊安全係組織爲了預防（Prevention）、偵測（Detection）與反應（Reaction），組織內外之資訊安全威脅（Threats）、弱點（Vulnerabilities）與衝擊（Impacts）所採取之權變管理（Contingency Management）策略，亦即爲因應環境變化與組織的管理上需要，而採取政策導向（Policy Orientation）、風險管理導向（Risk Management Orientation）、控制與稽核導向（Control and Auditing Orientation）或管理系統導向（Management System Orientation）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

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，組織爲因應內外環境的快速變遷，常採行權變方式（Contingency Approach），以作爲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）。

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）提出資訊安全管理模式（Information Security Management Model, ISM），ISM 是由五個資訊安全水準所構成：理想水準（Ideal）、規範水準（Prescribed）、基線水準（Base Line）、現在水準（Current）與生存水準（Survival），依序形成層次的軸（Axis）。除了理想水準之外，其餘都是動態的（Dynamic），亦即組織的資訊安全水準高低的決定，應視組織的環境變數，亦即組織所面對的資訊安全威脅、弱點與衝擊，與管理及技術變數而定，其中亦隱含「權變」的概念。

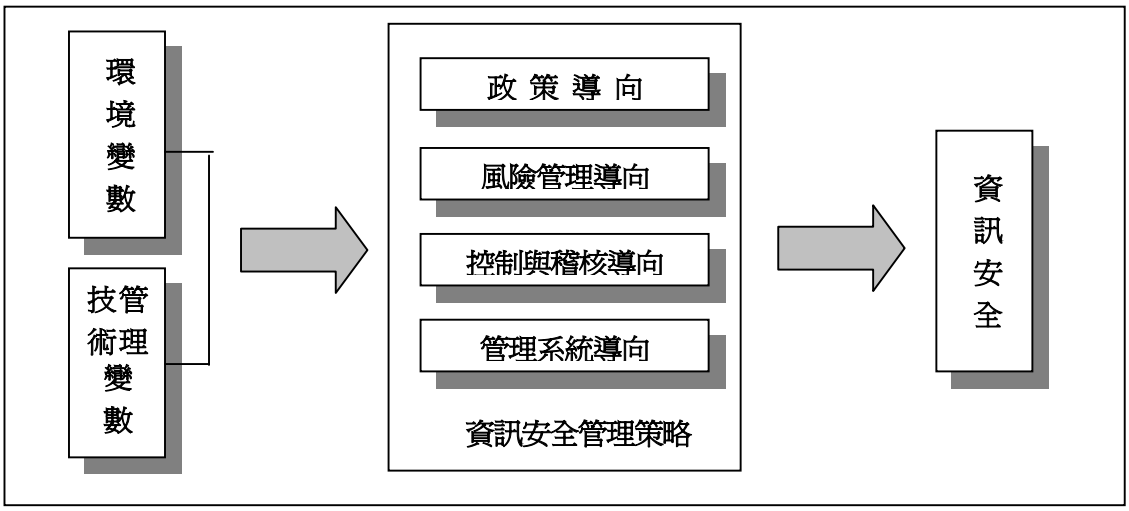


圖六　資訊安全「管理系統理論」示意圖（資料來源：本研究）

李東峰與林子銘（2001）提出：以風險策略、資訊策略、企業內外部環境及資訊架構等四項變數，用以規劃企業資訊安全管理，並制定資訊安全管理決策。其考量的環境變數是：風險策略與企業內外部環境；管理與技術的變數是：資訊策略與資訊架構，企圖找出兩組變數的互動關係。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）



圖七　資訊安全管理「權變理論」示意圖（資料來源：本研究）

組織在解決資訊安全問題並非是固定的程序，係視組織內外之資訊安全環境、資訊管理與技術等因素，而選擇政策導向（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）之資訊安全管理策略的一種權變管理（Contingency Management）程序，示意如圖七所示。其資訊安全的決定

權變管理=f（組織環境，管理，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	• 以資訊安全政策爲主要內涵，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，對環境的應變能力較低	Kabay（1996） 黃承聖（2000） Gupta 等（2001） Flynn（2001） 洪國興等（2003）
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了解與應變，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（2001）
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爲主要內涵，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） 林勤經等（2001） ISO/IEC 17799（2000） 楊金炎（2001） COBIT（1998） ISACA(2002)
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

肆、整合系統理論之建構

科學理論創造的一種基本傾向爲：摒除雜念，「靜觀萬物」，當觀察事實累積得足夠多時，客觀規律自然就會呈現。這種認爲純粹的觀察可以導致理論發現的信念，在方法論史上可以追溯近代實驗科學始祖，16 世紀英國哲學家培根（張瓊等，1994）。

理論的建構（Construction），顧名思義即是從無到有建立理論，理論建構是一種過程，它同時發展出觀念、構念及命題（Kaplan, 1964；張紹勳，2000）。建構理論模型是爲了給某些已知事實作出合乎情理的解釋，但解釋的過程是一個演繹過程，是把待解釋表示爲某種假想機制作用的必然結果；而理論模型的構思過程卻是一個逆繹的、溯因的過程，是爲一個已知的結論尋找其適當的邏輯前提。它要求研究者能深刻地領悟和洞察相關經驗事實的真正意義，並通過創造性的想像和聯想，將各類背景知識融會貫通，凝成爲新的概念和原理（張瓊等，1994）。理論模型的建構是一個典型的解題過程。從問題的提出（爲何事物遵循此種規律運行？）到最後解決（即理論模型的確立），通常需要經歷下列階段（張瓊等，1994）：

1.準備：對問題進行有條理的分析和思考的過程。
2.醞釀與模型「種子觀念」的產生：即下意識完成的直覺創造過程，其思維過程帶有跳躍性和隨機性，經過直覺想像與聯想的自覺思維所提出一系列新奇的觀念，再通過理性審察，其直覺成果才得以湧現出來，成爲理論模型的「種子觀念」。
3.理論模型的擴充、定形和檢驗：對問題情勢進行通盤考慮，形成一個大致的解決方案（模型的基本假定），並引入適當的概念、命題、圖表、公式加以刻畫及表述，再運用各種邏輯方法，從其基本假定推導出具體結論。一個初步成型的理論模型，須進一步檢驗，包括：(1)從現有的背景理論來看，該理論模型的基本假設能否成立？(2)該理論模型的基本假設之間有無潛在的邏輯矛盾？(3)該模型的具體結論是否與經驗事實相一致？一個理論模型只有順利通過了這些檢驗，才能最終確立其在科學上的地位。

理論模型的建構是一項複雜的創造性活動。就每一個具體的研究過程而言，其「種子觀念」何時產生？何種條件下產生？其觀念能否順利繼續發展？及其發展的方式爲何？均由諸多因素所共同決定的。有些是研究者個人的因素，如：知識結構、生活經歷、個性素質和世界觀、方法論信條等；有些則是社會的、歷史的因素，包括整個時代的認識發展水準以及實踐檢驗所能達到的範圍和精度。因此，不同的研究者，由於背景理論不同，所掌握的事實材料不同，專業研究經驗不同，其建構理論模型的方式也是千差萬別的。然

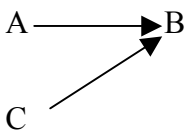
而，如果把目光轉向整個科學認識發展的歷史長河，那麼將會看到，在理論模型建構方式的千變萬化的表象之後，卻潛藏著某些始終一貫的作用及永恒的東西，那就是理論思維的基本方法和技巧。雖然不可能給理論模型的建構提出一套通用的操作程序，就像人們無法給文學藝術的創作過程列出規則一樣。但是，卻可以從方法論的角度爲這些基本的思維技巧及其在模型建構中的應用方式勾畫出一個大致的輪廓，此類思維技巧爲：類比、抽象、演繹、歸納等。

理論建構的具體途徑有（Kaplan, 1964；張紹勳，2000）：

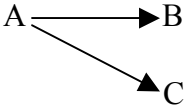
1. 內部細緻化（Knowledge Growth by Intention），在一個完整的領域內，使內部的解釋更加細緻、更適當化。例如，在「自變數 A 影響依變數 B」關係中，增加一個中介變數 C，使得原來的「A→B」，變成「A→C→B」的關係。
2. 外延法（Knowledge Growth by Extension），在一個較小的領域，先求取完整的解釋，然後將結論延伸至相似的領域，其有下列的作法：

（1）由已知「A→B」延伸爲「A→B→C」

（2）由已知「A→B」延伸爲下圖關係



（3）由已知「A→B」延伸爲下圖關係



回顧資訊安全管理的理論有：安全政策理論（Security Policy Theory）、風險管理理論（Risk Management Theory）、控制與稽核理論（Control and Auditing Theory）、管理系統理論（Management System Theory）與權變理論（Contingency Theory）等，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：安全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的內涵則是雷同的，尤其內部控制（Internal Control）幾乎是受到各家理論的重視，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），縱使以其環節較完整的「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）管理系統有始有終，但未能形成循環週期，與資訊安全持續改善之精神不符。

（5）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。

基於以上的分析，目前的任何資訊安全管理理論，都只適用於部分資訊安全管理活動或機制，沒有任何理論是可以適用於組織的各種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，及符合組織的目標。

洪國興等（2003）進而以個案研究法對組織資訊安全所涉及之安全政策（Security Policy）、風險管理（Risk Management）、內部控制（Internal Control）與資訊稽核（Information Auditing）等四個資訊安全活動進行了解，其結果：對於四個資訊安全管理活動的實施順序，其中個案 D、E 與 F 係按安全政策、風險管理、內部控制、資訊稽核之順序實施，其餘個案 A、B 與 C 並均未按上開順序實施，且彼此均不相同，如表二所示，顯示組織解決資訊安全問題是一種權變管理。再者除個案 D 主張組織在進行資訊安全管理活動，應採取循序程序（Sequential Process），即按安全政策、風險管理、內部控制與資訊稽核之順序實施外，其餘個案均主張應採取權變程序（Contingency Process），依組織所面臨資訊安全的環境，及業務上的需要，採取不同的資訊管理活動，如表三所示。由以上顯示資訊安全政策理論（Security Policy Theory）、風險管理理論（Risk Management Theory）、控制與稽核理論（Control and Auditing Theory）、管理系統理論（Management System Theory）或權變理論（Contingency Theory）等，以上任何單一的理論均無法同時具備循序程序（Sequential Process）與權變程序（Contingency Process），需建構同時具有循序程序與權變程序，可以適應於組織環境的各種不同需要的資訊安全管理理論。

表二 資訊安全管理活動之順序

資訊安全管理活動	個案A	個案B	個案C	個案D	個案E	個案F
制定資訊安全政策	1	1	3	1	1	1
進行資訊安全風險評估與控制	4	3	4	2	2	2
建立資訊安全內部控制制度	2	2	1	3	3	3
進行資訊稽核	3	4	2	4	4	4

資料來源：洪國興等，2003

表三 資訊安全管理程序之特性

特　　性	個案A	個案B	個案C	個案D	個案E	個案F
循序程序（Sequential Process）				V		
權變程序（Contingency Process）	V	V	V		V	V

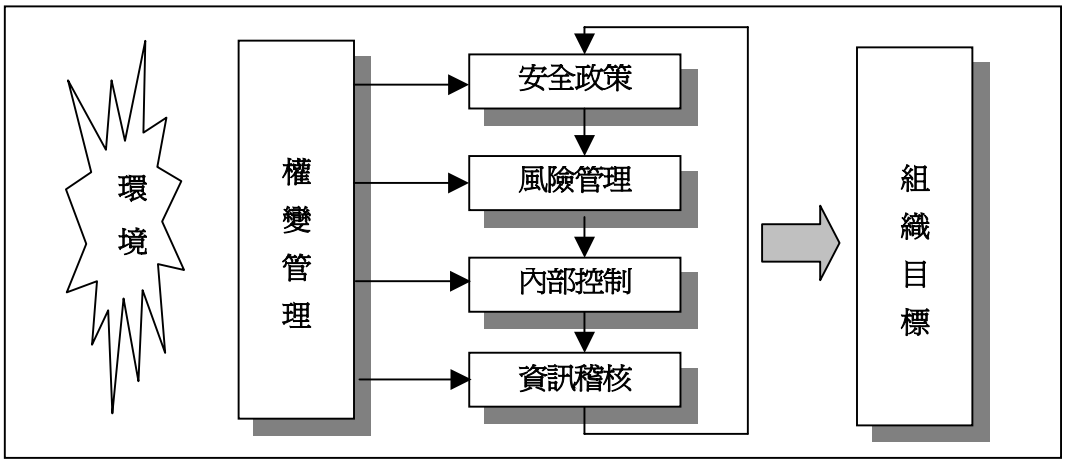
資料來源：洪國興等，2003

在六個研究個案中，對於資訊安全管理活動（Information Security Management Activity），包括：資訊安全政策（Information Security Policy）、風險管理（Risk Management）、內部控制（Internal Control）與資訊稽核（Information Auditing）等均有各種不同的作為，在實務上並不是只有單一的循序程序（Sequential Process）或單一的權變程序（Contingency Process）而已，而是有多元循序程序（Multi-Sequential Process）與多元權變程序（Multi-Contingency Process），簡言之，為多元程序（Multiple Process）（洪國興等，2003）。換言之，即組織可制定多個資訊安全政策，進而在不同時間對不同的資訊安全標的進行風險管理，也在先後制定各類的內部控制制度，執行之後，再進行資訊稽核，在多元的情況下，仍有循序程序與

權變程序之分，而不是部分學者所認爲其程序係結構化（Structure），就如同軟體發展生命週期（Software Development Life Cycle, SDLC）一般（如表一所示）；從實務上觀察資訊安全管理活動，較類似軟體發展的雛型法（Prototyping），由此更可以印證組織資訊安全管理活動是一個整合性資訊安全管理系統（Integrated Information Security Management System），而非單一的資訊安全管理理論所可以涵蓋，亦更足以驗証更有需要建構更周延、更完整及其可用性高的資訊安全管理理論。

因此，本研究即以紮根法建構理論，先歸納目前資訊安全管理理論特性與不足之處，比較整合，並以個案蒐集之資料及研究者的觀察、體驗等綜合判斷（Hammersley & Atkinson, 1989；徐宗國，1996），加以整合，使其更切合組織資訊安全管理行爲，更具包容性與解釋力，而建構爲整合性資訊安全管理系統（Integrated Information Security Management System, IISMS），此一系統係由（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，並與組織目標充分結合，形成一個整合性之資訊安全管理系統，如圖八所示。

IISMS 的理論基礎係「整合系統理論」（Integrated System Theory, IST），所謂「整合系統理論」係以權變管理（Contingency Management）爲基礎，整合資訊安全政策（Security Policy）、風險管理（Risk Management）、內部控制（Internal



圖八 資訊安全「整合系統理論」示意圖（資料來源：本研究）

Control ）與資訊稽核（ Information Auditing），構成與組織目標充分結合之資訊安全架構（ Information Security Architecture ），其理論建構的途徑（Approach）係屬歸納法，建構策略係採紮根法。此一理論之特性爲：

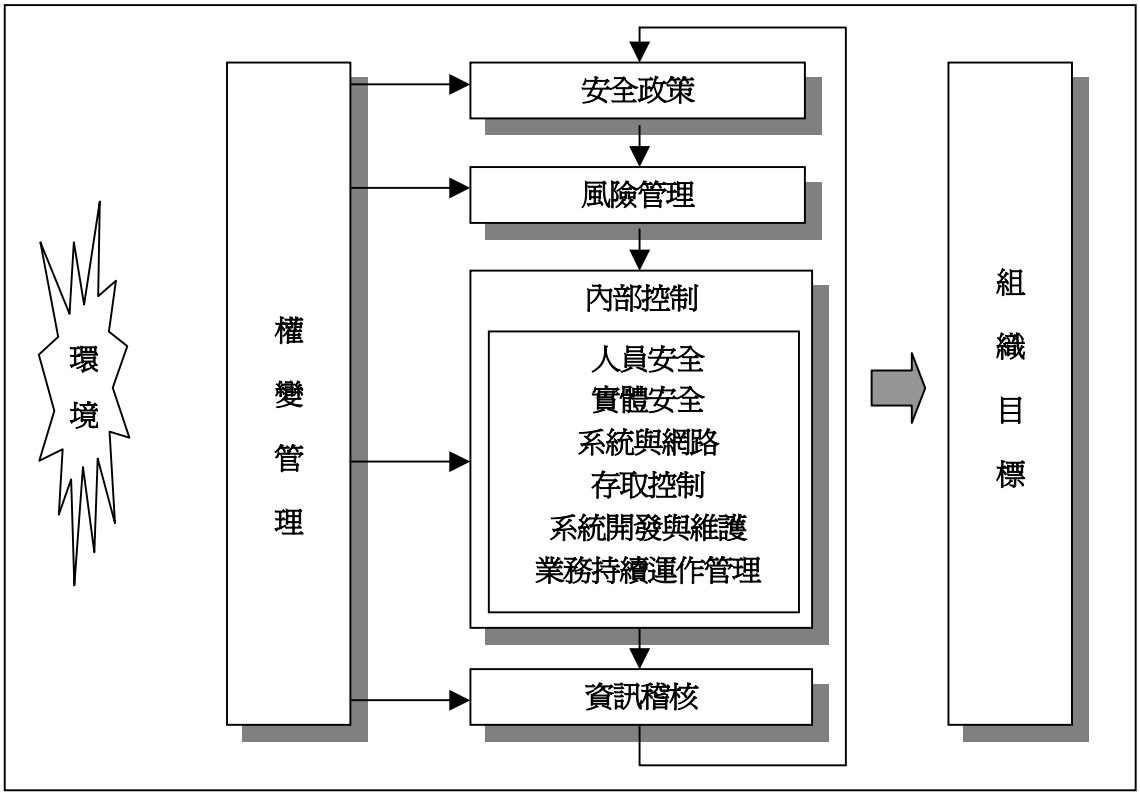
1. 以權變管理（Contingency Management）爲基礎，爲因應環境與組織業務之需求，任何一個資訊管理活動或組成（Component）都可以是組織資訊安全管理的切入點，不限於由資訊安全政策切入。
2. 系統流程可分爲：循序程序（Sequential Process ）與權變程序（ Contingency Process）。循序程序係按（1）安全政策；（2）風險管理；（3）內部控制；（4）資訊稽核之順序進行。權變程序係由任何一個資訊安全管理活動開始，再由該活動往下循序進行，例如：自風險管理開始，接著內部控制，再資訊稽核，又回到安全政策。但權變程序可進行一個資訊安全管理活動，也可以是多個資訊安全管理活動，以權變處理之，換言之，可以係多元程序。
3. 形成一個循環週期，週而復始，但權變程序之組成可以是獨立的，也可以連結，可以形成週期，也可以不是週期，視需要而定。循環週期回饋到開始的資訊安全管理活動，但也可回饋至開始之前的任何一個資訊安全管理活動。
4. 每一個資訊安全管理活動之間可以是先後關係，也可以是輸出/入關係。
5. 每一個資訊安全管理活動都與組織目標密切結合。

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）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、系統開發與維護、業務持續運作管理等安全控制，如圖九所示，其組織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，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）



圖九　資訊安全「整合系統理論」示意圖（續）（資料來源：本研究）

如何衡量一個理論的價值或決定那一個理論較優，可以從四個角度衡量（謝安田，1983）：

1. 範圍（Scope）

衍生名詞（Derived Term）對原始名詞（Primitive Term）的比率愈高，則理論的範圍愈廣。

2. 簡潔（Parsimony）

用很少的敘述而能解釋很多的現象，稱爲有力的理論（Powerful Theory）（朱柔若，2000）。

3. 解釋的正確性（Accuracy of Explanation）

解釋現象的準確性愈高，則愈有力。解釋力表現於理論模型對已知事實的解釋所能達到的精度與難度（張瓊等，1994）。

4. 預測的精準性（Precision of Prediction）

對現象的預測愈精準，則愈有力。預測力則表現於理論模型對未知事物或過程的預見能力－預測事實的多少、預測的精確度，特別是預測的新穎程度（張瓊等，1994）。

一個理論的解釋或預測能力愈強，則愈有用，故 Bacharach（1989）認爲評估一個理論的一般要件是：謬誤性（Falsifiability）與有用（Utility），故逐一評估變數（Variables）、構念（Constructs）與關係（Relationships），以知其是否謬誤與有用。

本研究所建構的資訊安全管理「整合系統理論」（Integrated System Theory, IST）與安全政策理論（SPT）、風險管理理論（RMT）、控制與稽核理論（CAT）、管理系統理論（MST）、權變理論（CT）等相較，前者 IST 在理論的完整性、適用範圍、實用性均較具優勢。從範圍、簡潔、解釋力與預測力等加以比較均優於當今後者各個理論，爲資訊安全管理理論之發展，向前邁進一大步。

伍、結論

由於組織對資訊科技的依賴日深，對於資訊安全管理亦日益受到重視，但實務界難尋資訊安全策略可資引用，有關資訊安全管理的實證研究亦難以發展，均直接間接與資訊安全管理欠缺一貫的理論有密切的關係。

理論模型是相關經驗事實的基礎上建立起來的，但它同時又是這些經驗事實的「辯護者」及發現新事實的重要工具，亦可用來了解、解釋與預測經驗與事實。此一過程存在著一種「循環」：我們是爲了解釋某些已知事實才建構一個理論模型，而這個理論模型又使我發現更多的待解釋的事實，爲此，我們又需要建構新的理論模型……。科學知識正是在這無限「循環」的過程中不斷地進步、不斷地逼近著客觀真理的（張瓊等，1994）。

經本研究對文獻探討、實務觀察，歸納整理安全政策理論（SPT）、風險管理理論（RMT）、控制與稽核理論（CAT）、管理系統理論（MST）、權變理論（CT）等資訊安全管理理論，並建構資訊安全管理之「整合系統理論」（IST），爲資訊安全管理之研究與實務，建立了新的里程碑，也爲資訊安全管理的研究，奠定了極爲堅實的基礎。

本研究有關資訊安全管理理論的歸納

整理與建構，在未來的資訊安全管理之研究與實務上，其貢獻為：

1. 使資訊安全管理的研究者，實務面有關資訊安全管理的決策者、規劃者，資源的提供者、使用者等，更了解資訊安全管理的策略、程序與方案。
2. 解釋組織資訊安全管理的行為，提供組織資訊安全管理策略的選擇方案。
3. 用於預測組織對資訊安全管理的先行活動與行為，在資訊安全所可能產生的結果，而對資訊安全管理的決策行為有所助益。
4. 對於資訊安全管理後繼的研究者，具有「指導研究」，提供「研究方向」，了解之前「研究基礎」等功能，使其在既有的研究基礎上更上一層樓，以加速資訊安全管理的研究，與其理論的發展。

對資訊安全管理後繼的研究，提出若干建議：

1. 以此資訊安全管理理論為基礎，建構資訊安全管理研究模式（Research Model），定義構念之間的關係，以作為實證研究的基礎。
2. 進行資訊安全管理之實證研究，有了理論基礎，建構研究模式，即可進行實證研究，以驗證模式及其構念的關係。
3. 將資訊安全管理理論與資訊管理或其他管理領域的理論比較、整合，以發展新的理論，建構新的資訊安全管理策略方案，以開拓新的研究空間，及提供實務界更有效的資訊安全策略選擇方案。

參考文獻

1. 行政院主計處電子處理資料中心（2001），「行政院及所屬各機關資訊安全管理規範」，資訊安全手冊，第三版，PP.28-77。
2. 朱柔若譯（2000），Neuman ,W. L. 原著，「社會研究方法：質化與量化取向」（Social Research Methods : Qualitative and Quantitative Approaches, 3rded），揚智文化公司。
3. 吳琮璠（2002），「會計財務資訊系統」，智勝文化事業。
4. 吳瑞明（1994），「系統安全問題與防護措施」，資訊與教育，40 期。
5. 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。
6. 宋鎧、范淨強、郭鴻志、陳明德與季延平（2001），「管理資訊系統」，華泰文化事業公司。
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. 林東清、許孟祥（1997）「資訊管理調查方法探討」，資訊管理學報，第四卷，第一期。

9. 林勤經、樊國楨與方仁威（2001），「資訊安全認證與電子化網路社會」，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託計畫，PP.80-104。
10. 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。
11. 林震岩（1996），「資訊系統與組織配合關係之研究」，國科會研究成果報告，NSC85-2416-H-033-001。
12. 洪國興、季延平與趙榮耀（2003），「組織制定資訊安全政策對資訊安全影響之研究」，資訊管理研究，第三期。
13. 洪祥洋（2000），「網路銀行風險管理」，存款保險資訊季刊， 第十三卷，第三期。
14. 徐宗國（1996），「紮根理論研究法：淵源、原則、技術與涵義」 ，質性研究：理論、方法及本土女性研究實例，巨流圖書公司，PP.47-73。
15. 高熏芳等譯（2001），Maxwell,J.A.原著（1996），「質化研究設計：一種互動取向的方法（Qualitive Research Design : An Interactive Approach）」，心理出版社。
16. 張　瓊、于祺明與劉文君（1994），「科學理論模型的建構」，淑馨出版社。
17. 張紹勳（2000），「研究方法」，滄海書局。
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. 黃承聖（2000），「企業資訊安全的起點－資訊安全政策」，網路通訊，2000 年 8 月。
20. 黃亮宇（1992），「資訊安全規劃與管理」，松岡電腦圖書公司。
21. 黃慶堂（1999），「我國行政機關資訊安全管理之研究」，國立政治大學公共行政學系碩士論文。
22. 楊金炎（2001），「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。
23. 樊國楨、方仁威與林勤經（2001），「資訊安全管理稽核概要－以電子銀行爲例」，資訊系統可信賴作業體制研討會論文集，PP.169-185。
24. 樊國楨、楊晉寧（1996），「互連網（Internet）電子信息交換安全－以電子公文交換作業安全爲本」，電腦稽核，PP.14-25。
25. 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。
26. 謝安田（1983），「企業研究方法」。
27. Anderson, J. M. (2003), “Why we Need a New Definition of Information Security”, Computers & Security, Vol.22, No.4, PP.308-313.
28. Bacharach, S.B.（1989）, “Organizational Theories: Some Criteria For Evaluation”,

Academy of Management Review, Vol. 14, No.4, PP.496-515.
29. BS 7799-2（1999）, "Information Security Management Part2: Specification for Information Security Management System", British Standards Institution, London.
30. Chapman, D. B. and Zwicky, E. D.（1995）, "Building Internet Firewalls", O'Reilly & Associates.
31. Cheon, M. J., Grover, V. & Teng, J. I. T., (1995), "Theoretical Perspectives on the Outsourcing of Information Systems", Journal of Information Technology, 10, PP.209-219.
32. COBIT (1998), "Governance, Control and Audit for Information and Related Technology", 3rd Edition Control Objectives.
33. Cozby, P. C. (1981), "Methods in Behavioral Research", 2nd ed., Palo Alton, California: Mayfield Publishing Co.
34. 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.
35. Drazin, R. & Van de Ven, A.H.（1985）, "Alternative Forms of Fit in Contingency Theory" Administrative Science Quarterly, 30, PP.514-539.
36. Dubin, R. (1976), "Theory Build in Applied Area", Dunnette M.(ed), in Handbook of Industrial and Organizational Psychology, (Rand Mc Nally : Chicago), PP.17-40.
37. Eloff, M. M. & Von Sloms, S. H. (2000a), "Information Security Management : An Approach to Combine Process Certification And Product Evaluation", Computers & Security, Vol.19, No.8, PP.698-709.
38. Eloff, M. M. & Von Solms, S. H. (2000b), "Information Security management : A Hierarchical Framework for Various Approaches", Computers & Security, Vol.19, No.3, PP.243-256.
39. Ettinger, J. E. (1993), "Key Issues in Information Security", Information Security, Chapman & Hall, London, PP.1-10.
40. Finne, T. (2000), "Information Systems Risk Management : Key Concepts and Business Processes", Computers & Security, Vol.19, No.3, PP.234-242.
41. Flynn, N.L.（2001）, "The e Policy handbook: Designing and Implementing Effective E-Mail, Internet, and Software Policies", American Management Association, New York, USA.

42. 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.
43. Gollmann, D. (1999), "Computer Security", John Wiley & Sons Ltd.
44. Gupta, M., Charturvedi, A. R., Metha, S. & Valeri, L. (2001), "The Experimental Analysis of Information Security Management Issues for Online Financial Services".
45. Hammersley, M. & Atkinson, P. (1989), "Ethnography: Prinicples in Practic", NY: Routledge.
46. ISACA (2002), "IS Standards, Guidelines and Procedures for Auditing and Control Professionals".
47. ISO / IEC 17799 (2000), "Information technology-code of practice for information security management".
48. Kabay, M.E. (1996), "The NCSA Guide to Enterprise Security", McGraw-Hill, 1996.
49. Kaplan, A. (1964), "The Conduct of Inquiry", New York: Chandler Co.
50. Lee, S.M., Luthans, F. and Olson, D.L. (1982), "A Management Science Approach to Contingency Models of Organizational Structure", Academy of Management Journal, Vol. 25, No.3, PP.553-566.
51. Lindup, K.R. (1995), "A New Model for Information Security Policies", Computers & Security, Vol.14, 1995, PP.691-695.
52. Loch, K. D., Carr, H. H. & Warkentin, M. E. (1992), "Threats to Information System : Today's Reality, Yesterday's Understanding", MIS Quarterly, June 1992, PP.173-186.
53. Luthans, F. (1976), "Introduction to Management: A Contingency Approach", NY : Mcgraw-Hill.
54. Reid, R. C. & Floyd, S. A. (2001), "Extending the Risk Analysis Model to Include Market-Insurance", Computers & Security, Vol.20, No.4, PP.331-339.
55. Robbins, S. P. (1994), "Management", 4thed, Prentice-Hall International.
56. Rusell, D. & Gangemi, G. T. (1992), "Computer Security Basics", California, U.S.A., O'Reilly & Associates Inc.
57. Schendel, D. & Hofer, C. W. (eds) (1979), "Strategic Management : A New View of Business Policy and Planning", (Little, Brown & Company, Boston).
58. Schneider, E. C. & Gregory, W. T. (1990), "How Secure Are Your System?" Avenues to Automation, Nov.

59. Schultz, E.E., Proctor, R.W., Lien, M.C. (2001), "Usability and Security An Appraisal of Usability Issues in Information Security Methods", Computer & Security, Vol.20, No.7, PP.620-634.
60. Sherwood, J. (1996), " SALSA: A method for developing the enterprise security architecture and Strategy ", Computer & Security, Vol.2, No.3, PP.8-17.
61. Simson, G. and Gene, S. (1991), Practical UNIX Security, O'Reilly & Associates, 1991.
62. Smith, M. (1989), "Computer Security–Threats, Vulnerabilities and Countermeasures", Information Age, October 1989, PP.205-210.
63. Trček, D. (2003), "An Integral Framework for Information Systems Security Management", Computers & Security, Vol.22, No.4, PP.337-360.
64. Tryfonas, T. , Kiountouzis, E. & Poulymanakou, A. (2001), "Embedding Security Practices in Contemporary Information Systems Development Approaches", Information Management & Computer Security, PP.183-197.
65. Tudor, J. K. (2001), "Information Security Architecture", Auerbach of CRC Press LLC, 2001.
66. Von Solms, R. (1996), " Information Security Management: The Second Generation", Computer & Security, Vol.15, No.4, PP.281-288.
67. Von Solms, R., Van Haar, H., Von Solms, S. H., & Caelli, W. J. (1994), "A Framework for Information Security Evaluation", Information & Management, 26, PP.143-153.
68. Weber, R. (1999), "Information System Control and Audit", Prentice Hall, Upper Saddle River, New Jersey.
69. Wright, M. (1999), "Third Generation Risk Management Practices", Computer Fraud & Security, Feb., PP.9-12.
70. Zmud, R. W. , Boynton, A. C. (1991) , "Survey Measures and Instruments in MIS : Inventory and Appraisal", In The Information Systems Research Challenge : Survey Research Methods, K. Kraemer(ed.) Boston : Harvard Business School, PP. 149-180.
71. Zmud, R. (1995), "The Role of Theory in Scholarly Manuscripts", Edit Comment. MIS Quarterly, September.

作者簡介

洪 國 興

交通大學管理科學研究所碩士，政治大學資訊管理學系博士，曾任中華民國資訊應用發展協會會長、副會長與資訊經理人協會常務理事，曾任台北市監理處、台北市政府捷運工程局、考試院等機關之資訊主管、監察院公職人員財產申報處副處長、交通委員會主任秘書等職務，現任監察院綜合劃室主任。曾參與公路監理、捷運工程等資訊系統專案。研究領域爲資訊系統整體規劃、資訊委外、資訊安全。

趙 榮 耀

台灣大學電機工程學碩士，美國杜克大電機工程博士，學成返國後任教於淡江大學，經歷工學院教授、院長、副校長、校長等職務，自民國八十二年二月擔任監察委員至今，歷任監察院教育、經濟、外交等委員會及國際事務、公共工程等小組召集委員。