國立交通大學

管理學院碩士在職專班經營管理組

碩 士 論 文

探討企業同時導入 ISO 系列(ISO 9001、ISO 27001、ISO 20000)與 CMMI 之比較分析與管理─
以台灣資訊服務業為例

A Study on the Concurrent Deployment of both ISO Series and CMMI into the Enterprises-
Practices of Information Service Industry in Taiwan

研 究 生：馬秀莉

指導教授：楊　千 教授

中 華 民 國　九十九　年 六 月

探討企業同時導入 ISO 系列(ISO 9001、ISO 27001、ISO 20000)與 CMMI 之比較分析與管理─以台灣資訊服務業為例

A Study on the Concurrent Deployment of both ISO Series and CMMI into the Enterprises-Practices of Information Service Industry in Taiwan

研 究 生：馬秀莉　　Student：Hsiu-Li Ma

指導教授：楊　千　　Advisor：Chyan Yang

國 立 交 通 大 學

管理學院碩士在職專班經營管理組

碩 士 論 文

A Thesis

Submitted to The Master Program of Business and Management

College of Management

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

of

Business Administration

June 2010

Taipei, Taiwan, Republic of China

探討企業同時導入 ISO 系列(ISO 9001、ISO 27001、ISO 20000)與 CMMI 之比較分析與管理—以台灣資訊服務業為例

研究生：馬秀莉　　指導教授：楊 千

國立交通大學管理學院碩士在職專班經營管理組

中文摘要

優良品質是企業保持競爭優勢的利器，一般企業多將核心業務的管理程序化，並依據 ISO 等國際標準組織所頒佈之標準加以訂定，期透過系統化方法，提昇產品/服務品質，並發揮整體效能。

本研究以臺灣資訊服務業為例，探討企業同時具有四類國際標準：ISO 9001(品質管理)、ISO 27001(資訊安全管理)、ISO 20000(資訊服務管理)以及 CMMI(能力成熟度整合模式)，各標準之間重覆、互補、互稽、引用、申論的各種關係。提供下列三項目研究結果，希望對企業在導入多項國際標準時有所助益。

1. 比較分析 4 類國際標準之異同

   運用系統方法(Systematic Approach)、啟發性規劃(Heuristic Programming)及黑盒子(Black Box)觀念，比較分析 ISO 9001、ISO 27001、ISO 20000、CMMI 等 4 類國際標準之異同。

2. 探討經營困難

   例如：多項國際標準對組織文化之衝擊以及員工感受等。

3. 提出管理對策及解決方案

   以 David Brewer〔10〕之管理系統整體架構，尋求管理對策及解決方案。

關鍵字：品質、ISO 9001、ISO 27001、ISO 20000、CMMI

A Study on the Concurrent Deployment of both ISO Series and CMMI into the Enterprises-Practices of Information Service Industry in Taiwan

Student：Hsiu-Li Ma Advisor：Chyan Yang

The Master Program of Business and Management
College of Management
National Chiao Tung University

ABSTRACT

Providing excellent product quality is the way for Enterprises to maintain competitive advantages. Generally, enterprises put processes to manage their core business, set standards by using International Standards such as ISO, and utilize systematic approaches to raise product quality and overall performance.

This research study investigates the concurrent deployment of four international standards which are used most often by professionals of the Information Service Industry in Taiwan; namely, ISO 9001 for quality management systems, ISO 27001 for information security management systems, ISO 20000 for information technology service management, and CMMI for process improvement in software engineering. Issues identified are: duplication in concurrent deployment, complementary coverage, mutually auditing, and cross referencing. The study presents three results which would add value to enterprises.

(1) Compares and analyzes the above four international standards by using three techniques: systematic approaches, heuristic programming, and the black-box concept.
(2) Identifies difficulties and issues arising from concurrent deployment. For example, deployment of multiple international standards has impact upon the organizational culture and employees.
(3) Proposes solutions to address these issues. David Brewer's framework is used to find these solutions.

Keywords: Quality、ISO 9001、ISO 27001、ISO 20000、CMMI.

誌 謝

終於完成研究所學程，即將離開學校，內心真有許多不捨。在學習過程中充滿快樂、豐富及成長，許多美好故事與回憶在台北三級古績-交通大學博愛校區裡發生，一幕又一幕讓人珍惜與感念。

謝謝學校給我讀書的機會，更謝謝於研究所期間指導教授楊千老師與鄭祥勝大哥之指導，無論是研究工作的專業知識或是待人處事，均對我有很大影響，他們是我生命中的導師，開啟我人生智慧，在此，致上我最誠懇的謝忱與敬意。同時，亦感謝林君信老師、黃宏仁老師、劉顯東老師、傅振華老師以及君華學姐，提供珍貴意見及改進方向，使論文內容更為完善。

我也要謝謝公司的栽培，柯先生、許副執行長、黃專家、李資顧、企劃室文玲主任及同仁們。未來，更要以主動積極的做事態度，將交通大學所學應用於工作，報答公司的培育。

研究過程中，感謝家人與好友們照顧與鼓勵，咪姐、大姐、啟銘、芬姐、梅子、幼英姐姐、辜國隆博士、陳皆成博士、熊伯伯、常伯伯、統英、大哥、美華、淑娟、修珮、Joanne、Louis、高惠堂顧問、長峯、青恩、佩廷以及陪著熬夜啃土司的蔡小熊。因為有您們，使我的學習過程中充滿關懷與温暖，感謝您們的一路相伴。

謹將這份成果獻給我最敬愛的爸爸與媽媽。由於您們開明的教育，包容自小不愛唸書的我，從排斥學習，到慢慢體會學習重要，並瞭解終身學習是投資自己最好的方法。

做你能做的事，做你喜歡做的事，做你值得做的事，交通大學是我一生最正確的選擇，秀莉珍惜這段學習過程，並願與大家分享收穫的喜悅。

秀莉 謹誌於交通大學

中華民國九十九年六月

目 錄

表目錄

圖目錄

一、 緒論

1.1 研究背景與動機

郭台銘說：鴻海能夠快速全球運作，主要就是靠四大管制系統：工程管理（工管）、品質管理（品管）、生產管理（生管），以及經營管理（經管）的力量，可見品質管理在企業經營的重要性。

「重視品質」是企業永續經營重要原因之一。品質管理方法很多，如：六標準差、JIT(Just in Time)、TQM(Total Quality Management)、精實生產(Lean Production)以及各類國際標準(International Standers)等。

多數企業多以國際標準作為提昇品質的工具，主要有以下考量：

(1) 外部需求：

a.專業能力及品質的最佳證明。

b.因應世界趨勢與潮流，提高競爭力。

c.配合客戶要求。

d.擴展國際化市場。

(2) 內部需求：

a.建立內部經營管理制度，以使產品/服務具備優良品質，滿足客戶需求與期望。

b.整合內部資源，塑造高品質組織經營文化

c.將個人的技術轉變為企業的知識，使得新人能夠盡速上手，縮短人才培訓時間

d.讓生產製造流程中知所有產品都能達到一樣的品質與服務水準，健全管理系統。

跟隨資訊工業發展脈動，目前與資訊服務業有關的國際標準愈來愈多，包括 ISO 9001、ISO 27001、ISO 20000、CMMI 等項目。國內已有資策會、中華電信、宏瞻公司等單位同時導入以上 4 項標準。未來，企業針對不同核心業務，分別導入適合領域之國際標準，為不可避免趨勢。

每項國際標準，均有特定之領域與用途，如 ISO 9001 用於各行各業。ISO 27001 應用於資訊安全管理，適用於高資訊安全之行業(如金融業、雲端運算中心)。ISO 20000 為只要使用資訊系統之行業都適用。以及應用於大型系統開發業者及軟體代工的 CMMI，另 CMMI 嚴格的規範，將有效協助軟體業者達到管理「時間」、「品質」及「成本」等三項重要指標。資訊服務業領域各國際標準整理如表 1。

表 1：資訊服務業領域應用較為廣泛之國際標準

發行組織	國際標準	頒布日期	應用領域
ISO	ISO 9001	1987 年	品質管理，適用於各行各業，例如：製造業、運輸物流業
	ISO 27001	2000 年	資訊安全管理，適用於高資訊安全的行業，例如：金融業
	ISO 20000	2005 年	資訊服務管理，適用於各行各業資訊化業務，例如：企業之資訊中心，金融業、保險業
SEI	CMMI	1991 年	軟體工程管理，適用於大型系統開發業者及軟體代工，例如：資訊服務業、資訊委外

參考資料來源：本研究整理

表 1 所介紹之國際標準，除 ISO 9001 頒布時間較早外，餘均為近期發行，並在政府推動下，方漸為國內所接受。ISO 27001、ISO 20000、CMMI 之規範均非常嚴謹且條文要求複雜，如未做適當整理，將造成多頭馬車、管理規範太多、工作重覆增加同仁工作量等問題。

有鑑於此，本研究以在品質工作領域實務工作經驗，參考國內外相關文獻及專家意見，整理以上 4 標準異同，提出經營問題與管理對策，期與有相同需求之企業分享研究心得。

1.2 研究目的

本論文為資訊服務業導入國際標準理論及實務經驗之研究，可做為企業導入單一國際標準或一項以上國際標準之參考，研究目的為：

(1) 比較 ISO 9001、ISO 27001、ISO 20000 及 CMMI 標準之異同。

(2) 探討企業在導入 ISO 9001、ISO 27001、ISO 20000 及 CMMI 後之困難。

(3) 提出企業導入 ISO 9001、ISO 27001、ISO 20000 及 CMMI 後的管理策略。

1.3 研究步驟

根據前述之研究動機，本研究首要釐清問題及界定範圍，以避免方向錯誤。藉由分析ISO 9001、ISO 27001、ISO 20000及CMMI條文，整理其間差異。再依此，就所發現之問題研擬管理策略。研究步驟如圖1所示：

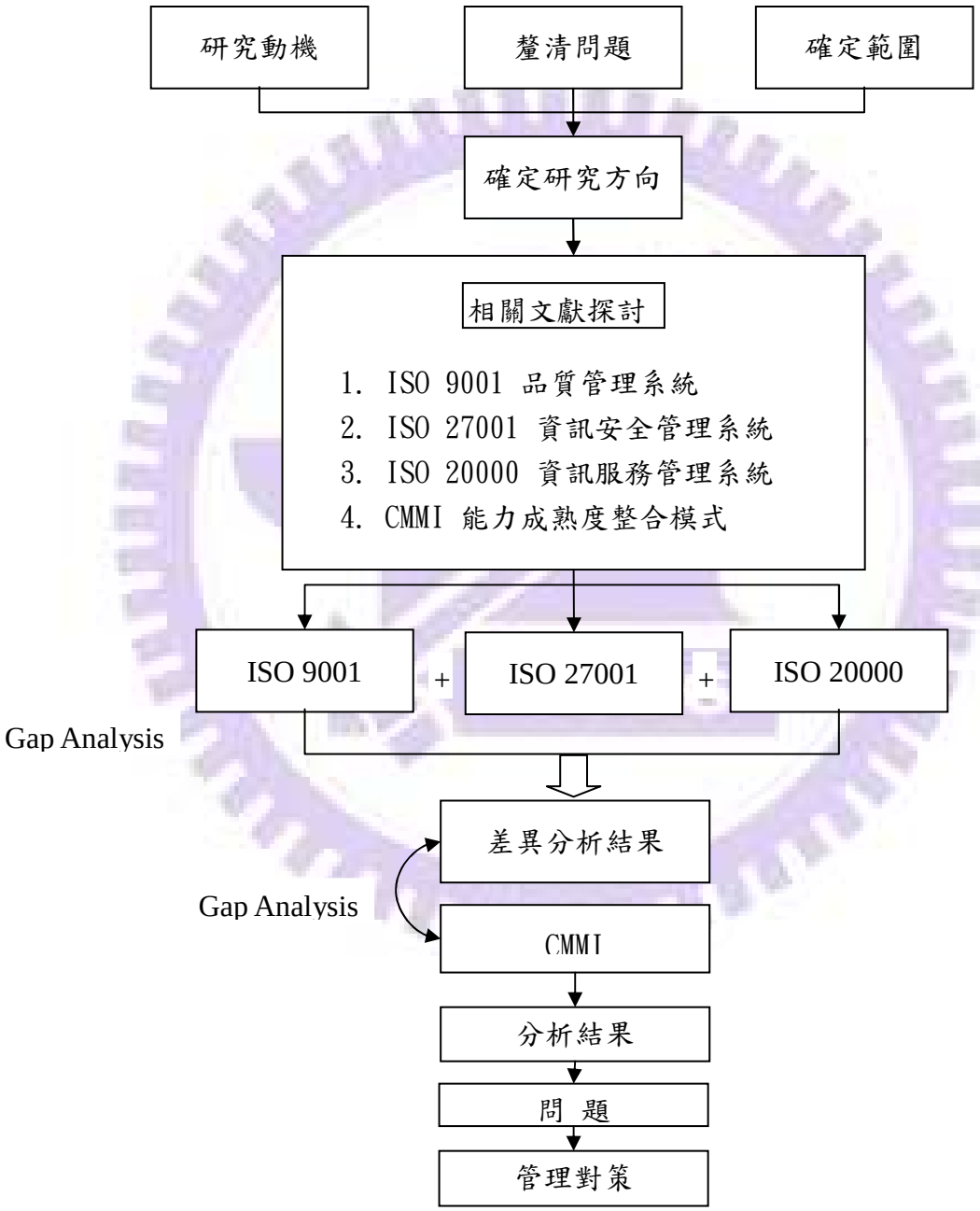

圖 1：研究步驟

資料來源：本研究整理

二、文獻探討

2.1 品質基本概念

品質管理系統是提昇產品/服務「品質」的方法，由高階管理階層，透過團隊合作方式，運用既有資源，建立一套「維持企業運作流暢，符合顧客滿意、法規需求及管理系統要求」的管理架構，隨著時間運作，累積企業專業、技術、資源...等，追求卓越，提升競爭力，達到客戶滿意。

表 2：品質的定義

學者	定義
ISO 9000:2008	一組固有的特性達成要求之程度
Dr. W. A. Shewhart	轉換顧客未來的需求成為可以衡量的品質特性，在顧客願意支付的價格下給予滿意
Dr. W. E. Deming	品質應為顧客現在和未來需求。
Dr. J. M. Juran	品質就是適用。品質功能在於達成適用的各項活動的集合體，而不論其活動發生於那裡。
Dr.A.V. Feigenbaum	品質係產品在市場、工程、製造及維護上的綜合特性，透過其使用可以滿足顧客需求和期望。
Dr. K. Ishikawa	產品品質係工程和製造的綜合特性，這些特性於產品使用時，將滿足顧客期望程度。
Dr. G. Taguchi	品質是產品出廠後帶給社會的損失。
P. B. Crosby	品質即是合乎標準或規格

品質概念發展歷程由早期品質管制 (QC，ISO 9002)至品質保證管理(QM，ISO 9001)到全面品質服務(Total Quality Service,TQS)，觀念演進如下：

表 3：品質觀念演進

年代	階段		觀念
1900 年以前	1	操作員的品質管制 (operator quality control)	品質是檢驗出來的
1920 年代	2	領班的品質管制 (foreman quality control)	
	3	檢驗員的品質管制 (Inspection Quality Control)	
1940 年代	4	統計品質管制 (Statistical Quality Control，SQC)	品質是製造出來的 品質是設計出來的
1960 年代	5	全面品質管制 (Total Quality Control，TQC)	品質是管理出來的
1980 年代	6	全面品質管理 (Total Quality Management，TQM)	品質是習慣出來的
2000 年以後	7	全面品質服務 (Total Quality Service，TQS)	品質是服務出來的

參考資料來源：本研究整理

品質概念發展歷程由早期品質管制(QC，ISO 9002)至品質保證(QM，ISO 9001)到全面品質管理(TQM)，發展歷程如下：

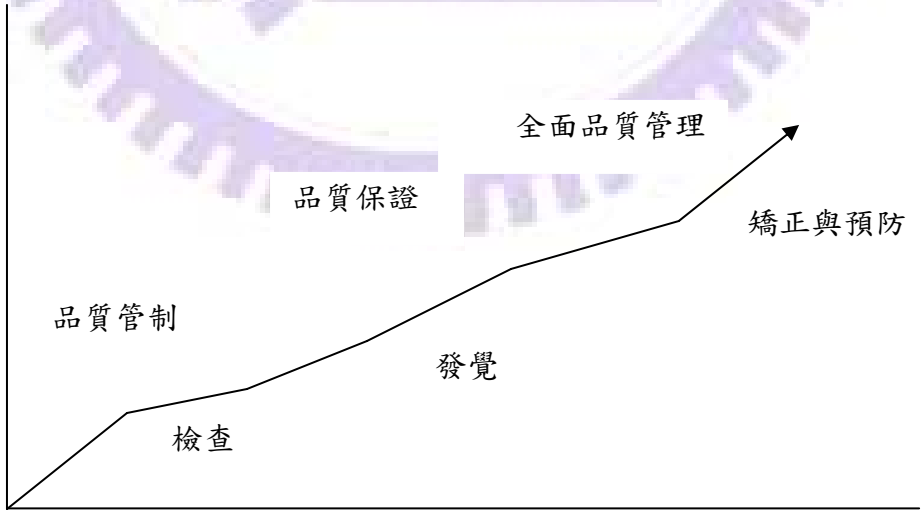

圖 2：品質發展歷程

參考資料來源：本研究整理

2.2 ISO國際標準組織

ISO 是國際標準組織（International Organization for Standardization）簡稱，於 1947 年 2 月於瑞士日內瓦正式成立。自 1951 年發佈第一個標準-工業長度測量用標準參考溫度後，至今已完成 17,500 項國際標準，每年並有 1,100 個新標準被公告，其發展的各類標準，為全球企業廣泛採用。

企業因某些業務需要(例如：申請標案、獲得客戶信任等)，在完成管理系統建置後，會向 ISO 組織提出申請，不過因 ISO 使用客戶廣大，通常會委託當地檢驗公司(如國內較有名 SGS、Bsi、DNV)為企業進行外部稽核，通過檢驗公司的外部稽核，我們稱為通過認證(Certification)，再由檢驗公司向 ISO 提出申請，由 ISO 組織頒發證書，稱為通過驗證(Verification)，通過驗證即代表該企業符合國際標準要求，產品/服務之品質有一定保證。

ISO 系列證書有效期為 3 年，每年固定由檢驗公司做外部稽核，每 3 年為一個循環，將納入 ISO 業務的工作全部檢核一次。通常，外部稽核前，企業內部會先做一次內部稽核，如果一個企業同時有 ISO 9001、ISO 27001、ISO 20000，一年分別有 6 次內外部稽核，相當耗費人力，且不易看出管理整體問題。

2.3 ISO 9001 品質管理系統

ISO 9000 系列品質管理系統之標準由 ISO/TC176 品質管理與品質保證技術委員會編訂，1987 年陸續公告 ISO 9001、ISO 9002、ISO 9003、ISO 9004。1994 年整合 ISO 9001、ISO 9002、ISO 9003 等 3 項驗證標準為 ISO 9001，成為唯一可以做為申請驗證的標準。ISO 9001 業歷經 2 次改版，ISO 國際標準組織於 2008 年 11 月正式發行第 3 版 ISO 9001:2008。

表 4：ISO 9000 系列

名稱	用途
ISO 9000:2005	品質管理系統—概念與辭彙
ISO 9001:2008	品質管理系統—系統要求(申請驗證的標準)
ISO 9004:2000	品質管理系統—績效改善指導綱要
ISO 19011:2002	品質及環境稽核指導綱要

參考資料來源：ISO 9001：2008 Standard

ISO 9000 系列早期於 1950 年代為美國軍方品質計畫需求標準，之後經歷 28 年漫長歲月測試，於 1987 年發展成熟並通過 ISO 國際標準組織審查，成為國際標準。由此可見，國際標準頒布均經嚴格之淬練及審查，故能獲得各企業信任與採用。

表 5：ISO 9000 系列發展紀要

年代	紀要
1959年	美國軍方品質計畫需求標準 (MIL-Q-9858A)
1965年	歐洲北大西洋公約企業轉訂為 AQAP (Applied quality assurance publication)
1979年	英國參照 AQAP，發展出一套適用於企業界的國家標準為 BS-5750
1980年	國際標準化企業 (International organization for standardization 簡稱 ISO)之 TC176 技術委員會開始草擬
1987年	ISO 9000系列正式頒布施行
2000年	ISO 9000系列第二次改版
2008年	ISO 9000系列第三次改版

參考資料來源：楊錦洲，流程管理與 ISO 簡報

由於 ISO 9000 規範了一個完整的品質作業，因此其後發展的 ISO 14001(環境管理系統標準)、ISO 27001(資訊安全管理系統)以及 ISO 20000 資訊服務管理系統，都以 ISO 9000 為基礎來架構，因此 ISO 9000 也就成為了國際上公認的品質系統基石。

ISO 9001 品質管理系統標準，使用範圍非常廣泛，適用於任何行業，包括政府機關及一般公、民營企業，依據 ISO 國際標準組織公佈目前近 80 個企業 160 餘國家通過 ISO 9001 驗證。其規範的作業範圍：從客戶需求瞭解確認、專案計畫/服務/產品的設計展開與管制、採購、外包與驗收到最終的交貨/結案、顧客服務都涵蓋在內。可作為高階主管指導企業提昇之的架構，其重點包括如下：

(1) 品質管理八大原則

原則一：顧客為重(Customer Focus)

原則二：領導統禦(Leadership)

原則三：人人參與(Involvement of People)

原則四：流程導向(Process Approach)

原則五：系統化管理(System Approach to Management)

原則六：持續改善(Continual Improvement)

原則七：依據事實決策(Factual approach to decision making)

原則八：與供應商的互利關係(Mutually beneficial supplier relationships)

(2) 顧客滿意

(3) 流程導向

(4) PDCA 循環

(5) 持續改善

(6) 資料分析

ISO 9001 條文內容包括：一般要求、管理責任、資源管理、產品實現、量測分析等五大項(條文內容詳如圖 3)。企業需依據外在環境(如政治、氣候、地形)、當地文化、法律規章及內部需要，量身訂做適合於自己企業之品質管理系統。

由於 ISO 9001 發展較早且成熟度高，如運輸物流業之首都客運、醫療業之萬芳醫院、資訊服務業之資訊工業策進會、政府機關、大學以及許多中小企業，均已獲得 ISO 9001 驗證。通過 ISO 9001 驗證並不等於品質優良的保證。企業需以持續改善的精神，方能發揮其功能。

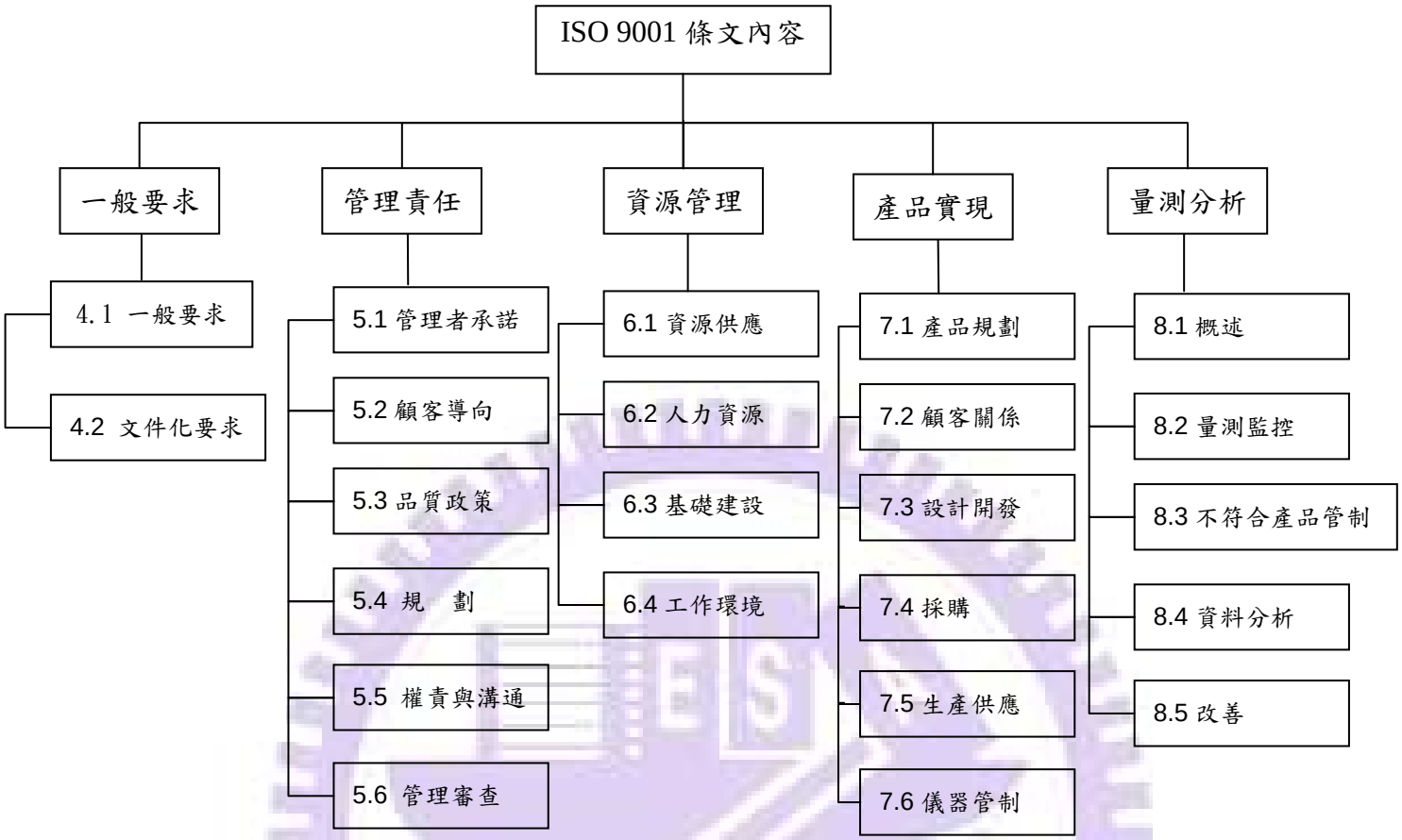

圖 3：ISO 9001:2008 條文內容

參考資料來源：ISO 9001:2008 Standard，本研究整理

2.4 ISO 27001 資訊安全管理系統

2.4.1 基本介紹

ISO 27000 系列主要為提供組織建置資訊安全管理系統(ISMS，Information Security Management System)制定之標準，最早稱為 BS 7799 由英國標準協會(BSI，British Standards Institute)所制定，分為二大部份：

第一部份：ISO 27001：前身為 BS 7799，為驗證標準。

第二部份：ISO 27002：前身為 BS 17799，為導入參考文件。

企業導入資訊安全管理系統除需參考 ISO 27001 及 ISO 27002 外，尚有 ISO 27003~ ISO 27006，使用功能如列表 6：

表 6：ISO 27000 系列相關標準

標準	內容
ISO 27000	principles and vocabulary (in development)
ISO 27001	ISMS requirements (BS7799)
ISO 27002	ISO/ IEC 17799:2005 (BS17799)
ISO 27003	ISMS Implementation guidelines (due 2007)
ISO 27004	ISMS Metrics and measurement (due 2007)
ISO 27005	ISMS Risk Management
ISO 27006	27010 – allocation for future use

參考資料來源：本研究整理

ISO 27000 自 1989 年雛型至 2000 年正式頒佈為 ISO 國際標準，僅短短 11 年，這段時期也正是全世界開始重視「資訊安全」議題。我國也在政府大力推動下於 2002 年，將 ISO 27000 標準中文化，命名為 CNS17800。

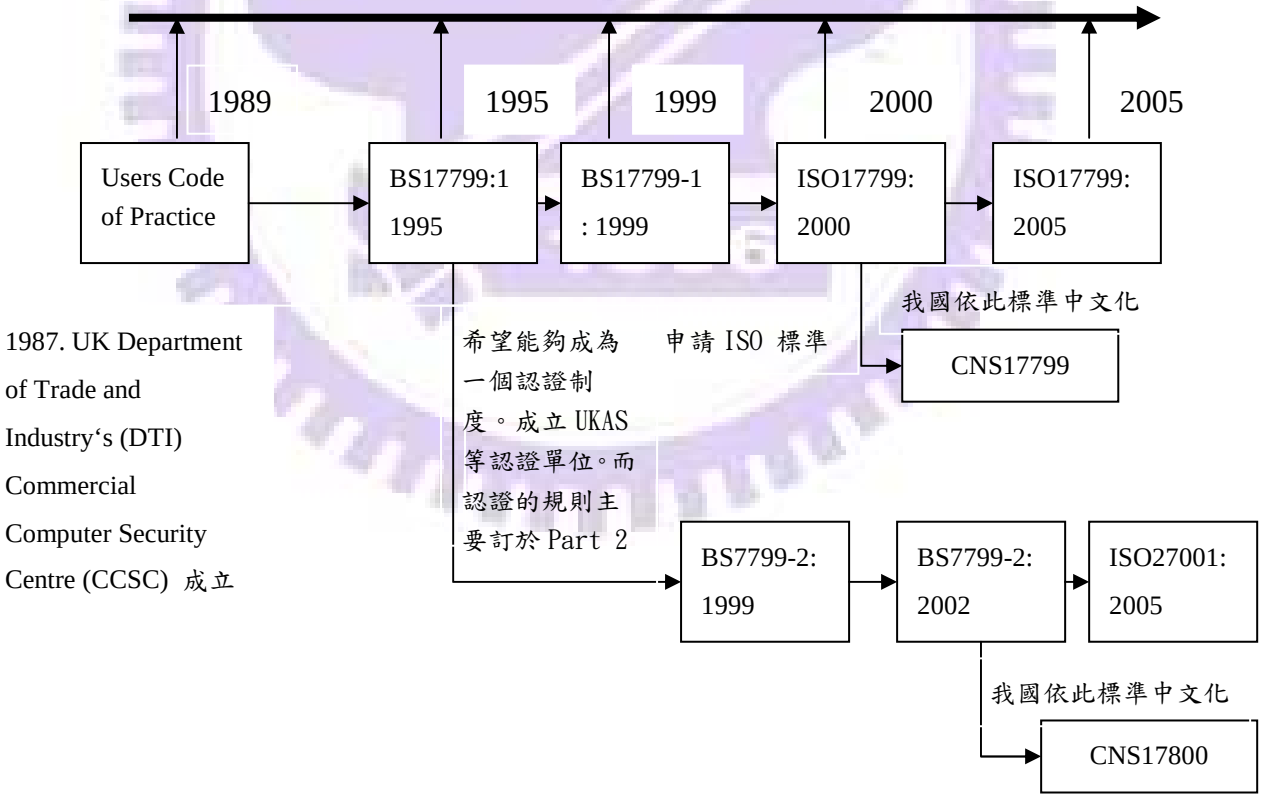

圖 4：ISO 27000 發展歷程

資料來源：查士朝 ISO17799/ISO27001 資訊安全管理制度介紹與導入實務

(1) 資訊資產

針對資訊安全管理建立的管理系統，為組織管理系統的一部份。資訊(Information)在資訊安全領域，被視為一項資產，如同組織營運資料一樣的重要，需要加以妥善的保護，以避免因意外造成資訊的損害，影響組織的正常運作，在資訊安全領域定義的資產，概分為以下類別：

表 7：資訊資產類別

項次	類別	內容
一	資訊資產	資料庫、資料檔案、系統文件、用戶手冊、訓練教材、備援計畫、各類法規及辦法等
二	軟體資產	應用程式、系統軟體、開發工具及工具程式等
三	實體資產	電腦設備、通訊設備、媒體、辦公設備、機房等
四	輕資產	人、公司聲譽、專利、智財權等

參考資料來源：ISO 27002 本研究整理

(2) 資訊安全的特性

資訊安全係要確保資訊資產符合；機密性（Confidentiality）、完整性（Integrity）、可用性（Availability），一般簡稱為 CIA，其特性如下：

a.機密性（Confidentiality）：只有經過授權的人，才能存取資訊。

b.完整性（Integrity）：保證資訊及其處理方法的正確與完整，例如：資料備份。

c.可用性（Availability）：確保經過授權的使用者，可以存取資訊並使用相關資訊資產。

(3) 脆弱點與威脅

就資訊資產來說，本身即有脆弱點(Vulnerabilities)，並且會面臨到外在的威脅(Threat) ，當威脅利用到這些脆弱點時，就會發生資安事件，而造成衝擊(Impact)。例如：納莉颱風造成台北市大淹水，捷運系統機房設在地下室(脆弱點)，納莉颱風的雨災(威脅)，其機房設備嚴重損害，捷運無法正常運作，造成社會大眾的不方便。

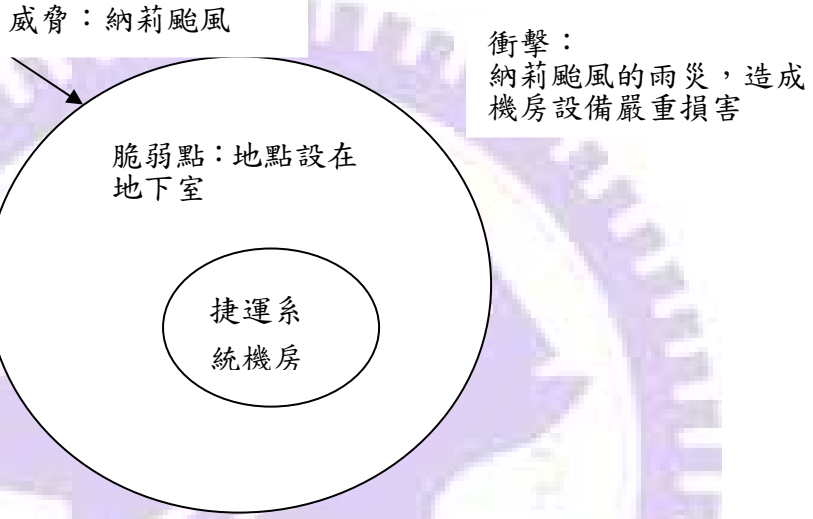

圖 5：脆弱點與威脅

參考資料來源：查士朝 ISO17799/ISO27001 資訊安全管理制度介紹與導入實務

(4) 風險評鑑與管理

為避免資訊資產的保護太過與不及，並把資源用在需要保護的資訊資產上，資訊安全管理系統會先對資訊資產做風險評鑑，風險評鑑結果可採用以下的方式處理： a.接受風險：當風險發生時，其損害程度是組織可接受，所以接受它。b.轉嫁風險：例如投保保險。c.控制風險：建立資訊安全管控措施，使重要的資訊資產有完善的管理與保護。一般組織以 ISO 27000 系列之規範，管理資訊，確保安全，並依 ISO 27001 條文規定，建立組織內之資訊安全管理體系，並申請國際驗證。

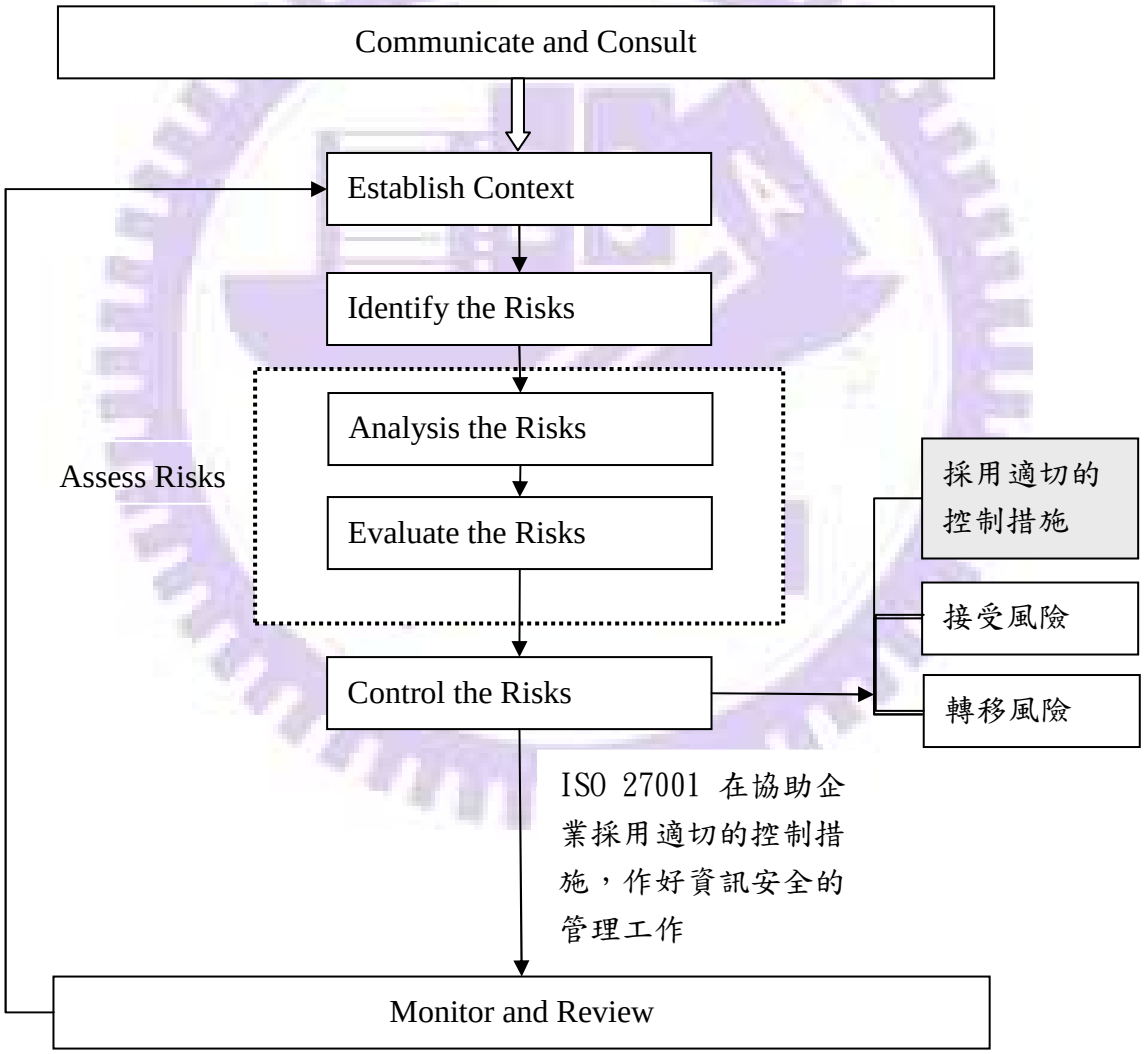

圖 6：風險評鑑與管理流程

參考資料來源：ISO 27001:2005 Standard 本研究整理

(5) ISO 27001 標準介紹

ISO 27001 係以風險的角度建立企業資訊安全管理系統(ISMS，Information Security Management System)，計有安全政策、安全組織、資產管理、人力資源、實體環境、通訊與作業、存取控制、系統開發、安全事件管理、業務永續、符合性等 11 個領域，39 項控制目標，133 項資訊安全管控措施。

ISO 27001 以 PDCA(Plan、Do、Check、Act)管理循環觀念設計，為組織申請驗證的標準。內容包括：

a.建立 ISMS（規劃）

b.實作與運作 ISMS（執行）

c.監視與審查 ISMS（檢查）

d.維持與改進 ISMS（行動）

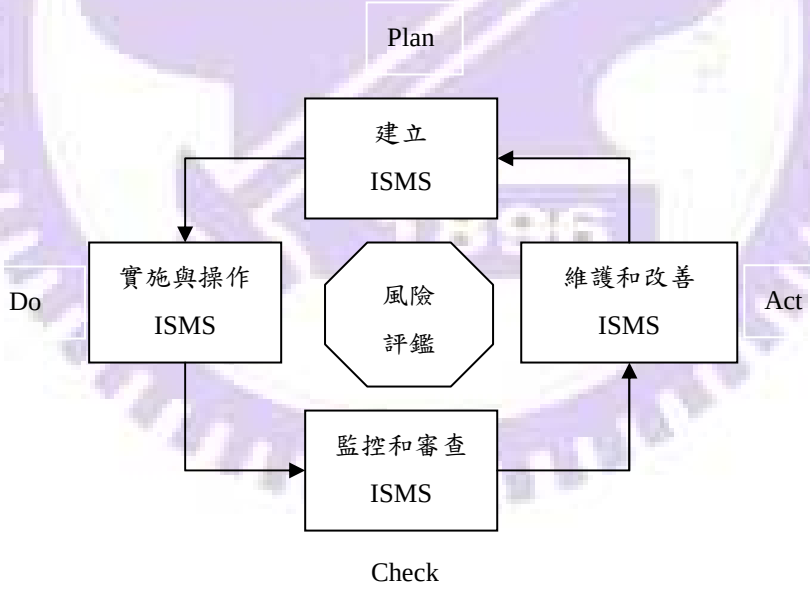

圖 7：應用於 ISMS 過程的 PDCA 模式

參考資料來源：ISO 27001:2005 Standard

表8： ISO 27001之控制措施

項次	領域	控制目標
一	安全政策	1. 資訊安全政策
二	資訊安全組織	2. 內部組織 3. 外部團體
三	資產分類與控制	4. 資產責任 5. 資訊分類
四	人力資源	6. 聘僱之前 7. 聘僱期間 8. 聘僱的終止或變更
五	實體環境安全	9. 安全區域 10. 設備安全
六	通訊與作業	11. 作業之程式與責任 12. 第三方服務交付管理 13. 系統規劃與驗收 14. 防範惡意碼與行動碼備份 15. 網路安全管理 16. 媒體的處置 17. 資訊交換 18. 電子商務服務 19. 監視
七	存取控制	20. 存取控制的營運要求 21. 使用者存取管理 22. 使用者責任 23. 網路存取控制 24. 作業系統存取控制 25. 應用系統與資訊存取控制 26. 行動計算與遠距工作
八	系統開發	27. 資訊系統的安全要求 28. 應用系統的正確處理 29. 密碼控制措施 30. 系統檔案的安全 31. 開發與支援過程的安全 32. 技術脆弱性管理
九	安全事件管理	33. 通報資訊事件與弱點 34. 資訊安全事故與改進的管理
十	業務永續	35. 營運持續管理的資訊安全
十一	符合性	36. 遵循適法性要求 37. 安全政策與標準的遵循性 38. 技術遵循性 39. 資訊系統稽核考量

參考資料來源：ISO 27001 Standard 本研究整理

2.5 ISO 20000 資訊技術服務管理系統

由於資訊技術的普及應用，相對而言，資訊安全與資訊技術的管理就更顯重要。ISO 組織於 2005 年公佈 ISO 20000，是一套適用於組織建立「資訊技術服務管理系統」(Information Technology Service Management System)的國際標準，任何運用資訊技術提升產品/服務的行業均可適用。

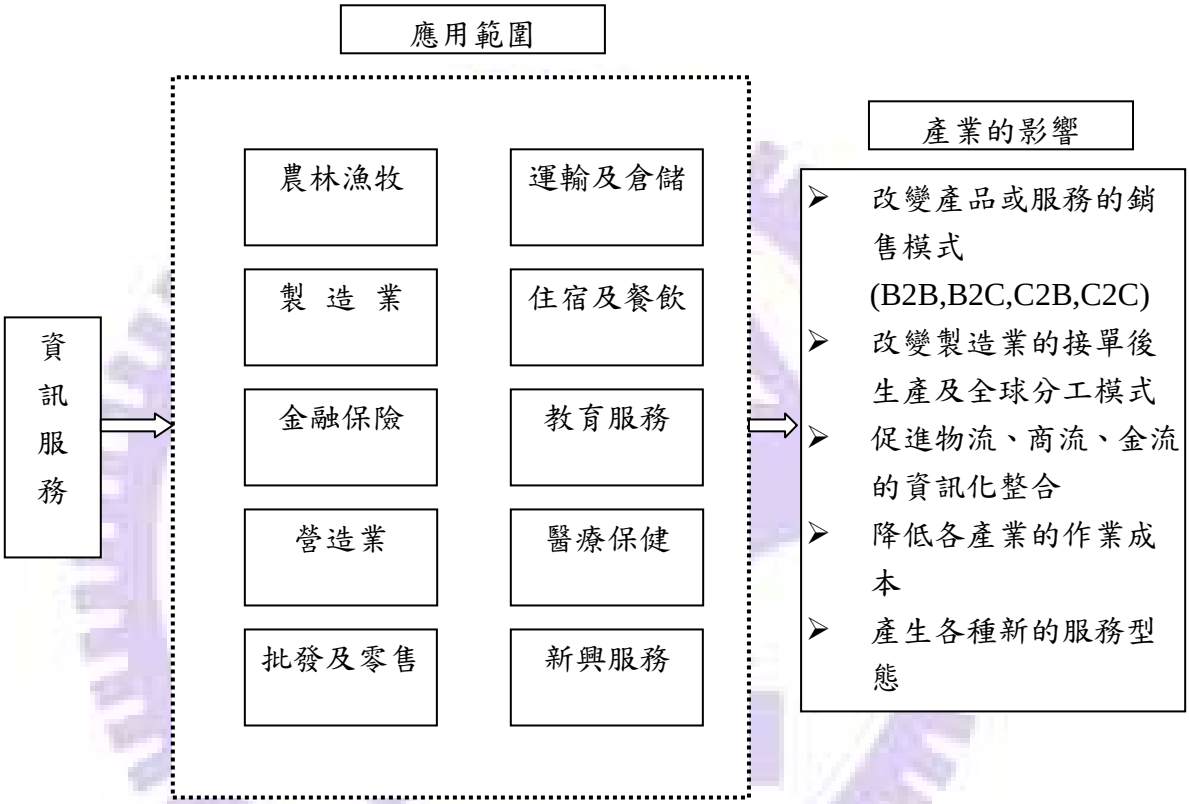

圖 8：資訊服務應用範圍及對產業的影響

資料來源：經濟部工業局資訊服務業發展計畫提案說明會

ISO 20000 主要包含二大部份，其中 ISO20000-1 為認證的標準。

(1)ISO20000-1：2005，服務管理規範，是建立、實施以及推行認證的標準。

(2)ISO20000-2：2005，服務管理最佳實務指南，提供整套的管理方法。

ISO 20000 的基礎來自於 ITIL(Information Technology Infrastructure Library)，但不同於 ITIL 的精緻化管理，它注重 IT 服務管理品質，以 IT 運維管理業務為核心，注重流程導向與 PDCA 管理模式。目前，IT 服務管理正處於起步階段，全球通過 IS020000 的驗證家數並不多。

表 9：2010 年全球通過 ISO 20000 認證家數

排名	國家	通過 ISO 20000 驗證家數
1	日本	48
2	英國	46
3	印度	38
4	南韓	35
5	中國	31
6	德國	17
7	台灣	17
8	美國	12
9	瑞士	11
10	香港	7

參考資料來源：itSMF 網站/2010 年 1 月

ISO 20000 遵循 PDCA 管理模式，以營運目標、客戶要求、資訊安全、新增/變更服務及其他業者/供應商為考量要素，藉由服務台(Helpdesk)的方式(問題分類→事件分析→事件處理→事件追蹤)執行資訊事件的管理。ISO 20000 分為：服務交付過程、關係過程、解決過程、控制過程及發行過程等 5 大領域，及 13 個子流程，每個流程都需有 KPI 以數字展現資訊服務績效。另外亦考慮到系統容量、新增系統與改變(Change)時所需的服務管理等以及財務預算、軟體管制及配送等問題。

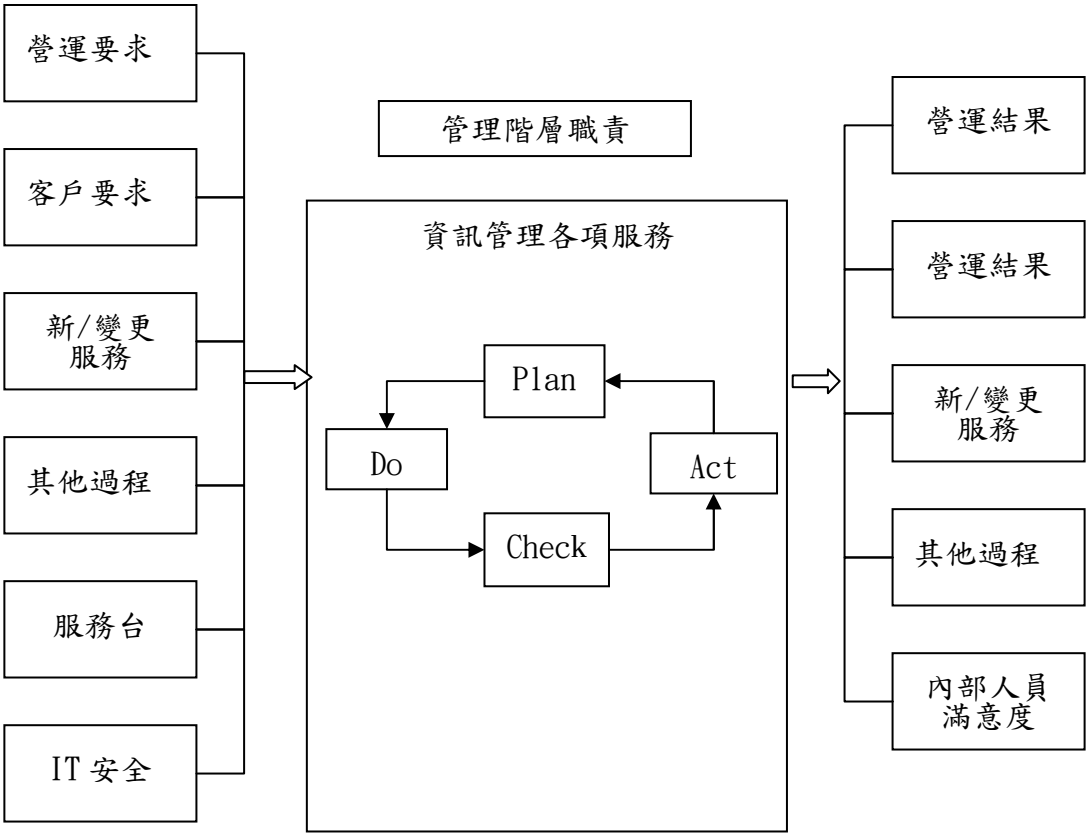

圖 9：ISO 20000 的 PDCA 管理流程

資料來源：ISO 20000:2005 Standard

表 10：ISO 20000 標準之要求

項次	領域	子流程
1	服務交付過程	(1) 服務等級管理 (2) 服務報告 (3) 持續性與可用性 (4) 預算與決算 (5) 容量管理 (6) 資訊安全管理
2	關係過程	(7) 營運關係管理 (8) 供應者管理
3	解決過程	(9) 事故管理 (10) 問題管理
4	控制過程	(11) 組態管理 (12) 變更管理
5	發行過程	(13) 發行過程管理

參考資料來源：ISO 20000:2005 Standard，本研究整理

2.6 CMMI 能力成熟度整合模式

早期開發軟體系統時，大概分為；系統分析、系統設計、系統開發、系統測試、建置與維護等項，一直缺少專案管理、建構管理(Configuration Management, CM)之觀念。資策會於 1988 年〔21〕參考美國 DOD 2167A 軟體發展標準研發出 SDG2.0「軟體發展指引」，始引進專案管理、建構管理、品質保證及採購的觀念，不再如以往只著重於系統工程。

CMMI 是美國國防部 1991 委託美國卡內基美隆大學的軟體工程學院(SEI；Software Engineering Institute)，發展一套用來評鑑團隊、單位、部門或組織之軟體專案開發能力成熟度整合模式(Capability Maturity Mode Integration，CMMI)。CMMI 範圍涵蓋 4 個專業領域，系統工程(System Engineering，SE)、軟體工程(Software Engineering ，SW)、整合的產品與流程發展(Integrated Product and Process Development，IPPD)及供應商供應(Supplier Sourcing，SS)。(註：另於 1997 年發表「採購」(Acquisition)概念及 2009 年發表「服務」(Services)為概念)。

表 11：CMMI 範圍涵蓋領域

項次	領域	內容
一	系統工程(SE)	系統工程含蓋了整合系統的發展，不論是否包括軟體。系統工程的重點是將客戶的需要，轉換為解決方案，並於產品生命週期中支援產品解決方案。
二	軟體工程(SW)	軟體工程含蓋軟體系統的發展，以系統化、嚴謹並可量化的方法運用至軟體發展、運作及維護。
三	產品與流程發展(IPPD)	以系統化方法建立相關之人員即時互動的方法。IPPD無法單獨完成目標，需配合SE或SW。
四	供應商供應(SS)	當一個專案規模變得愈來愈龐大時，組織可以透過供應商協助完成專案，供應商應作整合性的管理，並應包括於專案管理流程領域之中。

參考資料源：適用於發展的能力成熟度整合模式(CMMI-DEV)1.2 版，

目前，在國際軟體市場上，通過 CMMI 評鑑，已為廠商能否承接軟體代工專案的重要條件。CMMI 分成 5 個等能力成熟度，評鑑等級愈高，代表其管理發展與管理能力愈好。

表 12 ：能力度與成熟度等級的比較

等級	連續式表述的能力度等級	階段式表述的成熟度等級
等級 0	不完整級	無
等級 1	執行級	初始級
等級 2	管理級	管理級
等級 3	調適級	調適級
等級 4	量化管理級	量化管理級
等級 5	最佳化級	最佳化級

參考資料源：適用於發展的能力成熟度整合模式(CMMI-DEV)1.2 版

2.7 服務業概念介紹

根據楊錦洲〔22〕對服務業的定義：服務是提供物品、勞力、技術、專業、知識、資訊、設施、時間或空間之中的某些項目給顧客一系列活動構成的流程(process)。

服務業的範圍非常廣泛，包括；提供專業技術的服務，例如：醫療服務、法律服務，資訊與知識的服務，例如：軟體系統開發、教育訓練，勞力服務，例如：家事服務。服務業特性包括：

(1) 無形性(Intangibility)：購買前看不到，很難看出服務品質的好壞，所以，顧客多以口碑、形象、過去經驗等因素，決定採購與否。

(2) 不可分割性(Inseparability)：實體的產品，有一定的過程，包括；生產、運送、銷售等。而服務一般是生產與消費同時產生，例如：法律服務、教育訓練、餐飲，其服務的提供與消費是同時產生，因此，服務流程管控對服務品質就產生極大的影響。

(3) 異質性(Heterogeneity)：服務是一種活動或流程，服務品質良好與否，由客戶主觀感覺評定，即使是同一位員工對不同顧客所提供之服務，也會因人、事、時、地、物及當時情境不同，而產生服務品質之差異。

(4) 易逝性(Perishability)：服務業無法如實體產品可預估產量及存貨量，多數服務都需於短期內使用，且有時間性。

Gronroos(1990)對「實體產品」與「服務產品」特性之比較如下：

表 13：「實體產品」與「服務產品」特性之比較

實體產品	服務產品
有形性	無形性
同質性	異質性
生產、銷售、消費分開	生產、銷售、消費同時間產生
一件物品	一個活動或過程
核心價值在工廠中生產	核心價值在與消費者服務過程中產生
顧客不參與生產過程	顧客參與提供服務的過程
可以庫存	無法庫存

參考資料來源：楊錦洲，服務品質-從學理到應用，民國九十八年

2.8 資訊服務業

2.8.1 定義與範圍

資訊服務業是新興產業，根據行政院經建會(2003)對資訊服務業的定義〔48〕：提供產業專業知識及資訊技術，使企業能夠創造、管理、存取作業流程中牽涉之營運資訊，並予以最佳化之服務。其產業範圍包括：.

(1)電腦系統設計服務業：凡從事電腦軟體服務、電腦系統整合服務及其他電腦系統設計服務之行業。

(2)資料處理及資訊供應服務業：凡從事資料處理及資訊供應等服務之行業（含網際網路服務提供者(ISP)）。

2.8.2 行業特性與常用的國際標準

資訊服務業是廣義的軟體相關產業〔48〕，包括：套裝軟體、轉鑰系統(Turn-key System)、系統整合、專業服務、資訊處理服務與網路服務等六類。

其服務的內容視業務型態而定，大型廠商可能這六種服務均提供；而小型的套裝軟體廠商就只有一種業務。例如：戶役政資訊系

統、通關自動化系統、國土資訊系統等，強調整體解決方案(Total Solution)，以系統整合、轉鑰系統居多。又如；套裝軟體(package)；包括系統軟體如 DOS、Windows 等作業系統，以及應用軟體如試算表、文書處理、會計進銷存軟體等。其他如；客制化應用軟體開發，諮詢與教育訓練、資訊硬體設施管理(Facility Management)、資訊委外(IT Outsourcing)、雲端運算中心(Cloud Computer Center)等。由於資訊軟體應用領域擴大，近年我國資訊服務業產值亦逐年成長〔25〕。

表 14：2005-2010 年台灣資訊服務業產值

單位：NT$佰萬元

產業/年度	2005 年	2006 年	2007 年	2008 年	2009 年	2010 年
系統整合	79,780	75,731	76,237	80,829	76,146	78,693
資訊委外	8,593	10,588	13,124	14,988	16,870	19,503
商用軟體	2,470	2,840	3,203	3,455	3,745	4,121
資訊安全	24,223	27,691	32,721	36,941	41,669	48,183
嵌入式軟體	4,423	5,874	7,322	8,353	9,188	10,083
資訊服務總產值	119,489	122,724	132,607	144,566	147,618	160,583
年成長率(%)	-	2.7%	8.1%	9.0%	2.1%	8.8%

資料來源：資策會 MIC，2009 年 11 月

資訊服務業之產業特質與製造或其他服務業不相同，它是一個專業知識及技術密集，受環境影響且變化極迅速的產業，員工以受過高等教育之「高級人力」為主，幾乎沒有材料成本，主要的成本是於研發人力的成本，行業特性如表 15。

表 15：資訊服務業之行業特性

特性	說明
知識及技術密集	軟體業乃為知識及技術密集之產業員工以具有受過高等教育之「高級人力」為主。
資本密集	如為套裝軟體或大型資訊系統，其設計及行銷費用，常為百萬美元甚至上億美金之支出計。
產品之多樣性、創新性	只要你想得出的功能，軟體都可以幫你做到。因此，如何找市場利基十分重要。要創新，抓住市場脈動，迅速成為主流產品，才有成功機會。
成本結構	軟體業相對於一般行業最為不同的是，幾乎沒有材料成本，軟體主要開發的成本在於研發人力的成本。
其他特性	1. 軟體可以千變萬化，故如何瞭解使用者潛在需求，便為商機在。使用者的需求一改再改，或因為時間不同而有新生需求，這些都是商機。 2. 如同創作藝術一樣，軟體需要健全的智慧財產權(Copyright, Patent)保障。

參考資料來源：資策會 MIC，1996 年 7 月

資訊服務業具有知識及技術密集之產業特性，「人」是其主要核心價值。另，在現今全球產業鏈分工趨勢下，企業組織橫向與直向管理複雜，需管理制度輔助，以維護服務品質。另，獲得專業國際證照，向顧客證明專業能力，以爭取承接專案的機會，也是企業導入管理系統的原因。例如：印度以軟體代工聞名世界，印度之資訊服務大廠都具備 CMMI5 最高標準(能力成熟度模式，Capability Maturity Model)。

表 16：印度資訊服務大廠軟體能力

公司名稱/標準	ISO	CMM	PCMM	CMMI	其他
TCS	9001/27001	CMM L5	PCMM L4	--	6 Σ
Infosys	9001	CMM L5	PCMM L5	CMMI L5	CII-EXIM
Wipro	--	CMM L5	PCMM L5	CMMI L5	6 Σ
Satyam	27001	CMM L5	PCMM L5	--	6 Σ
HCL Technology	9001	CMM L5	--	--	
CTS India	--	CMM L5	PCMM L5	--	6 Σ

參考資料來源：資策會 2006 資訊服務年鑑，2006/08/01

台灣資訊服務業的主要以國內市場為主（約佔 75%），其次為中國大陸 11%、歐洲 6%、北美 3%以及其它地區 4%〔26〕。認證類型以 ISO 系列中之 ISO 9001、ISO 27001、ISO 20000 與 CMMI 為主。

三、研究方法

3.1 系統方法

系統方法(Systematic Approach)為本論文之主要研究方法，以ISO 9001、ISO 27001、ISO 20000與CMMI條文為要素(Element)，比較其異同，依其特性歸類，逐步建構管理系統模型；

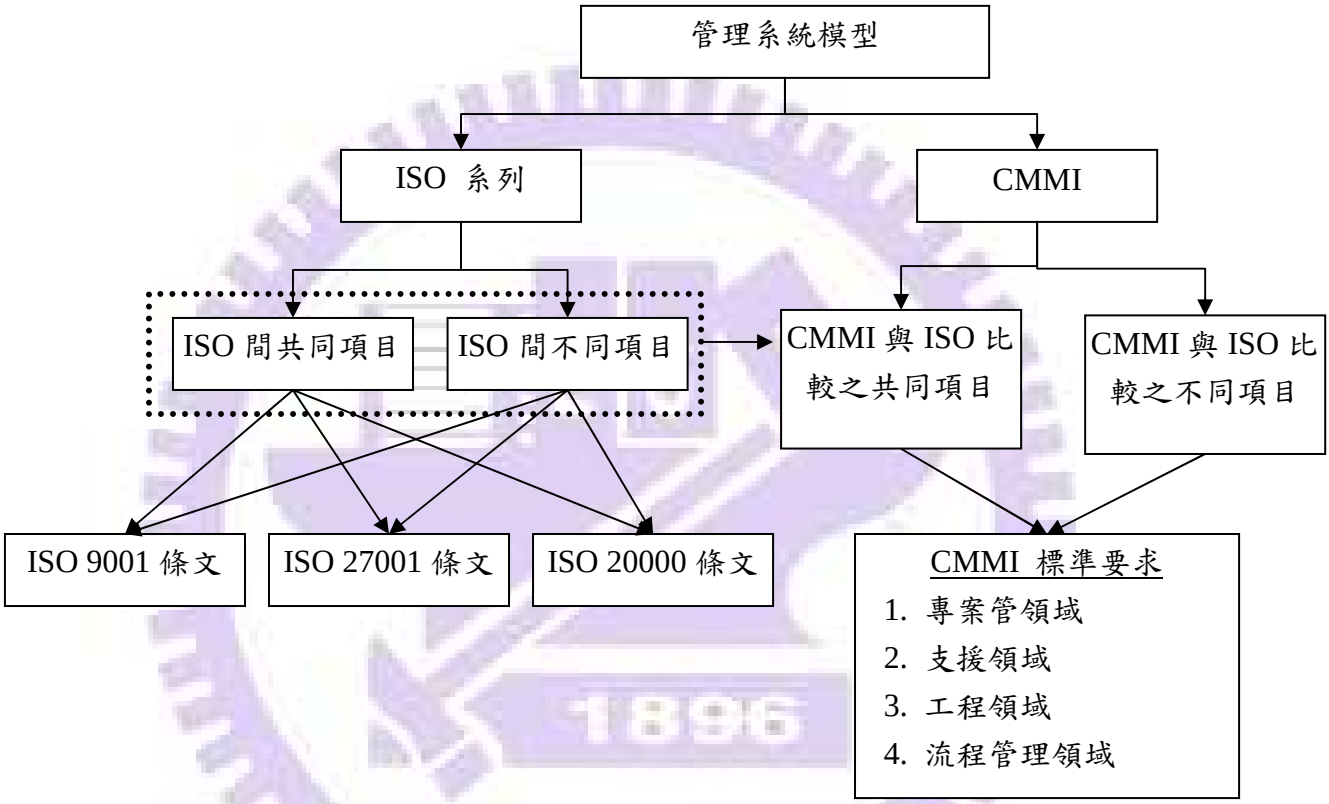

圖 10：系統方法(Systematic Approach)

資料來源：本研究整理

3.2 啟發性規劃

由於國內資訊服務業同時導入ISO 9001、ISO 27001、ISO 20000與CMMI之個案不多，取樣困難，無法以計量方式驗證研究結果有效性，故採啟發性規劃(Heuristic Programming)方法，以相關文獻、個人經驗與判斷及專家意見，以驗證實證研究結果之可執行性。

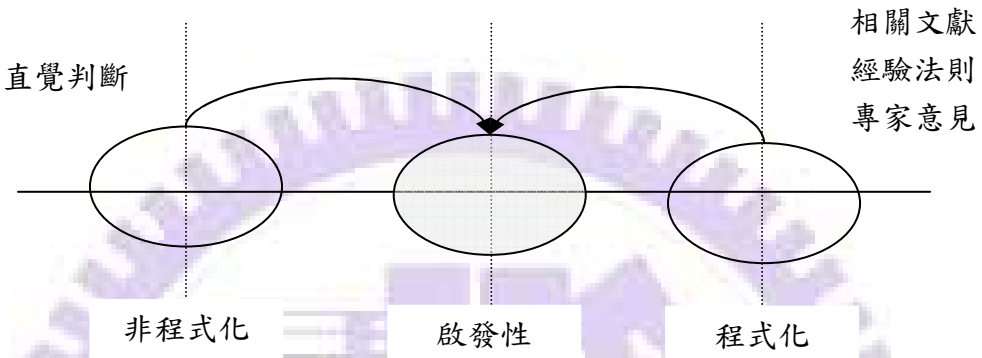

圖 11：啟發性規劃(Heuristic Programming)概念

3.3 黑盒子概念

黑盒子(Black Box)概念〔28〕，係由西方學者提出之觀點，將欲研究的重點視為一個黑盒子，暫不理會其內部的架構與原理，而將注意力著重於輸入(Input)，依照轉換法則(Laws of Transformation)之運作，產生對應輸出(Output)。

本研究之輸入項目包括ISO 9001、ISO 2700、ISO 20000、CMMI等條文以及考量環境、文化、法律規範等輸入特性，運用條文比較分析、歸納法、專家意見法之轉換法則，產生出期望與非期望之輸出。黑盒子概念如圖12所示：

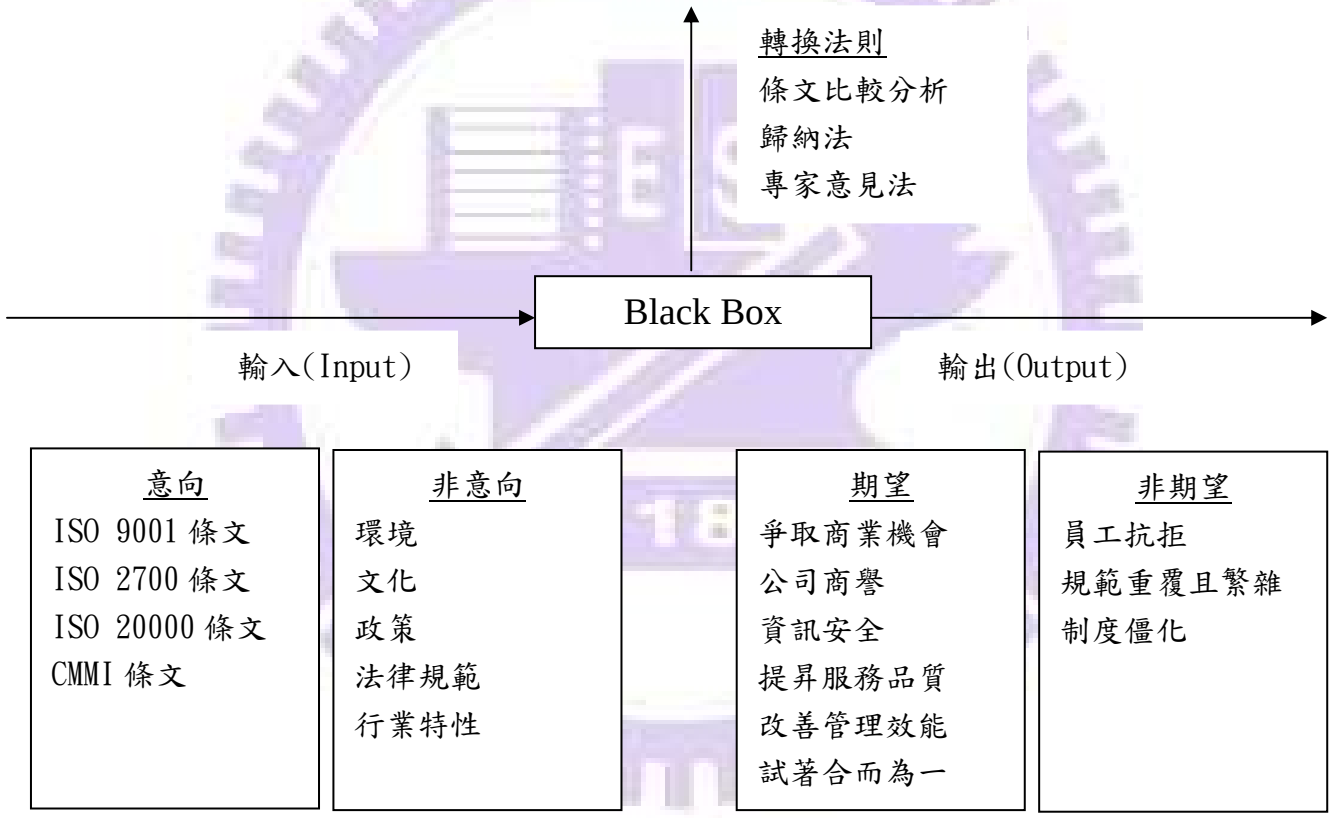

圖 12：黑盒子概念

資料來源：本研究整理

四、分析結果

4.1 ISO 9001、ISO 2700、ISO 20000 差異分析

根據前述探討，由於 ISO 9001 早於 1987 年頒佈，多數企業多已具備 ISO 9001 證照。近年來，隨著國際標準組織陸續頒布 CMMI (1991 年)、ISO 27001(2000 年)、ISO 20000(2005 年)。故多數之資訊服務業多以 ISO 9001 為基礎，之後依業務需求加入 CMMI 或 ISO 27001 或 ISO 20000。另，由於 ISO 系列與 CMMI 分屬不同國際標準組織所有，故企業於導入以上四類標準時，通常以 ISO 自成一體系，之後再加入 CMMI 相關規定。四類標準之間關聯性及比較分析順序如圖 13 與 14 所示：

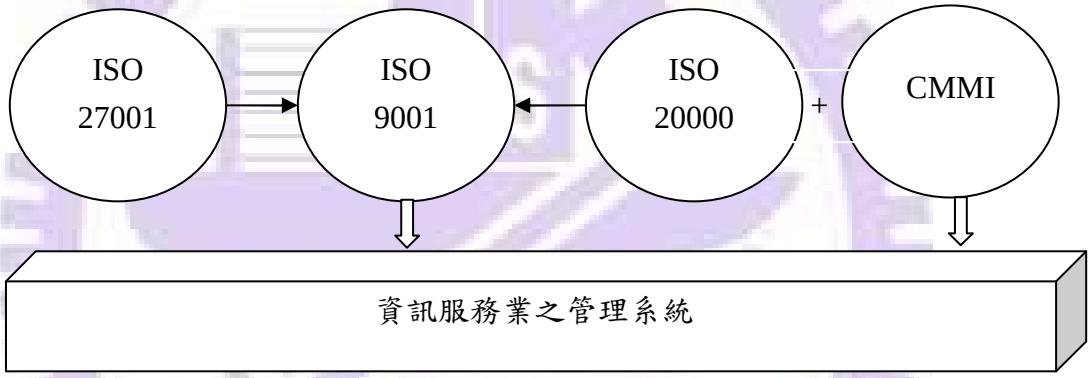

圖 13：資訊服務業之管理系統與各標準之關聯
資料來源：本研究整理

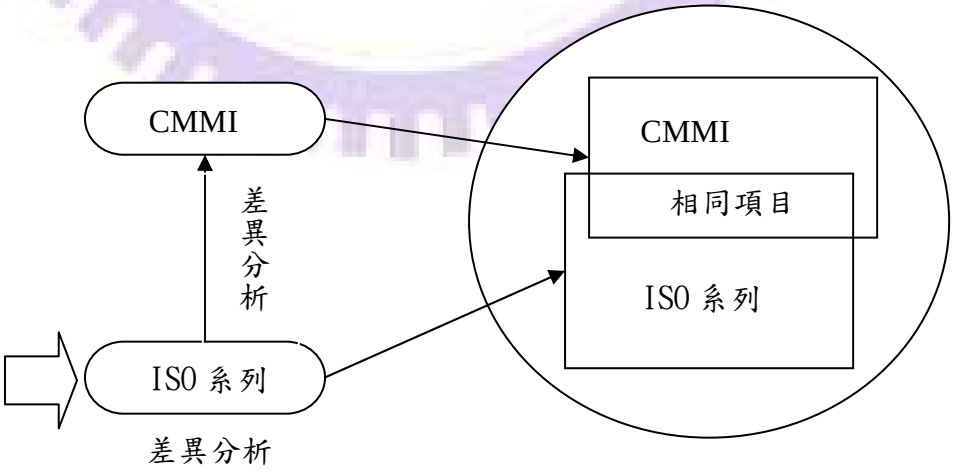

圖 14：ISO 9001、ISO 2700、ISO 20000 與 CMMI 分析
參考資料來源：Sys. Process Improvement Using ISO 9001:2000 and CMMI

4.1.1 共同項目

(1) 彈性選擇標準之適用範圍

企業經過評估後，可以依需要，選擇業務導入範圍。例如：某研發機構其導入範圍如下：

表 17：標準適用範圍之範例說明

標準	ISO 9001 標準	ISO 27001 標準	ISO 20000 標準	CMMI L3
適用範圍	部份業務適用	部份業務適用	部份業務適用	部份業務適用
規模註	55.7%	8.6%	8.6%	35.7%
適用業務	1. 智庫幕僚與產業推動 2. 人才培育 3. 國際合作 4. 資訊建設	1. 資訊建設-資安業務 2. 該機構之資訊中心	1. 資訊建設-資安業務 2. 該機構之資訊中心	資訊技術研發

參考資料來源：本研究整理

註：規模計算方式：(業務人數/機構總人數)%

(2) 導入與維護流程相似：由高階主管宣佈後，依資源決定導入範圍，第 1 次通過外部驗證後，即進入 PDCA 管理循環模式。

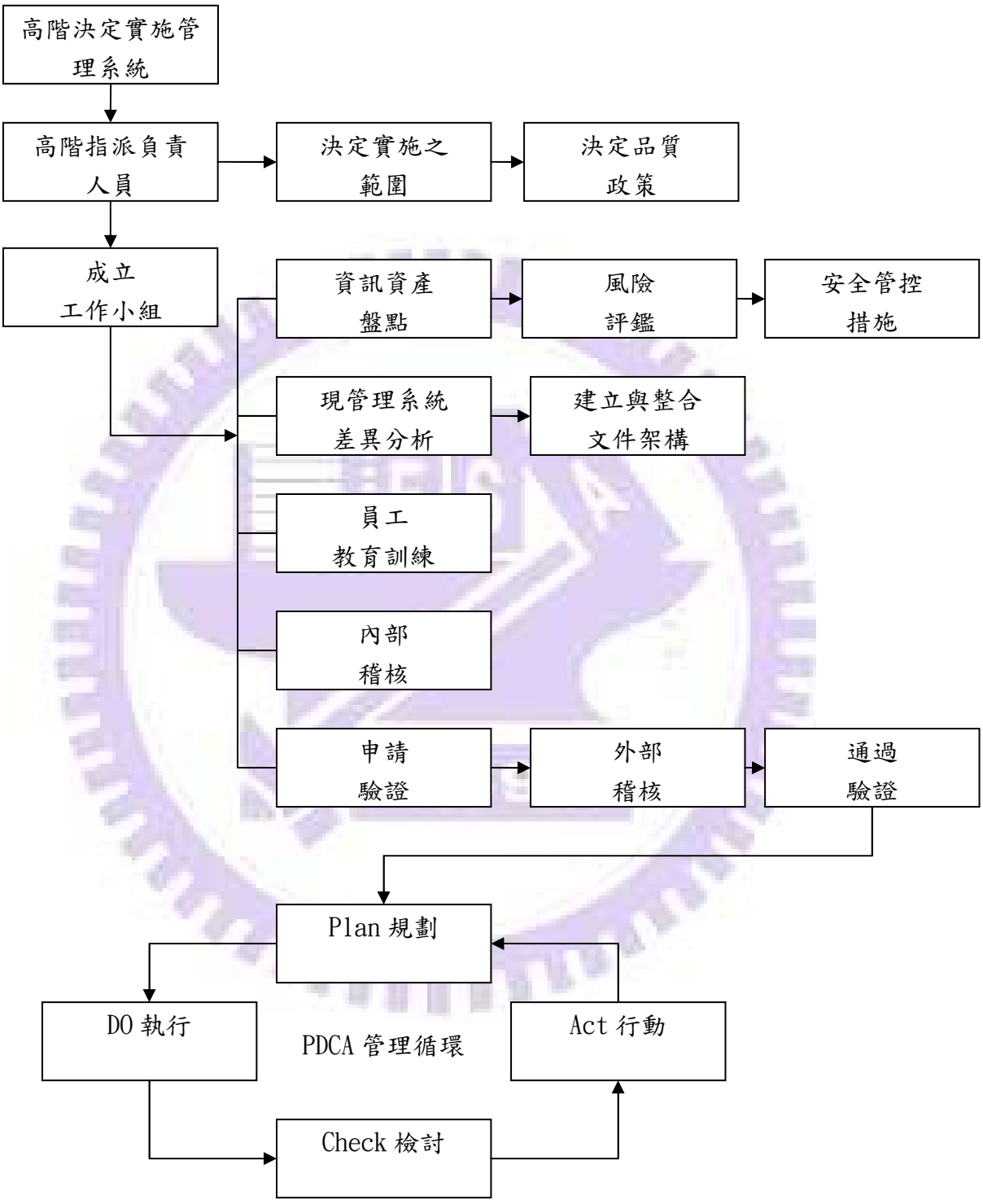

圖 15：ISO 系列導入流程

參考資料來源：本研究整理

(3) PDCA 管理循環

PDCA 管理循環是 ISO 系列共同特點，目的即便於整合。

(4) 著重持續改善精神

只要是人，都會犯錯，ISO 的精神不在懲罰錯誤，著重持續改善及預防在先的精神。

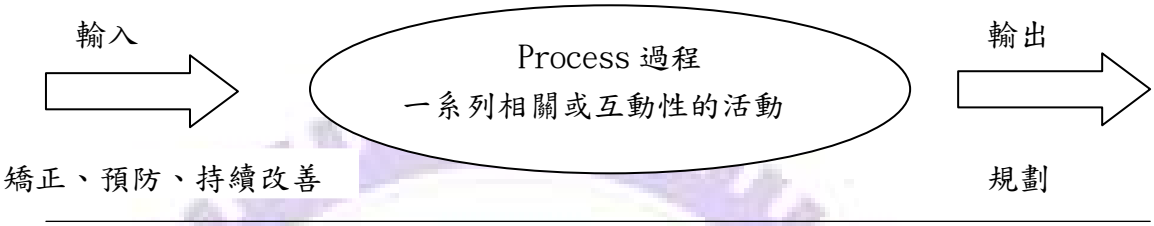

圖 16：矯正、預防、持續改善

(5) 具備「風險管理」的觀念

風險管理在於預防災害的發生，例如：富士康半年內陸續發生員工跳樓事件，富士康經由這次事件，以正面積極態度改善內部管理工作。

(6) 重視管理階層承諾

品質是企業策略管理整體績效中的一環〔47〕，需全員參與，故高階主管的支持，是推動品質管理系統成功的關鍵因素。

(7) 定期辦理管理審查

均要求定期辦理管理審查，以確保品質政策符合企業營運目標。

(8) 文件化觀念相同

都要求不能流於口頭形式，應予書面化，以避免認知造成的差異。執行的成效必須提出具體紀錄。文件的層級畫分以 5 個 W、1 個 H 原理設計。

圖 17：品質文件架構概念

(9) 重視員工之能力、認知及訓練

(10) 定期辦理內部稽核

稽核是品質管理系統很重要的項目，透過內部稽核的檢視，可及早發現問題，避免員工有犯錯的機會及降低外部稽核驗證失敗機率。

(11) ISO 20000 (條文 6.6) 資訊安全管理與 ISO 27001 相同。

4.1.2 差異項目

(1) 應用領域不同

ISO 9001-各行各業均適用

ISO 27001-資訊安全領域

ISO 20000-資訊服務領域

CMMI-軟體工程

(2) 著重之管理重點不同

ISO 9001-產品/服務品質

ISO 27001-資訊安全

ISO 20000-資訊服務

CMMI-軟體成熟能力

(3) 外部稽核過程不同

依據 ISO 國際組織規定，ISO 證照有效期 3 年，每年執行 1-2

次外部定期稽核。而 CMMI 是沒有證照的，僅於 SEI 網站中登錄，有效期也是 3 年，不過 3 年期間不做外部稽核，企業需有內部稽核工作之相關紀錄。

(4) ISO 20000 有成本預算觀念，及每項流程均規定量化之績效指標。

(5) 通過認證後結果不同

通過 ISO 認證，由 ISO 國際組織頒發證書，通過 CMMI 認證為評定軟體能力成熟度(L1-L5)，成熟度愈高，代表軟體工程管理能力愈好。

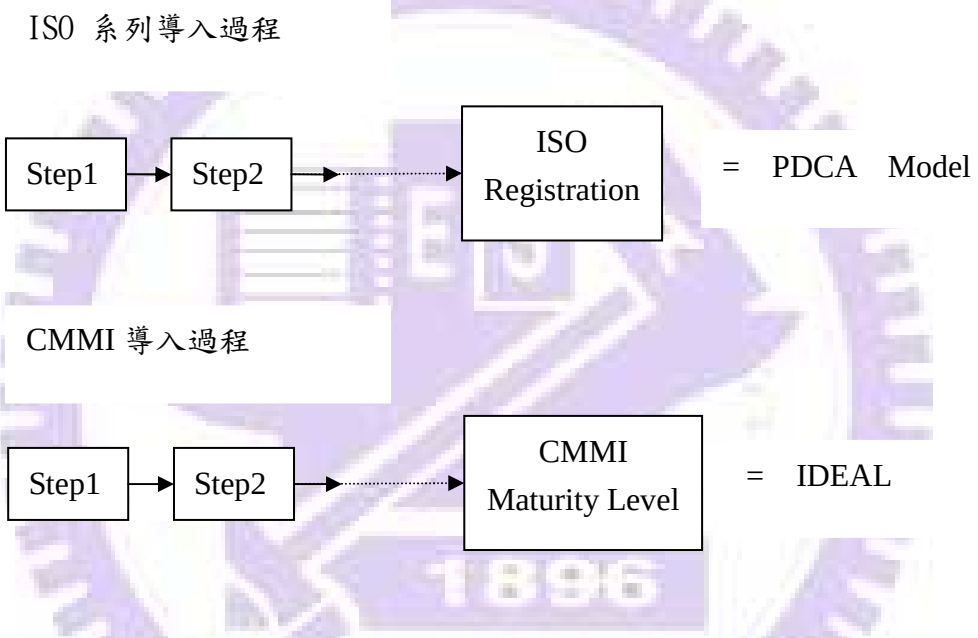

圖 18：ISO 系列與 CMMI 通過認證後結果

參考資料來源：Systematic Process Improvement Using ISO 9001:2000 and CMMI，2003

4.2 建構管理系統模型

為達簡潔不繁瑣目的，本研究採用 David Brewer(2005)〔10〕提出管理系統整合架構，內容分述如後：

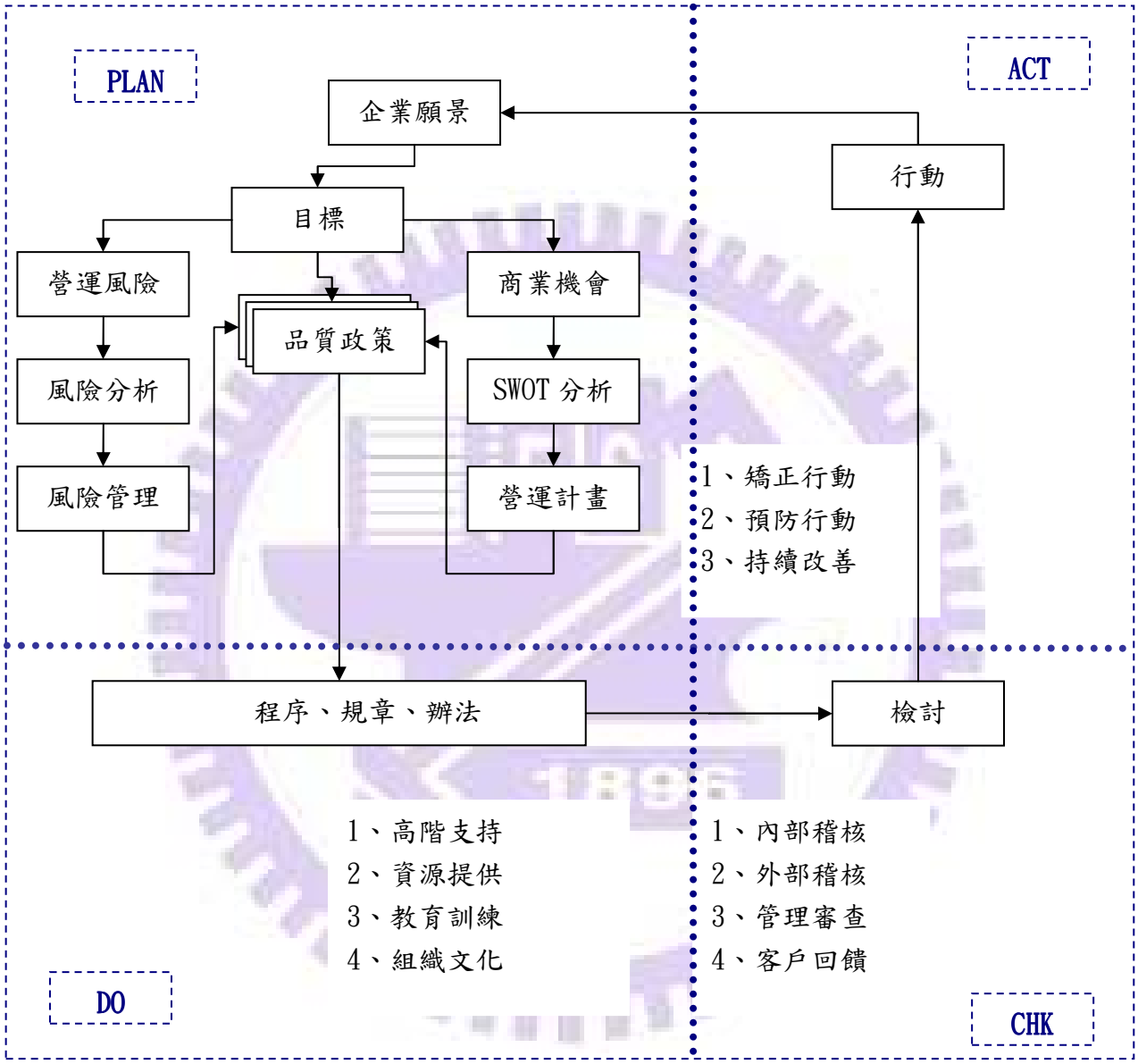

圖 19：管理系統之整體架構

參考資料來源： David Brewer，Exploitation an Integrated Management System〔10〕

4.2.1 Plan 階段

(1) 願景(vision)

企業得以永續經營，是因為有明確的「願景」，並且建立實現願景的「結構」，然後每天專注執行願景的「事件」〔20〕。Google「願景」是「整理全世界的資訊」，為此建立的「結構」是獨特的搜尋公式和全球最大的伺服器中心，而專注的「事件」是資訊的產品：搜尋引擎、Google 地圖、Google 圖書、YouTube 等。管理系統是協助專注執行「事件」的工具，故在設計時應符合企業願景。

(2) 目標(Object)

目標需依據遠景而設定，且為明確可達。最常用 SMART 表示；S(Specific)，具體明確。M(Measurable)，可衡量及以數據表達。A(Achievable)，可具體達到。R(Realistic)，合乎實際考量，T(Time-Based)，有時效性〔47〕。以國際標準而言；ISO 外，尚有美國卡隆大學的 CMMI、英國標準學會(BSI; British Standards Institution)等單位。組織在作長、中、短期目標規劃時，最好應考量用同一國際組織的產品，以避免因屬性不同，造成整合的困難。

(3) 商業機會(Business Opportunities)

沒有優良品質的產品/服務，就無法獲得顧客的信任。沒有顧客就沒有企業。擁有國際品質證書在 SWOT 分析具有 S(Strength)優勢，許多國際標案的企業，會要參與求廠商具備某類領域的國際品質證書，例如：食品安全領域的 HACCP、CAS、CMP、HALAL、軟體工程領域的 CMMI 等，不但提供顧客安心使用又具行銷能量優勢，及提升海外競爭能力。

(4) 品質政策

品質政策是管理系統的核心，必需與組織的遠景與目標契合，通常組織的品質政策都會以易記、易懂且易量化為制定的方向。例如：中油的品質政策：「中油為大家加油，大家為台灣加油」。連續蟬連臺北市優良公車第一名的首都客運的品質政策：「首都用心，乘客放心」。

並不是所有的國際標準都要求要有品質政策，以 ISO 9001、ISO 27001、ISO 20000 及 CMMI 為例。其中僅 ISO 9001、ISO 27001 於條文中明確規範應有品質政策。品質政策應每年檢討其合適性，尤其當組織之營運目標有變更時或新增國際標準時，都應重新做檢視。

4.2.2 Do 階段

(1) 程序、規章、辦法

管理系統的精神強調「寫你所做，做你所寫」，故一般企業都會將相關的規定文件化，以避免因人員的流動造成知識的斷層。

由於多數資訊服務業都由 ISO 9001 開始，文件化的工作已具備基礎，例如 ISO 9001 規定之文件管制程序、紀錄管制程序、內部稽核程序等，都可與 ISO 27001、ISO 20000、CMMI 共用，儘量由 ISO 9001 的文件化架構發展，有特殊需求再個別發展，以避免規範過多，造成執行困難。

(2) 資源提供

包括；支援服務系統、工作環境管理、供應商管理、軟、硬體設備等，均可透過共同的平臺管理，以使員工作能在良好安全的環境中工作。

(3) 教育訓練

ISO 系列與 CMMI 各有不同的教育訓練需求，不可能整合，但可透過整體規劃，以使其訓練效益最佳化。

表 18：ISO 系列與 CMMI 的教育訓練需求

ISO 9001	ISO 27001	ISO 20000	CMMI
1、主導稽核員訓練 2、內部品質系統稽核訓練 3、品質文件撰寫教育訓練 4、ISO 9001 建置	1、 主導稽核員訓練 2、 內部品質系統稽核訓練 3、 ISMS 建置課程 4、 風險管理	1、 主導稽核員訓練 2、 ISO 20000 Foundation 3、 ITIL V3 Foundation	1、Introduction to CMMI 2、Intermediate Concepts of CMMI 3、Instructor Training 4、SCAMPI Lead Appraiser Training

資料來源：本研究整理

4.2.3 Check階段

(1) 管理審查

依據 ISO 之規定由高階主管成立管理審查委員會議，以檢視管理系統的執行情形，CMMI 也有同樣的要求。審查重點：

a. 品質政策與品質目標之達成狀況與變更需求
b. 品質制度與辦法之適切性（包括品質手冊、政策、目標、作業制度）
c. 品質管理系統運作之有效性（包括過程績效及產品符合性、以及資源使用之合理性）
d. 品質管理系統之組織與權責檢討
e. 品質稽核結果檢討
f. 客戶回饋與檢討(如：客戶滿意度調查結果報告抱怨)
g. 矯正預防措施之執行有效審查
h. 影響品質管理系統變更(法令, 組織…)相關議題及改善建議

(2) 客戶回饋

一般企業以客戶滿意度調查作為業瞭解客戶回饋意見的管道，重點在於客戶意見妥適處理，共同辦理較佳。

(3) 內部稽核

無論 ISO 或 CMMI 均明確規定要內部稽核，ISO 的部份可考慮整合一起做，並以流程稽核方法，較易檢查出整體系統問題。CMMI 也是流程導向，以軟體工程為主，稽核的內容與重點與 ISO 不同相，無法與 ISO 整合。

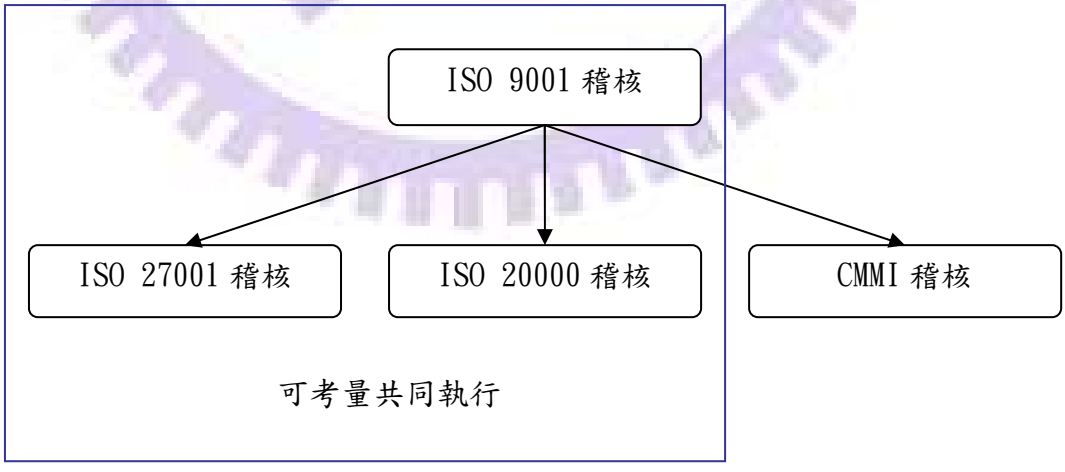

圖 20：稽核整合

資料來源：本研究整理

4.2.4 Act階段

矯正、預防是管理系統持續改善重要工作，ISO 系列與 CMMI 由於差異性大，無法共同辦理。

(1) 矯正行動

不符合的作業補正，採取措施消除根因，以防止再發生。

(2) 預防行動

採取措施，防止潛在原因及異常發生。

(3) 持續改善

已符合要求，採取措施讓績效更好

五、結論

5.1 經營困難

經由以上的分析結果可以得知，當企業同時導入 ISO 系列(ISO9001、ISO 27001、ISO 20000)與 CMMI 時，主要會面臨以下困難：

(1)專注不同，影響管理

CMMI 專注在階段(Staged)，ISO 則是持續改善(Continuous)。也因為專注不同，兩者存在共同項目與不同項目。詳見第 4.1.1 及 4.1.2 節及附件一與二。在研究個案中，就曾出現在管理上有取捨的現象。

(2)企業文化影響整體成效

資訊服務業是一個專業知識及技術密集的產業，過於用流程規範管理員工，會限制員工的想像空間，對創意不利。

(3)不要勉強一定要整合

依據本研究 4.1.1 與 4.1.2 章節所述，ISO 系列與 CMMI 許多的工作可以共同執行。但是管理系統是否要整合，需視企業的組織文化而定。整合的優點是化繁為簡，省去許多重覆的工作，而最大的困難是跨部門間的溝通，事情好解決，人的問題難處理，所以不要勉強一定要整合。

雖然如此，但是企業若能將其困難引導或衍生為綜效(Synergy)，可確實提昇整體企業品質之改善。亦即，同時導入可衍生出品質管理的綜合效益。因此，專注不同與企業文化即變成品質改善的助力。下一節即針對這綜效，提報在管理上的對應策略。

5.2 管理對策

本研究藉由實證研究，探討企業同時導入 ISO 系列(ISO9001、ISO 27001、ISO 20000)與 CMMI 之比較分析與管理，研究發現整理如下：

1. 建立明確、直接、一貫的管理系統

提昇品質是企業管理重要工作，其精髓就在流程管理，讓流程充份發揮功能，時時找尋改進流程的機會，然後把機會化為事實。企業導入品質管理系統，最大的功能，就明確、直接、一貫，泰勒(Frederick Taylor)所提倡的「科學化管理」就是把員工的每個動作，變成標準的工作習慣。

2. 流程規範與企業文化

無論 ISO 或 CMMI 均有文件化的要求，以文字敍述每項工作流程規範，避免造成員工認知差異。惟資訊服務業是一個專業知識及技術密集的產業，過於用流程規範管理員工，會限制員工的想像空間，對創意不利。在流程規範與實務之間，一方面企業管理要夠鬆，好讓同仁發展自己的新知識，另一方面管理要夠嚴謹，以使這些知識能夠沿著流程規範而保留下來。

3. 重品質也要重利潤

企業要獲得 ISO 或 CMMI 國際證照，常是商業上的考量。惟國際標準規範繁多而嚴謹，事前需要投入大量人力與時間，再加上顧問輔導費用、外部稽核費用、國際證照維護費用等，投資金額不菲。所以，為何說管理系統第一強調的重點是：高階主管的支持。企業在採用國際標準導入管理系統前，即應審慎思考與評估，國際證照帶來的利潤要大於導入成本。

4. 員工抗拒改變與組織衝突

依據前述實證研究探討，資訊服務業「人」是其主要核心價值，員工多為「高級知識工作者」，包括：工作經驗豐富、高學歷、優秀學府畢業、工作績效優良等。在管理制制度推動前，一定要有充分溝通，並獲得共識與認同，避免造成上有政策，下有對策的現象。

5. 橘子與柳丁的比較

經過實證研究的發現，ISO 與 CMMI 就好比是橘子與柳丁，雖然外表都是圓的，口味有些相似但又不盡相同，與其談 ISO 與 CMMI 的整合，倒不如以互補的觀念來執行。

6.「風險管理」的觀念

「風險管理」已是企業重要的課題，俗話說：防火成本低，壓力高，救火成本高，萬本無利。ISO 與 CMMI 都具備「風險管理」的觀念，尤其是 ISO 27001 更有一套風險評鑑的方法，可提供企業參考。

7. 「零缺失」的迷失

ISO 與 CMMI 的外部稽核結果，通常分為四大類：(1)主要缺失-不建議發證；(2)次要缺失-矯正改善，下次查證；(3)改善事項-矯正改善，下次查證；(4)建議事項-提供企業改善參考。經常在報章雜誌看到，XX 企業以「零缺失」通過驗證。「零缺失」就能代表管理系統沒有問題嗎?學生認為，只要是人執行的工作，不可能沒有缺失。只要不發生「主要缺失」，影響發證，一位企業的管理者應以正面的態度看待稽核缺失，畢竟管理系統強調的是持續改善的精神，而不是「零缺失」。

8. 重視員工品德

吳子說：「內修文德，外治武備」，在現今資訊發達的環境，引誘犯罪的機會大大的增加。楊瑞仁在國票任職A走一佰零二億兩仟萬元，曾有記者問出獄後的楊瑞仁，如果再有一次機會，還會不會犯同樣的錯誤，楊瑞仁的回答是：「會」；因為安控機制太鬆散，誘惑太大。目前本論文所研究的國際標準，僅 ISO 27001 對人員的安全作規範，但也僅止於形式上，無法杜絕有心犯罪的人。企業除加強安控機制管理外，於人才的選、訓、育、用的過程中，唯德是用，並塑造誠信的組織文化，讓良好的品德環境中發揮潛移默化的功能，由員工自主管理才是根本解決之道。

5.3 未來研究建議

本研究以 ISO 9001、ISO 27001、ISO 20000 與 CMMI 條文為基礎，比較分析異、同，找出相同項目及整合建構模式，以解決條文繁多，執行不易的管理困難。並未就績效面及成本面做研究。

品質是績效的一環，也需要量化的評估指標，來判定其執行成效。另，全面品德管理(Total Ethical Management, TEM)是近年來極為受重視的議題，由「人」的觀點探討「品質」與「品德」，亦是後續值得加以研究的方向。

表 19：品質管理與品德管理比較

項目	品質管理	品德管理
管理對象	人	人
學術領域	科學管理	社會學/心理學
衡量標準	可制定量化指標	主觀之認定
管理方法	程式/規範/SOP	規範/自主管理
養成方法	組織文化/教育訓練	組織文化/教育訓練
最終目標	內化為工作習慣	內化為行為習慣

資料來源：本研究整理

參考文獻

一、英文文獻

1. IT Service Management System Lead Auditor Course，The British standards Institution，2009。
2. International Organization for Standardization，ISO 9001:2008 Standard。
3. International Organization for Standardization，ISO 27001:2005 Standard。
4. International Organization for Standardization，ISO 20000:2005 Standard。
5. Boris Mutafelija，Harvey Stromberg ，Systematic Process Improvement Using ISO 9001:2000 and CMMI，2003 ARTECH HOUSE, INC., p8。
6. Dale R. Spaulding，“CMMI-ISO Can we all just get along?”， The Boeing Company，2008。
7. Mikko Siponen 、 Robert Williston， “Information security management standards: Problems and solutions”，Information & Management，p267–p270，2009。
8. Ditech Networks Inc.，”Integrated Management System Manual- ISO 9001:2000 and 14001:2004”，2006。
9. Dimitris Petropoulos，”ISO/IEC 27001:2005A brief introduction”，Information Risk Management，September 2006。
10. David Brewer，" Exploitation an Integrated Management System "，Quality Progress，p1-p6，2005。
11. Boris Mutafelija & Harvey Stromberg ，ISO 9001:2000 – CMMI v1.1 Mappings，July 2003，p1-p31。
12. Mikko Siponen 、 Robert Williston b，“Information security management standards: Problems and solutions”， Information & Management，No.46 ，p267–p270， 2009。
13. Ho-Won Jung 、Robin Hunter，“The Relationship between ISO/IEC 15504

Process Capability Levels，ISO 9001 Certification and Organization size: An Empirical Study”， The Journal of System and Software，59，p43-p55，2001。

14. Chanwoo Yoo 、 Junho Yoon、Byungjeong Lee ，“A unified model for the implementation of both ISO 9001:2000 and CMMI by ISO-certified organizations”，The Journal of System and Software，p954-p961，January 2006。

15. Bilge Karabacaka,& Ibrahim Sogukpinarb，“A quantitative method for ISO 17799 gap analysis”，Computers and Security，p413-p419，2006。

16. Mustafa V. Uzumeri，“ISO 9000 and Other Met standards：Principles for Management Practice”，IEEE Engineering Management Review，V26 N.3，p5-p15，Fall 1998。

二、中文文獻

17. 楊政學，企業研究方法，初版，台北，普林斯頓國際有限公司，民國九十四年。

18. Thomas L.Good & Jere Brophy 著，當代教育心理學，李素卿譯，五南圖書出版有限公司，台北，民國 98 年 3 月。

19. 高旭，深入探討 ISO 9001/14001 文件資料管理制度，五版，台北，中華民國品質學會，民國九十八年八月。

20. 王文華，「帶我們爬樓梯-給馬總統的信」，聯合報， A4 版，民國九十九年五月十六日。

21. 卡內基美隆大學軟體工程學院，適用於發展的能力成熟度整合模式(CMMI-DEV)，1.2 版，民國九十五年八月。

22. 楊錦洲，服務品質-從學理到應用，初版，台北，華泰文化，民國九十八年，p4-p20。

23. CMMI 產品團隊，適用於發展的能力成熟度整合模式(CMMI-DEV)1.2 版，財團法人資訊工業策進會，民國九十六年十一月。

24. 資策會 MIC，資訊服務業市場現況與發展趨勢分析，財團法人資訊工業策進會，民國八十五年七月，p8-p11。

25. 翁偉修、林信亨、王義智、李震華、黃正傑、洪聖敏，”台灣資訊服務產業發展現況與趨勢”，MIC 產業研究報告，民國九十八年十二月。

26. 經濟部工業局，2008 年台灣自由軟體產業產銷調查報告- 軟體與服務，民國九十七年十一月，p1-p4。

27. 管倖生，設計研究方法，二版，台北，全華科技，民國九十八年，第十五章。

28. 黃承傳，系統方法上課講義，民國九十九年二月，P2-P5。

29. 資策會，適用於發展的能力成熟度整合模式(CMMI-DEV)，1.2 版，民國九十六年十一月。

30. 高小玲，「企業道德風險及基於中國企業的實證研究」，復旦大學管理學院，博士論文，民國九十八年二月。

31. 吳佳純，「企業策略與資訊系統策略之策略性校準對企業流程之影響-MIT90s 模式之應用」，國立交通大學經營管理研究所，博士論文，民國九十六年一月。。

32. 標準檢驗局，標準檢驗局 97 年年報，民國九十八年二月。

33. 黃鴻順、游伯龍，「探討消費者的潛在領域，創造企業價值－以《Wii》產品為例」，第 16 屆習慣領域年會論文集，p169-p181，民國九十七年七月。

34. 湯玲郎、林李旺，“企業文化與推行 ISO 品質制度對組織績效之影響”，品質學報 Vol. 14, No. 3，p251-p265，民國九十六年。

35. 資策會，”2009 年台灣資訊市場-資訊硬體、資訊軟體市場”，MIC 調查報告，民國九十八年。

36. 資策會，”2010 不容忽視的網路七大安全威脅”，MIC 調查報告，民國

九十九年二月。

37. 高惠堂，CMMI 簡介，民國九十五年十二月。

38. 唐震，”企業流程標準化對組織內部協調影響之研究”， 管理與資訊學報，13 期，p41-p76，民國九十七年。

39. 王小芳、王瑞芳、杨兴涛，”基于 I SO 2 0 0 0 0 的 IT 服务管理平台的研究与实现”， 计算机系统应用，第 5 期，民國九十八年。

40. 查士朝，“BS7799/ISO17799/ISO27001 資訊安全管理制度介紹與導入實務”，資誠企管簡報。

41. 吳政叡，“ISO 27001「資訊安全管理系統要求」在圖書館的應用”， 臺灣圖書館管理季刊，第四卷第二期，p89-p99，民國九十七年四月。

42. 黃能堂，“未來優質公民：品格力修練”， 臺北市終身學習網通訊網，37 期，p26-p30。

43. Yuan, Yu Rong，“Build a Two-Tier TQM Model Beyond ISO 9000”， 中華民國品質學會第 43 屆年會暨第 13 屆全國品質管理研討會，p1-p12。

44. 李旭華、黃翠鈴，“全面品德管理之特性分析”， 中華民國品質學會第 42 屆年會暨第 12 屆全國品質管理研討會，p1-p10。

45. 陳皆成，推動 CMMI 認證的基礎概念簡報檔，民國九十五年五月。

46. 經濟部工業局，經濟部工業局資訊服務業發展計畫提案說明會簡報檔。

47. 楊千，策略管理-理論與實務，初版，台北，華泰文化，p209，民國九十六年一月。

48. 洪震宇，資訊夢工廠-資策會：數位台灣推手，第一版，台北，天下文化，民國九十三年。

49. 游伯龍，HD：習慣領域-IQ 和 EQ 沒有談的人性軟體，初版，台北，時報文化，民國八十七年。

50. 蔡今中，如何撰寫與發表社會科學論文-國際刊物指南，初版，北京，北京大學出版社，民國九十八年一月。

51. SGS 台灣檢驗科技公司，ISO 9001:2008 版實務與驗證指引-重新檢視調整以增進系統效益，初版，民國九十八年一月。

52. 畢恆達，白痴造句法，把論文變難看了，聯合報 A4 版，民國九十八年二月二十八日。

53. Richard Whiteley and Diane Hessan，贏得顧客心，譚家瑜譯，天下文化，台北，民國九十六年六月。

54. John Seely Brown，資訊革命了什麼，顧淑馨譯，初版，北京，先覺出版社，民國九十年一月。

三、網站

55. 台灣服務業聯網，http://www.twcsi.org.tw/columnpage/service/definition.aspx。

56. 資策會網站 http://www.iso.org/iso/home.html。

附件一：ISO 9001、ISO 27001、ISO 20000 條文比較

ISO 9001 條文	ISO 27001 條文	ISO 20000 條文	差異說明
1 範圍 1.1 概述 1.2 應用 2 引用標準 3 名詞及定義	1. 適用範圍 1.1 概述 1.2 應用 2. 引用標準 3. 用語釋義.	1. 適用範圍 2. 用語解釋	1.異：應用領域不同 ISO 9001-各領域 ISO 27001-資訊安全 ISO 20000-資訊服務 2.同：適用範圍可選擇部份適用，或全部適用
4 品質管理系統 4.1 一般要求 4.2 文件化要求 4.2.1 概述 4.2.2 品質手冊 4.2.3 文件管制 4.2.4 記錄管制	4. 資訊安全管理系統 4.1 一般要求 4.2 建立與管理 ISMS 4.2.1 建立 ISMS 4.2.2 實作與運作 ISMS 4.2.3 監視與審查 ISMS 4.2.4 維持與改進 ISMS 4.3 文件化要求 4.3.1 概述 4.3.2 文件管制 4.3.3 紀錄管制	3.管理系統之要求 3.1 管理職責 3.2 文件化要求 3.3 能力、認知與訓練 4.服務管理規劃與實作 4.1 規劃服務管理(規劃) 4.2 實作服務管理與提供服務(執行) 4.3 監視、量測與審查(檢查) 4.4 持續改善(行動) 4.4.1 政策 4.4.2 改善管理 4.4.3 活動	1.異：無 2.同： (1) PDCA 管理循環 (2)文件化要求相同，包括；品質政策及品質目標、品質手冊、國際標準所要求的書面化程序及紀錄、組織為確保規劃的有效性、過程運作及管制所需的文件包括紀錄
5.管理階層責任 5.1 管理階層承諾	5.管理階層責任 5.1 管理階層承諾		1.異：無 2.同：

ISO 9001 條文	ISO 27001 條文	ISO 20000 條文	差異說明
5.2 顧客為重 5.3 品質政策 5.4 規劃 5.4.1 品質目標 5.4.2 品質管理系統規劃 5.5 職責、權限及溝通 5.5.1 職責及權限 5.5.2 管理代表 5.5.3 內部溝通 5.6 管理階層審查 5.6.1 概述 5.6.2 審查輸入 5.6.3 審查輸出	7. ISMS 之管理階層審查 7.1 概述 7.2 審查輸入 7.3 審查輸出		(1)重視管理階層承諾 (2)明訂管理階層審查及審查輸入與輸出 (3)「風險評估」的精神→控制→監控→改善方法 (4)至少每年要定期審查品質政策之適用性
6 資源管理 6.1 資源提供 6.2 人力資源 6.2.1 概述 6.2.2 能力、認知及訓練 6.3 基礎架構 6.4 工作環境	5.2 資源管理 5.2.1 資源提供 5.2.2 訓練、認知及能力		1.異：無 2.同： (1)重視管理階層承諾 (2)明訂管理階層審查及審查輸入與輸出 (3)「風險評估」的精神→控制→監控→改善方法
7 產品實現 7.1 產品實現之規劃	資訊安全控制目標與控制措施 A.5 安全政策	5. 新增或變更之服務的規劃與實作	1.異： (1)著重之管理重點不同

ISO 9001 條文	ISO 27001 條文	ISO 20000 條文	差異說明
7.2 顧客有關之過程	A.5.1.1 資訊安全政策文件	6. 服務交付過程	ISO 9001-產品/服務品質
7.2.1 產品有關要求之決定	A.5.1.2 資訊安全政策之審查	6.1 服務等級管理	ISO 27001-資訊安全
7.2.2 產品有關要求之審查	A.6 資訊安全的組織	6.2 服務報告	ISO 20000-資訊服務
7.2.3 顧客溝通	A.6.1 內部組織	6.3 服務持續性與可用性管理	(2) ISO 20000 有成本預算觀念
7.3 設計及開發	A.6.1.1 管理階層對資訊安全的承諾	6.4 IT 服務之預算編列與結算	(3) ISO 20000 明訂績效指標
7.3.1 設計及開發規劃	A.6.1.2 資訊安全協調工作	6.5 容量管理	
7.3.2 設計及開發輸入	A.6.1.3 資訊安全責任的配置	6.6 資訊安全管理	2.同：
7.3.3 設計及開發輸出	A.6.1.4 資訊處理設施的授權過程	7. 關係過程	(1) ISO 20000 6.6 談到資訊安全管理可與 ISO 27001 串連
7.3.4 設計及開發審查	A.6.1.5 機密性協議	7.1 概要	
7.3.5 設計及開發查證	A.6.1.6 與權責機關的聯繫	7.2 營運關係管理	
7.3.6 設計及開發確認	A.6.1.7 與特殊利害相關團體的聯繫	7.3 供應者管理	
7.3.7 設計及開發變更之管制	A.6.1.8 資訊安全的獨立審查	8. 解決過程	
7.4 採購	A.6.2 外部團體	8.1 背景	
7.4.1 採購過程	A.6.2.1 與外部團體相關的風險之識別	8.2 事故管理	
7.4.2 採購資訊	A.6.2.2 處理客戶事務的安全說明	8.3 問題管理	
7.4.3 所購產品之查證	A.6.2.3 第三方協議中之安全說明	9. 控制過程	
7.5 生產及服務提供	A.7 資產管理	9.1 組態管理	
7.5.1 生產及服務提供之管制		9.2 變更管理	
7.5.2 生產及服務提供過程之確認		10. 發行過程	
7.5.3 識別及追溯性		10.1 發行過程管理	
7.5.4 顧客財產			
7.5.5 產品防護			

ISO 9001 條文	ISO 27001 條文	ISO 20000 條文	差異說明
7.6 監督及量測裝置之管制	A.7.1.1 資產清冊 A.7.1.2 資產的擁有權 A.7.1.3 資產之可被接受的使用 A.7.2 資訊分類 A.7.2.1 分類指導綱要 A.7.2.2 資訊標示與處置 A.8 人力資源安全 A.8.1 聘僱之前 A.8.1.1 角色與責任 A.8.1.2 篩選 A.8.1.3 聘僱條款與條件 A.8.2 聘僱期間 A.8.2.1 管理階層責任 A.8.2.2 資訊安全認知、教育及訓練 A.8.2.3 懲處過程 A.8.3 聘僱的終止或變更 A.8.3.1 終止責任 A.8.3.2 資產的歸還 A.8.3.3 存取權限的移除 A.9 實體與環境安全 A.9.1 安全區域		ISO 27001 條文 A.8 對人員工作品德的管理仍不易規範，除由系統軟硬體的安全措施管理外，仍需經由內部加強品德觀念。

ISO 9001 條文	ISO 27001 條文	ISO 20000 條文	差異說明
	A.9.1.1 實體安全周界 A.9.1.2 實體進入控制措施 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.9.1.5 在安全區域內工作 A.9.1.6 公共進出、收發及裝卸區 A.9.2 設備安全 A.9.2.1 設備安置與保護 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.9.2.5 場所外設備的安全 A.9.2.6 設備的安全汰除或再使用 A.9.2.7 財產的攜出 A.10 通訊與作業管理 A.10.1 作業之程序與責任 A.10.1.1 文件化作業程序 A.10.1.2 變更管理 A.10.1.3 職務的區隔		

ISO 9001 條文	ISO 27001 條文	ISO 20000 條文	差異說明
	A.10.1.4 開發、測試及運作設施的分隔 A.10.2 第三方服務交付管理 A.10.2.1 服務交付 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 系統規劃與驗收 A.10.3.1 容量管理 A.10.3.2 系統驗收 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 A.10.4.2 對抗行動碼的控制措施 A.10.5 備份 A.10.5.1 資訊備份 A.10.6 網路安全管理 A.10.6.1 網路控制措施 A.10.6.2 網路服務的安全 A.10.7 媒體的處置 A.10.7.1 可移除式媒體的管		

ISO 9001 條文	ISO 27001 條文	ISO 20000 條文	差異說明
	理 A.10.7.2 媒體的汰除 A.10.7.3 資訊處置程序 A.10.7.4 系統文件的安全 A.10.8 資訊交換 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.10.8.5 營運資訊系統 A.10.9 電子商務服務 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 監視 A.10.10.1 稽核存錄 A.10.10.2 監控系統的使用 A.10.10.3 日誌資訊的保護 A.10.10.4 管理者與操作者日誌 A.10.10.5 失誤存錄 A.10.10.6 鐘訊同步		

ISO 9001 條文	ISO 27001 條文	ISO 20000 條文	差異說明
	A.11 存取控制 A.11.1 存取控制的營運要求 A.11.1.1 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 A.11.2.2 特權管理 A.11.2.3 使用者通行碼管理 A.11.2.4 使用者存取權限的審查 A.11.3 使用者責任 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 網路存取控制 A.11.4.1 網路服務的使用政策 A.11.4.2 外部連線的使用者鑑別 A.11.4.3 網路設備識別 A.11.4.4 遠端診斷與組態埠保護		

ISO 9001 條文	ISO 27001 條文	ISO 20000 條文	差異說明
	A.11.4.5 網路區隔 A.11.4.6 網路連線控制 A.11.4.7 網路選路控制 A.11.5 作業系統存取控制 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.11.5.5 會談期逾時 A.11.5.6 連線時間的限制 A.11.6 應用系統與資訊存取控制 A.11.6.1 資訊存取限制 A.11.6.2 敏感性系統的隔離 A.11.7 行動計算與遠距工作 A.11.7.1 行動計算與通信 A.11.7.2 遠距工作 A.12 資訊系統獲取、開發及維護 A.12.1 資訊系統的安全要求 A.12.1.1 安全要求分析與規格 A.12.2 應用系統的正確處理		

ISO 9001 條文	ISO 27001 條文	ISO 20000 條文	差異說明
	A.12.2.1 輸入資料確認 A.12.2.2 內部處理的控制措施 A.12.2.3 訊息完整性 A.12.2.4 輸出資料確認 A.12.3 密碼控制措施 A.12.3.1 使用密碼控制措施的政策 A.12.3.2 金鑰管理 A.12.4 系統檔案的安全 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.12.4.3 程式源碼的存取控制 A.12.5 開發與支援過程的安全 A.12.5.1 變更控制程序 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.12.5.4 資料洩漏		

ISO 9001 條文	ISO 27001 條文	ISO 20000 條文	差異說明
	A.12.5.5 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 A.13 資訊安全事故管理 A.13.1 通報資訊安全事件與弱點 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 資訊安全事故與改進的管理 A.13.2.1 責任與程序 A.13.2.2 從資訊安全事故中學習 A.13.2.3 證據的收集 A.14 營運持續管理 A.14.1 營運持續管理的資訊安全層面 A.14.1.1 資訊安全納入營運持續管理過程 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		

ISO 9001 條文	ISO 27001 條文	ISO 20000 條文	差異說明
	A.14.1.4 營運持續計畫框架 A.14.1.5 營運持續計畫的測試、維護及重新評鑑 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 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		
8 量測、分析及改進 8.1 概述 8.2 監督及量測 8.2.1 顧客滿意度 8.2.2 內部稽核 8.2.3 過程之監督及量測 8.2.4 產品之監督及量測 8.3 不符合產品之管制 8.4 資料分析 8.5 改進 8.5.1 持續改進 8.5.2 矯正措施 8.5.3 預防措施	6. ISMS 內部稽核 8. ISMS 之改進 8.1 持續改進 8.2 矯正措施 8.3 預防措施		1.異：無 2.同： (1)內部稽核(ISO 20000 於 4.3 規範 (2)持續改善精神

附件二：CMMI 與 ISO 之比較

CMMI L3			與 ISO 系列比較之相關項目(☆)		
4 大流程領域	22 個子領域/(首字母縮寫)	特殊目標(Special Goal)	ISO 9001	ISO 27001	ISO 20000
1.流程管理類	組織流程定義(OPD)	SG 1 建立組織流程資產		☆	☆
		SG 2 促成 IPPD 管理			
	組織流程專注(OPF)	SG 1 決定流程改善機會			
		SG 2 規劃與執行流程改善			
		SG 3 推展組織流程資產及彙整學習心得			
	組織訓練(OT)	SG 1 建立組織訓練能力	☆	☆	☆
		SG 2 提供必要的訓練	☆	☆	☆
	組織流程績效(OPP)	SG 1 建立績效基準及模式			
	組織創新與發展(OID)	SG 1 選擇改善措施	☆	☆	☆
		SG 2 推展改善措施	☆	☆	☆
2.專案管理類	專案規劃(PP)	SG 1 建立估計值			
		SG 2 發展專案計畫			
		SG 3 取得對計畫的承諾			
	專案監控(PMC)	SG 1 依計畫監控專案			
		SG 2 管理矯正措施直到結案	☆	☆	☆
	供應商協議管理(SAM)	SG 1 建立供應商協議	☆	☆	☆
		SG 2 滿足供應商協議	☆	☆	☆

CMMI L3			與 ISO 系列比較之相關項目(☆)		
4 大流程領域	22 個子領域/(首字母縮寫)	特殊目標(Special Goal)	ISO 9001	ISO 27001	ISO 20000
	整合專案管理(IPM)	SG 1 使用專案的已調適流程			
		SG 2 與關鍵人員協調與合作			
	風險管理(RSKM)	SG 1 風險管理準備	☆	☆	☆
		SG 2 界定並分析風險	☆	☆	☆
		SG 3 降低風險	☆	☆	☆
	量化專案管理(QPM)	SG 1 量化管理專案			
		SG 2 統計化管理子流程的績效			
3.系統工程類	需求管理(REQM)	SG 1 管理需求			
	需求發展(RD)	SG 1 發展客戶需求			
		SG 2 發展產品需求			
		SG 3 分析並確認需求			
	技術解決方案(TS)	SG 1 選擇產品組件解決方案			
		SG 2 發展設計			
		SG 3 實作產品設計			
	產品整合(PI)	SG 1 準備產品整合			
		SG 2 確保介面相容性			
		SG 3 組合產品組件並交付產品			

CMMI L3			與 ISO 系列比較之相關項目(☆)		
4 大流程領域	22 個子領域/(首字母縮寫)	特殊目標(Special Goal)	ISO 9001	ISO 27001	ISO 20000
	驗證(VER)	SG 1 驗證準備			
		SG 2 執行同仁審查			
		SG 3 驗證工作產品			
	確認(VAL) 3	SG 1 確認準備			
		SG 2 確認產品或產品組件			
4.支援類	建構管理(CM) 2	SG 1 建立基準			☆
		SG 2 追蹤並管制變更構項目			☆
		SG 3 建立完整性			☆
	流程與產品品質保證(PPQA) 2	SG 1 客觀評估流程與工作產品	☆	☆	☆
		SG 2 提供客觀的洞察力	☆	☆	☆
	度量與分析(MA) 2	SG 1 安排度量與分析的活動	☆	☆	☆
		SG 2 提供度量結果	☆	☆	☆
	決策分析與解決方案(DAR) 3	SG 1 評估備選方案	☆	☆	☆
	原因分析及解決方案(CAR) 5	SG 1 決定造成缺失的原因			
		SG 2 處理造成缺失的原因			