國立交通大學

管理學院碩士在職專班管理科學組

碩 士 論 文

以 ISO 27001 為基礎評估電信業資訊安全管理
－ 以第一類電信業者為例

Evaluating Information Security Management Based on ISO 27001 for Type I Telecom Service Providers

研 究 生：徐弘昌

指導教授：林君信　教授

中 華 民 國 九 十 八 年 六 月

以 ISO 27001 為基礎評估電信業資訊安全管理
- 以第一類電信業者為例

Evaluating Information Security Management Based on ISO 27001 for Type I Telecom Service Providers

研 究 生：徐弘昌　　Student: Hung-Chang Hsu

指導教授：林君信　　Advisor: Dr. Chiun-Sin Lin

國 立 交 通 大 學

管理學院碩士在職專班管理科學組

碩 士 論 文

A Thesis

Submitted to The Master Program of Management Science

College of Management

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Management Science

June 2009

Hsinchu, Taiwan, Republic of China

中 華 民 國 九 十 八 年 六 月

以 ISO 27001 為基礎評估電信業資訊安全管理
- 以第一類電信業者為例

研究生：徐弘昌　　指導教授：林君信 博士

國立交通大學管理學院碩士在職專班管理科學組

摘　　要

科技與網路的發展迅速，增進人類生活的便利與效率，然而日益複雜的資訊安全問題，對於個人、組織甚至於國家，都已造成嚴重威脅。鑒於此，英國標準協會於 1995 年首先提出 BS 7799 資訊安全管理標準，架構出涵蓋技術面與管理面的全方位資訊安全管理系統(Information Security Management System，ISMS)，而後逐漸演變至今日的 ISO 27001。眾所皆知沒有 100%的資訊安全，只能採取適當的應變措施以及降低風險發生的機率來將損害減輕至最低，而遵循資訊安全管理的標準便是一個最好的方式。

本研究以 ISO 27001 的 11 大控制要項、39 個控制目標與 133 項控制措施為基礎，建立符合驗證規範的評核表，以深度訪談與實地查察的方式，評估電信業資訊安全管理的現況；同時彙整業者的實務經驗與專家意見，發展出適用於電信業的資訊安全管理建議：ISO 27001 核心版，其內容集合了 ISO 27001 控制措施的重點項目，提供有意自行導入資訊安全管理的電信業者參考；並運用重要性-表現程度分析法(Important-Performance Analysis，IPA)說明電信業者對於 133 項控制措施的施行策略。

研究結果顯示，根據 ISO 27001 的控制措施，電信業者的整體符合程度達到 90%，顯示電信產業的資訊安全管理具有不錯的水準，而在控制要項的執行情況上，表現較佳的是「資產管理」與「遵循性」，而表現欠佳需要加以改善的是「安全政策」與「資訊安全組織」；以資訊安全管理的三個面向探討，策略面表現優於管理面，而管理面優於作業面；針對適用於電信產業的 ISO 27001 核心版，則提出 58 項重要的控制措施作為資訊安全管理建議。

關鍵字：ISO 27001、資訊安全、ISMS、電信業

Evaluating Information Security Management Based on ISO 27001 for Type I Telecom Service Providers

Student: Hung-Chang Hsu Advisor: Dr. Chiun-Sin Lin

The Master Program of Management Science
College of Management
National Chiao Tung University

Abstract

Rapid growth on science and technology increases life convenience and efficiency, however the emerging information security issues become serious threat to personnel, organizations and countries. BSI released BS 7799, the Information Security Management Standard, on 1995 for building up the comprehensive ISMS, today's ISO 27001 is evolved from BS 7799. There is no 100% guaranteed information security, follow the international standard is the best way to minimize the damage caused by information security issues.

An ISO 27001 based evaluation form is created to appraisal information security management situation in telecom industry via physical interview and verification. The telecom industry oriented information security management suggestion, ISO 27001 Core Edition, is developed as reference for those who intend to deploy ISMS. IPA (Important-Performance Analysis) is used to illustrate the strategy of performing 133 controls by service providers.

The research result indicates telecom service providers reach 90% of conformance level against ISO 27001 controls, and have good performance on "Asset management" and "Compliance" control sections, but need to improve on "Security policy" and "Organization of information security" control sections. The proposed ISO 27001 Core Edition includes 58 important controls which can be the information security management suggestion for telecom industry.

Keyword: ISO 27001, Information Security, ISMS, Telecom Industry

誌　　謝

丁亥歲末思塾堂　勤書卷季餘　登竹塹名校金榜　螢窗腹中學

管院二載會英豪　笑逐知論間　獻章道文迎碩寶　舉觴得意回

冀以此詩「竹鹿」為交通大學兩年的碩士求學歷程畫下完美的句點，在即將完成人生另一個里程碑的此時此刻，首先要感謝指導教授林君信老師在進行論文研究的過程中所給予的引領與指導，啟發我獨立思考的能力與嚴謹學習的態度，令我受益良多；同時也感謝口試委員姜齊教授、陳台霖教授與張巧真教授所提供的寶貴建議與指正，讓論文更臻完善；此外，所上其他老師的悉心教導，令我沉浸於管理的無涯領域，亦一併致上最真誠的謝意。

我的學業與論文得以順利完成，還要感謝朋友、同學、同事對我的關心與鼓勵，感謝世強、文騰與鵬源分享論文寫作的經驗，感謝海鵬、迪穎、尹貞、力蓉與千慧等同窗在求學過程中的陪伴與勉勵，感謝淑娟與慧婷在論文撰寫過程中給予的專業意見與幫忙，感謝受訪者的協助，讓研究得以進行資料收集與分析。

回首這一段難忘的學習旅程，在繁忙的工作與沉重的課業之中努力取得平衡，雖然辛苦卻是人生中美好的回憶。最後，謹以此論文獻給我摯愛的家人，父母親與岳父母的栽培與鼓勵；永遠在背後默默支持的老婆大人佳玲是我精神上的依靠；可愛的雙胞胎寶貝兒子睿言與睿平總是在我需要思緒的時候能給予片刻的寧靜，謝謝你們過去兩年的體諒與包容，讓我無後顧之憂地衝刺事業與學業，在兩年內順利取得碩士學位，我的榮耀屬於你們！

目　　錄

表 目 錄

圖 目 錄

第一章 緒論

本章旨在概述本研究之主題，共分為四節。1.1 節介紹本研究的背景現況；1.2 節說明選擇本研究主題的動機；1.3 節闡述本研究所期望達成的目標；最後，1.4 節說明本研究的架構與流程。

1.1 研究背景

科技與網路的快速發展，徹底改變了人類的生活型態，不過卻也帶來副作用：資訊安全問題。回想 15 年前，那個網際網路即將起飛的年代，當時，沒有所謂的資訊安全專家，也沒有資訊安全長(Chief Information Security Officer，CISO)這樣的職位，組織最大的威脅是電腦病毒，然而不過是十年的光景，如今資訊安全事件頻傳，影響層面愈來愈廣，網路成了黑暗的溫床，說網路改變了罪犯賴以為生的方式也不為過，現今駭客走向組織化且國際化，其來無影、去無蹤，難以追查的特性，使得企業為了防範客戶資料、商業機密與智慧財產遭受竊取，進而造就資訊安全產品市場的蓬勃發展，例如：入侵偵測系統(Intrusion Detection System，IDS)、入侵防護系統(Intrusion Prevention Systems，IPS)、資料遺失防護(Data Loss Prevention，DLP)等。普渡大學的一份研究結果與 McAfee 的報告預估 2008 年全球企業的資料外洩損失可能高達 1 兆美元。

網路也將是未來國家之間的戰場，利用網路攻擊達成軍事機密的竊取以及軍事設施的癱瘓顛覆，中國「網軍」的成立可說明「網路戰」將成為未來主宰戰爭勝負的重要關鍵。鑒於資訊安全威脅與日俱增，各國政府也開始意識到資訊安全的重要性，英國標準協會於 1995 年率先提出 BS 7799 資訊安全標準，其後經過多次的修正與發展，演變為今日的 ISO 27001 與 ISO 27002，提供資訊安全管理的最佳實踐。

根據統計，85%的資訊安全事件是由於人為疏失所造成，因此資訊安全不僅是「技術面」的問題，還必須搭配「管理面」的具體措施，才能降低資訊安全的風險。ISO 27001 標準提供一套全方位的資訊安全管理架構(Jayawickrama, 2006)，目前廣為世界各地的國家或企業所採用，同時這項標準設計得相當彈性，能夠套用在所有類型的組織，而非限定於特定的產業或企業，如今 ISO 27001 已成為資訊安全管理的通用語言(Humphreys, 2008)。

行政院「國家資通安全會報」於 2001 年實施「建立我國通資訊基礎建設安全機制計畫」，目的是建立一完整的資通安全整體防護體系，並推動四大工作要項：建立國家資通安全事件通報及危機應變體系、健全國家資通安全防護能力、強化國家資通安全認知與訓練推廣作業、確保國家資通安全及促進國際合作等。該計畫將政府機關分為 A、B、C 與 D 四個等級，其中規定 A 與 B 等級的政府機關，其資訊安全管理系統(Information

Security Management System，ISMS)必須通過 ISO 27001 認證，在政府大力推動之下，再加上民間企業的努力，截至 2009 年 3 月 8 日為止，我國計有 221 家組織通過 ISO 27001 認證。

全球目前有 5206 家組織通過 ISO 27001 認證，我國排名全世界第四，其中前十名分別為：1.日本(2997 家)、2.印度(435 家)、3.英國(370 家)、4.台灣(221 家)、5.中國(180 家)、6.德國(112 家)、7.美國(85 家)、8.韓國(82 家)、9.捷克(70 家)、10.匈牙利(64 家)，如表 1-1 所示。

表 1-1 全球通過 ISO 27001 認證國家組織統計表

名次	國 家	數量	名次	國 家	數量	名次	國 家	數量
1	日本	2997	26	冰島	12	51	阿曼	3
2	印度	435	27	巴基斯坦	12	52	祕魯	3
3	英國	370	28	荷蘭	11	53	葡萄牙	3
4	台灣	221	29	新加坡	11	54	越南	3
5	中國	180	30	菲律賓	10	55	孟加拉	2
6	德國	112	31	俄羅斯	10	56	加拿大	2
7	美國	85	32	沙烏地阿拉伯	10	57	曼島	2
8	韓國	82	33	希臘	9	58	摩洛哥	2
9	捷克	70	34	斯洛維尼亞	9	59	葉門	2
10	匈牙利	64	35	瑞典	7	60	亞美尼亞	1
11	義大利	58	36	斯洛伐克	6	61	比利時	1
12	波瀾	35	37	南非	6	62	埃及	1
13	香港	31	38	巴林	5	63	伊朗	1
14	西班牙	30	39	哥倫比亞	5	64	哈薩克	1
15	奧地利	29	40	克羅埃西亞	5	65	吉爾吉斯	1
16	澳洲	28	41	印尼	5	66	黎巴嫩	1
17	愛爾蘭	26	42	科威特	5	67	立陶宛	1
18	馬來西亞	26	43	瑞士	5	68	盧森堡	1
19	巴西	20	44	保加利亞	4	69	馬其頓	1
20	墨西哥	20	45	直布羅陀	4	70	摩爾多瓦	1
21	泰國	20	46	挪威	4	71	紐西蘭	1
22	阿聯	18	47	卡達	4	72	烏克蘭	1
23	土耳其	17	48	斯里蘭卡	4	73	烏拉圭	1
24	羅馬尼亞	15	49	智利	3			
25	法國	12	50	澳門	3			

資料來源：International Register of ISMS Certificates，本研究整理

普渡大學教授 Spafford 曾說：「唯一真正安全的系統是將電源切斷，送至一個混凝土建築物並放入一間以鉛密封的房間之中，再加上武裝警衛的看守 – 儘管如此，我還是懷疑它是安全的」(Freeman, 2007)。資訊安全的重要性已不言可喻，然而要達到滴水不漏的 100%安全是不可能的事情，我們只能透過適當的應變措施以及降低風險發生的機率來將損害減輕至最低，而遵循資訊安全管理的標準便是一個最好的方式。

1.2 研究動機

電信服務是國人生活最息息相關的服務之一，每個家庭幾乎都有固接的市內電話，行動電話普及率長年維持在 100%以上(如圖 1-1)，寬頻上網的人口逐年上升，有線電視普及率也相當高，我國可說是通信密度極高的國家。

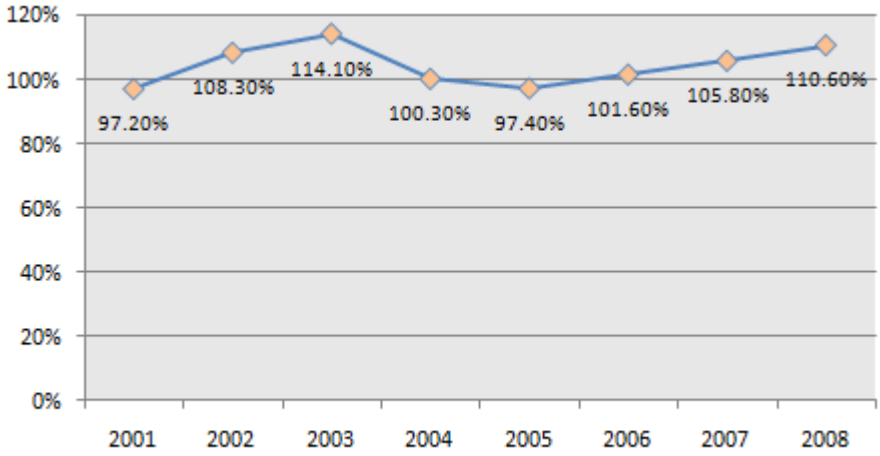

圖 1-1 國內行動電話普及率

資料來源：國家通訊傳播委員會，本研究整理

根據國家通訊傳播委員會(National Communications Commission，NCC)統計資料，國內經營電信業務的業者高達 606 家，共計 993 張執照。根據電信法規定，我國電信事業分為第一類與第二類電信事業。第一類電信事業指設置電信機線設備，連接發信端與受信端之網路傳輸設備，提供電信服務之業者，執照發給採「特許制」；第二類電信事業指第一類電信事業以外之電信事業，執照發給採「許可制」。其中第一類電信業者有 95 家，總計 115 張執照，經營業務涵蓋固網通信、有線電視、2G 行動電話、3G 行動通信、無線寬頻接取行動通信(WiMAX)、數位式低功率無線電話(PHS)、無線電、衛星通信及國際海纜等；第二類電信業者則有 511 家，總計 878 張執照，主要業務範圍為批發轉售第一類電信業者提供的語音數據等通信服務。

電信服務與民眾的日常生活如此密不可分，使得電信業者的競爭日趨激烈，許多業者除了提供良好的通信服務之外，也開始在資訊安全方面下功夫，例如：中華電信 Hinet 除了提供使用者數據上網服務之外，也提供垃圾郵件過濾、防毒防駭、色情守門員及線上掃毒等加值服務。電信業正從封閉系統(Closed System)走向開放系統(Open System)，同時業者也提供愈來愈多的加值服務，其資訊安全管理就顯得格外重要，一旦系統故障或是遭受到攻擊而癱瘓，將對客戶造成難以彌補的傷害。

以下幾則國內、外資訊安全案例顯示，電信服務業者未來將在資訊安全領域扮演重要的守門員角色：

1. 資訊安全軟體廠商賽門鐵克(Symantec Corporation)於 2008 年 4 月 10 日發表的資訊安全研究報告指出，國內電信龍頭業者中華電信，登上全球最多惡意活動 ISP(Internet Service Provider)排行榜的第七名，在亞太區僅次於排名第二的中國網通。鑒於客戶可能缺乏專業能力，中華電信表示近年來推動的機房端入侵偵測防護(IPS)、安全上網等服務，目的就是讓客戶增加多一層保障。

2. 美國三大 ISP 業者(Verizon、Time Warner Cable 與 Sprint)於 2008 年 6 月首次聯手協助整頓網路兒童色情，未來將攔阻相關新聞群組的網路存取，及關閉相關的網路代管伺服器，從源頭阻斷相關服務。紐約州檢察長 Andrew M. Cuomo 讚揚這些業者樹立了新的責任標準，並認為該模式應該延伸到整個產業。

3. 美國兩大 ISP 業者 Global Crossing 及 Hurricane Electric 於 2008 年 11 月 11 日先後切斷惡名昭彰的垃圾郵件發源地 McColo 的網路流量，根據 IronPort Systems 及 MessageLabs 等資訊安全業者的垃圾郵件偵測機制，發現全球垃圾郵件數量在隔天 2008 年 11 月 12 日大幅下滑了 41%；資訊安全專家並估計，自 McColo 送出的垃圾郵件約佔全球垃圾郵件總數的 75%。

4. 國家通訊傳播委員會於 2008 年 11 月 24 日在委員會議中通過「濫發商業電子郵件管理條例草案」，行政院於 2009 年 2 月 26 日於通過該草案，未來可望於立法院通過，草案第六條第一項明文規定「網際網路接取服務提供者」(Internet Service Provider，ISP)採行必要措施，防止濫發商業電子郵件，同時收到垃圾郵件的民眾將可向濫發者求償，每封可求償新台幣 500 至 2,000 元。

5. 2009 年 3 月 2 日起陸續發生「神秘網頁轉址攻擊事件」，CNET、ZDNet 與 MSN 等知名網站的網頁疑遭綁架，之所以稱之為神秘的原因是，經過兩個禮拜的時間，國內資訊安全專家仍無法確切指出攻擊者的目的及其攻擊手法。部分網友與同業質疑 CNET 與 MSN 網站遭綁架源自於中華電信的 DNS(Domain Name System)主機遭攻擊，不過對此中華電信澄清未發現任何異常的路由指向發生。

網路上所有的流量都會通過電信業者的網路設備，因此當資訊安全事件的威脅程度與日俱增，監控、攔截與阻斷相關服務，避免傷害持續擴大，電信業者就有責無旁貸的責任與義務，也突顯出電信業者的資訊安全管理之重要性，因為如果連電信業者的資訊安全管理都做不好，如何做好把關的工作？如何確保使用者的資訊安全？

過去國內以 BS 7799 或 ISO 27001 探討相關產業、組織或企業的資訊安全管理之文獻，大多以醫療體系、政府機關、軍事單位與金融機構為主，尚未見到電信產業方面的研究，因此本研究冀以 ISO 27001 為基礎探討電信業者的資訊安全管理現況，期盼電信業者能意識到其在資訊安全領域的角色與重要性，進而建立健全的資訊安全管理系統。

1.3 研究目的

本研究之主要目的在於運用 ISO 27001 的控制項目來評估電信業資訊安全管理的現況，並提出適合國內電信業之資訊安全管理建議：ISO 27001 核心版，作為相關業者未來計畫導入資訊安全管理時的參考，同時依據評核分析的結果說明電信業者對於 ISO 27001 控制措施的施行策略。

研究者詳實彙整資訊安全管理系統的發展與應用，以國際認同之資訊安全標準 ISO 27001 的 11 大控制要項、39 個控制目標與 133 項控制措施為基礎，運用李克特(Likert)的總加量表法，建立四分量表，仿照 ISO 稽核驗證機制，以實地訪查方式評估本研究之個案業者的資訊安全管理系統。

國內第一類電信事業的規模與業務複雜程度大多高於第二類電信事業，因此本研究以第一類電信業者為主要研究對象，為使本研究之結果也能適用於其他電信業者，研究者嘗試從國內 95 家第一類電信業者中挑選出具代表性的 5 家業者進行個案分析研究，藉以瞭解國內電信業者之整體資訊安全管理的現況。

對於計畫自行建立資訊安全管理系統的電信業者而言，可能受限於資源不足而無法全面實施 ISO 27001 所載錄的 133 項控制措施，因此研究者將參考個案業者的資訊安全管理部門主管或員工的經驗，並採納 ISO 27001 主導稽核員的專家意見，發展出一套適用於電信業的資訊安全管理建議，稱之為「ISO 27001 核心版」，其內容為 ISO 27001 控制措施的重點項目，提供其他規模較小的電信業者或未來的新進業者導入資訊安全管理時參考依循。

因此，本研究期望能達到以下目的：

- 探討資訊安全管理之相關議題。
- 探討 ISO 27001 之內涵與其控制要項。
- 依據 ISO 27001 的驗證規範，評估電信業的資訊安全管理之現況。
- 提出符合電信業特性的資訊安全管理建議之「ISO 27001 核心版」。
- 運用 IPA(Important-Performance Analysis)矩陣分析電信業者對於 133 項控制措施的施行策略。
- 促進電信業者之資訊安全管理意識，建立完整的安全防護體系。

1.4 研究架構

本研究之架構，首先根據研究動機與目的來確立本研究的方向與範圍，以探討電信業的資訊安全管理為主題，透過蒐集國內、外相關文獻與探討 ISO 27001 之內涵，建立以 ISO 27001 為基礎的評核表，並仿照 ISO 27001 稽核驗證的方式，針對個案電信業者進行深度訪談與實地查察，藉以瞭解電信業者的資訊安全管理現況，最後依據所蒐集的資料與訪查結果作彙整分析，提出本研究的結論與相關研究建議。

本研究共分為五章，各章摘要如下：

第一章　緒論

說明本研究之背景、動機與目的，概述研究的方向與範圍，並解釋本研究的架構與流程。

第二章　文獻探討

定義資訊安全，介紹國際相關標準機構，說明 ISO 27001 的內涵與驗證規範，闡釋風險評鑑的內涵與應變措施，描述我國資訊安全發展現況與施行計畫，最後探討國內、外相關文獻。

第三章　研究方法

說明本研究採用個案研究法的理由，介紹質性研究法，並敘述研究方法的設計及研究程序，說明本研究資料蒐集的方式，建立以「ISO 27001」為基礎的評核表，最後說明研究範圍與限制。

第四章　研究分析

分析各項文件資料、數據與訪談查察的結果，呈現個案業者在資訊安全管理的執行狀況，提出具體的資訊安全管理建議予以電信業者參考，並說明電信業者對 133 項控制措施的施行策略。

第五章　結論與建議

綜合研究分析的結果，簡述本研究之貢獻，並總結電信業之資訊安全管理的評估報告，最後提出後續研究建議。

本研究的研究架構與流程，如圖 1-2 所示。

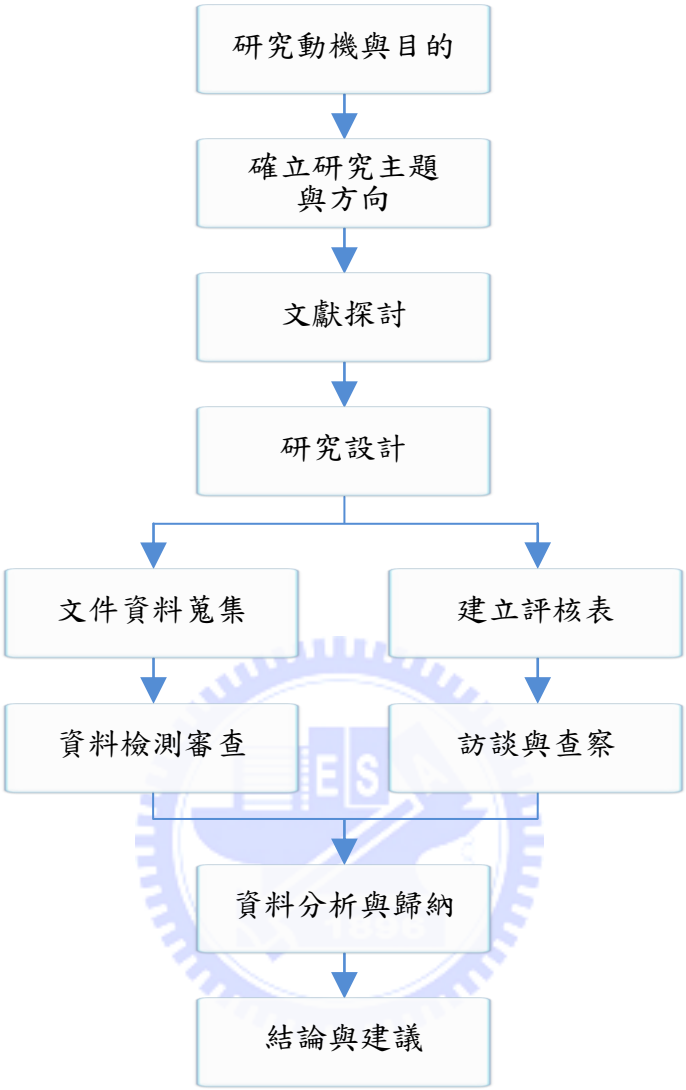

圖 1-2 研究架構與流程

資料來源：本研究整理

第二章 文獻探討

本章旨在說明本研究主題相關的文獻探討，共分為六節。2.1 節說明資訊安全的定義、內涵與特性；2.2 節介紹三個國際性的標準機構：國際標準組織(ISO)、英國標準協會(BSI)與國際電工技術委員會(IEC)；2.3 節介紹 ISO 27001 的演變發展與內容；2.4 節闡釋風險評鑑的過程與因應方式；2.5 節說明我國資訊安全管理的發展狀況與施行計畫；最後，2.6 節介紹國內、外相關的研究文獻。

2.1 資訊安全

資訊是一種資產，與支援過程、系統及網路一樣都是重要的營運資產，對組織營運是不可或缺的，因此需要妥善保護。在互連性增長的營運環境中，由於資訊暴露在日益成長與多樣的威脅與脆弱性中，資訊也因此顯得更加重要。資訊存在的形式有許多種，可以列印或書寫於紙上表示、可以用電子方式儲存、可以用郵寄或是電子方式傳送、也可以用膠卷展現或在交談中口述。然而，無論資訊的形式為何，以何種方式分享或儲存，均應加以適當的保護。

資訊安全是使資訊不受各種廣泛的威脅之保護，以降低營運風險，確保營運的持續性，進而得到豐厚的投資報酬率及商機。資訊安全經由實作一套適當的控制措施達成，包括政策、過程、程序、組織結構及軟硬體功能，必要時必須建立、實作、監視、審查與改進這些控制措施，以確保達成組織的特定安全與營運目標。定義、達成、維持及改進資訊安全，可能攸關維繫競爭優勢、現金流量、獲利能力、適法性及商業形象。

資訊安全為保存資訊的以下三項特性：

- 機密性(Confidentiality)：資訊不可被未經授權的個人、實體或流程取得或揭露。
- 完整性(Integrity)：保護資訊以及資產的準確度(Accuracy)與完全性(Completeness)。
- 可用性(Availability)：經授權的個體在需要時可以存取或使用資訊及相關資產。

除此之外，資訊安全亦同時涉及資訊的鑑別性(Authenticity)、可歸責性(Accountability)、不可否認性(Non-repudiation)與可靠度(Reliability)。

對於任何造成資產損害的潛在可能性稱為威脅(Threat)，威脅利用脆弱性[1]造成對資產、組織和系統的傷害和損毀。資訊安全的威脅一般可分為兩大類：

[1] 脆弱性(Vulnerability)是安全的漏洞或弱點，本身並不會造成傷害，而是可能允許威脅影響資產的情況，若沒有適當處理將促使威脅形成。例如：未安裝防火牆、權限設定錯誤、缺乏安全意識、不穩定的系統與安全訓練不足等。

- 環境威脅(天災)：天然災害，例如：火災、颱風和地震等；或是系統故障，例如：網路設備異常、硬碟故障和線路中斷等。
- 人為威脅(人禍)：又可分為人為疏失與蓄意破壞。人為疏失大多來自於內部人員，主要為系統操作不慎、不當使用習慣(濫用電子郵件、任意下載檔案)與管理鬆散等；蓄意破壞則可能來自於內部人員與外部人員，主要為內部人員竊取公司資料、離職員工挾怨報復、駭客入侵與商業間諜等。

資訊安全是一個管理過程而非技術過程，必須永無止境的不斷調整與改善，以「資訊安全管理」為核心加以整合「資訊安全技術」層面，在企業組織裡架構一套專屬且適用的資訊安全管理機制與策略，因應管理企業所面臨的資訊安全風險，以控制與降低資訊安全事件所帶來的威脅與衝擊。

2.2 國際標準機構

標準為一致同意並列入正式紀錄的文件化協定(Documented Agreement)，範圍涵蓋技術規格或其他引用為規範特性之規則、指引或定義之準據，標準之運用係為確保物質、產品、製程以及服務等均能符合使用目的，最顯而易見的標準為信用卡格式的標準化。試想如果不同國家或不同區域採行之技術相似但卻缺乏調和標準，勢必對貿易造成技術性障礙，依賴出口的產業為促使國際貿易程序合理化，因而產生建立全球性標準的需求，此為國際標準之由來。

2.2.1 國際標準組織(ISO)

國際標準始於 1906 年的國際電工技術委員會(International Electrotechnical Commission，IEC)，專責電子技術標準的研定。其他領域之標準，則由 1926 年設立的國際國家標準化協會聯盟(International Federation of the National Standardizing Associations，ISA)負責，ISA 初始的工作重點在於機械工程。ISA 的活動在 1942 年因第二次世界大戰而停止，戰後 25 國代表於 1946 年在倫敦開會決議設立新國際組織，以加速工業標準之國際調和與單一化、促進貨品與服務之國際交換以及發展智慧財產權、科學、技術以及經濟活動的合作，隨後於 1947 年 2 月 23 日成立非政府組織(Non-governmental organization，NGO)之國際標準組織(International Organization for Standardization，ISO)，組織各成員國和技術委員會進行情報交流，同時與其他國際組織進行合作，推動國際單一的工業標準，促使全球貿易、學術交流和經濟合作等活動，透過 ISO 運作達成的國際協定即公布為國際標準。

ISO 標準的形成根據三項原則：第一為共識性，採納所有利害相關團體之意見；第二為全球工業性，尋求適合全球工業及消費者的解決方案；最後為自願性，基於市場導向的特性，國際標準之推行是建立在市場內所有關係人自願採行的基礎上。

形成 ISO 標準則有三步驟：首先由一國內工業部門基於市場需求提出建立國際標準的要求，並透過該國國內具有 ISO 會員成員身分的國家標準機構向 ISO 提議新工作項目；一旦該項提議獲得同意，第一步驟由對該項議題有興趣國家的技術專家代表，組成工作小組以界定未來新標準的技術範圍；工作小組如就技術議題達成協議後，第二步驟即為協商標準規格的細節，此為建立共識階段；等到完成國際標準草案後即進入第三步驟表決，應有三分之二參與本標準討論的會員成員以及四分之三 ISO 會員成員的表決通過，始得成為國際標準。

由以上標準制定程序可知 ISO 所制訂的國際標準並無強制性的規範，其發展基於所有關係人的共識並且符合市場導向，為符合科技發展、新方法與新物質以及新品質與安全等需求，ISO 要求國際標準應至少每五年定期檢討。

ISO 雖然制定標準但不負責監督標準的執行，標準之採行完全由供應商與顧客或將 ISO 標準納為國家標準的主管機關決定。ISO 標準執行的監督評估，則由公正獨立的第三方實驗機構或審核單位負責稽核，這些提供稽核服務單位的權能，或為政府主管機關的授權，或為建立供應商及顧客間之互信所產生的商業活動需求。ISO 並不監督稽核服務的商業活動，惟提供稽核指引(Guide)，建立國際認同的自願性審核標準。

從事 ISO 驗證的機構甚多，然而鑒於驗證公司的驗證品質良莠不齊，各國或各區域均成立國家級的認證機構加以管理，以齊一驗證公司的品質。各認證機構可透過國際合作簽署多邊相互承認協議，以減少重複的認證程序。我國為因應國際趨勢，經濟部於八十六年三月訂定「中華民國品質管理及環境管理認證制度實施辦法」及「中華民國品質管理及環境管理認證委員會設置要點」。

ISO 所公布的各項標準中，較為眾人知悉的 ISO 9000 及 ISO 14000 系列，ISO 9000 系列為規範品質保證方面的標準，ISO 14000 則為規範環境管理方面的標準。

2.2.2 英國標準協會(BSI)

英國標準協會(British Standard Institute，BSI)成立於 1901 年，是全球第一家國際性標準組織，也是國際標準組織(ISO)的創始會員，除了標準制定之外，目前也是全球最大的稽核驗證機構，驗證佔有率為世界第一，全世界平均每八張證書中就有一張由 BSI 頒發，在全球 100 多個國家中透過 BSI 驗證合格的機構有 60,000 多家。BSI 是全世界驗證機構中唯一被國際標準組織委託進行標準研發及制定的驗證機構，在資訊安全管理系統(Information Security Management System，ISMS)領域中，BSI 被全世界公認是目前最為公正且專業嚴謹的驗證及訓練機構。BSI 制定並頒布了許多首創的商業標準，包括：品質管理系統、環境管理系統、職業安全衛生管理系統以及相關專案管理，BSI 平均每年制定超過 2,000 種標準。世界 500 大企業，其中約有四分之一的公司選擇 BSI 作為他們通過 ISO 9000、ISO 14000 和歐盟「環境管理與稽核制度」(Eco- Management and Auditing

Scheme，EMAS)等認證的輔導機構。

BSI 至今已發展成為全球頂尖之獨立專業服務企業，BSI 集團主要分為三個事業群，負責全球的營運：BSI 英國標準、BSI 管理系統與 BSI 產品服務，其中「BSI 英國標準」發行、推廣並且分享最佳實踐的標準及革新，出版超過 27,000 種英國標準；「BSI 管理系統」則提供管理系統全面性的稽核、驗證與訓練服務；「BSI 產品服務」提供產品測試服務作為產品認證程序的一部分，部分測試有助於認證標誌的核發，而部分測試則是為了評估產品的性能及設計。

著名的資訊安全標準 BS 7799 在 1995 年公布之後，國際標準組織於 2005 年通過將 BS 7799-2:2005 發展為 ISO 27001，也是本研究將用以來評估電信業資訊安全管理的標準；BS 7799-1:2005 則發展為 ISO 17799，而 ISO 17799 於 2007 年 7 月，正式更名為 ISO 27002。

2.2.3 國際電工技術委員會(IEC)

國際電工技術委員會(International Electrotechnical Commission，IEC)是全球成立最早的非政府性國際電工標準化機構，於 1906 年 6 月 26 日由英國的 IEE 和美國的 IEEE 以及其它相關組織舉行了其成立會議，是聯合國經社理事會(ECOSOC)的甲級諮詢組織。目前 IEC 成員國包括了絕大多數的工業發達國家及部分發展中國家，這些國家擁有世界人口的 80%，其生產和消耗的電能占全世界的 95%，製造和使用的電氣、電子產品占全世界產量的 90%。IEC 的宗旨：促進電工標準的國際統一，電工、電子工程領域中標準化及有關方面的國際合作，增進國際間的相互瞭解。目的在於為所有電工、電子相關的技術制定符合政府、商業、社會規範的國際化標準，涵蓋電工和電子方面的詞彙、標誌、兼容性、測量與評估、設計與發展、安全與環境等基本規範。IEC 與 ISO 是互補的國際性標準機構。

2.3 ISO/IEC 27001

ISO/IEC 27001 即本研究主題之 ISO 27001，為資訊安全管理的標準，源自於英國國際標準 BS 7799 Part-2:2002，英國標準協會於 2005 年公布新版之 BS 7799 Part-2:2005，國際標準組織於 2005 年 10 月 14 日將 BS 7799 Part-2:2005 編納為 ISO 27001，是目前國際公認最完整的資訊安全管理標準，其規範安全內容涵蓋：建立、實施、操作、監督、審查、維持與改善資訊安全管理系統(Information Security Management System，ISMS)。

英國標準協會於 1995 年 2 月提出 BS 7799 資訊安全管理規範，並於 1999 年公布 BS 7799 Part-1 與 Part-2，內容涵蓋當前組織所有的安全議題，是一套詳盡且嚴謹的資訊安全標準。BS 7799 全名為「BS 7799 Code of Practice for Information Security」，從基本的資訊安全政策制定、資產管理、人員安全責任的歸屬、組織風險的評估、存取控制、

防毒與相關策略、組織業務永續經營計畫以及災難應變計畫，到最後定義組織內部的安全係數與強化組織資訊安全係數等。

BS 7799 Part-1 是資訊安全管理作業要點，主要是提供組織建置資訊安全管理系統的指南及一般原則，可作為參考的文件與建議，內容涵蓋廣泛的資訊安全控制措施以及施行資訊安全的最佳方法(Best Practice)，國際標準組織於 2000 年將 BS7799 Part-1 編納為 ISO 17799「Information Technology - Security Techniques - Code of Practice for Information Security Management」，並於 2007 年 7 月正式更名為 ISO 27002。

BS 7799 Part-2 是資訊安全管理系統要求，依據 BS 7799-1:1999 以及 ISO 17799:2000 的架構，提供資訊安全管理系統的建立、實施、維護與書面化的具體要求，同時 BS 7799 Part-2 也是驗證標準，組織若要取得 BS 7799 的認證，則必須遵循 BS 7799 Part-2 的要求。國際標準組織於 2005 年將 BS 7799 Part-2 編納為 ISO 27001「Information Technology - Security Techniques - Information Security Management Systems - Requirements」。

BS 7799 演進至 ISO 17799 及 ISO 27001/ISO 27002 的發展如圖 2-1 所示。

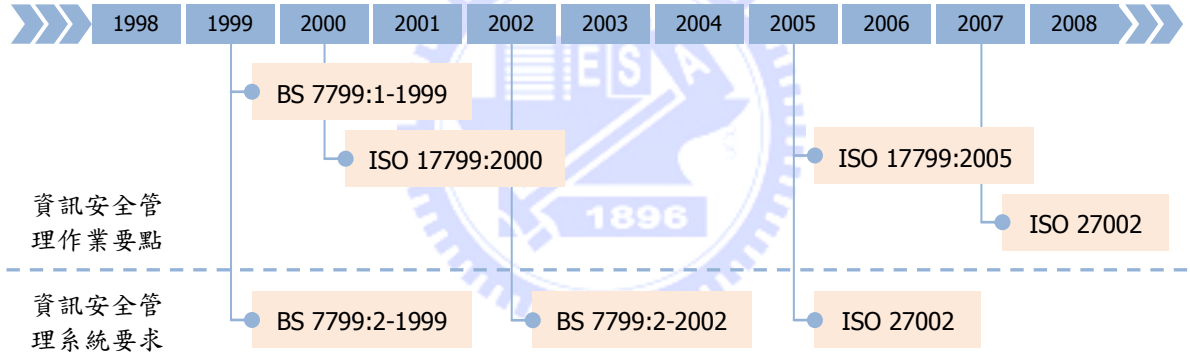

圖 2-1 ISO 27001 發展沿革

資料來源：英國標準協會，本研究整理

ISO 27001 的架構與內容如圖 2-2 所示，分為簡介、適用範圍、引用標準、用語釋義、資訊安全管理系統、管理階層責任、ISMS 內部稽核、ISMS 之管理階層審查與 ISMS 之改進等九節以及附錄 A~C。

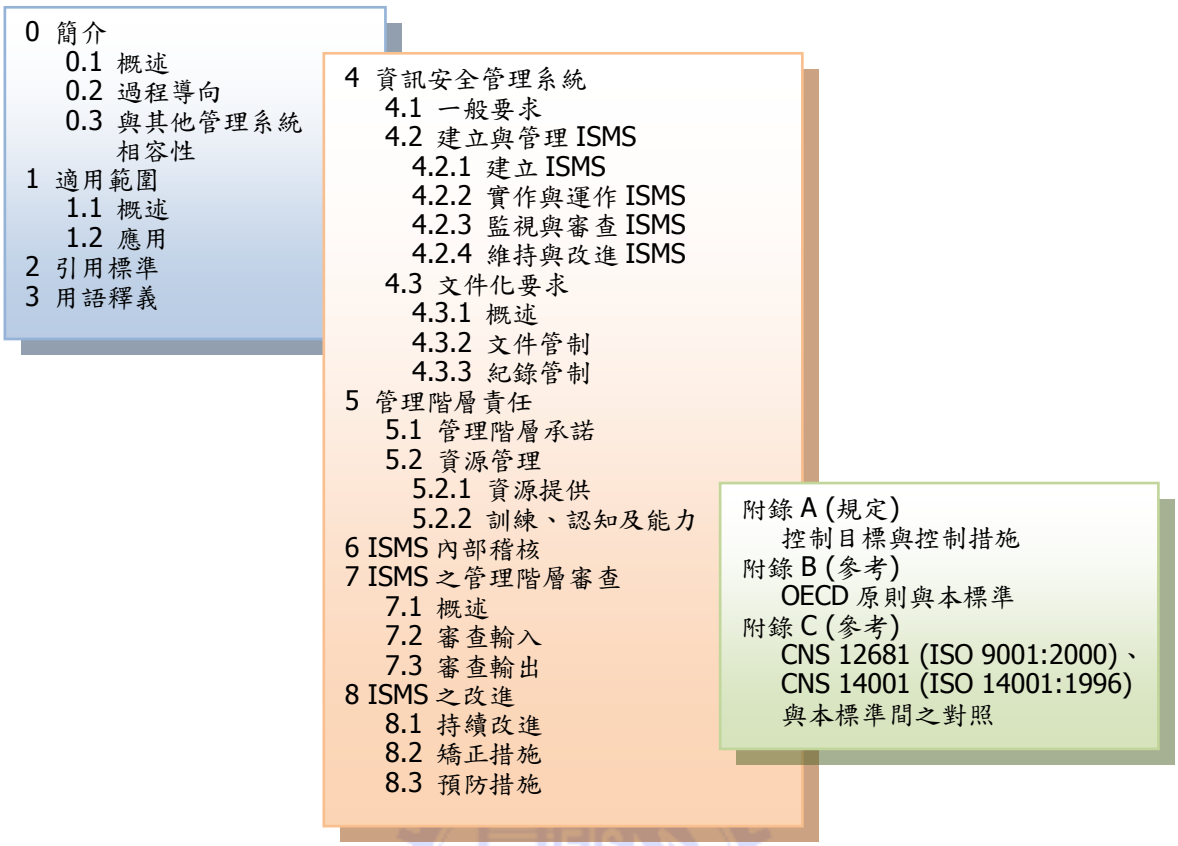

圖 2-2 ISO 27001 架構與內容

資料來源：ISO/IEC 27001:2005，本研究整理

ISO 27001 適用於所有類型的組織(例如，商業企業、政府機構、非營利組織)，其採用「規劃-執行-檢查-行動」(Plan-Do-Check-Act，PDCA)模型於建置所有資訊安全管理系統，圖 2-3 說明資訊安全管理系統如何採納利害關係人的資訊安全要求與期望作為輸入，經過各個必要的行動與過程，產生符合此要求與期望的資訊安全輸出結果。同時圖 2-3 也說明 ISO 27001 從第 4 節「資訊安全管理系統」、第 5 節「管理階層責任」、第 6 節「ISMS 內部稽核」、第 7 節「ISMS 之管理階層審查」到第 8 節「ISMS 之改進」如何環環相扣。PDCA 模型也反應經濟合作暨發展組織(Organisation for Economic Co-operation and Development，OECD)指導綱要[2]內所宣告之治理資訊安全系統與網路安全的原則，OECD 原則與 PDCA 模型的對應關係如本研究之附錄 A 所示。

[2] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, OECD Publications, Paris, July 2002, www.oecd.org

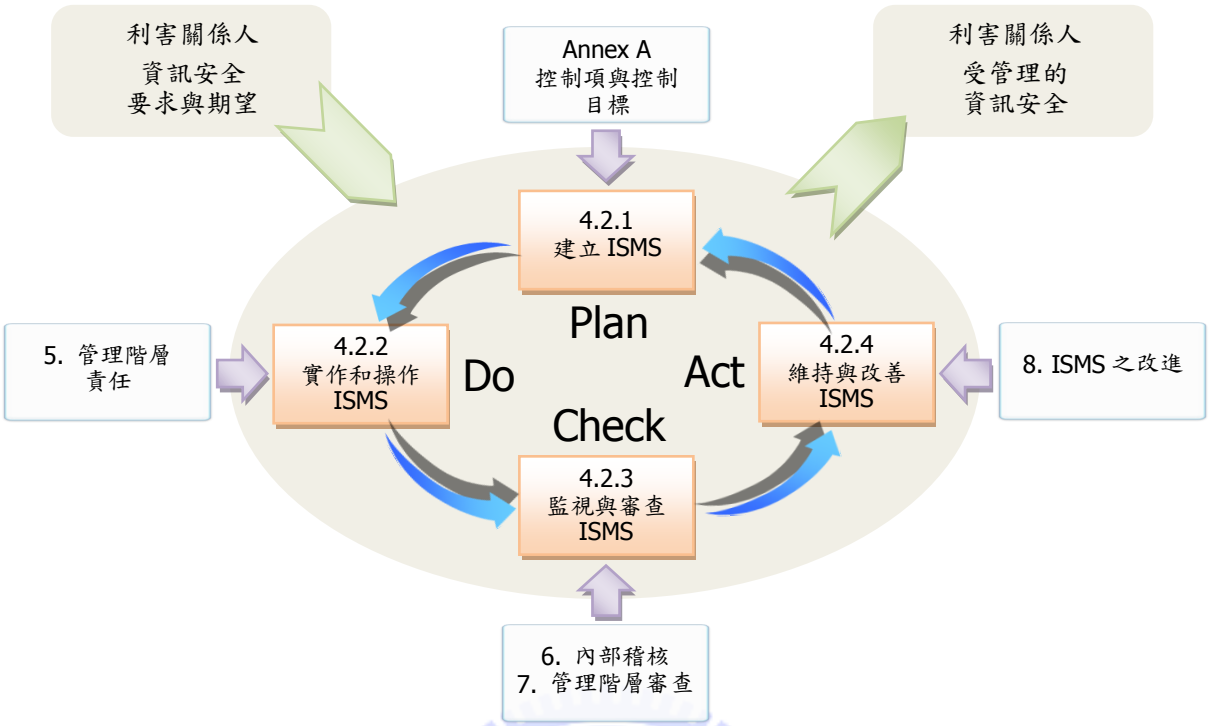

圖 2-3 適用於 ISMS 之 PDCA 模型

資料來源：ISO/IEC 27001:2005，本研究整理

- 規劃(建立 ISMS)：建立與管理風險及改進資訊安全相關之 ISMS 的政策、目標、過程及程序以產生與組織整體政策和目標一致的結果。
- 執行(實作與運作 ISMS)：實作與運作 ISMS 的政策、控制措施、過程及程序。
- 檢查(監視與審查 ISMS)：依據 ISMS 政策、目標及實際經驗，評鑑及在適用時測量過程績效，並將結果回報給管理階層審查。
- 行動(維持與改善 ISMS)：基於 ISMS 內部稽核與管理階層審查結果或其它相關資訊採取矯正與預防措施，以達成 ISMS 的持續改進。

建立資訊安全管理系統，組織應執行下列事項：

1. 依據營運、組織、其所在位置、資產及技術等特性，界定資訊安全管理系統導入的範圍。
2. 依據營運、組織、其所在位置、資產及技術等特性，定義資訊安全管理系統政策[3]。

[3] 為 ISO 27001 之目的，資訊安全管理系統政策被視為資訊安全政策的超集合。

3. 定義組織的風險評鑑做法。
   - 識別適合的資訊安全管理系統及已識別之營運資訊安全、法律與法規要求的風險評鑑方法論。
   - 發展風險接受的準則，並識別風險可接受的等級。
   - 所選擇的風險評鑑方法應確保風險評鑑產生可比較以及可再產生的結果。
4. 識別各項風險。
   - 識別資訊安全管理系統範圍內的各項資產及其擁有者[4]。
   - 識別對該等資產的各項威脅。
   - 識別此等威脅可能利用的各項脆弱性。
   - 識別對此等資產可能造成機密性、完整性及可用性之損失的各項衝擊。
5. 分析與評估各項風險。
   - 評估安全失效時可能對組織造成的營運衝擊，並將資產的機密性、完整性及可用性之損失的後果納入考量。
   - 根據最常見的威脅、脆弱性及與此等資產有關的衝擊，以及現行實作的控制措施，來評估此種安全失效發生的實際可能性。
   - 估計各風險之等級。
   - 決定風險是否可接受或使用風險接受準則來處理。
6. 識別並評估風險處理之各種選項做法。
   - 採用適當的控制措施。
   - 若符合組織的政策與風險接受準則，則客觀地接受此等風險。
   - 迴避風險。
   - 轉移相關的營運風險至第三方，例如：保險公司、供應商。
7. 選擇各項風險之處理的控制目標與控制措施。
   - 應選擇並實作控制目標與控制措施，以符合由風險評鑑和風險處理過程所識別的各項要求，應考量風險接受準則，以及法律、法規與契約的要求。
8. 取得管理階層對所提議之各項剩餘風險的核准。
9. 取得管理階層對實作和運作資訊安全管理系統的授權。
10. 擬定適用性聲明書。
    - 所選擇之各項控制目標與控制措施，以及其選擇的理由。
    - 目前已實作的各項控制目標與控制措施。
    - 所排除的各項控制目標與控制措施及其被排除的衡量理由。

[4] 「擁有者」指的是負有被認可管理責任的個人或個體，其控制資產的維護、使用及安全，而非指該人員實際上對該資產有任何財產權。

以上執行程序都必須符合 ISO 27001 的文件化要求，如圖 2-4 所示，並依循文件管理與記錄管制的程序。文件化應包括管理階層決策的紀錄，確保各項措施可追溯至管理階層決策及政策，且所記錄的結果是可再產生的(Reproducible)，同時也能夠展示從所選擇的控制措施回溯到和風險評鑑與風險處理過程之結果間的關係。

資訊安全管理系統文件化應包括如下：

- 資訊安全管理系統政策與各項目標之已文件化聲明。
- 資訊安全管理系統之範圍。
- 支援資訊安全管理系統之各項程序及控制措施。
- 風險評鑑方法論的描述。
- 風險評鑑報告與風險處理計畫。
- 組織為確保有效規劃、運作及控制其資訊安全過程，以及描述如何量測控制措施的有效性所需之文件化程序。
- 適用性聲明書。

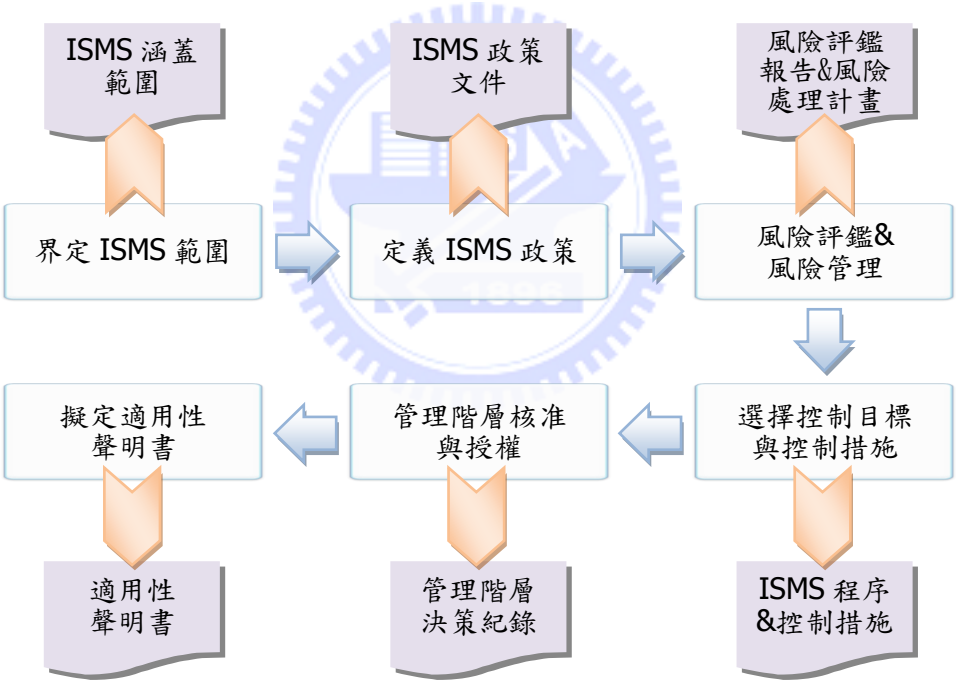

圖 2-4 資訊安全管理系統的建置流程

資料來源：ISO/IEC 27001:2005，本研究整理

根據相關研究與經驗顯示，組織的資訊安全管理成功與否，常繫於以下幾點關鍵要素：

- 能反映營運目標的資訊安全政策、目標及活動。
- 與組織文化一致的實作、維持、監視及改進資訊安全的做法與架構。
- 所有層級之管理階層的支持和承諾。

- 對資訊安全要求、風險評鑑以及風險管理的充分理解。
- 向全體人員及其他各方有效推廣資訊安全，分發並宣傳資訊安全政策和各項標準的指引。
- 提供適當的認知、訓練及教育。
- 建立有效的資訊安全事件管理程序。
- 建置量測系統以評估資訊安全管理的績效及回饋建議，以便改進。

ISO 27001 的驗證規範分成 11 大控制要項、39 個控制目標以及 133 項控制措施，如表 2-1 所示。

表 2-1 ISO 27001 控制措施項目統計

控制要項	控制目標	控制措施(項)
A.5 安全政策	A.5.1 資訊安全政策	2
A.6 資訊安全組織	A.6.1 內部組織	8
	A.6.2 外部團體	3
A.7 資產管理	A.7.1 資產責任	3
	A.7.2 資產分類	2
A.8 人力資源安全	A.8.1 聘僱之前	3
	A.8.2 聘雇期間	3
	A.8.3 聘僱的終止或變更	3
A.9 實體與環境安全	A.9.1 安全區域	6
	A.9.2 設備安全	7
A.10 通訊與作業管理	A.10.1 作業程序與責任	4
	A.10.2 第三方服務交付管理	3
	A.10.3 系統規劃與驗收	2
	A.10.4 防範惡意碼與行動碼	2
	A.10.5 備份	1
	A.10.6 網路安全管理	2
	A.10.7 媒體的處置	4
	A.10.8 資訊交換	5
	A.10.9 電子商務服務	3
	A.10.10 監控	6
A.11 存取控制	A.11.1 存取控制的業務需求	1
	A.11.2 使用者存取管理	4
	A.11.3 使用者責任	3

	A.11.4 網路存取控制	7
	A.11.5 作業系統存取控制	6
	A.11.6 應用程式與資訊存取控制	2
	A.11.7 行動運算與遠距工作	2
A.12 資訊系統獲得、開發與維護	A.12.1 資訊系統的安全需求	1
	A.12.2 應用程式的正確處理	4
	A.12.3 密碼控制措施	2
	A.12.4 系統檔案的安全	3
	A.12.5 開發與支援過程的安全	5
	A.12.6 技術脆弱性管理	1
A.13 資訊安全事件管理	A.13.1 報告資訊安全事件與弱點	2
	A.13.2 資訊安全事件與改善管理	3
A.14 營運永續管理	A.14.1 營運永續管理的資訊安全層面	5
A.15 遵循性	A.15.1 遵循適法性要求	6
	A.15.2 遵循安全政策、標準和技術符合	2
	A.15.3 資訊系統稽核考量因素	2

ISO 27001 的 11 大控制要項在建置資訊安全管理系統的順序關係上，如圖 2-5 所示。

圖 2-5 ISO 27001 控制要項關係圖

資料來源：BSI 英國標準協會(2007)

以 ISO 27001 建立、實施、操作、監督、審查、維持與改善資訊安全管理系統時，我們可將其控制要項分為「策略面」、「管理面」以及「作業面」，方便組織各負責單位的執行，如圖 2-6 所示。其中安全政策、營運永續管理及遵循性屬於「策略面」，必須符合組織的發展目標；資訊安全組織、資產管理、人力資源管理及資訊安全事件管理屬於「管理面」，著重於一般日常的營運管理；實體與環境安全、通訊與作業管理、存取控制及資訊系統開發與維護屬於「作業面」，與資訊安全技術的關聯性較高。

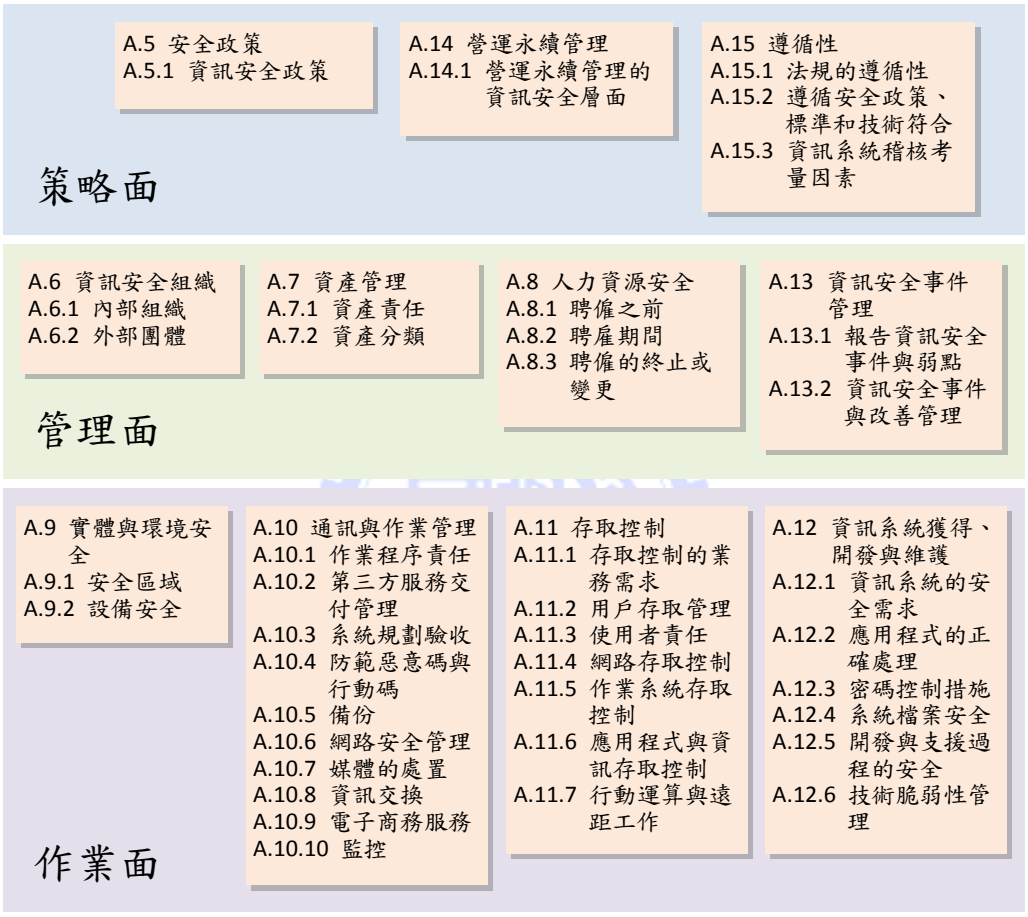

圖 2-6 ISO 27001 控制要項與控制目標分類

資料來源：查士朝(2006)

許多資訊系統並未設計得夠安全，透過技術手段可達成的安全性亦有限，因此應藉由適當的管理與程序來支援，規劃過程應注意細節以識別有哪些適合的控制措施可供組織採行。資訊安全管理的最低要求是組織內所有員工的參與，也需要股東、供應商、第三方、客戶或其他利害關係人的參與，可能也需要外部專家的建議，以共同建構安全的資訊環境。

2.4 風險評鑑

風險評鑑是建構資訊安全管理系統的重要環節，組織有必要識別其各項安全要求，各項安全要求皆有三個主要來源：

- 風險評鑑(Risk Assessment)：考量組織整體的營運策略及目標，經由風險評鑑能識別資產所面臨的各項威脅，並能評估各項脆弱性及其發生的可能性，進而估計可能造成的衝擊。
- 法令規章：組織、交易夥伴、承包商及服務供應商必須滿足法律、法令、法規及契約的各項要求，並符合社會文化環境的期望。
- 組織原則：組織為了支持其營運活動而發展的資訊處理原則、目標及營運要求。

各項安全要求透過具體方法的風險評鑑識別，風險評鑑的結果有助於引導及決定適當的管理行動和優先順序用以管理資訊安全風險，以及用以實作為防範這些風險所選擇的控制措施，施行控制措施的花費與安全失效後可能造成的營運損失需相稱。

資訊安全風險評鑑的執行效果，對於資訊安全管理系統的建置有決定成敗的影響性，風險評鑑透過分析組織資訊資產的重要程度、潛在的威脅、弱點發生的機率以及現有的控制措施來決定組織的各項資訊資產風險值，風險程度關係圖如圖 2-7 所示。

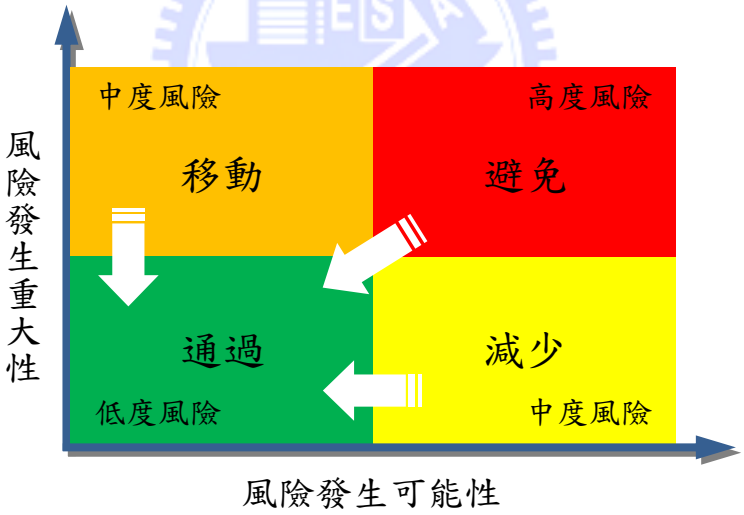

圖 2-7 風險程度關係圖

資料來源：經濟部標準檢驗局(2006)

風險發生的重大性(風險值)及風險發生的可能性評估計算公式如下(李慧蘭，2006)：

- 風險值 = 資產價值 × 破壞事件嚴重程度
- 資產價值 = 機密性評價 + 完整性評價 + 可用性評價
- 破壞事件嚴重程度 = 威脅等級 × 脆弱點等級 × 衝擊等級
- 風險可能性 = 發生機率 / 目前實施狀況

資產價值在於對資訊資產在「機密性」、「完整性」及「可用性」三方面做出評估，瞭解各項資訊資產對組織整體的重要性，接著執行組織風險衝擊性分析，對潛在的威脅作弱點及衝擊性探討，威脅與弱點評估著重於假設情境的模擬，以瞭解風險危機的嚴重程度，根據分析的結果，可以得知各項資訊資產在意外發生時對組織造成傷害的影響層面。威脅、弱點與風險的相互關係如圖 2-8 所示。

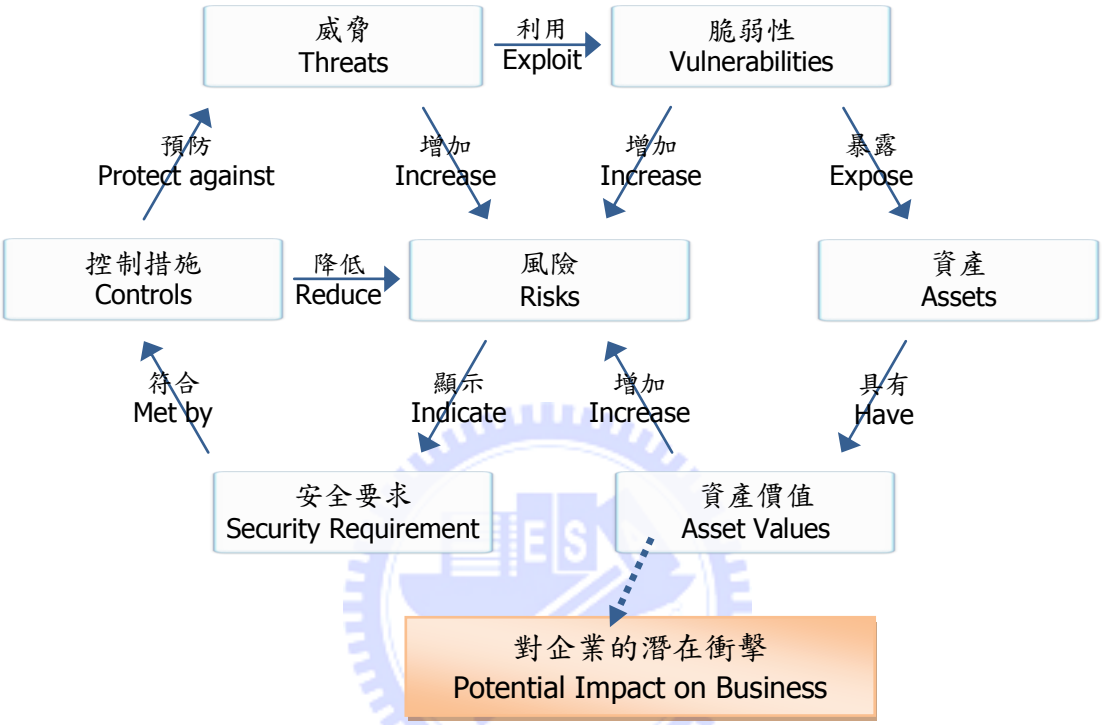

圖 2-8 威脅、弱點與風險關係圖

資料來源：BSI 英國標準協會(2007)

風險評鑑應依風險接受和與組織相關的目標等準則，識別、量化各項風險，並排定其優先順序，風險評鑑結果將作為指導與決定用以管理資訊安全風險、實作防止該等風險所選定的控制措施。評鑑風險與選擇控制措施的過程可能需要履行數次，以涵蓋組織或個別資訊系統的不同部分。風險評鑑應包括估計風險大小的系統性做法(風險分析)，及將預估風險與風險準則作比較以決定風險的顯著性(風險評估)之過程。

風險評鑑應定期重覆進行，以因應安全要求的變更及風險情況的變化等任何可能影響風險評鑑結果的改變，例如：資產、威脅、脆弱性、衝擊、風險評估等變更，並於顯著變更發生時立即執行風險評鑑。風險評鑑應以有條理的方式進行，才能產出可比較與可重製的結果，資訊安全風險評鑑應有明確界定的範圍以具有效性，同時與其他領域中風險評鑑保持關連性的關係。

只要是實用及有幫助的，風險評鑑的範圍可為整個組織、部分組織、個別資訊系統、特定的系統組件或服務。風險評鑑後識別出的各項風險，均需做風險處理決策，作為組織決定是否接受風險的判定準則，此決策應加以記錄，例如，若評鑑為低風險或處理風險的成本對組織不符成本效益時，風險可能被接受。

風險處理的可能選項包括：

- 採用適當的控制措施以降低各項風險。
- 若風險滿足組織之政策與風險接受準則，則接受此等風險。
- 藉由防止風險發生的行動以避免風險。
- 轉移相關風險至第三方，例如：保險公司或供應商。

對於部分風險根據風險處理決策，採取某些適當控制措施應符合風險評鑑所識別的要求，控制措施應考量下列因素，確保風險降低至可接受程度：

- 國家、國際之法律與法規的要求與限制條件。
- 各項組織目標。
- 各項運作要求與限制條件。
- 風險降低的相關運作成本必需根據組織之要求與限制條件。
- 投入各項控制措施的運作成本和安全失效可能導致的傷害兩者之間需取得均衡。

資訊安全控制措施應在系統與專案的需求規格與設計階段考量，然而沒有任何一套控制措施可達到完全的安全，必須透過額外的管理行動以監控、評估及改進安全控制措施的效率與有效性，以支援組織的目標。

2.5 我國資訊安全發展現況

中華民國的標準規範大多依循國際標準組織所公佈的標準作為制定國家標準(Chinese National Standard，CNS)的範本，CNS 27001 與 CNS 27002 為我國施行資訊安全管理的國家標準，經濟部標準檢驗局參考國際標準組織的 ISO 27001「Information Technology – Security Techniques – Information Security Management Systems – Requirements」，制定國家標準 CNS 27001「資訊技術－安全技術－資訊安全管理系統-要求事項」；參考 ISO 27002「Information Technology – Security Techniques – Code of Practice for Information Security Management」，制定 CNS 27002「資訊技術－安全技術－資訊安全管理之作業規範標準」。

為建立我國整體資訊安全防護、識別與回復的能力，行政院國家資訊基礎建設(National Information Infrastructure，NII)專案推動小組於 1995 年成立，負責資訊應用資料方面的安全相關規劃作業，經審慎的研擬，於 2001 年 1 月 31 日召開「國家資通安全會報」第一次會議，積極推動資通安全基礎建設工作，正式開啟我國資訊安全發展的新

頁。國家資通安全會報的組織運作架構如圖 2-9 所示，其中標準規範工作組負責訂定規畫資訊安全相關的標準與規範，主要職掌工作如下：

1. 訂定資通安全技術標準。
2. 訂定各機關辦理資通安全有關作業規範。
3. 規劃建置資通安全驗證方法。
4. 規劃建置資通安全認證程序。

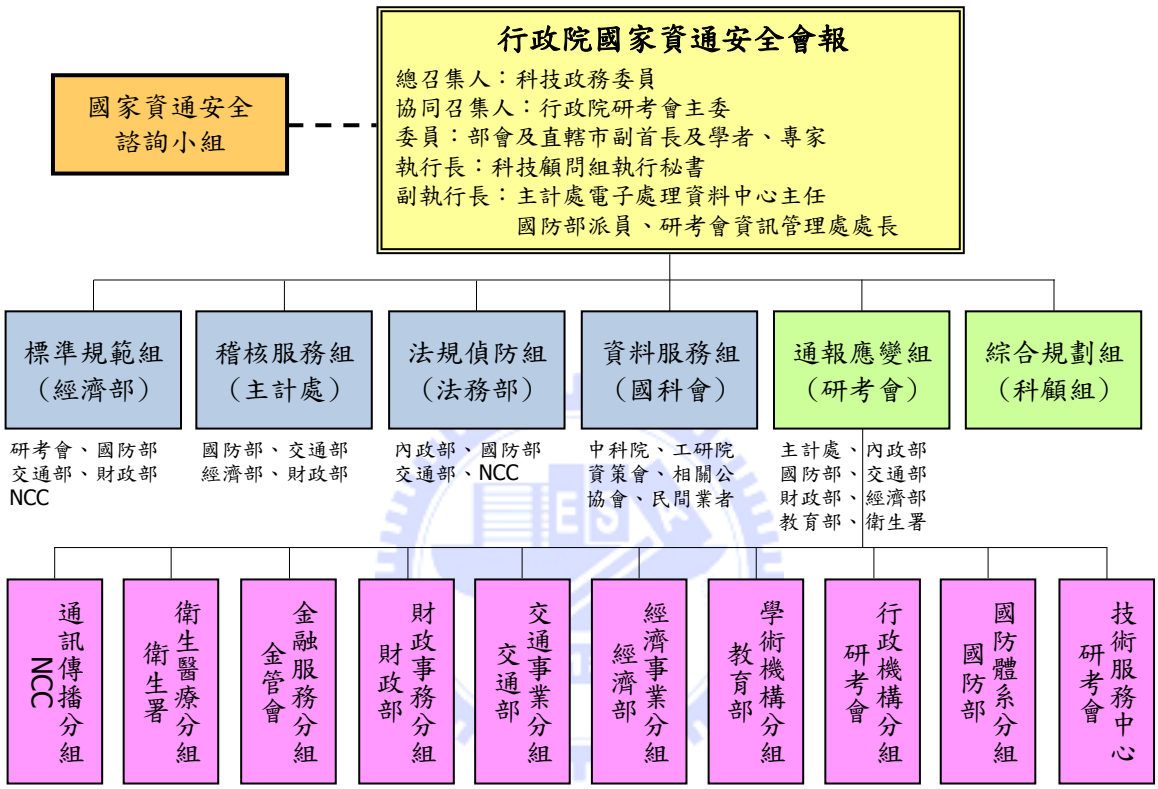

圖 2-9 國家資通安全會報組織架構

資料來源：行政院國家資通安全會報(2009)

行政院國家資通安全會報推動資訊安全基礎建設與建立資訊安全防護體系，為明確各政府機關的資訊安全責任等級分級作業與流程，特別訂定「政府機關（構）資訊安全責任等級分級作業施行計畫」與「各政府機關（構）落實資安事件危機處理具體執行方案」，將全國 3713 個政府機關依「國防體系」、「行政機構」、「學術機構」以及「事業機構」分組，並就各機關單位區分「A、B、C、D」四等級，賦予不同的資訊安全要求，期以透過有效的資訊安全管理，進而全面提升國家資通安全防護水準，其中明文規定 A 與 B 等級的政府機關，其資訊安全管理系統必須通過 ISO 27001 認證。首先透過評估資訊資產價值與其潛在影響，明確定義分級的內容，如表 2-2 所示，依機構屬性進行分級，分級後依據作業施行計畫執行該等級所賦予的工作事項，如表 2-3 所示，同時要

求各機關單位建立資訊安全長(Chief Information Security Officer，CISO)責任制度，確實掌握重點資訊資產，做好資訊安全防護的工作。

表 2-2 資訊資產價值等級分類

級別	分類內容	潛在影響等級
A 級 (重要核心)	違反資訊安全保護政策，會對**國家安全**之重要機敏資訊或系統等造成工作營運停頓或嚴重之損害，影響**業務推動持續一個月(含)以上**之損害。	極高度
B 級 (核心)	違反資訊安全保護政策，會對**社會秩序、民生體系運作及民眾隱私**之機敏資訊或系統，影響**業務推動持續一星期(含)以上**之損害。	高度
C 級 (重要)	違反資訊安全保護政策，會對**地方縣市級之社會秩序、人民生命財產**之重要資訊或系統，影響**業務推動持續一天(含)以上**之損害。	中度
D 級 (一般)	違反資訊安全保護政策，造成意外的事件不影響業務工作或營運。	低度

資料來源：國家資通安全會報(2005)，本研究整理

表 2-3 資訊安全系統等級執行工作事項

作業名稱 / 內容 / 等級	防禦機制強度	防護深度	ISMS 推動作業	稽核方式	資安教育訓練(主官、主管、技術、一般)	專業證照
A 級 (重要核心)	強度 等級 4	NSOC 防護/ 自建 SOC、 IDS、 防火牆、防毒	2007 年通過 第三者 認證	每年至少 執行二次 內稽	每年至少 (4,6,18,4 小時)	2007 年 資安專業 鑑定二張
B 級 (核心)	強度 等級 3	SOC(Optional) 、IDS、 防火牆、防毒	2008 年通過 第三者 認證	每年至少 執行一次 內稽	每年至少 (4,6,16,4 小時)	2007 年 資安專業 鑑定一張
C 級 (重要)	強度 等級 2	IDS、 防火牆、防毒	各單位自行 成立推動小 組規劃作業	自我檢視	每年至少 (2,6,12,4 小時)	資安專業 訓練
D 級 (一般)	強度 等級 1	防火牆、防毒	推動 ISMS 觀念宣導	自我檢視	每年至少 (1,4,8,2 小時)	資安專業 訓練

資料來源：國家資通安全會報(2005)

表 2-3 中，資訊安全防禦機制強度等級(Strength Mechanism Level，SML)分類說明如下：

- 強度等級 1：經由良好的資訊安全作業可達成的基本強度，用以防衛不複雜的威脅，應能保護低價的資訊資產。
- 強度等級 2：中等強度，可以抵抗諸如個人發動之攻擊活動的複雜威脅，能夠保護中等價值的資訊資產。
- 強度等級 3：高強度，用以防禦來自駭客組織的威脅，能夠保護高價值的資訊資產。
- 強度等級 4：極高強度，用以防禦來自國家級的威脅，能夠保護極高價值的資訊資產。

2.6 相關研究文獻

資訊安全管理標準的演進從 BS 7799 到 ISO 17799 再到今日的 ISO 27001 與 ISO 27002，國內、外相關文獻亦隨著版本的更新，持續研究探討這項標準所帶來的影響、成效及運用層面。國外文獻大多著重於論述 ISO 27001 的重要性及其影響力，未見以 ISO 27001 來評估相關產業或企業的案例，而國內論文有不少 BS 7799/ISO 27001 之個案研究的發表，大多以探討醫療體系、政府機關、軍事單位與金融機構為主。

Ezingeard 與 Birchall 探討「Information Security Standards: Adoption Drivers；What drives organisations to seek accreditation? The case of BS 7799-2:2002」，該研究發現競爭優勢是驅使企業主動採用資訊安全標準的最主要原因，同時也發現一個很重要的驅使因素是，組織採用國際標準來執行資訊安全管理的最佳典範，藉此促進外部關係以及與內部關係人溝通。反倒是法令規章的要求、資訊安全團體的推動、政府及貿易組織等並非是顯著的驅動因素，有別於一般的認知。

Jayawickrama 探討「Managing Critical Information Infrastructure Security Compliance: A Standard Based Approach Using ISO/IEC 17799 and 27001」，該研究建議流程控制系統(Process Control System)以 ISO 27001 標準為資訊安全管理系統的架構，以確保此一全面性且系統性的方法能與業務目標及組織風險管理計畫結合在一起。

Humphreys 探討「Information security management standards: Compliance, governance and risk management」，該研究說明管理資訊安全(Managing Information Security)相對於資訊科技安全(IT Security)，過去的安全主要是由資訊部門與技術專家所負責的工作，不過在資訊安全管理標準 BS 7799 出現之後，除了資訊科技之外，安全也關聯到了人、流程與資訊。

曾淑惠探討「以 BS 7799 為基礎評估銀行業的資訊安全環境」，分析本國銀行及外商銀行在資訊安全方面的運用現況，該研究發現：本國銀行及外商銀行在資訊安全運用

上最重視的三個控管要點依序為「存取控制」、「實體與環境安全」與「系統開發與維護」，而最需要加強是「安全組織」、「遵行」、「安全政策」方面的運用。

林曙熙探討「企業資訊安全管理之認知與實施研究」，該研究結論歸納：唯有在組織管理階層正確之理念下，方能制定出合宜的政策與方針，在目標引導下經由教育訓練之實施，以提昇組織全體成員安全意識，進而共同參與系統之建置與維護，最終依據階段式目標，以漸進方式建構符合企業個別需求的安全管理系統。

侯皇熙探討「植基於 BS 7799 探討政府部門的資訊安全管理 ─ 以海關資訊部門為例」，在 BS 7799 運用現況方面，該研究發現：海關在資訊安全管理運用上比較重視的三個控制要項依序是「實體與環境安全」、「安全政策」與「組織安全」，而需要加強的是「資產分類與控制」、「企業永續管理」與「系統開發與維護」等方面的運用。

楊智翔探討「運用 CNS 17799 檢視醫療院所之資訊安全管理-以屏東地區大型醫院為例」，該研究發現：除了「應付客戶時的安全處理」與「線上交易」之外，CNS 17799 作業要點應可適合用於國內醫療產業檢視其資訊安全管理之作業現況。個案醫院在資訊安全管理上，比較重視的三個控制要項是「資訊安全管理事故」、「人力資源安全」與「資產管理」，而「通訊與作業管理」及「存取控制」則是最需要加強改進的兩個要項。

陳兆祺探討「導入 BS 7799 標準對建立資訊安全文化影響之經驗研究-以 Y 公司為例」，該研究發現：導入 BS 7799 標準對於資訊安全文化的發展有顯著影響，其中以「安全政策」對於資訊安全文化整體發展的影響最重要；導入 BS 7799 資訊安全管理制度對於資訊安全認知與責任的建立、反應與應變能力的強化、安全設計與執行上與存取控管的落實以及資訊倫理的內化等方面，皆有明顯的成效。

李仁暉探討「台灣金融業導入資訊安全管理系統關鍵成功因素研究-以 A 金控為例」，該研究發現：高階主管的全力支持並參與運作、專責的資訊安全管理單位與顧問經驗豐富並提供過去導入的經驗法則在所有階段均重要，其他因素僅在部分階段為關鍵成功因素。另外該研究顯示具有完善的資訊安全防禦設備與具備資訊安全專業技能的資訊安全人員等技術層面因素，並非導入資訊安全管理系統之關鍵因素。

本研究參考的相關資料眾多，族繁不及備載，上述所列之文獻與本研究主題皆屬資訊安全管理領域，雖然研究的方向與本研究並不相同，探討的對象也非電信產業，然而其研究內容與成果提供予研究者對於資訊安全管理有更全面且深入的瞭解，讓研究者在構思研究架構、設計研究方法、研擬實地訪查與動筆撰寫的過程中，不斷激盪出許多心得與想法，並持續做深入的思考，使得本研究更臻完善。

第三章 研究方法

本章旨在說明所採行的研究方法，共分為五節。3.1 節介紹質性研究法並說明本研究採用個案研究法的理由；3.2 節敘述研究方法的設計及所遵循的研究程序；3.3 節介紹本研究的個案業者並解釋資料蒐集的方式；3.4 節建立以「ISO 27001」為基礎的檢驗評核表；最後，3.5 節說明本研究的研究範圍與限制。

3.1 研究方法的選擇

社會科學之研究方法種類繁多，主要可分為量化研究法(Quantitative，或稱定量研究)與質性研究法(Qualitative，或稱定性研究)，兩種研究方法都是為了探討問題背後的事實及原因，各有其適用的時機。量化研究法沿襲了自然科學的研究，透過量化的模型推演，能夠客觀地得到結論，然而，社會現象遠比自然現象來得複雜，事件發展的過程中涵蓋許多的變數，所處理的表象是隨時間動態演變的，也因此量化研究的結果難以充分解釋社會的複雜現象，此外，社會科學的研究需要研究者實地的去查訪觀察，才能得知其中細微的關鍵因素，因此本研究主題實有必要採取質性的研究方法，以利深入瞭解國內第一類電信業者在資訊安全管理的實際情況。

質性研究法的特性使其在與理論的關係、資料來源與蒐集方式皆與定量研究法迥異，質性研究法認為社會現象無法使用單純的模型來解釋，因為現實世界是動態的環境，其中包含多種層面的意義與關係，彼此之間相互影響，因此質性研究的價值在於發現(Discovery)而非驗證(Verification)，研究事先並不作理論架構或假設，根據實際的資料彙整歸納，加上對研究主題的先前理解(Pre-understanding)進行詮釋與修正，最後賦予整體意義。本研究衡量與觀察的對象是社會實際發生的現象，因此研究者以自然主義[5](Naturalistic)的方式蒐集資料，觀察所要研究的對象，不作任何情境的操弄或設計，主要是以半結構訪談加上實地查察的方式，深入探討少數個案。

本研究彙整 ISO 27001 以及其指導原則 ISO 27002 的主要內容，參考李克特總加量表法(Likert scale)，依據 ISO 27001 的控制要項、控制目標與控制措施設計出四分量表，並運用 ISO 驗證稽核的方式進行探討，過去國內資訊安全管理領域與相關研究論文多集中於醫療體系、政府機關、軍事單位與金融機構，尚未見到關於電信產業的研究，因此本研究議題於本質上屬於質性研究法。

[5] 自然主義是一種古老的質性研究傳統，是田野調查的一種類型，其假設是客觀的社會實體真實地存在，其能夠觀察與正確地記錄(Babbie, 2007)。

各項研究議題皆可採取不同的研究策略，不同的研究策略會造成研究方向與研究深度的差異，因此應審慎衡量不同的研究問題特徵，選擇適當的研究策略，表 3-1 為質性研究法的策略選擇原則，在五種質性研究方法中，依「研究問題的型態」、「對行為事件的控制要求」與「是否著重於當代事件」為考量，從中選擇適合的研究方法。根據本研究設計的評核表與訪談稽核方式，絕大多數屬於「How」與「Why」的問題類型，且遵循質性研究自然主義的精神之下，不需要(也不容易)針對某一行為事件進行控制，此外本研究探討個案業者當下的現況，一般的次級資料無法完全闡明其運作情形，必須藉由研究者實地親訪方能瞭解實際的情況，綜合以上條件，「個案研究法」是本研究主題最理想的研究方法，藉由實地訪查能夠得到接近事實的資料，並洞察其中的相互關係。

表 3-1 質性研究法的劃分與研究策略選擇

研究方法	研究問題的型態	對行為事件的控制要求	是否著重於當代事件
實驗法 (Experiment)	How、Why	是	是
調查法 (Survey)	Who、What、Where、How Many、How Much	否	是
檔案分析法 (Archival Analysis)	Who、What、Where、How Many、How Much	否	是/否
歷史研究法 (History)	How、Why	否	否
個案研究法 (Case Study)	How、Why	否	是

資料來源：Yin(2002)

3.2 研究方法設計與程序

任何一種研究方法所產生的研究結果，均應允許另一位獨立的研究者驗證其結果，與量化的研究方法一樣，個案研究法亦不例外，必須重視研究的品質，而非任由個人主觀的意見造成事實真相的扭曲，因此同時兼顧效度與信度的研究過程關鍵在於事先研究方法的設計，這也是個案研究與一般新聞媒體報導的主要差異所在。個案研究方法必須是運用科學的方法，有系統地探究事實真相，欲提升個案研究的品質，應就「建構效度」、「內部效度」、「外部效度」與「信度」等四項社會科學研究品質的衡量標準，提出相關的個案研究策略，與其策略應用所相對應的各個發展階段，使整體研究設計趨於完善，如表 3-2 所示。

表 3-2 個案研究品質之衡量標準

衡量	提升品質的策略	策略的應用階段
建構效度 (Construct Validity)	● 使用多重證據來源 ● 建立一個證據鏈 ● 讓主要的資料提供者檢視個案研究報告初稿	→ 資料蒐集階段 → 資料蒐集階段 → 報告撰寫階段
內部效度 (Internal Validity)	● 採用類型比對法 ● 採用解釋建立法 ● 採用時間序列分析法	→ 資料分析階段 → 資料分析階段 → 資料分析階段
外部效度 (External Validity)	● 在多重個案研究中使用重複邏輯	→ 研究設計階段
信度 (Reliability)	● 使用個案研究計劃書 ● 發展個案研究資料庫	→ 資料蒐集階段 → 資料蒐集階段

資料來源：Yin(2002)

上述四項衡量標準的內容為：建構效度是用來建立正確的操作性衡量(Operational Measure)，使其能衡量所欲研究主題的真正現象，並歸納出具有意義的結論；內部效度則是強調研究者對於個案本身內容分析的推論過程之嚴謹性；外部效度是針對研究發現的結果是否能夠一般化的類推(Generalization)；信度是指重複相同的研究操作可得到相同研究結果的程度。

基於個案研究品質的要求，本研究採用個案研究法配合 ISO 27001 資訊安全管理系統的內涵，設計出四分量表作為評核的標準，透過與個案業者的深度訪談與實地查察，並輔以相關研究主題的文件與佐證資料，包括公司年報、公開說明書、公司簡介、公司網站、產品介紹、報章雜誌與網路媒體等相關資料，使其達到多重證據來源，同時相互參照並重覆勾稽，以維持證據的連鎖性，期可增加本研究的建構效度。

本研究於實地訪談前即針對個案業者著手建立資料庫，包括所蒐集到關於該公司的資料，作為日後訪談的基礎，而在訪談過程中，全程摘記重點，必要時覆述已記錄的重點內容，確認得到的訊息正確無誤，事後將訪談資訊依據資料類型，輸入已建立的資料庫中並做整理，期間若發現資訊不一致或需要再做確認之處，則尋求其他證據來源或透過電話與電子郵件的方式釐清及驗證，以維持證據邏輯的連貫，期能提升本研究的信度且增進建構效度。

本研究第四章的研究分析將以系統歸納方式，具體呈現個案業者實踐 ISO 27001 控制措施的現狀，並進行類型比對，探究個案業者的資訊安全系統管理之共通處或相異處，同時提出分析與解釋，如此期能提高本研究的內部效度。

外部效度往往成為個案研究結果的爭論之處，對於影響外部效度的因素，本研究採取多重個案的研究設計方式，以避免「個案研究是以少數個案為研究對象，難以作成一般化結論」的批評。同時利用個案研究重複邏輯的特性，將個案研究發現的資料反覆檢驗，並分析產業特性及個案業者屬性，促使研究成果之可類推化，達到增進外部效度的目標。

以上針對提升建構效度、信度、內部效度與外部效度的研究設計應可促進本研究的嚴謹程度，並達成提升個案品質的使命。

關於個案研究法的執行步驟，本研究遵循史丹佛大學教授 Eisenhardt 於 1989 年所整理的個案研究法之建構理論程序：定義研究問題、選擇個案、蒐集資料、實地查察、分析資料、形成假說、文獻參照與作出結論，如表 3-3 所示。

表 3-3 個案研究法的建構程序

程　序	行　動	原　因
開始 (Getting Started)	● 定義研究問題 ● 預擬一個可能的構思	→ 聚焦 → 提供較佳的構思衡量基礎
選擇個案 (Selecting Cases)	● 放棄理論與假設 ● 指定母體 ● 理論性抽樣(非隨機)	→ 保持理論的彈性 → 限制額外的變異，強化外部效度 → 聚焦在理論上有用的個案，例如：某些個案透過填補概念性種類來複製或延伸理論
開發工具與協定 (Crafting Instruments and Protocols)	● 多重資料蒐集方法 ● 整合質化與量化資料 ● 多個調查人員	→ 藉由證據的三角測量來強化理論的基礎 → 證據的協同作用觀點 → 培養多元的觀點與強化基礎
進入田野 (Entering the Field)	● 同時進行資料蒐集與分析，包括田野摘記 ● 彈性且伺機的資料蒐集方法	→ 加速分析與展現對資料蒐集有益的調整 → 允許調查人員利用新興的主題與獨特的個案特徵
分析資料 (Analyzing Data)	● 個案內分析 ● 使用多元的技術做跨個案型態調查	→ 獲得資料理解與建立初步的理論 → 要求調查人員跳脫初始印象並從多個角度觀察證據
形成假說 (Shaping Hypotheses)	● 為每一構思反覆表列證據 ● 跨個案複製邏輯(非抽樣) ● 尋找關係背後的原因之證據	→ 銳化構思定義、效度與可衡量性 → 確認、延伸並銳化理論 → 建立內部效度

文獻參照 (Enfolding Literature)	● 對照衝突的文獻 ● 對照類似的文獻	→ 建立內部效度，提升理論層次與銳化構思定義 → 銳化可歸納性，改善構思定義與提升理論層次
作出結論 (Reaching Closure)	● 在可能的情況下讓理論飽和	→ 在邊際進展有限的情況下，終止研究流程

資料來源：Eisenhardt(1989)

3.3 個案業者與資料蒐集

本章第二節曾說明將採取多重個案的研究設計方式以提升外部效度，本研究探討對象為國內電信業者，而國內電信事業分為第一類與第二類電信事業，一般而言，第一類電信業者的規模相較於第二類電信業者為大，業務性質也較為複雜，此外，第一類電信業者經營的業務範圍涵蓋固網通信、有線電視、2G 行動電話、3G 行動通信、無線寬頻接取行動通信(WiMAX)、數位式低功率無線電話(PHS)、無線電、衛星通信及國際海纜…等，為使研究結果具有代表性及完整性，研究者嘗試從不同業務領域的第一類電信業者中尋求適當的研究對象，考量我國固網通信、行動通信與有線電視的高普及率，因此挑選出五家相關業者作為個案研究的對象，其中 T 公司與 V 公司是行動通信業者的代表，S 公司與 A 公司可代表固網通信業者，W 公司則為有線電視業者的代表。表 3-4 為個案業者的基本資料彙整，從基本資料可以發現，研究的樣本個案間有相似之處，但亦有各自獨特的地方，可作為日後資料分析時比對的基礎。

表 3-4 個案業者之基本資料

公司	成立時間	實收 資本額	2008 年 營收	主要 經營業務	員工人數
T 公司	1997 年	380 億	543 億	2G/3G 行動通信	2000
S 公司	2000 年	400 億	69.4 億	固網通信	850
A 公司	2000 年	328 億	143 億	固網/行動通信	1400
V 公司	2000 年	195 億	44 億	3G 行動通信	900
W 公司	1996 年	4.58 億	4.73 億	有線電視	100

資料來源：個案業者，本研究彙整

在資料蒐集方面，Yin(2002)曾整理過去文獻，歸納出「相關文件」、「歷史檔案」、「深入訪談」、「直接觀察」、「參與觀察」與「實體產出」等六種個案研究的資料蒐集方法，並且進一步說明各種不同資料蒐集方法的優、缺點，如表 3-5 所示。

資料蒐集方式的主要考量在於，單獨的相關文獻或歷史資料過於瑣碎，往往形成資料內容在廣度與深度上有明顯的抵換關係，無法兩全其美，造成主題無法聚焦；至於評估電信業的資訊安全管理，採取直接觀察或間接觀察有其困難度，因為研究過程中必須投入大量時間與資源，個案業者難以同意這樣的研究方式作為提供研究者的資料來源；因此本研究以深入訪談的方式作為資料蒐集來源。本研究之受訪者皆為個案業者負責資訊安全管理的部門主管或員工，現場訪談時依據本章第四節所建立的評核表為訪談基礎，以開放式問題瞭解該公司執行資訊安全管理的情況，若該公司宣稱其符合評核表上的評估內容，則輔以實地查察加以確認，例如針對「A.9.2.7 財產的攜出」提出詢問：貴公司如何控管財產攜出？依據其回覆的施行方式，然後實地進行驗證。

表 3-5 六種資料蒐集方法之優缺點分析

資料蒐集方法	優點	缺點
相關文件 (Documentation)	➢ 資料能重複檢視 ➢ 不會膨脹個案研究結果 ➢ 能夠對於事件內的參考資料提供確切的名稱 ➢ 可以涵蓋過去長期的時間範圍	➢ 資料對於研究主題意義不大，過於瑣碎 ➢ 可能發生選擇性的偏誤 ➢ 可能發生文件作者的偏誤 ➢ 可能發生文件窗飾的偏誤
歷史檔案 (Archival Record)	➢ 同相關文件 ➢ 提供大量訊息	➢ 同相關文件 ➢ 除非透過私人關係，否則不易接近
深入訪談 (Interview)	➢ 直接針對研究主題聚焦 ➢ 資料本身較為深入，較易察覺問題彼此間的因果推論	➢ 非結構性問題可能產生偏誤 ➢ 受訪者有意的窗飾事實 ➢ 受訪者回憶的不確實性
直接觀察 (Direct Observations)	➢ 實際觀察整個事件發生經過 ➢ 較能掌握事件發生的脈絡	➢ 必須耗費相當的時間與資源 ➢ 往往無法全程觀察，只能做選擇性觀察 ➢ 受訪者基於事件被觀察，而有別於真實的運作過程
參與觀察 (Indirect Observations)	➢ 同直接觀察 ➢ 對於互動者彼此的行為動機將會有較深層的瞭解	➢ 同直接觀察 ➢ 研究者的參與，造成對真實的運作過程產生偏誤
實體產出 (Physical Artifacts)	➢ 對於整個文化特徵會有較深層的瞭解 ➢ 對於整個專業上的操作會有較深層的瞭解	➢ 選擇性 ➢ 可接近性

資料來源：Yin(2002)

3.4 建立 ISO 27001 為基礎之評核表

ISO 27001 的控制要項涵蓋了「安全政策」、「資訊安全組織」、「資產管理」、「人力資源安全」、「實體與環境安全」、「通訊與作業管理」、「存取控制」、「資訊系統獲得、開發與維護」、「資訊安全事件管理」、「營運永續管理」、「遵循性」等 11 項範圍，若依此評估驗證個案業者的資訊安全管理施行現況，則應建立評核表以利執行訪談與實地查察的作業。因此根據 ISO 27001 的 11 大控制要項、39 個控制目標與 133 項控制措施，同時運用李克特總加量表法之四等級模式，進而發展成如表 3-6 之四分量表，評核表的題號編排直接參照 ISO 27001 之控制要項、控制目標與控制措施的編號，不再另行編碼。

過去以 BS 7799/ISO 27001 探討產業或組織之資訊安全管理的相關文獻，其問卷或評量表的設計以五分量表者，評分的五等級標準為：已完成、部分完成、建置中、規劃中與未考慮；以四分量表者，評分的四等級標準為：非常適當、適當、不適當與極不適當。本研究評核表之設計有別於其他文獻的評等方式，為符合 ISO 標準的精神，定義四分量表的四等級評量標準為：完全符合、次要缺失、主要缺失與不符合，具體呼應 ISO 27001 稽核驗證的方式與準則。

本研究的評估模式係以 ISO 27001 之資訊安全管理系統的要求事項為評核依據，其相關評核作業的標準定義如下：

1. 評核方式：

   依據表 3-6 之「ISO 27001 資訊安全管理系統評核表」作為訪談以及實地查察的基礎，並就評核結果與事實發現於評核表上作勾選記錄。其中，「列入核心版」欄位是受訪者根據其主觀意識及實務經驗答覆，作為發展電信產業之 ISO 27001 核心版的基礎。

2. 評核量化：

   評核量化之依據採稽核驗證的方式，其界定標準與評分準則如下：

   - 完全符合：符合控制措施的內容精神與要求，作業、流程與文件皆完整、完善，量化值為 3 分。
   - 次要缺失：符合控制措施的內容精神與要求，部分作業、流程與文件有輕微瑕疵，組織風險性程度屬於低度風險，量化值為 2 分。
   - 主要缺失：不完全符合控制措施的內容精神與要求，部分作業、流程與文件有重大瑕疵，組織風險性程度屬於中、高度風險，量化值為 1 分。
   - 不符合：完全不符合控制措施的內容精神與要求，亦缺乏相關作業、流程與文件，量化值為 0 分。

   若個案業者認為該控制措施不適用於其公司業之務性質，可予以忽略。例如：個案業者未提供電子商務，則對於「A.10.9 電子商務服務」之控制措施不進行訪查。

3. 核心版遴選：

受訪者依其建立、實作、監視、審查、維護及改善資訊安全管理系統的實務經驗，認為該控制措施足以列為核心版，則在「列入核心版」欄位進行勾選。為促使核心版的資訊安全管理建議具有專業級的可靠性，除受訪者的意見之外，同時也向兩位擁有 ISO 27001 主導稽核員(Lead Auditor)認證資格，且具備電信產業經驗的專家請益，經由訪談作意見之採納。

表 3-6 ISO 27001 資訊安全管理系統評核表

題號	評估項目	評估內容	評核				列入核心版
			不符合	主要缺失	次要缺失	完全符合	
A.5	安全政策						
A.5.1	資訊安全政策						
A.5.1.1	資訊安全政策文件	資訊安全政策文件應由管理階層核准，並公布傳達給所有員工與相關各外部團體。	□	□	□	□	
A.5.1.2	資訊安全政策之審查	資訊安全政策應依規劃之期間或發生重大變更時審查，以確保其持續的適用性、充分性及有效性。	□	□	□	□	
A.6	資訊安全組織						
A.6.1	內部組織						
A.6.1.1	管理階層對資訊安全的承諾	管理階層應在組織內藉由清楚的指示、展現的承諾、明確的指派及對資訊安全責任的確認，主動地支持安全。	□	□	□	□	
A.6.1.2	資訊安全協調工作	資訊安全活動應由組織內具有相關角色與工作功能之不同部門的代表協調。	□	□	□	□	
A.6.1.3	資訊安全責任的配置	應明確界定所有資訊安全責任。	□	□	□	□	
A.6.1.4	資訊處理設施的授權過程	應定義與實作對新資訊處理設施的管理階層授權過程。	□	□	□	□	
A.6.1.5	機密性協議	宜識別與定期審查反映組織對資訊保護之需求的機密性或保密協議要求。	□	□	□	□	
A.6.1.6	與權責機關的聯繫	應與相關權責機關維持適當聯繫。	□	□	□	□	
A.6.1.7	與特殊利害相關團體的聯繫	應與各特殊利害相關團體或其他各種專家安全性論壇及專業協會維持適當聯繫。	□	□	□	□	

A.6.1.8	資訊安全的獨立審查	應依所規劃的期間或當安全實作發生顯著變更時，獨立審查組織對管理資訊安全的做法與其實作(例如：資訊安全的各項控制目標、控制措施、政策、過程及程序)。	□□□□	
A.6.2	外部團體			
A.6.2.1	與外部團體相關的風險之識別	由涉及外部團體的營運過程產生對組織資訊及資訊處理設施之風險，應在核准外部團體存取之前加以識別，並實作適當的控制措施。	□□□□	
A.6.2.2	處理客戶事務的安全說明	在賦予客戶存取組織資訊或資產的權限之前，應闡明所有已識別的安全要求。	□□□□	
A.6.2.3	第三方協議中之安全說明	涉及存取、處理、通信或管理組織的資訊或資訊處理設施，或在資訊處理設施上附加產品或服務的與第三方之協議，應涵蓋所有相關的安全要求。	□□□□	
A.7	資產管理			
A.7.1	資產責任			
A.7.1.1	資產清冊	應明確識別所有資產，並製作與維持所有重要資產的清冊。	□□□□	
A.7.1.2	資產的擁有權	與資訊處理設施相關的所有資訊及資產應由組織指定的部門〝擁有〞。	□□□□	
A.7.1.3	資產之可被接受的使用	與資訊處理設施相關的資訊與資產，其可被接受的使用之規則應予以識別、文件化及實作。	□□□□	
A.7.2	資產分類			
A.7.2.1	分類指導綱要	資訊應依其對組織的價值、法律要求、敏感性及重要性加以分類。	□□□□	
A.7.2.2	資訊標示與處置	應依照組織所採用的分類法，發展與實作一套適當的資訊標示與處置程序。	□□□□	
A.8	人力資源安全			
A.8.1	聘僱之前			
A.8.1.1	角色與責任	員工、承包者及第三方使用者的安全角色與責任，應依照組織的資訊安全政策加以界定與文件化。	□□□□	
A.8.1.2	篩選	應依照相關法律、法規及倫理，並兼顧營運要求的相稱性、所存取資訊的保密類別及所察覺的風險，對所有聘僱之應徵者、承包者及第三方使用者的背景查證檢核(verification check)。	□□□□	

A.8.1.3	聘僱條款與條件	身為契約義務的一方，員工、承包者及第三方使用者應同意並簽署其聘僱契約之條款與條件，該契約應陳述其與組織對資訊安全的責任。	□□□□	
A.8.2	聘雇期間			
A.8.2.1	管理階層責任	管理階層應要求員工、承包者及第三方使用者，依照組織已制定的政策與程序施行安全事宜。	□□□□	
A.8.2.2	資訊安全認知、教育及訓練	組織所有員工和相關的承包者及第三方使用者，均應接受與其工作職務相關，以及定期更新的組織政策與程序內容之適切認知訓練。	□□□□	
A.8.2.3	懲處過程	對違反安全的員工，應有正式的懲處過程。	□□□□	
A.8.3	聘僱的終止或變更			
A.8.3.1	終止責任	執行聘僱終止或變更的責任應明確的界定與指派。	□□□□	
A.8.3.2	資產的歸還	所有員工、承包者及第三方使用者在其聘僱、契約或協議終止時，應歸還其擁有的所有組織資產。	□□□□	
A.8.3.3	存取權限的移除	所有員工、承包者及第三方使用者對資訊及資訊處理設施的存取權限，在其聘僱、合約或協議終止時，或因變更而調整時，均應予以移除。	□□□□	
A.9	實體與環境安全			
A.9.1	安全區域			
A.9.1.1	實體安全周界	應使用安全周界(諸如牆、卡控入口閘門或人員駐守的接待櫃檯等屏障)，以保護含有資訊及資訊處理設施的區域。	□□□□	
A.9.1.2	實體進入控制措施	安全區域應藉由適當的入口控制措施加以保護，以確保只有經授權人員方可允許進出。	□□□□	
A.9.1.3	保全辦公室、房間及設施	應設計辦公室、房間及設施的實體安全並施行之。	□□□□	
A.9.1.4	對外部與環境威脅的保護	應設計並施行實體保護，以避免遭受火災、洪水、地震、爆炸、民眾暴動及其它天然或人為災難的損害。	□□□□	
A.9.1.5	在安全區域內工作	應設計在安全區域內工作的實體保護與指導綱要，並施行之。	□□□□	

A.9.1.6	公共進出、收發及裝卸區	諸如收發與裝卸區及其他未經授權人員可進入作業場所之進出點宜加以控制；若可能，並宜與資訊處理設施隔離，以避免未經授權的存取。	□□□□	
A.9.2	設備安全			
A.9.2.1	設備安置與保護	應安置或保護設備，以降低來自環境之威脅與危害造成的風險，以及未經授權存取之機會。	□□□□	
A.9.2.2	支援的公用設施	應保護設備不受電源失效及其他支援的公用設施失效所導致的中斷。	□□□□	
A.9.2.3	佈纜的安全	應保護傳送資料或支援資訊服務之電源與電信佈纜，以防止竊聽或損害。	□□□□	
A.9.2.4	設備維護	應正確地維護設備，以確保其持續的可用性與完整性。	□□□□	
A.9.2.5	場所外設備的安全	安全應適用於場外設備的，並考慮其在組織場所外工作的各種不同風險。	□□□□	
A.9.2.6	設備的安全汰除或再使用	含有儲存媒體的設備，其所有項目在汰除前應加以檢核，以確保任何敏感性的資料與有版權的軟體已被移除或安全地覆寫。	□□□□	
A.9.2.7	財產的攜出	未經事前授權，設備、資訊或軟體不應帶出場外。	□□□□	
A.10	通訊與作業管理			
A.10.1	作業程序與責任			
A.10.1.1	文件化作業程序	操作程序應加以文件化、維持，並讓有需要的所有使用者均可隨時取得。	□□□□	
A.10.1.2	變更管理	對資訊處理設施與系統的變更應受控制。	□□□□	
A.10.1.3	職務的區隔	職務與責任領域應加以區隔，以降低組織資產遭未經授權或非意圖的修改或誤用之機會。	□□□□	
A.10.1.4	開發、測試及運作設施的分隔	應分隔開發、測試及運作之設施，以降低對運作之系統未經授權存取或變更的風險。	□□□□	
A.10.2	第三方服務交付管理			
A.10.2.1	服務交付	應確保包含於第三方服務交付協議內的安全控制措施、服務定義及交付等級已由第三方予以實作、執行及維持。	□□□□	
A.10.2.2	第三方服務的監視與審查	應定期監視與審查由第三方提供的服務、報告及紀錄，並定期執行稽核。	□□□□	

A.10.2.3	第三方服務變更的管理	所提供服務的變更，包括維持與改進現有的資訊安全政策、程序及控制措施均應加以管理，並考量所涉及之營運系統與過程的重要性以及風險的重新評鑑。	□□□□	
A.10.3	系統規劃與驗收			
A.10.3.1	容量管理	應監視、調諧(tune)各項資源的使用，並對未來容量要求預作規劃，以確保所要求的系統效能。	□□□□	
A.10.3.2	系統驗收	應建立新資訊系統、系統升級及新版本的驗收準則，並在開發期間與驗收前應實行適當之系統測試。	□□□□	
A.10.4	防範惡意碼與行動碼			
A.10.4.1	對抗惡意碼的控制措施	應實作防範惡意碼的偵測、預防及復原控制措施以及適切的使用者認知程序。	□□□□	
A.10.4.2	對抗行動碼的控制措施	行動碼若經授權使用，其組態應確保授權的行動碼係依據明確界定的安全政策在作業，並應防止執行未經授權的行動碼。	□□□□	
A.10.5	備份			
A.10.5.1	資訊備份	應依據所議定的備份政策，定期進行資訊與軟體的備份與測試。	□□□□	
A.10.6	網路安全管理			
A.10.6.1	網路控制措施	網路應適切地加以管理與控制，使其不受威脅，並且維護使用網路的系統與應用程式的安全，包括輸送中資訊。	□□□□	
A.10.6.2	網路服務的安全	應識別所有網路服務的安全特徵、服務水準及管理要求，並應被納入網路服務協議中，不論是此等服務是由內部或委外所提供。	□□□□	
A.10.7	媒體的處置			
A.10.7.1	可移除式媒體的管理	應有適當的程序以管理可移除式媒體。	□□□□	
A.10.7.2	媒體的汰除	媒體不再需要時，應使用正式程序加以安全地和無害地汰除。	□□□□	
A.10.7.3	資訊處置程序	應建立資訊的處置及儲存程序，以保護此資訊免於未經授權的揭露或誤用。	□□□□	
A.10.7.4	系統文件的安全	系統文件應加以保護，免遭未經授權的存取。	□□□□	

A.10.8	資訊交換			
A.10.8.1	資訊交換政策與程序	應備妥適當的正式交換政策、程序及控制措施，以保護經由使用所有型式通訊設施的資訊交換。	□□□□	
A.10.8.2	交換協議	組織與外部團體間資訊與軟體的交換應建立協議。	□□□□	
A.10.8.3	輸送中的實體媒體	應保護含有資訊的媒體在組織實體邊界外傳送時，不受未經授權的存取、誤用或毀損。	□□□□	
A.10.8.4	電子傳訊	電子傳訊涉及的資訊應適當地加以保護。	□□□□	
A.10.8.5	營運資訊系統	應發展與實作政策和程序，以保護與營運資訊系統互連有關的資訊。	□□□□	
A.10.9	電子商務服務			
A.10.9.1	電子商務	應保護在公眾網路上傳輸而涉及電子商務的資訊，使不受詐欺行為、契約爭議及未經授權的揭露與修改。	□□□□	
A.10.9.2	線上交易	應保護涉及線上交易的資訊，以防止不完整的傳輸、誤選路(mis-routing)、未經授權的訊息修改、未經授權的揭露、未經授權的訊息複製或重演。	□□□□	
A.10.9.3	公眾可用的資訊	應保護公眾可用系統上可取得資訊的完整性，以防止未經授權的修改。	□□□□	
A.10.10	監控			
A.10.10.1	稽核存錄	稽核日誌係記錄使用者活動、異常及資訊安全事件，宜產生與保留一段議定的期間，以協助未來的調查與存取控制監視。	□□□□	
A.10.10.2	監控系統的使用	應建立資訊處理設施使用的監視程序，並定期審查監視活動的結果。	□□□□	
A.10.10.3	日誌資訊的保護	應保護存錄設施與日誌資訊，不受竄改與未經授權的存取。	□□□□	
A.10.10.4	管理者與操作者日誌	系統管理者與操作者的活動應加以存錄。	□□□□	
A.10.10.5	失誤存錄	失誤應予以存錄、分析，並採取適當措施。	□□□□	
A.10.10.6	鐘訊同步	組織或安全領域內所有相關資訊處理系統的鐘訊，應與議定的準確時間來源同步。	□□□□	

A.11	存取控制			
A.11.1	存取控制的業務需求			
A.11.1.1	存取控制政策	應基於存取的營運與安全要求，建立、文件化及審查存取控制政策。	□□□□	
A.11.2	使用者存取管理			
A.11.2.1	使用者註冊	應有適當的正式使用者註冊與註銷註冊程序，以對所有資訊系統與服務核准和撤銷存取。	□□□□	
A.11.2.2	特權管理	應限制與控制特權的配置與使用。	□□□□	
A.11.2.3	使用者通行碼管理	應以正式的管理過程控制通行碼的配置。	□□□□	
A.11.2.4	使用者存取權限的審查	管理階層應定期使用正式過程審查使用者的存取權限。	□□□□	
A.11.3	使用者責任			
A.11.3.1	通行碼的使用	應要求使用者遵照良好安全實務去選擇與使用通行碼。	□□□□	
A.11.3.2	無人看管的使用者設備	使用者應確保無人看管的設備有適當保護。	□□□□	
A.11.3.3	桌面淨空與螢幕淨空政策	應採用對紙本媒體與可移除式儲存媒體之桌面淨空政策，及資訊處理設施的螢幕淨空政策。	□□□□	
A.11.4	網路存取控制			
A.11.4.1	網路服務的使用政策	應僅提供使用者經特定授權可存取使用的服務。	□□□□	
A.11.4.2	外部連線的使用者鑑別	應使用適當的鑑別方法，以控制遠端使用者的存取。	□□□□	
A.11.4.3	網路設備識別	應考量使用自動設備識別方法，以作為鑑別來自特定地點與設備的連線之手段。	□□□□	
A.11.4.4	遠端診斷與組態埠保護	應對診斷與組態埠的實體與邏輯存取加以控制。	□□□□	
A.11.4.5	網路區隔	應將資訊服務、使用者及資訊系統各群組使用的網路加以區隔。	□□□□	
A.11.4.6	網路連線控制	對分享的網路，特別是穿越組織邊界的網路，應依存取控制政策與營運應用的要求，限制使用者連線至網路的能力。	□□□□	
A.11.4.7	網路選路控制	應實作網路選路控制，以確保電腦連線與資訊流未違反企業應用系統之存取控制政策。	□□□□	

A.11.5	作業系統存取控制			
A.11.5.1	保全登入程序	應由保全登入程序控制作業系統的存取。	□□□□	
A.11.5.2	使用者識別與鑑別	所有使用者應有僅限其個人使用的唯一識別符(使用者 ID)，並應選擇適切的鑑別技術，以證實使用者宣稱之身分。	□□□□	
A.11.5.3	通行碼管理系統	管理通行碼的系統應為互動式，並應確保通行碼嚴謹。	□□□□	
A.11.5.4	系統公用程式的使用	應限制與嚴密控制可能篡越系統與應用控制措施的公用程式之使用。	□□□□	
A.11.5.5	會談期逾時	在超過界定的不動作時限後，宜關閉不動作的會談期。	□□□□	
A.11.5.6	連線時間的限制	對高風險的應用，連線時間應加以限制，以提供額外的安全性。	□□□□	
A.11.6	應用程式與資訊存取控制			
A.11.6.1	資訊存取限制	應根據所界定的存取控制政策，限制使用者與支援人員對資訊與應用系統功能之存取。	□□□□	
A.11.6.2	敏感性系統的隔離	敏感性系統應有專屬的(隔離的)電腦作業環境。	□□□□	
A.11.7	行動運算與遠距工作			
A.11.7.1	行動計算與通信	應備妥正式政策，並應採取適當的安全措施，以防範使用行動計算與通信設施的風險。	□□□□	
A.11.7.2	遠距工作	應發展與實作遠距工作活動的政策、作業計畫及程序。	□□□□	
A.12	資訊系統獲得、開發與維護			
A.12.1	資訊系統的安全需求			
A.12.1.1	安全要求分析與規格	新資訊系統或現有資訊系統提升的營運要求聲明中，應詳述安全控制措施的要求。	□□□□	
A.12.2	應用程式的正確處理			
A.12.2.1	輸入資料確認	輸入應用系統的資料應予確認，以確保該資料正確且適切。	□□□□	
A.12.2.2	內部處理的控制措施	確認查核(validation check)宜併入應用系統，以偵測經由處理錯誤或故意行為之任何資訊毀損。	□□□□	
A.12.2.3	訊息完整性	應識別應用系統內為確保鑑別性與保護訊息完整性的要求，並識別與實作適當的控制措施。	□□□□	

A.12.2.4	輸出資料確認	應用系統資料輸出應經確認，以確保所儲存資訊的處理正確且合乎實際情況。	□□□□	
A.12.3	密碼控制措施			
A.12.3.1	使用密碼控制措施的政策	使用密碼控制措施以保護資訊的政策應加以發展與實作。	□□□□	
A.12.3.2	金鑰管理	應備妥適當的金鑰管理，以支援組織使用密碼技術。	□□□□	
A.12.4	系統檔案的安全			
A.12.4.1	作業軟體的控制	應備妥各項程序，以控制作業系統上軟體的安裝。	□□□□	
A.12.4.2	系統測試資料的保護	應小心選擇、保護及管制測試資料。	□□□□	
A.12.4.3	程式源碼的存取控制	應限制對程式源碼的存取。	□□□□	
A.12.5	開發與支援過程的安全			
A.12.5.1	變更控制程序	應藉由使用正式的變更控制程序，以控制變更的實作。	□□□□	
A.12.5.2	作業系統變更後的應用系統技術審查	作業系統變更時，應審查與測試關鍵應用系統，以確保對組織作業或安全無不利的衝擊。	□□□□	
A.12.5.3	套裝軟體變更的限制	軟體套件之修改應不鼓勵，且僅限於有必要的變更，並應嚴格管制所有的變更。	□□□□	
A.12.5.4	資訊洩漏	應防範資訊洩漏的機會。	□□□□	
A.12.5.5	委外的軟體開發	組織應監督與監視委外的軟體開發。	□□□□	
A.12.6	技術脆弱性管理			
A.12.6.1	技術脆弱性控制	應取得關於使用中資訊系統之技術脆弱性的及時資訊、評估組織對此等脆弱性的暴露，以及採取適當的措施以因應相關的風險。	□□□□	
A.13	資訊安全事件管理			
A.13.1	報告資訊安全事件與弱點			
A.13.1.1	通報資訊安全事件	循適切的管理管道，儘速通報資訊安全事件。	□□□□	
A.13.1.2	通報安全弱點	應要求資訊系統與服務的所有員工、承包者及第三方使用者，注意並通報系統或服務之任何觀察到或可疑的安全弱點。	□□□□	

A.13.2	資訊安全事件與改善管理			
A.13.2.1	責任與程序	應建立管理責任與程序，以確保對資訊安全事件做迅速、有效及依序的回應。	□□□□	
A.13.2.2	從資訊安全事件中學習	應有各項適當的機制，對資訊安全事件的型式、數量及成本能加以量化與監視。	□□□□	
A.13.2.3	證據的收集	在涉及法律行動(民事或刑事)的資訊安全事件後，對人員或組織的跟催措施，應收集、保存及呈現證據，以符合在相關審判時提出證據的規則。	□□□□	
A.14	營運永續管理			
A.14.1	營運永續管理的資訊安全層面			
A.14.1.1	資訊安全納入營運永續管理過程	應發展與維持整個組織營運永續的管理過程，以因應組織營運永續所需的資訊安全要求。	□□□□	
A.14.1.2	營運永續與風險評鑑	應識別能導致營運過程中斷的事件，與此等中斷事件的機率及衝擊，以及其後果對資訊安全的影響。	□□□□	
A.14.1.3	發展與實作包括資訊安全的永續計畫	應發展與實作各項計畫，當重要營運過程中斷或失效後，可藉以維持或恢復運作，並確保資訊的可用性在要求時間內達到所要求等級。	□□□□	
A.14.1.4	營運永續計畫框架	應維持營運永續計畫之單一框架，以確保所有計畫有一致性，持續一致地因應資訊安全要求，並識別測試與維護的優先順序。	□□□□	
A.14.1.5	營運永續計畫的測試、維護及重新評鑑	營運永續計畫應定期測試與更新，以確保維持最新且有效。	□□□□	
A.15	遵循性			
A.15.1	遵循適法性要求			
A.15.1.1	識別適用之法條	對每一個資訊系統與組織，所有相關法定、法規與契約要求及組織用以符合此等要求之做法，宜加以明確界定、文件化及維持最新。	□□□□	
A.15.1.2	智慧財產權	應實作適當程序，以確保所使用的資料可能涉及智慧財產權與所使用的專屬軟體產品，可遵循法律、法規及契約的要求。	□□□□	
A.15.1.3	組織紀錄的保護	應依據法令、法規、契約及營運要求，保護重要紀錄，免於遺失、毀損及偽造。	□□□□	

A.15.1.4	個人資訊的資料保護與隱私	應如同相關法令、法規及若適用的契約條文所要求的，確保資料保護與隱私。	□□□□	
A.15.1.5	防止資訊處理設施的誤用	應制止使用者以未經授權的目的使用資訊處理設施。	□□□□	
A.15.1.6	密碼控制措施的規定	應使用密碼控制措施，以遵循所有相關的協議、法律及法規。	□□□□	
A.15.2	遵循安全政策、標準和技術符合			
A.15.2.1	安全政策與標準的遵循性	管理人員應確保其責任範圍內所有安全程序皆正確執行，以達成各項安全政策與標準的遵循性。	□□□□	
A.15.2.2	技術遵循性查核	應定期查核資訊系統是否遵循安全實作標準。	□□□□	
A.15.3	資訊系統稽核考量因素			
A.15.3.1	資訊系統稽核控制	有關運作之系統的查核，其稽核要求與活動宜謹慎規劃及議定，使營運過程中斷之風險降至最低。	□□□□	
A.15.3.2	資訊系統稽核工具的保護	應保護資訊系統稽核工具之存取，以防止任何可能的誤用或破解。	□□□□	

資料來源：ISO/IEC 27001:2005，本研究整理

3.5 研究範圍與限制

進行本研究的過程中，研究者秉持力求本研究完整與真實之研究態度，然而由於若干因素限制，以致有不盡圓滿之處，本節將針對研究過程中所遭遇到的研究限制提出說明。

任何科學的理論發展，無論是自然科學還是社會科學的研究發現皆受到不同時空背景的挑戰，其中，個案研究最大的研究限制來自於證據來源的局限，企圖透過少數個案的發現，類推至其他適用的情境，本有其先天的困難，這也是量化研究對個案研究結果普及性，抱持質疑的主要原因。為此，以下將說明本研究的個案對象以界定本研究的研究範圍。

本研究所訪談的五家企業，其中 T 公司、S 公司、A 公司以及 V 公司均為國內知名的電信業者，分別提供行動通信與固網通信服務，W 公司則是知名的地方有線電視業者，除提供有線電視服務之外，亦提供寬頻上網服務。五家公司皆成立於 1996 年至 2000 年，正值我國行動通信與寬頻上網即將起飛的年代，在激烈的競爭之下，T 公司目前為國內前三大行動通信的領導業者，S 公司則是國內前三大固網通信業者，A 公司現在是國內經營固網與行動通信事業的第二大企業，V 公司為國內以 3G 行動通信為主要業務的業者，W 公司雖然只是一家地區性的有線電視業者，規模與聲譽遠不及上述四家業務

範圍涵蓋全省的電信業者，然而其有線電視經營績效成績斐然。

上述研究範圍的界定並無法保證本研究之內、外部效度的完整性，本研究從國內九十五家第一類電信業者中，挑選出其中具有代表性的五家公司，然而，在電信產業具有代表性地位的公司，仍有不少未成為本研究的樣本個案，礙於時間、資源與成本等因素考量，若要逐一查訪，實有其困難性。本研究的不足之處，有賴後續研究者以大量樣本抽樣方式加以驗證，或持續將新的個案研究納入，使研究發現趨於完整。

此外，造成個案研究結果失真，最主要的誤差來自於研究者的偏誤(Error)與受訪者的偏差(Bias)。

研究者的偏誤方面，儘管本研究事前不作任何理論架構或假設，而是基於事實的發現作資料歸納，然而，可能因為研究者學識與經驗不足，先前理解與個案分析能力有限，對於訪談資料闡釋，可能會過於主觀，陷入迷思而不自覺，進而造成個案研究結果的客觀性受到影響，此部分偏誤幸經由指導教授的指導並與業界人士討論切磋，不斷地思考辨證，而加以修正。

受訪者的偏差方面，本研究的訪談對象為掌管資訊安全管理系統的部門主管或人員，由於本研究係以仿照 ISO 稽核驗證的方式進行，針對每一項控制措施皆仔細評核，需耗費大量的時間，個案業者基於公司業務運作與受訪者個人意願的考量下，訪談時間往往十分緊迫，同時也難以增加受訪人數與次數，雖然可以經由電話與電子郵件作後續問題的釐清，但仍難以取代實地訪查的效果，形成研究的限制。

本研究畢竟是探討資訊安全管理系統，當涉及到「安全」的議題時，就可能有機密性或敏感性的考量，本章第四節所建立的 ISO 27001 評核表，其中部分控制措施對個案業者而言屬於機密性質者，研究者無法直接驗證個案業者的執行方式是否符合評估內容，受訪者也可能對於部分敏感議題的回答傾向持保留態度，因此難以滿足資料蒐集的信度要求，僅能以受訪者意見及觀察訪談過程中所透露的訊息來加以研判。

第四章 研究分析

本章旨在說明本研究之分析結果，共分為三節。4.1 節描述個案業者依據 ISO 27001 之 11 大控制要項與 133 項控制措施的施行現況；4.2 節介紹 ISO 27001 核心版的遴選結果並解釋其選擇的條件與理由；最後，4.3 節以重要性-表現程度分析法(Important-Performance Analysis，IPA)呈現電信業者對 133 項控制措施的執行策略。

4.1 評核結果分析

本節將依據深度訪談與實地查察所發現的真實情況，呈現個案電信業者在 ISO 27001 要求規範中的 11 大控制要項與 133 項控制措施之統計結果，並提出歸納與分析。

4.1.1 評核結果統計分析

根據 ISO 稽核驗證的精神與方式，次要缺失(Minor Non-Conformance)指在資訊安全的施行做法上有輕微瑕疵，但沒有立即危害的安全風險，可在處理改善後再次複查而予以認可通過；主要缺失(Major Non-Conformance)則是在資訊安全的施行做法上有重大瑕疵，足以造成嚴重且立即性的安全風險，因此將無法通過驗證。

透過 3.4 節建立的評核表與定義的評分量化準則進行電信業者資訊安全管理的評估，以 ISO 27001 的 133 項控制措施為評核標準，根據實地訪查結果，其資訊安全符合狀況與量化分數的統計結果如表 4-1 所示。W 公司由於業務性質的關係，有 3 項控制措施為「不適用」，因此這 3 項控制措施不予以計分。

T 公司與 S 公司皆已獲得 ISO 27001 資訊安全管理系統認證，其在資訊安全的推動與努力也反應在評核的結果上面，T 公司的控制措施平均分數是 2.95，S 公司則是 2.93，都非常接近 3 的滿分值，雖然此次評估的結果並未百分之百做到完全符合，不過其缺失都屬於次要缺失，並不會造成重大的損害，整體表現算是可圈可點，然而，日常資訊安全管理的執行細節上仍需持續要求，以達到無時無刻皆滴水不漏的安全防護。

A 公司與 V 公司並未導入與推動 ISO 27001 資訊安全管理系統，因此從評核結果可發現其在資訊安全管理的表現上明顯低於 T 公司與 S 公司，評估的結果顯示次要缺失偏多，也有少部分的主要缺失，雖然無法通過 ISO 27001 的驗證，不過 A 公司的控制措施平均分數是 2.64，V 公司為 2.68，都有接近 90%的符合度，A 公司與 V 公司的規模皆屬於大型電信業者，只要願意投入資源，針對主要缺失做修正，並改善次要缺失，可期待資訊安全管理將更為周延完善，達到 ISO 27001 要求的水準。

W 公司同樣未導入與推動 ISO 27001 資訊安全管理系統，且其規模遠比上述四家公司來得小，在資源有限的情況下，整體的評比也有一段差距，評估的結果顯示主要缺失與不符合的項目過多，無法通過 ISO 27001 的驗證，而次要缺失所佔比率竟然高出完全符合的項目，控制措施平均分數是 2.28，只有 75.9%的符合度，整體表現可說是差強人意，未來需將有限的資源先投入到主要缺失與不符合的項目，然後逐步檢討並改善次要缺失，以提升資訊安全管理的層次。

整體而言，5 家個案業者在 ISO 27001 資訊安全管理之 133 項控制措施的平均分數為 2.70，符合程度達到 90%，顯示電信產業的資訊安全管理具有相當的水平，電信業者也都意識到資訊安全管理的重要性。

表 4-1 個案業者之 ISO 27001 整體符合狀況

符 合 狀 況	T 公司	S 公司	A 公司	V 公司	W 公司
完全符合	126	124	88	93	55
次要缺失	7	9	42	38	58
主要缺失	0	0	3	2	15
不符合	0	0	0	0	2
不適用	0	0	0	0	3
量化分數總和	392	390	351	357	296
控制措施平均分數	2.95	2.93	2.64	2.68	2.28
符合程度百分比	98.25%	97.74%	87.97%	89.47%	75.90%

4.1.2 11 大控制要項符合狀況分析

4.1.1 節分析個案業者依據 ISO 驗證方式所展現的整體資訊安全管理狀況，本節將分析個案業者在 ISO 27001 之 11 大控制要項的符合狀況，如表 4-2 所示，控制措施平均分數的分佈情況以雷達圖方式呈現，如圖 4-1 所示。

表 4-2 個案業者於 11 大控制要項之符合狀況

控 制 要 項	控制措施數量(C)	量化分數總和(S)					控制措施平均分數(S/C)
		T	S	A	V	W	
A.5 安全政策	2	6	6	4	6	3	2.50
A.6 資訊安全組織	11	33	32	24	30	22	2.56
A.7 資產管理	5	15	15	14	15	14	2.92
A.8 人力資源安全	9	27	26	25	24	21	2.73

A.9 實體與環境安全	13	38	39	35	37	33	2.80
A.10 通訊與作業管理	32	95	94	81	82	65	2.66
A.11 存取控制	25	72	73	69	61	57	2.66
A.12 資訊系統獲得、開發與維護	16	46	46	44	43	33	2.65
A.13 資訊安全事件管理	5	15	15	14	14	10	2.72
A.14 營運永續管理	5	15	14	13	15	11	2.72
A.15 遵循性	10	30	30	28	30	27	2.90
總計	133	392	390	351	357	296	2.70

- 個案業者在「A.7 資產管理」與「A.15 遵循性」的表現上優於其它控制要項，都達到 2.90 以上的分數，接近 3 的滿分值，符合程度在 96.67%以上，顯示電信業者在資產的管理與分類、法規與技術的遵循、智慧財產權與個人隱私的保護上執行的相當不錯。
- 個案業者在「A.8 人力資源安全」、「A.9 實體與環境安全」、「A.10 通訊與作業管理」、「A.11 存取控制」、「A.12 資訊系統獲得、開發與維護」、「A.13 資訊安全事件管理」與「A.14 營運永續管理」的表現分數介於 2.65 至 2.80 之間，符合程度則介於 88.33%至 93.33%，屬於表現中等的控制要項。
- 相對於其它控制要項，個案業者在「安全政策」與「資訊安全組織」的表現較差，分數在 2.56 以下，符合程度介於 83.33%至 85.33%，顯示電信業者在資訊安全政策文件、資訊安全的獨立審查與資訊安全的機密要求等措施尚待加強。

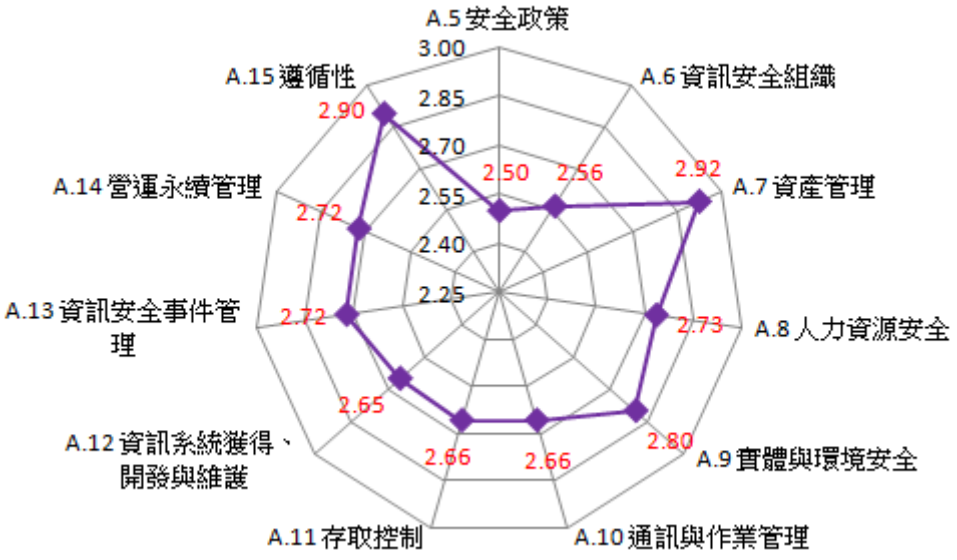

圖 4-1 ISO 27001 控制要項雷達圖

依據 2.3 節 ISO 27001 的控制要項可分為策略面、管理面以及作業面，其中「安全政策」、「營運永續管理」及「遵循性」屬於策略面，「資訊安全組織」、「資產管理」、「人力資源管理」及「資訊安全事件管理」屬於管理面，「實體與環境安全」、「通訊與作業管理」、「存取控制」及「資訊系統獲得、開發與維護」屬於作業面。

以此三個面向分析個案業者的 ISO 27001 符合狀況如表 4-3 所示，整體而言，電信業者的資訊安全管理之策略面表現優於管理面，而管理面優於作業面，策略面的控制措施平均分數為 2.80，管理面是 2.70，作業面是 2.68，差距並不大，顯示電信業者在這三方面的表現相當平均。

T 公司與 V 公司在策略面表現最佳，控制措施平均分數都達到 3 的滿分值，100%符合所有控制措施的要求；管理面是 T 公司表現最佳，控制措施平均分數也是 3 的滿分值；作業面則是 S 公司表現最佳，控制措施平均分數有 2.93，達到 97.67%的水準。

表 4-3 個案業者於策略面、管理面與作業面之符合狀況

控制要項分類	控制措施數量(C)	量化分數總和(S)					控制措施平均分數(S/C)
		T	S	A	V	W	
策略面	17	51	50	45	51	41	2.80
管理面	30	90	88	77	83	67	2.70
作業面	86	251	252	229	223	188	2.68

4.1.3 133 項控制措施符合狀況分析

4.1.2 節呈現 11 大控制要項的符合狀況，本節將依各個控制要項，分別說明將其控制目標與控制措施的符合狀況。

A.5 安全政策

安全政策包含 1 個控制目標「資訊安全政策」以及 2 項控制措施。

- 資訊安全政策：依照營運要求及相關法律與法規，提供管理階層對資訊安全之指示與支持。

個案業者於安全政策的符合狀況，如表 4-4 所示；個案業者於安全政策的符合程度，如圖 4-2 所示。

表 4-4 個案業者於安全政策之符合狀況

題 號	控 制 措 施	量 化 分 數					平 均
		T	S	A	V	W	
A.5.1	資訊安全政策 (2 項控制措施)						
A.5.1.1	資訊安全政策文件	3	3	2	3	2	2.60
A.5.1.2	資訊安全政策之審查	3	3	2	3	1	2.40
平均		3.00	3.00	2.00	3.00	1.50	2.50

- 個案業者在「A.5.1.1 資訊安全政策文件」的平均分數是 2.60，符合程度達 86.67%，顯示 ISO 27001 資訊安全管理最基礎的具備事項：資訊安全政策文件，這部分的施行落實尚有待檢討改善。
- 個案業者在「A.5.1.2 資訊安全政策之審查」的平均分數是 2.40，符合程度為 80%，顯示縱有資訊安全政策文件，但在持續審查、保持政策文件之適用性與有效性的努力仍不夠，必須依據客觀環境與條件落實政策文件的修訂。

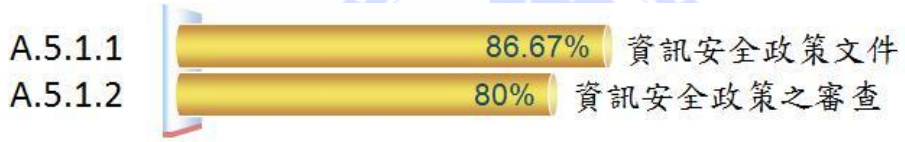

圖 4-2 個案業者於安全政策之符合程度

A.6 資訊安全組織

資訊安全組織包含 2 個控制目標「內部組織」與「外部團體」以及 11 項控制措施。

- 內部組織：於組織內管理資訊安全。
- 外部團體：維持外部團體所存取、處理、管理或與其通信之組織資訊與資訊處理設施的安全。

個案業者於資訊安全組織的符合狀況，如表 4-5 所示；個案業者於資訊安全組織的符合程度，如圖 4-3 所示。

表 4-5 個案業者於資訊安全組織之符合狀況

題號	控制措施	量化分數					平均
		T	S	A	V	W	
A.6.1	內部組織 (8 項控制措施)						
A.6.1.1	管理階層對資訊安全的承諾	3	3	2	3	2	2.60
A.6.1.2	資訊安全協調工作	3	3	2	3	2	2.60
A.6.1.3	資訊安全責任的配置	3	3	3	3	3	3.00
A.6.1.4	資訊處理設施的授權過程	3	3	2	3	2	2.60
A.6.1.5	機密性協議	3	2	2	2	1	2.00
A.6.1.6	與權責機關的聯繫	3	3	2	2	2	2.40
A.6.1.7	與特殊利害相關團體的聯繫	3	3	2	3	2	2.60
A.6.1.8	資訊安全的獨立審查	3	3	2	3	1	2.40
A.6.2	外部團體 (3 項控制措施)						
A.6.2.1	與外部團體相關的風險之識別	3	3	2	3	2	2.60
A.6.2.2	處理客戶事務的安全說明	3	3	2	3	2	2.60
A.6.2.3	第三方協議中之安全說明	3	3	3	2	3	2.80
平均		3.00	2.91	2.18	2.73	2.00	2.56

- 個案業者在「A.6.1.5 機密性協議」的平均分數是 2.00，符合程度為 66.67%，顯示電信業者對於機密性的資訊安全要求無法明確界定其範圍，也因此無法落實定期審查以反應公司的需求，此部分應確實檢討，加以改善。
- 個案業者在「A.6.1.6 與權責機關的聯繫」與「A.6.1.8 資訊安全的獨立審查」的平均分數皆為 2.40，符合程度只達到 80%，顯示平日疏於聯繫相關的權責機關，應建立適當的溝通管道與程序，在資訊安全事件發生時能做到即時通報；而資訊安全的審查需避免球員兼裁判的情事發生，應由獨立的管理人員或第三方組織來執行。
- 個案業者在資訊安全組織的其它控制措施，例如：「A.6.1.1 管理階層對資訊安全的承諾」、「A.6.1.2 資訊安全協調工作」與「A.6.1.4 資訊處理設施的授權過程」等，平均分數多為 2.60，符合程度為 86.67%，尚有進步的空間。
- 個案業者在「A.6.1.3 資訊安全責任的配置」的平均分數是 3.00 的滿分，完全符合該控制措施的要求，顯示電信業者能夠明確的界定所有的資訊安全責任與範圍，並正確的執行。

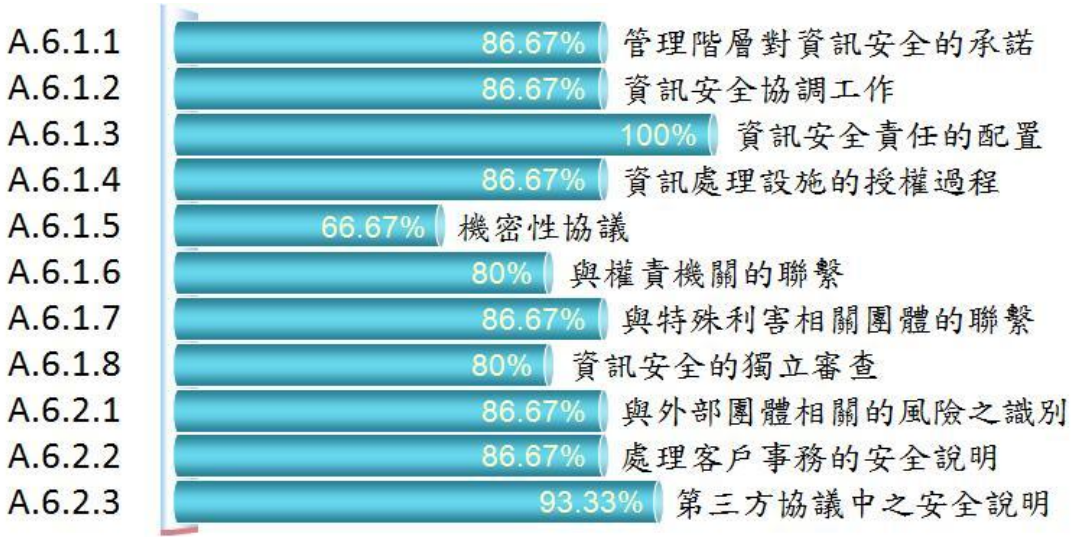

圖 4-3 個案業者於資訊安全組織之符合程度

A.7 資產管理

資產管理包含 2 個控制目標「資產責任」與「資產分類」以及 5 項控制措施。

- 資產責任：達成及維持組織資產的適切保護。
- 資產分類：確保資訊受到適切等級的保護。

個案業者於資產管理的符合狀況，如表 4-6 所示；個案業者於資產管理的符合程度，如圖 4-4 所示。

表 4-6 個案業者於資產管理之符合狀況

題 號	控 制 措 施	量 化 分 數					平 均
		T	S	A	V	W	
A.7.1	資產責任 (3 項控制措施)						
A.7.1.1	資產清冊	3	3	3	3	3	3.00
A.7.1.2	資產的擁有權	3	3	3	3	3	3.00
A.7.1.3	資產之可被接受的使用	3	3	2	3	3	2.80
A.7.2	資產分類 (2 項控制措施)						
A.7.2.1	分類指導綱要	3	3	3	3	2	2.80
A.7.2.2	資訊標示與處置	3	3	3	3	3	3.00
平均		3.00	3.00	2.80	3.00	2.80	2.92

- 個案業者在資產管理的所有控制措施，平均分數都在 2.80 以上，整體符合程度達到 97.33%以上，顯示電信業者在資產的維護與權責指派，以及資訊的分類與處置上，做得相當完善，只有些許瑕疵需要改善。

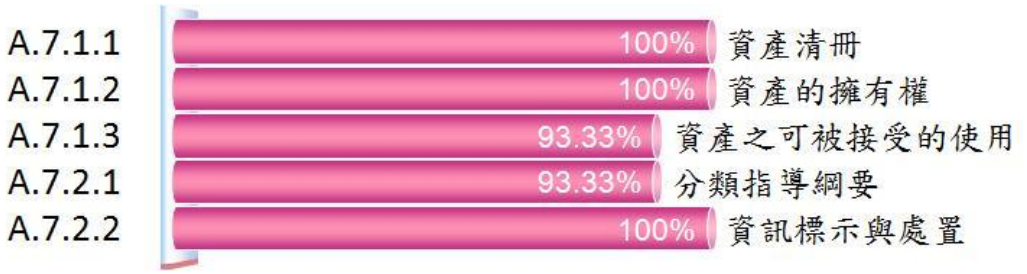

圖 4-4 個案業者於資產管理之符合程度

A.8 人力資源安全

人力資源安全包含 3 個控制目標「聘僱之前」、「聘僱期間」與「聘僱的終止或變更」以及 9 項控制措施。

- 聘僱之前：確保員工、承包者及第三方使用者了解其責任，並勝任其所被認定的角色，以降低竊盜、詐欺或設施誤用的風險。
- 聘僱期間：確保所有員工、承包者及第三方使用者認知資訊安全的威脅與關切事項、其基本責任與強制責任，並有能力在日常工作中支持組織安全政策與降低人為錯誤的風險。
- 聘僱的終止或變更：確保員工、承包者及第三方使用者以有條理的方式脫離組織或變更聘僱。

個案業者於人力資源安全的符合狀況，如表 4-7 所示；個案業者於人力資源安全的符合程度，如圖 4-5 所示。

表 4-7 個案業者於人力資源安全之符合狀況

題 號	控 制 措 施	量 化 分 數					平 均
		T	S	A	V	W	
A.8.1	聘僱之前 (3 項控制措施)						
A.8.1.1	角色與責任	3	3	3	3	3	3.00
A.8.1.2	篩選	3	2	2	2	2	2.20
A.8.1.3	聘僱條款與條件	3	3	3	2	3	2.80
A.8.2	聘僱期間 (3 項控制措施)						
A.8.2.1	管理階層責任	3	3	3	3	3	3.00
A.8.2.2	資訊安全認知、教育及訓練	3	3	2	2	2	2.40
A.8.2.3	懲處過程	3	3	3	3	2	2.80
A.8.3	聘僱的終止或變更 (3 項控制措施)						
A.8.3.1	終止責任	3	3	3	3	2	2.80
A.8.3.2	資產的歸還	3	3	3	3	2	2.80

A.8.3.3	存取權限的移除	3	3	3	3	2	2.80
平均		3.00	2.89	2.78	2.67	2.33	2.73

- 個案業者在「A.8.1.2 篩選」與「A.8.2.2 資訊安全認知、教育及訓練」的平均分數偏低，在 2.4 以下，符合程度不到 80%，顯示電信業者在聘雇之前對於應試者與承包商的背景查核驗證做得不夠徹底，而在聘雇期間對於相關的資訊安全訓練則未落實執行，需加以檢討改善。
- 個案業者在人力資源安全的其他控制措施，平均分數都在 2.8 以上，符合程度皆高於 93.33%，顯示電信業者在聘僱之前對於工作的責任與聘僱條款，聘僱期間管理階層對於資訊安全的要求，以及聘僱的終止或變更時對於資產歸還與權限移除等措施有做到確實執行。

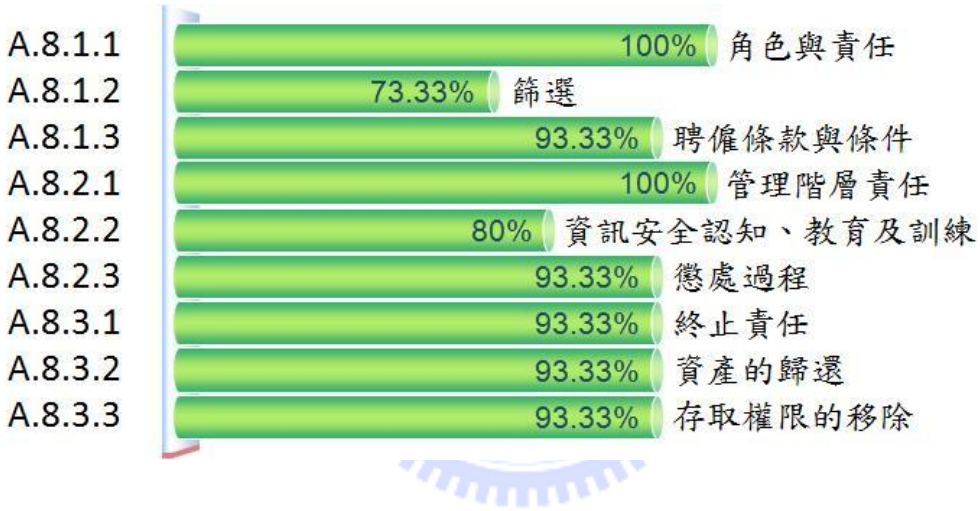

圖 4-5 個案業者於人力資源安全之符合程度

A.9 實體與環境安全

實體與環境安全包含 2 個控制目標「安全區域」與「設備安全」以及 13 項控制措施。

- 安全區域：防止組織場所與資訊遭未經授權的實體存取、損害及干擾。
- 設備安全：防止資產的遺失、損害、竊盜或破解，並防止組織活動的中斷。

個案業者於實體與環境安全的符合狀況，如表 4-8 所示；個案業者於實體與環境安全的符合程度，如圖 4-6 所示。

表 4-8 個案業者於實體與環境安全之符合狀況

題 號	控 制 措 施	量 化 分 數					平 均
		T	S	A	V	W	
A.9.1	安全區域 (6 項控制措施)						
A.9.1.1	實體安全周界	3	3	2	3	3	2.80
A.9.1.2	實體進入控制措施	3	3	3	3	3	3.00
A.9.1.3	保全辦公室、房間及設施	3	3	2	3	3	2.80
A.9.1.4	對外部與環境威脅的保護	3	3	3	3	3	3.00
A.9.1.5	在安全區域內工作	2	3	2	2	2	2.20
A.9.1.6	公共進出、收發及裝卸區	3	3	3	3	2	2.80
A.9.2	設備安全 (7 項控制措施)						
A.9.2.1	設備安置與保護	3	3	3	3	3	3.00
A.9.2.2	支援的公用設施	3	3	3	3	3	3.00
A.9.2.3	佈纜的安全	3	3	3	3	3	3.00
A.9.2.4	設備維護	3	3	3	3	3	3.00
A.9.2.5	場所外設備的安全	3	3	2	3	2	2.60
A.9.2.6	設備的安全汰除或再使用	3	3	3	3	2	2.80
A.9.2.7	財產的攜出	3	3	3	2	1	2.40
平均		2.92	3.00	2.69	2.85	2.54	2.80

- 個案業者在「A.9.1.5 在安全區域內工作」與「A.9.2.7 財產的攜出」的平均分數都在 2.40 以下，符合程度低於 80%，顯示電信業者在安全區域內對於員工、承包商與第三方使用者的保護措施不足，而對於公司設備資產的攜出管控也有明顯的漏洞，應儘快檢討改善。
- 個案業者在「A.9.2.5 場所外設備的安全」的平均分數是 2.60，符合程度為 86.67%，顯示電信業者對於放置在公司以外場所的資產設備，還需要多加考量其安全風險，例如：損害、竊盜或竊聽等。
- 個案業者在實體與環境安全的其他控制措施，平均分數都達到 2.80 以上，符合程度在 93.33%以上，顯示電信業者對於工作場所的實體安全防護與資產設備的保護大多能有效掌控。

圖 4-6 個案業者於實體與環境安全之符合程度

A.10 通訊與作業管理

通訊與作業管理包含 10 個控制目標「作業之程序與責任」、「第三方服務交付管理」、「系統規劃與驗收」、「防範惡意碼與行動碼」、「備份」、「網路安全管理」、「媒體的處置」、「資訊交換」、「電子商務服務」與「監控」以及 32 項控制措施。

- 作業之程序與責任：確保正確與安全地操作資訊處理設施。
- 第三方服務交付管理：實作與維持適切等級之資訊安全及服務交付，並能與第三方服務交付協議一致。
- 系統規劃與驗收：使系統失效的風險最小化。
- 防範惡意碼與行動碼：保護軟體與資訊的完整性。
- 備份：維持資訊及資訊處理設施的完整性與可用性。
- 網路安全管理：確保對網路內資訊與支援性基礎建設的保護。
- 媒體的處置：防止資產被未經授權的揭露、修改、移除或破壞，以及營運活動的中斷。
- 資訊交換：維護組織內及與任何外部個體所交換資訊與軟體的安全。
- 電子商務服務：確保電子商務服務的安全性及其安全的使用。
- 監控：偵測未經授權的資訊處理活動。

個案業者於通訊與作業管理的符合狀況，如表 4-9 所示；個案業者於通訊與作業管理的符合程度，如圖 4-7 所示。

表 4-9 個案業者於通訊與作業管理之符合狀況

題號	控制措施	量化分數					平均
		T	S	A	V	W	
A.10.1	作業之程序與責任 (4 項控制措施)						
A.10.1.1	文件化作業程序	3	3	3	3	2	2.80
A.10.1.2	變更管理	3	3	2	2	1	2.20
A.10.1.3	職務的區隔	3	3	2	2	2	2.40
A.10.1.4	開發、測試及運作設施的分隔	3	2	1	2	2	2.00
A.10.2	第三方服務交付管理 (3 項控制措施)						
A.10.2.1	服務交付	3	3	3	3	3	3.00
A.10.2.2	第三方服務的監視與審查	3	3	2	3	2	2.60
A.10.2.3	第三方服務變更的管理	3	3	3	2	2	2.60
A.10.3	系統規劃與驗收 (2 項控制措施)						
A.10.3.1	容量管理	3	3	1	2	2	2.20
A.10.3.2	系統驗收	3	3	2	2	1	2.20
A.10.4	防範惡意碼與行動碼 (2 項控制措施)						
A.10.4.1	對抗惡意碼的控制措施	3	3	3	2	2	2.60
A.10.4.2	對抗行動碼的控制措施	3	3	2	2	1	2.20
A.10.5	備份 (1 項控制措施)						
A.10.5.1	資訊備份	3	3	3	3	3	3.00
A.10.6	網路安全管理 (2 項控制措施)						
A.10.6.1	網路控制措施	3	3	3	3	3	3.00
A.10.6.2	網路服務的安全	3	3	2	3	3	2.80
A.10.7	媒體的處置 (4 項控制措施)						
A.10.7.1	可移除式媒體的管理	3	3	2	3	3	2.80
A.10.7.2	媒體的汰除	2	3	3	3	3	2.80
A.10.7.3	資訊處置程序	3	3	2	3	2	2.60
A.10.7.4	系統文件的安全	3	3	3	2	2	2.60
A.10.8	資訊交換 (5 項控制措施)						
A.10.8.1	資訊交換政策與程序	3	3	3	3	3	3.00
A.10.8.2	交換協議	3	3	3	3	3	3.00
A.10.8.3	輸送中的實體媒體	3	3	3	3	3	3.00
A.10.8.4	電子傳訊	3	3	3	3	3	3.00
A.10.8.5	營運資訊系統	3	3	3	2	2	2.60
A.10.9	電子商務服務 (3 項控制措施)						

A.10.9.1	電子商務	3	3	3	3	NA	3.00
A.10.9.2	線上交易	3	3	3	3	NA	3.00
A.10.9.3	公眾可用的資訊	3	3	3	3	NA	3.00
A.10.10	監控 (6 項控制措施)						
A.10.10.1	稽核存錄	3	3	3	2	3	2.80
A.10.10.2	監控系統的使用	3	3	2	2	2	2.40
A.10.10.3	日誌資訊的保護	3	3	3	3	3	3.00
A.10.10.4	管理者與操作者日誌	3	3	2	2	1	2.20
A.10.10.5	失誤存錄	3	2	2	2	0	1.80
A.10.10.6	鐘訊同步	3	3	3	3	3	3.00
平均		2.97	2.94	2.53	2.56	2.24	2.65

- 個案業者在「A.10.1.4 開發、測試及運作設施的分隔」與「A.10.10.5 失誤存錄」的平均分數過低，只有 2.00 與 1.80，符合程度低於 66.67%，顯示電信業者並未對運作、測試與開發系統的環境間做出有效區隔，因此開發與測試的過程可能會對營運系統造成嚴重損害，而對於錯誤和失誤的日誌檔案也沒有加以留存分析，必須儘速檢討審查。
- 個案業者在「A.10.1.2 變更管理」、「A.10.3.1 容量管理」、「A.10.3.2 系統驗收」、「A.10.4.2 對抗行動碼的控制措施」與「A.10.10.4 管理者與操作者日誌」的平均分數也是偏低，只有 2.20，符合程度為 73.33%，顯示電信業者對於資訊系統的變更、資源容量的監控管理、系統驗收測試的準則、行動碼(Mobile Code)的封鎖控制與系統管理者的操作過程記錄等並沒有確切施行，有待進一步改善。
- 個案業者在「A.10.1.3 職務的區隔」、「A.10.2.2 第三方服務的監視與審查」、「A.10.2.3 第三方服務變更的管理」、「A.10.4.1 對抗惡意碼的控制措施」、「A.10.7.3 資訊處置程序」、「A.10.7.4 系統文件的安全」、「A.10.8.5 營運資訊系統」與「A.10.10.2 監控系統的使用」，平均分數介於 2.40 至 2.60 之間，符合程度則是 80%至 86.67%，顯示電信業者在職務與責任的區隔不甚明確、未定期審視第三方提供的服務與報告、沒有周延考量第三方服務變更可能導致的風險、缺乏惡意碼(Malicious Code)偵測預防機制、資訊保護的處理程序不夠完整、敏感資訊的系統文件防護不足、營運資訊系統相關資訊的保護有漏洞以及監視資訊處理設施的程序不夠嚴謹，需再加以嚴格要求。
- 個案業者在通訊與作業管理的其他控制措施，平均分數達到 2.8 以上，符合程度在 93.33%以上，顯示電信業者在作業程序文件化、第三方提供的服務交付、資訊的備份、網路的安全管控、媒體的管理與汰換、資訊的交換傳送程序、電子商務的安全性、稽核日誌檔案的保存與防護以及資訊處理系統的時間同步等控制措施處置得宜。

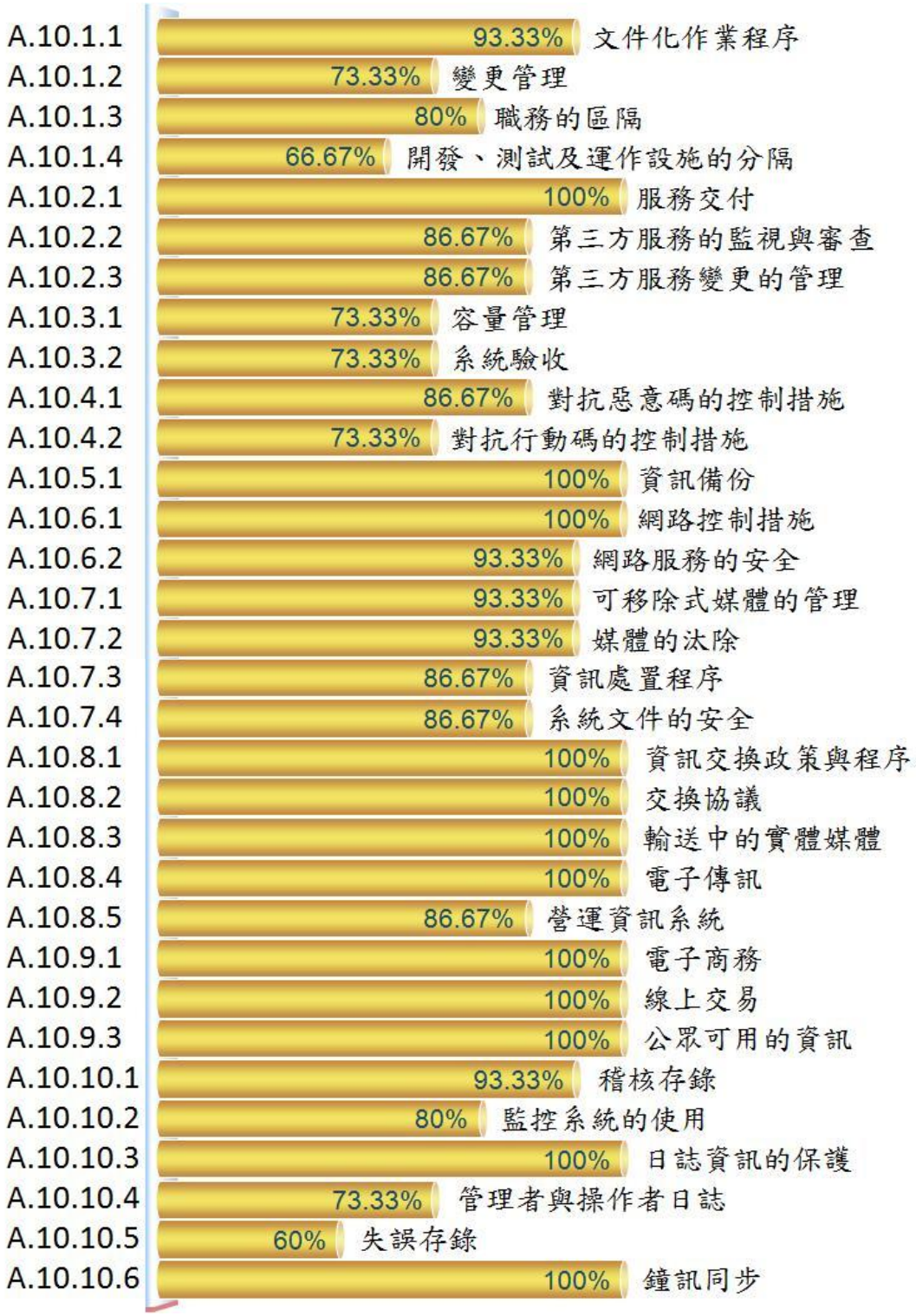

圖 4-7 個案業者於通訊與作業管理之符合程度

A.11 存取控制

存取控制包含 7 個控制目標「存取控制的營運要求」、「使用者存取管理」、「使用者責任」、「網路存取控制」、「作業系統存取控制」、「應用系統與資訊存取控制」與「行動計算與遠距工作」以及 25 項控制措施。

- 存取控制的營運要求：控制資訊的存取。
- 使用者存取管理:確保經授權使用者對資訊系統的存取與防止未經授權的存取。
- 使用者責任：防止未經授權的使用者存取資訊與資訊處理設施，以及使其遭受破壞或竊盜。
- 網路存取控制：防止網路服務遭未經授權的存取。
- 作業系統存取控制：防止作業系統遭未經授權的存取。
- 應用系統與資訊存取控制：防止應用系統中的資訊遭未經授權的存取。
- 行動計算與遠距工作：確保使用行動計算與遠距工作設施時之資訊安全。

個案業者於存取控制的符合狀況，如表 4-10 所示；個案業者於存取控制的符合程度，如圖 4-8 所示。

表 4-10 個案業者於存取控制之符合狀況

題號	控制措施	量化分數					平均
		T	S	A	V	W	
A.11.1	存取控制的營運要求 (1 項控制措施)						
A.11.1.1	存取控制政策	3	3	2	3	2	2.60
A.11.2	使用者存取管理 (4 項控制措施)						
A.11.2.1	使用者註冊	3	3	3	3	3	3.00
A.11.2.2	特權管理	3	3	3	3	2	2.80
A.11.2.3	使用者通行碼管理	3	3	3	3	2	2.80
A.11.2.4	使用者存取權限的審查	2	3	2	1	1	1.80
A.11.3	使用者責任 (3 項控制措施)						
A.11.3.1	通行碼的使用	3	3	2	2	2	2.40
A.11.3.2	無人看管的使用者設備	3	2	3	2	2	2.40
A.11.3.3	桌面淨空與螢幕淨空政策	2	2	2	1	1	1.60
A.11.4	網路存取控制 (7 項控制措施)						
A.11.4.1	網路服務的使用政策	3	3	3	3	3	3.00
A.11.4.2	外部連線的使用者鑑別	3	3	3	2	3	2.80
A.11.4.3	網路設備識別	3	3	3	2	2	2.60
A.11.4.4	遠端診斷與組態埠保護	3	3	3	3	3	3.00
A.11.4.5	網路區隔	3	3	3	3	2	2.80
A.11.4.6	網路連線控制	3	3	3	2	3	2.80

A.11.4.7	網路選路控制	3	3	3	3	2	2.80
A.11.5	作業系統存取控制 (6 項控制措施)						
A.11.5.1	保全登入程序	3	3	3	3	3	3.00
A.11.5.2	使用者識別與鑑別	3	3	3	3	3	3.00
A.11.5.3	通行碼管理系統	3	3	3	3	3	3.00
A.11.5.4	系統公用程式的使用	3	3	3	3	2	2.80
A.11.5.5	會談期逾時	3	3	2	2	2	2.40
A.11.5.6	連線時間的限制	3	3	2	2	2	2.40
A.11.6	應用系統與資訊存取控制 (2 項控制措施)						
A.11.6.1	資訊存取限制	3	3	3	3	3	3.00
A.11.6.2	敏感性系統的隔離	2	3	3	2	2	2.40
A.11.7	行動計算與遠距工作 (2 項控制措施)						
A.11.7.1	行動計算與通信	3	3	3	2	2	2.60
A.11.7.2	遠距工作	3	3	3	2	2	2.60
平均		2.88	2.92	2.76	2.44	2.28	2.66

- 個案業者在「A.11.2.4 使用者存取權限的審查」與「A.11.3.3 桌面淨空與螢幕淨空政策」的平均分數不甚理想，分別只有 1.80 與 1.60，符合程度為 60%與 53.33%，顯示電信業者沒有落實定期審查使用者的存取權限，可能發生資訊的不適當存取而造成潛在的風險威脅，同時也未確實要求桌面與螢幕淨空的措施，導致重要資訊可經由員工的桌面或資訊處理設施的螢幕上直接取得，以上兩項控制措施應進一步加以檢討。
- 個案業者在「A.11.1.1 存取控制政策」、「A.11.3.1 通行碼的使用」、「A.11.3.2 無人看管的使用者設備」、「A.11.4.3 網路設備識別」、「A.11.5.5 會談期逾時」、「A.11.5.6 連線時間的限制」、「A.11.6.2 敏感性系統的隔離」、「A.11.7.1 行動計算與通信」與「A.11.7.2 遠距工作」，平均分數介於 2.40 至 2.60 之間，符合程度則是 80%至 86.67%，顯示電信業者在以營運與安全為基礎的存取控制政策、通行碼(Password)的實務管理、無人看管設備的保護措施、網路設備的自動鑑別方法、關閉超過規定時限沒有動作的連線、限制連線時間以增加高風險應用程式的安全性、區隔出敏感性系統專屬的作業環境、行動運算設備的管理措施以及遠距工作的政策與程序等控制措施，執行管理上達到基本的水準，不過還需持續檢討改善。
- 個案業者在存取控制的其他控制措施，平均分數達到 2.8 以上，符合程度在 93.33%以上，顯示電信業者在使用者註冊程序、權限管理、通行碼的設定管理、網路存取的識別與控制、資訊群組的網路區隔、網路連線的存取限制、網路的路由控制、作業系統的防護管理與應用系統的資訊存取管理等控制措施上能有效地予以落實。

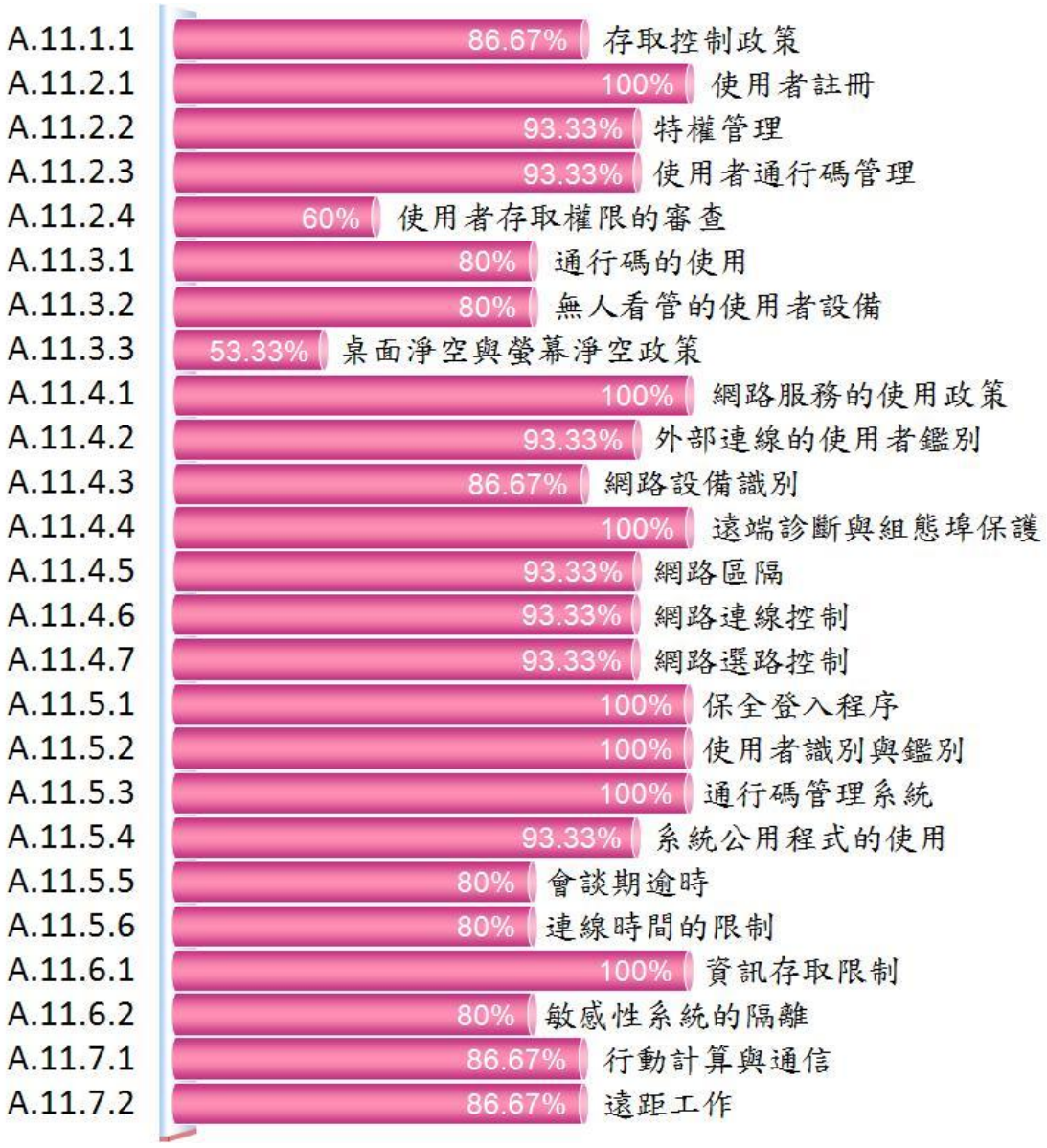

圖 4-8 個案業者於存取控制之符合程度

A.12 資訊系統獲得、開發與維護

資訊系統獲得、開發與維護包含 6 個控制目標「資訊系統的安全要求」、「應用系統的正確處理」、「密碼控制措施」、「系統檔案的安全」、「開發與支援過程的安全」與「技術脆弱性管理」以及 16 項控制措施。

- 資訊系統的安全要求：確保安全是整體資訊系統的一部分。
- 應用系統的正確處理：防止應用系統中資訊的錯誤、遺失、未經授權的修改或誤用。
- 密碼控制措施：藉由密碼方式以保護資訊的機密性、鑑別性或完整性。
- 系統檔案的安全：確保系統檔案的安全。

- 開發與支援過程的安全：維持應用系統軟體與資訊的安全。
- 技術脆弱性管理：降低因利用已公布的技術脆弱性所導致的風險。

個案業者於資訊系統獲得、開發與維護的符合狀況，如表 4-11 所示；個案業者於資訊系統獲得、開發與維護的符合程度，如圖 4-9 所示。

表 4-11 個案業者於資訊系統獲得、開發與維護之符合狀況

題號	控制措施	量化分數					平均
		T	S	A	V	W	
A.12.1	資訊系統的安全要求 (1 項控制措施)						
A.12.1.1	安全要求分析與規格	3	3	3	3	2	2.80
A.12.2	應用系統的正確處理 (4 項控制措施)						
A.12.2.1	輸入資料確認	3	3	3	2	1	2.40
A.12.2.2	內部處理的控制措施	3	3	3	2	2	2.60
A.12.2.3	訊息完整性	3	3	3	3	3	3.00
A.12.2.4	輸出資料確認	3	3	3	3	3	3.00
A.12.3	密碼控制措施 (2 項控制措施)						
A.12.3.1	使用密碼控制措施的政策	3	3	3	3	3	3.00
A.12.3.2	金鑰管理	3	3	2	2	1	2.20
A.12.4	系統檔案的安全 (3 項控制措施)						
A.12.4.1	作業軟體的控制	3	3	3	3	3	3.00
A.12.4.2	系統測試資料的保護	3	3	3	3	2	2.80
A.12.4.3	程式源碼的存取控制	3	3	3	3	2	2.80
A.12.5	開發與支援過程的安全 (5 項控制措施)						
A.12.5.1	變更控制程序	3	2	1	3	1	2.00
A.12.5.2	作業系統變更後的應用系統技術審查	3	3	3	3	3	3.00
A.12.5.3	套裝軟體變更的限制	3	3	3	3	3	3.00
A.12.5.4	資訊洩漏	2	2	2	2	2	2.00
A.12.5.5	委外的軟體開發	2	3	3	3	0	2.20
A.12.6	技術脆弱性管理 (1 項控制措施)						
A.12.6.1	技術脆弱性控制	3	3	3	2	2	2.60
平均		2.88	2.88	2.75	2.69	2.06	2.65

- 個案業者在「A.12.3.2 金鑰管理」、「A.12.5.1 變更控制程序」、「A.12.5.4 資訊洩漏」與「A.12.5.5 委外的軟體開發」的平均分數偏低，在 2.00 至 2.20 之間，符合程度不到 73.33%，顯示電信業者未妥善使用密碼金鑰管理系統、缺乏標準的開發與支

援過程之變更程序、資訊洩漏的防範準則不夠周延以及沒有對委外的軟體開發善盡監督的工作，對於以上四項控制措施必須予以檢討改善。

- 個案業者在「A.12.2.1 輸入資料確認」、「A.12.2.2 內部處理的控制措施」與「A.12.6.1 技術脆弱性控制」，平均分數為 2.40 至 2.60 之間，符合程度在 80%至 86.67%，顯示電信業者在確保正確輸入資料至應用系統、應用系統的驗證機制確認資訊是否有毀損以及評估資訊系統技術上的弱點並採取應變計畫等控制措施，實際執行情況尚可，然而仍有待改善的空間。
- 個案業者在資訊系統獲得、開發與維護的其他控制措施，平均分數都有 2.8 以上，符合程度則在 93.33%以上，顯示電信業者對於資訊系統的安全要求、應用系統的訊息完整性與資料輸出的確認、作業系統的控制程序、管制系統測試資料、限制程式源碼的存取、作業系統變更時審查關鍵的應用系統以及管控套裝軟體的變更等控制措施能有效執行。

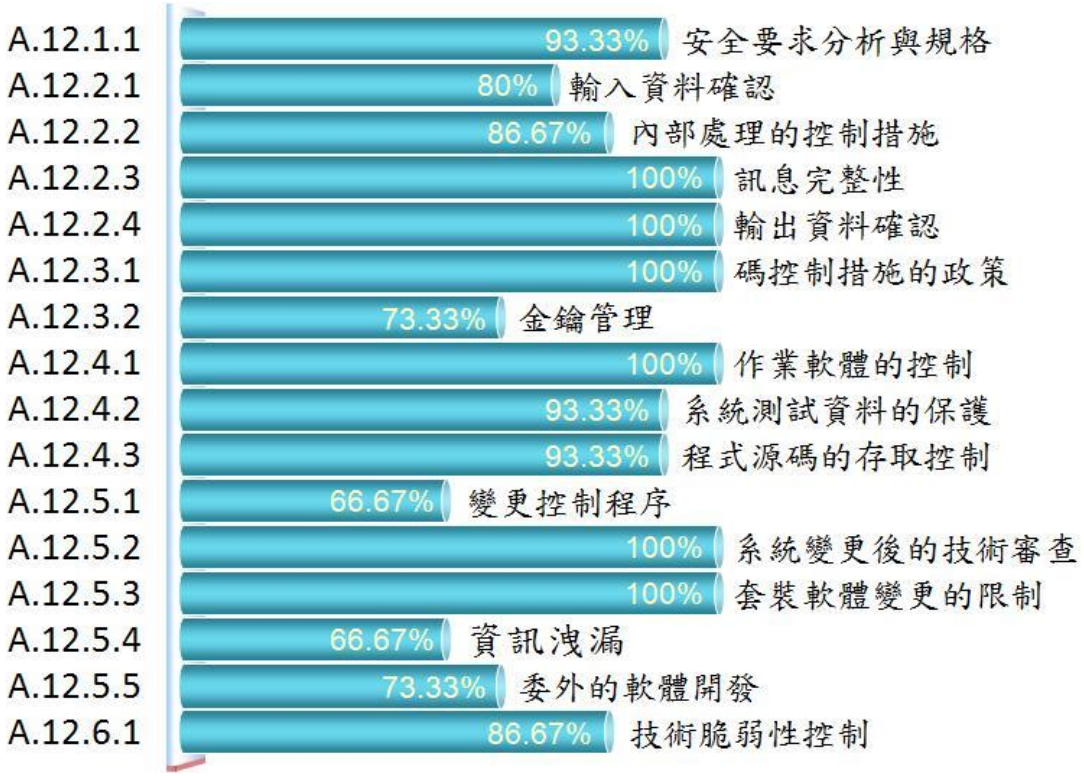

圖 4-9 個案業者於資訊系統獲得、開發與維護之符合程度

A.13 資訊安全事件管理

資訊安全事件管理包含 2 個控制目標「通報資訊安全事件與弱點」與「資訊安全事件與改進的管理」以及 5 項控制措施。

- 通報資訊安全事件與弱點：確保與資訊系統相關的資訊安全事件與弱點，被以能夠採取及時矯正措施的方式傳達。

● 資訊安全事件與改進的管理:確保採用一致與有效做法於資訊安全事件的管理。

個案業者於資訊安全事件管理的符合狀況，如表 4-12 所示；個案業者於資訊安全事件管理的符合程度，如圖 4-10 所示。

表 4-12 個案業者於資訊安全事件管理之符合狀況

題 號	控 制 措 施	量 化 分 數					平 均
		T	S	A	V	W	
A.13.1	通報資訊安全事件與弱點 (2 項控制措施)						
A.13.1.1	通報資訊安全事件	3	3	3	3	2	2.80
A.13.1.2	通報安全弱點	3	3	3	3	2	2.80
A.13.2	資訊安全事件與改進的管理 (3 項控制措施)						
A.13.2.1	責任與程序	3	3	3	3	3	3.00
A.13.2.2	從資訊安全事件中學習	3	3	2	3	2	2.60
A.13.2.3	證據的收集	3	3	3	2	1	2.40
平均		3.00	3.00	2.80	2.80	2.00	2.72

- 個案業者在「A.13.2.2 從資訊安全事件中學習」與「A.13.2.3 證據的收集」的平均分數稍低，為 2.60 與 2.40，符合程度則是 86.67%與 80%，顯示電信業者對於資訊安全事件的量化機制以及資訊安全事件發生後的證據收集行動，在執行程序上仍有待進一步改善。
- 個案業者在資訊安全事件管理的其他控制措施，平均分數在 2.8 以上，符合程度具有 93.33%以上，顯示電信業者在通報傳達資訊安全事件與弱點的程序，以及建立管理責任以確保資訊安全事件能迅速有效的反應等控制措施上處理得相當完善。

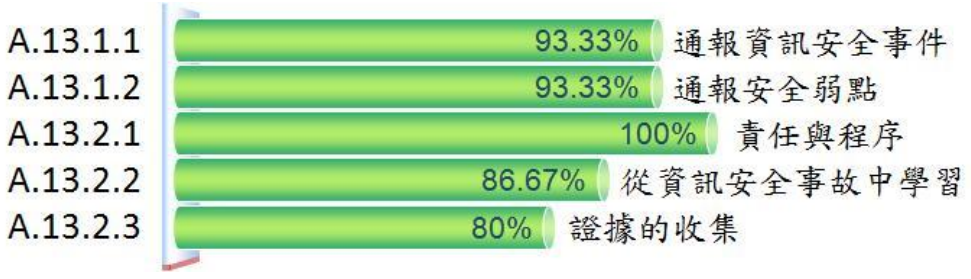

圖 4-10 個案業者於資訊安全事件管理之符合程度

A.14 營運永續管理

營運永續管理包含 1 個控制目標「營運永續管理的資訊安全層面」以及 5 項控制措施。

- 營運永續管理的資訊安全層面：為對抗營運活動中斷，保護重要營運過程不受重大資訊系統失效或災害的影響，並確保及時再續(Resumption)。

個案業者於營運永續管理的符合狀況，如表 4-13 所示；個案業者於營運永續管理的符合程度，如圖 4-11 所示。

表 4-13 個案業者於營運永續管理之符合狀況

題號	控制措施	量化分數					平均
		T	S	A	V	W	
A.14.1	營運永續管理的資訊安全層面 (5 項控制措施)						
A.14.1.1	資訊安全納入營運永續管理過程	3	3	2	3	2	2.60
A.14.1.2	營運永續與風險評鑑	3	3	2	3	3	2.80
A.14.1.3	發展與實作包括資訊安全的永續計畫	3	3	3	3	3	3.00
A.14.1.4	營運永續計畫框架	3	3	3	3	2	2.80
A.14.1.5	營運永續計畫的測試、維護及重新評鑑	3	2	3	3	1	2.40
平均		3.00	2.80	2.60	3.00	2.20	2.72

- 個案業者在「A.14.1.1 資訊安全納入營運永續管理過程」與「A.14.1.5 營運永續計畫的測試、維護及重新評鑑」的平均分數分別為 2.60 與 2.40，符合程度則是 86.67%與 80%，顯示電信業者的營運永續管理層面並未完整涵蓋資訊安全的部分，也沒有定期更新營運永續管理計畫，此部分有必要儘速加以檢討。
- 個案業者在營運永續管理的其他控制措施，平均分數在 2.8 以上，符合程度具有 93.33%以上，顯示電信業者對於評鑑可能導致營運中斷的事件之機率及影響層面、發展涵蓋資訊安全的營運永續計畫以及維持營運永續計畫的一致性架構等控制措施能予以適當執行。

圖 4-11 個案業者於營運永續管理之符合程度

A.15 遵循性

遵循性包含 3 個控制目標「遵循適法性要求」、「遵循安全政策、標準和技術符合」與「資訊系統稽核考量因素」以及 10 項控制措施。

- 遵循適法性要求：避免違反任何法律、法令、法規或契約義務，以及任何安全要求。
- 遵循安全政策、標準和技術符合：確保系統遵循組織的安全政策與標準。
- 資訊系統稽核考量因素：使資訊系統稽核過程的有效性最大化，並使其產生或受到之干擾降至最低。

個案業者於遵循性的符合狀況，如表 4-14 所示；個案業者於遵循性的符合程度，如圖 4-12 所示。

表 4-14 個案業者於遵循性之符合狀況

題號	控制措施	量化分數					平均
		T	S	A	V	W	
A.15.1	遵循適法性要求 (6 項控制措施)						
A.15.1.1	識別適用之法條	3	3	3	3	2	2.80
A.15.1.2	智慧財產權	3	3	3	3	3	3.00
A.15.1.3	組織紀錄的保護	3	3	3	3	3	3.00
A.15.1.4	個人資訊的資料保護與隱私	3	3	3	3	3	3.00
A.15.1.5	防止資訊處理設施的誤用	3	3	3	3	3	3.00
A.15.1.6	密碼控制措施的規定	3	3	3	3	3	3.00
A.15.2	遵循安全政策、標準和技術符合 (2 項控制措施)						
A.15.2.1	安全政策與標準的遵循性	3	3	2	3	3	2.80
A.15.2.2	技術遵循性查核	3	3	2	3	2	2.60
A.15.3	資訊系統稽核考量因素 (2 項控制措施)						
A.15.3.1	資訊系統稽核控制	3	3	3	3	2	2.80
A.15.3.2	資訊系統稽核工具的保護	3	3	3	3	3	3.00
平均		3.00	3.00	2.80	3.00	2.70	2.90

- 個案業者在「A.15.2.2 技術遵循性查核」的平均分數是 2.60，符合程度則是 86.67%，雖然執行情況尚可，但相較於遵循性的其它控制措施，算是分數偏低的部分，顯示電信業者並未確實地定期查核資訊系統是否遵循安全的實作準則。
- 個案業者在遵循性的其他控制措施，平均分數都在 2.8 以上，若不計入 A.15.2.2 技術遵循性查核，符合程度達到 97.78%，顯示電信業者在遵循法規的安全要求、組織

重要紀錄的保護、個人隱私的保護、防止資訊處理設施遭到誤用、確保遵循安全政策與標準的程序以及最大化資訊系統稽核過程的有效性並降低其干擾等控制措施落實得相當徹底。

圖 4-12 個案業者於遵循性之符合程度

4.2 核心版遴選分析

本研究 2.3 節說明了 ISO 27001 適用於所有類型的組織，4.1 節的評核結果分析也顯示 ISO 27001 可適用於電信事業，因此對於尚未建置與實作資訊安全管理系統的電信業者，ISO 27001 所包含的控制措施是相當合適的遵循準則。ISO 27001 所載錄的控制措施雖然都有其重要性，然而對於有計畫自行建立資訊安全管理系統的電信業者而言，要全面實施 ISO 27001 的 133 項控制措施，可能受限於經費或資源不足等因素，有實務上的困難，因此實際施行時必須有所取捨，應挑選部分控制措施為優先執行項目。

研究者實地訪談個案業者的資訊安全管理部門之主管或員工，參考他們在建立、實作、監視、審查、維護及改善資訊安全管理系統的實務經驗與意見，發展出一套適用於電信業的資訊安全管理建議，稱之為「ISO 27001 核心版」，核心版的內容集合了 ISO 27001 控制措施的重點項目，提供其他規模較小的電信業者或新進電信業者參考，有意導入資訊安全管理的業者在初期時可以聚焦在本研究建議的核心版控制措施上，先以提升組織的資訊安全管理層次為目標，待資源充裕或具備資訊安全管理的基礎與經驗時，再繼續進行其他剩餘的 ISO 27001 控制措施。

為促使本研究提出的核心版內容更具專業性且可昭公信，研究者另外向兩位具備電信產業背景且擁有 ISO 27001 主導稽核員(Lead Auditor)認證的專家請益，綜合他們在資訊安全管理的經驗以及長期對電信產業的瞭解，希望以有別於局內人的觀點，為本研究提供客觀的意見。

以下說明核心版的遴選原則：

- 該項控制措施超過一半業者(即 3 家以上) 認為應列入核心版。
- 該項控制措施至少有一位專家認為應列入核心版。

必須同時符合上述兩項條件才得以列入核心版，依循這樣的遴選原則，最後從 133 項控制措施中篩選出 58 項控制措施，作為核心版的內容，如表 4-15 所示，並整合說明受訪者選擇的理由。

表 4-15 電信業之 ISO 27001 核心版

題 號	控 制 措 施	遴 選 理 由
A.5 安全政策		
A.5.1.1	資訊安全政策文件	資訊安全政策文件定義組織資訊安全的目的、範圍、原則與方針。
A.5.1.2	資訊安全政策之審查	資訊安全政策應與時俱進，以因應組織環境、營運環境、法律條件或技術環境的改變。
A.6 資訊安全組織		
A.6.1.1	管理階層對資訊安全的承諾	資訊安全管理若無管理階層的支持與承諾，則必然受到阻礙而無法全力的推動。
A.6.1.2	資訊安全協調工作	資訊安全管理並非只是資訊部門的工作，必須跨部門協調配合，才能順利地推動執行。
A.6.1.3	資訊安全責任的配置	應明確定義各項資產的安全責任，並陳述管理人員的負責範圍，以避免灰色地帶。
A.6.1.5	機密性協議	組織應清楚定義機密性或保密協議的要求，對於資訊保護的要求才能有所遵循。
A.6.2.1	與外部團體相關的風險之識別	允許外部團體對組織的資訊存取之前，必須執行風險評鑑並採取適當的控制措施，且應確保外部團體瞭解其義務與責任。
A.7 資產管理		
A.7.1.1	資產清冊	若不識別所有的資產並記錄其資訊、價值及重要性，則無法進行風險評鑑，而風險評鑑是建立資訊安全管理系統的重要環節。
A.7.1.2	資產的擁有權	應指定資產的擁有者，以確認資產管理責任的歸屬，也方便日後追蹤。
A.7.2.1	分類指導綱要	資訊分類是決定如何處置和保護資訊的最快方法，適當的分類提供不同的保護等級，以採取合適的控制措施。
A.7.2.2	資訊標示與處置	針對不同分類等級，定義相對應的標示與處理程序，以避免不當的操作。

A.8 人力資源安全		
A.8.1.3	聘僱條款與條件	確保該員在取得資訊存取權限之前瞭解並同意組織資訊安全的政策與要求。
A.8.2.2	資訊安全認知、教育及訓練	唯有組織全體人員具備資訊安全意識與認知，並瞭解資訊安全政策與程序，才能做好安全防護工作，教育訓練活動是推動資訊安全管理的基本環節。
A.8.3.2	資產的歸還	資產是組織營運的重要基礎，落實資產歸還以確保重要資訊的安全。
A.8.3.3	存取權限的移除	避免離職人員的蓄意行為使得資訊毀損或資訊洩漏，應立即移除存取的權限。
A.9 實體與環境安全		
A.9.1.1	實體安全周界	實體的防護能供組織與資訊設施最基本的安全保障，避免未經授權的人員擅自闖入。
A.9.1.2	實體進入控制措施	建立進出安全區域的權限控制程序與管理方式以保護資訊處理設施。
A.9.2.1	設備安置與保護	適當地安置設備可以避免環境的潛在威脅，提高資訊處理設施的安全性。
A.9.2.6	設備的安全汰除或再使用	避免敏感性資訊外流，應在設備丟棄之前確保資訊徹底刪除且無法被回復擷取。
A.10 通訊與作業管理		
A.10.1.1	文件化作業程序	將資訊處理設施的相關操作程序予以文件化，可以確保一致性的作業流程，不會因為不同人員操作而有不同的方式。
A.10.1.2	變更管理	必須有充分的營運理由才能對運作中的系統做變更，且應遵循嚴格的變更管理程序，以避免系統因不當變更而發生故障。
A.10.1.3	職務的區隔	透過區隔職務與責任，可以降低資訊資產遭到意外或蓄意毀損的風險。
A.10.4.1	對抗惡意碼的控制措施	電腦病毒的威脅重大，應使用防毒軟體做預防、偵測與清除，並定期更新病毒碼與掃描引擎。
A.10.5.1	資訊備份	備份是維持資訊完整性與可用性的最後一道防線，應定期執行備份工作並確保資料可從災難事件中還原回復。
A.10.6.1	網路控制措施	網路攻擊的威脅嚴重，應以多重防禦機制確保網路安全，降低駭客入侵與外在襲擊的風險。
A.10.7.3	資訊處置程序	組織應建立一致性的程序以規範資訊的處理、存取與儲存方式。
A.10.7.4	系統文件的安全	系統文件包含敏感的資訊，應考量其安全性，避免未經授權的存取。
A.10.8.5	營運資訊系統	資訊系統涵蓋的範圍廣泛，也因此增加營運資訊散布的機會，必須建立適當的規章與程序。

A.10.9.1	電子商務	電子商務有別於實體商店，需提高安全性以降低詐欺活動與合約糾紛等威脅。
A.10.9.2	線上交易	許多買賣關係透過線上交易而建立，應提升線上交易各個環節的安全性。
A.10.9.3	公眾可用的資訊	對外公開的資訊應要求完整性，並且以適當機制保護避免受到不當的竄改。
A.10.10.1	稽核存錄	對於使用者的存取過程的細節、系統狀態與資訊安全事件均應予以記錄。
A.10.10.6	鐘訊同步	組織資訊系統的時間同步可避免系統之間的溝通產生問題，且可確保日誌檔案的準確性。
A.11 存取控制		
A.11.1.1	存取控制政策	組織內有存取資訊或資訊系統的需求，因此應建立政策作為存取管理的指導原則。
A.11.2.1	使用者註冊	基於存取管理的需求，應建立正式的使用者註冊與註銷程序。
A.11.2.3	使用者通行碼管理	使用者在存取資訊系統與服務之前，需以通行碼作為驗證的方法，因此應有適當的管理程序。
A.11.4.1	網路服務的使用政策	組織對於存取網路與網路服務，應建立政策作為施行程序與規範。
A.11.4.5	網路區隔	依不同的安全性需求將網路區隔，可簡化網路架構，也方便網路管理。
A.11.4.6	網路連線控制	對於不同的網路連線需求，依據存取控制政策管控存取權限與連線能力。
A.11.6.1	資訊存取限制	個別應用系統有不同的資訊存取考量，應依據存取控制政策予以限制。
A.12 資訊系統獲得、開發與維護		
A.12.2.1	輸入資料確認	資訊必須具有高度的可靠性，因此在資料輸入到系統時應實施核對。
A.12.2.2	內部處理的控制措施	雖然資料輸入時經過核對，但仍可能發生錯誤，需透過系統的查核做再次的確認。
A.12.2.4	輸出資料確認	理論上，經由資料輸入確認及系統查核確認可以確保資料輸出的正確性無誤，但在某些情況下，系統有極小的偏誤值，因此確認輸出資料做最後的把關動作。
A.12.4.3	程式源碼的存取控制	程式源碼對於系統有相當高的重要性，因此程式源碼的存取應予以嚴格控制。
A.12.5.1	變更控制程序	系統軟體的變更會衝擊營運環境，為降低資訊系統毀損的風險，應建立變更管理程序以控制變更的實作過程。

A.12.6.1	技術脆弱性控制	資訊系統存在許多潛在的弱點，因此必須及時取得相關技術資訊，以評估其影響範圍，並採取適當的行動。
A.13 資訊安全事件管理		
A.13.1.1	通報資訊安全事件	資訊安全事件應儘速受到控制，必須建立通報程序以及事件回應程序，以採取必要的行動。
A.13.1.2	通報安全弱點	資訊系統與服務的弱點可能由員工、承包商或第三方使用者發現，應建立通報程序以預防資訊安全事件的發生。
A.13.2.1	責任與程序	為確保資訊安全事件一旦發生，能迅速有效的採取行動，應建立相關的管理責任與程序。
A.13.2.2	從資訊安全事件中學習	應從資訊安全事件中得到教訓，評估各項得到的資訊，以避免事件重複發生。
A.14 營運永續管理		
A.14.1.1	資訊安全納入營運永續管理過程	確保組織的營運永續發展，應建立一套永續管理過程並涵蓋資訊安全管理。
A.14.1.2	營運永續與風險評鑑	世事難以預料，透過風險評估瞭解任何可能導致營運中斷的事件之機率與衝擊。
A.14.1.3	發展與實作包括資訊安全的永續計畫	為確保重要的營運過程發生中斷時，可以在最短時間內恢復運作，應建立營運永續計畫，具體規範所需服務與資源的安排。
A.14.1.5	營運永續計畫的測試、維護及重新評鑑	環境不斷變化，因此營運永續計畫也應測試並定期審查，以確保其有效性。
A.15 遵循性		
A.15.1.1	識別適用之法條	遵守相關法規是最基本的要求，因此應識別資訊系統所適用的法條。
A.15.1.2	智慧財產權	避免侵犯智慧財產權，組織資料與資訊系統軟體應遵守相關法規要求。
A.15.1.3	組織紀錄的保護	部分組織記錄受到法規要求或支援必要的營運活動，需要予以安全的保存。
A.15.1.4	個人資訊的資料保護與隱私	組織應視顧客資料與隱私為重要資產，必須遵守相關法規要求予以嚴密的保護。

4.3 IPA 矩陣分析

本節運用重要性-表現程度分析法(Important-Performance Analysis)或稱 IPA 矩陣，整合 4.1 節與 4.2 節的分析結果，說明電信業者對於 133 項控制措施的施行策略。

IPA 矩陣最早由 Martilla 與 James 於 1977 年分析汽車機械產品屬性研究時所提出的架構，將重要性與表現情況以二維矩陣呈現，是測量屬性重要程度與表現程度的理想工具，分析的結果以四個象限表示，各象限有不同的策略意義，如圖 4-2 所示。

圖 4-13 IPA 分析矩陣

第一象限：表示重要程度高同時表現程度良好，應予以繼續保持。

第二象限：表示重要程度高但表現程度不佳，應集中資源於此，專心致力改善措施。

第三象限：表示重要程度與表現程度皆差，因重要程度不高，所以改善的優先順序較低。

第四象限：表示重要程度低但表現程度良好，有過度供給的狀況。

本研究採用 IPA 矩陣，在表現程度上利用 4.1 節的評核分析結果，以個案業者在 133 項控制措施的符合狀況之平均分數 2.70 為分隔點，控制措施平均分數若高於 2.70 為表現程度較佳，低於 2.70 則為表現程度較差；至於重要程度則利用 4.2 節的核心版遴選結果，列入核心版的控制措施為重要程度較高，未列入核心版的控制措施為重要程度較低。

根據上述重要程度與表現程度的分隔點條件，藉由 IPA 矩陣將 133 項控制措施歸類至 IPA 矩陣的 4 個象限，各象限內的控制措施可依該象限的指導方針採取適當的行動：

第一象限內的控制措施應繼續保持良好的表現；第二象限內的控制措施應優先予以改善；第三象限內的控制措施則是行有餘力時再加以改善；第四象限內的控制措施則可忽略，應避免投入過多資源於此。ISO 27001 的 133 項控制措施之 IPA 矩陣分析結果如表 4-16 所示。

表 4-16 ISO 27001 控制措施之 IPA 矩陣分析結果

象限	控制措施	
保持優勢 (37 項控制措施) 第一象限	A.6.1.3 資訊安全責任的配置	A.7.1.1 資產清冊
	A.7.1.2 資產的擁有權	A.7.2.1 分類指導綱要
	A.7.2.2 資訊標示與處置	A.8.1.3 聘僱條款與條件
	A.8.3.2 資產的歸還	A.8.3.3 存取權限的移除
	A.9.1.1 實體安全周界	A.9.1.2 實體進入控制措施
	A.9.2.1 設備安置與保護	A.9.2.6 設備的安全汰除或再使用
	A.10.1.1 文件化作業程序	A.10.5.1 資訊備份
	A.10.6.1 網路控制措施	A.10.9.1 電子商務
	A.10.9.2 線上交易	A.10.9.3 公眾可用的資訊
	A.10.10.1 稽核存錄	A.10.10.6 鐘訊同步
	A.11.2.1 使用者註冊	A.11.2.3 使用者通行碼管理
	A.11.4.1 網路服務的使用政策	A.11.4.5 網路區隔
	A.11.4.6 網路連線控制	A.11.6.1 資訊存取限制
	A.12.2.4 輸出資料確認	A.12.4.3 程式源碼的存取控制
	A.13.1.1 通報資訊安全事件	A.13.1.2 通報安全弱點
	A.13.2.1 責任與程序	A.14.1.2 營運持續與風險評鑑
	A.14.1.3 發展與實作包括資訊安全的持續計畫	A.15.1.1 識別適用之法條
	A.15.1.2 智慧財產權	A.15.1.3 組織紀錄的保護
	A.15.1.4 個人資訊的資料保護與隱私	
優先改善 (21 項控制措施) 第二象限	A.5.1.1 資訊安全政策文件	A.5.1.2 資訊安全政策之審查
	A.6.1.1 管理階層對資訊安全的承諾	A.6.1.2 資訊安全協調工作
	A.6.1.5 機密性協議	A.6.2.1 與外部團體相關的風險之識別
	A.8.2.2 資訊安全認知、教育及訓練	A.10.1.2 變更管理
	A.10.1.3 職務的區隔	A.10.4.1 對抗惡意碼的控制措施
	A.10.7.3 資訊處置程序	A.10.7.4 系統文件的安全
	A.10.8.5 營運資訊系統	A.11.1.1 存取控制政策
	A.12.2.1 輸入資料確認	A.12.2.2 內部處理的控制措施
	A.12.5.1 變更控制程序	A.12.6.1 技術脆弱性控制

	A.13.2.2 從資訊安全事件中學習	A.14.1.1 資訊安全納入營運持續管理過程
	A.14.1.5 營運持續計畫的測試、維護及重新評鑑	
次要改善(33項控制措施) 第三象限	A.6.1.4 資訊處理設施的授權過程	A.6.1.6 與權責機關的聯繫
	A.6.1.7 與特殊利害相關團體的聯繫	A.6.1.8 資訊安全的獨立審查
	A.6.2.2 處理客戶事務的安全說明	A.8.1.2 篩選
	A.9.1.5 在安全區域內工作	A.9.2.5 場所外設備的安全
	A.9.2.7 財產的攜出	A.10.1.4 開發、測試及運作設施的分隔
	A.10.2.2 第三方服務的監視與審查	A.10.2.3 第三方服務變更的管理
	A.10.3.1 容量管理	A.10.3.2 系統驗收
	A.10.4.2 對抗行動碼的控制措施	A.10.10.2 監控系統的使用
	A.10.10.4 管理者與操作者日誌	A.10.10.5 失誤存錄
	A.11.2.4 使用者存取權限的審查	A.11.3.1 通行碼的使用
	A.11.3.2 無人看管的使用者設備	A.11.3.3 桌面淨空與螢幕淨空政策
	A.11.4.3 網路設備識別	A.11.5.5 會談期逾時
	A.11.5.6 連線時間的限制	A.11.6.2 敏感性系統的隔離
	A.11.7.1 行動計算與通信	A.11.7.2 遠距工作
	A.12.3.2 金鑰管理	A.12.5.4 資訊洩漏
	A.12.5.5 委外的軟體開發	A.13.2.3 證據的收集
	A.15.2.2 技術遵循性查核	
過度重視(42項控制措施) 第四象限	A.6.2.3 第三方協議中之安全說明	A.7.1.3 資產之可被接受的使用
	A.8.1.1 角色與責任	A.8.2.1 管理階層責任
	A.8.2.3 懲處過程	A.8.3.1 終止責任
	A.9.1.3 保全辦公室、房間及設施	A.9.1.4 對外部與環境威脅的保護
	A.9.1.6 公共進出、收發及裝卸區	A.9.2.2 支援的公用設施
	A.9.2.3 佈纜的安全	A.9.2.4 設備維護
	A.10.2.1 服務交付	A.10.6.2 網路服務的安全
	A.10.7.1 可移除式媒體的管理	A.10.7.2 媒體的汰除
	A.10.8.1 資訊交換政策與程序	A.10.8.2 交換協議
	A.10.8.3 輸送中的實體媒體	A.10.8.4 電子傳訊
	A.10.10.3 日誌資訊的保護	A.11.2.2 特權管理
	A.11.4.2 外部連線的使用者鑑別	A.11.4.4 遠端診斷與組態埠保護
	A.11.4.7 網路選路控制	A.11.5.1 保全登入程序
	A.11.5.2 使用者識別與鑑別	A.11.5.3 通行碼管理系統
	A.11.5.4 系統公用程式的使用	A.12.1.1 安全要求分析與規格
	A.12.2.3 訊息完整性	A.12.3.1 使用密碼控制措施的政策

	A.12.4.1 作業軟體的控制	A.12.4.2 系統測試資料的保護
	A.12.5.2 作業系統變更後的應用系統技術審查	A.12.5.3 套裝軟體變更的限制
	A.14.1.4 營運持續計畫框架	A.15.1.5 防止資訊處理設施的誤用
	A.15.1.6 密碼控制措施的規定	A.15.2.1 安全政策與標準的遵循性
	A.15.3.1 資訊系統稽核控制	A.15.3.2 資訊系統稽核工具的保護

- 第一象限：計 37 項控制措施列入核心版且平均分數高於 2.70，應繼續維持此優勢。
- 第二象限：計 21 項控制措施列入核心版但分數低於 2.70，應利用所有資源予以優先改善。
- 第三象限：計 33 項控制措施未列入核心版且分數低於 2.70，為次要改善項目，待第二象限項目改善完成後再做處理。
- 第四象限：計 42 項控制措施未列入核心版但分數高於 2.70，其表現程度良好但非重要項目，因此可不予理會。

第五章 結論與建議

本章旨在總結本研究之成果與建議，共分為二節。5.1 節摘要彙整研究之發現；5.2 節提出未來的研究建議，供後續研究者、電信業者與資訊安全相關業者做進一步探討。

5.1 研究結論

資訊科技的發展之迅速超乎想像，凡事資訊化的環境徹底顛覆人類的生活方式，但伴隨而來的是令人頭疼的資訊安全問題。資訊安全涵蓋範圍廣泛，除了一般人熟知的網路安全、侵入攻擊與電腦病毒，也包括了實體安全、資產管理、作業管理、資訊安全事件管理、營運永續管理及法規的遵循等方面，因此要做好資訊安全的工作，單靠軟、硬體並不足以應付無所不在的安全威脅，必須以全面性的思維，兼顧技術面與管理面來鞏固資訊安全的防禦工事。

電信服務業與人們的生活密不可分，作為網路服務的提供者，電信業者負責傳遞所有的訊息與流量，因此電信業者能扮演守門員的角色，攔阻所有的惡意活動，以提供使用者乾淨安全的網路環境，未來可預期電信業者將被賦予更多維護資訊安全的重任，對此電信業者本身的資訊安全管理也值得探討。

本研究以電信業者的資訊安全管理系統(ISMS)為研究的核心主軸，運用資訊安全標準 ISO 27001 的要求規範，實地訪查電信業者的資訊安全管理執行現況，其具體成果簡述如下：

- 建立以 ISO 27001 控制要項與控制措施為基礎的評核表，且仿照 ISO 的稽核驗證方式，將電信業者的資訊安全管理狀況具體呈現並予以量化，以利分析歸納。
- 整體而言，依據 ISO 27001 的控制措施，個案業者的資訊安全管理之符合程度達到 90%，顯示電信產業的資訊安全管理具有不錯的水準。電信業者在資訊安全管理的表現，與公司的規模及獲利情況有相當程度的關聯性，規模愈大、獲利愈佳的電信業者較有意願投入資訊安全管理，並積極取得相關認證。
- 個案業者在資訊安全管理執行情況上，表現較佳的是「資產管理」與「遵循性」，而表現欠佳需要加以改善的是「安全政策」與「資訊安全組織」；以資訊安全管理三個面向探討，整體而言，策略面表現優於管理面，而管理面優於作業面。個案業者在 133 項控制措施的符合情況與數據，可作為其他業者爾後建立資訊安全管理系統時參考。
- 綜合個案業者的實務經驗與 ISO 27001 主導稽核員的專家意見，提出包含 58 項 ISO 27001 控制措施且適用於電信產業的資訊安全管理建議：ISO 27001 核心版，

供有意自行建立資訊安全管理系統，但礙於實際環境因素無法全面推動 ISO 27001 的業者參考。

- 運用 IPA(Important-Performance Analysis)矩陣分析電信業者對於 133 項控制措施的施行策略。其中 37 項控制措施列入核心版且平均分數高於 2.70，應繼續維持；21 項控制措施列入核心版但分數低於 2.70，予以優先改善；33 項控制措施未列入核心版且分數低於 2.70，為次要改善項目；42 項控制措施未列入核心版但分數高於 2.70，可不予理會。
- 國內文獻過去未有相關研究以資訊安全標準為基礎探討電信產業的資訊安全管理，本研究開風氣之先，以 ISO 27001 評估國內第一類電信業者的資訊安全管理施行現況，希望能提升電信業者的資訊安全意識，建立完整的安全防護體系，也期盼此舉有拋磚引玉的效果，未來有更多研究者持續深入的探討。

5.2 後續研究建議

本研究之研究方法與研究結論，礙於若干因素限制(請參考 3.5 節)，未臻完備之處，尚待後續研究持續探討：

- 本研究主題探討電信業者的資訊安全管理，對於部分敏感的資訊，受訪者在安全考量與自我防衛的前提之下，陳述時傾向持保留態度，建議採長期參與觀察的方法，以利深入瞭解；此外，本研究根據有限的個案資料歸納分析，缺乏量化數據的支持，未來藉由結構化問卷的方式進行定量研究，以做進一步驗證。
- 國內電信業務繁雜，經營業者眾多，總計高達 606 家，本研究以第一類電信業者為研究對象，未來可將第二類電信業者納入研究範圍，以對整體電信產業的資訊安全管理狀況有完整的瞭解。
- 本研究以 ISO 27001 作為探討電信業者資訊安全管理的基礎，其標準規範的 133 項控制措施雖然涵蓋範圍廣泛，但仍可能有未盡之事宜，未來可針對電信產業的特性，發展額外的控制目標與控制措施，讓電信業者的資訊安全管理更為完善。
- 資訊系統的發展趨勢由封閉式系統過渡至開放式系統，電信產業亦不例外，許多通訊標準與設備逐漸走向開放式架構，這也意謂著電信業者將面臨更為嚴峻的資訊安全威脅，未來可針對開放式系統對於電信業者在資訊安全管理的影響層面做深入的探討。
- 現階段電信業者提供網路服務予使用者，但並未阻斷惡意的攻擊活動，因此在某種程度上電信業者間接成了資訊安全問題的幫兇，未來如何提供更多資訊安全的解決方案或加值服務(例如：病毒掃描或入侵偵測防護等)，提升電信服務的等級與價值，可作為市場行銷的研究主題，也是電信業者需加以思考的課題。

參考文獻

中文部分

[1] Babbie, Earl R. (2007)，社會科學研究方法，十版，陳文俊譯，雙葉書廊，台北。

[2] BSI 英國標準協會(2007)，「資訊安全管理系統基礎課程」。

[3] 方仁威(2006)，「資訊安全管理系統驗證作業之研究」，國立交通大學，博士論文。

[4] 行政院國家資通安全會報，http://www.nicst.nat.gov.tw，2009 年 3 月。

[5] 李仁暉(2008)，「台灣金融業導入資訊安全管理系統關鍵成功因素研究—以 A 金控為例」，淡江大學管理科學研究所，碩士論文。

[6] 杜偉欽(2006)，「結合 HIPAA 與 ISO27001 為基礎探討醫療院所資訊安全管理之研究」，國立成功大學，碩士論文。

[7] 李慧蘭(2006)，「國際資訊安全標準 ISO 27001 之網路架構設計－以國網中心為例探討風險管理」，TANET2006，台北。

[8] 林曙熙(2004)，「企業資訊安全管理之認知與實施研究」，國立清華大學工業工程研究所，碩士論文。

[9] 侯皇熙(2004)，「植基於 BS7799 探討政府部門的資訊安全管理—以海關資訊部門為例」，國立成功大學，碩士論文。

[10] 查士朝(2006)，「BS 7799/ISO 17799/ISO 27001 資訊安全管理制度介紹與導入實務」，資誠會計師事務所。

[11] 柯心瀅(2000)，「大陸軟體研發人才招募與管理」，國立交通大學，碩士論文。

[12] 國家通訊傳播委員會，http://www.ncc.tw，2009 年 2 月。

[13] 國家資通安全會報(2004)，「各政府機關(構)落實資安事件危機處理具體執行方案」。

[14] 國家資通安全會報(2005)，「政府機關(構)資訊安全責任等級分級作業施行計畫」。

[15] 許雪蓮(2006)，「以 BS7799 為基礎評估軍事單位資訊安全環境之研究：以國軍 M 單位為例」，大同大學資訊經營研究所，碩士論文。

[16] 陳兆祺(2007)，「導入 BS7799 標準對建立資訊安全文化影響之經驗研究—以 Y 公司為例」，大同大學資訊經營研究所，碩士論文。

[17] 陳連枝(2003)，「國內金融控股公司資訊安全管理系統之探討」，長庚大學企業管理研究所，碩士論文。

[18] 曾淑惠(2002)，「以 BS 7799 為基礎評估銀行業的資訊安全環境」，淡江大學資訊管理研究所，碩士論文。

[19] 楊智翔(2007)，「運用 CNS17799 檢視醫療院所之資訊安全管理—以屏東地區大型醫院為例」，屏東科技大學，碩士論文。

[20] 經濟部標準檢驗局(2006)，「ISO 27001:2005 資訊安全管理系統要求」。

[21] 葉相好(2002)，「運用 BS 7799 檢測醫療院所資訊安全管理作業文件之研究」，國立陽明大學衛生資訊與決策研究所，碩士論文。

[22] 鄭東昇(2005)，「資訊安全管理系統與企業網路安全實作探討」，國立交通大學資訊管理研究所，碩士論文。

英文部分

[1] Bellone, Jason (2008), "Reaching escape velocity: A practiced approach to information security management system implementation", Information Management & Computer Security, 16(1), pp. 49-57.

[2] Boehmer, Wolfgang (2008), "Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001", The Second International Conference on Emerging Security Information, Systems and Technologies, pp. 224-231.

[3] Broderick, J. Stuart (2006), "ISMS, security standards and security regulations", Information Security Technical Report, 11(1), pp. 26-31.

[4] Chang, Shuchih Ernest & Ho, Chienta Bruce (2006), "Organizational factors to the effectiveness of implementing information security management", Industrial Management & Data Systems, 106(3), pp. 345-361.

[5] Eisenhardt, Kathleen M. (1989), "Building Theories from Case Study Research", Academy of Management Review, 14(4), pp. 532-550.

[6] Ezingeard, Jean-Noel & Birchall, David (2006), "Information Security Standards: Adoption Drivers", IFIP International Federation for Information Processing, 193, pp. 1-20.

[7] Freeman, Edward H. (2007), "Holistic Information Security: ISO 27001 and Due Care", Information Security Journal: A Global Perspective, 16(5), pp. 291-294.

[8] Huang, Shi-Ming (2006), "Balancing performance measures for information security management - A balanced scorecard framework", Industrial Management & Data Systems, 106(2), pp. 242-255.

[9] Humphreys, Edward (2008), "Information security management standards: Compliance, governance and risk management", Information Security Technical Report, 13(4), pp. 247-255, November 2008.

[10] Humphreys, Ted & Plate, Angelika (2005), Measuring the effectiveness of your ISMS implementations based on ISO/IEC 27001, BSI Standards.

[11] International Register of ISMS Certificates, http://www.iso27001certificates.com, Mar 2009.

[12] ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements, October 2005.

[13] ISO/IEC 27002:2005, Information technology – Security techniques – Code of practice for information security management, April 2008.

[14] Jayawickrama, Wipul (2006), "Managing Critical Information Infrastructure Security Compliance: A Standard Based Approach Using ISO/IEC 17799 and 27001", Lecture Notes in Computer Science, 4277, pp. 565-574.

[15] Klempt, Philipp (2007), “Business Oriented Information Security Management – A Layered Approach”, Lecture Notes in Computer Science, 4804, pp. 1835-1852.

[16] Lambo, Taiye (2006), “ISO/IEC 27001: The future of infosec certification”, ISSA Journal.

[17] Laudon, Kenneth C. & Laudon, Jane P. (2006), Management Information Systems： Managing The Digital Firm, 10th Edition, Pearson Education.

[18] Sanchez, L.E. (2006), “Practical approach of a secure management system based on ISO/IEC 17799”, First International Conference on Availability, Reliability and Security (ARES’06).

[19] Yin, Robert K. (2002), Case Study Research: Design and Methods, 3rd Edition, Applied Social Research Methods Series, Vol 5, Sage Publications.

附錄 A

OECD 對資訊系統與網路安全指導綱要中所提供的各項原則，可應用至所有治理資訊系統與網路安全的政策及運作等級。ISO 27001 提供實作使用 PDCA 模型與第 4 節「資訊安全管理系統」、第 5 節「管理階層責任」、第 6 節「ISMS 內部稽核」、第 7 節「ISMS 之管理階層審查」與第 8 節「ISMS 之改善」所描述的過程，其中部分 OECD 原則對應到 ISMS 架構，如表 A-1 所示。

表 A-1 OECD 原則與 PDCA 模型

OECD 原則	對應的 ISMS 過程與 PDCA 階段
認知 參與者應瞭解安全對於資訊系統與網路的必要性，以及其如何能加強安全性。	本活動為「執行」(Do)階段的部分。
責任 所有參與者對資訊系統與網路的安全皆負有責任。	本活動為「執行」階段的部分。
回應 參與者應以即時和合作的方式行動，以預防、偵測及回應安全事件。	本項部分為「檢查」(Check)階段的監視活動，而部分為「行動」(Act)階段的回應活動。本項亦能由「規劃」(Plan)與「檢查」階段的部分層面涵蓋。
風險評鑑 參與者應施行風險評鑑。	本活動為「規劃」階段的部分，且風險評鑑亦為「檢查」階段的部分。
安全設計與實作 參與者應將安全性納入為資訊系統與網路的基本要件。	一旦完成風險評鑑，即選擇風險處理之控制措施，作為「規劃」階段的部分。「執行」階段隨後涵蓋上述控制措施的實作與運作使用。
安全管理 參與者應採用廣泛的做法進行安全管理。	風險的管理是一個包含對事件的預防、偵測與回應、持續維持、審查與稽核的過程。所有的這些層面包括在「規劃」、「執行」、「檢查」及「行動」階段中。
重新評鑑 參與者應審查並重新評鑑資訊系統與網路的安全性，並對安全政策、實務、措施及程序作適當的修訂。	資訊安全的重新評鑑是「檢查」階段的一部分，同時應採取定期審查以查核資訊安全管理系統的有效性，而安全性的改進是「行動」階段的一部分。

資料來源：ISO/IEC 27001:2005