國立交通大學

資訊管理研究所

博 士 論 文

資訊安全管理系統驗證作業之研究

A Study on the Certification of Information Security Management Systems

研 究 生：方 仁 威

指導教授：黃 景 彰 博士

樊 國 楨 博士

中 華 民 國 九 十 三 年 五 月

目　錄

圖　目　錄

表　目　錄

資訊安全管理系統驗證作業之研究

研究生：方仁威　　指導教授：黃景彰 博士
樊國楨 博士

國立交通大學資訊管理研究所

中文摘要

隨著近年來國內與國外的資訊安全事件層出不窮，造成許多企業組織的重大損失，甚至影響層面已擴及至整個國家社會，世界各國已逐漸體認到資訊安全的重要性，特別是針對關鍵性資訊基礎建設的安全防護議題。國際標準組織面對類似資訊安全事件的一再發生與管理不當等缺失，已於 2000 年前後通過資訊安全管理系統(Information Security Management System，簡稱 ISMS)標準系列，希望從整體性的安全對策著手，思考如何達到保護組織內之資訊的機密性、完整性及可用性，藉由資訊資產的風險分析、評估與處理步驟等程序而達到安全控管、有效降低資訊安全事件發生的頻率及衝擊，進而健全組織資訊安全管理的能力。

在我國提出的「挑戰 2008－國家發展重點計畫」中，已將「政府主要部會實施資訊安全管理系統制度達 50% 」列為建置安全的資訊環境之計畫指標，可見如何建立完善的資訊安全管理制度是政府 e 化當中重大的課題。「沒有百分之百的資訊安全」是眾所皆知的事實，建立整體性的安全對策應是較務實且可行的做法。根基於國際標準、已頒佈之相關規範與類似個案的實際做法為出發點，兼顧安全工程、管理與稽核等方法

論，於資訊安全管理系統驗證作業加以做深入的探討；並進而提出我國與國際接軌之「資通訊基礎建設安全機制」中之資訊安全管理系統之分級處理構想，藉由「規劃、執行、檢查與行動」的 PDCA 工作循環模式，將資訊安全作為制度化及合理化，儘可能降低伴隨在安全事件內的風險因素，以持續改善作業品質及達到防範於未然之目標。

有鑑於此，依據 2002 年 7 月 25 日 OECD 公布的「資訊系統與網路安全指導綱要－朝向安全的文化」，更進一步提出資訊安全管理系統驗證作業中計畫、評估與內部稽核的作法，試圖整合 ISO/IEC 15408、ISO/IEC 17799 與 ISO/IEC 21827 等標準的資訊安全管理系統驗證與認證過程，訂定資訊安全稽核及其工作能力上宜具備之教育與訓練的內涵，提出新的研究觀點，作為未來資訊安全管理系統實作之參考，確保組織的資訊安全及永續經營。

關鍵詞：資訊安全管理系統、資訊技術保證框架、美國(國家)資訊安全驗證與認證過程、資訊安全稽核、資訊安全教育與訓練課程。

A Study on the Certification of Information Security Management Systems

Student：Andrew Ren-Wei Fung　　Advisors：Dr. Jing-Jang Hwang

Dr. Kwo-Jean Farn

Institute of Information Management

National Chiao Tung University

ABSTRACT

Due to the continual occurrence of many information security problem incidents, there have been a lot of disasters in many organizations Many countries are paying more attention to the problems and the Information Security Management System (ISMS) Standard was passed in 2000. The aim of ISMS is to protect the confidentiality, integrity and availability in the organizations. By risk analysis, evaluation and management of the information assets, we cab lower the frequencies of the information security problem incidents and impact so as to improve the organizational information security management capabilities.

Taiwan has brought out “Challenge 2008 – Nation’s Major Focus Plan” in which “The accomplishment of 50% information security management system in any government branch” is an indicator for the set up of secure information. Setting up a complete information security system is helpful to upgrade the country’s overall information and communication environments. In view with that, our study is based on the integrated operation mechanism of ISMS. It’s known that there is no such a thing as

“Absolute information security”. Thus, it is practical to establish an integrated security solution. In this study, I am using the international standards, the related guides and similar studies as my research reference. Then this study also includes the security engineer, management and auditing and ISMS certification process.

In the thesis, I also bring out the leveling process of ISMS for our country to meet the standard internationally. Through a “Plan, Do, Check and Action (PDCA) life cycle model” by making a systematic and rational information security and lowering the risk factors of accompanying security incidents, we can improve the process quality continuously and protect the systems.

Hence, According to the “OECD Guidelines for the Security of Information Systems and Networks —Towards a Culture of Security” published by the OECD on July 25,2002. The planning, evaluation and internal auditing of are studied. In this study, we try to integrate ISO/IEC 15408, ISO/IEC 17799, and ISO/IEC 21827 for National Information Assurance Certification and Accreditation (NIACAP), and formulate the information security auditing capability and the its required education training for the future ISMS implementation guideline to ensure the organizational information systems security and long-term operation.

Keywords: Information Security Management System, Information Security Assurance Framework, National Information Assurance Certification and Accreditation, Information Security Audit, Information Security Education and Training.

誌　　謝

在交通大學資管所漫長的博士班求學歷程中，首先要感謝指導教授黃景彰博士及樊國楨博士，在他們的引領下，使我得以進入資訊安全的研究領域，讓我能就學理面、管理制度、實作可行性及國際標準現行的做法上去深入瞭解資訊安全管理範疇，由於兩位指導教授的豐富學養讓我獲益良多。

此外，要感謝口試委員葉義雄老師、蔡榮隆老師、陳奕明老師、楊中皇老師、陳介山老師及所長陳安斌老師、陳瑞順老師於口試期間，對論文的悉心指導與詳加審閱，使論文內容更臻完善；而所上的游伯龍老師、楊千老師及劉敦仁老師等等，無論是在其專業的領域或者做研究的執著態度上，讓我看到學者風範並益匪淺，在此亦一併提出，向他們致上最深的謝意。

對一位省立竹南高中及國防管理學院資管學系畢業的我而言，能獲得國防部補助全時進修名額，有幸來到交大資管所攻讀博士學位，實屬不易，若非啟蒙恩師果芸上將、碩士班指導教授張克章博士與徐熊健博士，以及昔日長官夏瀛洲上將、丁之發上將、曾金陵上將、唐紀洪中將、謝抗建中將、何遺模中將、黃炳麟將軍、金壽豐將軍與現在的直屬長官林勤經次長等人不斷的鼓功勵與提攜，及黃景彰老師指導的資訊安全實驗室的夥伴們共同研討、腦力激盪與相互砥礪；還有國防部通次室的同仁－雄飛學長、贛彰兄、新正、立勇、成吉、貴允、宏周、旭生以及許許多關心我的師長與好友，如：汪正志老師、賴淑珠老師、泉明學長、

阿德、興華、天華等人的諸多協助，才能造就我得以順利取得博士學位。

最後，要感謝從小到大栽培我的父母、岳父母及其他家人們；尤其是髮妻素琴及一對子女喻萱及梓銘的支持與包容，讓我得以克服重重的挫折，醉心並鑽研學術研究。雖然研究成果不甚豐碩，頗有遺珠之憾，但在這段難得的求學生涯中，兒子梓銘的出世、岳父莊添木及父親方國強的相繼仙逝，都對我造成莫大的衝擊與影響；但終於挺過來了，希望將來在工作表現上能讓人刮目相看。

回首這一段珍貴的學習經驗，已是我人生中取得專業知識的重要來源；更是我未來人生中繼續衝刺的動力泉源。在此，謹以本論文獻給我的父母、岳父母、愛妻素琴及兒女、妹仁華、弟仁武，以及所有協助過我的人，是您們的幫忙、疼惜及愛護，我才能如期完成此博士論文。希望過世的父親及岳父泉下有知，以完此論文告慰兩位老人家在天之靈！

第一章、緒論

1.1 研究動機

在現實的生活中，「安全」被視為是各個議題上至為重要的一環，諸如國家安全、社會安全，乃至於涉及個人健康安全等等……各個議題都備受關注及重視，近來美伊戰爭及SARS傳染病風暴等熱門話題皆與「安全」議題息息相關是最好的印證；而隨著資訊科技的一日千里、個人電腦的普及、網路通信結構的改進以及網際網路(Internet)的風行，促使虛擬的數位世界對我們的影響力正與日俱增。在現今的社會中，每天都有數以百萬計的人們透過網際網路以蒐尋各類所需資訊，各個國家的政府機關及企業組織無不將與本身營運相關的資訊系統視為是核心的資產，愈是倚賴資訊系統愈覺得「安全」議題更加值得正視及面對解決之。

由於資訊科技的蓬勃發展，使得非法入侵與篡改存取電腦資料等違反安全的事件正層出不窮、有增無減的持續發生，如：結合自我複製、緩衝區溢位（Buffer Overflow）與阻斷服務（Denial of Service，簡稱DOS）的紅色警戒（Code Red）網蟲事件等，已造成組織資訊架構的巨大損傷。在網路發達與入侵事件頻傳的今天，「資訊安全」的概念已從實驗室中神秘難懂研究，轉變成社會大眾關心的主要議題。

百分之百的資訊安全是無法達成的目標，為確保通資訊基礎建設的安全性，防禦性資訊系統已成為美、英等先進國家通資訊安全研究的重心之一，防禦性通資基礎建設的安全的目標在於：「從確保通資訊資源的合法存取，到在所有可能遭受通資訊攻擊的階段，提供完整（Complete）、未中斷的通資訊系統運作。」，其功能性典範（Functional Paradigm）可經由下面這三個措施加以說明：

1. 防護（Resistance）
2. 識別（Recognition）
3. 回復（Recovery）

防禦性的技術必須能防止硬體、軟體與使用者資料遭受來自外部或內部的威脅。其牽涉的範圍可能從簡單的金鑰管理機制到複雜的存取控制機制與資訊完整

性機制。這些機制在設計時應考量風險管理（Risk Management）的概念，而風險管理隱含著在通資訊科技的脆弱性（Vulnerability）與利用這些弱點（Weakness）的威脅效力間取得平衡。

快速且正確的偵測與辨識出惡意的通資訊攻擊，對通資訊系統的存活是很重要的。無論防禦措施多完善，在分散式網路運算環境下要修復所有的資訊安全脆弱性是很困難的；譬如，在資源共享的網路上每個人所能接受的風險程度是不同的，整個系統的安全性，宛如一個鍊條，其強韌度將視最脆弱的一節而定。既然無法做到全面性的防護，必須謹慎地注意可能出現攻擊癥兆的任何異常活動報告；若有資訊攻擊事件發生，受攻擊者必須有能力立即降低並復原受損害的資料服務，而正確地瞭解系統在任何時點的狀態才能成功地偵測入侵與辨識非法使用的攻擊。

為確保通資訊基礎建設的安全性，應瞭解組織資訊系統的風險主要是來自於外在的威脅與自身的弱點，組織應著重風險管理機制，擬定一套適當、有效的資訊安全管理制度，藉以提昇我們事前規劃資訊安全政策、事發具從容不迫及隨機應變、事後有妥善萬全的補強措施；以降低可能面臨的威脅及弱點，減少損失，打造一個安全無虞的資訊作業環境。

1.2 研究目的

在資訊軟體產業不斷推陳出新，讓產品快速循環，暴露出的安全問題，一般估計，大約在1,000行程式中有15隻蟲(Bug)，這樣的調查報告換算到有50,000,000萬行程式碼的Windows 2000時，Windows 2000中應該有750,000隻蟲。2001~2002年交際時，微軟公司董事長比爾・蓋茲先生正式宣布：「微軟公司包括Windows在內的所有產品，安全與隱私的重要性，將凌駕各種新功能。」的重大策略轉變。同時，劍及履及，要求微軟公司於2002年2月停止研發新的作業系統軟體，派遣7,000名系統程式師接受軟體安全的特別訓練。以建立商譽的角度來看，微軟公司以公開宣示進行「建立可信賴資訊系統的戰爭」；誓言，「盡力做到像是電力、水力公司及電信業一樣安全的資訊產品。」微軟公司的誓言，間接證實了3~5年之內，類似如「流光」等駭客提供之自動化線上破解工具，仍將經常在數位世界中「攻城掠地」，無怪乎美國國家安全局會堅持要求必須有技術上安全的資訊作業環境，方能進行資訊安全管理系統的稽核。

一般而言，風險評鑑（Risk Assessment）是資訊安全管理系統建置流程的關鍵步驟，風險評鑑的過程是一種：「透過資訊安全政策及資訊安全裝置之選擇，以保護資訊資產免於遭受經由人、設施、硬/軟體、通訊網路、作業系統等之脆弱性而產生安全威脅的傷害。」之方法。在對組織的某個機能進行風險評鑑時，應分析脆弱性有關之安全性威脅，並依據威脅發生後所具有之衝擊影響，將風險等級區分出來；如能善加運用可提昇資訊系統的安全性，亦有助於數位化台灣品質文化之塑造。本論文的研究係植基於國際規範，研析建置一個可信賴的資訊系統作業環境之資訊安全管理系統(Information Security Management System，簡稱ISMS)驗證作業機制，並提出建置ISMS之P-D-C-A工作循環須遵循標準的模式、ISMS稽核訓練的基本課程內涵，以作為ISMS驗證工作時宜具備之知識與技能討論的基礎；另提出整合ISO/IEC 15408及ISO/IEC 17799、ISO/IEC 21827的驗證與認證過程之構想，作為未來ISMS實作時之主要參考。

1.3 研究方法

社會學者們經常透過歸納推理等方法(Inductive method)來進行研究主題的理論建構，一般依研究特性將社會科學研究方法區分為定性研究(Qualitative research)及定量研究(Quantitative research)等兩大類。本論文主要係參考社會科學研究方法中之定性研究，以敘述、了解與闡述等方式來統合本研究的知識，並建立系統化的模式[4,74]；且依據本論文的研究目的、研究動機、欲解決的問題與相關標準、較具代表性的期刊論文、書籍與技術報告等的做法，尋求洞察問題的本質、可能之決策方案及所要考慮的相關關鍵因素，探索並審視研究的論點，以強化本論文研究的可行性及確保論述資料的信度。

本論文之研究方法、步驟及流程將遵照一般社會科學之要求，並滿足研究範圍及限制上之相關要求，其研究架構及流程陳述如圖 1.1 所示：

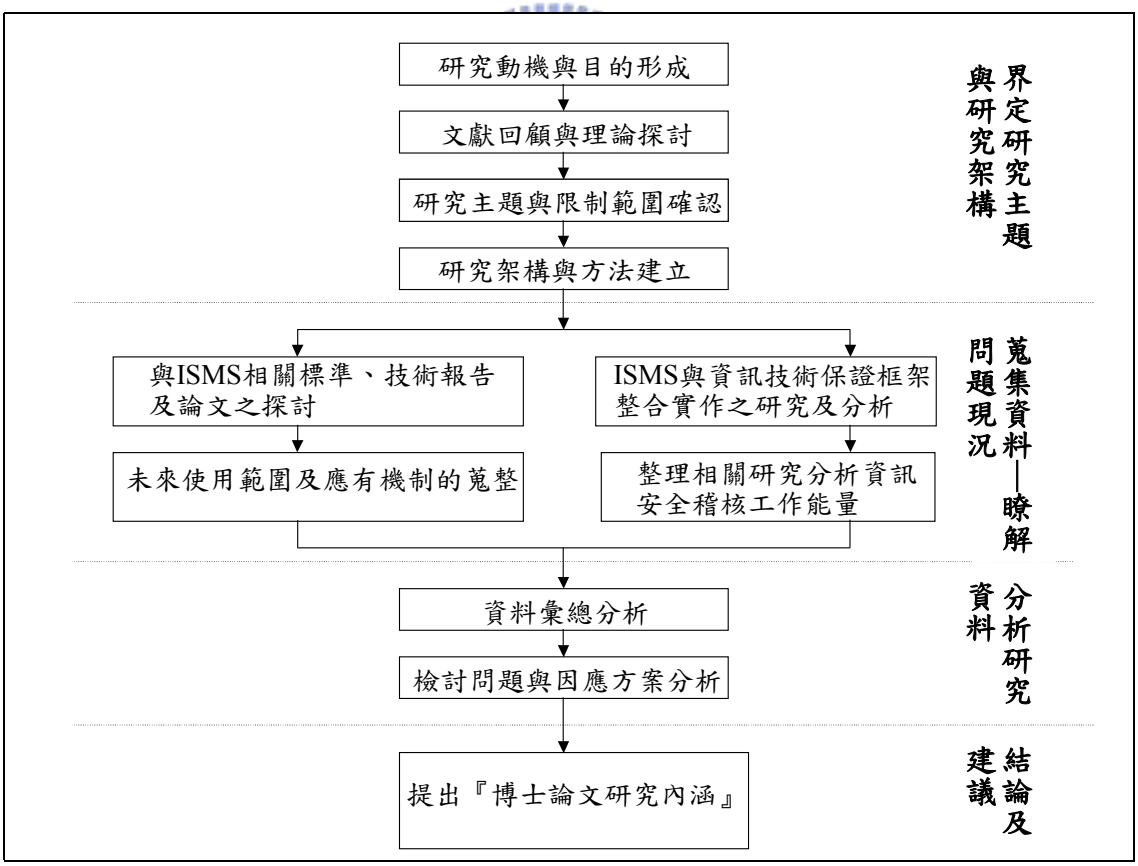


圖 1.1：論文研究之流程架構示意圖

1.4 研究範圍及論文章節概述

「資訊安全管理系統」主要的目的在於定義及提供組織作為保護自身或客戶關鍵資訊之機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)的管制方法。因資訊已被視為是組織中之重大資產，為確保安全的目標可達成，應涵蓋所有的安全議題納入至資訊安全管理制度中，本論文之研究旨在有效的導入實作機制，將資訊安全作為合理化，並儘可能的降低伴隨在安全事件內的風險因素，以防範於未然。

本論文章節結構陳述如下：

第一章為緒論，包括了研究動機、研究目的、研究方法、研究限制範圍與論文章節架構概述等。

第二章根基國際標準、相關已頒佈之規範與類似個案的探究，於資訊安全管理系統驗證作業加以探討，並研提可作為我國與國際接軌之「通資訊基礎建設安全機制」中資訊安全管理系統之分級處理構想[23]。

第三章根基於資訊技術保證框架，探討資訊安全管理系統分級之程序做法，在這部份將整合 ISO/IEC TR 13335 等國際標準在資訊安全管理系統實作過程中所扮演的角色及詳細做法[5]。

第四章簡介美國國家資訊保證驗證與認證過程(National Information Assurance Certification and Accreditation，簡稱 NIACAP)之指導綱要對資訊安全管理系統驗證工作分階段處理之做法，並根基於美國 NIACAP 在通信基礎建設的先導計畫探討資訊安全管理系統之框架；以做為日後建立資訊安全管理系統認、驗證標準規範及作業準繩之主要參考依據[49]。

第五章以資訊及相關技術之控管目標(Control Object of Information and Related Technology，簡稱 COBIT)之作業項目與階段[32]，探究其在安全控管方面的作業模式，並研析資訊安全管理系統內部稽核工作宜俱備之知識與技能，提出資訊安全教育與訓練課程的內容。

最後，在第六章為研究結論與建議，以做為後續研究方向的建議與討論。

第二章、資訊安全管理系統驗證作業研究

今日有關資訊安全可信賴性的策略，均是在不完整的資訊內容下做決定的，標準可以減輕因不完整資訊所引發的困難，因為標準可以減少選擇的範圍而簡化可信賴性供給與需求決策的過程。

近來世界先進國家對資訊安全管理都挹注了不少的資源去投入，且國內行政院已於民國八十八年即依照英國標準協會所訂定的 BS 7799 為範本擬定「行政院所屬各機關資訊安全作業要點」，作為各機關建立資訊安全管理制度的主要遵循依據；故本論文之研究係植基於經濟部標準檢驗局依據國際標準及其相關組織已頒佈之規範與正進行中之工作上的實務需求，於資訊安全管理系統驗證作業加以探討，並研提可作為我國與國際接軌之「建立我國國家通資訊基礎安全機制計畫」中資訊安全管理系統分級處理構想。

2.1 我國通資安全發展現況

近年來世界各國(如：美、英、蘇聯及中國大陸等)皆全力投入推動資訊安全基礎建設[8－10]，再加上「七二九全台大停電」及「九二一大地震」對台灣社會所造成莫大的衝擊，有鑑於此，有關單位於 1999 年春季起意識到通資訊基礎建設安全對國家的重要性，隨即著手規劃「我國通資訊基礎建設安全機制」。於 2000 年 5 月奉中華民國總統指示研題「國家通資訊基礎建設安全機制計畫」，同年 8 月 30 日，總統核定中華民國國家安全會議之「建立我國國家通資訊基礎安全機制」建議書，責成行政院專案辦理，經規劃準備後，為能達成「2008 年均能在安全無慮的環境下使用資通網路環境」之願景目標。

有鑑於此，且由於我國現有之通資訊安全措施均侷限於局部性，並無整體防護、識別及回復能力等，為爭取時效及達成總統的指示，行政院國家資訊通信基本建設專案推動(National Information Infrastructure，簡稱 NII)小組研討相關規劃作業；經審慎研擬，於 2001 年 1 月 31 日召開「國家資通安全會報」第一次會議，期以 4 年的時間，完成「建立我國通資訊基礎建設安全機制計畫」[10]。於 2001 年 2 月 5 日，行政院函送「建立我國資通訊基礎建設安全機制計畫」至各所屬機關並要求切實配合辦理[9]，正式開啟了我國資訊安全發展的新

頁。

前述計畫在行政院正式成案之前，動員人數之多、牽涉層面之廣、民間互動之深等各方面，於我國資訊安全領域均屬空前，未來對資訊安全方面之科技專案研發方向，可能亦將產生深遠的影響。根據計畫內容，國家通資安全會報是由行政院長與副院長分別擔任正、副召集人(自 2003 年 3 月起改由行政院副院長擔任本會報之總召集人)，並由行政院資訊通信發展推動小組(National Information and Communication Initiative，簡稱 NICI)的總召集人擔任執行長，會報下設立綜合業務工作組、危機通報工作組、技術服務中心、網路犯罪工作組、資料蒐集工作組、稽核服務工作組與標準規範工作組等七個組，負責推動國家通資訊安全基礎建設之各項工作，其中標準規範工作組是由經濟部為主要負責單位，而研考會、國防部、交通部、財政部則配合協辦，主要職掌陳述如下：

1. 訂定資通安全技術標準。
2. 訂定各機關辦理資通安全有關作業規範。
3. 規劃建置資通安全檢測技術 (現行國家通資安全會報已將本項職掌刪除)。
4 規劃建置資通安全驗證方法。
5. 規劃建置資通安全認證程序。

為達成前述計畫之工作計畫目標，我標準檢驗局已根基於世界貿易組織烏拉圭回合多邊貿易談判協定(The Results of The URUGUAY Round of Multilateral Trade Negotiations)技術性貿易障礙協定(Agreement of Technical Barriers to Trade，簡稱 TBT)附件 1~3(Annex 1~3)之規範，分以：

1. 資訊技術安全評估共通規範 (ISO/IEC 15408) 系列、資訊安全管理 (ISO/IEC 17799、ISO/IEC TR 13335)、軟體處理評估 (ISO/IEC TR 15504)等標準之制定。
2. ISO/IEC 15408 系列標準中針對不同產品 (例：存取管制、密碼模組、金鑰憑證發行及管理) 之保護剖繪 (Protection Profile，簡稱 PP) 與其之共通性檢測技術之建置。
3. 將 BS7799-2 (Information Security Management Systems Part 2：Specification with Guidance for Use) 訂定為我國家標準，以建置我國通資訊安全之管理系

統驗證作業體系。

4. 依據 ISO/IEC Guide 62、ISO/IEC Guide 65 與 ISO/IEC 17025 之要求，分別建置資訊安全管理系統認證、產品驗證認證之驗證機構以及實驗室認證之認證程序。

推動相關工作中。

2.2 資訊安全管理規範介紹

國際間建立數位社會資訊安全管理驗證的工作，可以上溯至 1988 年 11 月，針對資訊安全專業人員應有的基本知識(Common Body of Knowledge，簡稱 CBK)如何認證呢？專門認證資訊安全專業人員的機構：國際資訊系統安全授證公會(International Information Systems Security Certification Consortium，簡稱 $(ISC)^2$)在英國的索爾斯伯利(Selisbury)正式成立了，通過 $(ISC)^2$ 包含如表 2.1 所示十大類 CBK 的測驗(通常是 6 小時的時間對 250 題選擇題作答)，答對 70%常模分配且已從事三年以上之資訊安全相關工作的人，方取得資訊安全師(Certified Information Systems Security Professionals，簡稱 CISSP)的資格。CISSP 的頭銜並非終身擁有，每三年必須重新評核，通過後方再授證。CIPS(Canadian Information Processing Society)、CSI(Computer Security Institute)、ISSA(Information Systems Security Association)等機構均承認 CISSP 的證書。$(ISC)^2$ 之外，SANS 等機構針對資訊安全專業技術(例：UNIX Security、Intrusion Detection Systems 等)亦有系列認證測試；除了資訊安全專業人員的授證外，資訊系統安全管理規範的國際標準制定工作也在持續推動之中[24,42]，表 2.2 是其發展簡史，表 2.3 是其增修後正式提交 ISO 審議之內容概述。

表 2.1：美國 $(ISC)^2$ 舉辦之資訊安全師證照認證考試範疇 [66]

1. 資訊安全管理實務 (Security Management Practices)。
2. 存取控制 (Access Control Systems)。
3. 通資與網路安全 (Telecommunications and Network Security)。
4. 密碼學 (Cryptography)。
5. 安全架構及模型 (Security Architecture and Models)。
6. 作業安全 (Operations Security)。

7. 應用系統軟體與系統開發 (Applications and Systems Development)。
8. 營運持續運作及災害復原計畫 (Business Continuity Planning and Disaster Recovery Planning)。
9. 法律犯罪調查與倫理 (Law, Investigations, and Ethics)。
10. 實體安全 (Physical Security)。

表 2.2：資訊安全管理驗證簡史

1.1990 年：世界經濟與發展合作開發組織（Organization for Economic Cooperation and Development，簡稱 OECD）轄下之資訊、電腦與通訊政策組織開始草擬「資訊系統安全指導方針」。
2.1992 年：OECD 於 1992 年 11 月 26 日正式通過「資訊系統安全指導方針」。
3.1993 年：英國工業與貿易部頒布：「資訊安全管理實務準則」。
4.1995 年：英國訂定「資訊安全管理實務準則」之國家標準 BS7799 第一部分，並提交國際標準組織（International Organization for Standardization，簡稱 ISO）成為 ISO DIS 14980。
5.1996 年：BS7799 第一部分提交國際標準組織（ISO）審議之結果，於 1996 年 2 月 24 日結束 6 個月的審議後，沒有通過成為 ISO 標準之要求。
6.1997 年：
  6.1 OECD 於 1997 年 3 月 27 日公布密碼模組指導原則。
  6.2 英國正式開始推動資訊安全管理認證先導計畫。
7.1998 年：
  7.1 英國公布 BS7799 第二部分：「資訊安全管理規範」並為資訊安全管理系統認證之依據。
  7.2 歐盟於 1995 年 10 月公布之「個人資料保護指令，自 1998 年 10 月 25 日起正式生效，要求以「適當標準（Adequacy Standard）」保護個人資料。
8.1999 年：增修後之 BS7799 再度提交 ISO 審議。

9.2000 年：增修後之 BS7799 第一部分於 2000 年 12 月 1 日通過 ISO 審議，成為 ISO/IEC17799 國際標準；第二部分未通過審議，將根基於公司治理（Corporate Governance）等原則修正。

10.2001 年：

10.1 2001 年 9 月 OECD 在東京的會議中要求在 ISO/IEC17799 之基礎標準外，應針對個別產業及特性建立適用之資訊安全管理標準。

10.2 英國於 2001 年 11 月公布 BS7799-2：2002 草案（Draft），並公開徵求意見，請各個使用者團體在 2002 年 3 月 31 日以前發表看法後，綜理歸納預定於 2002 年 6 月公布增修後之 BS7799-2 第二部分。

11.2002 年：

11.1 2002 年 7 月 25 日，OECD 公布「資訊系統與網路安全指導綱要：朝向安全的文化」，並取代 1992 年 11 月 26 日通過之版本。

11.2 2002 年 9 月 5 日，BS7799-2：2002 年版遵照 OECD 同年 7 月 25 日頒布之「資訊系統與網路安全指導綱要－ 朝向安全的文化」中的原則修正後正式發行。

11.3 2002 年 11 月，英國之已驗證稽核員登錄國際組織(International Register Certificated Auditors，簡稱 IRCA)公佈 BS7799-2：2002 稽核員訓練課程驗證準則。

11.4 2002 年 12 月 5 日，我國經濟部標準檢驗局分別根基於 ISO/IEC 17799 與 BS7799-2：2002 年版公布中華民國國家標準 CNS 17799 及 CNS 17800。

12.2003 年：

12.1 2003 年 1 月，IRCA 公佈 BS7799-2：2002 稽核員驗證規範。

註：目前除英國之外，已有荷蘭、丹麥、挪威、瑞典、波蘭、捷克、德國、瑞士、愛爾蘭、冰島、加拿大、巴西、澳洲、紐西蘭、日本、南韓、新加坡、馬來西亞、印度、阿拉伯聯合大公國、南非等同意使用BS7799。

表 2.3：BS7799-1(ISO/IEC 17799)內容增修概述

	內容	1999年增修部分
一	安全政策	強化評估鑑核章節。
二	安全組織	1.強化第三者存取控管事項。2.增加委外安全管理章節。
三	資產分類與控制	增加安全標號管理章節。
四	人員安全	增加重大事故學習章節。
五	實體與環境安全	加強辦公室與員工安全的注意事項，同時減少強調專用電腦房的應注意事項。
六	電腦與網路管理	1.詳細規範開放系統安全事項。2.增加公眾可用系統安全章節。 3.改名為通訊與操作管理。
七	系統存取控制	1.強化系統監控事項。2.增加可攜式資訊使用安全章節。
八	系統開發與維護	1.增加密碼技術控管章節。2.增加可信賴資訊系統章節。
九	業務持繼運作規劃	詳細規範安全衝擊分析與計畫撰寫方式。
十	遵行	1.強化法規事項。2.增加事件蒐集方式章節。3.增加密碼控管法規章節。

資料來源：Parkin, R. (1999) BS 7799, in Web Sec'99

資訊安全管理驗證規範之理念與架構和 ISO 14001 等相同，均秉持如圖 2.1 所示之：重點要求、目標管理、風險預防、法規遵循、持續改善之制度化安全理念，執行如圖 2.2 所示之 P-D-C-A(Plan -Do- Check- Action)的工作循環，唯其風險評鑑因涵蓋所有組織，所有部門、地區、人員與活動且其評鑑的合理性與一致性仍是研究的課題[11,37,40,43,66]，相較於 ISO 14001 較為困難，圖 2.3 是資訊安全管理風險評鑑過程之圖示與說明[40]；其中風險分析在界定風險的範圍並做風險的識別及推估(Estimation)、風險評估在訂定可容忍(Tolerability)之風險決策及對策分析、風險減少與控制在做方案的決策並據以建置與稽核作業，圖 2.4 是風險管理作業程序的示意說明[11,37]。一般而言，一個安全事件產生之風險是所有的威脅經由全部的弱點對每一項資訊資產帶來的金錢與生產力之損失，以及對機構的困窘等每一類風險之彙總，表 2.4 是風險等級之定義，表 2.5 是風險等級之示意說明，表 2.6 是以金鑰憑證驗證中心為例說明風險等級；其實作方法可以參考 ISO/IEC TR 13335 [43]。

圖 2.3 中之 4 個威脅在 BS 7799 中精簡為如表 2.7 所示之 C、I 以及 A 的威脅，英國標準協會(British Standards Institution，簡稱 BSi)更進一步將如下所述之符合性(Compliance)要求納入威脅以 L 表示之，以表 2.8 加以詳細闡述說明。使用 C、I、A 與 L 之威脅分類，對能更有效的選擇資訊安全管理系統之控制目標與對策。

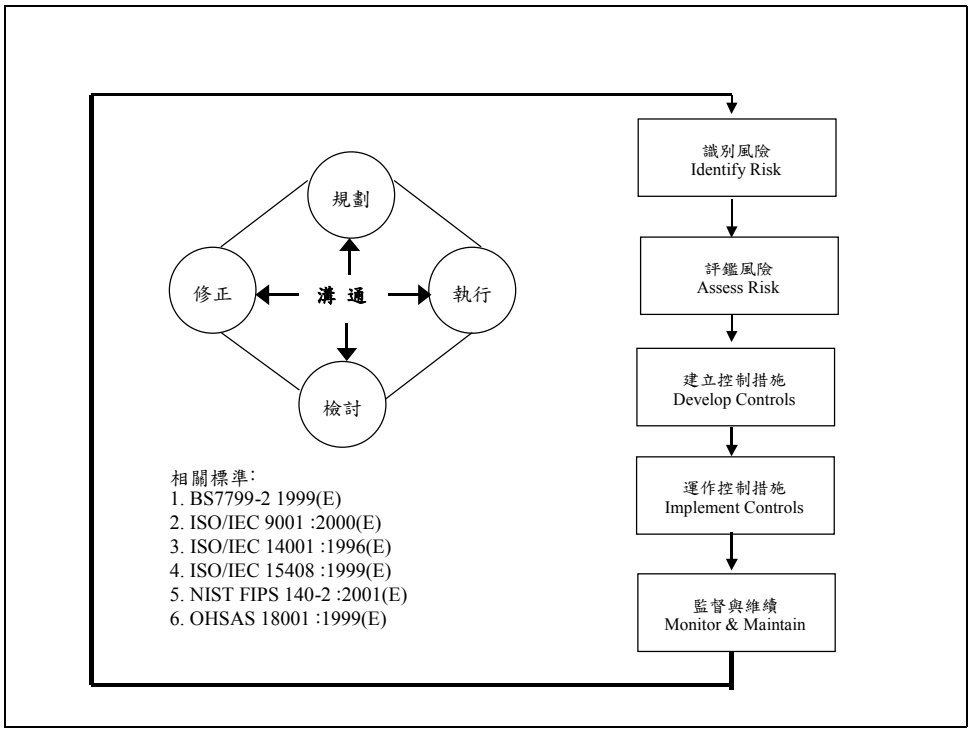


圖 2.1：制度化的安全管理

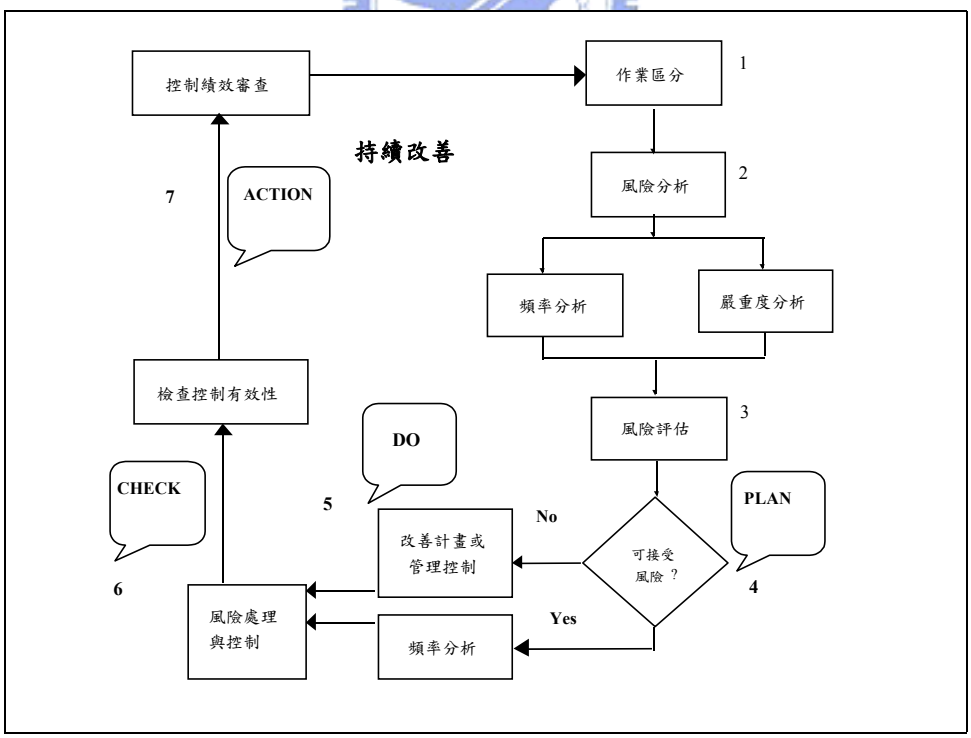
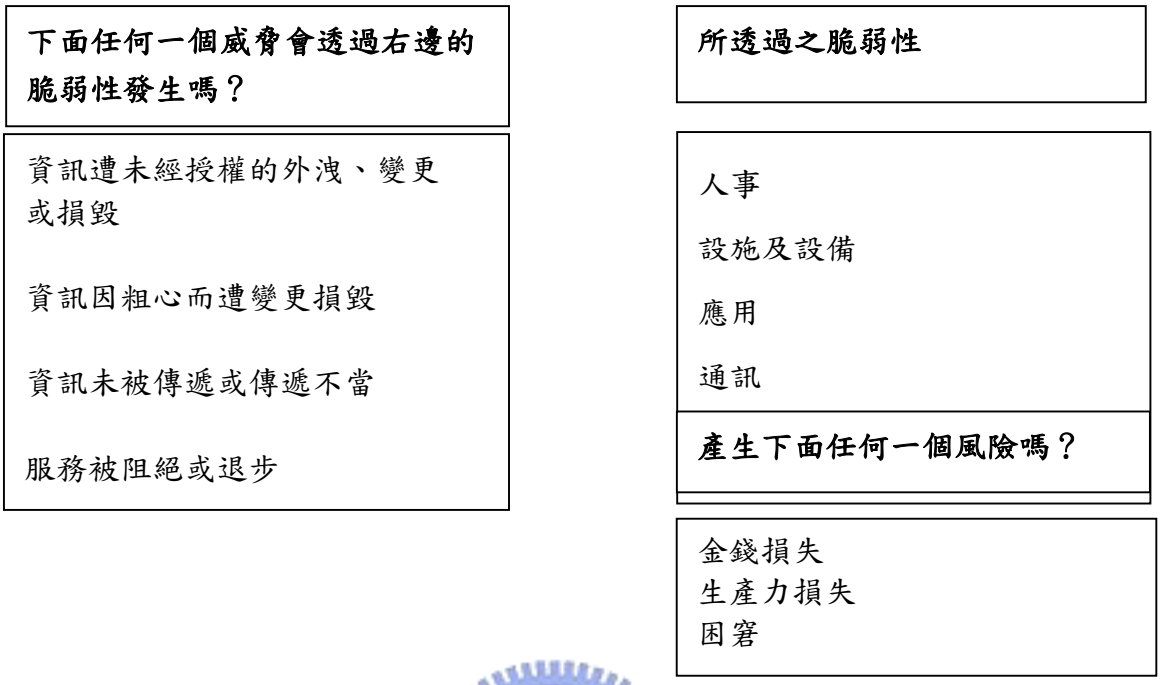


圖 2.2：資訊安全管理系統風險管理步驟示意說明



威脅：與任何營運機能、過程及活動有關的資訊安全性可從許多方式受到威脅。銀行業已辨識出其發生將會損弱對一營運機能產品服務之信心或其整體性，或是驚擾營運永續性的 4 個特定威脅。

下列圖表針對這 4 個威脅逐一說明。

威脅	說明
資訊遭未經授權的外洩、變更或損毀	此威脅為人於正常職責執行中存取或未存取工作過程而使資訊遭意外或故意釋出及遭故意之添補、變更或損毀。
資訊因粗心而遭變更或損毀	此威脅為資訊因不小心、疏忽或意外而遭漏失、添補、變更或損毀。此威脅的發生可能來自人們的行為或不行為、硬體、軟體或通訊故障及天災。
資訊未被傳遞或傳遞不當	此威脅為紙張或電子格式的資訊遭意外刪除及不當傳遞。此包括硬體、軟體及通訊故障與天災。
服務被阻絕或退步	此威脅為整個工作過程或某工作部份發生了出乎計畫外的短期或長期退步表現或可用性不足。

圖 2.3：風險分析與風險評鑑過程圖示及其說明

脆弱性：脆弱性為威脅發生所透過之方法。
下列圖表逐一說明這些脆弱性。

脆弱性	說明
人事	此脆弱性說明員工、廠商及約聘人員。此處理了員工訓練及對部門運作程序及控制之瞭解與遵守度。
設施及設備	此脆弱性說明工作區域及設備的實體安全，及對工作區域及設備的存取。
應用	此脆弱性說明一事業機能所用的資訊處理方法。應用牽涉到對輸入的處理以產生輸出。
通訊	此脆弱性說明資訊在兩個端點之間的電子移動。
環境軟體及作業系統	此脆弱性說明應用程式被研發及執行所在的作業系統軟體及子系統。

風險分類：在進行風險評鑑時，有三個主要風險一定要被考慮。
下列圖表逐一說明這些風險分類。

風險分類	說明
金錢損失	金錢損失的定義為有價值物損失或成本、支出增加。金錢損失風險越高或損失的潛在價值越高，事業機能風險的分類也越高。 舉例： 有價值物－現金 －債券 －資金轉移 增加成本：－發行債券 －遭竊 －不利的法律判決等
生產力損失	當職員無法繼續執行其指定職責或當職責執行須被重複時，生產力損失就會發生。當事業機能無法可用或當結果不正確時，就會發生工作中斷或努力重複。
對機構的困窘	此風險分類考慮影響公信度的情況。機密性、精確性及一致性應亦被考慮。

圖 2.3：風險分析與風險評鑑過程圖示及其說明(續)

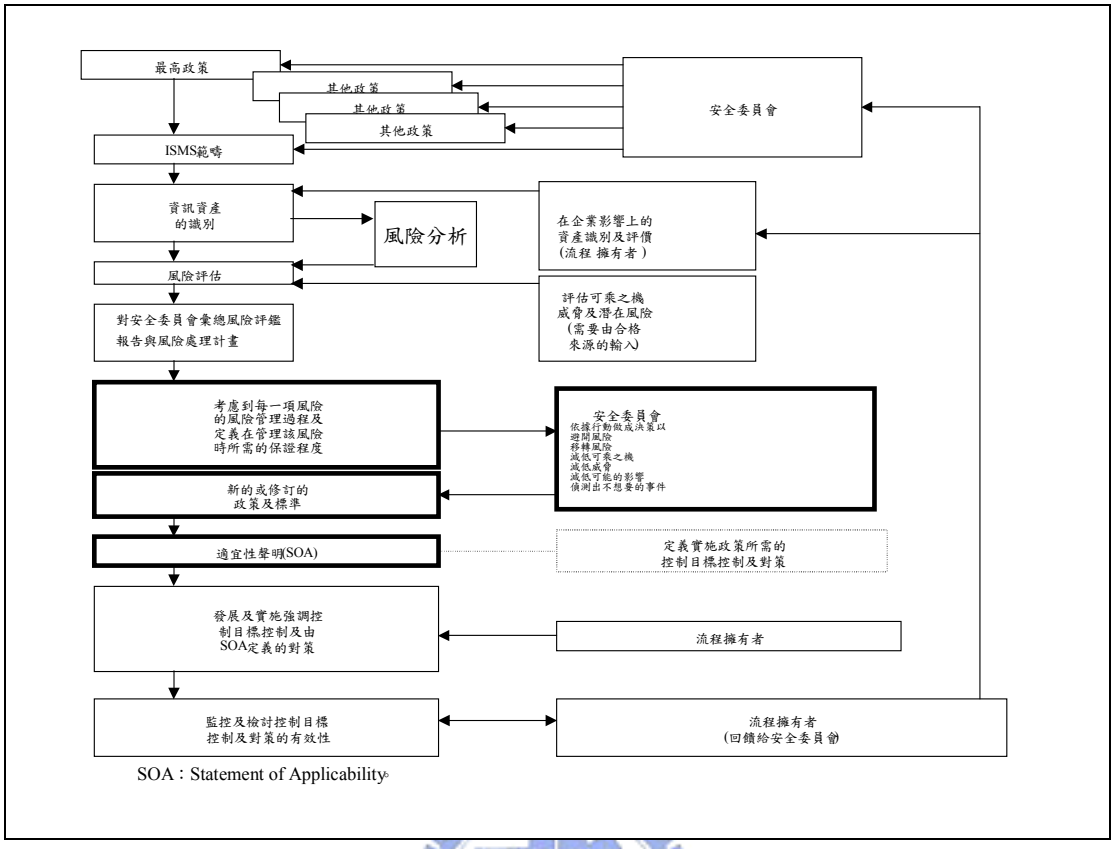


圖 2.4：通資訊安全管理風險評鑑示意說明

說明：這圖是引用並修正 BSi BS7799 之主導評審員課程內容。

表 2.4：IEC(International Electrotechnical Commission) 61508 風險等級

風險等級	可能遭遇的風險	適用範圍例
Ⅰ	可能會有無法容忍的風險	一般個人 電腦系統
Ⅱ	可能會有不受歡迎的風險，只有在該風險所造成的損壞衝擊不重，或改善該風險的代價高於所能避免的損失情況下，尚可容忍此一風險的存在	地方政府之 資訊系統
Ⅲ	只有在改善該風險的代價高於所能避免損失的情況下，容忍此一風險的存在	中央政府之 資訊系統
Ⅳ	只能存在極微小的風險	國家安全之 資訊系統

表 2.5：IEC 61508 風險等級示意

	後果 (Consequences)			
	災難 (Catastrophic)	危機 (Critical)	有限的風險 (Marginal)	無足輕重的風險 (Negligible)
經常發生 (Frequent) (>1)	I	I	I	II
可能發生 (Probable) (1~ 10^{-1})	I	I	II	III
偶爾發生 (Occasional) (10^{-1} ~ 10^{-2})	I	II	III	III
少有 (Remote) (10^{-2} ~ 10^{-4})	II	III	III	IV
不太可能 (Improbable) (10^{-4} ~ 10^{-6})	III	III	IV	IV
罕見 (Incredible) (<10^{-6})	IV	IV	IV	IV

表 2.6：金鑰憑證驗證中心風險等級說明示意

風 險 等 級	事 件 狀 況
災難 (Catastrophic)	驗證中心密鑰或使用者密鑰被破解
危機 (Critical)	金鑰憑證被偽造
有限的風險 (Marginal)	電子信封秘密金鑰被破解
無足輕重的風險 (Negligible)	正確金鑰憑證被拒絕接受

表 2.7：資訊安全具有之特徵

1. 機密性 (Confidentiality，簡稱C)：確保只有經過授權的人才能存取資訊。 2. 完整性(Integrity，簡稱I)：資訊及其處理方法的正確性(Accuracy)與完全性(Completeness)的安全保證(Safeguarding)。 3. 可用性 (Availability，簡稱A)：確保經過授權的用戶在需要時可以存取資訊並使用相關資訊。

表 2.8：資訊安全管理認證對「符合性」之要求事項

符合性 (ISO/IEC 17799：2000(E)，12)：
1. 符合法律要求 (ISO/IEC 17799：2000(E)，12.1)：
目標：不違反刑法、民法、成文法、法規或合約義務以及任何安全要求。 資訊系統的設計、操作、使用和管理要依據成文法、法規或合約安全的要求。 應該向組織的法律顧問或合格的律師諮詢關於具體法律要求的建議。法律要求各國不一，有關在一國創建而傳輸到另一國的資訊(即跨國界資料流程動)的法律要求也不盡相同。
2. 安全政策和技術符合性的評審 (ISO/IEC 17799：2000(E)，12.2)：
目標：保證系統符合組織的安全政策和標準。 應該對資訊系統的安全定期評審。 應該根據適當的安全政策進行此類評審，還應該對技術平臺和資訊系統是否符合安全實施標準進行稽核。
3. 系統稽核因素 (ISO/IEC 17799：2000(E)，12.3)：
目標：最大限度地提高有效性，最大程度地減少系統稽核過程的干擾和對系統稽核過程的干預。 在系統稽核過程中，應該採取適當的控制措施保障作業系統和稽核工具的安全。同時還要求採取保護措施保障稽核工具的完整性，防止濫用。

2.3 資訊安全管理系統認、驗證機制

鑑於我國品質管理及環境管理方面之驗證發展迅速，蔚為風潮，唯發證品質良莠不齊，易對貿易產生負面影響，經濟部特於 1997 年 3 月 5 日以經濟部商檢字第 86350708 號令訂定發布「中華民國品質管理及環境管理認證制度實施辦法」，並於同年 3 月 26 日以經濟部商檢字第 86260244 號令訂定發布「中華民國品質管理及環境管理認證委員會設置要點」，設置中華民國品質管理及環境管理認證委員會專責辦理相關認證業務，並自 1998 年 7 月 30 日起正式受理相關驗證機構與稽核員訓練機構之認證申請。根基於前述辦法第四條之用詞定義：

1. 認證：指主管機關給予書面正式承認驗證或訓練機構有能力執行規定工作之過程或活動。
2. 驗證：指驗證機構授予書面保證稽核員、產品、程序或服務符合規定要求之過程或活動。

為因應諸如職業安全衛生、消防安全設備、資訊安全管理系統等驗證作業之需求，於 2001 年 3 月 14 日以經濟部經(90)認字第 09004601220 號令訂定發布「中華民國認證實施辦法」，除原有之品質管理及環境管理外，一般性之驗證機構(例：資訊安全管理系統驗證機構等)以及產品驗證、檢驗(Inspection)機構之認證工作均由中華民國認證委員會(Chinese National Accreditation Board，簡稱 CNAB)負責；並於 2001 年 3 月 2 日以經濟部經(90)認字第 09003504120 號函修正下達：「中華民國認證委員會設置要點」，公佈周知。換言之，如圖 2.5 所示，自關稅暨貿易總協定(General Agreement on Tariff and Trade，簡稱 GATT)體系之技術性貿易障礙協定中要求各國為安全、衛生、環保或保護消費者等因素，而訂定之技術法規或標準，以及證明相關產品符合這些技術法規或標準之符合性評鑑程序(Conformity Assessment Procedure，簡稱 CAP)，不應對國際貿易造成沒有必要的障礙後。鑑於沒有真確性(Integrity)等安全可靠性質的資訊，電子商務與電子化/網路化政府等均將遙不可及，虛擬世界仍將跳不出文娛和廣告的格局；國際間建立電子化/網路化社會資訊安全機制之業務已於 2001 年 3 月 2 日起，由「中華民國認證委員會」主管；根據標準檢驗局的規劃，於 2002 年 3 月正式起動如圖 2.6 所示之資訊安全管理系統認驗證作業。

資訊系統常因作業形態之不同而對相關安全的要求也不同，譬如：美國聯邦

存款保險公司(Federal Deposit Insurance Corporation，簡稱 FDIC)之監理部門(Division of Supervision，簡稱 DOS)提出之「電子銀行安全與穩健檢查程序」(Electronic Banking Safety and Soundness Examination Procedures，簡稱 S&S Exam.)中，針對金融機構所提供電子銀行業務性質及所面臨風險程度之不同，明定分成如表 2.9 所示之三種不同等級，根基於「資訊風險管理成熟度」與「風險分級管理」管理之概念與參照其他國家如表 2.10 所示的辦法[40,43,58,63,70,73,75]，在我們推動資訊安全管理系統驗證工作時，可以分成如表 2.11 所示之五級，第三級以上與國際 BS7799-2 之驗證接軌，第五級則除 BS7799-2 之要求外，尚需考慮資訊安全管理系統與品質管理系統、環境管理系統等之整合性。在另一方面，在第三級(含)以上，應善用如圖 2.7 與表 2.12 所示之市場與保險的機制，強化如圖 2.8 所示 ISO/IEC 17799 不足之處，圖 2.9 是資訊安全管理防護措施的選擇方法決定程序之參考作業流程[43]。

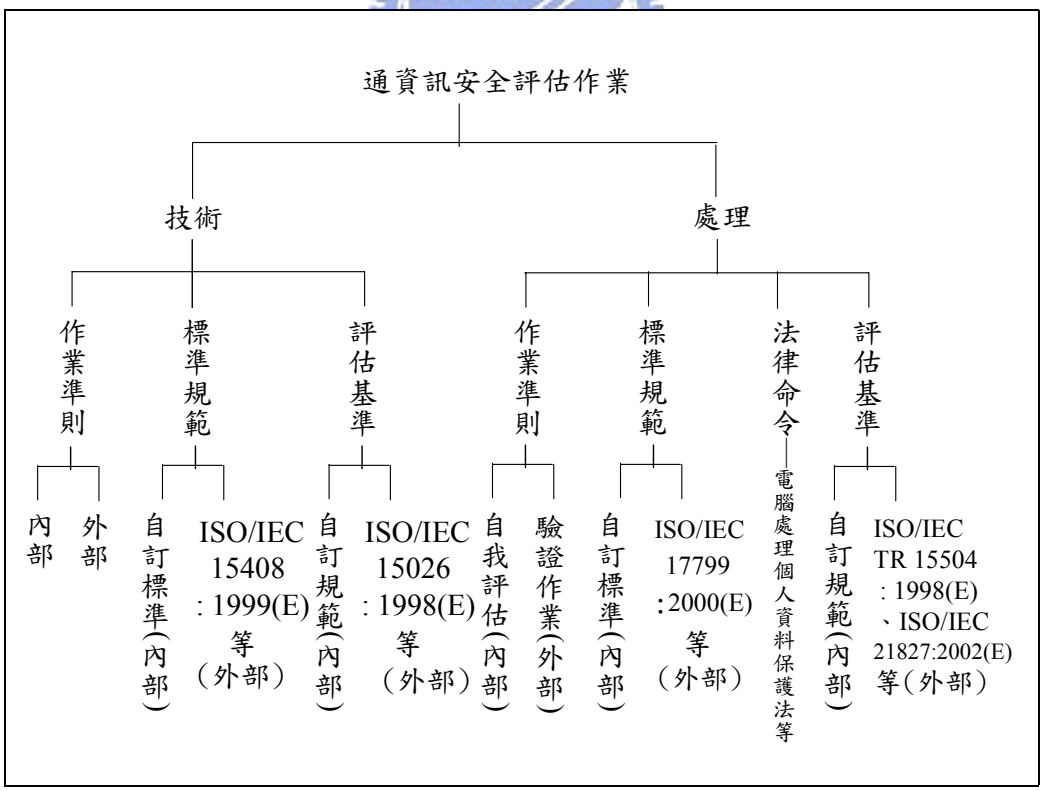


圖 2.5：通資訊安全評鑑作業示意說明

資訊安全管理系統之一般性要求事項： 4.1　資訊安全政策。 4.2　資訊安全組織。 4.3　資訊資產分類管理。 4.9　業務持續性管理。 4.10 遵循法律要求。	人員的要求事項： 4.4　人員安全。 4.5　實體與環境的安全。 4.8　開發與支援過程的安全。
實體與環境的要求事項： 4.5　實體與環境的安全。	資訊技術的要求事項： 4.6　通信與操作管理。 4.7　存取控制的管理。 4.8　開發與支援過程的安全。

圖 2.6：資訊安全管理系統驗證(BS7799-2)強制性要求事項

表 2.9：美國聯邦存款保險公司監理部門「電子銀行安全與穩健檢查程序」分級示意說明[73]

級　別	電　子　銀　行　功　能　說　明
1	單純提供資訊的系統(Information-only Systems)
2	電子資訊轉移系統(Electronic Information Transfer Systems)
3	完全交易資訊系統(Fully Transactional Information Systems)

表 2.10：美國聯邦政府資訊安全管理系統評鑑框架示意說明

第一級準則：敘述安全政策的要素。
1. 目的與範圍。合時宜的安全政策需涵蓋全公司或某資產的所有重要措施及營運項目。這項政策需經主要相關單位核准，且涵蓋安全規劃、風險管理、安全控管措施審核、行為規範、生命週期管理、授權程序、人事、實體安全及環境安全、電腦支援及作業、意外事件規劃、文件記錄、訓練、事件處理、存取控制、查核軌跡等。政策需明訂計畫的目的及施行範圍。
2. 權責。安全計畫包含安全管理架構。這個架構必須有充分的權限和專業人才。資訊安全經理除了管理公司整體，還要負責底下的各層級相關業務。資產保管人、使用人、資訊資源管理人員、資訊處理人員、高級主管、安全主管等的安全責任和行為守則需加以明訂。
3. 遵循法令。政策中需明訂一般法令和特定懲戒措施。
第二級準則：敘述安全流程的要素。
1. 列出控制範圍、明訂組織定位。明訂最新安全程序，涵蓋所有主要設施和作業。安全程序需經主要相關單位核准，且涵蓋安全政策、安全規劃、風險管理、安全控管措施審核、行為規範、生命週期管理、授權程序、人事、實體安全及環境安全、電腦支援及作業、意外事件規劃、文件記錄、訓練、事件處理、存取控制、查核軌跡等。安全流程需明訂主管的定位及是否有其他規定或例外情形。
2. 程序執行內容。安全程序需明訂特殊程序適合的場合、方式、時間、對象及詳細的內容。
3. 分配資訊安全職責和行為守則。安全程序需明訂(1)資產保管人及使用人、(2)資訊資源管理人員及資料處理人員、(3)主管、(4)安全主管等的安全責任和行為守則。
4. 聯絡人及補充資料。安全流程包括其他資料、規定、法令的相關聯絡人。
第三級準則：說明組織如何徹底執行安全程序。
1. 保管人及使用者需瞭解安全政策及程序。安全政策及程序需發給所有相關人員，內容包括系統、應用程式使用規定及行為守則。必須定期確認使用者瞭解並接受自己的安全責任。
2. 正式採用安全政策及程序，並以技術進行控制。平時以自動工具等監控

安全狀況。既有的政策管理事項包括系統日誌檔審核工作、穿透測試及內、外稽核。
3. 安全管理措施涵蓋完整的系統生命週期。從啟始、開發或採購、建置、營運和廢棄等每個階段都要考量到安全問題。
4. 以制訂授權處理程序(認證及驗證)。管理人員一定要經過正式手續批准系統作業並管理風險。
5. 明文記錄的安全定位說明。職務內容說明中的所需技能及安全責任需說明清楚。
6. 員工接受安全程序訓練。教育、宣導計畫需根據職務內容做調整，且應規劃、建置、維護與評估。
第四級準則：測試與檢查之程序及控制。
1. 制定計畫，以便評估安全政策、程序及控管措施是否足夠且有效。評估要求(包括測試種類與間隔時間的需求)要有文件記錄並經過核准、徹底執行。個別控制措施的測試間隔時間及嚴格程度，要根據若該控制措施未有效施行時所造成的風險來決定。至少在重要系統變更或其他風險要素(如所處理的資料敏感程度) 改變時要評估控管措施。就算是風險不高的作業也至少每三年測試一次。
2. 發生安全事件及安全警報時，要有找出弱點所在的機制。平時要有負責分析安全事件記錄的單位，包括可能暴露安全弱點的不正常記錄和可疑活動。另外這些單位要常閱讀 FedCIRC、廠商等組織發出的安全警報。
3. 要有通報重大安全弱點並執行有效補救行為的流程(Process)。這類流程要有測試程序等方法找出的安全弱點、制訂的補救行動計畫、所需資源分配方式、後續確認工作等做成日常報表，讓高級主管審核。另外，應針對若未立刻處置則後果不堪設想的重大弱點制定快速處理程序。
說明：FedCIRC：Federal Computer Incident Response Center (美國聯邦政府電腦事件回應中心)。
第五級準則：說明安全整合計畫的要件。
1. 整個組織要有正在施行的安全計畫，提供符合成本效益的安全措施。
2. 資訊安全是所有資產的工作項目之一。
3. 瞭解安全弱點並已進行管理。
4. 不斷對安全威脅進行評估，且採取控管措施修改安全環境。

5. 有需求時能採取更多或更符合經濟效益的安全措施。
6. 測量安全成本與效益的方式儘可能精確、可行。
7. 建立安全計畫的狀態量測標準(Metrics)，且能符合該標準。

表 2.11：資訊安全管理系統驗證分級要求構想

級　別	驗　證　要　求
1	1. 法律之遵循(BS 7799-2：1999, 4.10.1)。 2. 資訊安全政策(BS 7799-2：1999, 4.1)。 3. 資訊資產分類管理(BS 7799-2：1999, 4.3)。 4. 惡意軟體的控制(BS 7799-2：1999, 4.6.3)。 5. 開發與支援過程的安全(BS 7799-2：1999, 4.8.5)。
2	1. 第一級的要求。 2. 資訊安全之遵循性(BS 7799-2：1999, 4.10)。 3. 資訊安全組織(BS 7799-2：1999, 4.2)。 4. 資訊安全的教育與訓練(BS 7799-2：1999, 4.4.2)。 5. 資訊安全事件與故障的處理(BS 7799-2：1999, 4.4.3)。 6. 業務持續性管理(BS 7799-2：1999, 4.9)。
3	BS 7799-2：2002。
4	BS 7799-2：2002 再加上不同行業如圖 2.8 所示之要求。
5	全面品質(含 BS 7799-2)經營(Total Quality Management，簡稱 TQM)之要求。

說明：BS 7799-2：1999 中之控制項目與 BS 7799-2：2002 附錄(Annex) A 相同，二者之差別在於對資訊安全管理系統 P-D-C-A 要求的不同。

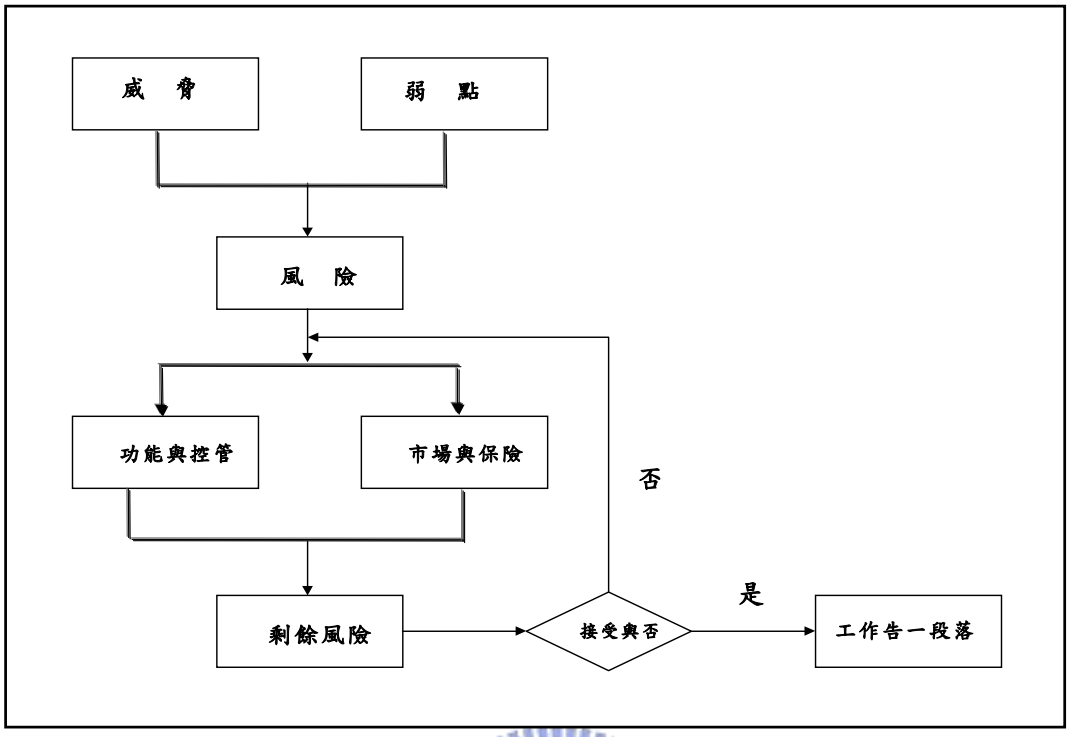
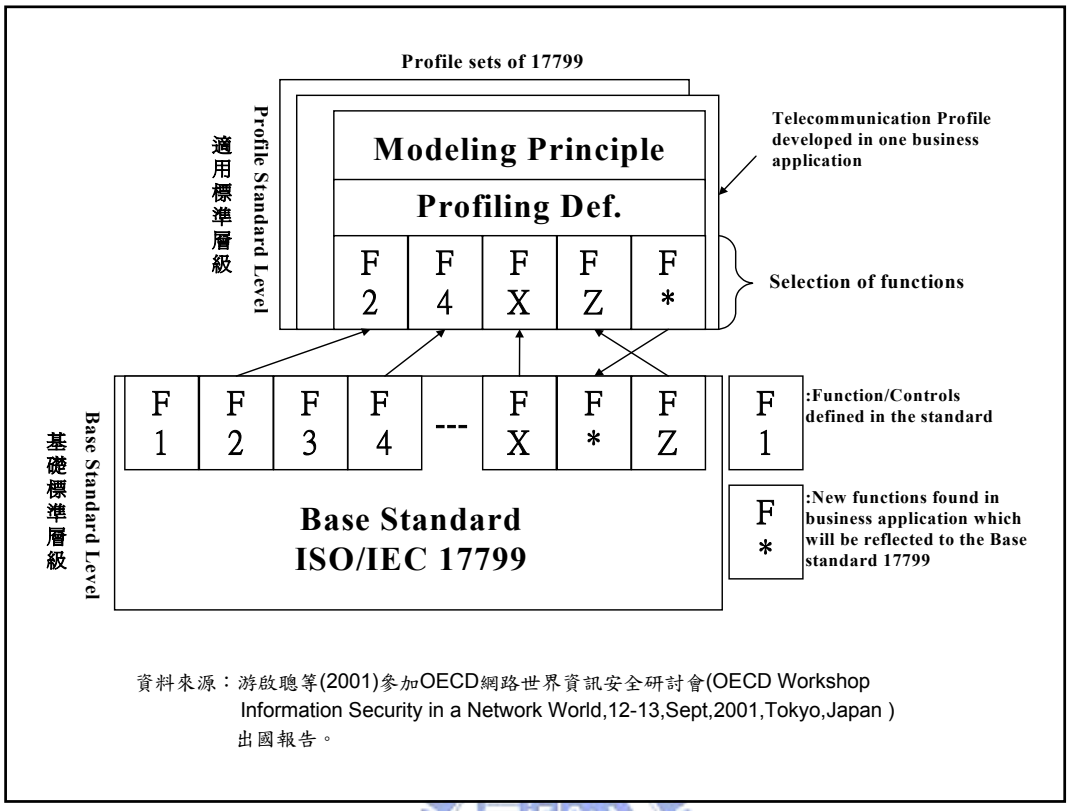


圖 2.7：資訊安全管理系統風險塑模

表 2.12：資訊安全保險市場 [63]

Provider	**Policy**	**Min.**	**Coverage Premium**	**Notes Limits**	**Source**
Cigna Property and Casualty	Secure Systems Insurance	$25,000	$25,000,000	Requires security assessment by approved vendor	Mello 1998
ICSA(International Computer Security Association)	TruSecure	$20,000[1]	$250,000	Requires ICSA security review	Attrino 1998 Weise 1998
J&H March	NetSecure	$5,000	$200,000,000	Requires E-Business Security Assessment[2]	netsecure.com 2000
Lloyds	CIDSI(Computer Information and Data Security Insurance)	$10,000	$50,000,000	Policy has Information Risk Group(IRG)as A required element	Koehn,1998
Reliance National/NRMS	InsureTRUST		$10,000,000	Requires NRMS (Network Risk Mgt Services of Atlanta)review	Weise 1998
Zurich Financial Services Group	E-Risk Protection Program	$4,000	$25,000,000	Requires IBM security certification	O D.Moore 1999

1. This figure covers the cost of the security review.
2. Ubizen has started providing security assessment services to policy holders 18 Feb 2000.



資料來源：游啟聰等(2001)參加OECD網路世界資訊安全研討會(OECD Workshop Information Security in a Network World,12-13,Sept,2001,Tokyo,Japan) 出國報告。

圖 2.8：運用 ISO/IEC 17799 之個別產業資訊安全管理標準方式

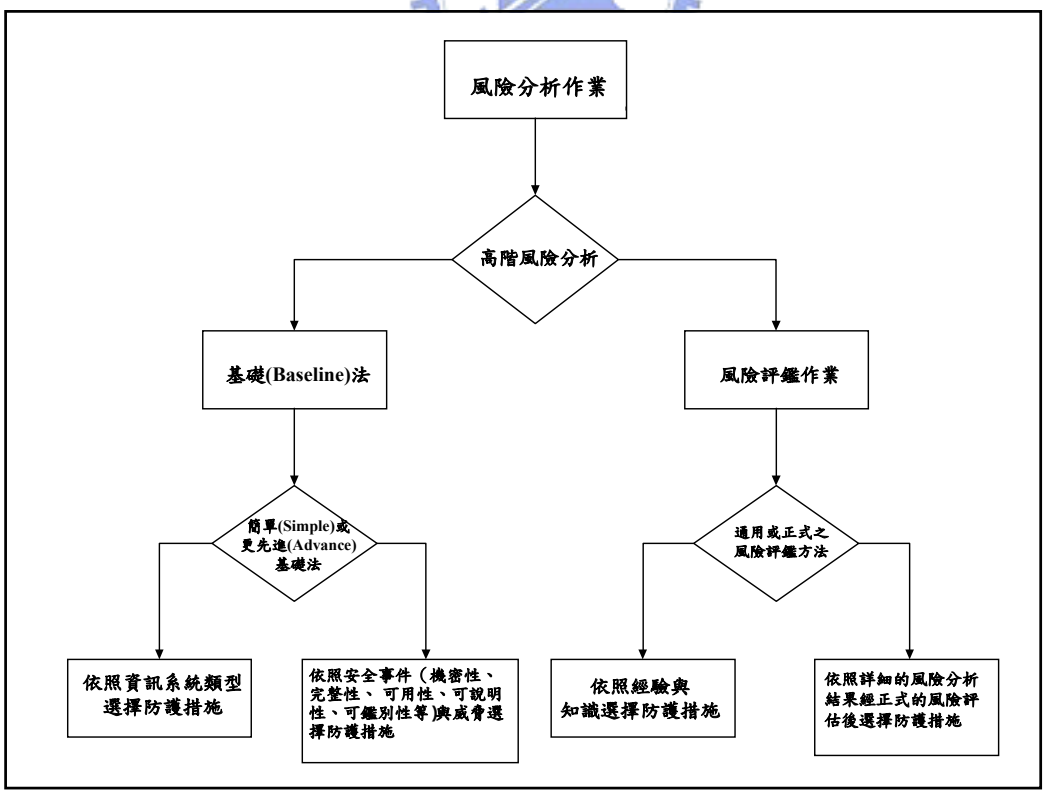


圖 2.9：資訊安全管理系統風險管理作業防護措施之選擇方法

國際上標準化的主要目的在於創造下列各項能促進物品交換、技術移轉的貿易環境：

1. 產品品質及信賴性與價格相符。
2. 保障使用者的安全並促進資源的再利用。
3. 物品、技術與服務的互運性以及彼此之間的接續性。
4. 單純化以減少塑模數，期能擴大生產規模以降低成本。
5. 強化維修保養的便利性與配銷的效率性。

自 1906 年起由電氣技術開始，至 1946 年 10 月 14 日在英國倫敦召開以「促進工業標準的國際統一和調整」為主要宗旨之國際性會議正式成立國際標準組織(ISO)，ISO 於 1947 年 2 月 23 日正式開始運作；因此，10 月 14 日又稱為世界標準日[8]。

所謂標準就是基於公平、公正、便利等觀點做好統一規範、單純化時之必要條件，對於物件、性能、配置、狀態、動作、操作手續、使用方法、工作程序、責任義務、權限概念等均應有一測度判斷的基準；而通稱的規格就是這些標準中直接或間接的有關產品或服務品質之技術上的規範事項。一般而言，規格或標準常因不同類別之組織而有不同的要求，表 2.10 與表 2.11 是其示意說明，表 2.13 是建置資訊安全管理系統 P-D-C-A 工作循環時可引用標準之示意說明。

表 2.13：標準化層次與遵循標準示意說明

風險管理的 層次		須遵循的國際標準
工作循環	分級	
規劃(Plan)		ISO/IEC TR 13335
執行(Do)	1	ISO/IEC 17799
	2	ISO/IEC 17799、ISO/IEC 15408 [41]
	3	ISO/IEC 17799、ISO/IEC 15408、ISO/IEC 21827 [35]
	4	ISO/IEC 17799 與行業別相關之標準(註：以醫療 PKI 為例亦須遵循 ISO/TS 17090 [45]等)
	5	ISO/IEC 17799、行業別標準與整合 ISO 9000 及 ISO 14000 之資訊安全管理系統
檢查(Check)		BS 7799-2：2002
行動(Action)		圖 2.5 中所列出的標準

在表 2.11 中提出了資訊安全管理系統我國(1~5 級)能與國際(3~5 級)接軌之驗證規範，在不同類別之組織中有關資訊技術驗證規範性能標準等之要求等之要求尚待進一步的研究。

九十年代全球文明歷經了重大的轉變，品質、環境和安全衛生管理逐漸朝向一致化與標準化，而相關的國際標準也影響了許多國家經濟的發展和組織管理與經營的方式，ISO 9000 品質管理和 ISO 14000 環境管理系列標準的遵從，是最佳的佐證。2002 年最後一個月，根基於 BS7799-2：2002 年版之資訊安全管理驗證的國家標準已正式公布，成為創建可信賴資訊作業環境的指引，若善加運用，不僅可以提昇資訊系統的安全性，亦有助於數位台灣品質文化之塑造。

2.4 資訊安全事件及事故之管理

國際標準組織(ISO)已正視資訊威脅的重要性，ISO/IEC TR 13335 系列標準強調唯有認清並分析其資訊應用的威脅，始可妥善擬定因應對策及降低運用上可能造成的衝擊。隨著資訊的普及，在現行的資訊安全政策及保護措施下，面臨層出不窮的威脅，仍可能存在殘餘弱點(Residual Weakness)，使得資訊安全變得沒效率；甚至伴隨的組織營運將衍生為具殺傷力的資安事故(Information security incident)，造成難以評估的衝擊。有鑑於此，即將公布之 ISO/IEC TR 18044 中已提及應對資安事件及事故管理須適當加以結構化並事先授權，因此，規劃適切、可行的作法是有其必要性 [47]。

因此圖 2.10「資安事故管理程序」[47]係希望藉此管理程序，以達成以下 4 項預期的目標：

1.有效偵測(如：將事故作分類及有效的歸納)並處置資安事故。

2.適切評鑑並回應已識別的資安事故。

3.經由事故回應時採行之保護措施，將資安事故對組織營運的可能衝擊降至最低。

4.很快的從事故中記取教訓，並進而改進資訊安全保護措施及強化資安事故的管理方案，避免類案事故不斷發生，並防患於未然。

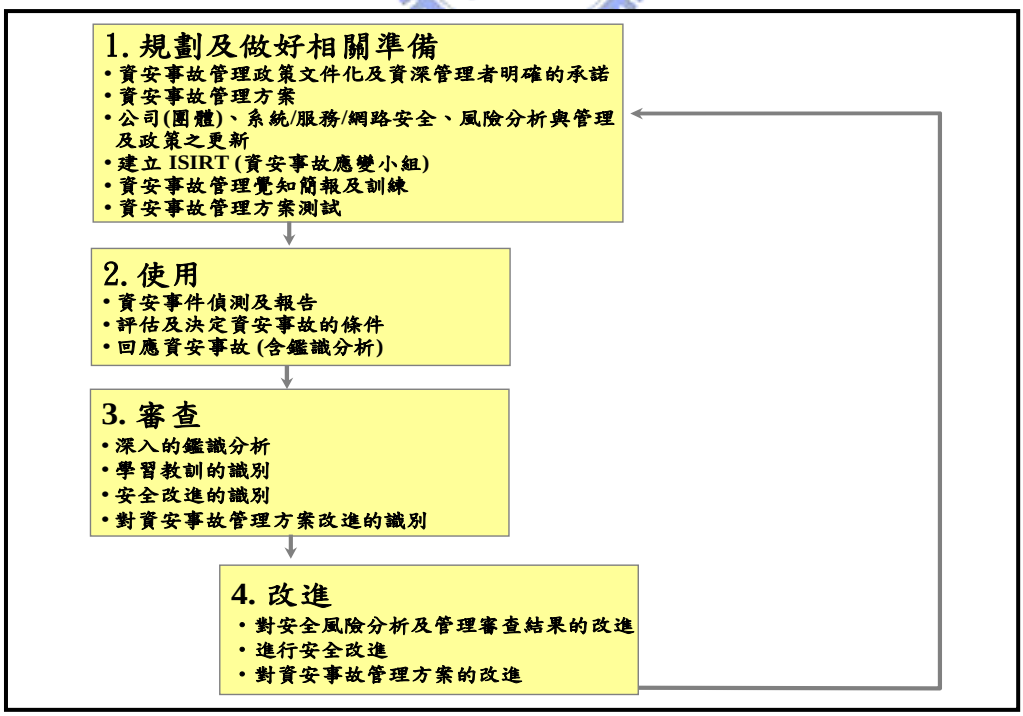


圖 2.10： 資訊安全事故管理程序

有關圖 2.10 對資安事故管理程序中，共包含了 4 個階段(過程)，各階段之主要功能可敘述如下：

1.規劃及做好相關準備：

(1)明訂資安事故管理政策，並予以文件化。

(2)發展資安事故管理方案(或應變計畫)，以支援資安事故管理政策；方案中應涵蓋偵測、報告、評鑑及回應資安事故的表格、程序及支援工具等，另可顯示事故嚴重性的程度。

(3)參考資安事故管理方案，更新組織內各個系統、服務及網路層級的資訊安全及風險管理政策。

(4)建立資安事故的管理組織架構(如：資安事故應變小組(Information Security Incident Response Team，簡稱 ISIRT)，諸如因應惡意碼(Malicious Code)攻擊的應變小組，可藉由組織中資深的管理者帶領具備處置惡意碼攻擊相關領域的專長人員，組成必要之團隊，以解決當前的問題。

(5)透過簡報或專業知識分享機制，使組織內的所有成員建立資安事故的管理共識及加強資安事故的適切訓練。

(6)徹底的測試資安事故的管理方案。

2.使用：

(1)偵測並報告資安事件的發生。

(2)蒐整事件相關的資訊並予以評鑑，判斷各個事件(Event)應歸類為哪一類資安事故。

(3)回應資安事故，針對回應採行的方式可區分為：

- 立即回應。
- 一旦資安事故已獲控制時，可能要花費較多的時間進行事故處置(如：從災難事故中進行復原作業)。
- 若資安事故無法獲得控制時，須建置危機行動(如：建置營運持續計畫)。
- 將資安事故與相關細節通知內部及外部人員(或組織)，俟需要可將事故情況進行深入評鑑(或決策)。
- 將所有行動與決策予以記錄，並進行更進一步的分析。
- 提出解決方案後，再予以結案。

3.審查：當資安事故圓滿解決或結案後，進行下列的審查動作是有必要的。

(1)視需要得進行更進一步的鑑識分析(Forensic Analysis)。

(2)由資安事故中學習並記取教訓。

(3)由資安事故中所學習的教訓結果，識別資安保護措施實作上應改進的部份。

(4)在整個審查作業中重視品質(如：處理的過程、程序、報告表格與組織結構上各項審查作業是確實有效的)，將學習並記取教訓之結果作為不斷改進資安事故管理方案的主要依據，以精益求精。

4.改進：資安事故的管理過程是相當強調緊密的互動，並定期改進(或補強)若干資安元件，這些改進作法可歸納為以下 3 點。

(1)將組織內現行的資安風險分析與管理上的審查結果，做必要之修訂。

(2)將資安事故管理方案做一改進，並予以文件化。

(3)對資安保護措施實作上進行必要的改進，如：特別對起始的保護措施加以改進。

圖 2.10 資安事故管理程序中之「使用」、「審查」及「改進」等 3 階段之關連性及處理流程，可參考圖 2.11 之「資安事件及事故處理流程圖」加以更進一步闡述說明，而對資安事件(或事故)範例應涵蓋基本的規範及執行作為，本論文整理成表 2.14「資訊安全事件報告內容」及表 2.15「資訊安全事故報告內容」，透過兩個表格將報告內容的主要重點做一綜述，將可作為組織中擬訂資安事件及事故之管理方案實作上具體的參考。

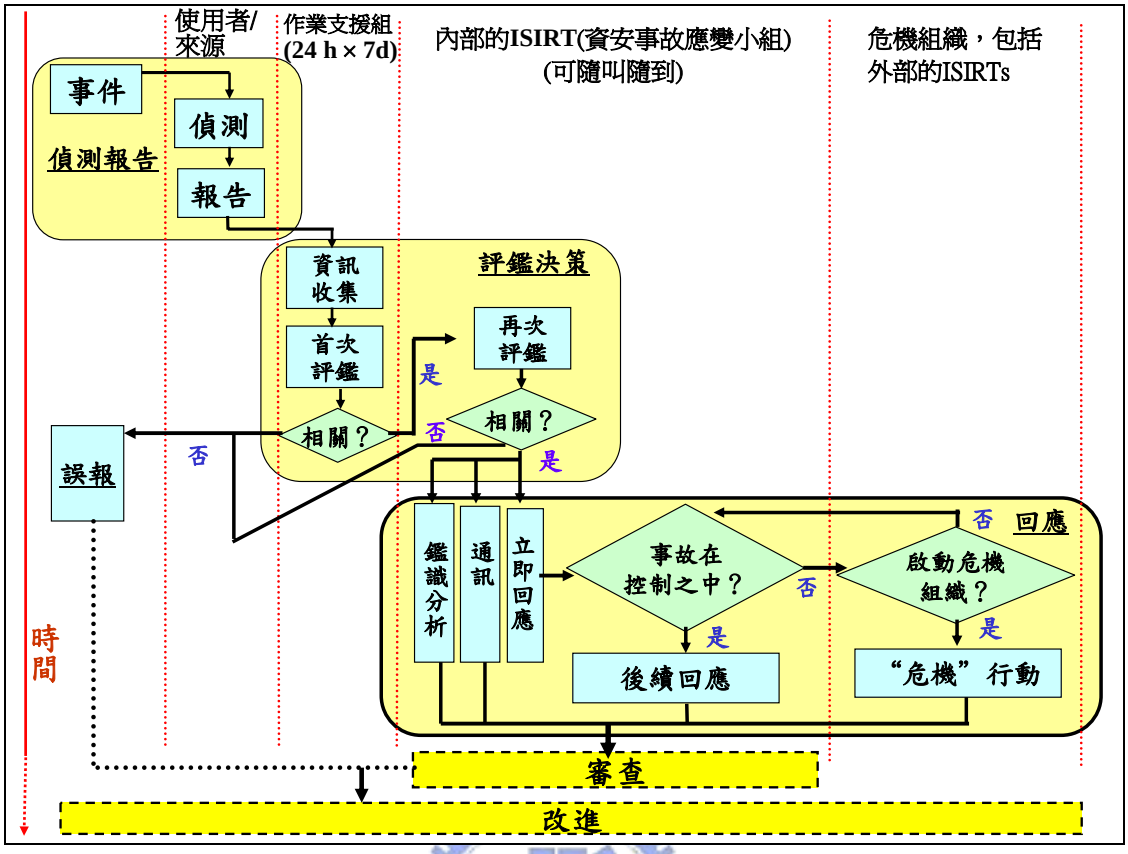


圖 2.11：資安事件及事故處理流程圖

表 2.14： 資訊安全事件報告內容

項次	項目名稱及內涵
1	事件日期
2	事件編號，若適用相關事件或與某一事故有關可加註一識別編號
3	報告人基本資料：含姓名、連絡地址、組織及隸屬部門、連絡電話及電子郵件等個人基本資料
4	資安事件描述：描述事件有關「發生什麼」、「如何發生」、「為何發生」、「受影響之元件有哪些」、「造成營運上不利的衝擊有哪些」、「任何可識別的脆弱性」等
5	資安事件細節：逐一對「事件發生的資料及時間」、「發現事件的資料及時間」、「報告事件的資料及時間」及「事件是否結束」等做說明；有關「事件是否結束」項目應以“日/時/分”方式陳述事件持續了多久。

表 2.15： 資訊安全事故報告內容

項次	項目名稱及內涵
1	事故日期
2	事故編號，若適用相關事件或與某一事故有關可加註一識別編號
3	作業支援小組成員基本資料：含姓名、連絡地址、連絡電話及電子郵件等基本資料
4	資安事故應變小組(ISIRT)成員基本資料：含姓名、連絡地址、連絡電話及電子郵件等基本資料
5	資安事故描述:描述事件有關「發生什麼」、「如何發生」、「為何發生」、「受影響之元件有哪些」、「造成營運上不利的衝擊有哪些」、「任何可識別的脆弱性」等
6	資安事故細節：逐一對「事故發生的資料及時間」、「發現事故的資料及時間」、「報告事故的資料及時間」及「事故是否結束」等做說明；有關「事故是否結束」項目，若事故已結束則採“日/時/分”方式陳述事故持續多久；若事故尚未結束則應陳述截至目前為止事故持續了多久，就現況加以說明。
7	資安事故的類型做一區分：
	(1)可分為「實際的」、「企圖的」、「有嫌疑的」等類型，依資安事故的概況做一分類
	(2)若屬「蓄意的」事故，可將事故型式再細分為「竊盜」、「駭客入侵」、「邏輯滲透」、「詐欺」、「資源不當使用」、「實體損害」、「惡意碼」及「其他」等類型，並補充說明
	(3)若屬「意外的」事故，可將涉及的威脅型式再細分為「硬體失效」、「軟體失效」、「通訊失效」、「水災」、「火災」、「其他自然事件」、「必要服務的漏失」及「其他」等類型，並補充說明
	(4)若屬「錯誤的」事故，可將涉及的威脅型式再細分為「作業造成錯誤」、「硬體維護錯誤」、「軟體維護錯誤」、「使用者錯誤」、「設計錯誤」及「其他失誤」等類型，並補充說明
8	受事故影響之資產描述，應包含「資訊/資料」、「硬體」、「軟體」、「通訊」及「文件」等，對相關資產的序號、許可證號及版本編號做一說明
9	事故對營運造成之衝擊及影響描述，應包含：

	(1)考量資安事故對組織營運活動造成之不利結果，可分為「財務漏失/營運活動作業中止」、「商業與經濟利益」、「個人資訊」、「法律與管理義務」、「管理與營運活動作業」及「商譽受損」等“指導綱要”，依據“值”(可設定為 1 到 10 等級)來記錄事故對營運造成衝擊之層級
	(2)造成之衝擊影響可依「未授權的揭露資訊(違反機密性)」、「未授權的修改資訊(違反完整性)」、「違反可用性」、「違反不可否認性」及「資訊/服務的破壞」等類型，並填寫“值”、“指導綱要” 及其“成本”等資料
	(3)事故復原之成本，可將“值”、“指導綱要” 及其“實際成本”等資料詳細填入
10	事故的解決，含「事故調查起始日期」、「事故調查者姓名」、「事故結束日期」、「衝擊結束日期」、「事故調查完成日期」及「調查報告的參考與位置」等基本資料
11	涉及的人員/犯罪者，可區分為「人」、「組織化的小組」、「合法建立的組織/機構」、「意外」、「無犯罪者」等類型
12	犯罪者描述，可區分為「犯罪/財務的取得」、「政治/恐怖活動」、「消遣/惡意入侵」、「報復」及「其他」等類型；並說明「解決事故所採取的行動」、「規劃解決事件的動作」及「未解決動作(如：其他成員仍要求繼續調查」等
13	資安事故報告結論：就事故整體復原所需總成本及事故的輕、重程度，陳述簡明扼要的具體結論；並由報告起草者、報告起草者之管理者、資訊安全管理者、資安事故應變小組(ISIRT)管理者、網站管理者、資訊系統管理者、警察及其他 ISIRT 等人參與審查並簽章，以示負責，另可彰顯報告之完整及真實性。

現針對圖 2.11 中「使用」階段部份核心的關鍵過程描述如下：

1.在資安事件發生時產生的偵測報告，將來自於系統的自動化或由組織成員、顧客的反映等各種可能的來源；如：來自於防火牆的自動示警功能。

2.組織內的作業支援組可依資安事件的資訊收集結果進行首次評鑑作業，作業支

援組將必須依收集事件結果判斷是否為一資安事故，或是系統誤判所發出的警告；而資安事故應變小組(ISIRT)可依收集事件結果進行再次評鑑作業，專業判斷該事件足以成為一資安事故。一經確認為資安事故，則依立即回應機制處置，並同時展開必要的鑑識分析及通訊行動作為。

3.一旦確認為資安事故，進行立即回應機制處置時，資安事故應變小組(ISIRT)將須審查並判定資安事故是否已在控制之中：

(1)此時若事故已獲控制，則將進一步進行後續回應機制的處置，並同時掌握事故所有資訊，以便辦理事故發生後的「審查」作業。

(2)若事故尚未能有效控制，則須啟動危機行動機制，將組織中相關的人員納編，在集體、有條不紊的運作下，共同處理並控制事故，期使事故問題可有效收斂，避免事故蔓延到一發不可收拾的窘境。

4.在整個資安事故的處理流程中，涉及的人、事、時、地、物皆須詳實的記錄，以便日後可進行後續的深入分析；並確保相關證據被完整且安全的保存下來，一旦未來要進行法律上的追訴或辦理懲罰時，讓證據說話。

5.為確保評鑑及決策作業的正確性，資訊收集及整個資安事故的資料庫須完整且即時更新、備份，以利資安事故管理機制可發揮預期功效。

6.後續回應機制預期應達成之目標為：

(1)動員組織內、外相關的人員，藉由評鑑及決策作業機制，分配安全事故管理行動的準據並律定有關責任。

(2)將正式的處置程序通知所有參與人員確實遵守，含安全事故報告的審查及修改、評鑑損害等作為。

(3)利用指導綱要對資安事故作完整的記錄，後續回應的每項處理步驟須逐一交代並詳實在報告內容中記錄，並同時更新整個資安事故的資料庫，確保資料可達一致性。

國際標準組織(ISO)在面對當前資安事故問題時，亟待須將管理機制加以結構化，因此提出了資安事故管理程序，預期將可達成以下 8 點效益，以健全資訊安全管理體系，俾利安全事故應變及因應更加合理、可行並一體適用：

1.改進資訊安全，並達防患未然之實質解決方案。

2.降低不利的營運活動衝擊，透過結構化活絡的作法，使組織的財務損失、商譽與信用的損害得以降至最低程度。

3.強化安全事故預防的重點，以便將有限的資源集中運用於事故的預防，扼止事故一再上演。

4.藉由明確且有優先順序的調查程序與事故復原動作及基本授權，除有助於確保資料的收集及處理，並可強化證據的完整性。

5.有助於組織內預算及資源的分配，如：運用較不熟練事故處理的員工，以識別並過濾誤報之可能類型；另可提供熟練事故處理的員工在作業上之更需精進的努力方向。

6.結構化的作法可提供已識別威脅類型之各項發生頻率數據，可大幅改進資訊安全風險分析及管理審查的結果。

7.組織內將安全事故文件化後，可將組織內、外真實發生的案例活靈活現的呈現在成員中，使所有人員避免產生「事不關己」或「不可能發生」的心態，正視安全事故的重要性及因無知而產生巨大的恐慌或抗拒。

8.資安事故管理方案的建立，其方案資料將有助於資安政策及相關安全管理文件的有效性審查與後續改進作為，使整個管理作為中改進的資料能不斷地在管理方案中輸入並回饋，使管理方案更臻完善。

第三章、資訊安全管理系統計畫作業研究

資訊技術安全保證是建置資訊安全管理系統(ISMS)的主要核心，在本章中將根基於資訊技術安全保證框架的內容下，探討 ISO/IEC TR 13335：資訊技術－管理資訊技術安全的指導原則（Information Technology －Guidelines for the Management of IT Security，簡稱 GMITS）國際標準在資訊安全管理系統實作過程中之計畫階段的扮演角色及闡述其運作方式。

3.1 資訊技術安全保證框架

為因應數位世界安全的要求，世界經濟與發展合作組織(OECD)自 2001 年 9 月 11 日起，由資訊安全及隱私工作委員會(Working Party on Information Security and Privacy，簡稱 WPISP)之工作小組(Working Group) 的專家群們經過 4 次 6 天的討論後提出草案，再由 WPISP 經過 3 次 6 天的討論送交 OECD 大會(Council)審議，於 2002 年 7 月 25 日公佈「資訊系統與網路安全指導綱要－朝向安全的文化(Guidelines for the Security of Information Systems and Networks：Towards a Culture of Security)」；同時宣佈此指導綱要取代 1992 年 11 月 26 日公佈之「資訊系統安全指導綱要(Guidelines for Security of Information Systems)」。根基於此，英國標準協會(BSi)在 2002 年 9 月 5 日修訂公佈 BS7799-2：2002 版，並在其前言中明述遵照 OECD 之原則訂定在規劃(Plan)、執行(Do)、檢查(Check)、行動(Act)(Plan-Do-Check-Act，簡稱 P-D-C-A)模式建置資訊安全管理系統(Information security management systems－Specification with guidance for use)之規範，經濟部標準檢驗局亦據以制定 CNS 17800 國家標準：資訊技術－資訊安全管理系統規範。

綜覽 10 年來 OECD 對數位社會安全機制的觀點除了在標題中增列網路安全之重要性外，同時將典範轉移至因應、風險管理以及安全設計與實作等如表 3.1 所示；換言之，資訊技術安全保證(Assurance)應為建置資訊安全管理系統的核心工作 [65]。

表 3.1：OECD 資訊系統安全指導綱要原則比較[58,60]

	認知	責任	反應	倫理	民主	風險評鑑	安全設計與實作	安全管理	重新評鑑	多層面紀律	成正比	整合	適時
OECD：1992	∨	∨		∨	∨				∨	∨	∨	∨	∨
OECD：2002	∨	∨	∨	∨	∨	∨	∨	∨	∨				

說明：

1. 10 年來，OECD 將反應、風險評鑑、安全設計與實作、安全管理取代多層面紀律、成正比、整合及適時之原則。
2. 倫理、民主與風險管理已成為 OECD 安全的文化原則之核心。

而資訊技術安全保證緣起於 1983 年起，由國際標準組織(ISO)在德國標準機構支援下，從 ISO 第 97 技術委員會(Technical Committee，簡稱 ISO/TC97)原無國家機構願意負責之資料加密(Data Encryption)工作小組 1 獨立之次級委員會(Sub-Committee，簡稱 SC)，成為 ISO/TC97/SC20 名稱為資料密碼學技術(Data Cryptographic Techniques)，正式展開資訊安全技術國際標準之製訂工作。1989 年，由 ISO 及國際電子技術委員會(the International Electrotechnical Commission，簡稱 IEC)在 1986 年開始合作，1987 年成立之第 1 聯合技術委員會(Joint Technical Committee，簡稱 JTC1)，於 1989 年根基於共同及一般之安全測量標準化已取代僅為密碼學之特殊標準，JTC1 重組 SC20 次級委員會，成立如圖 3.1 所示之資訊技術(Information Technology，簡稱 IT)安全技術(Security Techniques)SC27 次級委員會。ISO/JTC1/SC27 於 1996 年 10 月起開始研訂「資訊技術安全保證框架(A Framework for Information Technology Security Assurance)」國際標準 ISO/IEC 15443(共分 3 部)，其工作文件(Working Document)在 2002 年 3 月起分別交付會員國投票中[46]。根據 ISO/IEC 已交付投票之標準草案，資訊技術安全保證框架

及其建議之標準部分已被接受[35,41]且使用於建置國家級通資訊基礎建設規範中[53]。

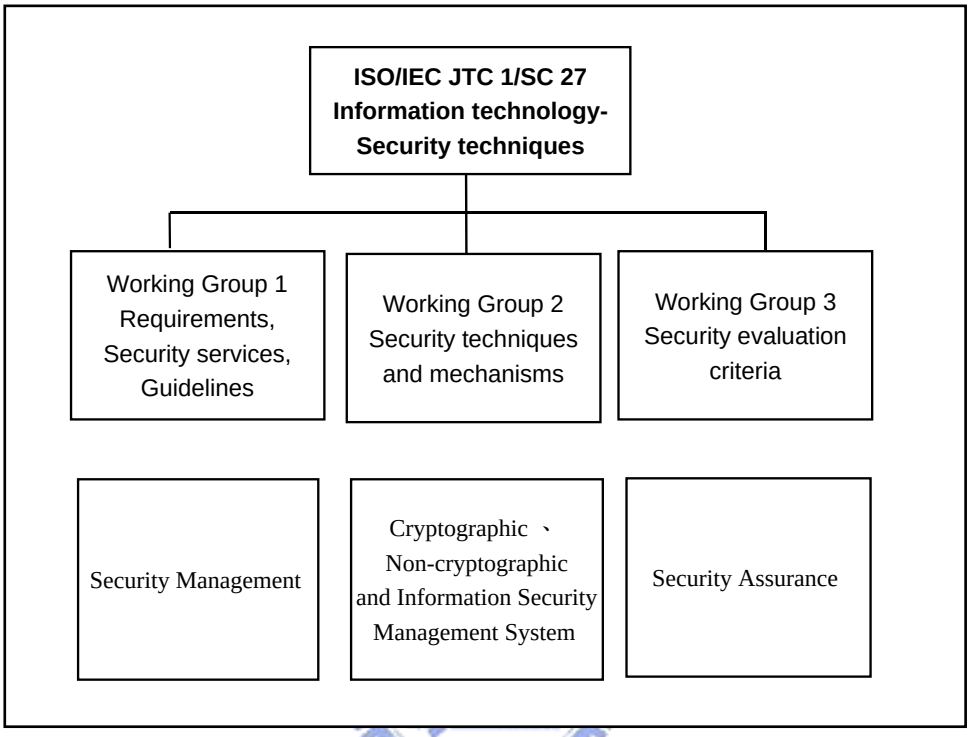


圖 3.1：ISO/IEC JTC1/SC27 組織架構

根基於此，我們將資訊技術安全保證框架國際標準 ISO/IEC 15443 發展的狀況於表 3.2 中陳述，且在表 3.3 中將資訊技術安全保證框架的內容做一說明，配合國際標準 ISO/IEC 15433 已公布的技術報告建議書草案（Proposed Draft Technical Report，簡稱 PDTR）之簡介，可以整理成如表 3.4 所示之產品、過程及環境(在此本論文將資訊技術安全保證方法區分為資訊安全工程、資訊安全管理與資訊安全稽核等三個部份)宜具備之知識（Knowledge）與技能（Skills）的說明；而表 3.5 是表 3.4 的比較分析說明[18,19]。

表 3.2：資訊技術安全保證框架國際標準(ISO/IEC TR 15443)簡介

1. 資料來源： ISO/IEC JTC1/SC27(Krystyna Passia)。
2. 1996 年 10 月 29 日~30 日 ISO/IEC JTC1/SC27 批准發展資訊技術安全保證框架國際標準的計畫。
3. 資訊技術安全保證框架國際標準目前狀況：
   - 3.1 Information Technology— Security Techniques — A Framework for IT Security Assurance：ISO/IEC TR 15443 目前之結構分成：
     - Part1：Overview and Framework (ISO/IEC TR 15443-1)。
     - Part2：Assurance Methods (ISO/IEC TR 15443-2)。
     - Part3：Analysis of Assurance Methods (ISO/IEC TR 15443-3)。
   - 3.2 ISO/IEC 15443 製定狀況：
     - Part1：DTR(Draft Technical Report)於 2003 年 6 月 11 日公布，即將公布為國際標準。
     - Part2：DTR(Draft Technical Report)於 2004 年 2 月 6 日公布，2004 年 5 月 26 日截止投票。
     - Part3：尚為工作草案 (Working Draft)，現為 4th WD：2004 年 4 月 21 日。

表 3.3：資訊技術安全保證框架內容說明

1. 資料來源：ISO/IEC WD 15443: 2004(E)。
2. 保證方法(Approach):
   - 2.1 產品(系統與服務)(例：ISO/IEC 15408)。
   - 2.2 作業(Process)(例：System Security Engineering Capability Maturity Model，簡稱 SSE-CMM)。
   - 2.3 環境(Environment)(人員與組織(Personnel and Organization)) (例：組織部份為 ISO 9000、資訊技術實施部份則為 ISO/IEC 17799)。

3.保證階段(Phase):

3.1 設計與實作(Design and Implementation) (例：ISO/IEC 14598)。

3.2 整合與查證(Integration/Verification) (例： 滲透測試(Penetration Testing，簡稱 PT)。

3.3 複製(Replication) (例：ISO/IEC 9000)。

3.4 轉換(Transition) (例：SSE-CMM)。

3.5 實施(Operation) (例：ISO/IEC TR 13335)。

表 3.4：資訊技術保證框架相關標準應用範疇

保證方法 \ 階段	設計/實作	整合/查證	轉換	實施
資訊安全工程 [產品(/系統/服務)]	ISO/IEC 15288 ISO/IEC 15408	ISO/IEC 15288 ISO/IEC 15408	ISO/IEC 15288 ISO/IEC 15408	ISO/IEC 15288 ISO/IEC 15408
資訊安全管理 [過程(Process)]	ISO/IEC 21827 ISO/IEC TR 15504	ISO/IEC 21827 ISO/IEC TR 13335 ISO/IEC TR 15504	ISO/IEC 21827 ISO/IEC TR 13335 ISO/IEC TR 15504	ISO/IEC 21827 ISO/IEC TR 13335 ISO/IEC TR 15504 ISO/IEC 17799
資訊安全稽核 [環境（/組織/人員）]	ISO 9000	ISO 9000	ISO 9000	ISO 9000

表 3.5：資訊安全保證相關標準比較

標準	目的	方法	範疇
ISO/IEC TR13335	改善資訊技術安全管理的規範	用來達到與維護資訊與服務適當安全等級之方法的指引	安全管理組織
ISO/IEC 14598	軟體技術評估的規範	軟體產品及系統評估規範	軟體產品及系統生產、使用與驗證組織
ISO/IEC 15288	軟體生命週期的規範	用來達到與維護軟體生命週期適當方法的指引	軟體系統生產、使用與驗證組織
ISO/IEC 15408	資訊技術安全評估的規範	資訊產品及系統的安全典範與評估規範	資訊產品與系統生產、籌獲之使用與驗證組織
ISO/IEC TR15504	軟體程序的改善與評鑑	軟體程序的改善模式與評鑑方法	軟體工程組織
ISO/IEC 17799	改善資訊安全管理系統品質的規範	資訊安全管理品質規範的特定要求	資訊安全管理事務性組織
SE-CMM	改善資訊系統或產品工程程序	系統程序規範的連續性成熟度模式與評定方法	系統工程組織
SSE-CMM (ISO/IEC 21827)	定義、改善和評定安全工程的能力	連續性的安全工程成熟度模式與評定方法	安全系統工程組織

3.2 資訊安全管理的指導原則

1996 年 12 月 15 日，國際標準組織（ISO）頒布之 ISO/IEC TR 13335：資訊技術－管理資訊技術安全的指導原則（GMITS），係資訊安全管理系統相關之國際標準中規劃之基石[6,28,38,43,72]。 2002 年 11 月，英國之已通過驗證稽核員登錄國際組織（IRCA）公布之 ISMS 第三者稽核中之稽核員（Auditor）/主導稽核員（Lead Auditor）訓練課程（含測驗）規範，明定 ISO/IEC TR 13335 是其知識類（Knowledge）賦能目標（Enabling Objectives）之一[38]。有鑑於 ISO/IEC TR 13335 之目的在於提供建立 ISMS 的資訊技術指導原則，亦為如圖 3.2 與表 3.6 所示之 ISMS 實作過程中重要的參考規範，其與前章所述的 ISO/IEC 17799 標準就九類資訊安全原則上作一比較[28]，其著重的方向有所不同，其差異性比較如表 3.7 所示。

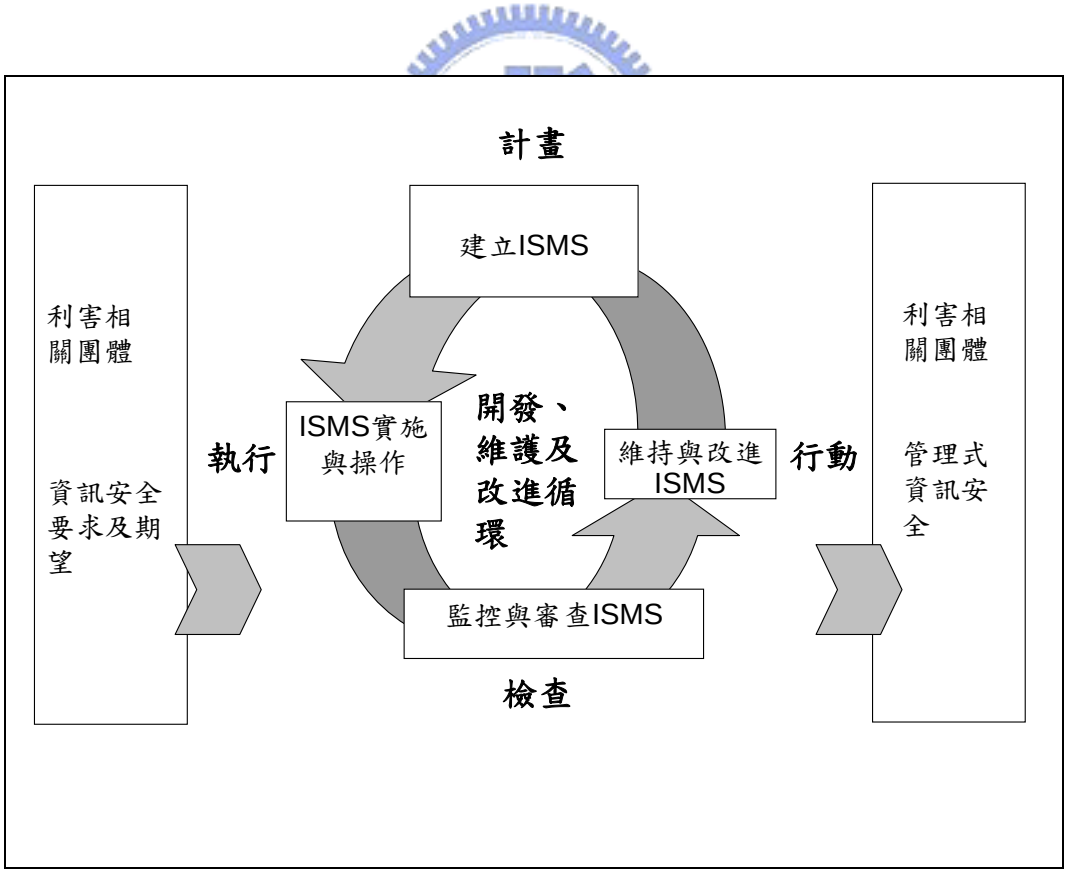


圖 3.2：資訊安全管理系統之處理模式

表 3.6：資訊安全管理系統過程模式在計畫階段實作之示意說明

輸入	輸出
1. 資產 2. 威脅 2.1 威脅等級 2.2 威脅發生的可能性（頻率值） 3. 弱點 4. 脆弱性 5. 衝擊（資產價值） 6. 控制措施標準	1. 安全政策與安全目標之書面聲明 2. ISMS 範疇 3. 風險評鑑報告 4. 風險處理計畫 5. 資訊安全管理系統控制措施 6. 適用性聲明書

表 3.7：ISO/IEC TR 13335 及 ISO/IEC 17799 於資訊安全原則上的差異性比較

資訊安全原則 (Information Security Principles)	ISO/IEC TR 13335	ISO/IEC 17799
法規與合約之遵循	V	V
使用者的認知與教育	V	V
惡意程式之預防與偵測		V
營運持續規劃	V	V
系統發展與架構	V	
風險管理	V	
人員議題	V	
委外管理	V	
事件處理	V	

管理資訊技術安全的指導原則自 1996 年 12 月 5 日公布第 1 部分起，至 2001 年 11 月 1 日公布第 5 部分方告一段落，其第 1 部分、第 2 部分、第 3 部分、第 4 部分及第 5 部分則分別介紹管理資訊技術安全之概念與模型（第 1 部分：Concepts and models for IT Security）、資訊安全的管理與規劃（第 2 部分：Managing and planning IT Security）、資訊安全的管理技術（第 3 部分：Techniques for the management of IT Security）、安全防衛的選擇（第 4 部分：Selection of Safeguard）以及對外部連結的安全防衛（第 5 部分：Safeguard for External Connections）等，且分別於 1996 年、1997 年、1998 年、2000 年及 2001 年完成整個系列技術性報告，以作為爾後各個企業組織制訂資訊安全管理程序之主要參考方針。在 ISMS 日益重要的 21 世紀，GMITS 第 1 部分提出之如圖 3.3 所示之安全元件的關係與圖 3.4 所示之風險管理的關係，使企業組織內的高階管理決策者得以據此擬訂其資訊安全的主要目標、戰略及相關方針，作為管理資訊技術安全之基石；其中圖 3.3 強調了現行企業組織內存在了許多重要的資訊資產，而一般是以資訊資產的重要程度來分析風險，各類資產則存在著數種的脆弱性，但若威脅不存在便不需要保護措施予以因應，是故為了保護資產、降低威脅的影響效果而選擇可行的對策，若此時仍存在著某些殘餘風險是被企業組織所容許的，則採行的因應對策便符合企業的需求。另 GMITS 第 2 部分提出如圖 3.5 所示之建立 ISMS 的框架，依舊是管理 IT 安全企劃工作的藍圖，據以闡述其有關資訊安全之管理與規劃的各個活動具體內容及組織內對應的職責；如表 3.8 等所示之 GMITS 第 3 部分附錄 E 提出的風險分析方法，在 ISMS 風險評鑑實作中，目前仍是普遍使用之工具。

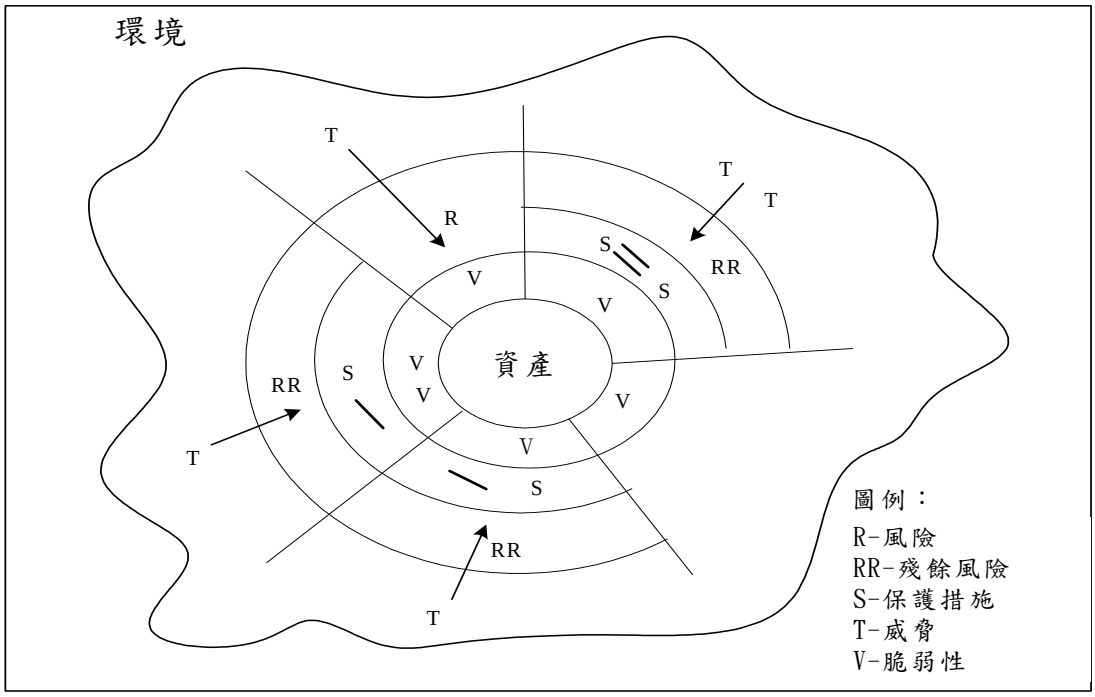


圖 3.3：資訊安全元件的關係

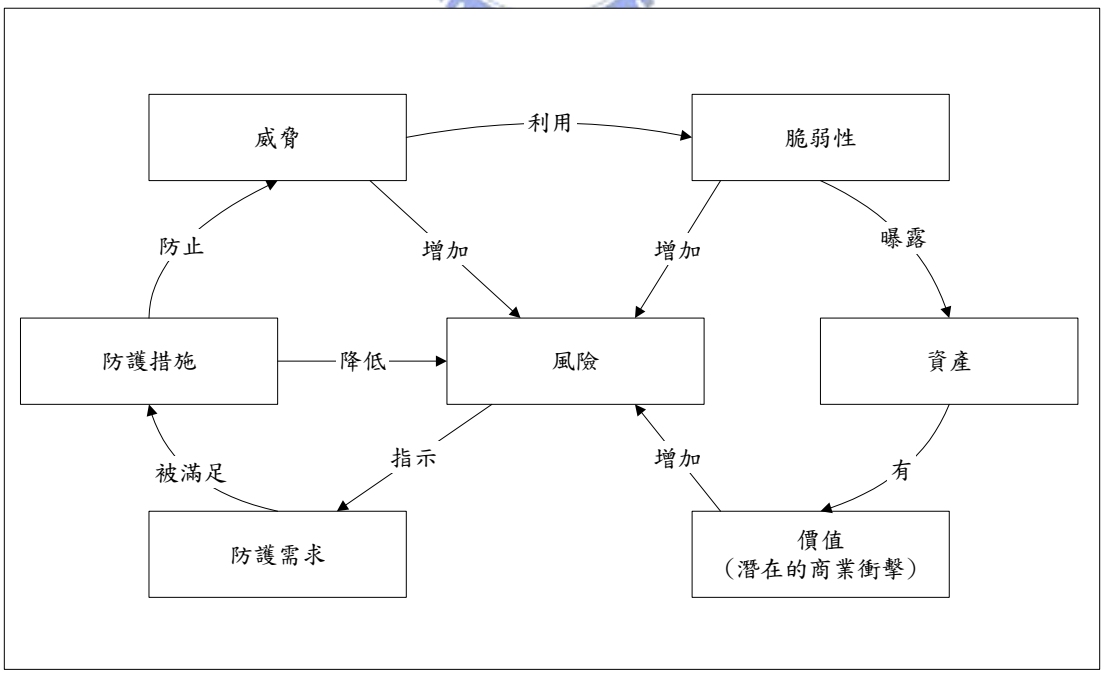
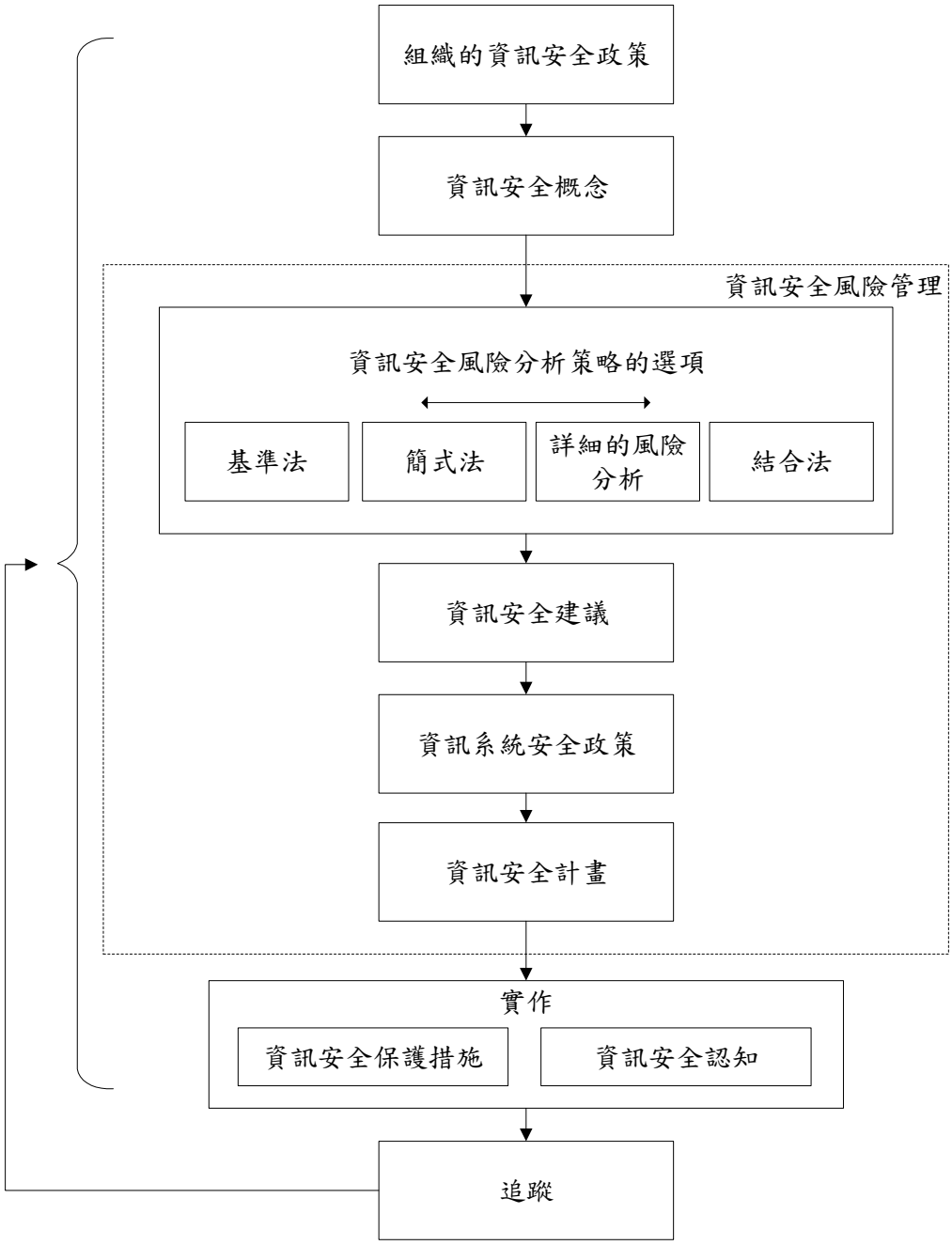


圖 3.4：資訊安全風險管理的關係



說明：ISO/IEC TR 13335-2:1997(E) 此圖中之資訊係指資訊技術（Information Technology，簡稱 IT）。

圖 3.5：資訊安全安全計畫和管理概要

表 3.8：資訊安全風險分析方法之一

	威脅的等級	低			中			高		
	脆弱性的等級	低	中	高	低	中	高	低	中	高
資產價值	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

2000 年 3 月 1 日公布之 GMITS 等第 4 部分探討如何選擇管理資訊技術安全之保護措施及其選擇方法，同時提供：

1. 資訊技術－資訊安全管理之作業要點（CNS 17799/BS7799-1:1999）。
2. ETSI 基本安全標準特性與機制（法國）。
3. 資訊技術基準保護手冊（德國）。
4. NIST 電腦安全手冊（美國）。
5. 醫療資訊：醫療資訊系統的安全歸責與保護。
6. 銀行及相關金融服務業資訊安全指引（CNS14644/ISO TR 13569）。
7. 保護未在正式機密法規涵蓋之敏感資訊－電腦工作站的建議。
8. 加拿大資訊技術安全工作手冊（加拿大）。

備考：CNS17799（ISO/IEC 17799）[13] 是根據 BS7799-1:1999 修改，唯二者幾無實質上之差異。

八種各國與業別之 ISMS 參考文件，表 3.9 是行政院「國家資通安全會報」整合各部會專責單位共同執行「建立我國通資訊基礎建設安全機制計畫」要求遵循 CNS 17800 [14] / BS7799-2:2002 附錄二中規範性控制目標與控制中識別與鑑別項目之 CNS17799 與 GMITS 中其他標準於使用時的比較及示意。在另一方面，如何選擇 ISMS 防護措施的方法 GMITS 亦提出了如圖 3.6 與圖 3.7 所示之決策樹的選擇方案。

表 3.9：資訊技術之識別和鑑別（Identification & Authentication，簡稱 I&A）

	CNS 17799 (ISO/IEC 17799)	ETSI 基本安全標準特性與機制	IT 基準保護手冊	NIST 電腦安全手冊	醫療資訊系統的安全歸責與保護	CNS 14644 (ISO TR 13569)	電腦工作站的建議	加拿大手 IT 安全工作手冊
1.I&A 基於使用者所知	92.3,9.3.1, 9.4,9.5.1	4.2.1,5.2.1 附錄 A	M4	16.1	*.3.2.1	7.2.1,7.2.2	6.2	16.1
2.I&A 基於使用者所有			--	16.2	*3.2.1		6.2	16.2
3.I&A 基於使用者身分			--	16.3	*3.2.1		6.2	16.3
*代表在 6 和 11 之間的任何數字。								

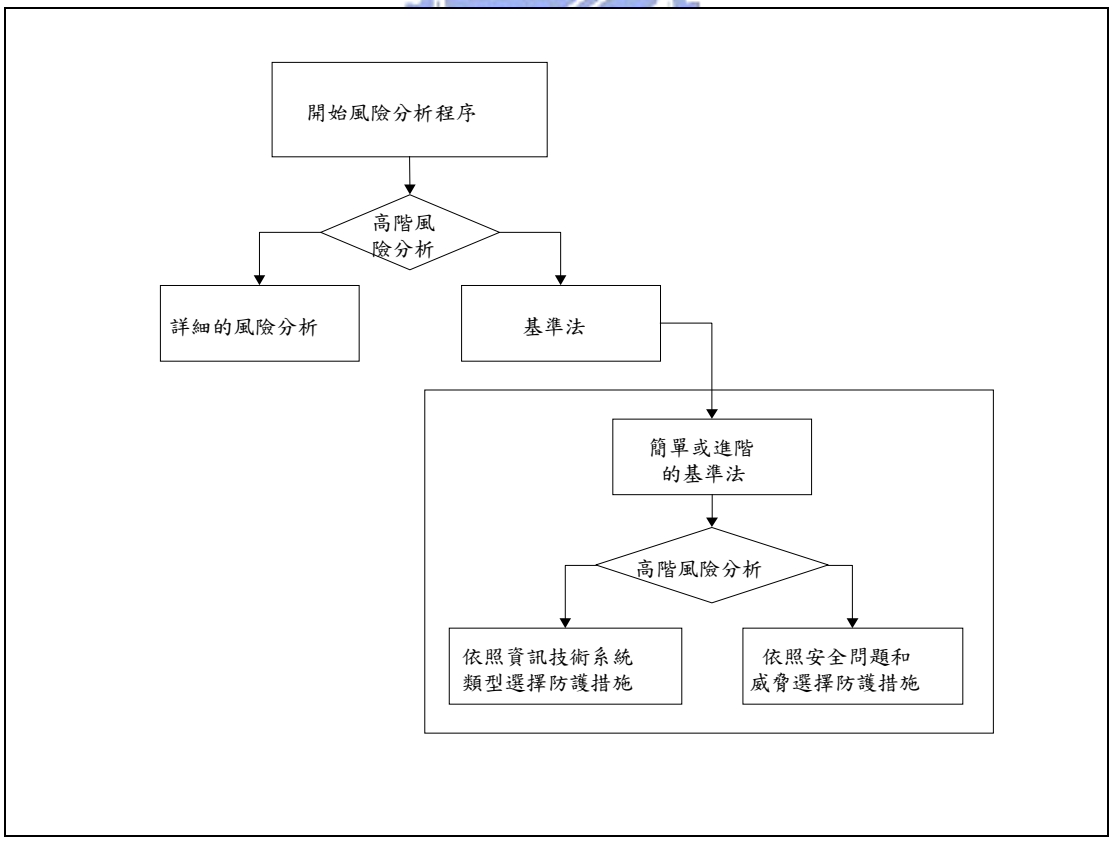


圖 3.6：資訊系統防護措施之選擇方法

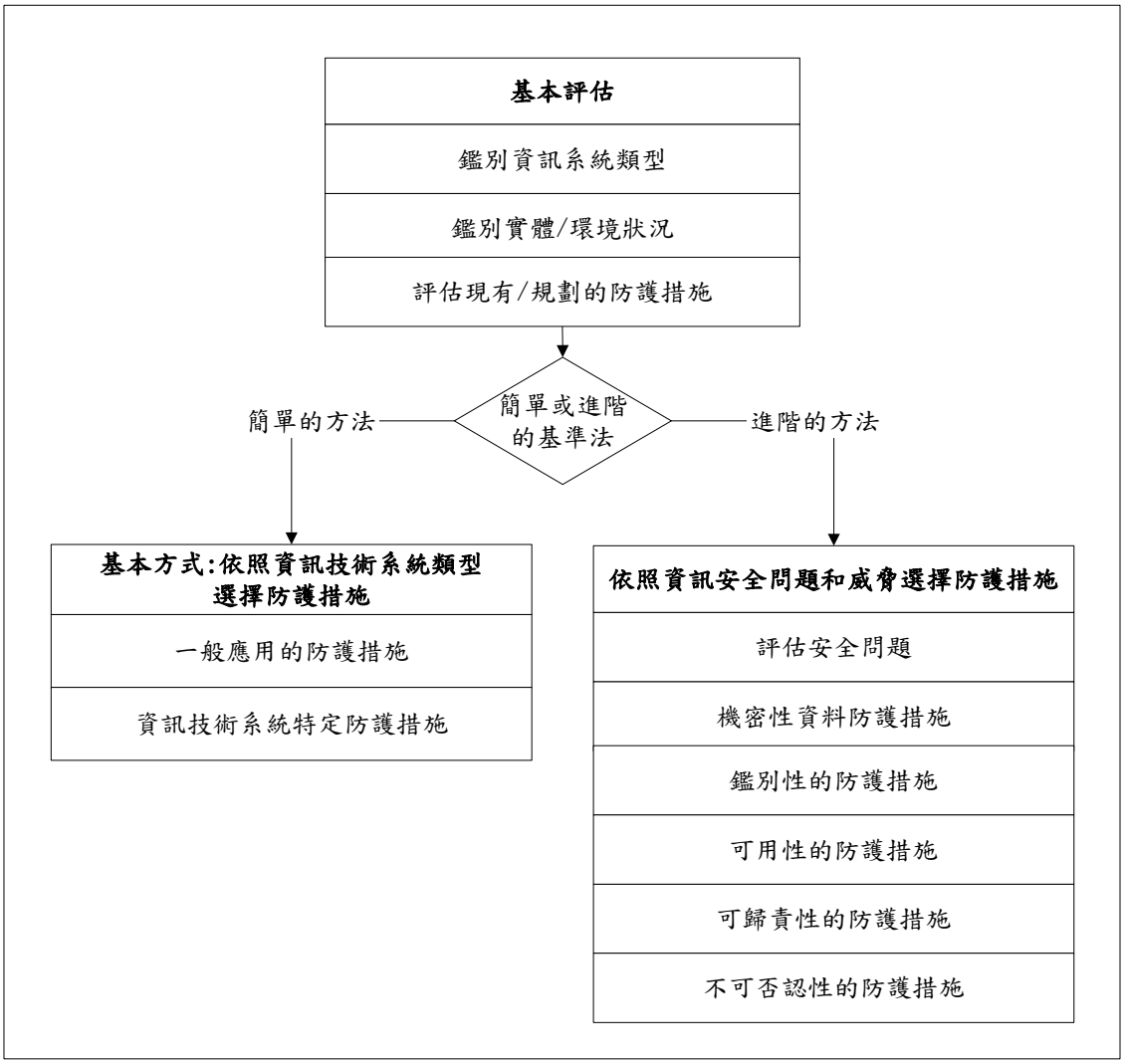


圖 3.7：依照資訊系統類型或依照安全問題與威脅選擇防護措施

3.3 網路安全管理指引

於 2001 年 11 月 1 日公布之 GMITS 的第 5 部分－網路安全管理指引(Management guidance on network security)則在描述保護外部聯結、服務，並使資訊系統免於威脅、風險，且減少弱點之安全防衛的選擇指引，以作為系統之安全管理人員(Administrator)從事網路安全管理的指導方針，這份網路安全管理指引係運用於建立網路安全需求時，須考量到通訊相關要素應如何進行識別與分析的整個過程。這份指引係植基於第 4 部分的安全保護措施及其選擇方法為基礎，針對連結至通訊網路上的安全性應如何識別適切的安全防衛措施區域並同時提供指示作一介紹，然並不涵蓋技術性的安全防衛措施區域(Technical safeguard areas)之細部設計(Detailed design)及實作面(Implementation aspects)的建議做法。

GMITS 第 5 部分－網路安全管理指引以結構上加以剖析，係陳述以下三個簡明扼要的準則，以協助負責 IT 安全性的人員能識別潛在的安全防衛措施區域。這些準則須識別：

1. 不同的網路連接類型。
2. 不同的網路特性與相關的信賴關係。
3. 關於網路連接之安全風險的潛在類型。

結合這些準則的結果，可指出潛在安全防衛措施區域。進而，可提供潛在安全防衛措施區域的大致上的入門描述，及更多細節之來源的指示。

正因許多組織的 IT 系統是透過網網相連，相互連結，在現今政府與各類商業組織活動都趨向全球化的經營理念，因此網路必須是完善而無安全上的疑慮，在此背景條件下致使 GMITS 的第 5 部分將重點置於網路安全管理上。其中如圖 3.8 說明建立網路安全需求時須考量到通訊相關要素應如何進行識別與分析的整個嚴謹處理過程(Process for the Identification and Analysis of Communications Related Factors Leading to the Establishment of Network Security Requirements)，並且提供了潛在安全防衛措施區域的指示說明。圖 3.8 中的實線表示每個處理過程的主要路徑，另虛線則表示經由安全風險分析與管理審查的協助，決定安全風險

的類型。檢驗處理過程中上下主要路徑的結果一致性將是審查整體 IT 安全政策的主軸之一。

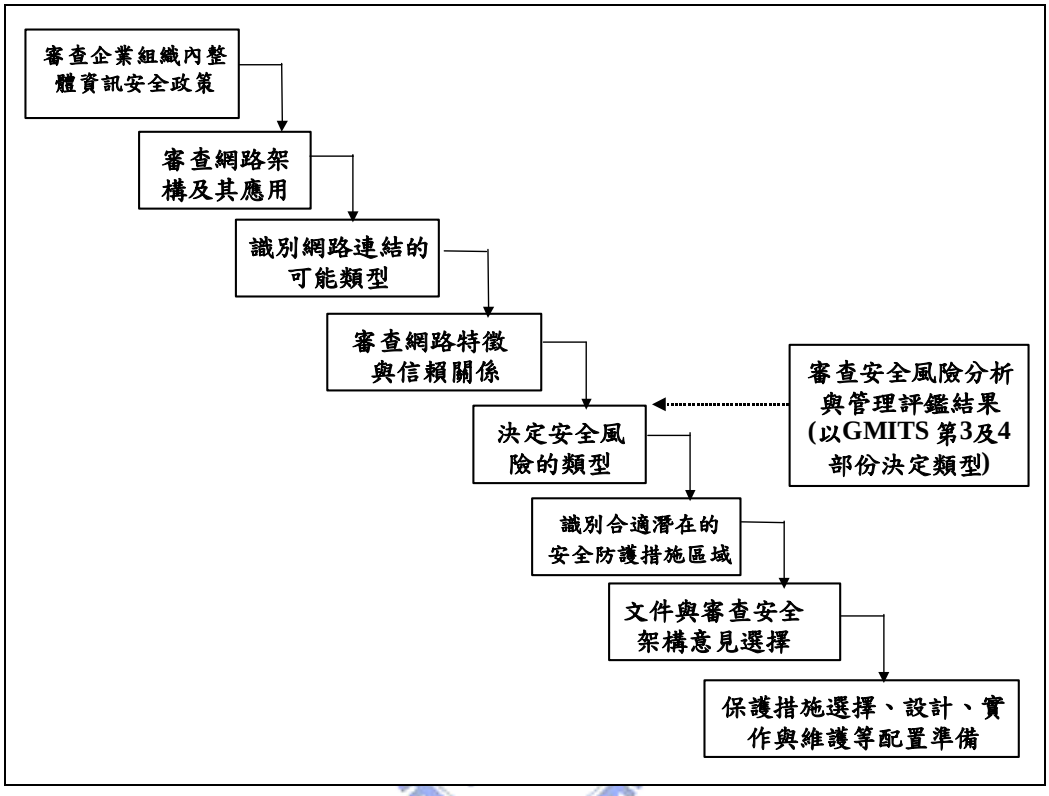


圖 3.8：建置網路安全需求產生的通訊相關因素之識別及分析過程

在「審查企業組織內整體資訊安全政策」的過程中可能包含了機密性、完整性、不可否認性等等需求的各項具體陳述，及對威脅的類型與直接關於網路連結保護措施需求的各個觀點；諸如：不允許經由撥接連線方式加以連接、所有與網際網路的連接必須透過一個安全的閘道器(Gateway)或沒有數位簽章的付款指令被視為是無效的等皆為安全政策的可能陳述實例。如果有類似如上述實例的這些安全需求，將會將這些潛在的安全防護措施區域收錄於其列表中，及必須反應在網路安全架構選項中。在 GMITS 的第 2 部分與第 3 部分提供了整體 IT 資訊安全政策文件的指導方針，以及對於其他安全文獻的內容與關係的指引參考。

「審查網路架構及其應用」的過程需要考量到網路類型(如：區域網路、都

會區域網路與廣域網路等互連範圍不同)、網路協定(如：不同協定間具有不同的安全特性且需求考量不同、協定可能使用到不同的網路拓撲型態，例如匯流排拓撲、環拓撲及星狀拓撲等，無論採行任一型態之技術實作，對於安全性都有深遠性的影響)、網路應用(如：主從架構設計方式的安全考量)及其他可能會產生較高風險的考量因素。另針對「識別網路連結的可能類型」的過程中考量到一般網路連結的類型係肆應組織的需求而希望採用私用(Private)網路或公眾(Public)網路等兩類達到可加以存取的目的。且這類網路連結的類型可能被要求提供採多樣化的服務功能，諸如電子郵件(E-mail)、電子資料交換(EDI)等，可能因連結的類型涉及到網際網路的使用、企業內部網路或外部網路設施，而每種類型存在著不同的安全考量。故各個連結類型可能擁有不同的弱點及相關的安全風險，因此最終需要選擇不同的保護措施集合。

「審查網路特徵與信賴關係」的過程中，首先應識別網路類型的安全性(如：私用網路被視為較公眾網路安全性高)並掌握網路傳輸的資料類型予以查核。一旦完成識別現存或建議提出的網路特徵，進而利用表 3.10 中的簡易矩陣建立網路連接相關的信賴關係。這些產生出的信賴關係參考(Relevant trust relationship)可進而確認資訊系統網路連接的安全風險類型與識別合適潛在的安全防護措施區域。

表 3.10：網路連接信賴環境描述

信賴關係 Trust relationship	描述 Descriptive
低 Low	與未知的使用者社群間的網路
中 Medium	與封閉(多於一個組織中的)商業團體中的已知社群使用者的網路
高 High	與單一組織中的已知使用者社群的網路

在「決定安全風險的類型」(Determine Types of Security Risk)的過程可參考 GMITS 第 3 部分：資訊安全的管理技術與第 4 部分：安全防衛的選擇來保護主機 IT 設施，其中包含識別、鑑別及邏輯存取控制。在較低的信賴情況下，允許必須確保只提供對資源的存取，該資源是由信賴模型與企圖存取的需求所組成。一旦安全防護措施的強度無法高於高信賴情況時，則必須實作增加額外的防護措施以加以因應。「識別合適潛在的安全防護措施區域」可參考 GMITS 第 4 部分以選取防護措施，訂定安全的服務管理方案(含安全操作程序、安全符合檢查、網路連接的安全條件、網路服務用戶之文件化安全條件、事件處置)，並考量識別與鑑別(如：遠端登入、鑑別增強與安全單一簽入)、入侵偵測、惡意程式碼防護、網路安全管理、安全閘道器、網路資料機密性、網路資料完整性、不可否認性、虛擬私有網路(Virtual Private Network，簡稱 VPN)、企業永續性/災變復原等作一通盤考量及檢視安全架構，至保護措施選擇腹案等配置準備就緒為止，達到機密性、完整性、可用性、不可否認性、可歸屬性及可靠性等安全原則。故在網路管理上，如同現實社會中的管理作為，各項問題亟待一一解決，除定期檢視維修及保養外，也要針對各個可能面對的問題擬妥對應之安全對策，期以做到滴水不漏為最高目標，不斷修訂對策，建立有效的安全。

3.4 整合資訊安全管理的指導原則

在 2002 年 12 月 5 日公布之 ISMS(驗證)規範 CNS17800(BS7799-2: 2002),於文件要求中規定應包括文件要求之一般要求：

1. 安全政策與安全目標之書面聲明。
2. 資訊安全管理系統之範圍及支援資訊安全管理系統之各程序及控制措施。
3. 風險評鑑報告。
4. 風險處理計畫。
5. 組織為確保有效規劃、操作與控制資訊安全過程所需之書面程序。
6. CNS17800 (BS 7799-2: 2002)要求之各記錄。
7. 適用性聲明書。

所有文件應依據資訊安全管理系統之政策要求隨時可供取用。

備考 1：CNS17800(BS7799-2: 2002)所言之「書面程序」係指已建立、文件化、實施及維持的程序。

備考 2：每個組織可能有不同之資訊安全管理系統文件化，因為：

---組織規模及其活動型式。

---安全要求及系統管理之範圍與複雜程度。

備考 3：文件及紀錄可為任何形式或型態之媒介物。

其中 1~5 是建立 ISMS 規劃（Plan）階段應完成的工作，圖 3.8 是前述規劃階段中風險評鑑與風險處理等在風險管理中之關係，GMITS 是建立 ISMS 規劃階段風險評鑑工作之指導原則。

一般而言，風險評鑑文件應解釋選用何種風險評鑑方法，以及何以該方法對安全要求與企業環境是合適的。所採用之方法，其目的應以最經濟、有效率之方式集中安全力量及資源。文件亦應包含所選用之工具及技術，及何以適合所定之範圍及風險，以及如何正確使用而得出有效結果，且並將風險評鑑細節應予文件化：

1. 資訊安全管理系統內資產之評估，包括所用評估標準之資訊。
2. 威脅及脆弱性之識別。
3. 威脅利用脆弱性之評鑑，以及該事件可能造成之衝擊。
4. 根據評鑑結果計算風險，以及識別殘餘風險（Residual risk）。

GMITS 分別在其第 3 部分與第 4 部分提供如圖 3.9 所示風險管理中之風險分析及風險評估的指導原則[15]，其第 5 部分是根基於 GMITS 第 4 部分對網路安全（Network Security）管理 IT 之指導原則。GMITS 之第 1 部分與第 2 部分，則分別對資訊安全政策、目標及其範圍，提供建立 ISMS 的指導原則。除此之外，GMITS 第 4 部分如圖 3.10 與表 3.11 所示，對建立 ISMS 之控制措施亦提供了如表 3.9 所示之 CNS17799 (BS7799-1:1999)等 8 種規劃時可供參考之已有的資訊安全規範、準則等之比較資訊，供不同類型之資訊技術系統選擇防護措施時的參考；而針對各個資訊技術系統所要求之安全等級有不同需求之考量，宜參考如圖 3.11 的方式訂定面對不同風險須建立不同基準等級之防護措施，使得整個系統獲得最適切妥善的保護。在表 3.4 中，已清楚的說明 GMITS 與 BS7799-2：2002 及 ISO/IEC 17799 的互補角色；質言之，GMITS 是建立 ISMS 計畫階段中，一份重要之指導原則的國際標準。

圖 3.9：風險管理標準使用指引示意

在現今高度 e 化的政府與企業組織皆相當倚賴利用資訊處理各類作業及活動，一旦喪失了資訊與服務的機密性(Confidentiality)、完整性(Integrity)、可用性(Availability)、不可否認性(Non-repudiation)、可歸責性(Accountability)、可信賴性(Authenticity)與可靠性(Reliability)，對組織的運作會有甚為不良的影響。因此，需要一個準則保護資訊及管理組織內的 IT 系統的安全，而 GMITS 正是在此背景下產生的準則。

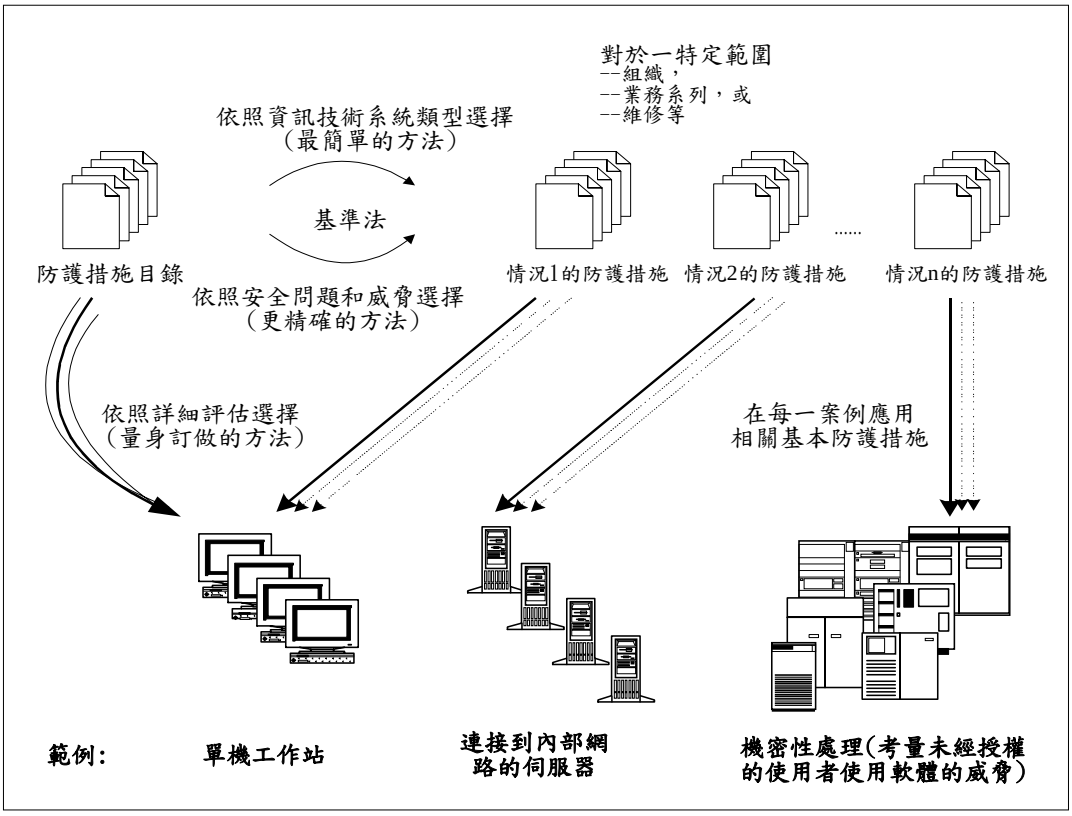


圖 3.10：選擇防護措施方式

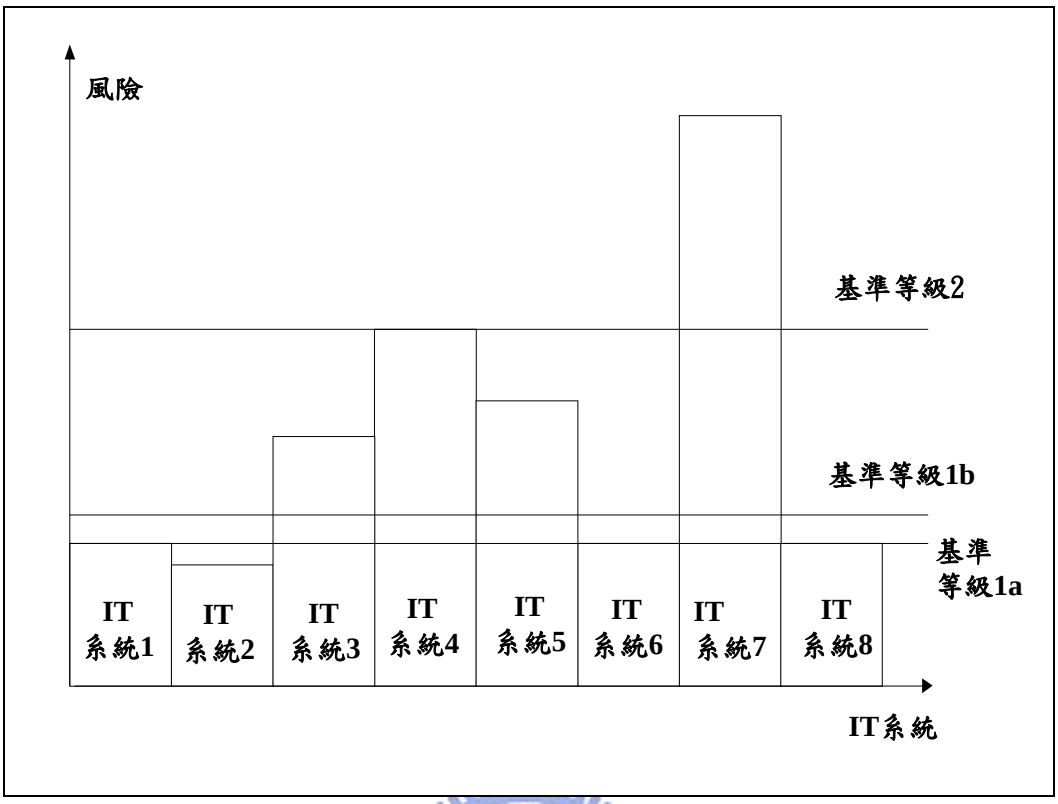


圖 3.11：不同安全等級須建立不同基準等級之方法示意

表 3.11：不同類型系統之資訊技術防護措施基準

	單機工作站	連接到網路的工作站(無分享資源的使用者端)	連接至網路分享資源的伺服器或工作站
I&A			
I&A 基於使用者所知	X	X	X
I&A 基於使用者所有	X	X	X
I&A 基於使用者身分	(X)	(X)	(X)
邏輯存取控制和稽核			
存取控制政策			X
使用者存取電腦	X	X	X
使用者存取資料、服務和應用程式	X	X	X
審查和更新存取權力			X
稽核登錄	X	X	X
惡意程式碼			
掃描器	X	X	X
完整性檢查	X	X	X
可移動的媒體流通控制	X	X	X
保護措施程序	X	X	X

網路管理			
操作程序			X
系統規劃			X
網路組態			X
網路隔離			X
網路監測			X
入侵偵測			X
密碼學			
資料機密性保護	(X)	(X)	(X)
資料完整性保護	(X)	(X)	(X)
不可否認性		(X)	(X)
資料確實性	(X)	(X)	(X)
金鑰管理	(X)	(X)	(X)

說明：

1. X 表示在正常使用環境下必須實施之控制措施。
2. (X)表示在某些使用環境下宜實施之控制措施。

GMITS 提出之資訊安全分類、分級的概念與圖 2.8 之 OECD 揭櫫的安全指導原則相符合。英國之 IRCA 要求 ISMS 第三者稽核員/主導稽核員訓練課程(含測驗)規範，明定必須包含 ISO/IEC TR 13335 是否代表英國對於 ISMS 的驗證，宜就不同安全等級有各別之要求，是推動 ISMS 須面對的課題，值得更進一步做深入的探討。

第四章、資訊安全管理系統評估之研究

行政院國家資通安全會報已於 2003 年正式實施資訊安全管理系統(ISMS)驗證要求；但我國迄今並未實施美國聯邦政府於 2002 年方要求之資訊安全管理系統自我評鑑指導原則[72]。美國國家標準與技術研究院（National Institute of Standards and Technology，簡稱 NIST）的安全、隱私與基礎建設委員會（Security, Privacy and Critical Infrastructure Committee），已於 2000 年 11 月 28 日提出聯邦資訊技術安全評鑑框架（Federal Information Technology Security Assessment Framework，簡稱 FITSAF）中之資訊安全管理系統等級 1～5 之定義[72]。一個會引起一般悍客有興趣入侵的資訊系統，假設其資訊安全管理系統設定之等級在 FITSAF 中是屬於等級第 3 級以下時，其稽核結果儘管是非常的完整，或已通過 BS7799-2:2002 之驗證，亦如矗立在沙灘上的城堡，是經不起任何悍客入侵之考驗；故通過 FITSAF 第 3 級以上要求之資訊系統，方能有效的防護諸如「流光(Fluxay)」等類似先進的駭客自動化入侵工具的威脅 [15,53,68,70,72]。

我國在進行資訊安全管理系統稽核工作時，若能參照前述 FITSAF 之定義要求各個機構自我評鑑並據以進行資訊系統技術安全之差距分析（Gap Analysis），其結果應更具參考價值。千禧年前，根基於歷史及薪傳之目的，遵照共同準則（Common Criteria，簡稱 CC）之資訊產品／系統安全評估的國際標準已正式頒布，成為創建可信賴資訊資訊安全管理品質文化技術之基準。然而，在另一方面，攻擊手法日新月異，資訊系統的威脅亦與時推移，除了工程面的解決方案外，利用教育訓練建立完整的資訊；同時進行滲透測試（Penetration Test）等的查證（Verification）與確認（Validation）以及驗證（Certification）與認證（Accreditation）之安全評估機制應是比較完整的解決方案，亦為 FITSAF 中第 3 級及其以上（等級 4 與等級 5）之標的。尤其是類似國家資通安全會報去（2002）年 7 月 31 日發布之流光入侵警訊，必須仰賴滲透測試與資訊安全技術稽核；事實上，近年來類似流光等駭客網站提供之自動化入侵工具已逐漸形成，成為資訊作業環境安全上極大的隱憂，如何有效防護此類攻擊已成為「資訊安全管理系統」能否落實的基石之一。有鑑於此，今年 5 月於聯合國國際聯邦資訊處理(International Federation for Information Processing，簡稱 IFIP)在其負責資訊安全之第 11 資訊委

員會(Technical Committees，簡稱 TC11)舉行的年度研討會中，已有學者提出如表 4.1 所示之對僅使用 BS 7799 進行資訊安全管理系統驗證工作對資訊安全保護不足的研究結果[26]。根基於此，本章將先簡介美國國家資訊保證驗證與認證過程（National Information Assurance Certification and Accreditation Process，簡稱 NIACAP）之指導綱要[54]；之後將根基於美國 NIACAP 在通信基礎建設的先導計畫，探討資訊安全管理系統之框架；最後，提出資訊安全管理系統驗證作業稽核宜具備之評估知識與技能。

表 4.1：ISO/IEC 17799：2001(E) 控制措施與保護等級之關連示意

ISO/IEC 17799：2001(E)	保護等級(Protection Class)			
	1.不合適(Inadequate)之保護	2.最小(Minimal)之保護	3.合理(Reasonable)之保護	4.合適(Adequate)之保護
1. (資訊)安全政策	×	×		
2.組織安全	×	×		
3.資產分類與控制	×	×		
4.人員安全	×			
5.實體與環境安全	×			
6.通信與作業管理	×			
7.存取控制	×			
8.系統開發與維護	×	×		
9.營運持續維護	×	×		
10.符合性	×	×		

說明：空白(無×) 處均表示實作過程(Processes)與程序(Procedures)宜增加控制措施。

4.1 美國國家資訊保證驗證與認證計畫指導綱要介紹

1990 年 12 月 5 日，美國國家研究評議會(National Research Council)安全系統研究委員會發表了其「電腦風險(Computers at Risk：Safe Computing in the Information Age，簡稱 CAR)報告」之結案報告指出[70]，在已來臨之無國界、不受距離時間限制的全球資訊社會中，個人、企業、政府等均深受資訊系統的影響，不僅是人與資訊系統共棲，並將演變成必須依賴報告資訊系統不斷發展演進的功能。譬如：資訊系統使用的增加，已經促使各個組織內部之體制機構與作業程序起了根本的變革；同時，更修正了組織內部交互運作的工作方式。在資訊系統無法運作的狀況下，現今的作業程序將無法繼續下去，亦無法回復至先前的運作方式；想想看，當資訊系統無法運作時，那將帶給如航空公司、證券交易、金融作業、健保門診、捷運系統等之影響，均已是公共安全的議題，即可知其相恃性(Dependability)的重要程度。在另一方面，因為資訊的使用日益頻繁，確實帶來許多利益；然而，資訊系統在安全防護的需求，相較之下，在程度上實相距甚遠；當包含公共服務、商業、個人等在內之整個社會均已十分依賴這尚不足以信任的種種技術時，所有資訊系統的使用都經不起些許的故障或甚至遭受攻擊。

CAR 報告之影響是立即且深遠的，根基於該報告，美國總統於 1992 年下令推動資訊系統安全之國家目標，並由美國國家標準與技術研究院(National Institute of Standards and Technology，簡稱 NIST)負責執行所需「標準與指導綱要」之工作，並與國際標準組織(International Organization for Standardization，簡稱 ISO)合作推動，10 年來已公布近 30 份相關規範，從資訊技術安全評估共同準則(Common Criteria，簡稱 CC)、資訊系統安全指導綱要與作業準則、規劃指引、風險管理、驗證(Certification)與認證(Accreditation)等加以研究、綜覽而頒佈專著，並於千禧年前(1999 年 12 月 15 日)由 ISO 將資訊技術安全評估共同準則公布成提供資訊產品/系統之資訊技術安全驗證之國際標準[41]。2002 年起，要求美國聯邦政府遵照過去 10 年頒佈之 NIST 規範執行資訊安全管理系統內部稽核，其中將資訊安全管理系統依能力成熟度與整合程度區分為 5 級，自第 3 級起要求依循驗證與認證作業；如表 4.2 所示之國家安全之電信與資訊系統安全政策第 11 號(National Security Telecommunications and Information Systems Security Policy No.11，簡稱 NSTISSP No.11)，已於 2002 年 7 月 1 日起強制實施；並於 2002

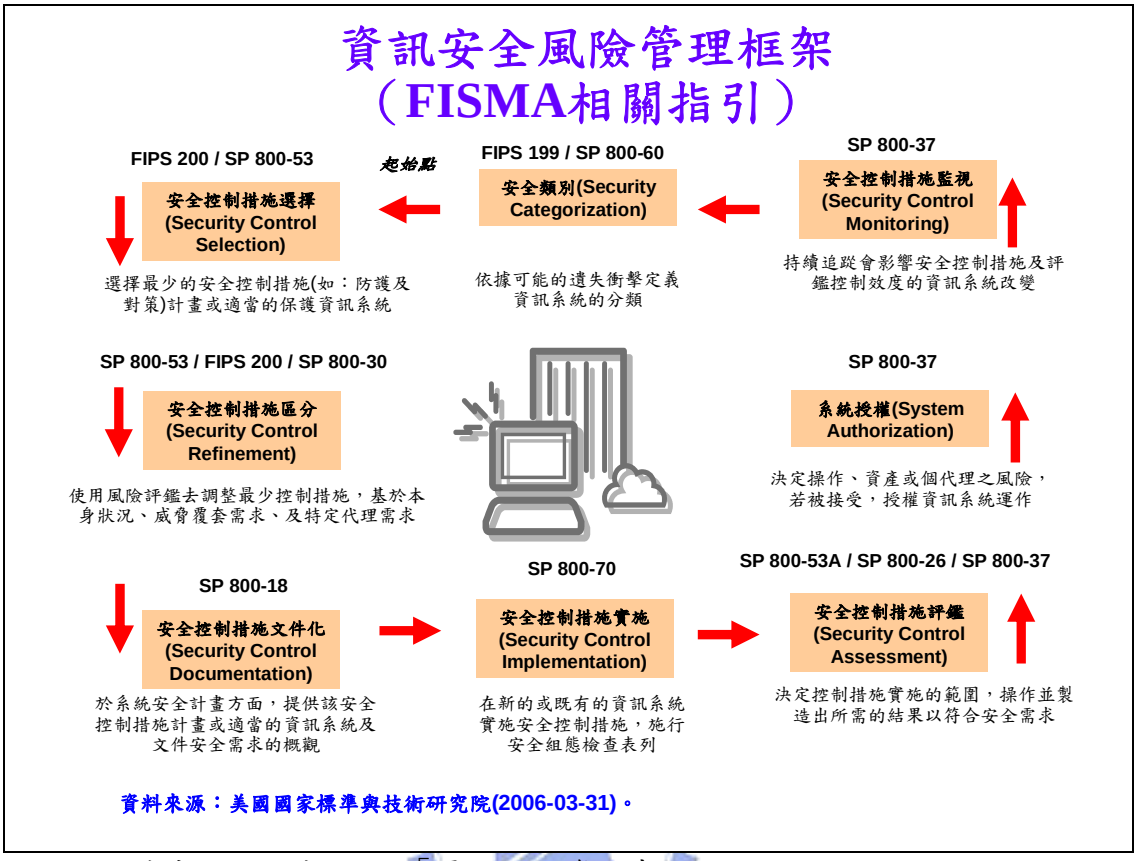
年 10 月 28 日，根基於 CC 2.1 與美國聯邦政府於 2001 年 5 月 25 日公布之密碼模組安全需求 FIPS(Federal Information Processing Standard) PUB(Publication)140-2 [56]，NIST 頒布如表 4.3 所示之資訊保證驗證與認證計畫供公開討論，預定在 2004 年秋季定案後實施 [68]，其遵循規範之說明文件如圖 4.1 所示 [48]，內容則應如表 3.4 所示[26,41,46,53,54,56,68,70,72]，圖 4.2 是其資訊安全保證作業之示意說明，其中將整個作業區分為定義、驗證(正確性查證)、驗證(有效性確認)及維護認證等四個階段加以描述作業整個流程。

表 4.2：美國國家安全之電信與資訊系統安全政策第 11 號

1. 美國國家安全之電信與資訊系統安全委員會(National Security Telecommunications and Information Systems Security Committee，簡稱 NSTISSC)，依據 1990 年 7 月之美國國家安全第 42 號指令(National Security Directive No.42，簡稱 NSD-42)，於 2000 年 1 月公布 NSTISSP No.11。
2. NSTISSC 為建立 NSTISSP No.11 之規範，於 1999 年 3 月 11 日先行公布 NSTISSAM (Advisory Memorandum) INFOSEC/1-99 預為準備；2000 年 4 月 NITISSC 頒布資訊保證驗證與認證過程 (National Information Assurance Certification and Accreditation，簡稱 NIACAP) 之 NSTISSI (Instruction) No.1000。
3. 政策訓令：
   3.1 2001 年 1 月 1 日起，通資訊基礎建設之資訊技遵循共同準則及國家技術與標準研究院(National Institute of Standards and Technology，簡稱 NIST)之確認計畫。
   3.2 2002 年 7 月 1 日起，總統決策令第 63 號(Presidential Decision Directive No.63，簡稱 PDD-63) 中之範疇，強制(Mandated)實施 3.1 中的規定。

表 4.3：美國聯邦政府資訊保證驗證與認證過程

1. 啟始階段： 1.1 準備。 1.2 資源識別與告示。 1.3 安全計畫分析、更新與承認。 2. 安全驗證階段： 2.1 安全控制措施查證。 2.2 安全驗證文件。 3. 認證階段： 3.1 安全認證決策。 3.2 安全認證文件。 4.持續督導階段： 4.1 組態管理與控制。 4.2 進階安全控制查證。 4.3 狀態報告與文件。 5.依據: 5.1 美國國家安全之電信與資訊系統安全委員會於 2000 年 4 月頒布之第 1000 號訓令。 5.2 2002 年 12 月公布之聯邦資訊安全管理法案(Federal Information Security Management Act，簡稱 FISMA)。



說明：這些出版品可由 NIST「電腦安全資源中心(Computer Security Resource Center)」(http://csrc.nist.gov)取得。

圖 4.1：美國聯邦資訊安全管理法驗證及鑑定程序之相關指引

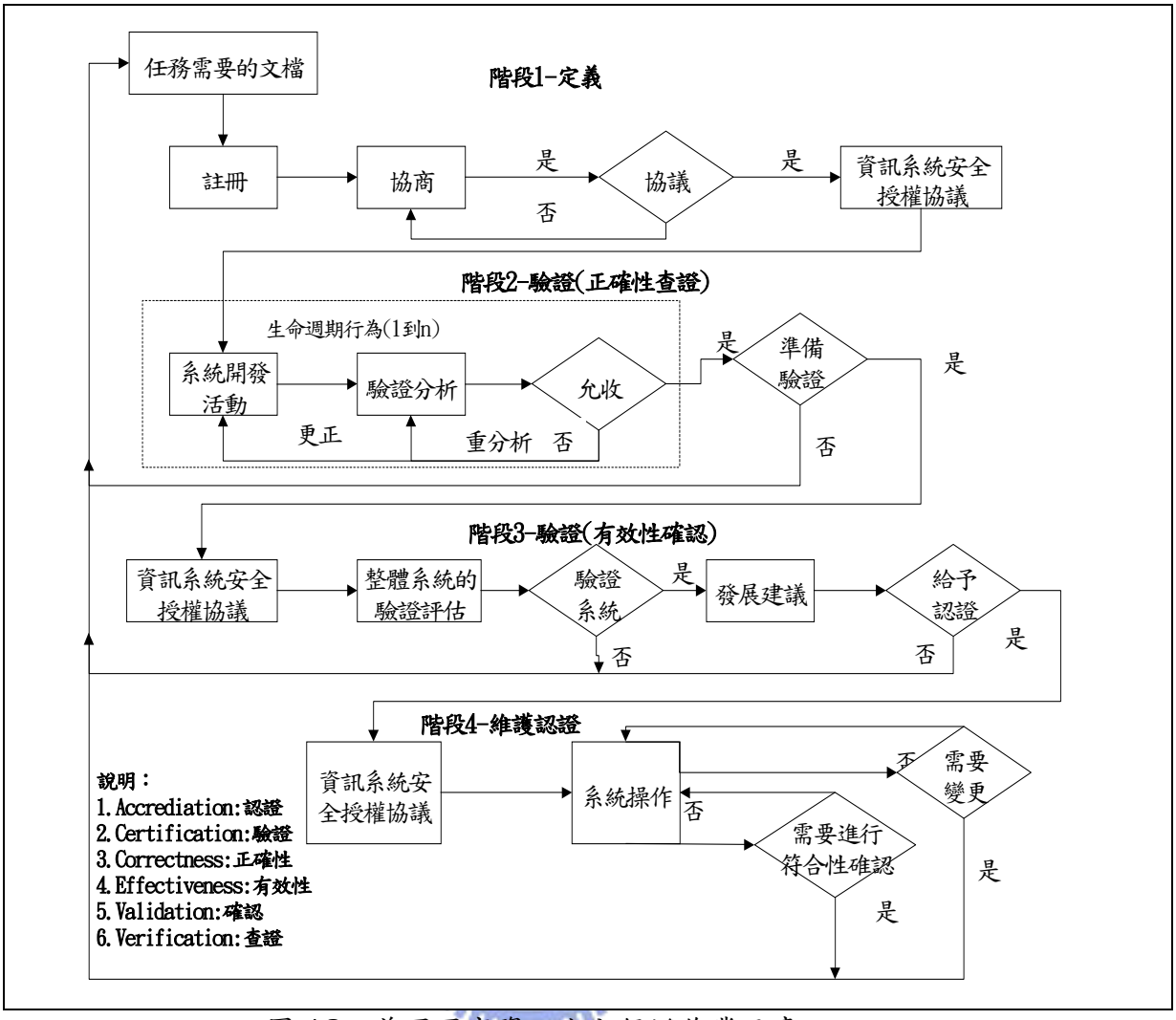


圖 4.2：美國國家資訊安全保證作業示意

依據美國已公布之文件，NIACAP 將由 CC 2.1 與 FIPS PUB 140-2 執行資訊安全工程面之產品(/系統/服務)的驗證，再以 CC 2.1 為基礎對資訊技術(Information Technology，簡稱 IT)面之系統進行驗證，同時遵循 ISO/IEC 17799 等標準進行資訊系統之操作環境面進行驗證，3 階段驗證工作所接受之殘餘風險的處理過程是否合理則是認證階段之工作 [68]。

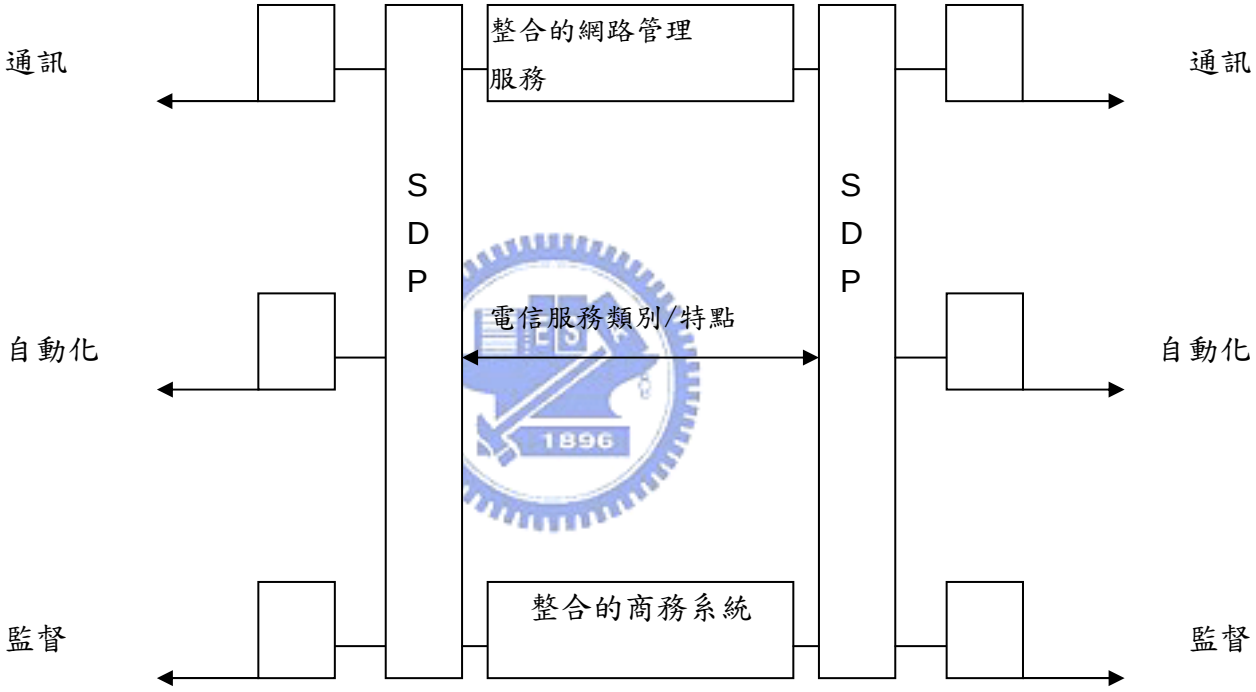
4.2 資訊安全管理系統評估探討

降低風險是資訊安全管理系統防護措施之標的，圖 3.4「資訊安全管理系統風險關係示意(ISO/IEC TR 13335-1)」是其示意說明[43]。為有效達成資訊安全管理系統的目的，早在 1998 年以前，NIACAP 之先導(Pilot)計畫，分從國防通信、銀行與金融等基礎建設執行如圖 4.2 所示之資訊安全保證作業，表 4.4 是其各階段的輸入與輸出示意說明。以通信基礎建設為例，1958 年成立於 1967 年併入美國交通部(Department of Transportation，簡稱 DoT)之美國民航局(Federal Aviation Administration，簡稱 FAA)，在 1996 年 2 月 21 日就公布了參照 NIST 1983 年 9 月 27 日發行的電腦安全驗證與認證指導綱要(Guideline for Computer Security Certification and Accreditation)規範的 FAA 自動化資訊系統與通信安全功能需求；同時引進發展中之資訊保證方法，於 1998 年 5 月開始進行圖 4.3 與圖 4.4 所示的 FAA 通信基礎建設(FAA Telecommunication Infrastructure，簡稱 FTI)之資訊保證作業，2000 年 9 月公布 FTI 安全規範第一階段的實作指引，提出如 FAA 通信基礎建設之根基於共同準則(Common Criteria，簡稱 CC)與系統安全工程能力成熟模型(System Security Engineering Capability Maturity Model，簡稱 SSE-CCM)之 ISO/IEC 21827 的資訊安全管理系統評鑑模式[20,26,41,46,53-56,68,70,72]。

表 4.4：資訊技術安全評估共同準則於資訊系統生命週期對照示意說明

資訊系統生命週期	共同準則加工活動
需求分析	1.保護剖繪(Protection Profile，簡稱 PP) 2.PP 評估保證(Assurance PP Evaluation，簡稱 APE)
設計(定義階段)	1.安全標的(Security Target，簡稱 ST) 2.ST 評估保證(Assurance ST Evaluation，簡稱 ASE)
開發(查證階段)	1.評估標的(Target of Evaluation，簡稱 TOE) 2.組態管理保證 3.交付與運行保證
查證(查證階段)	1.測試保證 2.脆弱性評鑑保證

確認(確認階段)	1.交付與運行保證 2.指導性文檔保證
操作與維護 (維護認證階段)	1.生命週期支援保證 2.脆弱性評鑑保證



說明： SDP：Service Delivery Point。

圖 4.3：FTI 功能架構示意

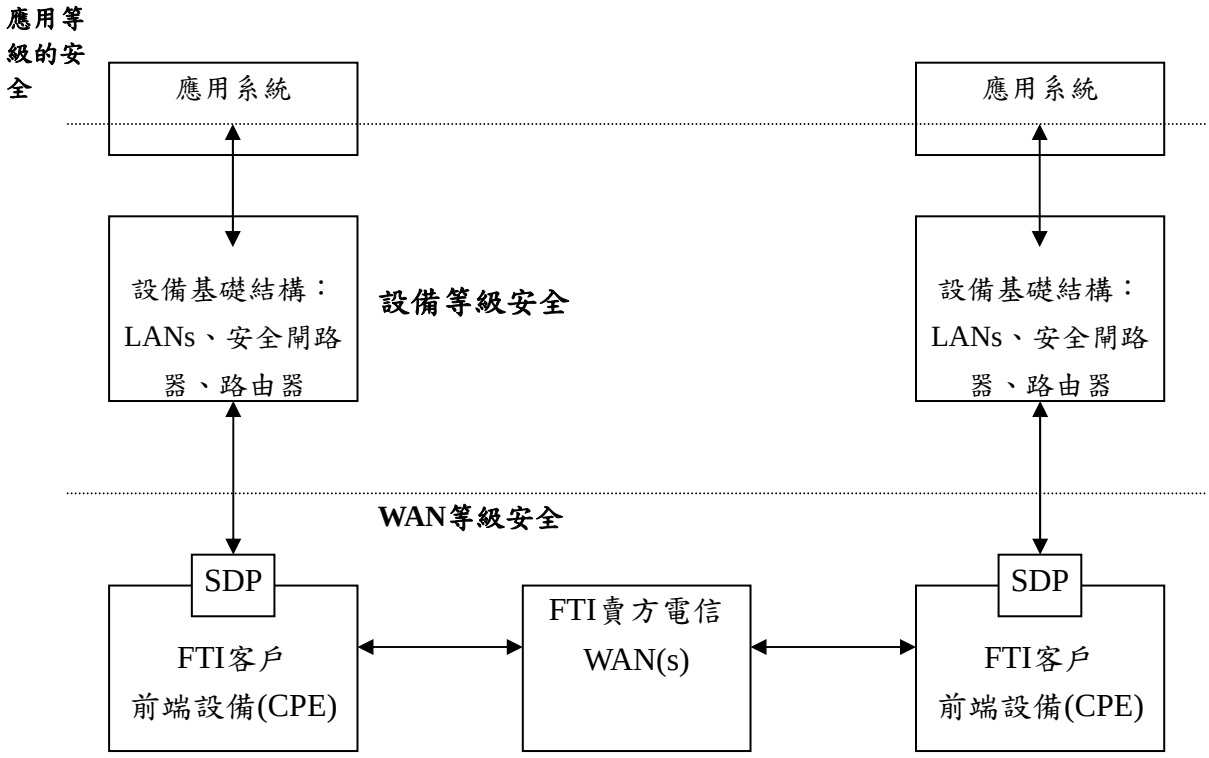


圖 4.4：FTI 安全服務範圍

針對如圖 3.4 所示之威脅、脆弱性與資產之資訊安全管理系統風險源池的 3 個構面，共同準則已提出如圖 4.5 所示之安全目標及需求關係，其中安全功能需求與安全保證需求應可就 ISMS 之脆弱性及威脅分別提供適宜的保護；在操作環境安全方面，共同準則僅假設在可控制之環境中，能滿足組織安全政策對威脅的保護[41,48,62]；結合 BS 7799-2：2002 等對資訊資產控制項目之要求[24]，我們提出如圖 4.6 所示之資訊安全管理系統框架與安全評估標的(Target of Evaluation，簡稱 TOE)規格內容的圖 4.7，分別針對強化資訊資產作業(Operation)構面之弱點(Weakness)的控制措施、強化資訊系統威脅(Threats)構面之弱點的組態管理、強化資訊系統脆弱性構面之弱點的設計與建造之功能正確性，根基於共同準則與經由適宜之防護(含控制)措施，降低 ISMS 之威脅，減少 ISMS 脆弱性被利用之可能性，減少 ISMS 資產曝露之或然率，建置 ISMS。

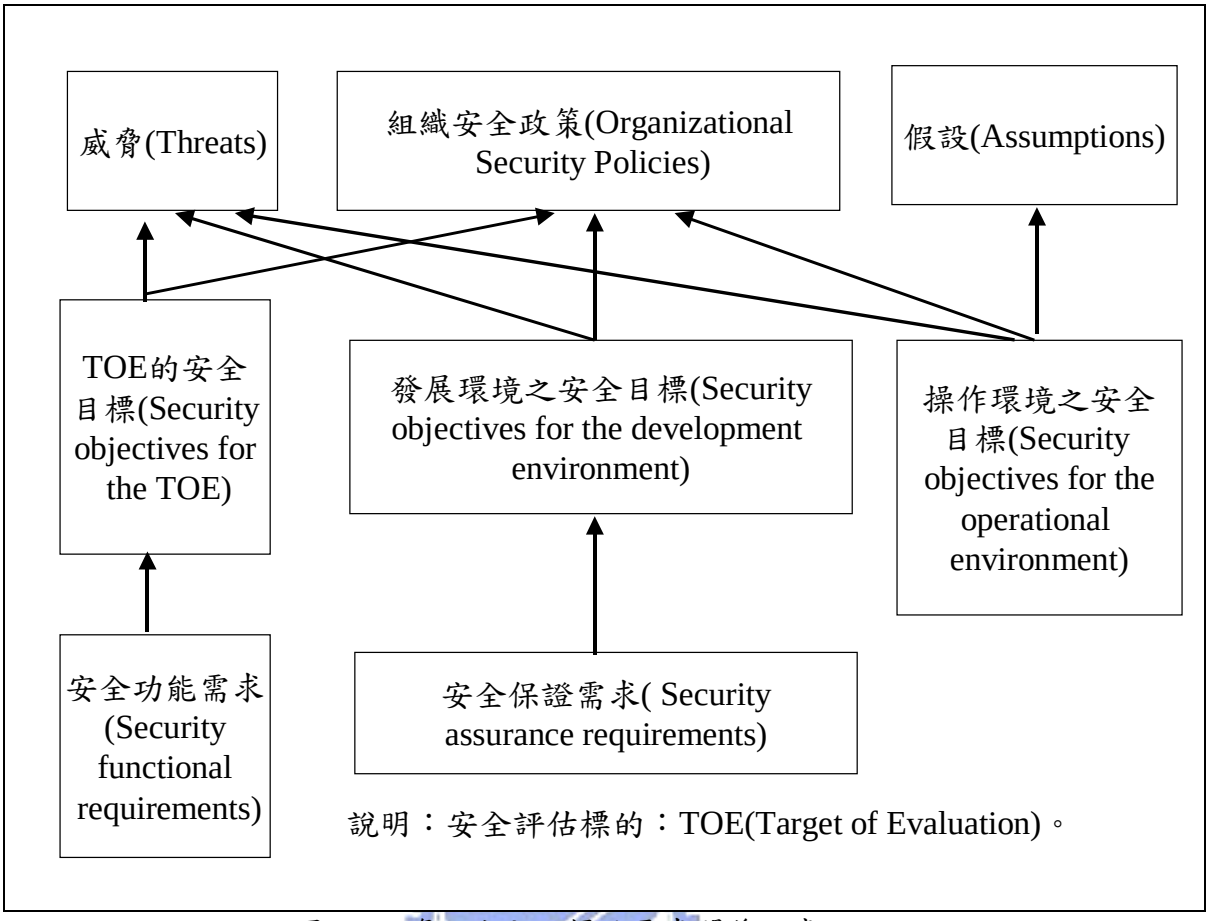


圖 4.5：資訊安全目標及需求關係示意

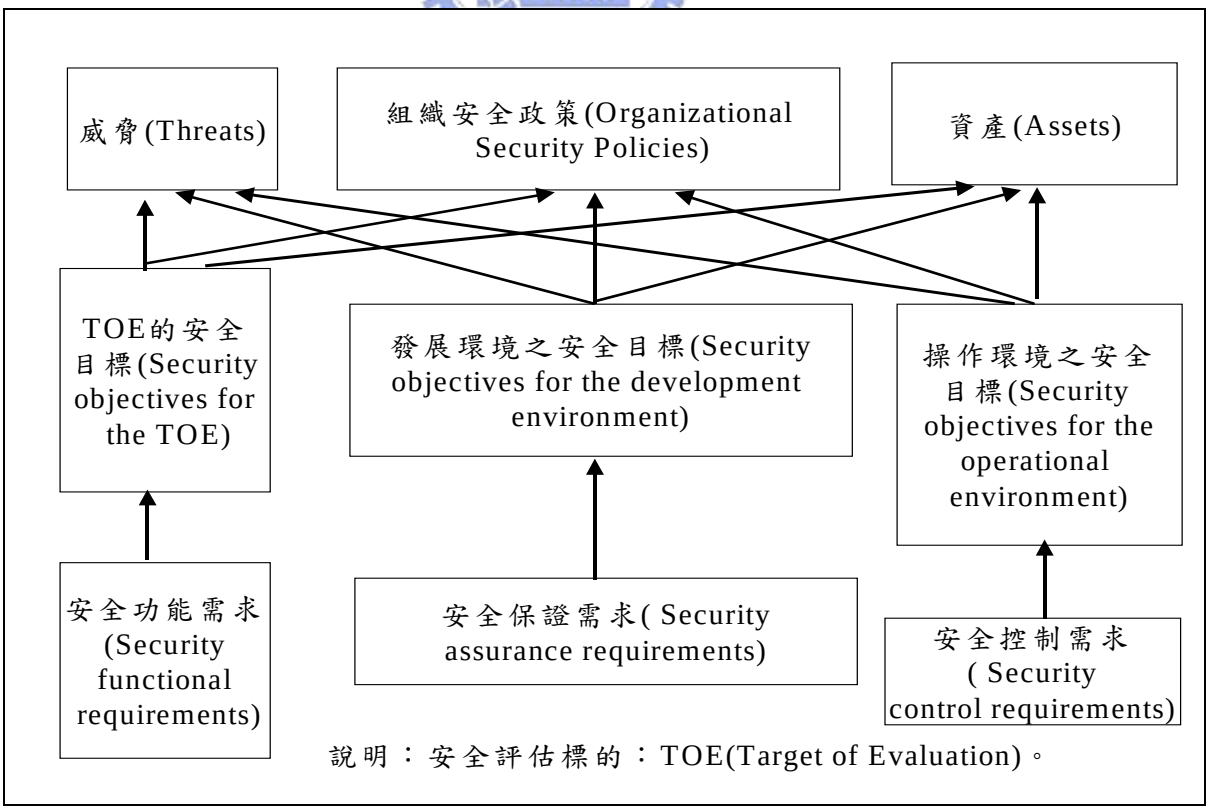


圖 4.6：資訊安全管理框架

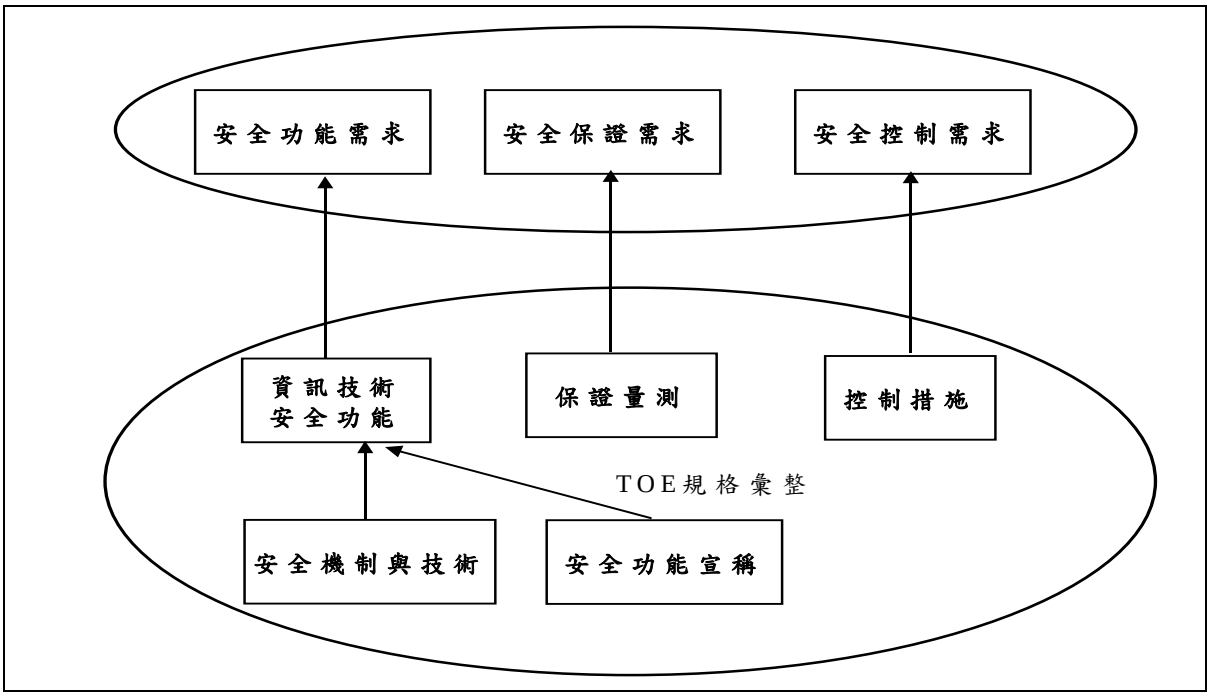


圖 4.7：資訊安全管理系統評估標的(TOE)規格內容

NIACAP 之目的在於達成：「在資訊處理作業中，經由確認資訊及資訊系統之可用性、完整性、鑑別性、機密性及不可否認性來保護與防禦資訊與資訊系統，並包含具體化的防護、偵測與反應能力以提供資訊系統損害之復原。(Information Operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.)」之資訊保證(Information Assurance)的目標。由於在資訊系統生命週期之每一階段均存在資訊與資訊系統因弱點(Weakness)曝露(Exposure)在外之脆弱性(Vulnerability)遭致威脅(Threat)形成的風險，如圖 4.5 所示，CC 2.1 已能提供資訊技術評估標的及發展環境之安全目標的驗證需求，如圖 4.6 與圖 4.7 所示，結合 BS 7799-2:2002 等資訊安全管理系統之驗證作業[52]，應能建構如圖 4.8 所示的整合 IT 及管理之資訊系統安全驗證機制的評估過程。

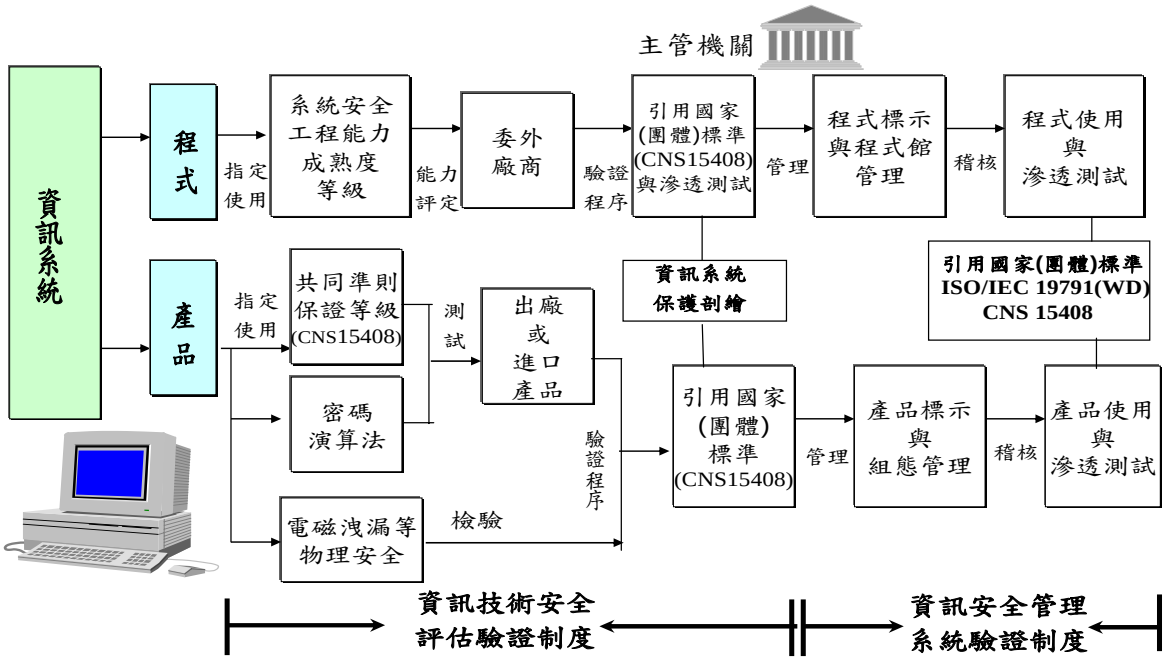


圖 4.8：資訊系統安全驗證機制運作示意

4.3 資訊安全管理系統建議之驗證作業稽核訓練

隨著電子科技的一日千里、個人電腦的普及、網路通信結構的改進以及全球資訊網的風行，網際網路以驚人的速度成長，使得資訊傳播無遠弗界。每天都有數百萬的人們在網際網路上搜尋各種資訊，而這些資訊有些是儲存在半個地球之外的電腦上；雖然大部分的使用者都是合法地存取資料，但仍常有非法入侵與存取其它電腦中資料的事件發生，而老練的駭客更經常苦心鑽研安全漏洞藉以闖入電腦系統。除了來自外部的攻擊外，內部人員也有入侵系統可能；這些攻擊可能只是想造成組織運作暫時的混亂，如：阻斷服務(Denial of Service，簡稱 DoS)，但也可能是想造成組織資訊架構的巨大損傷。在網路發達與入侵事件頻傳的今日，資訊安全的概念已從實驗室中神祕難懂的研究轉變成社會大眾關心的主要議題之一。

資訊安全管理系統的目標在於：「從確保資訊資源的合法存取，到在所有可能遭受資訊攻擊的階段，提供完整(Complete)、未中斷的資訊系統運作」。ISMS 之設計與實作及其運作必須能防止硬體、軟體與使用者資料遭受來自外部或內部

的威脅；其牽涉的範圍可能從簡單的金鑰管理機制到複雜的存取控制機制與資訊完整性機制。這些機制在設計時應考量風險管理(Risk management)的概念，而風險管理隱含著在資訊科技的脆弱性(Vulnerability)與利用這些脆弱性源池之威脅效力間取得平衡[25]。

保護資訊資產的安全，已成為當今文明國家之共識，亦為民主法制國家、社會與人民必備的素養。然而，人性本非全然善良，監守自盜侵害資產安全者，所在多有。資訊安全管理除事涉「公共安全」，更因涉及組織層面與尚需考慮面對心懷惡意的外人，以及監守自盜的內賊等因素，較諸環境管理系統、工業衛生安全等之驗證工作更形困難，如何因應與數位生活息息相關之資訊安全管理系統驗證作業等議題，實應展開更深入的思考與討論。

國際標準組織(International Organization Standardization，簡稱 ISO)自 1983 年起，由德國標準機構支援，從 ISO 第 97 技術委員會(Technical Committee，簡稱 TC)原無國家機構願意負責之資料加密(Data Encryption)工作小組(Working Group)分立，成為單一之第 20 子委員會(Sub-Committee，簡稱 SC)，正名為資料密碼學技術(Data Cryptographic Techniques)之 ISO/TC97/SC20，正式展開資訊安全技術國際標準之制訂工作。1989 年，由 ISO 與國際電子技委員會(International Electro Technical Commission，簡稱 IEC)，在根基於共同與一般之安全測量標準已取代僅就密碼學應用的特定範圍標準之發展潮流，成立資訊技術(Information Technology，簡稱 IT)安全技術(Security Techniques，簡稱 ST)的第 27 子委員 ISO/IECJTC/SC27。自 1990 年起，ISO/IECJTC/SC27 開始制訂資訊安全驗證之國際標準，並分於 1999 年 11 月 15 日頒布資訊技術安全評估準則之 ISO/IEC15408 系列標準做為 IT 安全評估的規範，2000 年 12 月 1 日，頒布 ISO/IEC17799 做為建置資訊安全管理系統的導引，表 4.5 是其第 3 工作小組(Working Group 3，簡稱 WG3)已頒布與進行中之相關標準，ISO/IEC 19791 即為針對圖 4.5 中操作環境安全評鑑正制定的標準 [21,49,61]。

表 4.5：ISO/IEC JTC1/SC27 WG3 (Security Evaluation)已完成與進行中計畫

1. ISO/IEC 15292 (2001-12-15): Protection Profile Registration Procedures.
2. ISO/IEC 15408 (1999-12-01): Evaluation Criteria for IT Security.
3. ISO/IEC TR 15443 (PDTR): A Framework for IT Security Assurance.
4. ISO/IEC TR 15446 (PDTR): Guide for the Production of Protection Profiles and Security Targets (PPST Guide).
5. ISO 18045 (WD): Methodology for IT Security Evaluation (CEM).
6. ISO/IEC 19790 (WD): Security Requirements for Cryptographic Modules.
7. ISO/IEC 19791 (WD): Security Assessment of Operational Systems.
8. ISO/IEC 19792 (WD): A Framework for Security Evaluation and Testing of Biometric Technology (SETBIT).
9. ISO/IEC 21827 (2002-10-01): Systems Security Engineering-Capability Maturity Model (SSE-CMM).

九十年代，全球文明歷經了重大的改變，品質、環境和工業安全衛生管理逐漸朝向一致化與標準化，而相關的國家標準也影響了許多國家經濟的發展和組織管理與經營的方式，ISO 品質管理和環境管理系統標準的遵從，是最佳的佐證。資訊安全的 ISO 標準 ISO/IEC 15408、ISO/IEC 17799、ISO/IEC 21827(SSE-CMM)等已陸續頒布，若善加運用，應有助於數住台灣安全文化的塑造。

資訊系統的安全性，宛如一個鍊條，其強韌度將視最脆弱的一節而定。根基於表 2.3 與圖 3.7，再參考英國已驗證稽核員登錄國際組織(International Register of Certificated Auditor，簡稱 IRCA)公布之資訊安全管理系統(Information Security Management System，簡稱 ISMS)稽核訓練規範[30]，表 4.6 之資訊安全管理系統稽核訓練課程芻議，應可做為 ISMS 驗證稽核執行如圖 4.8 所示之 ISMS 驗證工作宜俱備之知識(Knowledge)與技能(Skills)討論的基礎。

表 4.6：ISMS 稽核訓練課程芻議

授課內容應包含之標準與法規	1. ISO/IEC TR 13335 (all parts) 2. ISO/IEC 21827 3. ISO/IEC 17799 (CNS 17799) 4. BS 7799-2：2002 (CNS 17800) 5. ISO 19011 6. ISO/IEC 15408 (all parts) 7. ISO/IEC TR 15504 (all parts) 8. ISO 13491 (all parts) 9. 資訊安全相關法規(…、電子簽章法、通訊保障監察法、資訊公開法等)
最少上課時數	56 小時
作業	1. 每天至少一次 2. 一組 5 人左右 3. 每次簡報與討論時間約 60 分鐘
測驗	每次 2 小時，共 4 小時
上課人數	1. 12~20(2 個講師) 2. 6~10(1 個講師)

大量使用商用元件建置資訊系統已是勢不可當，在整合舊有、現行與未來之電腦軟、硬體、網路、應用系統與文等時，如何確保委外廠商的成果能符合安全之需求？此時，擔任資訊安全管理系統驗證稽核之人員，於風險評估等工作時宜具備共同準則、SSE-CMM 與 ISO/IEC 17799 等知識方能勝任愉快。

第五章、資訊安全管理系統稽核作業研究

稽核工作之良窳關係到整個資訊安全管理系統(ISMS)執行之成效，在我國方開始推展 ISMS 之驗證工作時，如何避免重蹈 10 年前，推動品質管理系統等：「驗證報告不實，人員素質低落」的覆轍，將是在推動 ISMS 時須探討的課題。本章將以資訊及相關技術之控制目標（Control Object of Information and Related Technology，簡稱 COBIT）為例，說明其在安全控管方面的作業模式；同時就 COBIT 所提出之區分四階段與三十四項之方式，衍生並研析資訊安全管理系統內部稽核作業之內涵，並對稽核之教育訓練提出建議。

5.1 稽核指導方針的訂定

在資訊化的工作環境中，如何控制其契合組織目標的探討，仍不多見，國際上的資訊系統稽核與控制協會（Information Systems Audit and Control Association，簡稱 ISACA），有鑑於此，邀集學者專家參考了三十六份世界公認的標準與規章等相關報告訂定了一份標題為「資訊及相關技術之控制目標」（COBIT）作業規範 [32]，自 1996 年首次發表，1998 年發表第二版，2000 年公布第三版以來，已成為一般公認的「資訊環境控制目標」之標準，在此節中將介紹 COBIT 為滿足對資訊的需求，將針對每一資訊流程訂定出相關的稽核指導方針；期使稽核人員可依據此方針來執行各項的稽核工作。

COBIT 訂定了資訊環境下企業需求、資訊技術資源、資訊技術流程三個交互相關的內部控制要素，提供管理當局、使用者，與稽核人員完整的架構，能輔助管理當局在資訊投資上和風險控制下找出平衡點；幫助使用者在他們獲得的產品與服務的安全和控制方面獲得保證，且提供稽核人員相關的工具與程序以進行內部控制。

為滿足組織對資訊的需求，COBIT 強調資訊科技的資源必須以企業流程的方式來管理。亦即是資訊流程強調建立有效之會計資訊系統與整合資訊系統等，使組織內的人能夠迅速取得並交換、管理及控制其內部工作流程運作所需之訊息；資訊流程可以區分為資訊系統規劃及組織、資訊系統獲得及建置、資訊服務

之交付及支援、資訊環境監督四大範圍，正達到稽核作業所涵蓋的範疇。COBIT 這四個範圍中設計了 34 個資訊流程如下：

一、 資訊系統規劃及組織：

1. 擬定策略規劃
2. 擬定資訊架構
3. 決定技術導向
4. 釐定組織及其關係
5. 專案之投資管理
6. 溝通管理的目標與方向
7. 人力資源管理
8. 確保符合外部需求
9. 風險評估
10. 專案管理
11. 品質管理

二、 資訊系統獲得及建置：

資訊系統獲得與實施範圍下有六個資訊流程。並且在這六個資訊流程下訂定更專門細節的控制目標。

1. 確認解決方案
2. 應用軟體的獲得與維護
3. 技術架構的獲得與維護
4. 開發及維護資訊程序
5. 安裝及認證系統
6. 變更管理

三、 資訊服務之交付及支援：

資訊系統傳送與支援範圍下有十三個資訊流程。並且在這十三個資訊流程下訂定更專門細節的控制目標。

1. 定義服務層次
2. 外包服務管理
3. 績效及容量管理
4. 確保持續服務

5. 確保系統安全

6. 分析及歸屬成本

7. 使用人員的教育及訓練

8. 客戶支援及諮詢

9. 裝備管理

10. 問題及意外管理

11. 資料管理

12. 設施管理

13. 操作管理

四、 資訊環境監控：

最後的領域是資訊環境監控，其下有四個資訊流程。並且在這四個資訊流程下訂定更細緻的控制目標。

1. 監督各項資訊流程

2. 評鑑內部控制的允當性(註：第二版新增)

3. 是否有獨立的品質保證(註：第二版新增)

4. 稽核獨立

COBIT 亦針對每一資訊流程訂定相關的稽核指導方針，使稽核人員可根據相關的指導方針，明確的執行各項稽核工作。內部稽核的過程可分為四個階段：

1. 確認資訊系統可能發生之錯誤與舞弊，風險為何：認識企業需求、相關的風險與控制衡量方法
2. 確認需有那些控制程序存在以降低風險：評量各控制程序的適合度
3. 系統複核和控制測試程序設計：調查測試各控制程序是否如預期的執行，與是否具有一致性與連續性
4. 評估內部控制缺失：使用分析技術與選擇的資料來偵測未符合控制目標的風險

資訊環境稽核過程主要重覆依如圖 5.1 所示之四個階段檢驗各項資訊流程，確保各項資訊流程被適當控管，能產生組織營運活動所需要資訊的品質標準。COBIT 提出了這個連結資訊技術程序、資訊技術資源及企業策略和目標的架構。再者，COBIT 整合及涵蓋了良好的規劃及組織、取得及建置、交付及支援、監控等制度流程，以確保企業資訊和相關技術能維持企業目標[1]。對照圖

5.1 與圖 3.2，BS 7799-2：2002 中資訊安全管理系統過程模式中之「計畫階段」即為 COBIT 中之「規劃及組織」階段，「執行階段」在 COBIT 中分成「獲得及建置」與「交付與支援」2 階段；一般而言，在 ISMS 中之執行階段均有相當比率之與供應商間的稽核工作需要執行，表 5.1 是 COBIT 各個階段作業項目與品質標準及資訊技術資源之關係示意說明。

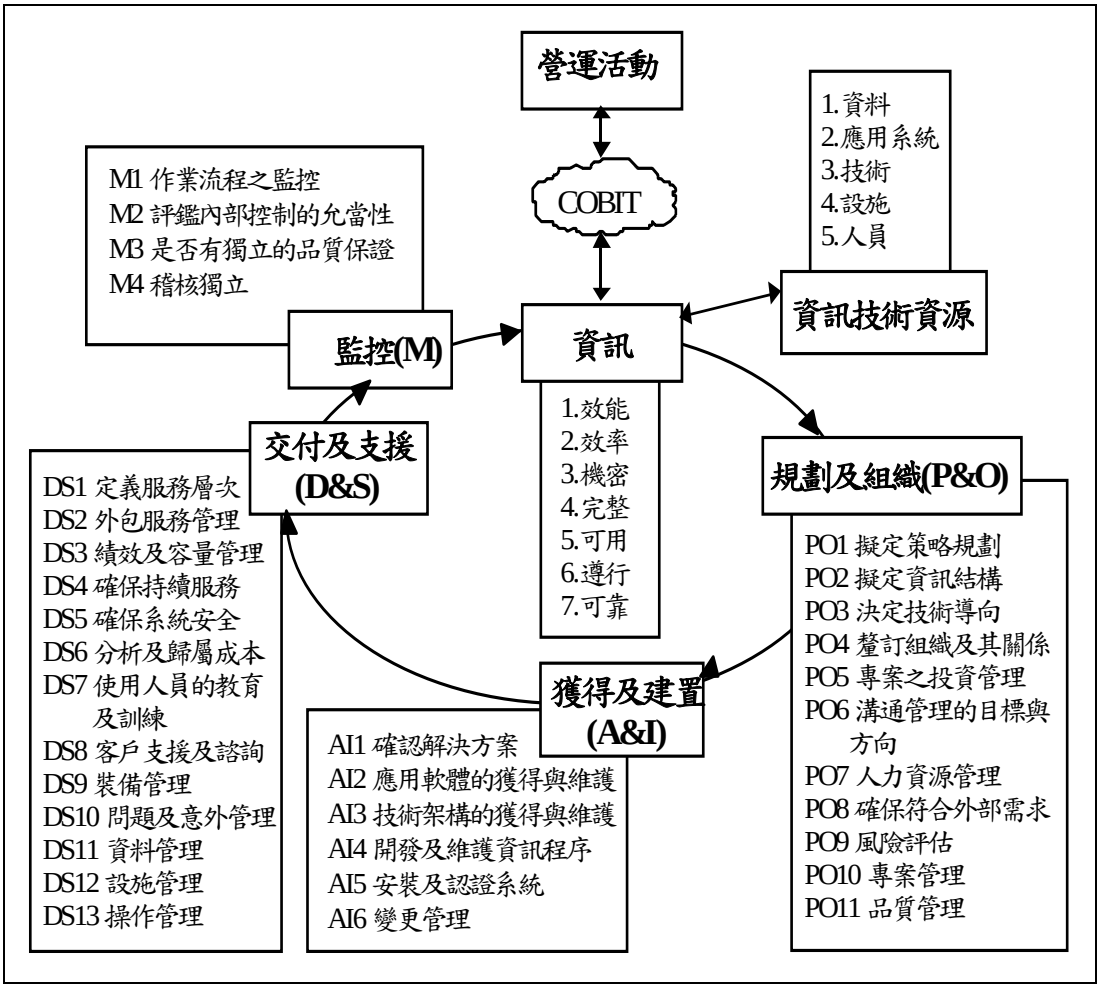


圖 5.1：達成組織營運活動所需要之資訊技術品質準則

表 5.1：COBIT 資訊技術控管作業程序項目

階段	作業	資訊品質標準							資訊技術資源				
		效能	效率	機密	完整	可用	遵行	可靠	人員	應用系統	技術	設施	資料
P&O	PO1	P	S						✓	✓	✓	✓	✓
	PO2	P	S	S	S					✓			✓
	PO3	P	S								✓	✓	
	PO4	P	S						✓				
	PO5	P	P					S	✓	✓	✓	✓	
	PO6	P					S		✓				
	PO7	P	P						✓				
	PO8	P					P	S	✓	✓			✓
	PO9	S	S	P	P	P	S	S	✓	✓	✓	✓	✓
	PO10	P	P						✓	✓	✓	✓	
	PO11	P	P		P			S	✓	✓			
A&I	AI1	P	S							✓	✓	✓	
	AI2	P	P		S		S	S		✓			
	AI3	P	P		S						✓		
	AI4	P	P		S		S	S	✓	✓	✓	✓	
	AI5	P			S	S			✓	✓	✓	✓	✓
	AI6	P	P		P	P		S	✓	✓	✓	✓	✓
D&S	DS1	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	DS2	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	DS3	P	P			S				✓	✓	✓	
	DS4	P	S			P			✓	✓	✓	✓	✓
	DS5			P	P	S	S	S	✓	✓	✓	✓	✓
	DS6		P					P	✓	✓	✓	✓	✓
	DS7	P	S						✓				
	DS8	P							✓	✓			
	DS9	P				S		S		✓	✓	✓	
	DS10	P	P			S			✓	✓	✓	✓	✓
	DS11				P			P					✓
	DS12				P	P						✓	
	DS13	P	P		S	S			✓	✓		✓	✓
M	M1	P	S	S	S	S	S	S	✓	✓	✓	✓	✓
	M2	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	M3	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
	M4	P	P	S	S	S	S	S	✓	✓	✓	✓	✓

說明：

1. 在 COBIT 中依作業需要訂定三種不同程度之應達到的品質標準，其中 P(Primary)：表示此項控管目的完全符合本項品質標準、S(Secondary)：表示此項控管目的稍可或間接符合本項品質標準、空白：表示此項控管目的較符合其他品質標準，或其他控管目的較符合本項品質標準。
2. 由上表可知各作業依其特性，對資訊品質標準之要求而有所不同，亦對資訊技術資源之控管亦所有不同。例如：交付及支援階段中(D&S)資料管理作業(DS11)對資訊技術資源中資料，要求需符合完整性及可靠性之品質標準。

COBIT 資訊技術控管架構如圖 5.2 所示，可區分為資訊技術資源、符合組織營運所需之品質準則及資訊技術作業等三方面加以分析；資訊技術之控管目的可整理成圖 5.3 所示，任一資訊作業之控管目的均可按照圖 5.3 之模式加以套用，並予以描述。

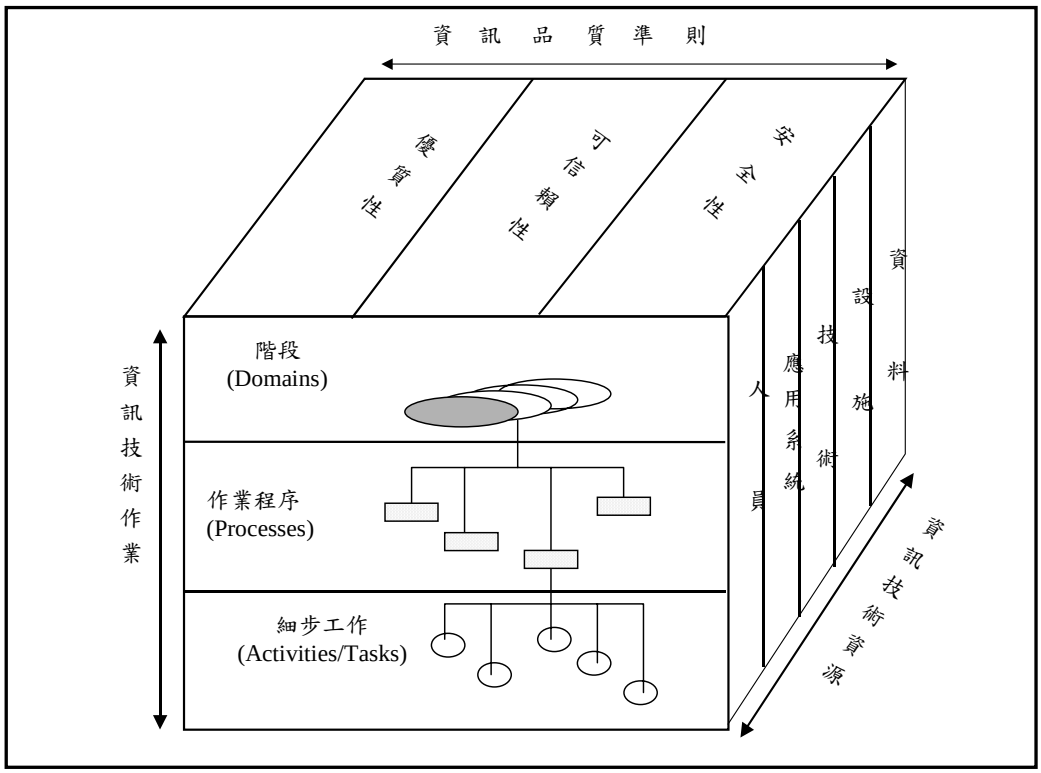


圖 5.2：資訊技術控管架構示意說明

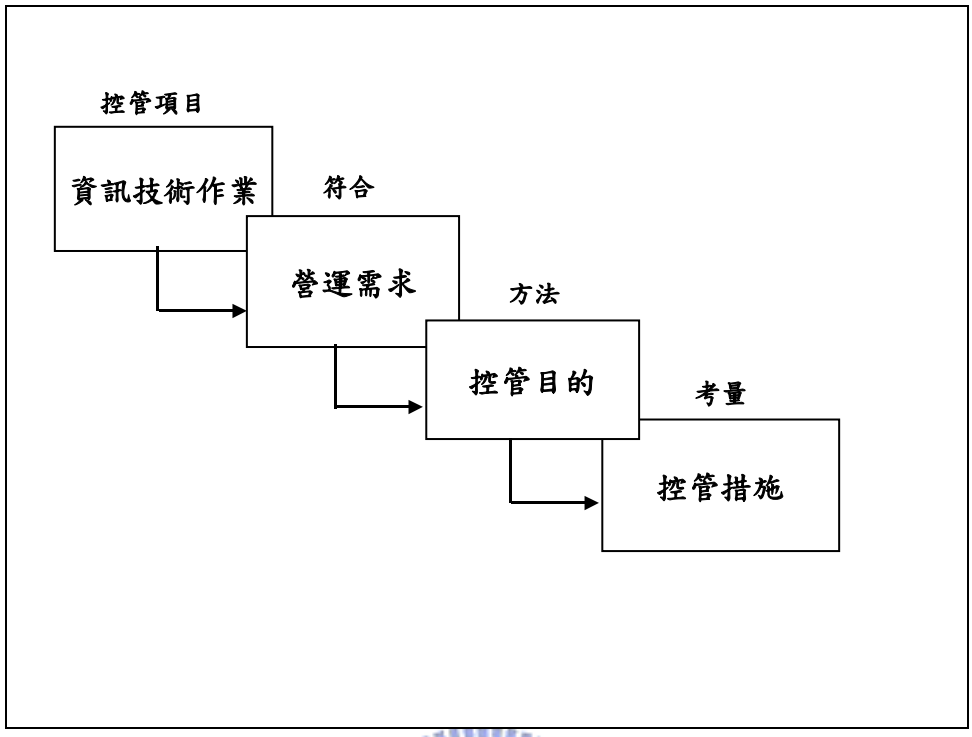


圖 5.3：資訊技術控管塑模示意

因 COBIT 之目的在於能確保達成組織營運所需之品質標準，並用以發現重大缺失；為了達成 COBIT 之標的，其遵循之資訊系統準則如表 5.2 所示。自 COBIT 第三版發行後，其中要求之合格證明準則已不斷地推陳出新，除 BS7799-2：2002 已整理於表 2.2 外，分別將 ISO/IEC 15408 與 ISO/IEC TR 15504 之沿革整理以圖 5.4 與表 5.3 及表 5.4 來表示，並契合如表 5.5 所示之資訊技術保證框架之 ISO/IEC 正研訂中成熟度標準上之要求 [7]。

表 5.2：COBIT 遵循之資訊系統準則

1.遵循規範：OECD 與 ISACA 等公布之原則。
2.技術標準：ISO 與 EDIFACT 等公布之標準。
3.合格證明準則(Qualification Criteria)：
3.1 ISO 9000 (BS7799-2：2002)。
3.2 ISO/IEC 15408。

3.3 ISO/IEC TR 15504 (SPICE)。

4.專業標準：COSO 與 ISACA 等公布之標準。

5.作業規範與需求：英國貿工部(Department of Trade and Industry，簡稱 DTI)及 NIST 等公布之作業規範與需求。

6.產業需求：銀行、電信及電子商務等產業之需求。

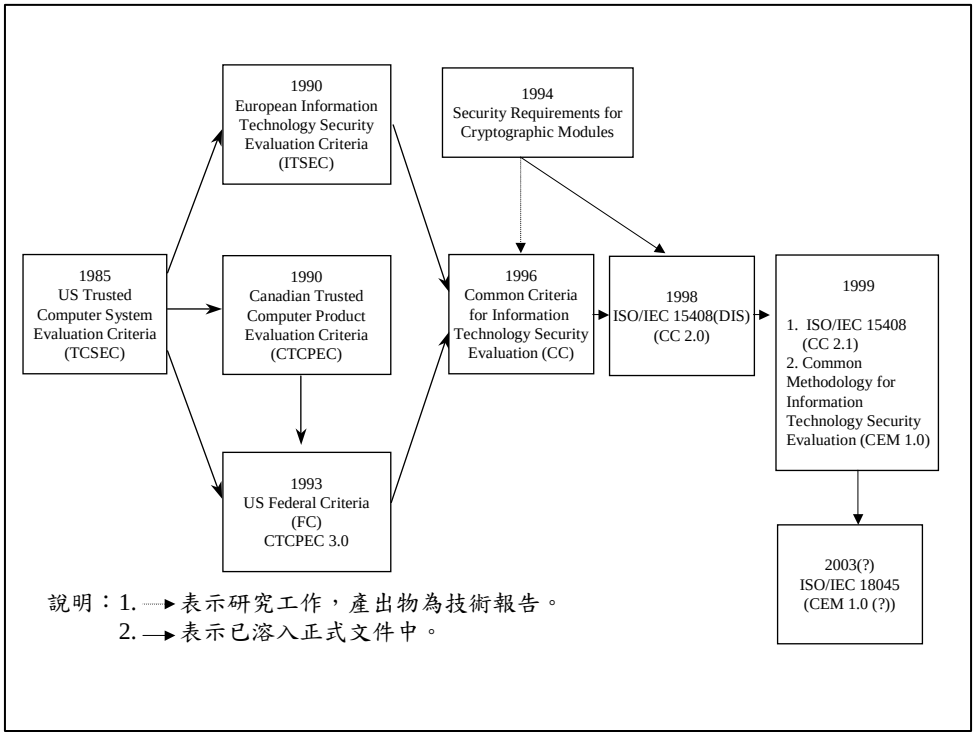


圖 5.4：可信賴資訊系統安全評估準則簡史

表 5.3：資訊技術安全評估準則認證機制簡史

1. 1997年10月7日，美國公告了針對ISO/IEC 15408(以下簡稱CC)通過後認證機制所需之TTAP(Trust Technology Assessment Program) Laboratories，接受植基於CC之測試與評估工作，做為NIAP (National Information Assurance Partnership) CCEVS(Common Criteria Evaluation and Validation Scheme)認證機制建立前之過渡期因應方案。
2. 1997年11月8日，TTAP提出植基CC之認證、驗證檢測工作建議。
3. 1999年4月，美國、加拿大、德國、英國、法國共同簽署CCMRA(Mutual Recognition Agreement)，預期歐洲、亞太其他各國將陸續加入。
4. 1999年5月14日，美國公告了CC認證計畫，同時宣布密碼模組認證計畫將併入此計畫。
5. 1999年6月8日，美國宣布CC 2.1版正式成為ISO/IEC 15408。
6. 2000年5月23~25日，在美國Baltimore International Convention Center舉辦第1次CC國際研討會。
7. 2000年8月30日，美國公告Computer Science Corporation(CSC)，CygnaCom Solutions, Science Applications International Corporation (SAIC)與 TUViT Incoporated 4家民間實驗室已經通過NIAP的認可$CCTL_S$(Common Criteria Testing Laboratories)。
8. 2000年10月13日，美國公告COACT Inc. CAFÉ Laboratory成為通過NIAP認可之第5家$CCTL_S$。
9. 2001年7月18~19日，在英國Brighton舉辦第二次CC國際研討會。
10. 2002年2月15日，美國公告Booz-Allen & Hamilton, Inc. Common Criteria Testing Laboratory成為通過NIAP認可之第6家$CCTL_S$。
11. 2002年5月13~14日，在加拿大Ottawa舉辦第三次CC國際研討會。
12. 2003年9月7~9日，在瑞典Stockholm舉辦第四次CC國際研討會。

表 5.4：ISO/IEC TR 15504 與 ISO/IEC 21827 發展簡史

1. 1991年：

   1.1 1991年6月，國際標準組織(ISO)與國際電子技術委員會(IEC)第一聯合技術委員會(Joint Technical Committee 1，簡稱JTC1)得第七子委員會(Sub-Committee 7，簡稱SC7)提出發展軟體過程評鑑國際標準的議案，經決議通過，由ISO/IEC JTC1/SC7之第十工作小組(Working Group 10，簡稱WG10)成立研究小組，先行準備。

   1.2 1991年8月15日，美國卡內基大學(Carnegie Mellon University)的軟體工程研究院(Software Engineering Institute，簡稱SEI)公布軟體能力成熟度模式(Capability Maturity Model，簡稱CMM)第1版。

2. 1992年6月：ISO/IEC JTC1/SC7大會時，決定成立第十工作小組(WG)執行1991年6月之ISO/IEC JTC1/SC7提案之決議。

3. 1993年：

   3.1 1993年1月，ISO/IEC JTC1/SC7/WG10成立軟體程序改進與能力測定(Software Process Improvement and Capability dEtermination，簡稱SPICE)專案，執行ISO/IEC JTC1/SC7提案。

   3.2 1993年4月，系統安全工程(System Security Engineering CMM，簡稱SSE-CMM)研發工作起動。

4. 1994年：英國貿工部(DTI)遵循ISO 9000，公布軟體品質管理系統建構與驗證指引(Guide to Software Quality Management System Construction and Certification，簡稱TickIT)。

5. 1995年1月：舉辦第一次SSE-CMM研討會。

6. 1996年10月：SEI公布SSE-CMM第1版。

7. 1997年：

   7.1 1997年第1季：SEI公布SSE-CMM鑑定方法(SSE-CMM Appraisal Method，簡稱SSAM) 第1版。

7.2 1997年7月：舉辦第二次SSE-CMM研討會。

8. 1998年10月：SSE-CMM送交 ISO/IEC JTC1/SC7。

9. 1999年：

9.1 1999年4月12日：SEI公布SSE-CMM第2版。

9.2 1999年4月16日：SEI公布SSAM第2版。

10. 2002年10月1日：ISO公布源自SSE-CMM之ISO/IEC 21827。

表 5.5：資訊風險治理成熟度示意說明

成熟度階段	內　　容
0	無： (1)程序或商業決策的風險評鑑作業均付諸闕如。組織未考慮安全脆弱性對業務會帶來哪些影響。組織尚未體認資訊技術的解決方案與服務和風險管理之間有何關係。 (2)組織不瞭解資訊安全的必要性。無人負責安全事務。無任何支援資訊安全管理的作為。若發生資訊安全事件，亦無資訊安全報告或處理程序。未見任何安全管理程序。 (3)管理單位不瞭解資訊作業或服務有哪些風險、脆弱性和威脅。
1	初步、特別狀況： (1)組織以特別案例的角度思考資訊風險的問題，未按照既定的工作程序或政策。採用的風險評鑑作業不是以正式的專案方式進行。 (2)組織已體認到資訊安全的必要性，但對安全的警覺性因人而異。已對資訊安全有處理動作，但無測量標準。若發現資訊安全漏洞，相關人員只會互踢皮球，因權責劃分尚不明確。對資訊安全事件的處理方式無法預估。 (3)負責業務持續運作的權責劃分不明確，權限不高。管理單位已瞭解業務持續運作會有的風險與必要性。
2	可重複，但仍靠直覺： (1)已漸漸瞭解資訊風險的重要性，以及審慎考量的必要性。已有風險評鑑的方式，但程序尚未成熟，且仍在改進中。 (2)資訊安全的權責已派任給資訊安全協調人員，但無管理權限。對

	安全的警覺性分散且有限。有安全資訊，但未進行分析。安全工作只針對事件作處理，採用的是第三人廠商提供的產品，未針對組織的特定需求做修改。安全政策已制訂，但人員技術與工具仍嫌不足。資訊安全報告不夠完整，或有誤導的可能。 (3)已指派人員負責使服務不中斷。但無維護服務持續運作的整套方法。系統可用性（Availability）的報告不完整，亦未考量對業務的影響。
3	已有程序： (1)已有全公司的風險管理政策，規定執行風險評鑑的時間與方式。風險評鑑有既定的程序，且有明文紀錄，所有員工皆可取閱。 (2)安全警覺性已有，且管理單位以正式的報告提醒員工。已定出資訊安全作業流程，並符合安全政策和作業流程的架構。已指派資訊安全的權責，但執行方式不統一。有資訊安全計畫，推動風險分析及安全解決方案。資訊安全報告以資訊技術為中心，而非以業務運作為中心。有非常態性的入侵測試。 (3)管理部門時常宣導服務不間斷的必要性。高可靠性（High availability）元件與系統備援只有零星部署。重要系統及元件的清單非常嚴謹。
4	有管理，且可測量： (1)風險評鑑是標準流程，且資訊管理單位會注意到例外狀況。資訊風險管理可能已是既定的管理部門權責。資深管理人員及資深資管人員已經制定組織可容忍的風險等級，並且有風險、報酬比率的標準量表。 (2)資訊安全的權責劃分明確，且有管理規則、確實執行。資訊安全風險及影響分析作業執行方式適當。安全政策及作業方式（Practice）都根據特定的安全基準完成。安全教育簡報、使用者 ID、身份識別及授權等措施已成為強制規定，並且標準化。入侵測試已標準化，且用來改良安全性。成本效益分析使用次數漸多。安全程序和全公司的組織安全部門協調，且回報機制和營運目標相連。 (3)已施行服務不間斷的權責劃分及標準。系統備援作業（Practice）（包括高可靠性元件）部署方法適當。
5	最適化： (1)風險評鑑已經有架構完整、通行全公司的程序，且員工遵守狀況良好、管理嚴謹。 (2)資訊安全是一般營運管理和資訊管理部門的共同職責，且和企業

	的業務目標整合。安全需求非常明確，且已加入安全計畫，該安全計畫也已經過鑑別。應用程式在設計階段就整合了各項功能，且一般使用者對安全的管理工作也越來越需要負起責任。資訊安全報告提供了早期預警功能，提醒風險已經改變或將來可能出現的危險，並對重要系統採用全自動的主動監測方法。遇到事件時有正式的事件處理程序，並有自動工具軟體協助迅速解決。定時的安全評估作業可評量安全計畫施行的效果。組織會以有系統的方式，蒐集有關新威脅和新脆弱性的資訊，並加以分析，且立刻宣導、執行適當的緩衝控制措施。入侵測試、安全事故根本原因（Root cause）分析和預先（Proactive）辨識風險等作業，都是持續改進工作的基礎。 (3)服務不間斷計畫及業務不間斷計畫互相整合、支援，且定期審核。向廠商及主要供應商購買可滿足服務不間斷需求的產品。

5.2 資訊安全管理系統稽核作業內涵

為確保資訊資產的安全，資訊安全管理系統制度中將稽核視為是重要的安全防護措施，其對資訊系統執行的監控、檢核審視，以及不法行為的偵測都有顯著的效益。資訊安全管理系統稽核之目的在於：「用以獲得作為資訊安全管理系統(ISMS)之一組政策、執行活動或一組將輸入轉換為輸出之相互關連或交互作用的活動(簡稱過程)所規定之方法(簡稱程序)，或要求有關並且能夠查證與確認的敘述所達成結果或提供所執行活動之文件、事實陳述或其他有意義的資料(簡稱(稽核)證據)，同時對它作客觀之評估，以決定 ISMS 作為依據的一組政策、程序或要求之系統，所滿足的程度之獨立的及文件化之過程。」，為達成前述之過程，一般而言，如圖 5.5 所示於稽核工作可以分為：

1. 第一者稽核：又稱為內部稽核，是由組織本身或其代表為內部目的所執行，並可作為組織的自我滿足要求聲明之基礎。
2. 第二者稽核：外部稽核之一，是由對組織的績效或成效有利害關係的個人或團體，例如客戶或由其他代表客戶的人員所執行。
3. 第三者稽核：外部稽核之一，是由外部獨立服務組織所執行，這種組織提供驗證或符合要求登錄資格(公正第三者亦可直接面對供應商/廠商)。

參照圖 5.1 與表 5.1，就 ISMS 第一者、第二者與第三者稽核之工作所需知識及技能等觀點來加以比較，可整理成表 5.6 所示。

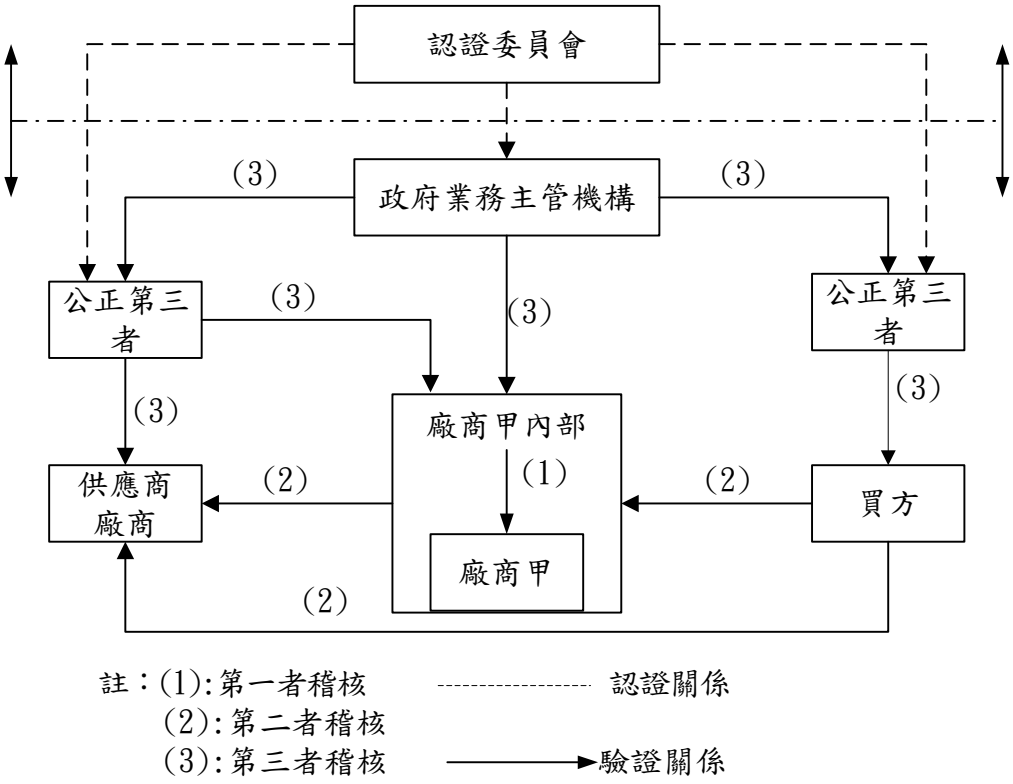


圖 5.5：資訊安全管理系統稽核工作及認證與驗證體系關係示意

表 5.6：資訊安全管理系統(ISMS)第 1、2、3 者稽核工作比較

	第一者稽核	第二者稽核	第三者稽核
稽核重點	有效性與符合性並重。	有效性與符合性並重。	符合性為主，有效性為輔。
稽核角度	察之於內。	內外均需兼顧。	察之於外。
所需知識	資訊安全管理與資訊安全稽核為主，資訊安全工程為輔。	資訊安全工程與資訊安全管理為主，資訊安全稽核為輔。	資訊安全管理與資訊安全稽核為主，資訊安全工程為輔。
所需技能	資訊安全管理為主，資訊安全工程與資訊安全稽核為輔。	資訊安全工程為主，資訊安全管理與資訊安全稽核為輔。	資訊安全稽核為主，資訊安全管理為輔。

5.3 資訊安全管理系統稽核教育與訓練

在英國之已驗證稽核員登錄國際組織（IRCA）公布之 ISMS 主導稽核員訓練課程驗證規範中[38]，分為知識（Knowledge）與技能（Skills）2 類訂定不同之賦能目標（Enabling Objectives），表 4.3 是其最少上課 5 天每天 8 小時的訓練標的之示意說明;在第 2 天的賦能目標中明定必須將 ISO/IEC TR 13335-3 資訊技術(IT)－管理 IT 安全之指導綱要(Guidelines for the management of IT Security ）（註：ISO/IEC TR13335 之簡稱為 GMITS）中之第 3 部分：管理資訊技術（IT）安全的技術（Techniques for the Management of IT Security）與第 4 部分選擇保護措施（Selection of Safeguards）納入。

整理我國現行採行的英國認證服務（United Kingdom Accreditation Service，簡稱 UKAS）規範與 IRCA 對 ISMS 第三者稽核／主導稽核員訓練課程之主要差異如表 5.7 所示，其中 ISO 19011 是新版稽核品質系統之指導綱要[39]；表 5.8 是 IRCA 公布之 ISMS 第三者稽核訓練課程內容引用之標準與學員持續評鑑紀綠，表 5.9 是其測驗之要求示意。台灣地區自 2000 年 9 月 25~29 日起開始，至 2003 年 5 月所舉辦的資訊安全管理系統主導稽核員訓練課程均遵循表 5.7 中 UKAS 之要求，唯無論是在課程內容還是上課時間各方面與 IRCA 公布之規範均有明顯的落差。由於 GMITS 是資訊技術安全風險管理中著名之國際標準，資訊安全風險管理是 BS 7799-2:2002 的基石，IRCA 之要求宜做為我國 ISMS 第三者稽核訓練課程規範的參考藍本之一；於涉及資訊基礎建設時，如執行如表 2.13 中之分級 3 以上的 ISMS，表 4.7 中提及的 ISMS 稽核訓練課程將可作為據以討論之芻議。

表 5.7：UKAS 與 IRCA 對 ISMS 第三者稽核訓練課程主要差異

	UKAS（目前）	IRCA
授課內容應包含之標準與法規	1.BS7799-2:2002(CNS 17800) 2.ISO/IEC17799(CNS 17799) 3.ISO19011 4.EA7/03 5.資訊安全相關法規(電腦處理個人資料保護法、智慧財產權法、電子簽章法等）	1. ISO/IEC TR 13335 (all parts) 2. ISO/IEC 21827 3. ISO/IEC 17799 (CNS 17799) 4. BS 7799-2：2002 (CNS 17800) 5. ISO 19011 6. ISO/IEC 15408 (all parts) 7. ISO/IEC TR 15504 (all parts) 8. ISO 13491 (all parts) 9.資訊安全相關法規（……、電子簽章法、通訊保障監察法、資訊公開法等）
最少上課時數	36 小時	56 小時
講師隨堂最少上課時數	28 小時	56 小時
上課人數	1. 12~20（2 個講師） 2. 6~10 （1 個講師）	1. 12~20（2 個講師） 2. 6~10 （1 個講師）

說明:

1.IRCA 要求之最少上課時間不包含測驗時間與學員自修時間。

2.UKAS 要求之最少上課時間包含學員自修時間(每天 2 小時以上)。

3.UKAS 之資料是至 2003 年 4 月，香港商英國標準協會太平洋有限公司台灣分公司提供之開課資訊。

4.IRCA 之資料是由 2002 年 11 月，IRCA 公布的「ISMS 稽核員（Auditor）/主導稽核員（Lead Auditor）訓練課程驗證準則（IRCA/2106）」整理而得。

5.USKS 之全名為「英國認證服務（United Kingdom Accreditation Service）」，IRCA 之全名為「已驗證稽核員登錄國際組織（International Register of Certificated Auditors，簡稱 IRCA）」。

表 5.8：IRCA BS7799-2:2002 稽核員／主導稽核員訓練課程學員持續評鑑紀錄樣本[38]

本範例文件根據 IRCA/2016 及 IRCA/2000 之最低需求設計。

學員持續評鑑紀錄與課程內容引用之標準

姓名：吳茲仁　　課程日期： 2003 年 4 月 1-5 日

能力	類別	訓練課程內容引用之標準	第一天	第二天	第三天	第四天	第五天	總成績
1.根據稽核作業前後脈絡解釋 BS 7799 的要求。 講員評語：	知識	1.BS7799-2	4	4	6	6	7	6
2.稽核作業的規劃及預備工作。 講員評語：	知識	1.BS7799-2 2.ISO/IEC17799 3.ISO/IEC TR13335-3 4.ISO/IEC TR13335-4 5.EA 7/03		6	8			7
3.藉由有效的訪談、觀察、採樣及製作筆記的方式蒐集客觀證據。 講員評語：	知識	1.ISO 19011 2.EA 7/03			6	6/7		6
4.分析、解釋資訊，以便決定符合要求的程度。 講員評語：	技能	1.BS7799-2 2.ES 7/03			6	8	7	7
5.回報稽核作業，包括製作有效、符合事實、且能增加價值的不符合規定報告。 講員評語：	技能	1.ISO 19011					6	6

每項能力的表現以 1 至 10 分計分（1-2 = 不合格、3-4 = 不理想、5-6 = 可接受、7-8 = 佳、9-10 = 優）。如果要通過課程，學生必須通過每個項目（即每項至少需 6 分），而且考試時必須達到 70 分以上。學生每個項目的表現不一定每天都會計分（灰色部分表示當天不會進行該學習目標的正式持續評鑑作業）。

講員簽名：講師甲　曾有心　　日期：2003 年 4 月 5 日

講員簽名：講師乙　賈悍客　　日期：2003 年 4 月 5 日

說明：

1. IRCA: International Register of Certificated Auditors。
2. IRCA/2016: Certification Security Management Systems。
3. IRCA/2000:Requirements of Training Organization Approval。

表 5.9：IRCA BS7799-2:2002 稽核／主導稽核員訓練課程測驗配分與時間

1. 單選題：15 題，每題 1 分。
2. 簡答題：5 題，每題 5 分。
3. 申論題：3 題，每題 10 分。
4. 不符合報告（Non-Conformity Report，簡稱 NCR）：1 題，至少包含 3 個情境，每題 30 分。
5. 測驗時間最多不得超過 2 小時，70 分（含）以上及格。

資訊安全管理系統（ISMS）第三者稽核之訓練課程未通過 IRCA 之驗證，上完課且考試及格之稽核員無法至 IRCA 登錄[39]，經其稽核過之 ISMS 的驗證合格證書在國際上自然不被認同；在國家資通安全會報的要求下，政府機關即將開始 ISMS 之驗證，如何規範 ISMS 資訊安全管理系統第三者稽核之訓練課程及其登錄機制已是必須面對之國際接軌的問題[12]。在另一方面，除了 ISMS 第三者稽核外，ISMS 第一者與第二者稽核之訓練課程亦宜早做規範，謹慎區分期待性思考（Wishful Thinking）與事實判斷之差異，方不致重蹈 ISO9000 品質管理驗證在我國推動之初時，「稽核報告不實，人員素質不佳」與 ISO14000 環境管理驗證啟動時，「知易行難」等傳言覆轍。根基於此，在圖 4.15 所示資訊系統安全驗證機制運作中，稽核工作宜具備之知識與技能的議題，在論文的第四章已提出如表 4.7 所示之 ISMS 稽核訓練課程芻議做為討論的基礎。

資訊安全稽核的工作環境與其所需扮演角色之多樣化，再加上全球性的資訊安全人才缺乏問題[63]，使得資訊安全稽核工作者在學校主修的學域幾乎無所不有，因之使資訊安全稽核工作專業訓練與人力資源規劃的複雜性更為突顯。資訊安全稽核工作生涯階段及其常扮演的工作角色如表 5.10 所示[16]；一般而言，在

ISMS 系統製作、訓練者與商議者的角色上需要具備資訊安全技術與管理、組織理論、管理資訊系統及數學和理則學方面之知識與技能。在概念孕育者與管理者的角色上，除了上述的資訊安全技術與管理、組織理論、管理資訊系統及數學和理則學外，還要具備作業研究、統計學與經濟學方面之知識與技能；在診斷者與技術者的角色上，需要一般典型之資訊工程科系畢業學生以及資訊安全技術與管理之知識與技能；在未來學者、技術引進者與決策者方面，則需具備上述所有以及危機管理之知識與技能。上述的知識與技能，有些源自其他的學域，有些是資訊學域中較成熟的學門，有些則尚在發展中；以美國為例，自 1992 年 11 月 16 日起，已頒布資訊系統安全專業等系列訓練課程，為執行 NIACAP 仍大量缺乏具備如表 5.11 所示之足夠能量的資訊安全驗證稽核人員[57]的機制。美國國防部已提出 ISMS 稽核員教育課程規劃[57]，海峽對岸在 2002 年已分如表 5.12[34]與表 5.13[36]所示之學士及研究所的 ISMS 專業人員教育課程做為如表 5.14 所示之 ISMS 所示之 ISMS 稽核專業人員證照考試內容的源池。

表 5.10：資訊安全管理工作生涯階段常扮演的工作角色

	第一階段	第二階段	第三階段	第四階段
中心工作項目	學習、協助並執行工作	獨立工作與創造績效	訓練、協助並執行規劃工作	指導、規劃整體工作
組織定位	新進人員(Apprentice)	同僚(Colleague)	指揮與咨議者(Mentor)	負責人(Sponsor)
主要工作哲學	跟隨者(Dependence)	工作者(Independence)	必須對其工作團體負責	對資訊管理整個團體負責
常扮演之工作角色	ISMS 系統製作者、訓練推廣者、商議者、概念孕育者、技術者	ISMS 系統製作者、訓練推廣者、商議者、概念孕育者、診斷者、技術引進者、技術者	ISMS 系統製作者、商議者、概念孕育者、診斷者、技術引進者、未來學者、管理者	商議者、概念孕育者、診斷者、技術引進者、未來學者、管理者、決策者

表 5.11：美國 NIACAP 驗證稽核一般性能量(Capabilities)要求

1. 行政管理安全 (Administrative security)。
2. 人員安全 (Personnel security)。
3. 通訊安全 (Communication security)。
4. 網路安全 (Network security)。
5. 伺服器安全 (Server security)。
6. 終端機/工作站安全 (Client/Workstation security)。
7. 資料庫安全 (Database security)。
8. 資訊安全 (INFOSEC)。
9. 應用安全 (Application security)。
10. 密碼學之金鑰管理 (Cryptographic key management)。
11. 作業安全 (OPSEC)。
12. 電磁洩露與防護 (TEMPEST)。
13. 商業背景 (Business background)。
14. 資訊科學背景 (Computer science background)。
15. 工程背景 (Engineering background)。
16. 稽核能量 (Audit Capabilities)。

表 5.12：北京郵電大學信息工程學院信息安全學士課程剖繪

1. 公共基礎課程：數學、物理、英語等。
2. 主要課程：離散數學、信號與系統、通信原理、軟體工程、編碼理論、信息安全概論、信息論、數據結構、作業系統、微處理機原理與介面技術、通信網理論基礎、計算機網路基礎、資訊系統工程、現代密碼學、網路安全、藏密學、入侵偵測、電腦病毒及其防治等。
3. 專題：大型軟件設計等。

表 5.13：上海交通大學信息安全工程學院碩士課程剖繪

1. 網路安全技術導引 (2 學分)。
2. 通信安全保密技術 (2 學分)。
3. 密碼理論與實踐 (2 學分)。
4. 公開金鑰基礎建設及其應用 (2 學分)。
5. 量子密碼理論 (2 學分)。
6. 電腦病毒 (2 學分)。
7. 高級計算機網路 (3 學分)。
8. 嵌入式系統原理與應用 (2 學分)。
9. 信息安全的數學基礎 (3 學分)。
10. 資料庫理論 (3 學分)。
11. 影像通訊 (3 學分)。
12. 分散式操作系統 (2 學分)。

表 5.14：海峽對岸註冊信息安全專業人員(Certified Information Security Professional，簡稱 CISP)中之註冊信息安全審核員(Certified Information Security Auditor，簡稱 CISA)考試內容

1. 培訓基本能力要求：
1.1 了解水平：培養對安全信息系統的威脅和脆弱性的敏感性，識別需要保護的數據、信息及其相應的保護方法，學習掌握有關信息系統安全的法則和條例的知識庫。
1.2 應用水平：培養有能力對信息安全過程進行設計、執行或者評估的人員，以保證他們在執行任務的時候，可以完整地應用安全概念。
2. 安全體系與模型：
2.1 多級安全模型：
2.1.1 引言
2.1.2 Bell-LaPadula 模型
2.1.3 Clark-Wilson
2.1.4 Biba 模型
2.2 多邊安全模型：
2.2.1 引言
2.2.2 訪問控制矩陣(Compartmentation and Lattice)模型

2.2.3 Chinese Wall 模型

2.2.4 BMA 模型

2.3 安全體系結構：

2.3.1 OSI 參考模型

2.3.2 開放系統互連安全體系結構

2.4 Internet 安全體系架構：

2.4.1 ISO 安全體系到 TCP/IP 映射

2.4.2 IPSec 協議

2.4.3 IPSec 安全體系結構

2.4.4 安全協議

2.4.5 IKE 概述及 IPSec 的應用

2.5 信息安全技術測評認證：

2.5.1 IT 評估通用準則

2.5.2 IT 評估通用方法

2.5.3 信息安全國內外情況

3. 安全技術：

3.1 密碼技術及其應用：

3.1.1 加密基本概念

3.1.2 對稱加密算法

3.1.3 非對稱加密算法

3.1.4 鏈路層加密技術(L2TP)

3.1.5 網絡層加密技術(IPSEC)

3.1.6 VPN 虛擬專網

3.1.7 IKE 概述及 IPSec 的應用

3.1.8 SSL/TLS 與 SSH

3.1.9 PKI

3.2 訪問控制

3.3 標識和鑑別

3.4 審計及監控

3.4.1 安全審計

3.4.2 安全監控

3.4.3 入侵監測

3.4.4 實際應用

3.5 網絡安全

3.5.1 網絡基礎(網絡組建、管理與安全)

3.5.2 網絡安全

3.5.3 安全邊界及邊界間安全策略

3.5.4 網絡攻擊與對策

3.6 系統安全

3.6.1 操作系統安全

3.6.2 數據庫系統安全

3.7 應用安全

3.7.1 計算機病毒

3.7.2 Web 安全

3.7.3 安全編程

4. 工程過程

4.1 風險評估

4.1.1 安全威脅

4.1.2 安全風險

4.1.3 評估過程

4.2 安全策略

4.2.1 組織安全策略

4.2.2 系統安全策略

4.2.3 安全策略示例

4.3 安全工程

5. 安全管理

5.1 安全管理基本原則

5.2 安全組織保障

5.2.1 政府計算機網絡安全管理機構的職責

5.2.2 中國信息安全產品測評認證中心

5.2.3 國家計算機病毒應急處理中心

5.2.4 中國計算機網絡安全應急處理協調中心

5.2.5 企業信息安全管理機構職責和工作制度

5.3 物理安全

5.3.1 設施安全

5.3.2 物理安全技術控制

5.3.3 環境安全

5.3.4 電磁洩漏

5.4 運行管理

5.4.1 網絡設備採購

5.4.2 網絡管理平台選擇

5.4.3 網絡產品安全檢測

5.4.4 網絡配置管理

5.4.5 網絡安全管理

5.4.6 網絡故障分析管理

5.4.7 網絡性能管理

5.4.8 網絡計費管理

5.4.9 網絡訪問控制與路由選擇

5.4.10 網絡管理的協議

5.5 硬件安全管理

5.5.1 設備選型

5.5.2 安全檢測

5.5.3 設備購置與安裝

5.5.4 設備登記與使用

5.5.5 設備維護

5.5.6 設備保管

5.5.7 質量控制

5.6 軟件安全管理

5.6.1 概述

5.6.2 軟件的選型與購置

5.6.3 軟件安全檢測與驗收

5.6.4 軟件安全跟蹤與報告

5.6.5 軟件版本控制

5.6.6 軟件安全審查

5.6.7 軟件使用與維護制度

5.7 數據安全管理

5.7.1 數據安全的基本概念

5.7.2 安全管理目標

5.7.3 數據載體安全管理

5.7.4 數據密級標籤管理

5.7.5 數據存儲實現管理

5.7.6 數據訪問控制管理

5.7.7 數據備份管理

5.7.8 數據完整性管理

5.7.9 數據可用性管理

5.7.10 不良信息監控管理

5.7.11 可疑信息跟蹤審計

5.8 人員安全管理

5.8.1 建立安全組織

5.8.2 安全職能獨立

5.8.3 人員安全審查

5.8.4 崗位安全考核

5.8.5 人員安全培訓

5.8.6 安全保密契約管理

5.8.7 離職人員安全管理

5.9 應用系統管理

5.9.1 系統自動安全審查管理

5.9.2 應用軟件監控管理

5.9.3 應用軟件版本安裝管理

5.9.4 應用軟件更改安裝管理

5.9.5 應用軟件備份管理

5.9.6 應用軟件維護安全管理

5.10 操作安全管理

5.10.1 操作權限管理

5.10.2 操作規範管理

5.10.3 操作責任管理

5.10.4 操作監控管理

5.10.5 讓操作恢復管理

5.11 技術文檔安全管理

5.11.1 文檔密級管理

5.11.2 文檔借閱管理

5.11.3 文檔登記和保管

5.11.4 文檔銷毀和監毀

5.11.5 電子文檔安全管理

5.11.6 技術文檔備份

5.12 災難恢復計畫

5.12.1 災難恢復的概念

5.12.2 災難恢復技術概述

5.12.3 災難恢復計畫

5.13 安全應急響應

5.13.1 安全應急響應的現狀

5.13.2 安全應急響應管理系統的建立

5.13.3 安全應急響應的過程

6. 信息安全標準

7. 法律法規

7.1 國家法律

7.2 行政法規

7.3 各部委有關規章及規範性文件

人才為 ISMS 稽核工作推動的根本，為奠定如圖 5.6 所示[44]的 ISMS 稽核工作能力(Competence)之教育基礎，參照如表 5.12、表 5.13 與英國等相關教育與訓練課程[2,29,33,69]，為培育 ISMS 稽核工作等之資訊安全專業人才，宜結合國內相關資源，開設類似國外已逾 10 年的資訊安全教育課程[69]，在此提出如表 5.15 與表 5.16 所示之資訊安全碩士課程芻議[17]，做為討論上的參考。

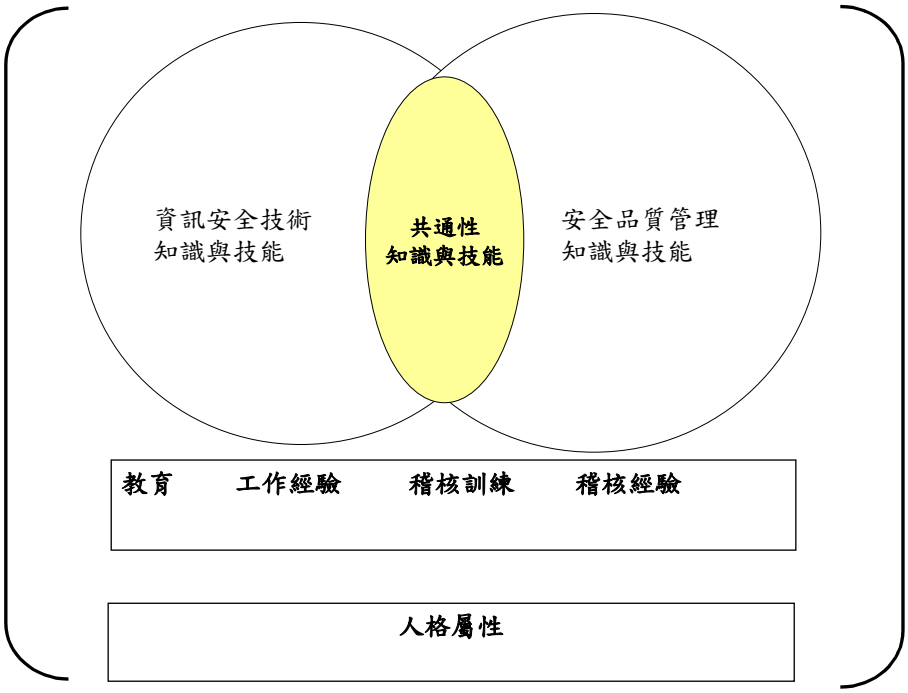


圖 5.6：ISMS 稽核能力概念

表 5.15：資訊安全課程內容芻議

1. 資訊安全管理(Information Security Management)(必)。
2. 密碼學與安全機制(Introduction to Cryptography and Security Mechanisms)(必)。
3. 網路安全(Network Security)(必)。
4. 電腦安全(Computer Security)(必)。
5. 電子商務安全與其應用(Secure Electronic Commerce and other Application)(必)。
6. 安全評估準則(Security Evaluation Criteria)(必)。
7. 資料庫安全(Database Security)。
8. 高等密碼學(Advanced Cryptography)。
9. 程式安全(Secure Programming)。
10. 入侵偵測(Intrusion Detection)。
11. 電腦犯罪與鑑識(Computer Crime and Forensics)。
12. 商業與安全議題(Business and Security Issues)。
13. 專題實作(Project Hands-on)(必)。
14. 論文(Thesis)(必)。

說明：1. 必：表示必修，其他為選修。

2. 每一課程均為一學期(Semester)，除論文與專題為 2 學分外，其他均為 3 學分。每一學生須修畢 24 學分(含)以上。

表 5.16：電子商務安全課程芻議

1. 商業與安全議題(Business and Security Issues)(必)。
2. 密碼學與安全機制(Introduction to Cryptography and Security Mechanisms)(必)。
3. 安全電子商務：基礎建設與標準(Secure Electronic Commerce: Infrastructure and Standard)(必)。
4. 電子商務相關法律與規範(Legal and Regulatory Aspects of Electronic commerce)(必)。
5. 電子商務安全發展近況(Current Developments in Secure Electronic Commerce)(必)。
6. 安全評估準則(Security Evaluation Criteria)(必)。
7. 資訊安全：電腦、網路與資料庫(Information Security: Computer, Network and Database)。
8. 高等密碼學(Advanced Cryptography)。
9. 程式安全(Secure Programming)。
10. 入侵偵測(Intrusion Detection)。
11. 電腦犯罪與鑑識(Computer Crime and Forensics)。
12. 資訊安全管理(Information Security Management)。

說明：1. 必：表示必修，其他為選修。

2. 每一課程均為一學期(Semester)，除論文與專題為 2 學分外，其他均為 3 學分。每一學生須修畢 24 學分(含)以上。

資訊安全的活動是一個尚待開拓的園地，我國開始關心資訊安全管理系統驗證與稽核的機制，時間還不算久，經驗的累積還少，如何建立能與國際接軌的合適方法並培育具備適宜能量的驗證稽核人員，實應展開更深入的思考與討論。

第六章、結論與未來研究方向討論

在現今資訊化與全球化的時代，由於資訊作業已逐漸取代人工作業，特別是關鍵性的資訊基礎建設一旦無法正常運作，將會造成企業組織莫大的傷害及衝擊，更可能攸關組織未來的存亡。鑑於資訊科技在企業組織內的各類應用已相當普及與深化，組織內的各個成員已瞭解資訊資產的重要性；因此在資訊管理的研究及實務的領域中，安全議題的探討已愈加顯得重要。諸如哈佛商業評論(Harvard Business Review)期刊於今年 6 月份發刊的尖端話題單元－「顛覆資訊安全的迷思(The Myth of Secure Computing)」論文中，就論及數位安全的議題，強調滴水不漏的防禦工事是不存在的；不過，你可以依循有效的資訊安全防護運作方式降低風險[66]。

本論文以資訊安全管理系統（ISMS）為研究的核心主軸，因 ISMS 的目標係透過一整體規劃之資訊安全解決方案，以確保企業組織所有資訊系統與各項作業在資訊安全政策接受之風險下，能持續安全並運作順暢，我們已分從 ISMS 驗證作業之分級與其計畫、檢查與稽核等三方面深入探討，綜理歸納已完成的主要貢獻有：

一、提出了建置資訊安全管理系統 P-D-C-A 工作循環時須遵循標準的模式，且與現行美國正推動之資訊安全管理系統驗證與認證過程計畫的要求[53,54,68]殊途同歸，得以印證本論文第二章研提與國際接軌之資訊安全管理系統分級處理構想的可行性。

二、提出資訊安全管理系統稽核訓練的基本課程內涵，可作為 ISMS 驗證工作時宜具備之知識與技能討論的基礎。

三、提出整合 ISO/IEC 15408 及 ISO/IEC 17799、ISO/IEC 21827 的驗證與認證過程，可作為未來 ISMS 實作之參考。

基於本論文已有之基礎，未來可繼續努力的研究方向有：

一、因資訊安全管理系統之模式，針對不同類別之組織特性，訂定有效且適合的評估與管理機制，應依個案性質而有所不同。針對特定系統的共同準則之保護剖繪[51]，研訂不同類別特性的資訊安全管理系統模式是應被探討之課

題。

二、如何結合現行我國對資訊教育訓練的做法，並參考國際上的課程要求；進而訂定相關教育與訓練課程綱要亦是未來尚待研究的議題。

三、進行風險評鑑，將威脅、脆弱點及資產等構面予以有效之量化，據以建立風險分級的基準，以便建立適宜之控制措施，是值得研究的議題。

近年來，資訊科技的進步及網際網路的迅速發展，伴隨而來之資安事件，已成為現今社會日益重要的議題。資安事件其造成的傷害輕者會導致組織內的資訊系統及作業受到影響，甚至停擺；造成的傷害重者將促使國家的關鍵資訊基礎建設之運作失效，一旦癱瘓了金融體系、電力系統或國家安全等層面之建設，其影響所及難以估計。當前資訊資產已成為組織營運上核心的一環，在我國推動「知識經濟 e-Taiwan 高科技服務島」的今天，構建「運用資訊通信科技、寬頻到家與 e 化交通、政府、商務、生活」等願景，確保資訊系統的安全將成為關鍵因素之一，其中運用共同準則建立資訊安全管理系統的機制是現行國際標準組織正致力推動的方向之一，也是本論文研究的重點，故提出資訊安全管理系統實作機制，並探究其規劃、稽核及教育與訓練的內涵，以健全組織資訊安全管理的能力，期使達到「防微杜漸、發奸摘伏」之成效以避免組織營運上的重大損害 [3,53]。

參 考 文 獻

[1] 中華民國內部稽核協會 (1995) 內部控制之觀念與責任－ 內部稽核執業準則公報第一號，中華民國內部稽核協會。

[2] 中國信息協會信息安全專業委員會 (2003) 2002 年~ 2003 年中國信息安全年鑑，中國信息協會信息安全專業委員會。

[3] 中國時報 7 版，2002 年 10 月 25 日，周克威、賴育漣/台北報導。

[4] 李美華譯，Babbie, E. 著（1998） 社會科學研究方法， 8th Edition，時英出版，台北。

[5] 徐鈺宗與樊國楨 （2002） 管理資訊技術安全指導原則運用初探，資訊安全論壇，第 12 期，頁 42－52。

[6] 徐鈺宗與樊國楨 （2003） ISMS 稽核工作初探，資訊安全論壇，第 13 期，頁 38－42。

[7] 徐鈺宗與樊國楨 (2003) 資訊及其相關技術之控管目的與資訊安全管理系統內部稽核簡析，堅實我國資訊安全管理系統稽核作業相關標準系列討論會之七(會議資料)，頁 91－106。

[8] 朱樹德 (1990) 國家標準國際化之研究，經濟部中央標準局。

[9] 行政院 (2001) 中華民國九十年二月五日，台九十經字第OO七四三一號函。

[10]行政院資訊與通信基本建設專案推動 (National Information Infrastructure，簡稱 NII)小組 (2001) 國家資通安全會報第一次會議(會議資料)，行政院資訊與通信基本建設專案推動小組。

[11] 經濟部標準檢驗局 (2001) APEC-SBS 研討會論文集，2001 年 9 月 22 日，台北市，經濟部標準檢驗局。

[12] 經濟部標準檢驗局 (2001) 品質系統稽核指導綱要，CNS 13351（所有部分），經濟部標準檢驗局。

[13] 經濟部標準檢驗局（2002） 資訊技術－ 資訊安全管理作業要點，CNS 17799，經濟部標準檢驗局。

[14] 經濟部標準檢驗局（2002） 資訊技術－ 資訊安全管理系統規範，CNS 17800，經濟部標準檢驗局。

[15] 溫鳳祺 (2003) ISO/IEC Guide 73：2002(E/F) 風險管理－詞彙－標準使用指

引，資訊安全論壇，第 11 期，頁 33－40。

[16] 樊國楨 (1990) 從組織觀點簡析資訊管理所需的專業教育與人力資源規劃，電腦學刊，第二卷，第一期，頁 30－41。

[17] 樊國楨、林樹國與羅濟群 (2003) 資訊安全管理系統驗證之教育與訓練課程的研究。

[18] 樊國楨與方仁威 (2003) 資訊系統安全評估及測試保證之研究，資訊安全論壇，第 9 期，頁 41－56。

[19] 樊國楨等 (2002) 資訊安全能力評鑑，行政院國家科學委員會科學技術資料中心。

[20] Abrams, M.D. and P.J. Brusil (2000) Application of the Common Criteria to a System: A Real-World Example, Computer Security Journal, Vol.16, No.2, pp.11－21.

[21] Ahlbin, M. and P. Ronn., “Implementation of an ISMS in the National Tax Board of Sweden”, in Presentation of The 4th International Common Criteria Conference, Sept 7~9, 2003, Stockholm, Sweden.

[22] Andrew Rathmell (2001) Protecting Critical Information Infrastructures, Computers & Security, Vol.20, pp. 43－52.

[23] Andrew Ren-Wei Fung, Kwo-Jean Farn, and Abe C. Lin (2003) A Study on the Certification of the Information Security Management Systems, Computer Standards & Interfaces. September 2003, Vol. 25, Issue 5, pp. 447－461.

[24] BSi (British Standards Institution) (2002) Information Security Management － Part 2： Specification for Information Security Management Systems, BS7799-2：1999；Information Security Management Systems— Specification with guidance for use. BS7799-2： 2002, BSi, September, London.

[25] Ellison, R.J. etal. (1999) Survivable Network System Analysis：A Case Study, IEEE Software, Vol.16, No.4, pp.70－77.

[26] Eloff, M. M. and J. H .P. Eloff (2003) Information Security Management System：Processes and Products, SEC 2003, Security and Privacy in the Age of Uncertainty, pp. 193－204, Kluwer Academic Publishes.

[27] Hernmann, D.AND S. Keith (2001) Application of the Common Criteria to a System: A Case Study, Computer Security Journal, Vol,17, No.2, pp21－28.

[28] Hone, K. and J.H.P. Eloff (2002) Information Security Policy－What Do International Information Security Standards Say？, Computer & Security, Vol.21, No.5, pp.402－409.

[29] http://is.lse.ac.uk/Support/guides01/IS476.htm 及 /IS484.htm (2002 年 2 月 22 日)。

[30] http://www.commoncriteria.org。

[31] http://www.faa.gov/ait/funcreq。

[32] http://www.isaca.org。

[33] http://www.lse.ac.uk/graduate/course/msc-information-systems-security.html (2003 年 10 月 12 日)。

[34] http://www.southcn.com/edu/zhuanti/xy2002gk/yxdt/200205310322.htm(2003 年 10 月 12 日)。

[35] http://www.sse-cmm.org。

[36] http://www.stdtc.com/xuexiao/zs/(2003 年 10 月 12 日)。

[37] IEC (1995) Dependability Management— Part 3： Application Guide— Section 9： Risk Analysis of Technology Systems, IEC 300-3-9：1995, IEC.

[38] IRCA (2002) Certification Criteria for the Information Security Management Systems Auditor/Lead Auditor Training Course, IRCA/2016, November 2002, IRCA.

[39] IRCA (2003) Certification as an Information Security Management Systems Auditor, IRCA/802, January 2003, IRCA.

[40] ISO (1997) Banking, Securities and Other Financial Services— Information Security Guidelines, ISO TR 13569：1997(E), ISO.

[41] ISO (1999) Information technology－ Security techniques－ Evaluation criteria for IT security (All parts), ISO/IEC 15408：1999(E), ISO.

[42] ISO (International Organization for Standardization)/IEC (International Electrotechnical Commission) (2000) Information Technology—Code of Practice for Information Security Management , ISO/IEC 17799：2000 (E), ISO.

[43] ISO (2001) Information Technology － Guidelines for the Management of IT Security Part 1－5, ISO/IEC TR 13335 (All Parts), ISO, Geneva.

[44] ISO (2002) Guidelines for Quality and/or Environmental Management Systems

Auditing, ISO 19011：2002, ISO.

[45] ISO (2002) Health informatics － Public Key Infrastructure Part 1－3, ISO/TS 17090 (All Parts), ISO.

[46] ISO (2004) Information technology－ Security techniques－ A framework for IT security assurance (All parts), ISO/IEC DTR 15443-1, DTR 15443-2 and 4th WD 15443-3, ISO.

[47] ISO (2003) Information technology—Security techniques-Information security incident management, ISO/IEC DTR 18044, ISO.

[48] Katzke, S. (2003) Protecting Federal Information systems and Networks, in Presentation of The 4th International Common Criteria Conference, Stockholm Sweden, 7~9, Sept, 2003.

[49] Katzke, S., "The Common Criteria (CC) Years (1993~2008): Looking Back and Ahead", in Presentation of The 4th International Common Criteria Conference, Sept 7~9, 2003, Stockholm, Sweden.

[50] Kwo-Jean Farn, Shu-Kuo Lin, and Andrew Ren-Wei Fung (2004) A Study on Information Security Management System Evaluation－ Assets, Threat and Vulnerability, Computer Standards & Interfaces. April 2004, Vol. 26, pp. 501－513.

[51] Marshall Potter (2001) System Level Protection Profiles： A Mechanism for defining ISS Requirements for the NAS(National Airspace System), Lecture Notes in March 7, 2001 Presentation, FAA(Federal Aviation Administration).

[52] Nash, M., "Evaluation the Parts Ordinary Criteria Cannot Reach: Using ISO 17799 to Evaluate Non-Deterministic Security Requirements", in Presentation of The 4th International Common Criteria Conference, Sept 7~9, 2003, Stockholm, Sweden.

[53] National Security Agency (2002) Information Assurance Technical Framework, Version 3.1, National Security Agency (http://www.iatf.net).

[54] National Security Telecommunications and Information Systems Security Committee (NSTISSC) (2000) National Information Assurance Certification and Accreditation Process, NSTISSC No. 1000, April 2000.

[55] NBS (National Bureau of Standards) (1983) Guideline for Computer Security Certification and Accreditation, FIPS(Federal Information Processing Standards) PUB(Publication) 102, NBS.

[56] NIST (2001) Security Requirements for Cryptographic Modules, FIPS PUB 140-2, NIST.

[57] NSTISSI (2000) NSTISSI No. 4015, December 2000.

[58] OECD (1992) Guidelines for Security of Information Systems, OECD.

[59] OECD Workshop (2001) OECD Workshop Information Security in a Network World, September 2001, Tokyo, Japan, pp. 12－13.

[60] OECD (2002) Guidelines for the Security of Information Systems and Networks － Towards a Culture of Security, OECD.

[61] Ohlin, M., "Common Criteria--Related Activities within International Standardization in JTC1/SC27", in Presentation of The 4th International Common Criteria Conference, Sept 7~9, 2003, Stockholm, Sweden.

[62] Out, D. – J. (2003) How to Write Useful security Targets, in Presentation of The 4th Information Common Criteria conference, Sept 7~9, 2003, Stockholm, Sweden.

[63] Rasmussen, C.W. etal. (2003) A Program for Education in Certification and Accreditation in Security Education and Critical Infrastructure, eds. By Irvine, C. and H. Armstrong, pp. 131－150, Kluwer Academic Publishes.

[64] Reid, R. C. and S. A. Floyd (2001) Extending the Risk Analysis Model to Include Market － Insurance, Computers & Security, Vol.20, No.4, pp. 331－339.

[65] Roback, E.A. (2000) Guidelines to Federal Organizations on Security Assurance and Acquisition/ Use of Tested/ Evaluated Product, NIST.

[66] Robert D. Austin and Christopher A.R. Darby (2003) The Myth of Secure Computing, Harvard Business Review, Vol.81, No.6, pp.120－126, June 2003.

[67] Ronald L.Krutz and Russell Dean Vines (2001) The CISSP Prep Guide：Mastering the Ten Domains of Computer Security, John Wiley & Sons, Inc., New York, U.S.A.

[68] Ross, R. and M. Swanson (2003) Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems, NIST SP 800-37, NIST.

[69] Royal Holloway, University of London (2002) MSC in Information Security, December 2002, Royal Holloway (http://www.rhul.ac.uk).

[70] Schneider, F.B. (1999) Trust in Cyberspace, National Academic Press, Washington, D.C., U.S.A.

[71] Solms, B. and R. Solms (2001) Incremental Information Security Certification, Computer & Security, Vol.20, No.4, pp. 308－310.

[72] Swanson, M. (2001) Security Self-Assessment Guide for Information Technology Systems, NIST SP 800-26, NIST.

[73] The White House (2000) National Plan for Information Systems Protection Version 1.0, pp. 101－102.

[74] U.S.A. Federal Deposit Insurance Corporation (1998) Division of Supervision. Electronic Banking：Safety and Soundness Examination Procedures, June 1998.

[75] Von Bertalanffy, L., (1968) General System Theory, New York：George Braziller.

[76] Williams, Paul, (2001) Information Security Governance, Information Security Technical Report, Vol.6, No.3, pp. 60－70.