國立台東大學資訊管理學系

碩士論文

指導教授：謝昆霖　博士

ISO 與 CMMI 兩驗證機制於組織資訊安全建構之關聯性研究

研 究 生：黃鎮屏　撰

中華民國九十八年六月

NTU Library

國立台東大學資訊管理學系

碩士論文

ISO 與 CMMI 兩驗證機制於組織資訊安全建構之關聯性研究

研 究 生：黃鎮屏　　撰
指導教授：謝昆霖　博士

中華民國九十八年六月

國立台東大學
學位論文考試委員審定書

系所別：資訊管理學系

本班 黃鎮屏 君

所提之論文 ISO與CMMI兩驗證機制於組織資訊安全建構之關聯性研究

業經本委員會通過合於 碩士學位論文 條件

論文學位考試委員會：

（學位考試委員會主席）

（指導教授）

論文學位考試日期：98 年 6 月 22 日

國 立 台 東 大 學

博碩士論文授權書

本授權書所授權之論文為本人在 國立台東大學 環境經濟資訊管理 系(所)

_____組 97 學年度第 2 學期取得 碩 士學位之論文。

論文名稱： ISO 與 CMMI 驗證機制於組織資訊安全建構之研究

本人具有著作財產權之論文全文資料，授予下列單位：

同意	不同意	單　位
☑	☐	國家圖書館
☑	☐	本人畢業學校圖書館

得不限地域、時間與次數以微縮、光碟或其他各種數位化方式重製後散布發行或上載網站，藉由網路傳輸，提供讀者基於個人非營利性質之線上檢索、閱覽、下載或列印。

本論文為本人向經濟部智慧財產局申請專利(未申請者本條款請不予理會)的附件之一，申請文號為：_____，請將全文資料延後半年再公開。

公開時程

立即公開	一年後公開	二年後公開	三年後公開
			V

上述授權內容均無須訂立讓與及授權契約書。依本授權之發行權為非專屬性發行權利。依本授權所為之收錄、重製、發行及學術研發利用均為無償。上述同意與不同意之欄位若未鉤選，本人同意視同授權。

指導教授姓名：謝銘勳 (親筆簽名)

研究生簽名：黃鎮輝 (親筆正楷)

學　　號：4396004 (務必填寫)

日　　期：中華民國 98 年 06 月 22 日

1.本授權書 (得自 http: //www.lib.nttu.edu.tw/theses/ 下載) 請以黑筆撰寫並影印裝訂於書名頁之次頁。

2.依據 91 學年度第一學期一次教務會議決議:研究生畢業論文「至少需授權學校圖書館數位化，並至遲於三年後上載網路供各界使用及校內瀏覽。」 *授權書版*

本:2005/06/09

II

博碩士論文電子檔案上網授權書

（*爲維護您的權益，請儘速寄回供授權管理用*） ID:097NTTTC396005

本授權書所授權之論文爲授權人在 國立臺東大學 資訊管理學系碩士班 _____組 97 學年度第 二 學期取得 碩士 學位之論文。

論文題目： ISO與CMMI兩驗證機制於組織資訊安全建構之關聯性研究

指導教授： 謝昆霖

茲同意將授權人擁有著作權之上列論文全文(含摘要)，非專屬、無償授權國家圖書館及本人畢業學校圖書館，不限地域、時間與次數，以微縮、光碟或其他各種數位化方式將上列論文重製，並得將數位化之上列論文及論文電子檔以上載網路方式，提供讀者基於個人非營利性質之線上檢索、閱覽、下載或列印。

☐ 上列論文爲授權人向經濟部智慧財產局申請專利之附件或相關文件之一（專利申請案號： ），請於 年 月 日後再將上列論文公開或上載網路。

☑ 因上列論文尚未正式對外發表，請於101年 7 月 18 日後再將上列論文公開或上載網路。

授權人： 黃鎮屏

親筆簽名及蓋章： _____ 民國 98 年 07 月 18 日

身分證字號： v120107956

電話： 傳真：

聯絡地址： 台東市志航路一段111巷17弄2號

E-Mail： chu.ui5460@msa.hinet.net

檔案上網授權書 第 1 頁，共 2 頁

博碩士論文電子檔案上網授權書

（提供授權人裝訂於紙本論文書名頁之次頁用）

本授權書所授權之論文爲授權人在 國立臺東大學 資訊管理學系碩士班 _____ 組 97 學年度第 二 學期取得 碩士 學位之論文。

論文題目： ISO與CMMI兩驗證機制於組織資訊安全建構之關聯性研究

指導教授： 謝昆霖

茲同意將授權人擁有著作權之上列論文全文（含摘要），非專屬、無償授權國家圖書館及本人畢業學校圖書館，不限地域、時間與次數，以微縮、光碟或其他各種數位化方式將上列論文重製，並得將數位化之上列論文及論文電子檔以上載網路方式，提供讀者基於個人非營利性質之線上檢索、閱覽、下載或列印。

- 讀者基非營利性質之線上檢索、閱覽、下載或列印上列論文，應依著作權法相關規定辦理。

授權人： 黃鎮屏

簽　名： _____ 中華民國 98 年 07 月 18 日

誌謝辭

馬亨亨大道的鳳凰花在夏日躍上枝頭綻放耀眼的火紅，這是結束與開始組合的季節，猶記得初入學時在教學大樓遠眺金光閃耀的西太平洋，而今驪歌將隨著花落花開與潮汐成為記憶的印記，回首凝望來時路，對於歷程中曾給予幫助的人，心存感恩之意，不會隨時空轉換淡忘，而是歷久彌堅銘記在心。

「師者，傳道、授業、解惑也。」感謝指導教授謝昆霖老師引導進入學術研究的領域開擴知識，得以完成此篇論文的撰寫。口試委員王昌斌教授及張耀中老師對於論文內容的指導與寶貴建議，使本論文更臻完備，謹致上最衷心的謝意。

求學期間感恩導師王文清教授循循善誘的關心進度與熱心開放的治學管理，使來自不同領域的同學，得以充實學養的廣度與深度。患難與共的俊宏、雅真、世弘與振民同學，還有相互鼓勵的同窗伙伴，在研究所的學習生涯，劃下句點後，期許彼此都能開啟人生另一學習的起點。

樣本蒐集期間，因參 CMMI 能力成熟度整合模式驗證的公務組織很少，樣本不易取得，特別感謝財稅中心長官與同仁的指導及協助，使本研究得以順利進行。

最後謹以此論文，獻給我最摯愛的家人，感謝陪我走過圖書館的許多角落，有了你們的支持，才有人生春夏秋冬的豐富養分，使我持續完成進修學程。

ISO 與 CMMI 兩驗證機制於
組織資訊安全建構之關聯性研究

作者：黃鎮屏

國立台東大學　資訊管理學系環境經濟資訊管理

摘　要

隨著全球網際網路的蓬勃發展，政府機關、企業組織與個人使用者越來越依賴網路之間流通的資訊，許多組織仰賴 IT 資源，並且相信它們是可靠的。因此，建構適切的組織資訊安全保護，應考量組織的屬性，依循有效的資訊安全管理策略，採用標準化的管理程序，可減輕因不對稱訊息所引發之管理困境，並落實組織資產的安全性保護。

許多組織在導入資訊安全管理系統時，都遇到不知如何著手的問題，本研究以導入 ISO27001 資訊安全管理系統為目標，運用「CMMI 之能力維度」指標，檢測組織資訊部門人員認知與控制措施之符合程度，探討可結合的控制項目，提升公務組織資訊安全管理及創新發展的能力度，建構民眾可信賴的資訊安全使用環境。透過單位內之資訊安全編組，依組織特性、診斷、建立、行動與學習模式，配合組織業務性質，提出導入流程改善之重點，並就個案推動所面臨挑戰與問題，提出相關的因應措施，減輕導入資訊安全管理系統模式時的龐大負擔，並逐步分析資訊安全管理系統與能力成熟度可能結合的模式。

研究結果顯示，透過 ISO27001 資訊安全管理實務，可同步完成具正向關係的 CMMI 流程領域部份一般目標，透過 PDCA 程序的不斷循環，觸發改善缺點的程序，同時支持組織核心業務目標導出的品質和流程績效。從整體的觀點而言，CMMI 能力成熟度整合模式，適用涵蓋面較廣泛，各流程領域目標的建構遵循，更有利於資訊管理人員對 ISO27001 安全管理實務認知相關觀念的確立。

關鍵字：資訊安全管理系統、驗證、能力成熟度、連續式表述模式

Establishing Organization Information Security using the Certification Systems of ISO27001 and CMMI

Author : Chenping Huang

ABSTRACT

With the flourishing development of the global Internet networks, government, enterprise organizations and personal users are increasingly reliant on information circulating via such networks. Numberous organizations depend on IT resources, and see them as reliable. However, significant online security issues exist, and once the security of organizing assets is endangered, confidential materials can flow outwards or the system can suffer major negative consequences lasting several days, resulting in significant organization losses. Therefore, adopting the standardized procedure,can reduce the predicament of management and help in implementing asset protection.

This study focuses on introducing the ISO 27001 information security administrative system and uses the indicator of CMMI to survey between cognition and excution degree of relation.To analyse inter-connected control projects, improve public affairs of organization information security management and abilities in innovative development, and establish an reliable net-environment by people.

The analytical results presented in this study shows that the administrative system of ISO 27001 information security, can achieve the general goal of CMMI part procedure field in step and simulitaneously support the quality of organizing the key objectives related to procedure performance. From an overall perspective, CMMI is a relatively extensive, most procedure goal construct, is suitable for performing cognition related to ISO 27001 security management.

Keywords : ISO , CMMI , INFORMATION SECURITY , CAPABILITY MATURITY

目　次

第一章 緒論.....1

第一節 研究背景與動機.....1
第二節 研究目的.....2
第三節 研究範圍.....3
第四節 研究流程.....3

第二章 文獻探討.....5

第一節 資訊安全議題的演進.....5
第二節 資訊安全發展趨勢.....7
第三節 國家資訊安全管理標準.....8
第四節 能力成熟度整合模式(CMMI).....12

第三章 研究設計.....21

第一節 研究架構.....21
第二節 研究方法.....23

第四章 個案分析.....25

第一節 個案說明.....25
第二節 ISO27001 導入流程規劃.....25
第三節 遭遇阻礙與解決之道.....27
第四節 問卷設計.....31

第五章 研究結果.....35

第一節 效度與信度分析.....35
第二節 受訪者分析.....36
第三節 敘述統計.....37
第四節 單因子變異數分析.....39
第五節 相關分析.....44
第六節 典型相關分析.....48
第七節 研究結果.....49

第六章 結論與建議.....51

第一節 研究結論.....51
第二節 研究限制.....54
第三節 未來研究的建議.....54

參考文獻.....55

附錄.....59

附錄 A　ISO27001 資訊安全管理系統要求項目認知次數分配表 59
附錄 B　ISO27001 資訊安全管理系統要求項目認知程度平均數與標準差 60
附錄 C　CMMI 能力成熟度相關流程領域執行程度次數分配表.....61
附錄 D　CMMI 能力成熟度相關流程領域執行程度平均數與標準差.....63
附錄 E　ISO27001 節次與 CMMI 流程領域對應統計表.....64
附錄 F　問卷 65

NTU Library

表目次

表 1-1　弱點記載統計表 1
表 1-2　行政院所屬機關安全等級分類 2
表 2-1　資訊安全管理理論彙總 6
表 2-2　PDCA 資訊安全管理程序與要求 10
表 2-3　階段表述方式與連續表述方式的優缺點比較表 13
表 2-4　CMMI 共同特徵描述 15
表 2-5　階段式流程領域分類與成熟度層級對照表 16
表 2-6　連續式流程領域分類與成熟度層級比較表 17
表 2-7　CMMI 之各個評鑑等級特性比較表 19
表 2-7　流程改善程序的主要工作及交付項目表 20
表 4-1　ISO27001 導入流程與 IDEAL 模式階段相對應表 26
表 4-2　衝擊等級評估表 28
表 4-3　營運衝擊等級對照表 29
表 4-4　風險發生可能性判定準則表 30
表 4-5　風險影響程度等級判定準則表 30
表 4-6　本研究問卷第一部份之衡量構面來源 31
表 4-7　本研究問卷第二部份之衡量構面來源 32
表 4-8　本研究問卷第三部份之衡量構面來源 33
表 5-1　ISO27001 資訊安全管理系統要求項目(第二部份)信度分析表 35
表 5-2　CMMI 能力成熟度相關流程領域項目信度分析表 35
表 5-3　ISO27001 與 CMMI 整體信度分析表 35
表 5-4　填答者職務別分析表 36
表 5-5　填答者所屬組織已通過 ISO27001 驗證分析表 37
表 5-6　填答者瞭解 ISO27001 要求事項比例 37
表 5-7　填答者知道 CMMI 能力成熟度相關流程領域比例 37
表 5-8　知悉 ISO27001 要求項目與資訊人員別認知程度變異數分析 . 40
表 5-8　知道 CMMI 與資訊職務人員別變異數檢定 41
表 5-9　ISO27001 認知程度在 CMMI 相關流程領域執行差異與否變異數檢定 42
表 5-10　不同 CMMI 成熟模式對 ISO27001 認知程度差異與否變異數檢定 43
表 5-11　不同 CMMI 成熟模式對 ISO27001 認知程度影響關係大小 44
表 5-12 ISO27001 認知程度項目與 CMMI 相關流程領域執行程度相關性 45
表 5-13　典型相關分析表 48
表 5-14 CMMI 相關流程領域部份一般目標與 ISO27001 要求項目關係

係數表.....49
表 6-1　CMMI 相關流程領域部份一般目標與 ISO27001 要求項目正向關係項目表.....53

圖目次

圖 1-1　研究流程 4
圖 2-1　2006 年資安調查各種攻擊型態，所造成的損失統計樣本數：313 份 7
圖 2-2　評估資安有效性的技術樣本數：496 份 7
圖 2-3　適用於 CNS27001 過程之 PDCA 模型 10
圖 2-4　資訊安全管理系統架構圖 12
圖 2-5　CMMI 階段表述流程領域之架構 14
圖 2-6　階層式與連續式階層式結構比較圖 18
圖 2-7　“The IDEAL SM model” 18
圖 3-1　研究架構圖 22
圖 5-1　資訊部門人員對 ISO27001 資訊安全管理系統要求項目認知程度統計 38
圖 5-2　CMMI 相關領域目標執行程度統計圖 39
圖 5-3　整體典型相關 48

辭彙說明

- 資訊安全(Information Security)-保護資訊的機密性、完整性與可用性；此外，此能涉及如鑑別性、可歸責性、求可否認性及可靠度等性質。（CNS27002：2007）
- 資訊安全管理系統(Information Security Management System ISMS)-整體管理系統的一部份，以營運風險導向(作法)為基礎，用以建立、實作、運作、監視、審查、維持及改進資訊安全。(CNS27001：2007)
- 機密性(Confidentiality)-使資訊不可用或不揭露給未經授權之個人個體過程的性質。（ISO/IEC 13335：2004）
- 完整性(Integrity)-保護資產的準確度(accuracy)和完全性(completeness)的性質。(ISO/IEC TR 18044：2004)
- 可用性(Avaliability)-經授權個體因應需求之可存取及可使用的性質。（ISO/IEC 13335-1：2004）
- 風險管理(Risk Management)-藉由協調各項活以指導與控管理組織之有關風險。(CNS14889)
- 風險評鑑(Risk Assessment)-風險分析與風險評估的整個過程。(CNS14889)
- 風險分析(Risk Analysis)-系統性的使用資訊，以識別綠由與估計風險。(CNS14889)
- 風險評估(Risk Evaluation)-把預估的風險和已知的風險準則進行比較的過程，以決定風險的顯著性。(CNS14889)
- 風險處理(Risk Treatment)-選擇與實作措施的過程以修正風險。(CNS14889)
- CMMI 模式組件-任何組成 CMMI 模式的主要結構元件，一些 CMMI 模式的主要元件包括特定執行方法、一般執行方法、特定目標、一般目標、流程領域、能力度及成熟度。(CMMI-DEV 1.2：2006)
- 能力成熟度模式-模式包含一個或多個專業領域的有效流程之基本元件。它也描述漸進的改善途徑，從隨興的不成熟的流程到具有改善品質及有效的有紀律的成熟流程。(CMMI-DEV 1.2：2006)
- 能力程度-個別流程領域內流程改善達到的程度，能力度由流程領域內適當的特定及一般執行方法所定義。(CMMI-DEV 1.2：2006)
- 連續式表述-一種能力成熟度模式架構，在每一特定的流程領域，能力度提供處理流程改善的建議順序。(CMMI-DEV 1.2)

第一章　緒論

第一節　研究背景與動機

資訊是一種資產，和其他重要的營運資產一樣，對組織營運是不可或缺的，此在日益互連的營運環境中特別重要。由於此互連性增長之結果，資訊也暴露在日益成長與多樣的威脅及脆弱中包括電腦輔助的詐欺行為、間諜行為、蓄意破壞、惡意毀損、火災或水災等，導致的損害也愈來愈嚴重。科技帶來了新型態的犯罪，入侵手法與工具更是日新月異、防不勝防，伴隨而起的將是網路上種種越權存取、入侵、電腦犯罪的新挑戰，屢見不鮮的網路攻擊事件，更突顯使用者及系統管理者安全防護觀念與措施的不足。

表 1-1　弱點記載統計表

年份	2001	2002	2003	2004	2005	2006	2007	2008(Q1-Q3)	total
數量	2437	4129	3784	3780	5990	8064	7236	6058	41478

資料來源：Carnegie Mellon University, SEI,(2009,april). Cataloged vulnerabilities. Retrieved April 5,2009,from the cert web site: http://www.cert.org/stats/cert_stats.html

觀察台灣電腦網路危機處理暨協調中心公布入侵事件求助統計表可發現非法網路攻擊事件，有升高的趨勢。行政院於 2004 年通過「建立我國通資訊基礎建設安全機制計畫」，其管理政策參酌國際標準組織(International organization for standardization，ISO)通過發行的 ISO27001 標準為基礎，經過翻譯及調整後，制定適用於我國之 CNS 27001 標準，來規範組織建構資訊安全管理系統之標準，包含安全政策、資訊安全組織、資產管理、人力資源安全、實體與環境安全、通訊與安全作業、存取控制、資訊系統獲取、開發與維護、資訊安全事故管理、營運持續管理及遵循等 11 大控制要項，主要任務是積推動資通訊安全基礎建設工作、建構資安應變中心及建立資安防護體系。對象是國內 3713 個重要政府機構(行政院國家資通安全會報，民 90)，將資通安全等級分為四級，評估公式為如下:

安全等級=遭受在因素破壞可能性*機關對通訊設備依賴度----(1)

表 1-2　行政院所屬機關安全等級分類

安全等級分類	影響層面	單位數(個)
A 級	影響公共安全、社會秩序、人民生命財產安全	126
B 級	系統停頓、業務無法運作	399
C 級	業務中斷、影響系統效率	999
D 級	業務短暫停頓，可立即修復	2189

資料來源:“非營利單位資訊災難備援機制建置之研究”,謝昆霖、呂易儒民95,資訊管理研究,6,82-100。

在行政院資通安全會報訂定行動方案執行要點與績效指標中，為落實資訊安全責任等級分級制度，依各資安等級應行事項完成一定時數教育訓練及通過專業鑑定,B 級機關應於 97 年底前通過第三者驗證(行政院國家資通安全會報，民 94)，以期在有限的資源下，能全面做好資通安全防護工作。

98 年參酌 2008 資通安全政策白皮書，研訂「國家資通安全發展方案(98 年至 101 年)」，包含「強化整體回應能力」、「提供可信賴的資訊服務」、「優質化企業競爭力」、「建構資安環境」四大政策目標，以『安全信賴的資訊化社會，安心優質的數位化生活』為願景。其中，為提升政府機關資訊服務的可信賴性，積極推動資安治理，訂定 B 級機關的資安治理比例：99 年達 30%；100 年 70%；101 年 100%，機關應自訂資安治理成熟度提升比例(行政院國家資通安全會報，民 98)。

第二節　研究目的

由於資訊通訊科技蓬勃發展，網際網路的訊速擴張，以及資訊社會對其依賴程度的深，導致生活型態與商業模式產生變革，資通安全風險隨之提高，諸如人為疏失操作不當、駭客攻擊與公務機密外洩等問題，悠關社會安定或國家安全，考量在有限的預算資源下，著手建置組織資訊安全管理流程，有效達成資訊安全管理目標。

對於組織資訊安全管理系統導入的探討，通常侷限於導入規範的各段落，缺乏全盤性的程序引導。許多組織面臨完成驗證全部程序的盲點；同時，基於組織資料之機密性，大部份的組織仍期望由內部同仁自行建置資訊安全管理系統，以確保組織擁有安全、可信賴的資訊通訊環境。

本論文為實務規劃研究，依據國際安全規範 ISO27001 對組織建置資訊安全管理系統的要求事項，以個案組織的情境和需求，循序建置資訊安全管理系統，達成 CNS27001 規範要求並完成驗證。在實作程序上，透過實務流程參考，建構組織計畫、執行、檢查及修正作業程序，持續不斷的調整安全性控制，提供實務建議供其它組織參考，共同連結安全管理的資通訊網路。

能力成熟度整合模式(Capability Maturity Model Integration ,以下簡稱 CMMI)，整合了資訊系統發展與維護活動等知識體系，且已列入中華民國國家

標準(Chinese National Standards,縮寫為 CNS)CNS15190。為促進公務機關資訊部門更有效率的流程改善，引用軟體科技創新管理模式，支援組織核心業務發展，進行 CNS27001 要求事項與 CMMI 需求管理、專案監控及支援等相關連續流程比對，分析資訊部門人員認知與實際執行的符合程度及其相關性，期能循序建置資訊安全管理系統及選擇適合的 CMMI 相關領域，提升公務部門資訊安全的能力度等級及建構組織發展創新的管理流程，以符合政府資通訊安全要求。

第三節　研究範圍

本論文依據 CNS27001 及 CNS27002 資訊技術、安全技術與資訊安全管理作業規範，進行實務導入，包含組織的安全政策、資訊安全的組織、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、資訊系統獲取、開發與維護、資訊安全事故管理、營運持續管理、遵循性等十一大項，經由適當的控制措施達成資訊安全，必須建立、實作、監視、審查與改進這些控制措施，以確保達成組織特定安全與營運目標，兼與其他營運管理過程一起達成。

本研究的個案單位是公務部門，屬 B 級單位部門組織，認證導入參酌資深顧問建議，依組織特性進行風險評鑑及處理，發展適合組織的指導綱要；相關 CMMI 流程領域能力度層級，則是以各流程領域中部份一般目標為分析範圍。研究標的組織，為目前可能參與 ISO27001 驗證或計畫申請驗證的業務屬性相關的 B 級公務機關，資訊部門人員為調查對象，專注於組織資訊安全流程改善及 CMMI 相關能力度部份一般目標執行程度。

第四節　研究流程

本論文透過個案實際操作，並依據國際安全規範 ISO27001 對組織建置資訊安全管理系統的建議，循序建置資訊安全管理系統，達成 CNS27001 規範要求並完成驗證，並以 CMMI 流程管理的連續表述的成熟度層級模式，進行內部自我檢測，分析組織資訊安全管理系統作業能力度，選擇可以同時進行的相關流程領域，作為組織資訊安全管理持續改進的參考，研究流程如圖 1-3 所示。

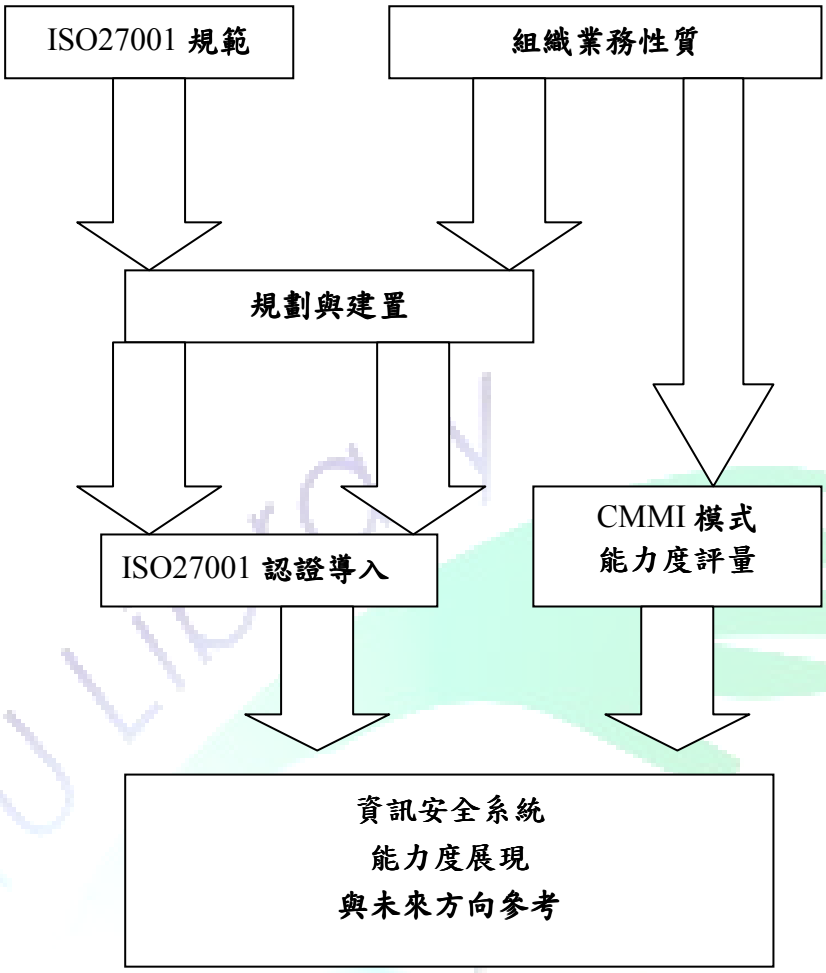

圖 1-1　研究流程

資料來源:本研究整理

第二章文獻探討

第一節　資訊安全議題的演進

一、　資訊安全的定義

自 90 年代從封閉走向開放，網際路的竄起，快速改變了組織的營運模式，電子化的經營模式隨之而起，而內外部所溝通的「資訊」逐漸成為重要的核心，因此從單純的「資訊」衍生「資訊安全」的議題，進而產生「資訊安全管理」的議題。資訊安全的全貌就是對於有關個人或組織在使用所有關於說的、印行的及自動化記錄等情事的保護；及保護資訊的產生、處理過程、傳遞、儲存使用、展示及控制執來源(Parker D.B.,1997)。確保資訊資產達以下的特性：機密性、完整性、可用性，藉由防範資訊資產遭受各種安全威脅，以達到企業持續經營、企業損失減至最小、投資報酬率及商機增至最大(ISO/IEC 17799　2000)（行政院國家資通安全會報，民 90)。

資訊安全是指用來防止非法存取、竄改、偷竊首對資訊系統造成傷害的一些政策、程序和方法。藉由一些技術和工具來保護硬體、軟體、通訊網路和資料，以提升資料的安全性。資訊安全管理系統(Information Management System ,ISMS) 的定義是，是用系統的方法對組織敏感資訊進行管理，涉及到人、程序和資訊技術系統 (BSI)。資訊安全管理之標的在於:「從確保資訊資源的合法存取，到所有可能遭受資訊攻擊之階段，提供完整、未中斷的資訊系統運行」(樊國楨，民 91)。

二、　資訊安全管理理論概述

由於資訊科技的快速進步，使得組織對資訊科技得依賴日深，資訊安全已不只是一種防禦性策略，更成為組織的競爭策略，也將關係到組織資訊安全策略之建構，在實務層面上觀察，資訊安全管理理論有：安全政策理論(Security Policy Theory. SPT)、風險管理理論 (Risk Management Theory. RMT)、控制與稽核理論 (Control and Audit Theory. CAT)、管理系統理論 (Management System Theory. MST)、權變理論 (Contingency Theory. CT) 等五種 (洪國興、徐鈺宗， 民 91)。

表 2-1　資訊安全管理理論彙總

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 ◆ 安全政維護	◆ 循序流程 ◆ 循環週期	◆ 以資訊安全政策為主要內涵，忽視風管理、內部控制與資訊稽核等安全機制 ◆ 重視循序與結化，對於環境的應變能力較低	Kabay(1996) 黃承聖(2000) Gupta 等(2001) Flynn(2001)
風險管理理論（Risk Management Theory. RMT）	◆ 風險評鑑 ✧ 風險分析 ✧ 風險評估 ◆ 風險處理 ✧ 建立控制制度 ✧ 實施控制制度 ◆ 檢討修正	◆ 循序流程 ◆ 循環週期	◆ 強調資訊安全環境的瞭解與應變，使控制可符合組織的需求 ◆ 忽視安全政策與資訊稽核等安全機制 ◆ 重視循序與結構化	Wright(1999) Reid & Floyd(2001) 樊國楨(2001b)
控制與稽核理論（Control and Audit Theory. CAT）	◆ 制定控制制度 ◆ 實施控制制度 ◆ 資訊稽核	◆ 循序流程 ◆ 循環週期	◆ 以內部控制及資訊稽核為主要內涵，忽視安全政策與風險評等安全機制 ◆ 重視內部控制之澈底執行，對於環境應變與需規劃較為不足	BS7799-2(1999) 林勤經(2001) ISO/IEC17799(2000) 楊金炎(2001) COBIT(1998)
管理系統理論（Management System Theory. MST）	◆ 制定安全政度 ◆ 定義風險範圍 ◆ 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較其他理論完整 ◆ 忽視資訊稽核 ◆ 欠缺循環週期與回饋功能	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，選擇適合的安全策略 ◆ 欠缺整合性與結構化	Robbins(1994) Drazm & Van &Ven(1985) Luthans(1976) Lee(1982) Von Solms(1994) 李東峰與林子銘(2001)

資料來源:“資訊安全評估準則層級結構之研究”，洪興國、季延平、趙榮耀,民92圖書館學與資訊科學,29(2),22-44。

第二節　資訊安全發展趨勢

一、　根據美國電腦犯罪與安全調查(CSI/FBI)2006 年資安調查各種攻擊型態，所造成的損失統計

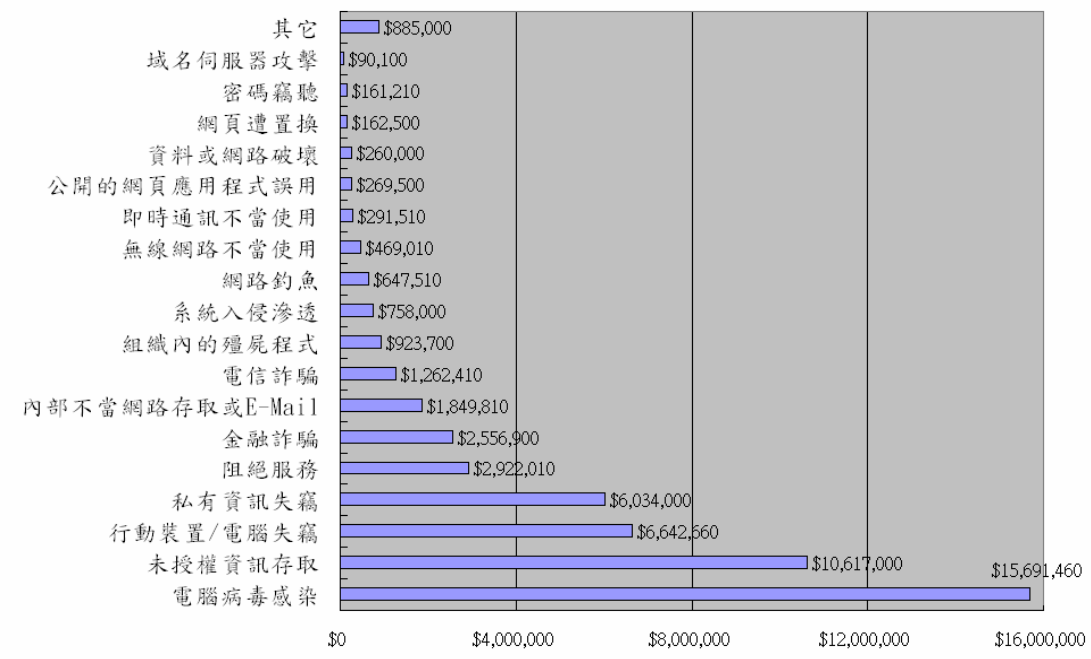

圖 2-1　2006 年資安調查各種攻擊型態，所造成的損失統計樣本數：313 份

資料來源: COMPUTER SECURITY INSTITUTE.(2006, September 28). CSI　2008 Security Survey. Retrieved November 12, 2008, from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf

二、　為減少資安事件造成組織損失，應採取有效內部控制程序及安全管理措失，評估資安有效性的技術，其中以內部稽核最為有效，達 64%。

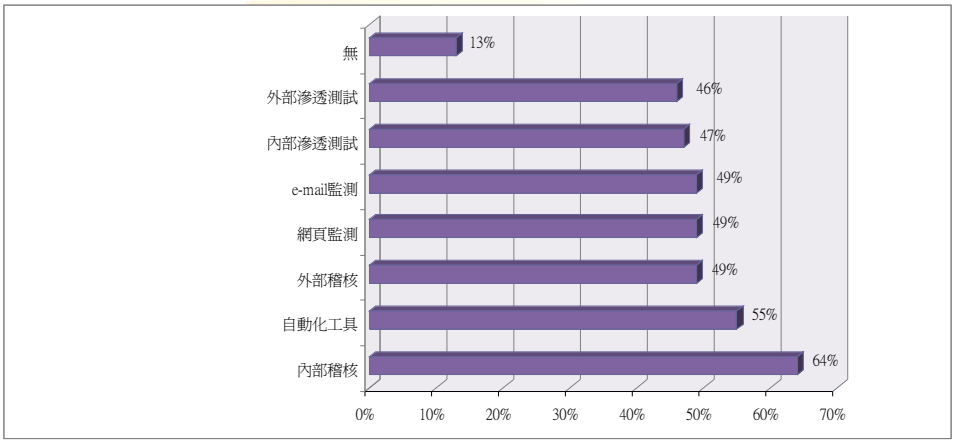

圖 2-2　評估資安有效性的技術樣本數：496 份

資料來源：COMPUTER SECURITY INSTITUTE.(2008). CSI 2008 Security Survey. Retrieved March 3, 2009, from http://www.gocsi.com/forms/csi_survey.jhtml

三、 SANS 網站專家預測，列出 20 資安風險重要趨勢:

1、 使用者端弱點(Client-side Vulnerabilities)

(1)網頁流覽器

(2)辦公室軟體

(3)電子信箱

(4)媒體播放器

2、 伺服器端弱點(Server-side Vulnerabilities)

(1)網頁應用

(2)微軟公司服務

(3)unix 和 mac 作業系統

(4)備援軟體

(5)防毒軟體

(6)伺服器管理

(7)資料庫軟體

3、 安全政策與員工(Security Policy and Personnel)

(1)過度的使用者權限和未經授權的設計

(2)網路釣魚

(3)未加密的膝上型電腦和可移動的媒體

4、 應用系統的濫用（Application Abuse）

(1)即時通訊

(2)點對點程式

5、 網路應用產品(Network Devices)

(1)網路電話(VoIP)與手機

6、 零時差攻擊

資料來源: The SANS (SysAdmin, Audit, Network, Security) Institute.(2007, November 28). ***Top-20 2007 Security Risks*** **.** Retrieved April 3, 2009, from http://www.sans.org/top20/

目前國內外系統開發，均已朝向開放系統之方向進行，資訊安全已成為社會能否進一步發展的關鍵。

第三節 國家資訊安全管理標準

一、 CNS27001 資訊安全管理系統-要求事項

由 BSI(The British Standards Institution（英國標準協會）邀集業界相關領導廠商為共同追求國際品質的資訊安全管理系統所共同開發而成，可適用於各種產業與組織，是的個包含了各面向的組織資訊安管理標準，原僅為英國國家標準(British Standards)，現已被多個國家採用成為國家標準，如瑞

典、挪威、澳洲、巴西、捷克、芬蘭、冰島、愛爾蘭、荷蘭及台灣等。

國際標準組織(International Organization for Standardization, ISO)為提供一套能供全球依循的資訊安全控管標準，乃將 BSI 所制定的 BS7799「資訊安全管理實務準則」的第一部分（朱慧德，民 91）納入世界標準，編號為:ISO/IEC 17799:2005 (Information Technology-Code of practice for information security management)資訊安全管理作業要點，包括領先企業提出的相關指導和建議。根據美國標準和技術國家機構(The Nation Institute of Standards and Technology‘s , NIST)對 ISO 17799 的詮釋:「ISO/IEC 17799 是個實施要則(code of practice)，也是因為如此，其提供了資訊安全管理的指導綱要(guidelines)和內發性指引(voluntary direction)。其提供了高質、通用的敘述以針對目前在工作領域被認為其有重要性的各項前引(initiating)、導入(implementing)其在企業組織內的資訊安全管理。2005 年，從整體架構調整、條款呈現方式、調整控管措施結構安排、調整控制目標與控制措施之分類與從屬關係、考慮適用範圍、以因應新的 IT 技術增加新控制措施及網路的趨勢修改控制措施用語等方向進行改版。

台灣資訊安全管理系統驗證標準 CNS27001，已於民國 95 年 6 月 16 日公告。提供用以建立、實作、運作、監視、審查、維持及改進資訊安全管理系統(Information Security Management System, ISMS)之模型，其設計與實作受其需求與目標、安全要求、所採用的過程，以及組織之規模與架構所影響，這些項目及其支援系統會隨時間而改變。所展現之資訊安全管理的過程導向，乃強調下列事項之重要性：

- ✧ 瞭解組織資訊安全要求，以及建立資訊安全之政策與目標需求。
- ✧ 在組織整體營運風險之全景（context）中，實作及運作各項控制措施以管理組織的資訊安全風險。
- ✧ 監視與審查 ISMS 之績效與有效性。
- ✧ 基於客觀的測量以持續改進。

CNS27001 採用“規劃－執行－檢查－行動(Plan-Do-Check-Act, PDCA)”過程模型，納採資訊安全要求與利害相關者之期望為輸入，經由各必要行動與過程(ISMS)，(如表 2-3)產生符合此等要求與期望的資訊安全輸出結果。

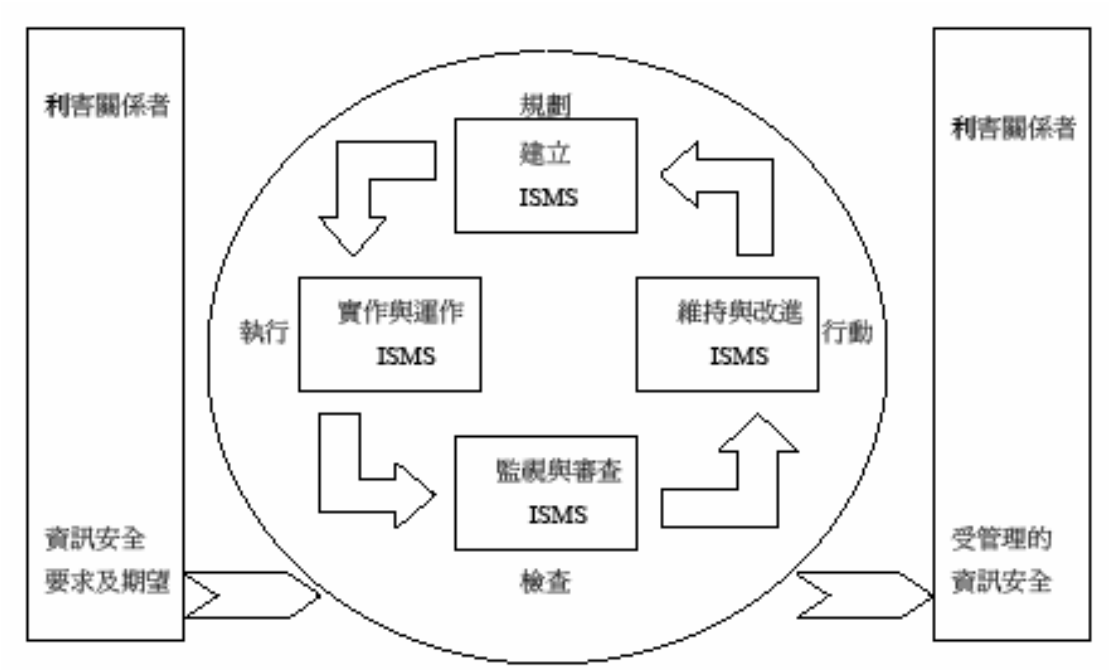

圖 2-3　適用於 CNS27001 過程之 PDCA 模型
資料來源:“中華民國國家標準”,CNS 27001,民96。

表 2-2　PDCA 資訊安全管理程序與要求

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策和目標一致之結果。
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(維持與改進 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 ISMS 的持續改進。

資料來源:“中華民國國家標準”,CNS 27001,民96。

二、 CNS27002 資訊安全管理系統-作業規範

提供了關於的資訊安全管理建立、實施和維護的要求。為資訊安全管理系統評估基準(驗證標準)，使資訊安全管理體系更容易和其他管理體系相協調。CNS27002 的十個章節概述如下：

✧ 資訊安全政策（Information Security Policy）:
定義高階管理對資訊安全之期許與要求，益將其文件化，以利企業內資訊安全之推行。

✧ 安全的組織（Security Organization）:
幫助成立資訊安全部門，並定義其組織架構、運作流程與責任歸屬。

- ✧ 資訊資產分類與控制（Asset Classification and Management）：
  依照資訊資產之運無流程與資產價值，將資訊資產作分類，並規劃各不同分類等級資產之保護措施。
- ✧ 人員資源安全（Personal Security）：
  為降低人為疏失發生機率，並減少人為之惡意侵害行為，將針對員工訓練、員工之資訊安全工作範圍與責任及重大事件呈報步驟，作相關規劃。
- ✧ 實體與環境安全（Physical and Environmental Security）：
  規範有形資產之保護措施、安全裝備與一般控管原則。
- ✧ 通訊與操作管理（Communications and Operations）：
  針對資訊運作設施所規劃之控措施，以確保資訊運作過程之正確與安全。
- ✧ 存取控制（Access Control）：
  使用者權限之設定應依設定使用者工作職權而給予，以降低未經授權存取系統資源之風險。
- ✧ 系統獲取發展與維護（System Development and Maintenance）：
  規劃企業內系統開發與維護過程，將資訊安全列入流程範圍。
- ✧ 資訊安全事故管理(Security Event Management) ：
  建立管理責任與程序，以確保對資訊安全事故做迅速、有效及依序的回應。
- ✧ 持續營運管理（Business Continuity Management）：
  規劃企業面臨重大意外事故時所需之應變措施與回復機制。
- ✧ 遵循性（Compliance）：
  避免企業之資訊管理系統違反相關法令，針對現有法律環境作適當之控管程序複核與改善。

圖 2-4　資訊安全管理系統架構圖

資料來源: “標準化應用於中小企業導入資訊安全管理系統之成功經驗”, 歐弘詹,民95,台北市:中華民國國家資訊基本建設產業發展協進會。

第四節 能力成熟度整合模式(CMMI)

一、能力成熟度模式

1986 年 SEI 在美國防部之資助下發展能力成熟度模式(CMM)，最初是希望發展出一個評估軟體承包商開發能力之模式，以提高軍方委外之軟體品質。另一方面，幫助軟體組織改善其體質，並解決需求日趨複雜，維護難度的急速升高之軟體危機。它規定了組織性成熟的階層式架構，以及如何判斷軟體開發所處的成熟度。CMM 是對企業管理的一種評估，經由評估管理過程中的強項與弱項，指出存在的問題，並進行指導，幫助組織改進。1997 年美國國防部，致力開發 CMMI(Capability Maturity Model Integration), SEI 宣佈 CMMI 取代 CMM，於 2000 年頒布 CMMI-SE/SW 1.0 版本。CMMI 主要在整合各種不同的成熟度模式，整體性地考量組織之作業流程，以提升產品或相關服務之開發、獲得及維護等作業能力。

CMMI 模式中的流程領域分為階段表述方式與連續表述方式二種。

(一)、 階段表述方式:利用被分組和設定好先後順序的流程領域為基礎，提供了如何提升與組織相關活動的準則(Ahern, Clouse and Turner，2003)，能提供一個以循序實作為主的實施方式。

(二)、 連續表述方式：允許選擇最符合組織經營目標的流程領域，為優

先改善順序，以降低組織經營風險（朱慧德，民國 91 年），適合單一流程領域，主要為可提供最大的彈性，以專注於特定的流程重點（CNNI Product Team ，2006）. 階段表述方式與連續表述方式的優缺點比較如表 2-2 所示

表 2-3　階段表述方式與連續表述方式的優缺點比較表

階段表述方式	連續表述方式
使組織有一個已定義且被證實的改善路徑	授予明確的自由度來選擇最符合組織經營目標與減少組風險範圍的改善順序
專注在一組織流程領域，此組流程領域為每一成熟度等級的特徵，是供組織特定的能力	增加每一個流程領域能力度透視度
以簡單的型式彙總流程改善結果-單一成熟度等級數目	允許對不同流程執行不同等級的改善
建立在一個相對長期的使用歷史，包含個案研究與數據以證明投資報酬率	一種新方法仍未有數據登其投資報酬率有關連

資料來源：Carnegie Mellon University, Software Engineering Institute. (2007,November).Capability Maturity Model Integration(CMMI-DEV 1.2 版,10). Retrieved March 2, 2009, from http://www.sei.cmu.edu/publications/documents/06.reports/06tr008.html

二、能力成熟度整合模式之架構

CMMI 的每個成熟度等級中各有多個個流程領域(Process Areas)，而在每個流程領域內都設定了一組目標（Goals），並延伸出主要的執行方法；此外，每個流程領內都有一組共同特徵，包括執行承諾、執行能力、督導履行、驗證。其架構如圖 2-5

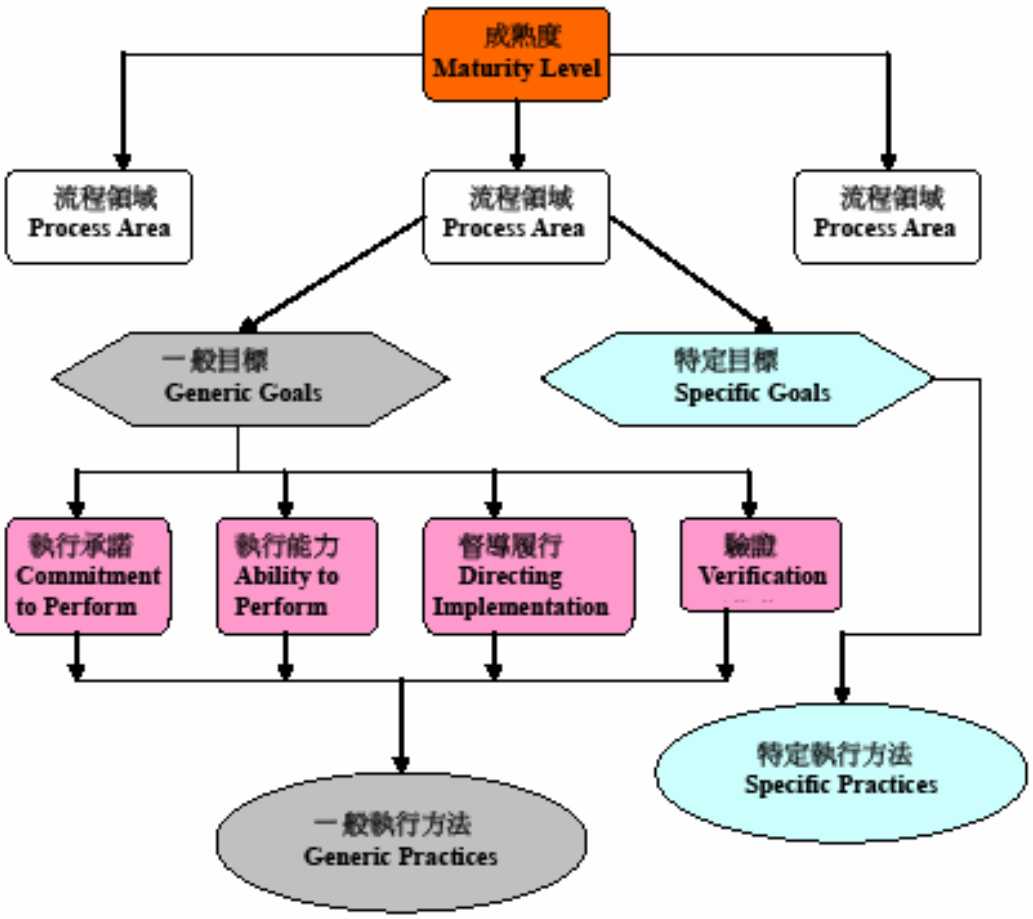

圖 2-5　CMMI 階段表述流程領域之架構

資料來源：Carnegie Mellon University, Software Engineering Institute. (2007,November).Capability Maturity Model Integration(CMMI-DEV 1.2 版,30). Retrieved March 2, 2009, from http://www.sei.cmu.edu/publications/documents/06.reports/06tr008.html

（一）　流程領域(Process Areas)

第二層到第五層，每一個成熟度都由數個流程領域所組成。所謂流程領域是指從某一層進入下一層所需改進的關鍵行動，並包括數個改善目標，提供了明確的改進方向。在整個成熟度模式中，共有 25 個流程領域。

（二）　一般目標（Generic Goals）

一般目標可適用於所有的流程領域。各流程領域中，一般目標之達成與否，代表各流程領域的執行與制度化，是否為有效，可重複與持久的。

（三）　一般執行方法（Generic Practice）

適用於任何流程領域，它們可以改善流程領域的績效與控制。一般執行方法，提供制度化的特性，確保流程領域為有效、可重覆與持久的，屬期望的模式組件。

（四） 特定目標(Specific Goals)

僅適用於單一的流程領域，並強調此唯一的特徵說明哪些是必須要執行以符合該流程領域。目標是必要的模式組件。

（五） 特定執行方法(Specific Practices)

特定執行方法是對應於特定目標的活動，可達成特定目標是重要的。特定執行方法說明一組活動，這組活動被期望可以幸成流程領域的特定目標。

（六） 共同特徵（Common features）

共通特徵提供一種方式，來表現一般執行方，以顯示流程建置與制度化是否有效、可重覆及可長久執行，這四個共同特徵如表 2-3 所示。

表 2-4 CMMI 共同特徵描述

共同特徵	描述與相關技巧
執行承諾 Commitment to Perform	管理政策的建立
執行能力 Ability to Perform	確保組織或專案有充分資源的一般行方法，以尋求流程改善
督導履行 Directing Implementation	蒐集、度量和資料分析有關的一般執行方法，其目的在於觀察流程的績效
驗證 Verification	證專或組織活動有關的一般執行方法，以驗證其是否符合要求

資料來源：“能力成熟度整合模式之導入-以文件管理系統為例”，姚俊羽，93

（七） 流程領域分類

1、 階段表述方式的流程領域分類

表 2-5　階段式流程領域分類與成熟度層級對照表

階層	重點	流程領域個數	流程領域
5 最佳調適級	持續流程改善	2	➢ 因果的分析和解決 ➢ 組織的創造和發展
4 量化管理級	量化管理	2	➢ 量化流程管理 ➢ 組織流程發展
3 調適級	流程標準化	14	➢ 需求發展 ➢ 技術支援 ➢ 產品整合 ➢ 驗證 ➢ 批准 ➢ 組織流程專注 ➢ 組織流程定義 ➢ 訓練課程 ➢ 整合專案管理 ➢ 風險管理 ➢ 決策分析及解決 ➢ 整合組織環境 ➢ 整合團隊合作 ➢ 整合供應商管理
2 管理級	基礎的專案管理	7	➢ 需求管理 ➢ 專案規劃 ➢ 專案監控 ➢ 供應商協議管理 ➢ 度量和分析 ➢ 流程和產品品質管理 ➢ 建構管理
1 初始級	無	無	➢ 無

資料來源：Carnegie Mellon University, Software Engineering Institute. (2007,November).Capability Maturity Model Integration(CMMI-DEV 1.2 版,36-48). Retrieved March 2, 2009, from http://www.sei.cmu.edu/publications/documents/06.reports/06tr008.html

2、　連續表述方式的成熟度層級

表 2-6　連續式流程領域分類與成熟度層級比較表

流程領域分類	流程領域	成熟度	流程領域個數
流程管理	1 組織流程專注	3	5
	2 組織流程定義	3	
	3 訓練課程	3	
	4 組織流績績效	4	
	5 組織的創新與發展	5	
專案管理	6 專案規劃	2	8
	7 專案監控	2	
	8 供應商協議管理	2	
	9 整合專案管理	3	
	10 整合團隊合作	3	
	11 整合供應商管理	3	
	12 風險管理	3	
	13 量化專案管理	4	
工程	14 需求管理	2	6
	15 需求發展	3	
	16 技術支援	3	
	17 產品整合	3	
	18 驗證	3	
	19 批准	3	
支援	20 度量和分析	2	6
	21 流程和產品品質管理	2	
	22 建構管理	2	
	23 決策分析及解決	3	
	24 整合組織環境	3	
	25 因果的分析和解決	5	

資料來源：Carnegie Mellon University, Software Engineering Institute. (2007,November).Capability Maturity Model Integration(CMMI-DEV 1.2 版,53-66). Retrieved March 2, 2009, from http://www.sei.cmu.edu/publications/documents/06.reports/06tr008.html

3　CMMI 階層式與連續式階層式結構比較

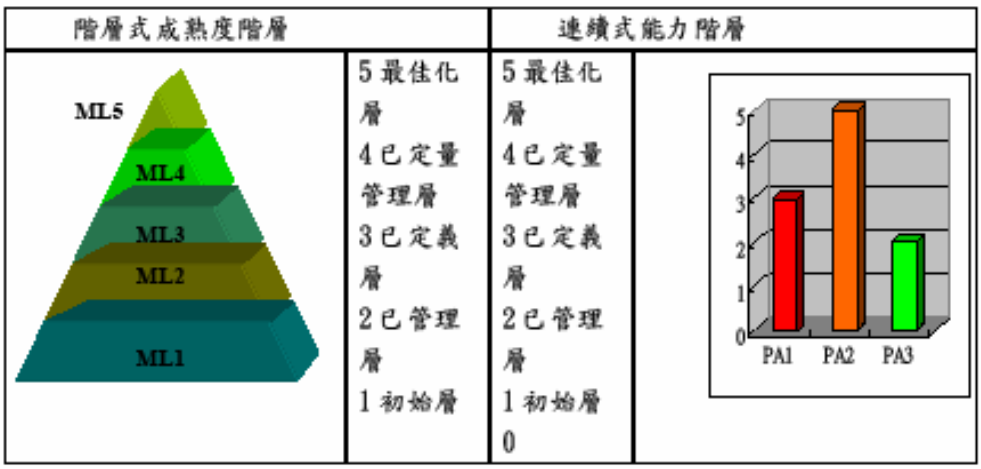

圖 2-6　階層式與連續式階層式結構比較圖

資料來源：“由ISO 9000至整合能力成熟度過程之模型之研究-以某校技術合作處為例”，翁玉麟, 民91。

（八）　流程改善程序

IDEAL 模式提供一個實用易於了解的五個步驟，說明如何建立一個成功的流程改善計畫，用於啟動、規劃和實現過程改善措施藍圖的模型。由五個時期所組成，如圖 2-7 所示。

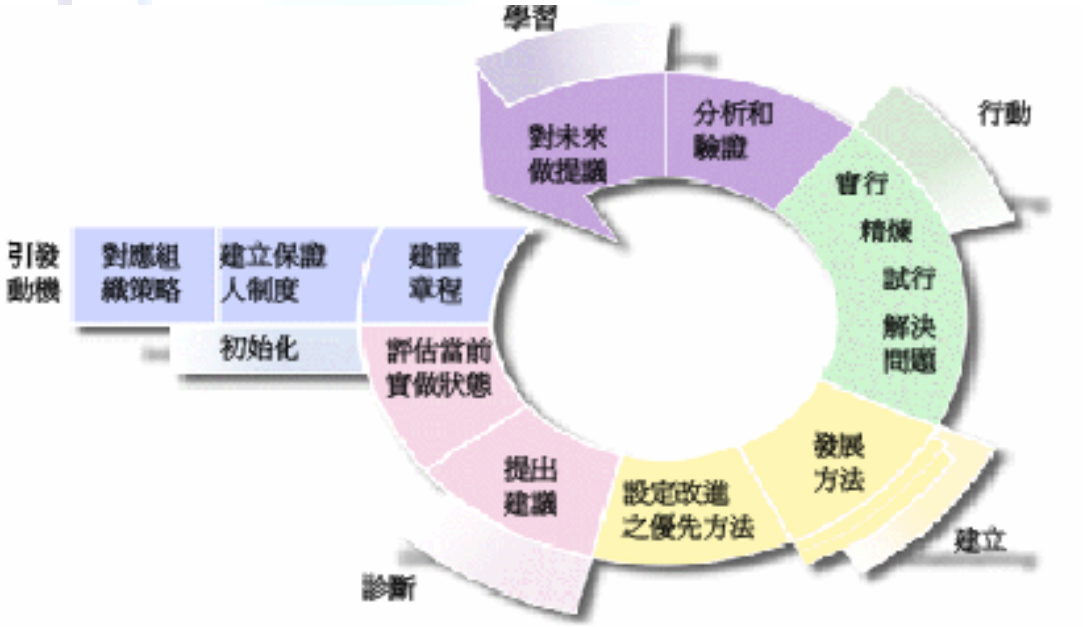

圖 2-7　“The IDEAL SM model”

資料來源：“能力成熟度整合模式之導入-以文件管理系統為例”，姚俊羽, 民 93 & Carnegie Mellon University, Software Engineering Institute.The IDEAL^{SM} model. Retrieved March 2, 2009, from http://www.sei.cmu.edu/ideal

（九） 評鑑

1、 SEI 的 ARC 與 SCAMP

SEI 自 1991 年推出 SW-CMM 之後，普遍受到各界的重視，而陸續提適用於各種不同領域的能力成熟度模，由於不同領域之能力成熟度模式所採用的表述方（Representation）、術語（Terminology）與評估方式（Assessment Approach）不一致，衍生了許多的問題，因此 SEI 為此發展 CMMI，一個共通性之整合構，以支援不同專業領域之特定能力成熟度模式，CMMI 改進了同時使用多不同領域之能力成熟度模式所造成的缺點，提供一致性的術語與評鑑方式來協助組織進行全面性流程的改善。

關於 CMMI 的評鑑方法，SEI 訂定了發展出能力成熟度整合模式評鑑需（The Appraisal Requirements for CMMI, 以下簡稱 ARC）標準，用以規範評鑑的準則。ARC 標準將 CMMI 評鑑分為 A、B 與 C 三個等級，並將這三級的需求規範詳細地地定義出來，CMMI 之各個評鑑等級特性比較表，如表 2-6所示。

表 2-7 CMMI 之各個評鑑等級特性比較表

特性	等級A	等級 B	等級 C
客觀証據收集量（相對高低）	高	中	低
能力等級的獲得	有	無	無
資源需求量（相對高低）	高	中	低
團隊大小（相對大小）	大	中	小
評鑑團隊領導者的要求	主任稽核員	主任稽核員或有經驗且受過訓練的人員	有經驗且受過訓練的人員

資料來源：“能力成熟度整合模式之導入-以文件管理系統為例”，姚俊羽，民 93

對評鑑結果的信心度，以等級 A 最高；評鑑的成本與時間長短，也以等級成本最高，所需時間也最長；基於評鑑等級 A 的規範，SEI 提出了流程改善標CMMI 評鑑方法（Standard CMMI Appraisal Method for Process Improvement, 下簡稱 SCAMPI），SCAMPI 評鑑方法將評鑑程序分為三個階段：規劃與準備段（Plan and Prepare for Appraisal）、執行評鑑階段（Conduct Appraisal）與報告結果階段（Report Results）。

2、 流程改善程序

流程改善的四個程序，各程序的主要工作及交付項目如表 2-7 所示。

表 2-7　流程改善程序的主要工作及交付項目表

程序	主要工作	交付項目
1 落差分析	建立組織流程改善基礎建設	落差分析報告
2 定出檢查點與決定流程改善時機	建立流程改善原則和基礎	CMMI 標準流程草案
3 建立流程改善計畫	指出流程改善中的活動	工具的教育訓練 組織流程改善計畫
4 實作流程改善	專案的試行與預評	預評報告

資料來源:洪肇奎(民 93 年 4 月)。如何成為一個具備流程改善基礎的組織。吳裕光(主持人)，台灣軟體流程改善聯盟：SPIN-Taiwan 研討會，中國文化大學。

第三章　研究設計

第一節　研究架構

本研究以行政院所屬機關安全等級為 B 級單位之公務機關，進行 ISO27001 實務導入，探討行政組織導入時，所面臨的實務困難及提出解決經驗，以提供公務組織導入的參酌。

綜合第二章文獻探討所述，根據個案以 ISO27001 驗證機制及 CMMI 之流程管理、專案管理及支援之連續式能力度流程領域相關一般目標，執行程度調查與分析，藉此了解組織之資訊安全能力，並據以提出 ISO27001 資訊安全管理系統與 CMMI 能力成熟度整合模式可能共舞的未來改進方向。此架構如圖 3-1 所示。

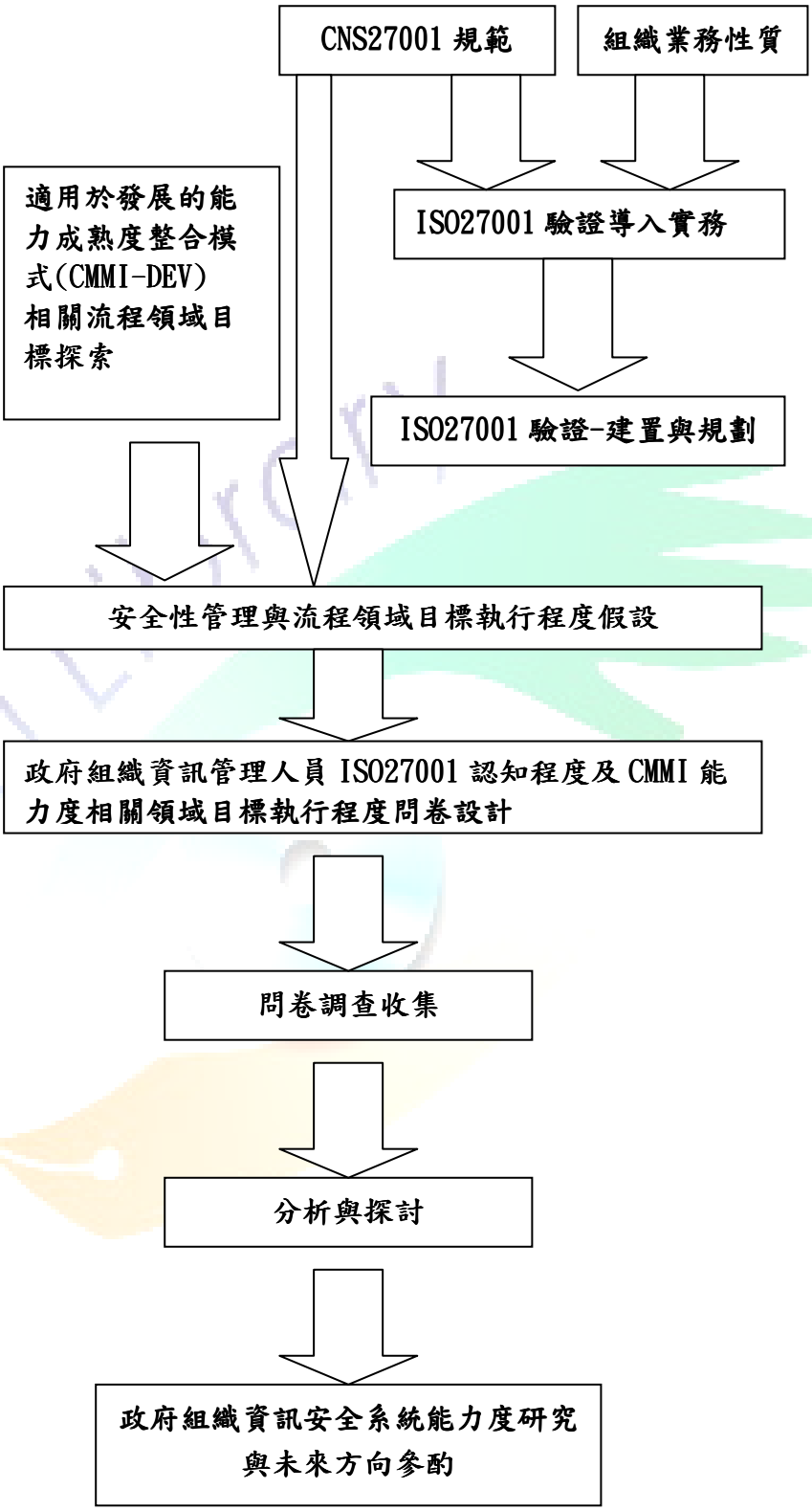

圖 3-1　研究架構圖

資料來源：本研究整理

第二節　研究方法

一、研究樣本

目前行政院所屬機關已有許多單位通過 ISO27001 的驗證,但業務性質不盡相同，導入實務也不同，本研究從公務行政部門探討導入經驗，期提供受預算限制而擬以較低成本自行導入的機關，分享實務經驗，提升整體行政體系的資訊安全管理系統，達成保護民眾個人財產資料，符合政府的資通訊安全要求。

台灣地區對 CMMI 的研究(鍾依萍、周樹林，民 93)多以民間企業軟體專案有關，公務機關對 CMMI 應用稀少；因 CMMI 評鑑要求已於民國 97 年 5 月列入中華民國國家標準，有利公務部門的適用導入。本研究從政府的資通訊安全性要求，考量作業環境等因素，從 ISO27001 導入著手，建立組織安全資訊系統框架及相關流程管理規範。然後，探討 CMMI 中連續式表述模式相關的流程管理類別與領域目標，調查 CMMI 相關各流程領域目標的執行程度，確認未涉及組織的業務機密後，定義欲評量的構面，以可能參與 ISO27001 認證的相關 B 級公務機關，進行問卷調查與歸納分析，對象是可能參與 ISO27001 認證組織的資訊系統單位管理人員，從實務面觀點出發，了解組織的資訊安全能力度，提出未來資訊安全管理創新發展的建議。

二、資料分析方法

本研究使用 SPSS for windows 13.0 與 statistica 7.0 統計套裝軟體作為分析工具，所採用的統計方法如下所示：

(一)、信度分析(Reliability analysis)

本研究採用 Cronbach s α 信賴係數法，檢驗 CNS27001 相關節次與 CMMI 相關領域測量問卷的信度。

(二)、敘述性統計分析（Descriptive Statistics analysis）

針對蒐集樣本的背景資料進行敘述性統計分析，包含職稱、組織參與 ISO27001 驗證情形與了解 ISO27001 情形、知悉 CMMI 情形，其所佔百分比及平均值的分佈情形。

(三)、單因子變異數分析(One-way ANOVA)

用以比較不同組織對 ISO27001 資訊安全管理系統的認知，與 CMMI 相關領域執行程度是否有差異。

(四)、相關分析

採用相關分析方式,利用 SPSS 軟體分析,CNS27001 相關節次與 CMMI 相關部份領域具有顯著相關的項目，進行相關分析，了解 CNS27001 相關節次認知程度與 CMMI 相關部份領域相關係數之比例。

(五)、典型相關分析

以 statistica 進行典型相關分析(canonical analysis)，透過典型變數的相關係數，綜合地描述兩組變數的線性關係。

三、問卷發放與抽樣

為衡量資訊安全管理系統有關的重要性認知與實際施行的程度關係，本問卷以各個公務部門資訊單位且以實際負責資訊安全管理等工作之相關人員為對象，選擇業務屬性相同的 B 級機關人員，包括台灣省之北部、中部、南部及東部，共 6 個組織以 e-mail 或紙本寄送方式發放。

四、研究步驟

本研究將回收問卷進行編碼與儲存建檔，以套裝軟體 SPSS13.0 及 STATISTICA 7.0 進行資料分析與假設驗證，研究步驟如下：

(一)、對問卷基本資料進行敘述統計分析，以了解各項資料之分配情況。

(二)、分析各組織資訊人員對 ISO27001 的認知重要程度與知悉 CMMI 情形，以探討它們之間的是否有關聯。

(三)、以單因子變異數分析，來比對 ISO27001 的認知重要程度與 CMMI 各個流程領域執行的實施程度的顯著情況。

(四)、進行相關分析與典型相關分析，探討 ISO 與 CMMI 兩組變項結構間的相關程度。

(五)、就各資訊安全管理系統及實際符合 CMMI 能力度等級分析，鑑別未來公務部門資訊安全管理適切的發展方向。

第四章　個案分析

第一節　個案說明

個案組織為公務行政機關，配合中央部會資訊作業平台計畫，辦理舊式伺服器主機汰換，持續擴充便民服務範圍及申辦服務項目，建構「以網路代替馬路」以加速電子化「e」政府的實現。配合「建立我國通資訊基礎建設安全機制計畫」於民國 97 年導入 ISO27001 作業規範，以資訊業務單位主導，建立符合政府資通訊安全的作業環境，保護民眾之財產資料機密；透過第三方驗證方式，展現公務組織對資訊安全管理的重視與努力，提升民眾的信賴程度。

第二節　ISO27001 導入流程規劃

規劃導入流程階段共分為前置規劃、現況分析、流程制定、流程執行、評估與改善及評鑑等六個階段。導入流程與 IDEAL 模式階段相對應如表 4-1 所示。

表 4-1　ISO27001 導入流程與 IDEAL 模式階段相對應表

SEI IDEAL 模式階段	ISO27001 導入流程階段	ISO27001 導入流程作業
初始階段 (Intinating)	前置規劃	1.1 設定工作內容 1.2 獲得高層支持 1.3 導入團隊建立 1.4 經費來源確定
診斷階段 (Diagnosing)	現況分析	2.1 瞭解組織內部流程 2.2 分析實際現況差異 2.3 制定改善建議
建立階段 (Establishing)	流程制定	3.1 研究適合方法 3.2 訂定組織規範與程序 3.3 規劃行動方案 3.4 建立基礎架構 3.5 教育訓練
行動階段 (Acting)	流程執行	4.1 實作風險控管 4.2 文件記錄 4.3 監視與審查 4.4 維持與改進
學習階段 (Learning)	評估與改善	5.1 檢討與分析導入實務 5.2 評估目標 5.3 持續性流程改善
	評鑑與報告	6.1 預先評鑑 6.2 缺失補強 6.3 正式評鑑

資料來源：本研究整理

一、　初始階段

由資訊部門的高階主管與具 ISMS 稽核員證照之高階主管研商，以符合「建立我國通資訊基礎建設安全機制計畫」要求之 ISO27001 認證，為本專案之工作容進行規劃。在獲得高層支持後，以有限的年度預算結餘，聘請資深顧問輔導。動員資訊單位，組織專案團隊協助改革。

二、　診斷階段

引導資深顧問研究組織流程實際狀況，分析組織流程與 ISO27001 資訊安全管理系統要求事項的差異程度，透過顧問對組織內部相關人員會談、收集與資料分析後，歸納各部門的作業流程，依據組織流程的核心價值，提出適合組織現況的改善建議。

三、　建立階段

專案團隊依據現況差異分析與流程改善建議，考慮組織本身業務目標、資源、成本、時程與風險，修訂組織管理規範與程序，規劃行動方案，決定導入流程的順序。執行計畫包含工作時程、里程碑、責任分配與風險度量與組織所需要的任何項目。在高階主管的承諾與支持下，建立符合 ISO27001 資訊安全管理系統要求事項的各項組織架構。

導入初期，組織人員因業務量突然大量增加，且對 ISO27002 的條文感覺陌生，易產生排斥感。解決方式採用柔性溝通方式，甚至以一對一溝通方式，詳細說明作業事項，以減少質恐懼或排斥感。人員的教育訓練，以 ISO27001 及 ISO27002 條文解析為一般指引，組織內資訊安全小組成員實施稽核訓練與持續營運狀況模擬推演等。

四、　行動階段

依組織業務功能，區分資訊資產類別；以資訊資類別，設定風險控制程序。根據風險控制程序，實施風險控制步驟；依據各項控制步驟，落實文件記錄。實體環境安全區隔，網路設備安全稽核，人力資源安全管理，程式組態上線安全管制，使用者安全存取控，資訊安全事故管理，營運持續測試維護，遵循適法性要求，持續審查、修正與改進。

五、　學習階段

收集前置規劃相關資料，例如時程、成本、人力與資源，分析是否符合組織要求，檢討執行缺失，評估導入 ISO27001 後，是否達到組織要求的目標，藉由持續性改善，讓組織流程越來越健全。辦理預先評鑑，評鑑缺失改善後，申請正式評鑑。

第三節　遭遇阻礙與解決之道

一、　資訊資產管理

資訊資產依其功能系統分門別類，屬較有效率切割方式，可免除單一設備建置資訊資產清冊的繁雜與費時。參酌教育部提昇校園資訊安全服務計畫，建議資訊資產清冊建置如下：

（一）、資訊資產（各系統）分類

1、資料資產：原始資料與經歸納及整理之文件、檔案。如資料庫、作業紀錄、資料檔案及原始程式碼等。

2、文件資產：對業務或作業有指導性質之文件。如合約、資訊安全政策、作業程序、作業細則、系統文件、使用者手冊等。

3、軟體資產：自行開發、委外開發及軟體供應商提供之資訊系統，包括作業系統、套裝軟體、工具軟體、網管軟體、應用軟體及其他相關軟體程式。

4、硬體資產：資訊硬體及實體環境與設備，包括各類不同規格及功能之電腦設備及個人用電腦、電腦周邊、終端機、工作站、區域與廣域網路。

5、服務資產：電腦維護服務、通信服務、顧問服務及一般公用設施服務，如電力供應、清潔服務及保全服務等。

6、人員資產：參與本組織各項資訊處理作業及資訊系統運作之相關同仁與服務廠商人員。

（二）資訊資產分級

文件類與資料類資訊資產分為公開使用、內部使用及限定使用三級，其定義如下：

1、公開使用：可對外公告之相關文件資料。

2、內部使用：本組織內部使用之資產、文件、表單及紀錄等，並在該資產明顯處標示『內部使用』之字樣或藍色標籤。

3、機密：本組織限定使用之資產、文件、表單及紀錄等，並在該資產明顯處標示『機密』之字樣或紅色標籤。

二、風險評鑑及風險管理

（一）營運衝擊分析

評量時不考慮既有控制項目，以最壞的狀況就機密性、完整性及可用性喪失時所造成有形及無形的影響與財物損失，進而評估對組織營運之衝擊性。

表 4-2　衝擊等級評估表

衝擊等級	營運影響
4	損害極巨
3	損害嚴重
2	損害顯著
1	衝擊較小
0	微不足道

資料來源：本研究整理

（二）營運衝擊分析評量指引

1、機密性：評量時以該系統或作業資產清冊中，資料類及文件類資產其機密等級為「限定使用」之資產洩漏角度來觀察。

2、完整性：評量時以該系統或作業資產清冊中資產類及文件類資產若不正確或作業執行錯誤所造成的影響來觀察。

3、可用性：可用性營運衝擊評估，先由負責評估人員就「營運衝擊分析評估項目準則」中可用性衝擊評估項目分別考量，並依最大衝擊評估項目，填寫可忍受中斷時間並說明理由及考慮因素，經風險評估小組收集整體之評估資料，決定評估標的中斷時間級距後，再由負責評估人員就可忍受之中斷時間級距分別給予 4~0 之「可用性衝擊等級。

（三）　營運衝擊等級對照表

表 4-3　營運衝擊等級對照表

衝擊等級	價值數值
4	100
3	75
2	50
1	25
0	不列入計算

資料來源：本研究整理

(四)決定接受風險水準

對各類評估標的之風險值由高到低進行排序，將風險值由最高風險值逐一往下累計，當累計風險值之和達該類評估標的整體風險前 25%時之風險值為風險等級 3 之參考風險值，當累計風險值之和達該類評估標的整體風險前 50%時之風險值為風險等級 2 之參考風險值。

對上述之風險等級 3 之參考風險值，進行評估並參考以往風險評鑑之經驗提出修正建議，作成「風險接受水準」。

(五)威脅與弱點

依資訊安全管理系統為評估範圍，進行風險分析與評估，建立威脅弱點之詳細配對狀況。

(六)風險管理

完成風險評鑑後，針對仍需控制之風險討論可行之控制方法。應對執行風險管理計畫後之殘留風險進行預估。殘留風險如仍高於風險接受水準，應再增加控制，並修正風險管理計畫，如不再進行控制仍應具體提報是否有進一步控制之可能及成本效益評估。但風險等級 3 之殘留風險應低於風險等級 3。

風險管理計畫實施後應於每半年之調整維護時一併確認新增之風險控制之有效性，並確認是否達成原先預估之殘留風險水準，經確認可有效控制風險且不需再調整改變之新增控制可轉列為既有控制。

三、風險值的計算

(一) 資訊資產價值：針對各執行人員所評定之營運衝擊分析等級依據「營運衝擊等級價值對照表」轉換為相對之價值數值。

(二)　風險發生可能性數：如表 4-4 風險發生可能性判定準則表所示

表 4-4　風險發生可能性判定準則表

能性等級	可能性等級參考	建議數值
極高	一年內發生四次以上	1.00 0.77
高	一年內發生二至四次	0.76 0.53
中	一年內發生一次	0.52 0.29
低	三年內發生一次	0.28 0.05
極低	三年以上發生一次	0.04 0.00

資訊來源：本研究整理

（三）　風險影響等級程度：如表 4-5 風險影響程度等級判定準則表所示

表 4-5　風險影響程度等級判定準則表

影響程度等級	影響程度參考		建議數值
極高	0.81	1	0.90
高	0.51	0.8	0.65
中	0.21	0.5	0.35
低	0.06	0.2	0.13
極低	0	0.05	0.025

資料來源：本研究整理

（四）　計算風險值：各評估標的應就機密性、完整性及可用性進行風險值計算。風險值=評估標的之價值*風險發生可能性數值*風險發生對評估標的影響程度數值。

四、　存取控制

應訂定資訊系統存取控制規定，界定存取控制之需求，並以書面、電子或其他方式紀錄之。應包含電腦系統的存取控制與稽核、應用系統與資料庫的存取控制與稽核。

五、　營運持續管理

實施重要系統的永續營運管理作業，結合預防、備援機制及復原控制措施，將災難和安全缺失（可能是由於自然災害、意外、設備故障和蓄意行為等引起）所造成的中斷情形降低至可接受情形。

第四節　問卷設計

一、　設計過程

本研究根據中華民國國家標準「ISO27001」、「ISO27002」、「CMMI-1.2 中文版」流程管理之能力度等級模式與文獻資料等，選擇適用於發展的能力成熟度整合模式（CMMI）之流程領域與 CNS 資訊技術－安全技術－資訊安全管理作業規範（ISO27002）條文符合性高度相關的內容設計問卷。問卷設計內容編排確定後，請有計劃導入 ISO27001 公務部門資訊人員、已導入 ISO27001 公務部門資訊人員與認證之相關人員進行前測，合計 6 人進行前測，修正缺失題目，修改題意不清或艱深詞句，最後與專家學者討論後，完成正式問卷，期資訊部門人員能夠了解問卷內容。問卷內容包含受訪者基本資料、ISO27002 的重要性認知及 CMMI-流程管理之能力度等級施行程度三部分，共 40 題，整個填答過程應可於十五分鐘內完成。

二、　正式問卷內容

本研究問卷內容共分為三個部用封閉式結構型問卷

1、　第一部份是組織資訊安全管理導入的選擇描述。

表 4-6　本研究問卷第一部份之衡量構面來源

分析項目	變項/題數	節次	衡量問題
基本資料	4		1、請問您目前的職務是? 2、請問貴單位對於 ISO27001 的導入情形? 3、請問您是否知悉 ISO27001 資訊安全管理系統要求事項? 4、請問您是否知道 CMMI 能力成熟度整合模式之流程管理?

資料來源：本研究整理

2、　第二部份是 ISO27002 對資訊安全管理的重要性認知，以李克特(Liker)五點量表進行調查。

表 4-7　本研究問卷第二部份之衡量構面來源

ISO27002 需求管理	執行重要性/12	04	01、您覺得「風險評鑑及處理」宜依組織目標選擇接受的風險，選定控制措施實做控管，確保風險降低至可接受程度是否有執行的必要?
		05	02、您覺得「資訊安全政策文件」宜由管理階層核准，並傳達給所有員工與相關各外部團體是否有執行的必要?
		06	03、您覺得「資訊安全的組織」係指在組織內宜建立管理框架以啟動與控制資安全的實作是否有執行的必要?
		07	04、您覺得「資產管理－所有資產宜有人負責，以達成及維持組織資產的適切保護」是否有執行的必要?
		08	05、您覺得「人力資源安全－確保員工、承包商及第三方使用者瞭解其責任，宜簽署其安全角色與責任的協議」是否有執行的必要?
		09	06、您覺得「實體與環境安全－防止組織場所與資訊遭未經授權的實體存取、損害及干擾」是否有執行的必要?
		09	07、您覺得「通訊與作業管理－確保正確與安全地操作資訊處理設施」是否有執行的必要?
		10	08、您覺得「存取控制」宜根據營運與安全要求，控制資訊存取、資訊處理設施及營運過程，是否有執行的必要?
		11	09、您覺得「資訊系統獲取、開發及維護」宜識別並議定安全要求，確保安全是整體資訊系統的一部分，是否有執行的必要?
		12	10、您覺得「資訊安全事故管理」係確保與資訊系統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播，是否有執行的必要?
		13	11、您覺得「營運持續管理－為對抗營運活動中斷，保護重要營運過程不受系統失效或災害的影響，並確保及時再續，是否有執行的必要?
		14	12、您覺得「遵循性－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，是否有執行的必要?

資料來源：本研究整理

3、 第三部份是ISO27001條文與CMMI高度相關的各流程領域部份目標施行程度，採用經濟部工業局軟體生產力提升計畫(經濟部工業局，民91)-軟體發展能力評估問卷之評分標準，參酌CMMI流程改善量化績效指標資料訂定衡量構面。

表 4-8 本研究問卷第三部份之衡量構面來源

ISO27001 要求事項對應 CMMI 各流程領域目標與執行方法

01	風險評鑑及處理	風險管理- SP 2.1 界定風險(p480)
02	風險評鑑及處理	風險管理-SP 2.2 評估、分類及排序風險(p483)
03	資訊安全政策文件	組織流程定義+ IPPD-SP 1.1 建立標準流程(p247)
04	資訊安全政策文件	組織流程定義+ IPPD-SP 1.3 建立調適準則及指引(p248)
05	資訊安全的組織	組織流程專注-SP 1.1 建立組織流程需要(p271)
06	資訊安全的組織	組織流程專注-SP 3.2 推展標準流程(p280)
07	資產管理	組織流程定義+ IPPD-SP 1.4 建立組織度量儲存庫(p251)
08	資產管理	組織流程定義+ IPPD-SP 1.5 建立組織流程資產館(p252)
09	人力資源安全	供應商協議管理-SP 2.1 執行供應商協議(499)
10	人力資源安全	專案監控-SP 1.5 監控關鍵人員的參與(p353)
11	實體與環境安全	風險管理-SP 1.3 建立風險管理策略(p479)
12	實體與環境安全	風險管理-SP 3.2 執行風險降低計畫(p489)
13	通訊與作業管理	建構管理-SP 1.2 建構管理系統(p127)
14	通訊與作業管理	建構管理-SP 3.1 建立建構管理記錄(p133)
15	存取控制	專案監控-SP 1.4 監控承諾事項(p351)
16	存取控制	專案監控-SP 2.3 管理矯正措施(p357)
17	資訊系統獲取開發及維護	專案監控-SP 1.7 進行里程碑審查 (p355)
18	資訊系統獲取、開發及維護	組織流程績效-SP 1.4 建立流程績效基準(p298)
19	資訊安全事故管理	組織流程績效-SP 1.3 設定品質及流程績效目標(p295)
20	資訊安全事故管理	組織流程專注-SP 3.4 彙整流程相關經驗納

		入組織流程資產(p281)
21	營運持續管理	組織創新與推展-SP 1.4 選擇改善措施以便推展(p228)
22	營運持續管理	組織創新與推展-SP 2.3 度量改善效果(p233)
23	遵循性	組織流程績效-GP 5.1 確保持續的流程改善(p306)
24	遵循性	組織流程績效-GP 2.9 客觀評估遵循程度(p304)

資料來源：本研究整理

NTU Library

第五章　研究結果

第一節　效度與信度分析

資料分析結果，兩部份問項整體的 Cronbach's α 值達 0.975，表示問卷量表之正確性與可靠性為高度可信水準。問卷第二部份與第三部份各別信度說明如下：

表 5-1　ISO27001 資訊安全管理系統要求項目(第二部份)信度分析表

Reliability Statistics

Cronbach's Alpha	N of Items
.916	12

資料來源：本研究整理

說明: ISO27001 項目整體信度達 0.914，達高度可信水準。

表 5-2　CMMI 能力成熟度相關流程領域項目信度分析表

Reliability Statistics

Cronbach's Alpha	N of Items
.986	24

資料來源：本研究整理

說明: CMMI 項目整體信度達 0.98，表示高度可信。

表 5-3　ISO27001 與 CMMI 整體信度分析表

Reliability Statistics

Cronbach's Alpha	N of Items
.973	36

說明: CMMI 項目與 CMMI 項目併計整體信度達 0.973，表示高度可信。內容效度(content validity)是一種定性的效度，它界定一個觀念的範圍並分析判斷測量是否真能代表此範圍。本研究的目的在控討 ISO27001 資訊安全管理標準認知與 CMMI 軟體成熟度相關流程領域執行程度關聯性。問卷主架構以 CNS27001 各節次與 CMMI 相關流程領域的一般流程所規範的要求事項，作為評估依據，故此，本研究問卷已具相當程度的內容效度。

依據評量統計結果編製 ISO27001 資訊安全管理系統要求項目認知的次數

分配表，列示各評量點的樣本數、百分比(附錄 A)、平均數與標準差(附錄 B); CMMI 能力成熟度相關流程領域執行程度的次數分配表(附錄 C)，列示各評量點的樣本數、百分比、平均數與標準差(附錄 D)。

第二節　受訪者分析

本研究問卷於 2008 年 3 月，透過組織部門主管協助回收問卷，總計發放問卷 60 件，回收 51 份，回收率 85%，扣除無效問卷 2 份，實際有效問卷 49 份。依據問卷所蒐集的資料，經由 SPSS 13.0 版統計軟體進行問卷信度分析、敘述性統計及變異數分析等，以瞭解 B 級機關資訊人員對 ISO27001 要求事項認知與組織內 CMMI 能力成熟度流程管理相關流程領域的執行程度關聯程度。本研究回收的有效問卷共 49 份，受訪者基本資料分析說明如下：

一、　職務別分類

表 5-4　填答者職務別分析表

類別	項目	人數	有效百分比(%)
職務	資訊安全長	1	2.0
	資訊部門主管	8	16.3
	基層主管	5	10.2
	管理師	4	8.2
	系統執行(開發)人員	16	32.7
	機器操作(管理)人員	7	14.3
	其他	8	16.3
	總計	49	100

說明：其他人員包含資訊單位之資料輸入或約聘（僱）人員等

資料來源：本研究整理

二、 已通過 ISO27001 驗證比例

表 5-5 填答者所屬組織已通過 ISO27001 驗證分析表

類別	項目	人數	有效百分比(%)
組織導入 ISO27001 情形	已經導入	36	73.5
	正在導入	1	2.0
	計畫導入	10	20.4
	無計畫導入	2	4.1
	合計	49	100

資料來源：本研究整理

三、 瞭解 ISO27001 要求事項比例

表 5-6 填答者瞭解 ISO27001 要求事項比例

類別	項目	人數	有效百分比
知悉 ISO27001 要求事項	未曾接觸	3	6.1
	部份了解	23	46.9
	大部份了解	19	38.8
	完全了解	4	8.2
	合計	49	100

資料來源：本研究整理

四、 知道 CMMI 能力成熟度相關流程領域比例

表 5-7 填答者知道 CMMI 能力成熟度相關流程領域比例

類別	項目	人數	有效百分比
知道 CMMI 能力成熟度整合模式	未曾接觸	22	44.9
	部份了解	15	30.6
	大部份了解	9	18.4
	完全了解	3	6.1
	合計	49	100

資料來源：本研究整理

第三節敘述統計

一、 ISO27001 項目認知比例

依回收樣本資料統計，B 級機關的資訊部門人員對 ISO27001 資訊安全管理系統要求項目中，以實體環境安全及存取控制的認知程度最高，其他項目的認知亦在安全管理認知的 80%以上。

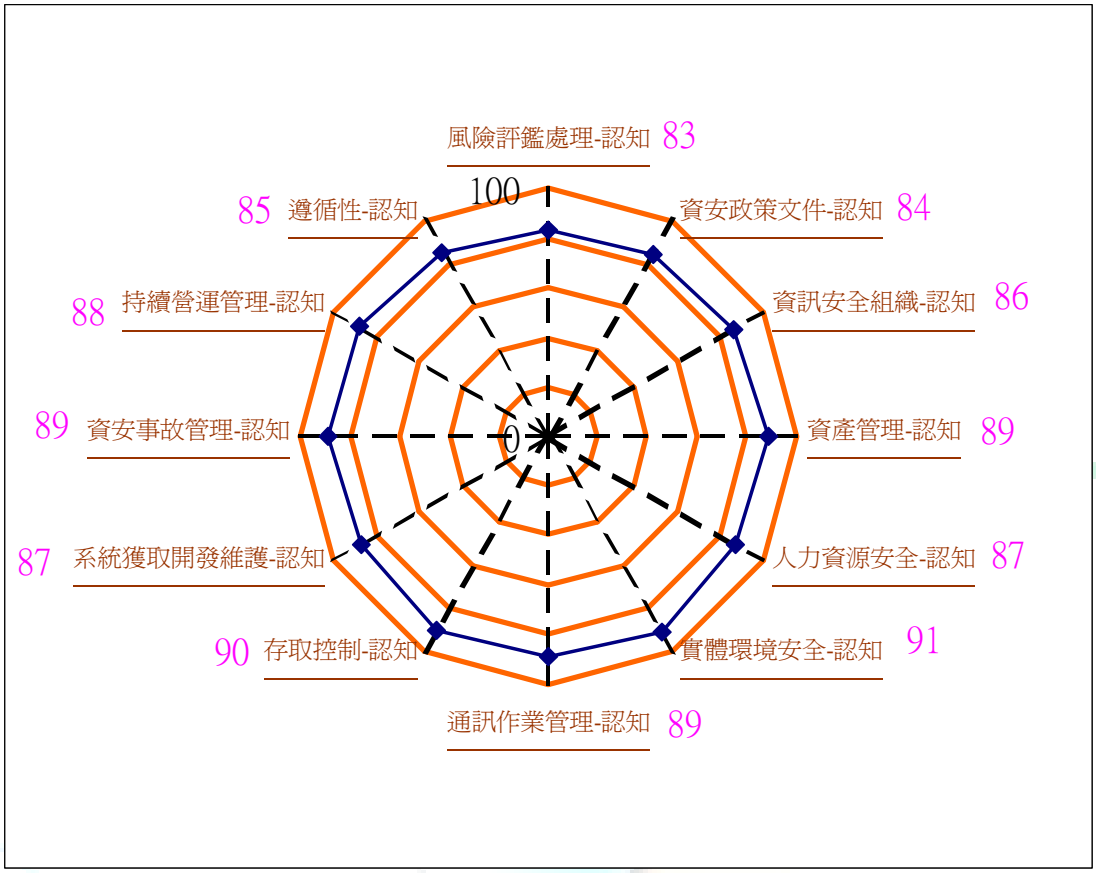

圖 5-1 資訊部門人員對 ISO27001 資訊安全管理系統要求項目認知程度統計

資料來源：本研究整理

說明:B 級機關資訊部門人員對 ISO27001 資訊安全管理系統的各項規範，均有較高的認知，達 83%以上，表示政府機關積極推廣資訊安全，獲得俱體成效。

二、 CMMI 相關領域一般目標執行程度比例

組織資訊部門人員對 CMMI 相關領域雖然不一定了解，但實際執行 ISO27001 要求項目時，其涉及 CMMI 能力成熟度整合模式相關領域的一般目標執行比例關係如下圖。

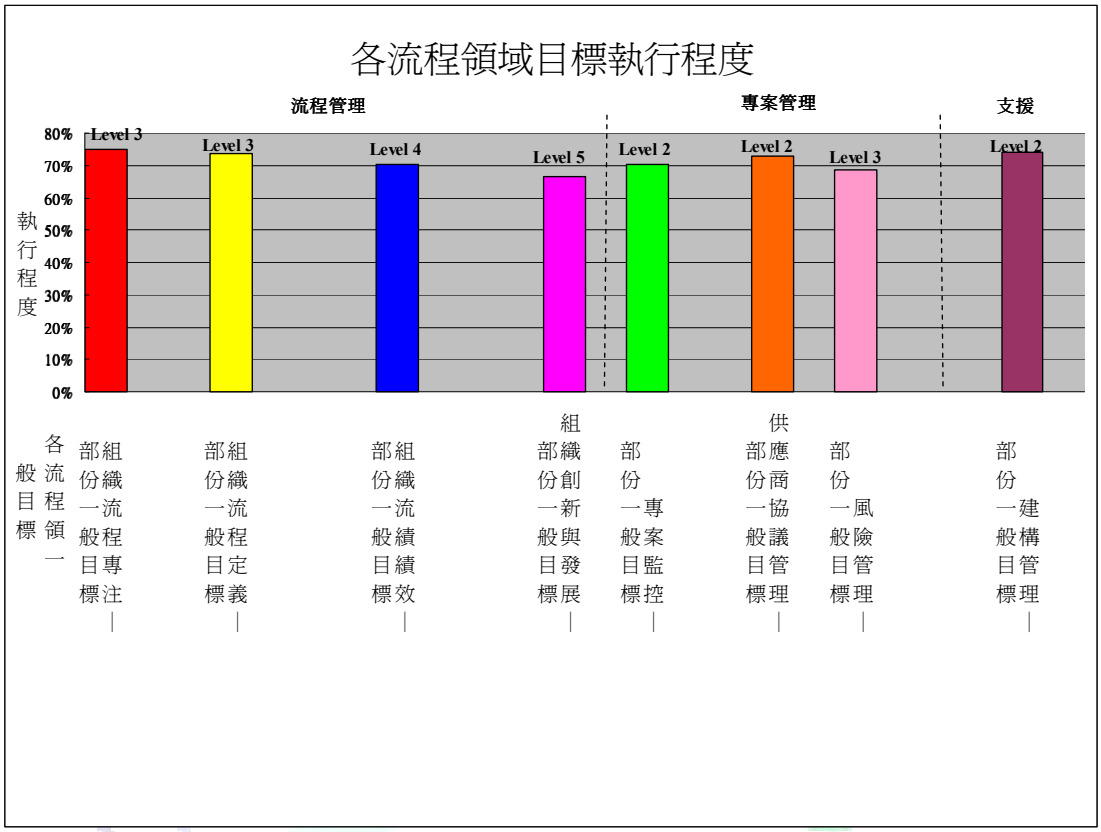

圖 5-2　CMMI 相關領域目標執行程度統計圖

資料來源：本研究整理

說明:依據蒐集樣本問項(附錄 E)所調查的 CMMI 各相關流程領域的執行程度，區分各類別統計，符合各流程領域平均實際執行程度，以流程管理之組織流程專注一般目標執行程度達最高。

第四節單因子變異數分析

單因素變異數分析測試某個控制變數的不同階層，觀察變數是否造成了顯著差異和變動(張太平、張一岑、蔡匡忠 ，2007)。

一、　知悉 ISO27001 資訊安全管理系統要求項目與資訊職務人員別認知程度的關係。

虛無假設 H_0:不同職務別人員對ISO27001項目認知無顯著差異

對立假設 H_1:不同職務別人員對ISO27001項目認知有顯著差異

表 5-8　知悉 ISO27001 要求項目與資訊人員別認知程度變異數分析

			df	F	Sig.
風險評鑑處理-認知	Between Groups	(Combined)	3	1.382	.261
資安政策文件-認知	Between Groups	(Combined)	3	1.329	.277
資訊安全組織-認知	Between Groups	(Combined)	3	1.770	.166
資產管理-認知	Between Groups	(Combined)	3	3.092	.036
人力資源安全-認知	Between Groups	(Combined)	3	.641	.593
實體環境安全-認知	Between Groups	(Combined)	3	2.647	.060
通訊作業管理-認知	Between Groups	(Combined)	3	3.093	.036
存取控制-認知	Between Groups	(Combined)	3	2.867	.047
系統獲取開發維護-認知	Between Groups	(Combined)	3	2.681	.058
資安事故管理-認知	Between Groups	(Combined)	3	2.394	.081
持續營運管理-認知	Between Groups	(Combined)	3	.808	.496
遵循性-認知	Between Groups	(Combined)	3	2.360	.084

資料來源：本研究整理

說明: 資產管理、通訊作業管理及存取控制等3項達顯著性，棄卻虛無假設 H_0，就ISO27001資訊安全管理系統作業要求項目的此3項規範，資訊職務人員知道與否，其認知程度有明顯差異。

二、知道 CMMI 成熟度整合模式執行程度項目與資訊職務人員別的關係。

虛無假設 H_0：不同職務別人員對CMMI執行程度項目的認知無顯著差異

對立假設 H_1：不同職務別人員對CMMI執行程度項目的認知有顯著差異

表 5-8　知道 CMMI 與資訊職務人員別變異數檢定

ANOVA

			df	F	Sig.
界定管理風險-執行程度	Between Groups	(Combined)	6	.954	.501
決定處理順序-執行程度	Between Groups	(Combined)	6	1.283	.286
滿足組織目標-執行程度	Between Groups	(Combined)	6	1.006	.435
資安調適準則-執行程度	Between Groups	(Combined)	6	1.686	.148
界定營運目標-執行程度	Between Groups	(Combined)	6	3.472	.007
維護流程記錄-執行程度	Between Groups	(Combined)	6	2.363	.047
實施訓練計畫-執行程度	Between Groups	(Combined)	6	1.493	.204
修訂標準流程-執行程度	Between Groups	(Combined)	6	1.217	.317
審查維護廠商-執行程度	Between Groups	(Combined)	6	.313	.927
審查關鍵人員-執行程度	Between Groups	(Combined)	6	1.190	.330
管理投入範圍-執行程度	Between Groups	(Combined)	6	.788	.584
建立時程績效-執行程度	Between Groups	(Combined)	6	.898	.505
建構管理系統-執行程度	Between Groups	(Combined)	6	.627	.707
管理變更記錄-執行程度	Between Groups	(Combined)	6	.827	.556
審查資安承諾-執行程度	Between Groups	(Combined)	6	.653	.687
記錄矯正措施-執行程度	Between Groups	(Combined)	6	.708	.645
審查管理記錄-執行程度	Between Groups	(Combined)	6	.559	.760
蒐集資安事件-執行程度	Between Groups	(Combined)	6	.686	.662
管理任務技能-執行程度	Between Groups	(Combined)	6	.675	.670
保存訓練記錄-執行程度	Between Groups	(Combined)	6	.718	.637
績效量化目標-執行程度	Between Groups	(Combined)	6	.965	.461
流程改善記錄-執行程度	Between Groups	(Combined)	6	1.120	.367
支援未來改善-執行程度	Between Groups	(Combined)	6	1.202	.364
法規遵循程度-執行程度	Between Groups	(Combined)	6	.732	.627

資料來源：本研究整理

說明:　CMMI相關流程領域組織執行程度項目中，界定營運目標與維護流程記錄顯著性，棄卻虛無假設 H_0，就CMMI相關流程領域組織執行程度而言，此二者對資訊職務人員知道與否，其執行程度有顯著差異。

三、　ISO27001 認知程度與 CMMI 相關流程領域執行上關係

虛無假設 H_0:ISO27001認知程度在CMMI相關流程領域執行上無顯著差異

對立假設 H_1:ISO27001認知程度在CMMI相關流程領域執行上有顯著差異

表 5-9　ISO27001 認知程度在 CMMI 相關流程領域執行差異與否變異數檢定

ANOVA

			df	F	Sig.
界定管理風險-執行程度	Between Groups	(Combined)	3	1.783	.164
決定處理順序-執行程度	Between Groups	(Combined)	3	1.408	.253
滿足組織目標-執行程度	Between Groups	(Combined)	3	1.319	.280
資安調適準則-執行程度	Between Groups	(Combined)	3	.790	.506
界定營運目標-執行程度	Between Groups	(Combined)	3	1.850	.152
維護流程記錄-執行程度	Between Groups	(Combined)	3	1.658	.189
實施訓練計畫-執行程度	Between Groups	(Combined)	3	1.741	.172
修訂標準流程-執行程度	Between Groups	(Combined)	3	1.089	.363
審查維護廠商-執行程度	Between Groups	(Combined)	3	.743.	.532
審查關鍵人員-執行程度	Between Groups	(Combined)	3	1.128	.348
管理投入範圍-執行程度	Between Groups	(Combined)	3	1.533	.219
建立時程績效-執行程度	Between Groups	(Combined)	3	.755	.525
建構管理系統-執行程度	Between Groups	(Combined)	3	.750	.528
管理變更記錄-執行程度	Between Groups	(Combined)	3	.942	.428
審查資安承諾-執行程度	Between Groups	(Combined)	3	1.586	.206
記錄矯正措施-執行程度	Between Groups	(Combined)	3	.907	.445
審查管理記錄-執行程度	Between Groups	(Combined)	3	1.376	.262
蒐集資安事件-執行程度	Between Groups	(Combined)	3	.957	.421
管理任務技能-執行程度	Between Groups	(Combined)	3	1.485	.231
保存訓練記錄-執行程度	Between Groups	(Combined)	3	1.839	.154
績效量化目標-執行程度	Between Groups	(Combined)	3	.632	.598
流程改善記錄-執行程度	Between Groups	(Combined)	3	1.501	.227
支援未來改善-執行程度	Between Groups	(Combined)	3	1.068	.372
法規遵循程度-執行程度	Between Groups	(Combined)	3	1.020	.393

資料來源：本研究整理

說明:　CMMI相關流程領域組織執行程度項目中，所有項目均未達顯著性，不棄卻虛無假設 H_0，不論ISO27001認知程度差異與否，其CMMI相關流程領域執行程度並無明顯差異。

四、　不同CMMI成熟模式對ISO27001認知程度的關係

虛無假設 H_0：不同 CMMI 成熟模式對 ISO27001 認知程度無顯著影響

對立假設 H_1：不同 CMMI 成熟模式對 ISO27001 認知程度有顯著影響

表 5-10 不同 CMMI 成熟模式對 ISO27001 認知程度差異與否變異數檢定

ANOVA

			df	F	Sig.
風險評鑑處理-認知	Between Groups	(Combined)	3	1.490	.230
資安政策文件-認知	Between Groups	(Combined)	3	4.634	.007
資訊安全組織-認知	Between Groups	(Combined)	3	3.140	.034
資產管理-認知	Between Groups	(Combined)	3	2.367	.083
人力資源安全-認知	Between Groups	(Combined)	3	2.490	.072
實體環境安全-認知	Between Groups	(Combined)	3	2.282	.092
通訊作業管理-認知	Between Groups	(Combined)	3	5.576	.002
存取控制-認知	Between Groups	(Combined)	3	2.506	.071
系統獲取開發維護-認知	Between Groups	(Combined)	3	3.355	.027
資安事故管理-認知	Between Groups	(Combined)	3	3.755	.017
持續營運管理-認知	Between Groups	(Combined)	3	4.025	.013
遵循性-認知	Between Groups	(Combined)	3	1.402	.255

資料來源：本研究整理

說明:資安政策文件、資訊安全組織、通訊作業管理、系統獲取開發維護、資安事故管理及持續營運管理等6項認知達顯著性，棄卻虛無假設 H_0，就不同CMMI成熟模式而言，顯著影響資訊安全管理系統作業要求項目相關規範的認知。

五、不同CMMI成熟模式對ISO27001認知程度顯著影響項目的關係大小

不同CMMI成熟模式對ISO27001認知程度顯著影響項目6項認知平均達顯著性F值為5.334，p值為0.003。

表 5-11 不同 CMMI 成熟模式對 ISO27001 認知程度影響關係大小

Post Hoc Tests

Multiple Comparisons

Dependent Variable: 認知平均
LSD

(I) 知道CMMI	(J) 知道CMMI	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
1	2	-.43965*	.12295	.001	-.6873	-.1920
	3	-.42298*	.14529	.006	-.7156	-.1303
	4	-.22854	.22599	.317	-.6837	.2266
2	1	.43965*	.12295	.001	.1920	.6873
	3	.01667	.15482	.915	-.2952	.3285
	4	.21111	.23224	.368	-.2566	.6789
3	1	.42298*	.14529	.006	.1303	.7156
	2	-.01667	.15482	.915	-.3285	.2952
	4	.19444	.24480	.431	-.2986	.6875
4	1	.22854	.22599	.317	-.2266	.6837
	2	-.21111	.23224	.368	-.6789	.2566
	3	-.19444	.24480	.431	-.6875	.2986

*. The mean difference is significant at the .05 level.

說明：不同CMMI成熟模式對ISO27001的認知影響程度的效果大小而言，對部份了解人員影響最大；影響大小依序為部份了解人員、大部分了解人員、完全了解人員及未曾接觸人員。

第五節　相關分析

二元區間變數的相關分析是指執行計算區間變數之間兩兩相關的相關係數，對兩個或兩個以上的區間變數之間兩兩相關的程度來做分析(張太平 & 張一岑 & 蔡匡忠 ，2007)。茲以本研究所設計的 ISO27001 資訊安全管理系統要求項目和 CMMI 軟體成熟度相關流程領域的執行程度的回覆樣本,所評量此兩項之相關分析如下:

ISO27001 資訊安全管理系統要求項目和 CMMI 軟體成熟度相關流程領域的執行程度彼此問項關性分析。

虛無假設 H_0:ISO27001 資訊安全管理系統要求項目和 CMMI 軟體成熟度相關流程領域的執行程度變項間無顯著關係

對立假設 H_1:ISO27001 資訊安全管理系統要求項目和 CMMI 軟體成熟度相關流程領域的執行程度變項間有顯著關係

表 5-12 ISO27001 認知程度項目與 CMMI 相關流程領域執行程度相關性

		風險評鑑處理-認知	資安政策文件-認知	資訊安全組織-認知	資產管理-認知	人力資源安全-認知	實體環境安全-認知	通訊作業管理-認知	存取控制-認知	系統獲取開發維護-認知	存取控制-認知	持續營運管理-認知	遵循性-認知
界定管理風險-執行程度	Pearson 相關	.287(*)	.410(**)	.321(*)	.344(*)	.167	.305(*)	.270	.157	.209	.237	.209	.113
	顯著性 (雙尾)	.045	.003	.025	.016	.251	.033	.061	.282	.150	.101	.149	.441
決定處理順序-執行程度	Pearson 相關	.285(*)	.341(*)	.216	.334(*)	.139	.268	.192	.100	.155	.192	.204	.083
	顯著性 (雙尾)	.047	.017	.136	.019	.339	.063	.185	.496	.287	.185	.160	.569
滿足組織目標-執行程度	Pearson 相關	.293(*)	.347(*)	.188	.230	.161	.274	.246	.164	.148	.172	.256	.085
	顯著性 (雙尾)	.041	.015	.196	.112	.269	.057	.089	.262	.309	.236	.075	.562
資安調適準則-執行程度	Pearson 相關	.193	.309(*)	.153	.163	.112	.230	.211	.214	.277	.137	.193	.111
	顯著性 (雙尾)	.185	.031	.293	.263	.442	.112	.145	.139	.054	.347	.185	.446
界定營運目標-執行程度	Pearson 相關	.260	.190	.015	.005	-.123	.192	.149	.297(*)	.110	.041	.148	-.002
	顯著性 (雙尾)	.071	.191	.916	.974	.398	.186	.306	.038	.452	.779	.310	.988
維護流程記錄-執程度	Pearson 相關	.035	.150	.074	.173	.146	.237	.185	.236	.139	.074	-.009	.051
	顯著性 (雙尾)	.813	.303	.613	.234	.315	.102	.202	.103	.342	.613	.952	.728
實施訓練計畫-執行程度	Pearson 相關	.005	.112	.123	.120	.141	.158	.129	.137	.024	.054	-.055	-.001
	顯著性 (雙尾)	.973	.442	.399	.410	.334	.278	.378	.350	.870	.714	.709	.992
修訂標準流程-執行程度	Pearson 相關	.084	.212	.032	.183	.059	.159	.122	.031	.049	.048	-.029	.052
	顯著性 (雙尾)	.565	.144	.828	.207	.686	.277	.404	.833	.738	.745	.845	.724

審查維護廠商-執行程度	Pearson 相關	.109	.203	.192	.212	.202	.169	.145	.035	.211	.104	.049	.058
	顯著性 (雙尾)	.458	.161	.187	.144	.165	.246	.320	.809	.146	.475	.736	.694
審查關鍵人員-執行程度	Pearson 相關	.117	.201	.163	.187	.112	.027	-.004	-.008	.086	-.033	.055	.010
	顯著性 (雙尾)	.423	.166	.264	.197	.443	.856	.977	.955	.559	.820	.707	.947
管理投入範圍-執行程度	Pearson 相關	.101	.183	.058	.097	-.036	.054	-.022	-.007	-.005	-.054	.021	-.064
	顯著性 (雙尾)	.491	.208	.690	.509	.809	.712	.878	.961	.971	.713	.886	.660
建立時程績效-執行程度	Pearson 相關	.216	.338(*)	.202	.270	.243	.102	.058	.004	.164	.029	.152	.127
	顯著性 (雙尾)	.137	.018	.165	.061	.092	.485	.694	.979	.261	.844	.297	.384
建構管理系統-執行程度	Pearson 相關	.021	.122	.085	.137	.131	.240	.186	.219	.137	.068	.021	-.001
	顯著性 (雙尾)	.885	.406	.563	.346	.370	.096	.200	.131	.348	.643	.886	.996
管理變更記錄-執行程度	Pearson 相關	.271	.372(**)	.276	.303(*)	.178	.248	.233	.119	.227	.203	.208	.120
	顯著性 (雙尾)	.060	.009	.055	.034	.221	.086	.107	.415	.117	.162	.151	.411
審查資安承諾-執行程度	Pearson 相關	.335(*)	.358(*)	.258	.262	.191	.267	.249	.163	.208	.188	.247	.188
	顯著性 (雙尾)	.018	.012	.073	.069	.188	.063	.084	.263	.152	.196	.087	.196
記錄矯正措施-執行程度	Pearson 相關	.201	.259	.164	.244	.097	.123	.055	.007	.047	.055	.109	.046
	顯著性 (雙尾)	.166	.072	.259	.091	.507	.400	.709	.961	.751	.709	.457	.752
審查管理記錄-執行程度	Pearson 相關	.234	.361(*)	.259	.335(*)	.215	.246	.237	.092	.206	.237	.238	.135
	顯著性 (雙尾)	.105	.011	.072	.019	.138	.088	.100	.531	.156	.100	.099	.355
蒐集資安事件-執行程度	Pearson 相關	.186	.305(*)	.171	.255	.126	.247	.143	.113	.210	.143	.244	.106
	顯著性 (雙尾)	.201	.033	.240	.077	.388	.088	.326	.437	.148	.326	.091	.470
管理任務技能-執	Pearson 相關	.208	.296(*)	.222	.243	.111	.273	.222	.202	.255	.185	.240	.087

行程度	顯著性 (雙尾)	.152	.039	.125	.093	.447	.057	.125	.165	.077	.202	.096	.553
保存訓練記錄-執行程度	Pearson 相關	.162	.165	.052	.108	.049	.305(*)	.262	.234	.189	.115	.151	.069
	顯著性 (雙尾)	.267	.258	.721	.461	.737	.033	.069	.105	.194	.430	.300	.640
績效量化目標-執行程度	Pearson 相關	.062	.220	.163	.271	.153	.064	.075	-.010	.089	.044	.095	-.005
	顯著性 (雙尾)	.674	.129	.265	.059	.293	.661	.610	.943	.545	.764	.514	.970
流程改善記錄-執行程度	Pearson 相關	.283(*)	.277	.124	.279	.134	.237	.170	.154	.138	.105	.206	.080
	顯著性 (雙尾)	.049	.054	.397	.052	.358	.101	.244	.289	.343	.471	.155	.584
支援未來改善-執行程度	Pearson 相關	.222	.264	.170	.254	.125	.221	.170	.099	.157	.102	.179	.117
	顯著性 (雙尾)	.125	.067	.244	.078	.393	.126	.244	.498	.280	.486	.218	.424
法規遵循程度-執行程度	Pearson 相關	.199	.235	.088	.203	.112	.119	.020	.006	.034	-.008	.147	.003
	顯著性 (雙尾)	.170	.104	.546	.162	.442	.415	.891	.965	.815	.956	.315	.982

** 在顯著水準爲0.01時 (雙尾)，相關顯著。

* 在顯著水準爲 0.05 時 (雙尾)，相關顯著。

資料來源：本研究整理

說明:相關達顯著性，表示其關係不為0， Pearson關係係數為正數項目，表示正相關關係，即透過運運用ISO27001認知程度項目的建置，可以達成CMMI相關流程領域部份目標的建構。風險評鑑處理--界定管理風險、決定處理順序、滿足組織目標、審查資安承諾、流程改善記錄；資安政策文件--界定管理風險、決定處理順序、滿足組織目標、建立時程績效、變更管理記錄、審查資安承諾；資訊安全組織--界定管理風險；資產管理--決定處理順序；實體環境安全--界定管理風險；存取控制--界定管理風險等對應項目達顯著性，棄卻虛無假設 H_0，表示其確有相關性。

第六節典型相關分析

針對準則變數(ISO27001)和預測變數(CMMI)分析，以典型負荷量(canonical loadings)表示兩組變數間相關程度。各變數的典型負荷量平方值的簡單平均數就是典型變量所解釋之共有變量之比例，即自我解釋的能力。

表 5-13 典型相關分析表

Canonical R: .9597864			
Chi-Square: 365.8333 df = (288) p = .0013461			
Number of valid cases: 49			
	No. of vars.	Variance extracted	Total redundancy given the other set
Left set(ISO27001)	12	100.00000000%	59.080093768%
Right set（CMMI）	24	34.306301784%	16.903303428%

資料來源：本研究整理

說明: 相關係數達0.96，顯示整體相關性極高；p值為0.0013461達顯著性，棄卻虛無假設 H_0，表示其兩個變項組相關性是顯著存在的不為零。未來公務組織不論是推動ISO27001資訊安全管理實務或CMMI能力成熟度整合模式，屬可同步建立相關的資訊流程管理。左邊(left set)指ISO27001的12個問項，右邊(right set)則是指CMMI的24個問項。從整體來看，ISO27001的12個問項可以被自已的典型變項解釋高達100%，而被CMMI的典型變項解釋能力也約達60%；CMMI的24個問項可以被自已的典型變項解釋僅達34%，而被ISO27001的典型變項解釋能力只有約17%，以關係結構而言，可以說CMMI執行程度對ISO27001認知有相當程度的影響效果.(如圖5-3)。

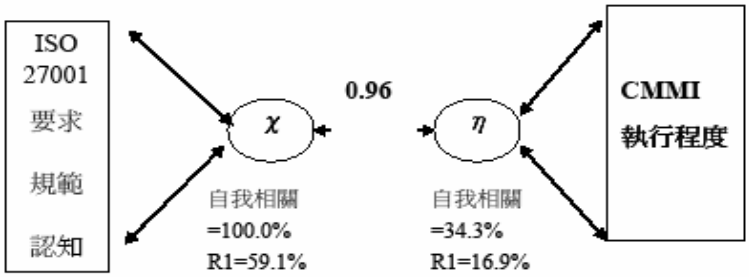

圖 5-3 整體典型相關

第七節　研究結果

一、　B 級機關的資訊部門人員對 ISO27001 資訊安全管理系統要求項目認知比例，平均值在 83%以上，收集樣本組織中有 65%已參與驗證，有助民眾對於政府所提供的資訊服務，產生正面的信賴感。

二、　ISO27001 資訊安全管理系統要求項目中，風險評鑑處理、資安政策文件、資訊安全組織、人力資源安全、實體安全管理、系統獲取開發維護、資安事故管理、持續營運管理、遵循性等 9 個項目，不論資訊部門人員知悉與否，已內化為個人的觀念中，足見此九項認知，已成為政府資訊人員的圭臬。

三、　CMMI 相關流程領域分類中，各流程領域相關執行程度的一般目標，除界定營運目標與流程改善記錄符，其餘項目不論資訊部門人員知道與否，其執行程度無明顯差異。

四、　已參與 ISO27001 驗證組織，資訊部門人員在風險評鑑處理的認知上，是有顯著的差異，與 ISO27001 驗證要求的量化並控制風險，已獲得確實的執行。

五、　CMMI 相關流程領域分類部份一般目標中，與 ISO27001 資訊安全管理系統要求項目具正向關係(關係係數達 0.3 以上)，透過 ISO27001 驗證制度，逐步建構組織資訊安全成熟度，有助組織的創新與發展，如表 5-14 CMMI 相關流程領域與 ISO27001 要求項目關係係數表。

表 5-14 CMMI 相關流程領域部份一般目標與 ISO27001 要求項目關係係數表

CMMI 相關流程領域-分類	CMMI 相關流程領域-執行	一般目標	ISO27001 要求項目	Pearson's 關係係數
專案管理	風險管理	界定風險	資安政策文件	0.410
專案管理	風險管理	評估、分類及排序風險	資安政策文件	0.341
流程管理	組織流程定義	建立標準流程	資安政策文件	0.347
專案管理	風險管理	執行風險降低計畫	資安政策文件	0.338
支援	建構管理	建立建構管理記錄	資安政策文件	0.372
專案管理	專案監控	監控承諾事項	資安政策文件	0.358
專案管理	專案監控	進行里程碑審查	資安政策文件	0.361
流程管理	組織流程績效	建立流程績效基準	資安政策文件	0.305
專案管理	風險管理	界定風險	資訊安全組織	0.321
專案管理	風險管理	評估、分類及排序風險	資產管理	0.334
專案管理	風險管理	界定風險	實體環境安全	0.305

資料來源：本研究整理

六、　公務部門組織蒐集樣本中，雖然有 44.9%不知道 CMMI 成熟度整合模式，但仍具有部份實質的執行關聯，顯見行政組織資訊部門有良善的管理基礎，更有利於導入 CMMI 成熟度整合模式，推動組織的創新與發展。

七、　ISO27001 要求項目與 CMMI 相關流程領域部份一般目標，具有整體典型相關關係。

第六章　結論與建議

第一節　研究結論

高度資訊化的社會，民眾對於政府與關鍵基礎建設的期待在於兩者所提供的資訊服務是可以安心且可信賴的。政府組織投入資源以強化資訊的作為組織要務之際，資安的重要性不應被忽視；以透過資安驗證方式，建構組織的能力成熟度，為組織的核心業務創造價值，達成未來的競爭優勢。

一、典型相關結果的呈現，顯示 CMMI 推動的成效，應能有效提昇 ISO27001 資訊安全管理系統的認知；在流程目標上，CMMI 所包含的成熟度領域，各層次構面寬廣，可能對組織資訊安全流程提供許多助益。實務上，CMMI 驗證所需的成本亦高於 ISO27001 驗證費用。若組織預算經費充足，可考量優先導入 CMMI 成熟度整合模式，除滿足各資訊系統的流程管理外，亦能提高組織資訊安全管理的相關認知，對未來 ISO27001 的導入將產生明顯效益。

二、以各節次大項分析結果，CNS27002 資訊安全管理系統規範實務，與 CMMI 能力成熟度整合模式的分類流程領域(部份一般目標)，具有正向關係項目(表 6-1)，說明如下：

(一)、風險評鑑及處理(節次 4.1)

- 專案管理-風險管理-界定管理風險（SP 2.1）應是有組織及透徹的方法，使用風險分類表來評量風險。
- 專案管理-風險管理-界定管理風險（SP 2.2）利用定義風險種類及參數，評估及分類每個已界定的風險，並決定其當的優先處理順序。
- 流程管理--組織流程定義-建立標準流程（SP 1.1）確保組織標準流程能滿足流程需要與組織目標。
- 專案管理-專案監控-監控資料管理（SP 1.4）定期審查承諾(包含外部及內部的)，記錄承諾審查的結果。

(二)、資安政策文件(節次 5.1.1)

- 流程管理-組織流程定義-建立調適準則及指引（SP 1.3）在調適與定義流程的彈以及確保全組織流程的適當一致性。
- 專案管理-風險管理-界定管理風險（SP 2.1）應是有組織及透徹的方法，使用風險分類表來評量風險。
- 專案管理-風險管理-界定管理風險（SP 2.2）利用定義風險種類及參數，評估及分類每個已界定的風險，並決定其當的優先處理順序。
- 流程管理--組織流程定義-建立標準流程（SP 1.1）確保組織標準流程能滿足流程需要與組織目標。
- 支援-建構管理-建立建構管理記錄（SP 3.1）建立並建構描述建構項目的記錄。

- 專案管理-專案監控-監控資料管理（SP 1.4）定期審查承諾(包含外部及內部的)，記錄承諾審查的結果。
- 流程管理-組織流程績效-建立流程績效基準（SP 1.4）從蒐集的度量資料及分析結果，建立並維護組織的流程績效基準。
- 流程管理-組織流程專注-彙整流程相關經驗納入組流程資產（SP 3.4）納入流程相關的工作產品、度量及導自規劃與執行流程的改善活動活動記錄，至組織的流程資產。

（三）、資訊安全組織(節次 6)

- 專案管理-風險管理-界定管理風險（SP 2.1）應是有組織及透徹的方法，使用風險分類表來評量風險。

（四）、資產管理(節次 7)

- 專案管理-風險管理-界定管理風險（SP 2.1）應是有組織及透徹的方法，使用風險分類表來評量風險。

（五）、實體與環境安全(節次 9)

- 專案管理-風險管理-界定管理風險（SP 2.1）應是有組織及透徹的方法，使用風險分類表來評量風險。

（六）、存取控制(節次 11)

- 流程管理-組織流程專注-建立組織流程需要（SP 1.1）界定適用於組織流程的政策、標準及經營模式。

表 6-1　CMMI 相關流程領域部份目標與 ISO27001 實務項目具正向關係之項目表

CMMI 流程領域 \ ISO27001 項目	風險評鑑處理-認知	資安政策文件-認知	資訊安全組織-認知	資產管理-認知	人力資源安全-認知	實體環境安全-認知	通訊作業管理-認知	存取控制-認知	系統獲取開發維護-認知	資安事故管理-認知	持續營運管理-認知	遵循性-認知
界定管理風險-執行程度	■	■	■	■		■						
決定處理順序-執行程度	■	■		■								
滿足組織目標-執行程度	■	■										
資安調適準則-執行程度		■										
界定營運目標-執行程度								■				
維護流程記錄-執行程度												
實施訓練計畫-執行程度												
修訂標準流程-執行程度												
審查維護廠商-執行程度												
審查關鍵人員-執行程度												
管理投入範圍-執行程度												
建立時程績效-執行程度		■										
建構管理系統-執行程度												
管理變更記錄-執行程度		■										
審查資安承諾-執行程度	■	■										
記錄矯正措施-執行程度												
審查管理記錄-執行程度		■		■								
蒐集資安事件-執行程度		■										
管理任務技能-執行程度		■										
保存訓練記錄-執行程度						■						
績效量化目標-執行程度												
流程改善記錄-執行程度	■											
支援未來改善-執行程度												
法規遵循程度-執行程度												

資料來源:本研究整理

ISO27001 資訊安全管理系統要求項目，與 CMMI 的專案管理、流程管理、支援等分類流程領域的部份正向關係，顯示可同時努力促成。透過組織核心業務導入資訊安全管理系統，通過國內或國外的 ISO27001 驗證，並建構 CMMI 成熟度能力(連續式)相關流程領域部份一般目標。

ISO27001 資訊安全管理系統要求項目中，落實執行「資安政策文件」要求

規範，符合 CMMI 相關流程領域一般目標(流程)最多，可見其關聯性最高，代表組織相當重視此項目且有效的落實執行；選定既有的流程領域流程，推展與公務組織核心業務相關的流程領域，有助未來可能的建置與推廣。

資訊安全流程管理大部份非組織的核心業務，但其重要性與日俱增，運用資訊安全管理流程支援組織核心業務的創新發展，有助提升公務部門的全球競爭力。在資通訊科技一日千里的數位經濟時代，以創造新法則與新思維的方式，結合政府與企業力量，共同營造台灣的優質安全的網路化社會。

第二節　研究限制

某些控制措施被視為實作資訊安全的很好起點，也適合用於大部分的環境中，但任何控制措施是否適用，取決於組織業務特性及其所面臨的特定風險。因此，儘管本研究的作法可被視為很好起點，但不能完全取代基於組織業務特性，而採用的風險評鑑控制措施選擇。另外，CMMI 的能力度等級的調整與改善，可衡量組織經費的年度預算，符合其支用科目原則，故試行導入之組織，亦應個別考量其經費來源及相關人力的負荷。

各組織核心業務不盡相同，標準流程適用指引亦有所差異，本研究所蒐集的 B 級機關，具有相同的業務特性，並非涵蓋所有的 B 級機關；CMMI 各流程領域一般目標與特定目標數量頗多，本研究選擇部份一般目標，僅推論其單項作法與 CNS27001 部份節次範圍，未及包含所有流程領域的目標及控制措施。

第三節　未來研究的建議

一、本研究以政府組織 B 級機關為研究對象，後續研究可擴大研究範圍，以 A 級或 C 級機關進行研究調查，在導入 ISO27001 資訊安全管理系統時，併同建構 CMMI 軟體成熟度部份相關流程領域，實際提升公務組織創新發展程度。

二、CMMI 軟體成熟度流程領域中，仍有相當多的特定目標與一般目標，具有資訊安全管理性質的特定流程與一般流程，選擇適合組織核心目標的相關流程領域，探討分析後，規畫建置組織的資訊安全管理系統。

三、資安治理成熟度已列入國家資通訊安全發案方案(98 年至 101 年)，未來可併同參酌建置研究。

參考文獻

【中文部分】

【1】 中華民國國家標準-資訊技術、安全技術、資訊安全、管理系統要求事項：CNS27001,X6049（民 96）。

【2】 中華民國國家標準- 資訊技術、安全技術、資訊安全管理之作業規範：CNS27002,X6040（民 96）。

【3】 中華民國國家標準-能力成熟度模型整合之評鑑要求：CNS15190,X6057(民 97)

【4】 卡內基美隆大學軟體工程學院(2006)。適用於發展的能力成熟度整合模式(CMMI-DEV)1.2 版(NO.FA872105C0003)。賓夕法尼亞州:卡內基美隆大學。

【5】 朱慧德(民 91)。CMMI 模式表述架構與選擇。軟體產業通訊，47，28-34。

【6】 行政院國家資通安全會報(民 90 年 1 月，民 93 年 3 月)。建立我國通資訊基礎建設安全機制計畫。

【7】 行政院國家資通安全會報（民 98）。 國家資通訊安全發展方案。

【8】 宋振華、楊子劍（2001）。組織資訊安全體系與資訊安全整體架構。張俊彥(主持人)，The Essentials of Audit for Information Security Management — Study on Electronic Banking 。資訊系統可信賴作業體制研討會論文集，交通大學。

【9】 李東峰（2001）。企業資訊安全控制制度之研究。二十一世紀台灣湧現中的資訊管理議題研討會暨第三屆全國資訊管理博士生聯合研討會。中正大學。

【10】 李東峰、林子銘（民90）。風險評估觀點的資訊安全規劃架構。第十二屆國際資訊管理學術研討會。台灣大學。

【11】 姚俊羽(民 93)。能力成熟度整合模式之導入-以文件管理系統為例。銘傳大學資訊管理研究所碩士論文，未出版，台北市。

【12】 洪肇奎(民93年4月)。如何成為一個具備流程改善基礎的組織。吳裕光(主持人)，台灣軟體流程改善聯盟：SPIN-Taiwan研討會，中國文化大學。

【13】 洪國興、徐鈺宗(民91)。資訊安全管理理論之探討。資管評論，第12期，17-47。

【14】 洪興國、李延平、趙榮耀(民92)。資訊安估準則層級結構之研究。圖書館學與資訊科學，29(2)，22-44。

【15】 翁玉麟(民91)。由ISO 9000至整合能力成熟度過程之模型之研究-以某校技術合作處為例。中國文化大學資訊管理研究所碩士論文，未出版，台北市。

【16】 張紹勳(2004)。研究方法。臺中市:滄海。

【17】 張太平、張一岑、蔡匡忠(2007)。統計建模與分析程序。台北市:文魁。
【18】 黃承聖(民89)。企業資訊安全的起點-資訊安全政策。網路通訊雜誌，109，100-103。
【19】 楊金炎（民90)。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，未出版。桃園縣。
【20】 經濟部工業局(民91)。軟體發展能力評估手冊二版(軟體生產力提升計畫)。台北市: 經濟部工業局。
【21】 葉至誠、葉立誠(2003)。研究方法與論文寫作。台北市:商鼎文化。
【22】 樊國楨（民 93 年 10 月)。美國聯邦政府資訊安全管理系統稽核作業與相關標準初探。張明桑(主持人)，網際空間：資訊、法律與社會。學術研究暨實務研討會，中央警察大學。
【23】 樊國楨（主編)(民91)。資通安全專輯之五：資訊安全風險管理。台北市：行政院國家科學委員會科學技術資料中心。[ISBN：9576190762]。
【24】 樊國楨（主編)(民91)。通資安全專輯之六：資訊安全能力評鑑。台北市：行政院國家科學委員會科學技術資料中心。 [ISBN：9576190764]。
【25】 歐弘詹(民95)。標準化應用於中小企業導入資訊安全管理系統之成功經驗。台北市:中華民國國家資訊基本建設產業發展協進會。
【26】 謝昆霖、呂易儒(民 95)。資訊管理研究。非營利單位資訊災難備援機制建置之研究，6，82-100。
【27】 鍾依萍、周樹林(民 93)。我國 CMM/CMMI 應用現況與發展趨勢。台北市:財團法人工業策進會。

【西文部分】

【1】 Bs7799-2(2002). Information Security Management-Part 2 : Specification for Information Security Management System. British Standards Institution (BSI). London.

【2】 CMMI Product Team,(2006) . ” CMMI for Systems Engineering/Software Engineering /Integrated Product and Process Development/Supplier Sourcing Version 1.2， Staged Representation”, CMU/SEI(NO.FA872105C0003)。Pittsburgh : Carnegie Mellon University.

【3】 Flynn, N. L. (2001). The e Policy handbook：Designing and Implementing Effective E-Mail , Internet, and Software Policies. New York : American Management Association.

【4】 Gupta,M., Chaturvedi,A.R., Mehta,S &Valeri,l. (2000). The Experimental Analysis of Information Security Management Issues for Online Financial Services. Information systems,667-675.

【5】 ISO/IEC 17799(2000)-Information technology-Code of Practice for Information Security Management.British Standards Institution.

【6】 Kabay, M. E. (1996). The NCSA Guide to Enterprise Security. Denver: McGraw: McGraw-Hill.

【7】 Parker D.B. (1997) . “Information Security in a Nutshell” . Information Security journal,6,14-19.

【8】 Reid,R.C. & Floyd, S.A.(2001). Extending the Risk Analysis Model to Include Market –Insurance. Computers & Security, 20(4), 331-339.

【9】 Sherwood, J. (1996). SALSA : A method for developing the enterprise security architecture and Strategy. Computer & Security, 2(3), 8-17.

【10】 The IT Governance Institute (2007). COBIT (4.1.ISBN:1933284722). Rolling Meadows Illinois: IT Governance Institute.

【11】 Von Solms, R. (1996). Information Security Management: The Second Generation. Computer & Security,15(4) , 281-288.

【12】 Von Solms, R., Van Haar, H., Von Solms, S. H. & Caelli, W. J. (1994). A Framework for Information Security Evaluation. Information & Management, 26, 143-153.

【13】 Wright, M. (1999). Third Generation Risk Management Practices. Computer Fraud & Security, 2, 9-12.

【網站部份】

【1】 Computer Security Institute. (2006, September 28).CSI 2008 Security Survey. Retrieved November 12, 2008， from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.p

【2】 Computer Security Institute. (2008).CSI 2008 Security Survey. Retrieved March 3, 2009, from http://www.gocsi.com/forms/csi_survey.jhtml

【3】 Carnegie Mellon University, SEI,(2009,april). Cataloged vulnerabilities. Retrieved April 5,2009,from the cert web site: http://www.cert.org/stats/cert_stats.html

【4】 Carnegie Mellon University, Software Engineering Institute. (2007,November).Capability Maturity Model Integration(CMMI-DEV 1.2 版). Retrieved March 2, 2009, from http://www.sei.cmu.edu/publications/documents/06.reports/06tr008.html

【5】 Carnegie Mellon University, Software Engineering Institute.The IDEAL^{SM} model. Retrieved March 2, 2009, from http://www.sei.cmu.edu/ideal

【6】 The SANS (SysAdmin, Audit, Network, Security) Institute.(2007, November 28). ***Top-20 2007 Security Risks*** **.** Retrieved April 3, 2009, from http://www.sans.org/top20/

附錄

附錄 A　ISO27001 資訊安全管理系統要求項目認知次數分配表

題號	要求項目執行必要認知程度	非常不同意←→非常同意					
			1	2	3	4	5
01	風險評鑑及處理	樣本數	0	0	5	32	12
		百分比	0	0	10.	65.3	24.5
02	資訊安全政策文件	樣本數	0	0	7	24	18
		百分比	0	0	14.3	49.0	36.7
03	資訊安全的組織	樣本數	0	0	2	31	16
		百分比	0	0	4.1	63.3	32.7
04	資產管理	樣本數	0	0	2	24	23
		百分比	0	0	4.1	49.0	46.9
05	人力資源安全	樣本數	0	0	2	27	20
		百分比	0	0	4.1	55.1	40.8
06	實體與環境安全	樣本數	0	0	1	21	27
		百分比	0	0	2.0	42.9	55.1
07	通訊與作業管理	樣本數	0	0	1	26	22
		百分比	0	0	2.0	53.1	44.9
08	存取控制	樣本數	0	0	2	21	26
		百分比	0	0	4.1	42.9	53.1
09	資訊系統獲取開發及維護	樣本數	0	0	1	31	17
		百分比	0	0	2.0	63.3	34.7
10	資訊安全事故管理	樣本數	0	0	1	26	22
		百分比	0	0	2.0	53.1	44.9
11	營運持續管理	樣本數	0	1	1	24	23
		百分比	0	2.0	2.0	49.0	46.9
12	遵循性	樣本數	0	0	3	31	15
		百分比	0	0	6.1	63.3	30.6

附錄 B　ISO27001 資訊安全管理系統要求項目認知程度平均數與標準差

Descriptive Statistics

	N	Mean	Std.	Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Std. Error
風險評鑑處理-認知	49	4.14	.577	-.006	.668
資安政策文件-認知	49	4.22	.685	-.807	.668
資訊安全組織-認知	49	4.29	.540	-.467	.668
資產管理-認知	49	4.43	.577	-.734	.668
人力資源安全-認知	49	4.37	.566	-.742	.668
實體環境安全-認知	49	4.53	.544	-.915	.668
通訊作業管理-認知	49	4.43	.540	-1.147	.668
存取控制-認知	49	4.49	.582	-.554	.668
系統獲取開發維護-認知	49	4.33	.516	-.882	.668
資安事故管理-認知	49	4.43	.540	-1.147	.668
持續營運管理-認知	49	4.41	.643	2.478	.668
遵循性-認知	49	4.24	.560	-.273	.668
Valid N (listwise)	49				

附錄 C　CMMI 能力成熟度相關流程領域執行程度次數分配表

題號	要求項目執行必要認知程度	非常不同意 ←→ 非常同意					
			1	2	3	4	5
01	風險管理-界定風險	樣本數	4	11	2	27	5
		百分比	8.2	22.4	4.1	55.1	10.2
02	風險管理-評估、分類及排序風險	樣本數	3	10	2	26	8
		百分比	6.1	20.4	4.1	53.1	16.3
03	組織流程定義+IPPD-建立標準流程	樣本數	2	7	6	26	8
		百分比	4.1	14.3	12.2	53.1	16.3
04	組織流程定義+IPPD-建立調適準則及指引	樣本數	3	6	9	26	5
		百分比	6.1	12.2	18.4	53.1	10.2
05	組織流程專注-建立組織流程需要	樣本數	2	6	5	25	11
		百分比	4.1	12.2	10.2	51.0	22.4
06	組織流程專注-推展標準流程	樣本數	3	5	2	32	7
		百分比	6.1	10.2	4.1	65.3	14.3
07	組織流程定義+IPPD-建立組織度量儲存庫	樣本數	2	5	3	28	11
		百分比	4.1	10.2	6.1	57.1	22.4
08	組織流程定義+IPPD-建立組織流程資產館	樣本數	2	5	5	26	11
		百分比	4.1	10.	10.2	53.1	22.4
09	供應商協議管理-執行供應商協議	樣本數	2	3	4	30	10
		百分比	4.1	6.1	8.2	61.2	20.4
10	專案監控-監控關鍵人員的參與	樣本數	8	4	6	23	8
		百分比	16.3	8.2	12.9	46.9	16.3
11	風險管理-建立風險管理策略	樣本數	6	5	3	28	7
		百分比	12.2	10.2	6.1	57.1	14.3
12	風險管理-執行風險降低計畫	樣本數	8	7	4	23	7
		百分比	16.3	14.3	8.5	46.9	14.3

題號	要求項目執行必要認知程度	非常不同意 ←→ 非常同意					
			1	2	3	4	5
13	風險管理-界定風險	樣本數	3	2	1	33	10
		百分比	6.1	4.1	2.0	67.3	20.4
14	風險管理-評估、分類及排序風險	樣本數	5	9	1	25	9
		百分比	10.2	18.4	2.0	51.0	18.4
15	組織流程定義+IPPD-建立標準流程	樣本數	4	10	4	21	10
		百分比	8.2	20.4	8.2	42.9	20.4
16	組織流程定義+IPPD-建立調適準則及指引	樣本數	7	3	7	21	11
		百分比	14.3	6.1	14.3	42.9	22.4
17	組織流程專注-建立組織流程需要	樣本數	4	10	2	22	11
		百分比	8.2	20.4	4.1	44.9	22.4
18	組織流程專注-推展標準流程	樣本數	5	5	5	26	8
		百分比	10.2	10.2	10.2	53.1	16.3
191	組織流程定義+IPPD-建立組織度量儲存庫	樣本數	2	6	5	27	9
		百分比	4.1	12.2	10.2	55.1	18.4
20	組織流程定義+IPPD-建立組織流程資產館	樣本數	2	4	10	21	12
		百分比	4.1	8.2	20.4	42.9	24.5
21	供應商協議管理-執行供應商協議	樣本數	7	7	6	24	5
		百分比	14.3	14.3	12.2	49.0	10.2
22	專案監控-監控關鍵人員的參與	樣本數	5	7	9	21	7
		百分比	10.2	14.3	18.4	42.9	14.3
23	風險管理-建立風險管理策略	樣本數	5	7	10	23	4
		百分比	10.2	14.3	20.4	46.9	8.2
24	風險管理-執行風險降低計畫	樣本數	7	6	4	20	12
		百分比	14.3	12.2	8.2	40.8	24.5

附錄 D　CMMI 能力成熟度相關流程領域執行程度平均數與標準差

Descriptive Statistics

	N	Mean	Std.	Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Std. Error
界定管理風險-執行程度	49	3.37	1.185	-.754	.668
決定處理順序-執行程度	49	3.53	1.174	-.509	.668
滿足組織目標-執行程度	49	3.63	1.055	.147	.668
資安調適準則-執行程度	49	3.49	1.043	.253	.668
界定營運目標-執行程度	49	3.76	1.071	.397	.668
維護流程記錄-執行程度	49	3.71	1.041	1.347	.668
實施訓練計畫-執行程度	49	3.84	1.028	1.207	.668
修訂標準流程-執行程度	49	3.80	1.040	.820	.668
審查維護廠商-執行程度	49	3.88	.949	2.401	.668
審查關鍵人員-執行程度	49	3.39	1.320	-.613	.668
管理投入範圍-執行程度	49	3.51	1.227	-.065	.668
建立時程績效-執行程度	49	3.29	1.339	-.962	.668
建構管理系統-執行程度	49	3.92	.975	3.559	.668
管理變更記錄-執行程度	49	3.49	1.277	-.665	.668
審查資安承諾-執行程度	49	3.47	1.260	-.836	.668
記錄矯正措施-執行程度	49	3.53	1.309	-.328	.668
審查管理記錄-執行程度	49	3.53	1.276	-.783	.668
蒐集資安事件-執行程度	49	3.55	1.191	.055	.668
管理任務技能-執行程度	49	3.71	1.041	.554	.668
保存訓練記錄-執行程度	49	3.76	1.051	.384	.668
績效量化目標-執行程度	49	3.27	1.255	-.771	.668
流程改善記錄-執行程度	49	3.37	1.202	-.545	.668
支援未來改善-執行程度	49	3.29	1.137	-.421	.668
法規遵循程度-執行程度	49	3.49	1.371	-.776	.668
Valid N (listwise)	49				

附錄E　ISO27001節次與CMMI流程領域對應統計表

ISO27001 要求事項	流程領域分類	流程領域	目標編號	各流程領域目標執行程度	各流程領域執行平均程度%
資訊安全組織-認知	流程管理	組織流程專注(一般目標)	SP1.1	5.界定營運目標-執行程度	75%
			SP3.2	6.維護流程記錄-執行程度	74%
資安事故管理-認知			SP3.4	20.保存訓練記錄-執行程度	75%
資安政策文件-認知		組織流程定義(一般目標)	SP1.1	3.滿足組織目標-執行程度	73%
			SP1.3	4.資安調適準則-執行程度	70%
資產管理-認知			SP1.4	7.實施訓練計畫-執行程度	77%
			SP1.5	8.修訂標準流程-執行程度	76%
系統獲取開發維護-認知		組織流績績效(一般目標)	SP1.4	18.蒐集資安事件-執行程度	71%
資安事故管理-認知			SP1.3	19.管理任務技能-執行程度	74%
遵循性-認知			GP5.1	23.支援未來改善-執行程度	66%
			GP2.9	24.法規遵循程度-執行程度	70%
持續營運管理-認知		組織創新與發展(一般目標)	SP1.4	21.績效量化目標-執行程度	65%
			SP2.3	22.流程改善記錄-執行程度	67%
存取控制-認知	專案管理	專案監控(一般目標)	SP1.4	15.審查資安承諾-執行程度	69%
			SP2.3	16.記錄矯正措施-執行程度	71%
系統獲取開發維護-認知			SP1.7	17.審查管理記錄-執行程度	71%
人力資源安全-認知		供應商協議管理(一般目標)	SP2.1	9.審查維護廠商-執行程度	78%
			SP1.5	10.審查關鍵人員-執行程度	68%
風險評鑑處理-認知		風險管理(一般目標)	SP2.1	1.界定管理風險-執行程度	67%
			SP2.2	2.決定處理順序-執行程度	71%
實體環境安全-認知			SP1.3	11.管理投入範圍-執行程度	70%
			SP3.2	12.建立時程績效-執行程度	66%
通訊作業管理-認知	支援	建構管理(一般目標)	SP1.2	13.建構管理系統-執行程度	78%
			SP3.1	14.管理變更記錄-執行程度	70%

附錄 F　問卷

親愛的填答者，您好：

在網際網路發達的今天，資安事件頻傳，不僅造成業界的難以計數的損失，政府單位也可能面臨資安事件的隱憂。這是一份有關資訊安全管理系統 ISO27001 與 CMMI 相關流程管理的問卷，希望了解並提供未來欲導入或已導入資訊安全管理系統的公務部門概況及改進之資料及依據，請資訊管理部門人員填寫後，利用函中所附之回郵信封寄回。本問卷共分三部份共 40 題，問卷內容純為學術研究之用，個別資料不公開，請您放心填寫，感謝您撥空惠填，叨擾之處，尚祈見諒。

國立台東大學　資訊管理研究所
指導教授　謝昆霖　教授
研究生　黃鎮屏　敬上

第一部份　貴單位資訊部門概況

1. 請問您目前的職務是?

□資訊安全長　□資訊部門主管　□基層主管　□管理師　□系統執行(開發)人員　□硬體設備操作(管理)人員　□其他（請填寫）_____

2. 請問貴單位對於 ISO27001 的導入情形?

□已經導入　□正在導入　□計畫導入　□無計劃導入

3. 請問您是否知悉 ISO27001 資訊安全管理系統要求事項?

□未曾接觸　□部份了解　□大部分了解　□完全了解

4. 請問您是否知道 CMMI 能力成熟度整合模式之流程管理?

□未曾接觸　□部份了解　□大部分了解　□完全了解

第二部份　就 ISO27001 建立組織的資訊安全安全管理作業，請依您的看法，以下各作業規範是否有執行的重要性。

題號	管理作業規範	規範事項說明
01	風險評鑑及處理	依組織目標選擇接受的風險，選定控制措施實做控管，確保風險降低至可接受程度
02	資訊安全政策文件	由管理階層核准，並傳達給所有員工與相關各外部團體
03	資訊安全的組織	在組織內宜建立管理框架以啟動與控制資安全的實作
04	資產管理	所有資產宜有人負責，以達成及維持組織資產的適切保護
05	人力資源安全	確保員工、承包商及第三方使用者瞭解其責任，宜簽署其安全角色與責任的協議
06	實體與環境安全	防止組織場所與資訊遭未經授權的實體存取、

		損害及干擾
07	通訊與作業管理	確保正確與安全地操作資訊處理設施
08	存取控制	依據營運與安全要求，控制資訊存取、資訊處理設施及營運過程
09	資訊系統獲取、開發及維護	識別並議定安全要求，確保安全是整體資訊系統的一部分
10	資訊安全事故管理	確保與資訊系統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播
11	營運持續管理	對抗營運活動中斷，保護重要營運過程不受系統失效或災害的影響，並確保及時再續
12	遵循性	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

	非常不同意	不同意	普通	同意	非常同意
01. 您覺得「風險評鑑及處理」有執行的必要?	□	□	□	□	□
02. 您覺得「資訊安全政策文件」有執行的必要?	□	□	□	□	□
03. 您覺得「資訊安全的組織」有執行的必要?	□	□	□	□	□
04. 您覺得「資產管理」有執行的必要?	□	□	□	□	□
05. 您覺得「人力資源安全」有執行的必要?	□	□	□	□	□
06. 您覺得「實體與環境安全」有執行的必要?	□	□	□	□	□
07. 您覺得「通訊與作業管理」有執行的必要?	□	□	□	□	□
08. 您覺得「存取控制」有執行的必要?	□	□	□	□	□
09. 您覺得「資訊系統獲取、開發及維護」有執行的必要?	□	□	□	□	□
10. 您覺得「資訊安全事故管理」有執行的必要?	□	□	□	□	□
11. 您覺得「營運持續管理」有執行的必要?	□	□	□	□	□
12. 您覺得「遵循性」有執行的必要?	□	□	□	□	□

第三部分　採用 CMMI-SE/SW/IPPD/SS 連續式表述模式－相關流程領域部份一般(特定)目標，請依您的看法，就各目標流程實際執行程度的重要性。

非常不同意	不同意	普通	同意	非常同意	
□	□	□	□	□	01. 分析組織內外部資訊來源以界定資訊安全管理風險。
□	□	□	□	□	02. 定義風險的種類及參數，評估並決定其相對優先處理順序。
□	□	□	□	□	03. 建立並維護資訊安全流程，滿足組織的目標與需要。
□	□	□	□	□	04. 建立並維護組織資訊安全調適準則及指引。
□	□	□	□	□	05. 界定組織政策及營運目標的資訊安全管理政策。
□	□	□	□	□	06. 執行維護組織資訊安全管理流程的執行記錄。
□	□	□	□	□	07. 建立組織資訊安全訓練的實施計劃。
□	□	□	□	□	08. 定期審查與修訂組織資訊安全標準流程。
□	□	□	□	□	09. 監督並審查維護廠商，遵循契約進行所承諾的事項。
□	□	□	□	□	10. 定期審查與記錄資訊安全管理關鍵人員參與專案的情形。
□	□	□	□	□	11. 界定風險管理投入的範圍並採取行動，包括可能性、結果及門檻。
□	□	□	□	□	12. 針對資訊安全風險處理活動，建立時程或某段期間的績效(包括起始日期和完成日期）。
□	□	□	□	□	13. 建構並維護管理系統，此管理系統包含儲存媒體、運作程序及存取管理系統的工具。
□	□	□	□	□	14. 建構並維護管理系統項目的修訂與變更記錄之完整性。
□	□	□	□	□	15. 定期審查及記錄組織資訊安全相關承諾事項。
□	□	□	□	□	16. 監控並記錄資訊安全管理矯正措施結果直到完成。
□	□	□	□	□	17. 審查資訊安全管理記錄及其影響。
□	□	□	□	□	18. 蒐集資安事件資料及分析結果，建立並維護組織資訊流程安全基準。
□	□	□	□	□	19. 實施組織資訊安全管理任務所必要的知識與技能。
□	□	□	□	□	20. 保存組織資訊安全相關訓練課程或活動的記錄。

非常不同意	不同意	普通	同意	非常同意	
□	□	□	□	□	21. 設定並維護組織資訊安全品質及管理績效的量化目標。
□	□	□	□	□	22. 彙整組織資訊安全管理流程改善活動的記錄。
□	□	□	□	□	23. 蒐集並度量資訊安全管理系統的結果，以支援組織的未來使用與改善。
□	□	□	□	□	24. 定期檢視法規，評估組織流程遵循程度，並決解不符合情況。

NTU Library