國 立 交 通 大 學

管理學院（資訊管理學程）碩士班
碩士論文

資訊安全管理系統與企業網路安全實作探討

A study on information security management system and implementation of a secure enterprise network

研 究 生： 鄭東昇
指導教授： 羅濟群 博士
樊國楨 博士

中華民國九十四年七月

資訊安全管理系統與企業網路安全實作探討

A study on information security management system and implementation of a secure enterprise network

研 究 生：鄭東昇　　Student：Tung-Sheng Cheng
指導教授：羅濟群 博士　　Advisor：Dr. Chi-Chun Lo
指導教授：樊國楨 博士　　Advisor：Dr. Kwo-Jean Farn

國 立 交 通 大 學
管理學院（資訊管理學程）碩士班
碩 士 論 文

A Thesis
Submitted to Institute of Information Management
College of Management
National Chiao Tung University
In Partial Fulfillment of the Requirements
For the Degree of
Master of Business Administration
in
Information Management
July 2005
Hsinchu, Taiwan, the Republic of China

中　華　民　國　九　十　四　年　七　月

資訊安全管理系統與企業網路安全實作探討

研 究 生：鄭東昇　　指導教授：羅濟群 博士
指導教授：樊國楨 博士

國立交通大學資訊管理研究所

摘要

許多組織仰賴 IT 資源，並且相信它們是可靠的。然而，網路安全問題卻會隨著時間變得更加錯綜複雜，影響也將會不斷擴大，一旦公司資產的安全性受到危害而導致災難性後果，停機數天所帶來的損失將會難以估算。今日有關資訊安全宜遵循的策略，都是在不完整之資訊內容下做決定的，標準可以減輕因不完整資訊引發之困難，因為標準可以減少選擇的範圍而簡化資訊之供給與需求決策制定的過程。

本研究以實例探討方式將評核企業已實施之資訊安全控制措施與我國經濟部標準檢驗局起草修訂之新版國家標準 CNS 17799（ISO/IEC 17799：2005（E））所列出之控制項目進行檢測比對。並以「符合度」指標探討該企業現行資訊安全制度與資訊安全管理規範之符合程度以分析有待改善之控制措施項目與所造成之風險，並且根基於標準相關控制措施提出「企業安全性修補程式之架構設計」是可用以支援可信賴資訊安全使用環境可行之解決方案之一。

本研究之成果從企業安全性修補程式之架構與相關網路安全偵測實作中比較發現新架構可將伺服器更新比率由 85%提高至 99%(提昇 14%)，並且在完成安全性修補程式更新時間方面，將工作站更新時間從 1394 人/天減少為 32 人/天，對於網路上未受管理之工作站可以採用更強烈的主動偵測方式移除此電腦的網路連線。實作結果可大幅提昇對抗惡意軟體的控制措施之有效性。

在資訊安全的研究與運用方面，由於電子商務活動的日益頻繁，網路安全勢必成為未來人類交易行為轉型的成功關鍵，而電腦病毒與系統入侵卻是在資訊科技發展中不易消除的障礙。本研究藉由分析企業網路安全宜採用之控制措施並且提出實作成果，希望對於企業之資訊人員從事企業網路安全規劃時，可依本研究結果做基礎進行規劃作業，則可有效減少資訊人員在規劃上進行評估及分析的時程。

關鍵字: 資訊安全管理系統（Information Security Management Systems）、缺點修補（Flaw Remediation）、標準（Standard）

A study on information security management system and implementation of a secure enterprise network

Student：Tung-Sheng Cheng　　Advisor： Dr. Chi-Chun Lo
Dr. Kwo-Jean Farn

Institute of Information Management
National Chiao Tung University
Hsinchu, Taiwan, Republic of China

Abstract

A lot of organizations are dependent on IT resources，and believe that they are reliable. However，the online security question will become more intricate、influential and expand constantly with time. Once the security of company's assets will be endangered and caused the calamitous consequence, the losses will be difficult to estimate to shut down for several days. Today all make the decision under the incomplete information that should be followed. The standard can lighten the difficulty caused because of incomplete information. Course that the standard can reduce the range and demand of simplifying information chosen and make policy.

This research is based on draft new national standard CNS 17799（ISO/IEC 17799：2005（E））that enterprises have already implement to analysing control measure project improved to remain in enterprise information security system. And the solution「Architecture design for enterprise security patch management」is proposed in the relevant control measure of the standard and it can be used to support the information security with feasible environment for use. To examine from the new structure can increase the upgrade rate of the server from 85% to 99%, and reduce the update time of workstation from 1394 man-day to 32 man-day. The solution is well approved for malice code protection.

Because electronic commercial activity is frequent day by day，the online security certainly will become the successful key that the human trading activity of future make the transition. It is obstacles difficult to dispel in the development in science and technology of information that electronic virus and system are invaded. This research is by analysing the control measure that enterprise's online security should be adopted. While hoping for personal who is engaged in enterprise's online security planning，can make the foundation and plan in accordance with this result of study.

Keyword：Information Security Management Systems、Flaw Remediation、Standard

誌謝

本論文得以順利完成，首先要感謝羅濟群博士及樊國楨博士的教誨與指導，從論文題目的研訂，研究架構的建立以及在撰寫過程中提供許多經驗的引導，使筆者在個案實作上更增進許多理論的基礎。此外也要感謝郭更生博士、蔡銘箴博士擔任本論文的口試委員，並提供筆者改進的建議與方向，使本論文更趨嚴謹。

有幸能在進入社會工作多年之後，能夠重新回到學校並且參與相關的研究工作，兩年期間雖然背負了工作與課業的雙重壓力，惟想起這段期間所曾參與發表之學術期刊及論文著作，對於自己的付出亦是一種肯定。此外與教授、助教、同學之間無論是課程上的研討或是課餘的參與活動、餐敘...等亦都充滿無盡的回味。

最後，要感謝我摯愛的妻子與家人。若沒有您們的體諒與支持，使我能在繁忙的工作與課業中取得平衡，則不敢奢望能於兩年內順利取得學位。此外，對於修業期間曾經提供協助的長官、同事與好友，藉此致上我最誠摯的謝意。

鄭東昇 謹誌

中華民國九十四年七月

目錄

圖目錄

表目錄

第一章 緒論

1.1 研究背景與動機

1.1.1 資訊安全現況

2004 年殺手病毒「WORM_SASSER.A」利用微軟視窗系統缺點 LSASS，透過 445 連接埠發動攻擊，感染用戶的電腦將會出現倒數關機畫面，Sasser 病毒侵入電腦後，會開啟程式攻擊其他網路上的用戶，造成網路堵塞，電腦運作緩慢，系統不斷倒數計時，並且重新開機，與 2003 年引起軒然大波的疾風病毒如出一轍。根據微軟發布的修補程式，與相對應攻擊病毒的誕生日比較，如表 1.1 所示 2001 年的娜妲病毒相差 336 天、2003 年的 Slammer 病毒相隔 185 天、同為 2003 年的疾風病毒距離 26 天，而 2004 年的殺手病毒與修正程式 MS04-011 公佈的日期只有 18 天就爆發災情，已經創下有史以來最快之紀錄。

從調查報告公佈的數據和狀況可以看出，各種網路安全漏洞的大量存在和不斷發現仍將是網路安全的最大隱患；漏洞公佈到利用相應漏洞的攻擊代碼出現的時間已經縮短到幾天甚至可能是一天的時間，這使得相關修補程式開發、安裝以及採取防範措施的時間壓力大大增加。網路攻擊行為日趨複雜，各種方法相互融合，使網路安全防禦更加困難，防火牆、入侵監測系統等網路安全設備已不足以完全阻擋網路安全攻擊；駭客攻擊行為組織性更強，攻擊目標從單純的追求“榮耀感”向獲取多方面實際利益的方向轉移，木馬、間諜程式、惡意網站、僵屍大軍(BotNet)等的出現和日趨氾濫，則是這類趨勢的實證。手機、掌上型電腦等無線終端設備的處理能力和功能通用性提高，使其日趨接近個人電腦，針對這些無線終端設備的網路攻擊已經開始出現，並將進一步發展。總之，網路安全問題變得更加錯綜複雜，影響將不斷擴大，很難在短期內得到全面解決。

▼表 1.1：電腦應急反應組/協調中心(CERT/CC)公佈重大安全事件分析

1. 資料來源：http://www.cert.org/
2. 重大蠕蟲漏洞攻擊週期：
   2001 年 Nimda 娜妲病毒從發現缺點到發作，相隔 336 天。
   2003 年 Slammer 病毒相隔 185 天。
   2003 年 Blaster 疾風病毒距離 26 天。
   2004 年 Sasser 殺手病毒，距離缺點公佈日期，只有 18 天。
3. 網路攻擊活動趨勢：
   趨勢 1－自動化，攻擊工具速度快。
   趨勢 2－攻擊工具愈來愈成熟。
   趨勢 3－發現漏洞的速度愈來愈快。
   趨勢 4－防火牆可滲透性增加。
   趨勢 5－非對稱的威脅增加。
   趨勢 6－對基礎設施攻擊的威脅增加。

1.1.2 資訊安全的迷思

一般使用者可能對電腦病毒或駭客攻擊具有初淺的瞭解，即使是企業的主管亦可能對一般的數位安全（digital security）未付出太多關注且避免直接參與應付這個問題。一方面是因為數位安全是個極端複雜的問題，要有各種專業化的科技知識才能處理；而另

一方面大部份的安全入侵實際上源自內部疏忽，若真的要預防得靠不斷的嘮叨叮嚀，而這卻是大多數主管不想做的事。此外，數位安全是無形的，如表 1.2 所示只有遇事不出事的時後才知道在這方面是成功的，所以即使員工在這方面做得好，但個人所獲得的獎勵卻極少【1】。

因此，企業的主管通常都是把數位安全的責任丟給技術人員或是外部的安全顧問，這種與安全保持距離的方式極為不智。根據產業的估計，網路攻擊事件每年影響 90%企業，如表 1.3 所示造成的損失達數十億美元，若加上入侵事件則損失可高達上百億美元。防護措施則相當昂貴，企業平均要花資訊科技預算的 5%~10%在安全防護上，甚至更重要的是，資訊安全事件對業務的影響會更為深遠，它使得營運停擺、造成顧客疏遠且有損商譽。

▼表 1.2：企業尋求安全風險與利潤間平衡的計算方式

1. 資料來源：哈佛商業評論
2. 財務數學估算企業尋求安全風險與利潤間平衡的計算方式：
   EV＝C×P
   EV：期望值
   C：安全事件的相關成本
   P：安全事件發生的機率
3. 當安全事件造成損失的機率是 0.01%、0,001%甚至於無法確定時，則花大錢才能避免損失的證明將會變得相當困難。

▼表 1.3：CERT/CC 公佈近年重大網路攻擊事件及所付出的代價

發生年份	病毒名稱	損失金額(以美金計算)
2001	娜妲 (Nimda)	6.35 億美金
2001	紅色警戒 (Code Red)	26.2億美金
2002	求職信 (Klez)	90 億美金
2003	SQL警戒 (SQL Slammer)	10 億美金
2004	疾風病毒 (Mblast)	26 億美金

1.1.3. 資訊科技投資走緩

1968 年英特爾（Intel）發明瞭微處理器，帶動一系列改造商業世界的科技重大突破，例如桌上型電腦、區域網路（LAN）、廣域網路（WAN）和網際網路（Internet）。如今，資訊科技為商業骨幹的說法已是無庸置疑，隨著資訊科技的影響力和普及性不斷擴大，企業開始視之為攸關成敗的重要資源，而且這樣的情形已明顯反映在企業的花費習慣上。依據美國國務部經濟分析局（Bureau of Economic Analysis）所進行的調查，在 1965 年美國企業的資本支出只有不到 5%的比例用於資訊科技。1980 年代初期個人電腦問世之後這個百分比一舉攀升至 15%，到了 1990 年代初期更是超過 30%；及至 1990 年代末期則是逼進 50%。隨著資訊科技的影響力和普及性不斷擴大，但其在策略上的重要性卻逐漸遞減。一項資源之所以具備真正的策略價值即在於具備維持長期競爭優勢之根基的能力，其所憑藉的並非普遍性而是稀有性。唯有擁有或執行競爭對手無法擁有或無能為力的事情，才能取得優勢。

科技可區分為專屬科技（proprietary technology）與基礎建設科技（infrastructural technology），前者可以實際為個別公司所有，只要持續受到保護則專屬科技就可以成為

長期策略優勢的基礎，促使公司獲利高於競爭對手。相形之下基礎建設科技（例如鐵路、電力、網路）在共用時比獨佔使用時更具價值，因為基礎建設科技促成嶄新、更有效率的營運方式並導致廣泛的市場變革。雖然基礎建設科技在初期階段也會以專屬科技的形勢呈現，但是當科技的商業潛能開始廣為人知，勢必會有大量現金擁入而使得科技取得的優勢機會只開啟非常短暫的時間，即使企業可以在基礎建設科技擴建完成後得到成本優勢的好處，但往往也非常難以長期延續。

資訊科技是非常容易複製的，而且大部份商業活動和流程都已被建入軟體，因此這些活動和流程也變得可以複製，當網際網路到來時則為應用軟體提供了一個完美的傳送通路，因而加速了資訊科技的商品化。從微軟到 IBM 等大多數商業科技提供商，紛紛試圖把自己定位為資訊科技公用事業（utility），此舉導致資訊科技的同質性更高。如表 1.4 所示由於科技發展的步調快速，因此延遲資訊科技投資或能成為另一個削減成本的有效方法並避免資訊科技迅速淘汰的高額成本【2】。Alinean 顧問公司在 2002 年比較了 7500 家美國大型企業的資訊科技支出和財務表現，結果發現績效最優異的企業往往是荷包掐得最緊的公司；研究機構 Forrester Research 近來進行的一項研究也驗證了相同的假設。隨著取得資訊科技優勢的機會愈來愈小，花費過多的懲罰將只會有增無減。

▼表 1.4：資訊科技影響力與投資指導方針

1. 資料來源：哈佛商業評論
2. 資訊科技投資已趨緩慢之跡象：
   - 網際網路的能力已趕上了需求。
   - 資訊科技的影響力逐漸超過它所能滿足的大部份商業需求。
   - 基本資訊科技的價格已經降低到幾乎人人負擔得起的程度。
   - 資訊科技供應商急於把自己定位為商品供應商，甚至是公用事業。
3. 企業投資資訊科技與管理系統之指導方針：
   - 減少支出。
   - 追隨即可，不要主導。
   - 鎖定弱點，而非機會。

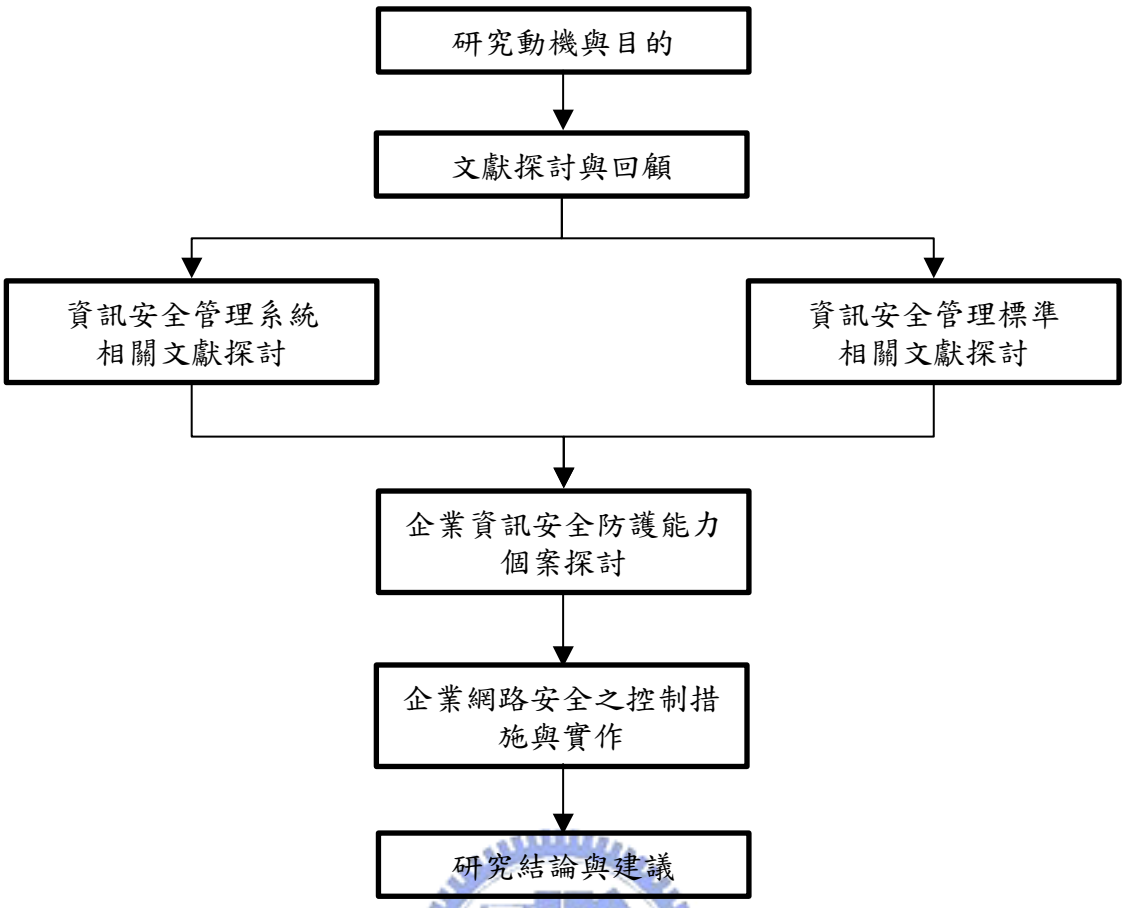
1.2 研究目的及範圍

在第一節的研究中，可以發現網路安全問題會隨著時間變得更加錯綜複雜，影響也將會不斷擴大，但是企業對於資訊科技的投資卻逐漸走緩而形成強大的對比，此舉似乎會加速網路安全事件的發生。事實上對於資訊科技的假設應該為當該項資源已變為競爭不可或缺的要素，但對策略卻不具影響性時，則它所造成的風險就比所提供的優勢更為重要；基礎建設科技雖不再左右個別公司策略，但影響的範圍卻會提昇至國家、國際總體經濟層次。當資訊科技為更多人所取得，基礎建設科技的擴建也會讓使用者採納統一的技術標準，隨著最佳實務漸漸廣為瞭解和模仿，即便是科技的使用也開始標準化。所謂標準就是基於公平、公正、便利等觀點做好統一規範與單純化時之必要條件；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。

今日有關資訊安全宜遵循的策略，都是在不完整之資訊內容下做決定的，標準可以減輕因不完整資訊引發之困難，因為標準可以減少選擇的範圍而簡化資訊之供給與需求決策制定的過程。筆者自 1997 起即進入民間大型企業任職，當中經歷 1998~2000 年網際網路的高成長期與 2002 網路泡沫在最大的時候破滅，對於企業資訊安全所遭遇之困境自是點滴在心頭，所以在本研究中，希望針對資訊安全管理標準應用於企業網路安全宜採用之控制措施進行分析並提出實作成果。對於企業資訊人員而言，在規劃企業網路安全時，可依本研究結果做基礎進行規劃作業，則可有效減少資訊人員在規劃上進行評估及分析的時程。

1.3 論文架構

本論文共分為五章，除了本章緒論外；在第二章文獻探討的部分，我們將探討資訊安全管理系統並列舉資訊安全管理標準與適用範圍；第三章探討企業資訊安全防護能力；第四章則是企業安全性修補程式架構之設計與實作；第五章，也是本論文的最後一章則是本研究的研究結論與建議。如圖 1.1 所示為本論文之研究流程圖。


研究動機與目的
文獻探討與回顧
資訊安全管理系統
相關文獻探討
資訊安全管理標準
相關文獻探討
企業資訊安全防護能力
個案探討
企業網路安全之控制措
施與實作
研究結論與建議

▲圖 1.1：研究流程圖

第二章 文獻探討

2.1. 資訊安全管理系統綜述

由於資訊科技的快速進步，計算機的使用從集中式大型主機、個人電腦、區域網路、逐步演進發展到目前的網際網路。資訊系統的使用者也從原本只侷限於組織內部的資訊技術人員，漸漸增加為組織內部的非技術人員與外部的使用者。隨著資訊新科技的不斷推陳出新，使用者的範圍不斷的擴大並且對資訊系統依賴程度與日俱增，這使得資訊安全面臨更大的挑戰。本節由管理理論的探討嘗試為建構資訊安全管理系統可為可信賴資訊作業環境之指引尋找佐證。

2.1.1. 資訊安全管理理論

對於研究者而言，瞭解資訊安全管理理論基礎可以將前人研究所累積的知識進一步整合與連結，以發展更成熟的理論。由於資訊科技的快速進步，使得組織對資訊科技得依賴日深，資訊安全已不只是一項防禦性策略，更成為組織的競爭策略，因此資訊安全管理理論將關係到資訊安全的研究，更影響到資訊安全策略之擬定。如表 2.1 所示利用分析文獻方式【3】可將資訊安全管理理論歸納為安全政策理論、風險管理理論、控制與稽核理論、管理系統理論與權變理論五種。安全政策理論、風險管理理論、控制與稽核理論均由資訊安全的某一環節切入，雖切入點不同但後續的資訊安全管理內涵則是相同的。上述各理論均為資訊安全管理的一個環節或部份所組成，這當中又以管理系統理論較為完整。

▼表 2.1：資訊安全管理理論彙總

理論	主要管理活動	管理程式	特性
安全政策理論	● 安全政策制定 ● 安全政策實施 ● 安全政策維護	● 循序流程 ● 循環週期	● 以資訊安全政策為主要內涵，忽視風險管理、內部控制與資訊稽核等安全機制 ● 重視循序與結構化，對於環境的應變能力較低
風險管理理論	● 風險評鑑 □ 風險分析 □ 風險評估 ● 風險處理 □ 建立控制制度 □ 實施控制制度 ● 檢討修正	● 循序流程 ● 循環週期	● 強調資訊安全環境的瞭解與與應變，使控制制度可符合組織的需求 ● 忽視安全政策與資訊稽核等安全機制 ● 重視循序與結構化
控制與稽核理論	● 制定控制制度 ● 實施控制制度 ● 資訊稽核	● 循序流程 ● 循環週期	● 以內部控制及資訊稽核為主要內涵，忽視安全政策與風險評估等安全機制 ● 重視內部控制之澈底執行，對於環境應變與需求規劃較為不足
管理系統理論	● 制定安全政策 ● 定義風險範圍	● 循序流程	● 資訊安全風險管理機制較其他理論完整

	● 風險管理 □ 風險評估 □ 風險控制 ● 實施		● 忽視資訊稽核 ● 欠缺循環週期與回饋功能
權變理論	● 政策導向策略 ● 風險管理導向策略 ● 控制與稽核導向策略 ● 管理系統導向策略	● 權變流程	● 可充分反應組織內外環境，選擇適當的安全策略 ● 欠缺整合性與結構化
資料來源：資管評論			

2.1.2. 資訊安全管理系統

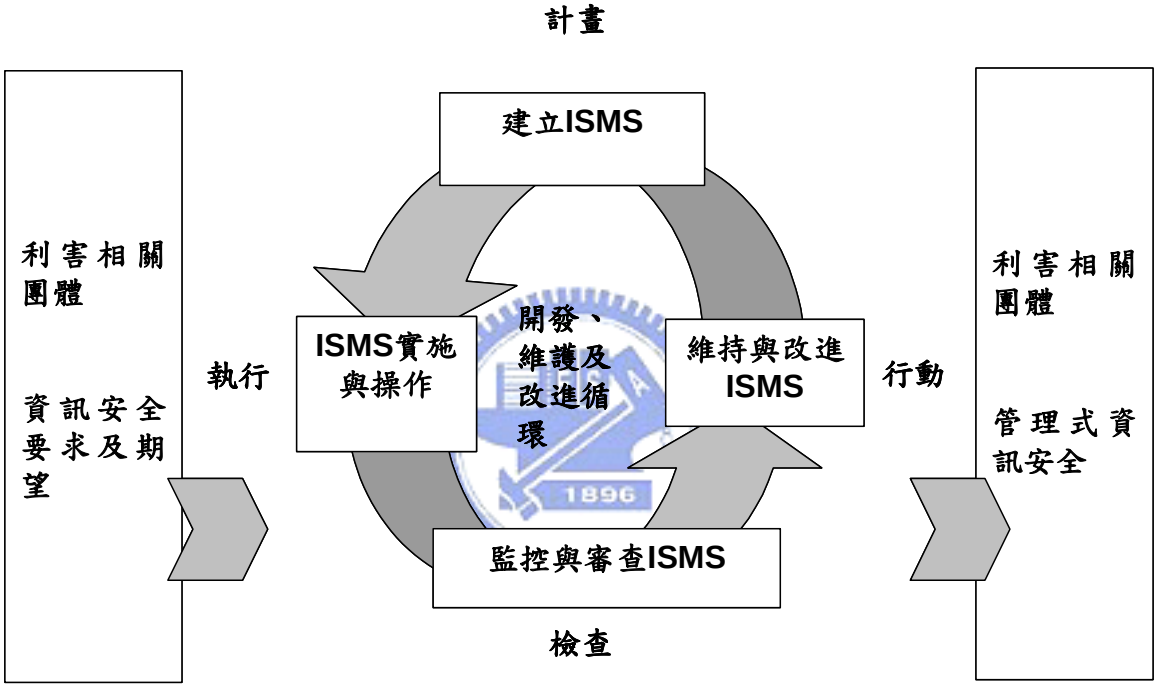
資訊安全管理系統（Information Security Management System，簡稱 ISMS）係指組織應建立及維護一套系統以強調需要被保護的資訊系統資產，並且採用風險管理方法、控制目標、控制方法、以及所需要的安全保證程式。ISMS 分為六大步驟：（1）定義政策；（2）定義範圍；（3）進行風險評估；（4）風險管理；（5）選擇要實行的控制目標及控制方法；（6）準備適用性聲明等，形成一個程式化的安全管理系統。一般熟悉之「計畫-執行-檢查-行動」（Plan-Do-Check-Act，簡稱 PDCA）模式【4】，可應用於資訊安全管理過程，如圖 2.1 所示為資訊安全管理系統如何採用資訊安全要求之輸入及利害相關團體之期望作為輸入端，經由如表 2.2 的措施產生符合所需要及期待的資訊安全輸出結果；圖 2.2 是建置資訊安全管理系統的過程。PDCA 過程模式可描述如下：

1. 計畫（建立 ISMS）：建立安全政策、目標、標的、過程及相關程序以管理風險及改進資訊安全，使結果與組織整體政策與目標相一致。
2. 執行（實施與操作 ISMS）：安全政策、控制措施、過程與流程之實施與操作。
3. 檢查（監控與審查 ISMS）：依據安全政策、目標與實際經驗，以評鑑及測量(適當時)過程績效，並將結果回報給管理階層加以審查。
4. 行動（維持與改進 ISMS）：依據管理階層審查結果採取矯正與預防措施，以達成持續改進資訊安全管理系統。

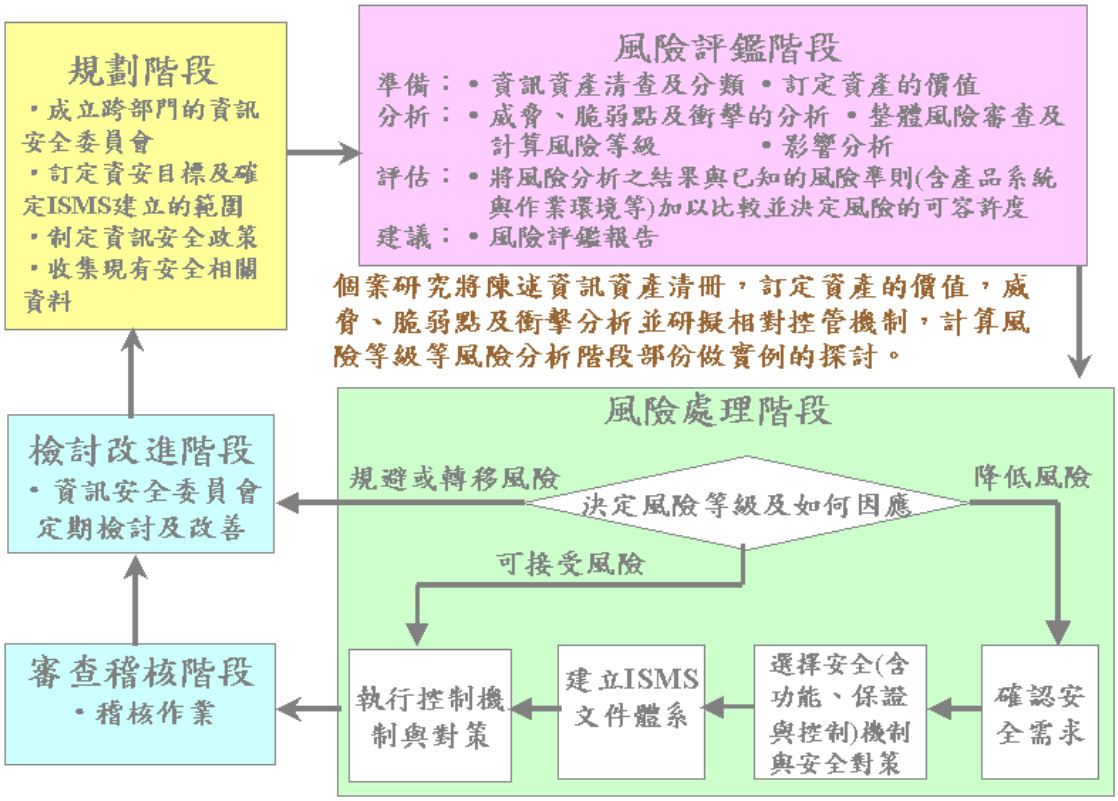
▼表 2.2：資訊安全管理系統過程要項

過程	實施要項
計畫	● 定義資訊安全管理系統的範圍與政策 ● 定義風險評鑑的系統化方法 ● 鑑別各項風險 ● 採用該系統化方法以評鑑風險 ● 鑑別並評鑑處理風險的選項作法 ● 選擇控制目標及控制措施以處理風險
執行	● 實施既定的管理規畫 ● 實施所選的控制措施 ● 作業管理 ● 管理資源 ● 實施作業程序及其他管制過程
檢查	● 執行作業程序及其他控制措施 ● 定期審查資訊安全管理系統的有效性 ● 審查殘餘風險（residual risk）與可接受風險（acceptable risk）之層級

	● 執行各項管理作業程序 ● 定期執行正式的資訊安全管理系統審查作業 ● 記錄與回報所有的措施與事件
行動	● 測量資訊安全管理系統的績效 ● 鑑別資訊安全管理系統之可改善處並有效實施 ● 採取適當矯正及預防措施 ● 與所有相關機構就結果及各項措施進行溝通並徵詢意見 ● 必要時修改資訊安全管理系統 ● 確認各修改措施已達到預期目標



▲圖 2.1：PDCA 過程模式



▲圖 2.2：建置資訊安全管理系統的過程

2.2 資訊安全管理標準與適用範圍

目前國內外系統開發，均已朝向開放系統之方向進行，且由於寬頻網路、無線網路及網際網路之盛行帶來數位社會的商機與風險，而資訊安全已成為數位社會能否進一步發展的關鍵。所謂標準就是基於公平、公正、便利等觀點做好統一規格與單純化時之必要條件；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。國際上標準化的主要目的在於創造物品交換、技術轉移的貿易環境；例如產品品質及信賴性與價格相符，保障使用者的安全並促進資源的再利用，物品、技術與服務的互運性以及彼此之間的接續性，單純化以減少塑模數。期能擴大生產規模以降低成本，並強化維修保養的便利性與配銷的效率性。資訊安全標準的制定早已在世界各國及若干國際組織行之有年，而我國中央標準檢驗局亦持續進行資訊安全相關國家標準之修訂工作，並且將資訊安全標準之修訂工作列為標準檢驗局重點工作

2.2.1 ISO 國際標準

國際標準組織(International Organization for Standardization，簡稱 ISO)為一世界性組織，其成員是由來自世界約 130 個國家級標準組織代表所組成（均為聯合國成員國），其下設有 2850 個技術委員會（Technical Committee，簡稱 TC）、分組委員會（Subcommittee，簡稱 SC）及工作小組（Working Group，簡稱 WG）負責各項國際標準之制定工作，如表 2.3 所示為 ISO 組織中與資料安全有關之 TC【5】。

1977 年 1 月 5 日，美國頒布聯邦資訊處理標準(Federal Information Processing Standards，簡稱 FIPS)出版品(Publication)第 46 號之資料加密標準(Data Encryption

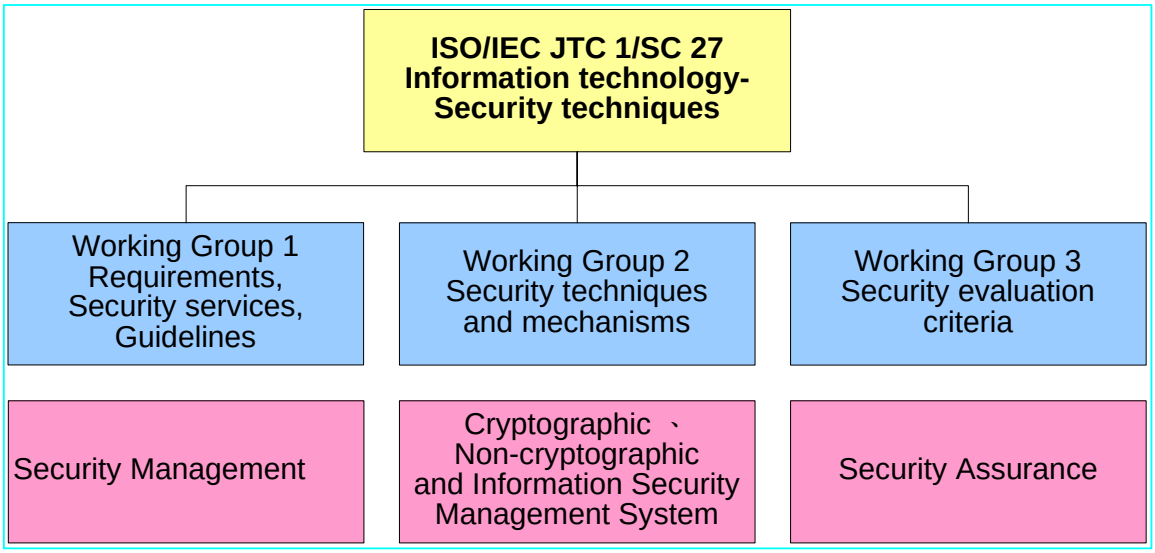
Standard，簡稱 DES)起，雖著金融交易的需求，至 1987 年 6 月 1 日 ISO 第 68 技術委員會(Technical Committee，簡稱 TC68)根基於 DES，頒布了 ISO 8731，成為第 1 分 ISO 之資訊安全的國際系列標準【6~7】。

為制定密碼技術之標準，負責訂頒資訊處理(Information processing)標準之 ISO TC 97 於 1981 年 1 月召開第 1 次之第 1 工作會(Working Part 1，簡稱 WP1)，自 1983 年起，TC 97 WP 1 將此項工作轉交由德國標準機構支援的「資料密碼學技術(Data cryptographic techniques)」的 20 分組(Subcommittee，簡稱 SC20)，SC20 下轄秘密金鑰演算法與應用(Secret key algorithms and applications)之第 1 工作小組(Working Group，簡稱 WG 1)、公開金鑰密碼系統與模的使用(Public key crypto-systems an modes of use)之 WG 2 與在通訊架構中使用加密技術(Use of decipherment techniques in communication architectures)的 WG 3，正式展開資訊安全國際標準的制定工作。

1989 年，由 ISO 與國際電工委員會(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根基於密碼學應用之特定範圍標準的制定工作，成立如圖 2.3 所示之 ISO/IEC 第 1 聯合技術委員會(Joint Technical Committee，簡稱 JTC 1)的資訊技術(Information Technology，簡稱 IT)安全技術(Security Techniques，簡稱 ST)之第 27 分組委員會(Sub-Committee，簡稱 SC27)。ISO/IEC JTC1/SC 27 下轄 3 個工作組(Working Group，簡稱 WG)分別就資訊安全之「需求、安全服務與指導綱要」、「安全技術與機制」及「安全評估準則」遵循如表 2.4 之流程制定國際標準，如表 2.5 是 ISO/IEC JTC1/SC27 WG1 已頒布和正制定中之國際標準。：

▼表 2.3：ISO 組織中與資料安全有關之 TC

1. TC 68 Banking、securities and other financial services 技術委員會，其下設有：
   - 1.1. SC 2 Security management and general banking operation 分組委員會
   - 1.2. SC 4 Securities and related financial instruments 分組委員會
   - 1.3. SC 6 Retail financial services 分組委員會
   - 1.4. WG 3 Bank-telecommunication messages 分組委員會
   - 1.5. WG 4 Security coordination 分組委員會
2. TC 154 Processes，data elements and documents in commerce，industry and administration 分組委員會
3. JTC 1 information technology 分組委員會，設有：
   - 3.1. SC 17 Identification cards and related devices 分組委員會，其下設有：
     - □ WG 1 Physical characteristics and test methods for ID-cards
     - □ WG 3 Identification cards－Machine readable travel documents
     - □ WG 4 Integrated circuit card with contacts
     - □ WG 5 Registration Management Group（RMG）
     - □ WG 7 Financial transaction cards
     - □ WG 8 Integrated circuit cards without contacts
     - □ WG 9 Optical memory cards and devices
   - 3.2. SC 27 IT Security techniques 分組委員會，其下設有：
     - □ WG 1 Requirements、security services and guidelines
     - □ WG 2 Security techniques and mechanisms
     - □ WG 3 Security evaluation criteria



▲圖 2.3：ISO/IEC JTC1/SC 27 組織架構

▼表 2.4：國際標準制定流程

1. 研究階段(Study Period)：就一標準之需求非正式的交由委員會加以研究，將其結果就此需求刪除或提交新工作項目建議書(New work item Proposal，簡稱 NP)進行票決。
2. 新工作項目建議書(NP)階段：完成提交 JTC1 秘書處之建議書。
3. 工作草案(Working Draft，簡稱 WD)階段：分項委員會(SC)或工作小組(WG)內部文件集。
4. 委員會草案(Committee Draft，簡稱 CD)或技術報告草案建議(Proposed Draft Technical Report，簡稱 PDTR)階段：當 WD 考量其穩健性已足夠充分後，由分項委員會向 ISO/IEC 之資訊技術工作組(Information Technology Task Force，簡稱 ITTF)登錄成為 CD，由 SC 國家會員代表在 3 個月內投票並提出評論，相關文件由 JTC1 派送。
5. 國際標準草案(Draft International Standard，簡稱 DIS)或技術報告草案(Draft Technical Report，簡稱 DTR)階段：當 CD 或 PDTR 已充分討論，無技術面被期待之修改，SC 向 ITTF 提出票決成為 DIS 或 DTR，由 JTC1 國家會員代表 4 個月內投票並提出評論。
6. 國際標準(International Standard，簡稱 IS)或技術報告(Technical Report，簡稱 TR)階段：遵循 IS 或 TR 出版之程式，就各個國家會員代表發現技術錯誤的瑕疵報告(Defect Report)，SC 決定此 IS 或 DTR 修正、取銷或頒布 IS 或 TR。
7. 審核(Review)階段：每分 IS 或 TR 在 5 年內應重新審核，由 SC 負責提出 IS 或 TR 宜修正、作廢或維持之確認報告後，由 JTC1 決定。

▼表 2.5：ISO/IEC JTC1/SC27 WG1 已完成與進行中計畫

1. SC27 目前有 31 個有投票權的成員，11 個無投票權的觀察員。
2. SC 27 WG1 已完成與進行中之計畫：
   2.1. ISO/IEC 9979 (1999-04-01)：Information technology - Security techniques - Procedures for the registration of cryptographic algorithms。
   2.2. ISO/IEC 11770-1 (1996-12-15)：Information technology - Security techniques

- Key management - Part 1: Framework。

2.3. ISO/IEC 13335-1 (2004-11-15)：Information technology - Security techniques - Management of information and communications technology security (MICTS) - Part 1: Concepts and models for information and communications technology security management。

2.4. ISO/IEC 4th WD 13335-2 (2004-10-23)：Information technology - Security techniques - Management of information and communications technology security (MICTS) - Part 2: Techniques for information and communications technology security risk management。

2.5. ISO/IEC TR 13335-3 (1998-06-15)：Information technology - Security techniques - Guidelines for the management of IT security (GMITS) - Part 3: Techniques for the management of IT security。

2.6. ISO/IEC TR 13335-4 (2000-03-01)：Information technology - Security techniques - Guidelines for the management of IT security (GMITS) - Part 4: Selection of safeguards。

2.7. ISO/IEC TR 13335-5 (2001-11-01)：Information technology - Security techniques - Guidelines for the management of IT security (GMITS) - Part 5: Management guidance on network security。

2.8. ISO/IEC TR 14516 (2002-06-15)：Information technology - Security techniques - Guidelines on the use and management of Trusted Third Party services。

2.9. ISO/IEC 15816 (2002-02-01)：Information technology - Security techniques - Security information objects for access control。

2.10. ISO/IEC 15945 (2002-02-01)：Information technology - Security techniques - Specification of TTP services to support the application of digital signatures。

2.11. ISO/IEC TR 15947 (2002-10-15)：Information technology - Security techniques - IT intrusion detection framework。

2.12. ISO/IEC 2nd FDIS 17799 (2005-02-11)：Information technology - Security techniques - Code of practice for information security management。

2.13. ISO/IEC 1st CD 18028-1 (2004-12-01)：Information technology - Security techniques - IT network security - Part 1: Network security management。

2.14. ISO/IEC 2nd FCD 18028-2 (2004)：Information technology - Security techniques - IT network security - Part 2: Network security architecture。

2.15. ISO/IEC 2nd FCD 18028-3 (2004)：Information technology - Security techniques - IT network security - Part 3: Securing communications between networks using security gateways。

2.16. ISO/IEC 18028-4 (2005)：Information technology - Security techniques - IT network security - Part 4: Remote access。

2.17. ISO/IEC 1st CD 18028-5 (2004-12-03)：Information technology - Security techniques - IT network security - Part 5: Securing communications across networks using Virtual Private Networks。

2.18. ISO/IEC 2nd CD 18043 (2004-12-10)：Information technology - Security techniques - Guidelines for the implementation, operation and management of Intrusion Detection Systems (IDS)。

2.19. ISO/IEC TR 18044 (2004-10-15)：Information technology - Security techniques - Information security incident management。

2.20.	ISO/IEC 1st WD 24742 (2005-01-10)：Information technology - Security techniques - Information security management metrics and measurements。
2.21.	ISO/IEC FCD 24743 (2004-12-04)：Information technology - Security techniques - Information security management systems requirements specification。I

2.2.2 CNS 國家標準

我國有關於資訊安全的標準大部份皆依 ISO 相關標準為制定之依據。1995 年行政院成立國家資訊通信基本建設(National Information Infrastructure，簡稱 NII)專案，「資訊安全」列入主要規劃項目之一，其目的在確保 NII 中各項資訊應用資料的安全使用。自 1996 年起，以 ISO/IEC JTC1/SC 27 WG2 的「實體驗證」與 ISO TC 68 及 ISO/IEC JTC1/SC 27 的「識別卡以及相關裝置(Identification card and related devices)」分組委員會制定之「金融交易卡」等國際標準等以委辦案方式轉訂成我國國家標準(Chinese National Standard，簡稱 CNS)草案，再由 CNS「資料安全技術」的 11 分組(SC 11)負責審議，公佈 CNS 標準【8】。2001 年起，前述委辦之方向，配合「建立我國通資訊基礎安全機制計畫」之工作，從密碼應用的特定範圍標準，轉換成 ISO/IEC JTC1/SC 27 WG1 與 WG3 之「資訊安全管理」及「資訊安全評估」相關國際標準和 ISO/IEC JTC1/SC 27 的「軟體工程過程評鑑」與「軟體產品評估」等相關國際標準等，轉訂成 CNS 草案的現行方向。

2001 年 2 月 5 日，行政院函送「建立我國通資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，正式開啟了我國資訊安全發展的新頁。近年來世界各國（如美、英等國）皆全力投入推動資訊安全基礎建設，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，根基於此，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」；但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，NII 專案推動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，以圖 2.4 與 2.5 之架構完成「建立我國通資訊基礎建設安全機制計畫」。

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。國家通資安全會報成立時，是由行政院院長與副院長分別擔任正、副召集人，並由行政院資訊通信發展推動小組(National Information and Communication Initiative Committee，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（備考：此項職掌已於 2004 年 10 月刪除）。
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式。

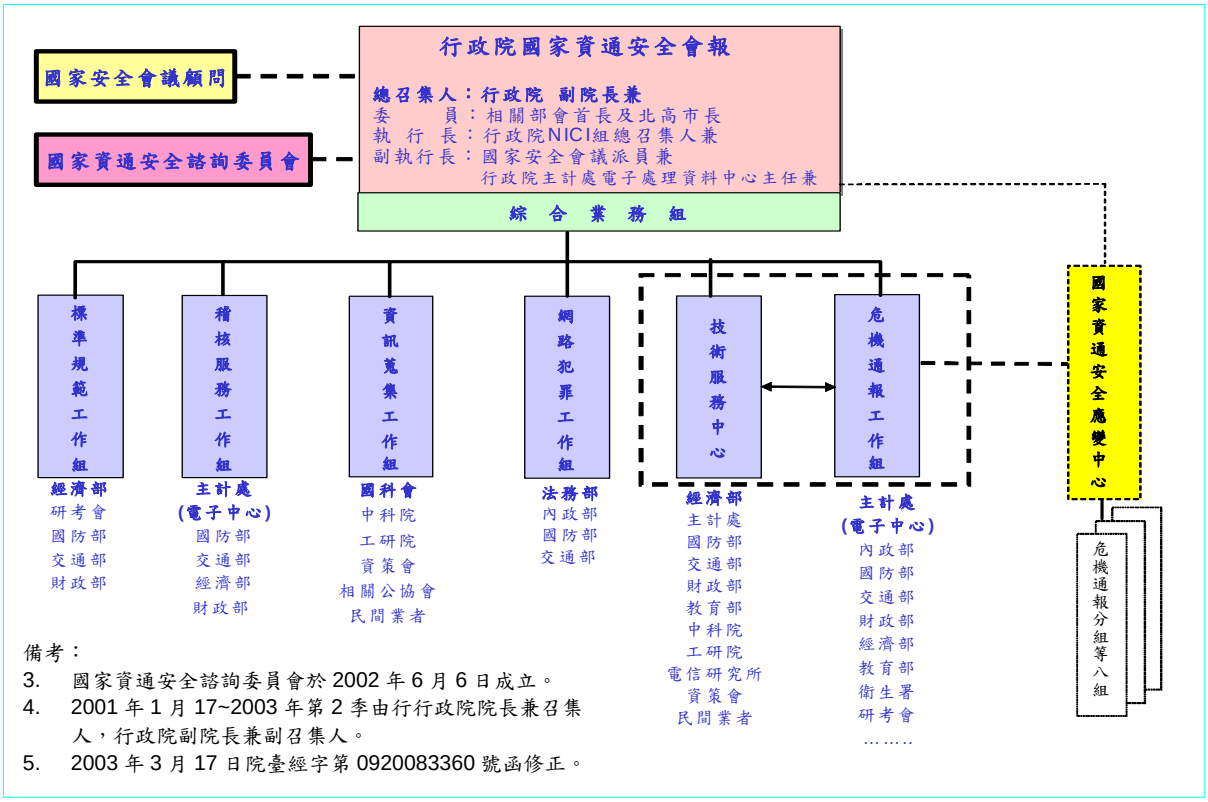
為達成前述計畫之工作計畫目標，經濟部標準檢驗局已根基於 1994 年公佈之世界貿易組織烏拉圭回合多邊貿易談判協定(The Results of The URUGUAY Round of Multilateral Trade Negotiations)技術性貿易障礙協定(Agreement on Technical Barriers to Trade，簡稱 TBT)附件 1~3(Annex 1~3)之規範，分以下述 4 項為工作方向推動相關工作中：

1. 資訊技術安全評估共同準則(ISO/IEC 15408)系列、資訊安全管理(ISO/IEC 17799)、軟體處理評估(ISO/IEC TR 15504)系列等標準之制定。
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

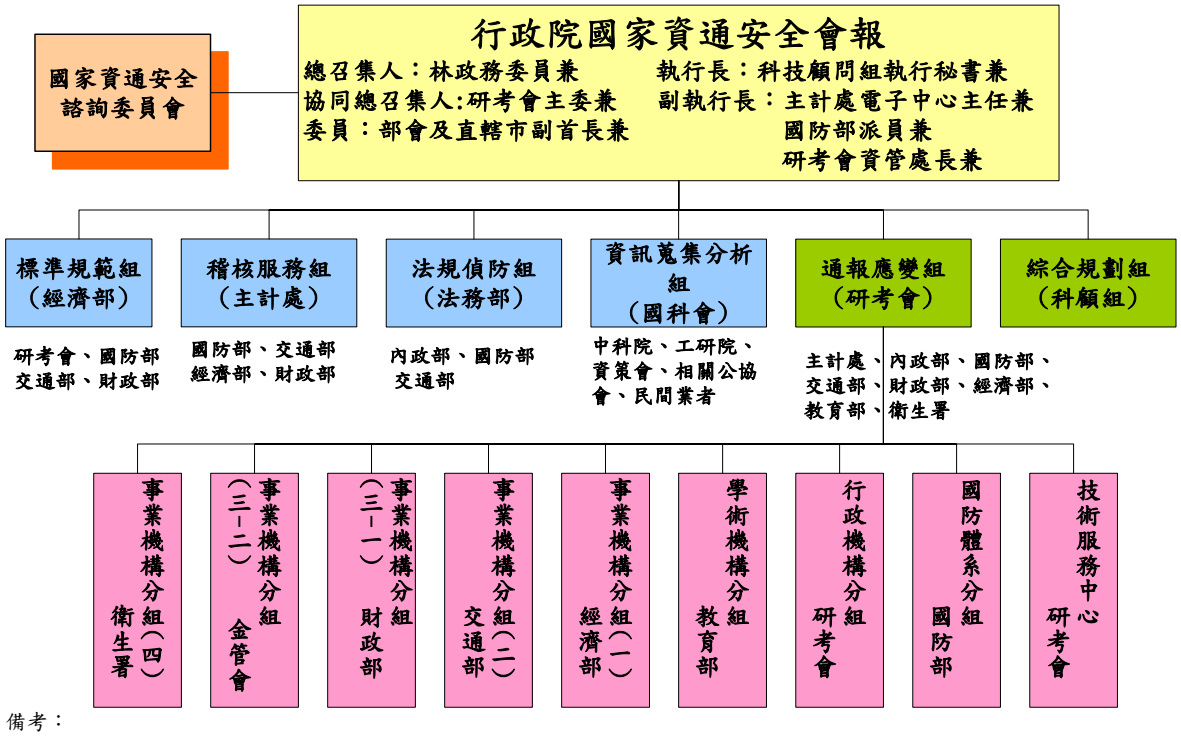
發行及管理)之保護剖繪(Protection Profile)與其之共同性檢測技術之建置。

3. 將 BS 7799-2(Information Security Management Systems Part 2：Specification for Information Security Management Systems)轉定為國家標準，建置我國通資訊安全之管理系統驗證作業體系。
4. 符合 ISO/IEC Guide 62、ISO/IEC Guide 65 與 ISO/IEC 17025 之要求，分別建置通資訊安全管理系統認證、產品驗證認證以及實驗室認證之認證程式。

2002 年 12 月 5 日經濟部標準檢驗局分別公佈 CNS 17799 與 CNS 17800，並於 2003 年 5 月 12 日根基於 EA7/03：2000 公佈「資訊安全管理系統驗證／登錄機構之認證指引」，完備資訊安全管理系統驗證作業相關的國家標準。在共同準則方面，經濟部標準檢驗局於 2004 年 1 月 9 日及 4 月 12 日，依序公佈「資訊技術－安全技術－資訊技術安全評估準則」之 CNS 15408 系列標準之第 1 部、第 2 部及第 3 部。前述計畫執行 3 年多來於推動政府機關對於資訊安全之重視，與帶動民間對於資訊安全防護工作的投入不遺餘力，並已具初步成效，唯因資訊安全工作係一需持續推動之重要工作，「行政院國家資通安全會報」於 2004 年 5 月 7 日已正式公佈我國 2005 至 2008 年的第二期「建立我國通資訊基礎建設安全機制計畫」，做為我國擬定資訊安全政策及如表 2.6 所示工作要項以及解決各層級資訊安全問題關連性的依據【9~15】。



▲圖 2.4：我國資通安全之組織架構(90 年 1 月 17 日~93 年 10 月)



備考：

1. 何全德(2004) 淺論國家資通安全工作推動方向，第六屆2004 年「網際空間：資訊、法律與社會」學術研究暨實務研討會論文集，頁 15~23，2004 年 10 月 15 日。
2. 2004 年 10 月 21 日院臺科字第 0930090197 號函。

▲圖 2.5：我國資通安全之組織架構(93 年 10 月~訖今)

▼表 2.6：工作要項與解決各層級資通安全問題關聯性

標示層級 ＼ 工作要項		建立國家資通安全事件通報及危機應變體系	建全國家資通安全防護能力	強化國家資通安全認知與訓練推廣作業	確保國家資通安全及促進國際合作
一級層	家庭使用者／小型企業			○	
二級層	大型企業	○	○	○	
三級層	重要產業／基礎建設	○	○	○	○
四級層	國家性議題	○	○	○	○
五級層	全球性議題				○
	行動方案	**1~10**	**11~38**	**39~55**	**56~59**

資料來源：行政院國家資通安全會報（2004）建立我國通資訊基礎建設安全機制計畫（九十四年至九十七年），頁 18 與頁 51~79。

2.3 資訊安全管理作業要點－CNS 17799（ISO/IEC 17799）

國際間建立數位社會資訊安全管理認證的工作，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）專門認證機構：國際資訊系統安全授證公會（International Information Sys tem Security Certification Consortium，簡稱$(ISC)^2$）在英國的索爾斯伯利（Selisbury）正式成立。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，表 2.7 是其發展簡史，表 2.8 是其增修後正式提交ISO 審議之內容概述。

2005 年 6 月 15 日公布之 ISO/IEC 17799:2005(E)對資訊安全之定義已修正如表 2.9 所示，除於層次之擴充外並擴及歸屬於相依性(Dependability)中的可靠性(Reliability)，其對資訊安全風險評鑑等作業過程產生深遠之影響。在每一個控制措施的陳述結構更分成表 2.10 之「控制」、「實作指引」與「其他資訊」三部分。原 2000 年 12 月 11 日公布之 ISO/IEC 17799:2000(E)的組織安全、人力資源與通信及作業管理三類資訊安全管理控制措施均有相當幅度之修正，在資產管理、存取控制、系統開發及維護等類的控制措施亦有增刪，同時增加「資訊安全事故管理(Information Security Incident Management)」類之控制措施，成為 11 類 133 項控制措施的資訊安全管理作業標準【16】。我國有關於資訊安全的標準大部份皆依 ISO 相關標準為制定之依據，2005 年 6 月經濟部標準檢驗局根基於 ISO/IEC 17799:2005(E)年版起草修訂中華民國國家標準 CNS 17799。

▼表 2.7：資訊安全管理認證簡史

1. 1990 年：世界經濟合作開發組織（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：英國訂定國家標準 BS7799 第一部分：「資訊安全管理實務準則」，並提交國際標準組織（International Organization for Standardization，簡稱 ISO）成為 ISO DIS14980。
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：
   - □ OECD 於 1997 年 3 月 27 日公佈密碼模組指導原則。
   - □ 英國正式開始推動資訊安全管理認證先導計畫。
7. 1998 年：
   - □ 英國公佈 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。
   - □ 歐盟於 1995 年 10 月公佈之「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：
    - □ 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。ISO/IEC JTC1/SC27 WG1 於同年著手修訂 ISO/IEC 17799:2000(E)。

- □ 英國於 2001 年 11 月公佈 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 月公佈增修後之 BS7799-2 第二部分。

11. 2002 年：
    - □ 2002 年 7 月 25 日，OECD 公佈「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。
    - □ 2002 年 9 月 5 日，BS7799-2：2002 年版遵照 OECD 同年 7 月 25 日頒布之「資訊系統與網路指導綱要－ 朝向安全的文化」中的原則修正後正式發行。
    - □ 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 年版公佈中華民國國家標準 CNS 17799 及 CNS 17800。
12. 2003 年：資訊安全管理認證正式成為 ISO17799 國際標準。
13. 2005 年：
    - □ 2005 年 6 月 15 日，OECD 公布 ISO/IEC 17799:2005(E)，我國經濟部標準檢驗局亦根基於 ISO/IEC 17799:2005(E)年版起草修訂中華民國國家標準 CNS 17799。

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、南非等國家同意使用 BS7799。

▼表 2.8：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		

▼表 2.9：ISO/IEC 17799:2005(E)之資訊安全用語釋義

1. 資訊安全(Information security)：保護資訊之機密性、完整性與可用性；得增加諸如鑑別性、可歸責性、不可否認性與可靠性。
2. 機密性(Confidentiality)：資料不得被未經授權之個人、實體或程序所取得或揭露的特性。
3. 完整性(Integrity)：對資產之精確與完整安全保證的特性。
   - 3.1 可歸責性(Accountability)：
     確保實體之行為可唯一追溯到該實體的特性。
   - 3.2 鑑別性(Authenticity)：
     確保一主體或資源之識別就是其所聲明者的特性。
     鑑別適用於如使用者、程序、系統與資訊等實體。
   - 3.3 不可否認性(Non-repudiation)：
     對一已發生之行動或事件的證明，使該行動或事件往後不能被否認的能力。
4. 可用性(Availability)：已授權實體在需要時可存取與使用之特性。
5. 可靠性(Reliability)：使終如一預期之行為與結果的特性。
6. 資料來源：
   - 6.1 ISO, (2005), Information technology – Security techniques - Code of practice for information security management, ISO/IEC FDIS 17799:2005-02-11, 2.6 節, 頁 1, ISO。
   - 6.2 ISO, (2004), Information technology - Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management, ISO/IEC 13335-1:2004, ISO。
   - 6.3 Avizienis, A. et al., (2004), Basic Concepts and Taxonomy of Dependable and Secure Computing, IEEE Transactions on Dependable and Secure Computing, Vol.1, No.1, pp.11~33, IEEE.

▼表 2.10：ISO/IEC 17799:2005(E)主要安全分類之脈絡

1. 每個主要安全類別包括：
   - 1.1 一個陳述何種目標要被達成的控制措施目標，
   - 1.2 一個或多個可用以達成該控制目標的控制措施。
2. 控制措施結構如下：
   - 2.1 控制(Control)：定義明確的控制陳述以符合該控制目標。
   - 2.2 實作指引(Implementation guidance)：提供更多詳細的資訊以支援該控制的實作，並符合該控制目標。有些指引可能不適用於所有的案例，因此使用其他方法的實作可能更合適。
   - 2.3 其他資訊(Other information)：提供可能須被考量的進一步資訊，例如：法律上的考量及其他標準的參考。

第三章 企業資訊安全防護能力分析與研究

3.1.背景說明與文件來源

本研究探討實例為總部設於台灣之大型跨國企業，該企業除台灣之外於美國、歐洲、日本、 中國均設有分工司，員工總數合計約 3 萬人。該企業自成立至今由於專注於提供最先進的製造技術及最完備的智財、設計工具、及設計流程，目前該企業已是該領域規模最大之專業製造公司。

本研究以該大型跨國企業例，收集資訊安全相關文件進行整理、分析與歸納。另一方面以我國經濟部標準檢驗局起草修訂之新版國家標準 CNS 17799（ISO/IEC 17799:2005(E)）第五至第十五節【16~17,22】所列出之控制項目為基礎進行檢測比對。

3.2.建立檢測評核要項表

CNS 17799（ISO/IEC 17799:2005(E)）包括十一大管理要項，三十九個執行目標與一百三十三種控制方法。如表 3.1~表 3.11 所示每一個要項「控制項目」的編號方式是依照 CNS 17799（ISO/IEC 17799:2005(E)）之章節編號；「控制措施」會先列出控制措施的標題，然後是評核方式的描述；「評核」的項目分為二級，評核原則如下：

符　合－文件內容有提到這項控制措施

未符合－文件內容沒有提到這項控制措施

▼表 3.1：安全政策 檢測評核要項表

項次	控制項目	控制措施	評核	
一	5.1	資訊安全政策	符合	未符合
	5.1.1	資訊安全政策文件：		
		資訊安全政策文件應由管理階層核准，並傳達給所有受雇人員與相關外部人員。	□	□
	5.1.2	審查與評估：		
		應定期或有重大變更時審查資訊安全政策，以確保其持續的適當性、充分性、及有效性。	□	□

▼表3.2：組織資訊安全 檢測評核要項表

項次	控制項目	控制措施	評核	
二	6.1	內部組織	符合	未符合
	6.1.1	管理階層對資訊安全的承諾：		
		管理階層在組織內應經由清楚的指示、顯示承諾、明顯的指派、及承認資訊安全責任，主動地支持安全有關計畫。	□	□
	6.1.2	資訊安全協調工作：		
		資訊安全活動應由組織內有相關角色與工作功能的不同部份代表共同協調。	□	□
	6.1.3	資訊安全責任的配置：		
		應明確劃分所有資訊安全責任。	□	□

	6.1.4	資訊處理設施的授權作業：		
		應定義與實施新資訊處理設施的管理人員授權程序。	☐	☐
	6.1.5	保密協議：		
		應區別與定期審查反映組織對保護資訊需求的機密要求或保密協定要求。	☐	☐
	6.1.6	與有關當局的聯繫：		
		應與有關當局維持適當聯繫。	☐	☐
	6.1.7	與特殊利益團體的聯繫：		
		應與特殊利益團體或其他專業人員的安全論壇及專業協會維持適當聯繫。	☐	☐
	6.1.8	獨立的資訊安全審查：		
		應定期或安全實作發生重大變更時，獨立審查組織管理資訊安全的方法與其實作（例如：資訊安全的控制目標控制措施、政策、過程、及程序）。	☐	☐
	6.2	外部團體		
	6.2.1	識別與外部團體有關的風險：		
		授權外部團體存取之前，應識別涉及外部團體營運過程的組織資訊及資訊處理設施的風險，與實施適當控制措施。	☐	☐
	6.2.2	應付客戶的安全處理：		
		在給予客戶存取組織的資訊或資產之前，應處理已識別的安全要求。	☐	☐
	6.2.3	第三方合約的安全處理：		
		涉及存取、處理、通訊或管理組織的資訊或資訊處理設施，或對資訊處理設施增加產品或服務的第三方合約，應涵蓋所有相關安全要求。	☐	☐

▼表3.3：安全政策資產管理 檢測評核要項表

項次	控制項目	控制措施	評核	
三	7.1	資產責任	符合	未符合
	7.1.1	資產清冊：		
		應清楚地鑑別所有資產，並製作與維護所有的重要資產之清冊。	☐	☐
	7.1.2	資產的擁有：		
		與資訊處理設施相關的所有資訊及資產應由組織指定的部份所“擁有”。	☐	☐
	7.1.3	資產的可接受使用：		
		與資訊處理設施相關的資訊及資產，其可接受使用的規則應予以識別、記錄、及實施。		
	7.2	資產分類		
	7.2.1	分類指導綱要：		
		資訊應以其對組織的價值、法律要求、敏感性、及重要性加以分類。	☐	☐
	7.2.2	資訊標示與處理：		

		應依照組織所採用的分類概要，發展與實施一套適當的資訊標示與處理的程序。	□	□

▼表3.4：人力資源安全 檢測評核要項表

項次	控制項目	控制措施	評核	
四	8.1	聘雇之前	符合	未符合
	8.1.1	角色與職務：		
		受雇人員、承包商及第三方使用者的安全角色與職務，應依照組織的資訊安全政策定義與文件化。	□	□
	8.1.2	篩選：		
		應依照相關法律、規章與倫理，並對照營運要求、將會存取的資訊分類、及所認知的風險，實施對受雇人員、承包商及第三方使用者所有應徵者的背景查證核對。	□	□
	8.1.3	聘用條件與限制：		
		受雇人員、承包商及第三方使用者應將聘用條件與限制視為契約合約的一部份，同意與簽訂陳述本身與組織對資訊安全之責任的聘雇合約。	□	□
	8.2	聘雇期間		
	8.2.1	管理責任：		
		管理當局應要求受雇人員、承包商及第三方使用者依照組織已建立的政策及程序應用安全。	□	□
	8.2.2	資訊安全認知教育與訓練：		
		組織所有受雇人員及相關的承包商及第三方使用者應接受與其工作功能相關，適當的認知訓練，與組織政策及程序的定期更新。	□	□
	8.2.3	懲罰程序：		
		對違反安全的受雇人員，應有正式的懲罰程序。	□	□
	8.3	聘雇終止或變更		
	8.3.1	聘雇終止：		
		執行聘雇終止或變更的職責應清楚的定義及指派。	□	□
	8.3.2	資產歸還：		
		所有受雇人員、承包商及第三方使用者在終止其聘雇、合約或協議時應歸還其擁有的所有組織的資產。	□	□
	8.3.3	移除存取權限：		
		受雇人員、承包商及第三方使用者對資訊及資訊處理設施的存取權限，在終止其聘雇、合約、協議、或因變更而調整時應予以移除。	□	□

▼表3.5：實體與環境安全 檢測評核要項表

項次	控制項目	控制措施	評核	
五	9.1	安全區域	符合	未符合
	9.1.1	實體安全邊界：		

		應使用安全邊界（例如牆、刷卡控制的進入大門、或人力接待處等阻礙）以保護存放資訊及資訊處理設施的區域。	□	□
	9.1.2	實體進入控制措施：		
		安全區域應有適當進入控制措施，確保只有授權人員方可進出。	□	□
	9.1.3	保護辦公處所及設施：		
		應設計與應用辦公室、房間及設施的實體安全。	□	□
	9.1.4	不受外在及環境的威脅：		
		應設計與應用實體保護，不受火災、洪水。、地震、爆炸、民間暴動、及其它自然或人為災難的損害。	□	□
	9.1.5	在保全區域內工作：		
		應設計與應用在保全區域內工作的實體保護及指導綱要。	□	□
	9.1.6	公共存取、收發、及裝卸區		
		應控制收發裝卸區及其它未經授權人員可進入邊界點等存取點，若可能，隔離資訊處理設施以防止未經授權的存取。	□	□
	9.2	設備安全		
	9.2.1	設備安置及保護：		
		應安置或保護設備，以降低來自環境之威脅及危險，以及未經授權存取之機會。	□	□
	9.2.2	公用設施支援：		
		應保護設備不受電力失效及其他公用設施失效導致的中斷。	□	□
	9.2.3	纜線的安全：		
		應保護傳送資料或支援資訊服務之電源與通訊纜線，以防止竊聽或損害。	□	□
	9.2.4	設備維護：		
		應正確地維護設備，確保其持續的可用性與完整性。	□	□
	9.2.5	場外設備之安全：		
		場外設備的適用安全，應考慮在組織邊界外工作的不同風險。	□	□
	9.2.6	設備之安全報廢或再使用：		
		在報廢前應核對所有包含儲存媒體的設備，確保任何敏感性資料及授權的軟體已被移除或安全地覆寫。	□	□
	9.2.7	攜出財產		
		未經事前授權，設備、資訊或軟體不應帶至場外。	□	□

▼表3.6：通訊與作業管理 檢測評核要項表

項次	控制項目	控制措施	評核	
六	10.1	安全區域作業程序與責任	符合	未符合
	10.1.1	書面的作業程序：		
		作業程序應製作文件、維護、及使有需要的所有使用者均可取得。	□	□
	10.1.2	變更管理：		

		應控制資訊處理設施與系統的變更。	□	□
	10.1.3	職責區隔：		
		應區分職務與責任範圍，以降低組織資產遭未經授權或非故意的修改之機會。	□	□
	10.1.4	分隔開發、測試、及作業設施：		
		應分隔開發、測試、及作業設施，以降低對作業系統未經授權存取或變更的風險。	□	□
	10.2	第三方服務遞送管理		
	10.2.1	服務遞送：		
		應確保第三方實施、執行、及維護包含於第三方服務遞送協議內的安全控制措施、服務定義及遞送等級。	□	□
	10.2.2.	監控與審查第三方服務：		
		應定期監控與審查由第三方提供的服務、報告、及記錄，並定期實行監視。	□	□
	10.2.3	管理第三方服務的變更：		
		考慮牽涉到營運系統及過程的重要性與重新評鑑的風險，應管理服務條款的變更，包括維護及改善現存的資訊安全政策、程序、及控制措施。	□	□
	10.3	系統規劃與驗收		
	10.3.1	容量規劃：		
		資源的使用應監控、調校、及預估未來容量需求，以確保所需的系統執行績效。	□	□
	10.3.2	系統驗收：		
		應建立對新資訊系統、系統升級、及新版本的驗收標準，且開發期間與驗收前應完成適當之系統測試。	□	□
	10.4	防範惡意碼與行動碼		
	10.4.1	對抗惡意碼的控制措施：		
		應實施防範惡意碼的偵測、預防、及復原控制措施與適當之使用者認知程序。	□	□
	10.4.2	對抗行動碼的控制措施：		
		授權使用行動碼時，其組態應確保授權的行動碼依據清楚定義的安全政策作業，並應阻止執行未經授權的行動碼。	□	□
	10.5	備份		
	10.5.1	資訊備份：		
		應依據協議的備份政策定期備份與測試資訊與軟體的拷貝。	□	□
	10.6	網路安全管理		
	10.6.1	網路控制措施：		
		應充分地管理與控制網路，使不受威脅，並且維護使用網路的系統與應用，包括傳輸中的資訊之安全。	□	□
	10.6.2	網路服務安全：		
		應識別所有網路服務的安全特性、服務等級、及管理需求，並納入不論是內部或外包的任何網路服務協議。	□	□
	10.7	處理媒體		
	10.7.1	可攜式媒體的管理：		

		應有適當的可攜式媒體的管理程序。	☐	☐
	10.7.2	媒體的報廢：		
		媒體不再使用時，應使用正式程序安全穩固地報廢。	☐	☐
	10.7.3	資訊處理程序：		
		應建立資訊的處理及儲存程序，以保護資訊不被未經授權的揭露或誤用。	☐	☐
	10.7.4	系統文件的安全：		
		應保護系統文件，不被未經授權的存取。	☐	☐
	10.8	資訊交換		
	10.8.1	資訊交換政策與程序：		
		應有適當的正式交換政策、程序、及控制措施，以保護經由使用所有型式通訊設施的資訊交換。	☐	☐
	10.8.2	交換協議：		
		組織與外部團體間資訊與軟體的交換應建立協議。	☐	☐
	10.8.3	運送過程中的實體媒體：		
		應保護運送中在組織實體界限之外、包含資訊的媒體，不被未經授權的存取、誤用或毀損。	☐	☐
	10.8.4	電子傳訊：		
		應適當地保護涉及電子傳訊的資訊。	☐	☐
	10.8.5	營運資訊系統：		
		應發展與實施政策及程序，以保護與營運資訊系統互連有關的資訊。	☐	☐
	10.9	電子商務服務		
	10.9.1	電子商務：		
		應保護在公用網路上傳輸、涉及電子商務的資訊，使不受詐欺行為、合約爭議、及未經授權的揭露與修改。	☐	☐
	10.9.2	線上交易：		
		應保護涉及線上交易的資訊，以防止不完整的傳輸、錯誤的路由、未經授權的訊息交替、未經授權的揭露、及未經授權的訊息複製或重送。	☐	☐
	10.9.3	公開可取得的資訊		
		應保護在公眾開放系統上可取得資訊的完整性，以防止未經授權的修改。	☐	☐
	10.10	監控		
	10.10.1	監視日誌：		
		應產生與保持一段協議期間的監視日誌記錄使用者活動、例外、及資訊安全事件，以協助未來的調查與存取控制監控。	☐	☐
	10.10.2	監控系統的使用：		
		應建立監控資訊處理設施使用的程序，並定期審查監控活動的結果。	☐	☐
	10.10.3	保護日誌資訊：		
		應保護記錄日誌設施與日誌資訊，不受竄改及未經授權的存取。	☐	☐
	10.10.4	管理者與操作員日誌：		

		應記錄系統管理者與操作員的活動日誌。	□	□
	10.10.5	失誤日誌：		
		失誤應予以記錄日誌、分析、及採取適當行動。	□	□
	10.10.6	時鐘同步：		
		組織或安全領域內所有相關資訊處理系統的時鐘應與同一協議的準確時間來源同步。	□	□

▼表3.7：存取控制 檢測評核要項表

項次	控制項目	控制措施	評核	
七	11.1	存取控制的營運要求	符合	未符合
	11.1.1	存取控制政策：		
		應建立、文件化、及依據存取的營運與安全要求審查存取控制政策。	□	□
	11.2	使用者存取管理		
	11.2.1	使用者註冊：		
		應有正式、適當的使用者註冊及註銷流程，對所有資訊系統及服務核准與撤銷存取。	□	□
	11.2.2	特權管理：		
		應限制與控制特權的分配與使用。	□	□
	11.2.3	使用者通行碼管理：		
		應以正式的管理過程控制通行碼的分配。	□	□
	11.2.4	使用者存取權限審查：		
		管理階層應定期使用正式過程審查使用者的存取權限。	□	□
	11.3	使用者責任		
	11.3.1	通行碼的使用：		
		應要求使用者遵守良好安全方式，選擇及使用通行碼。	□	□
	11.3.2	無人看管的資訊設備：		
		使用者應確保無人看管的資訊設備有適當保護措施。	□	□
	11.3.3	桌面淨空與螢幕淨空政策：		
		應採取文件與可攜式儲存媒體的桌面淨空政策及資訊處理設施的螢幕淨空政策。	□	□
	11.4	網路存取控制		
	11.4.1	網路服務的使用政策：		
		應只能提供使用者存取被明確准許使用的服務。	□	□
	11.4.2	外部連線的使用者鑑別：		
		應使用適當的鑑別法以控制遠端使用者的存取。	□	□
	11.4.3	網路設備識別：		
		應考慮自動的設備識別方法以鑑別來自特定位置與設備的連線。	□	□
	11.4.4	遠端診斷與組態埠保護：		
		應控制對診斷與組態埠的實體與邏輯存取。	□	□
	11.4.5	網路區隔：		
		應區隔在網路上的資訊服務、使用者、及資訊系統群組。	□	□
	11.4.6	網路連線控制：		

		應限制使用者連線至共享網路，特別是穿越組織界限的能力與存取控制政策與營運應用的要求一致。	□	□
	11.4.7	網路路由控制：		
		應實施網路路由控制，以確保電腦連線與資訊流不破壞企業應用系統之存取控制政策。	□	□
	11.5	作業系統存取控制		
	11.5.1	安全登入程序：		
		應由安全登入程序控制作業系統的存取。	□	□
	11.5.2	使用者識別與鑑別：		
		所有使用者應有個人使用的專屬識別符（ 使用者識別序號）。應選擇適切的鑑別技術以證實使用者宣稱之身分。	□	□
	11.5.3	通行碼管理系統：		
		管理通行碼的系統應為互動式且確保通行碼品質。	□	□
	11.5.4	使用系統公用程式：		
		應限制與嚴密控制可能能夠置換系統與應用控制的公用程式之使用。	□	□
	11.5.5	連線階段逾時：		
		一定時間的不活動後，應關閉不活動的連線階段。	□	□
	11.5.6	連線時間限制		
		對高風險的應用系統，應使用連線時間限制以提供額外的安全性。	□	□
	11.6	應用與資訊存取控制		
	11.6.1	資訊存取限制：		
		應根據已定義的存取控制政策限制使用者與支援人員對資訊及應用系統功能之存取。	□	□
	11.6.2	敏感性系統的隔離：		
		敏感性系統應有專屬（ 隔離） 的電腦作業環境。	□	□
	11.7	行動式電腦作業與遠距工作：		
	11.7.1	行動式電腦作業與通訊：		
		應制訂正式政策及採取適當的安全量測，以防止使用行動式電腦與通訊設施的風險。	□	□
	11.7.2	遠距工作：		
		應發展與實施遠距工作活動的政策、作業計畫、及流程。	□	□

▼表3.8：資訊系統取得、開發、及維護 檢測評核要項表

項次	控制項目	控制措施	評核	
八	12.1	資訊系統的安全要求	符合	未符合
	12.1.1	安全要求分析及規格：		
		新資訊系統或現有資訊系統提升的營運要求聲明中，應詳述安全控制措施的要求。	□	□
	12.2	應用系統的正確處理		
	12.2.1	輸入資料確認：		
		輸入應用系統的資料應予確認，以確保該資料正確且適當。	□	□

	12.2.2	內部處理控制：		
		系統內應包含有確認核對，以偵測任何資訊經由處理錯誤或故意行為的損壞。	□	□
	12.2.3	訊息完整性：		
		確保應用系統內資訊鑑別性與保護訊息完整性的要求應予識別，並識別與實施適當的控制措施。	□	□
	12.2.4	輸出資料確認：		
		應用系統資料輸出應經確認，以確保儲存資訊的處理程序正確且合乎實際情況。	□	□
	12.3	密碼控制措施		
	12.3.1	使用密碼控制措施政策：		
		應發展與實施使用密碼控制措施以保護資訊的政策。	□	□
	12.3.2	金鑰管理：		
		應有金鑰管理以支援組織使用密碼技術。	□	□
	12.4	系統檔案的安全		
	12.4.1	作業軟體的控制：		
		應有各程序以管制作業系統上軟體的安裝。	□	□
	12.4.2	系統測試資料的保護：		
		應小心地選擇測試資料，並保護及控制。	□	□
	12.4.3	程式原始碼的存取控制：		
		應限制對程式原始碼的存取。	□	□
	12.5	開發及支援作業的安全		
	12.5.1	變更控制程序：		
		變更的實施應使用正式變更控制程序予以控制。	□	□
	12.5.2	作業系統變更後的應用系統技術審查：		
		作業系統變更時，應審查與測試重要營運應用系統，以確保對組織作業或安全無不利的衝擊。	□	□
	12.5.3	套裝軟體變更的限制：		
		應阻止修改套裝軟體，限制有必要的變更，應嚴格管制所有的修改。	□	□
	12.5.4	資料洩漏：		
		應防止資訊洩漏的機會。	□	□
	12.5.5	軟體開發委外：		
		組織應監督與監控軟體開發委外。	□	□
	12.6	技術脆弱性管理		
	12.6.1	技術脆弱性控制		
		應取得及時的使用中資訊系統之技術脆弱性資訊、評估組織對該脆弱性的暴露、及採取適當的量測，以處理有關的風險。	□	□

▼表3.9：資訊安全事件管理 檢測評核要項表

項次	控制項目	控制措施	評核	
九	13.1	通報資訊安全事件與弱點	符合	未符合
	13.1.1	通報資訊安全事件		

		應循適當的管理管道儘快通報資訊安全事件。	□	□
	13.1.2	通報安全弱點		
		應要求資訊系統與服務的所有受雇人員、承包商及第三方使用者記錄與通報明顯的或可疑的系統或服務之任何安全弱點。	□	□
	13.2	管理資訊安全事件與改善		
	13.2.1	職務與程序：		
		應建立管理職務與程序，確保對資訊安全事件迅速、有效、及有條理的回應。	□	□
	13.2.2	從資訊安全事件中學習：		
		應有適當的機制使資訊安全事件的型式、數量、及成本能被量化與監控。	□	□
	13.2.3	蒐證：		
		資訊安全事件後，對人或組織的跟催行動涉及法律行動（不是民事就是刑事）時，應遵照證據規則收集、保留、及提交證據，以在相關審判時交出。	□	□

▼表3.10：營運持續管理 檢測評核要項表

項次	控制項目	控制措施	評核	
十	14.1	營運持續管理的資訊安全層面	符合	未符合
	14.1.1	營運持續管理過程中包含資訊安全：		
		應發展與維護全組織持續營運的管理過程，處理組織持續營運所需的資訊與資訊安全要求。	□	□
	14.1.2	營運持續與風險評鑑：		
		應識別能導致營運過程中斷的事件，連同該中斷的或然率及衝擊，以及它們對資訊安全的衝擊與後果。	□	□
	14.1.3	發展與實施包含資訊安全的持續計畫：		
		應發展與實施計畫，在重要營運過程中斷、或失效後，維持或恢復作業，並確保所要求等級資訊在所要求時間級別之前的可用性。	□	□
	14.1.4	營運持續規劃框架：		
		應維持單一營運持續計畫之框架，以確保所有計畫皆一致，一貫地處理資訊安全要求，並識別測試及維護的優先順序。	□	□
	14.1.5	營運持續計畫的測試、維護、及重新評鑑：		
		營運持續計畫應定期測試與更新，以確保維持最新且有效。	□	□

▼表3.11：營運持續管理符合性 檢測評核要項表

項次	控制項目	控制措施	評核	
十	15.1	遵守法規要求	符合	未符合
	15.1.1	識別適用的法令：		

		對組織與每一資訊系統，應清楚定義、文件化、及維持最新所有與資訊系統有關之法規、管理規定、及合約要求，與組織滿足上述要求的方法。	□	□
	15.1.2	智慧財產權（IPR）：		
		應實施適當流程，以確保關於可能有智慧財產權及專屬軟體產品資料的使用上遵守法令的、管理規定的、及合約的要求。	□	□
	15.1.3	組織記錄的保護：		
		應依據法令的、管理規定的、合約的、及營運的要求保護重要記錄，以防止遺失、毀損、及偽造。	□	□
	15.1.4	個人資訊的資料保護與隱私：		
		應如相關法令、管理規定、及若適用合約條款所要求的，確保資料保護與隱私。	□	□
	15.1.5	防止資訊處理設施的誤用：		
		應制止使用者以未經授權的目的使用資訊處理設施。	□	□
	15.1.6	密碼控制的規定		
		應依照所有相關的協議、法律、及管理規定使用密碼控制措施。	□	□
	15.2	遵守安全政策與標準		
	15.2.1	遵守安全政策與標準		
		管理者應確保其責任範圍內所有安全流程皆正確執行，以達到遵守安全政策與標準。	□	□
	15.2.2	核對技術符合性		
		應定期核對資訊系統是否符合安全實施標準。	□	□
	15.3	資訊系統稽核的考量		
	15.3.1	資訊系統稽核控制		
		涉及作業系統檢查的稽核要求與活動應謹慎規劃且獲得同意，以降低營運過程崩潰之風險。	□	□
	15.3.2	資訊系統稽核工具的保護		
		應保護資訊系統稽核工具之存取，以防止任何可能的誤用或危害。	□	□

3.3.評核結果與問題檢討

CNS 17799（ISO/IEC 17799:2005(E)）為通用的資訊安全管理規範，雖未特別針對該領域之特殊性，惟仍可經此評核探討該企業之資訊安全防護能力與應需要加強之控制項目，如表 3.12 所示為該企業檢測未符合項目，合計數量為 50 項。為瞭解該企業資訊安全防護能力之罩門，本研究以「符合度」指標探討該企業現行資訊安全文件與 CNS 17799（ISO/IEC 17799:2005(E)）資訊安全管理規範之符合程度（十一大管理要項中，企業各項評核符合 CNS 17799（ISO/IEC 17799:2005(E)）標準之百分比例），並依「符合度」百分比例分為三級，評核原則如下：

良好－符合比例達 80%

普通－符合比例達 60%

待加強－符合比例未達 60%

如表 3.13 所示該企業在十大管理要項中，有五項評核等級為「良好」、三項評核等級為「普通」。惟在「通訊與作業管理」、「存取控制」、「資訊系統取得、開發、及維護」項目之評核成績均不甚理想，當中又以「存取控制」項目與標準之要求差距甚多，需加以改善。

▼表 3.12：企業檢測未符合項目

項次	控制項目	控制措施
二	6.1	內部組織
	6.1.6	與有關當局的聯繫：
		應與有關當局維持適當聯繫。
	6.1.7	與特殊利益團體的聯繫：
		應與特殊利益團體或其他專業人員的安全論壇及專業協會維持適當聯繫。
	6.2	外部團體
	6.2.1	識別與外部團體有關的風險：
		授權外部團體存取之前，應識別涉及外部團體營運過程的組織資訊及資訊處理設施的風險，與實施適當控制措施。
三	7.1	資產責任
	7.1.3	資產的可接受使用：
		與資訊處理設施相關的資訊及資產，其可接受使用的規則應予以識別、記錄、及實施。
四	8.1	聘雇之前
	8.1.2	篩選：
		應依照相關法律、規章與倫理，並對照營運要求、將會存取的資訊分類、及所認知的風險，實施對受雇人員、承包商及第三方使用者所有應徵者的背景查證核對。
	8.2	聘雇期間
	8.2.2	資訊安全認知教育與訓練：
		組織所有受雇人員及相關的承包商及第三方使用者應接受與其工作功能相關，適當的認知訓練，與組織政策及程序的定期更新。
五	9.1	安全區域
	9.1.5	在保全區域內工作：
		應設計與應用在保全區域內工作的實體保護及指導綱要。
	9.1.6	公共存取、收發、及裝卸區
		應控制收發裝卸區及其它未經授權人員可進入邊界點等存取點，若可能，隔離資訊處理設施以防止未經授權的存取。
	9.2	設備安全
	9.2.3	纜線的安全：
		應保護傳送資料或支援資訊服務之電源與通訊纜線，以防止竊聽或損害。
六	10.1	安全區域作業程序與責任
	10.1.4	分隔開發、測試、及作業設施：
		應分隔開發、測試、及作業設施，以降低對作業系統未經

		授權存取或變更的風險。
	10.2	第三方服務遞送管理
	10.2.2.	監控與審查第三方服務：
		應定期監控與審查由第三方提供的服務、報告、及記錄，並定期實行監視。
	10.4	防範惡意碼與行動碼
	10.4.1	對抗惡意碼的控制措施：
		應實施防範惡意碼的偵測、預防、及復原控制措施與適當之使用者認知程序。
	10.4.2	對抗行動碼的控制措施：
		授權使用行動碼時，其組態應確保授權的行動碼依據清楚定義的安全政策作業，並應阻止執行未經授權的行動碼。
	10.6	網路安全管理
	10.6.1	網路控制措施：
		應充分地管理與控制網路，使不受威脅，並且維護使用網路的系統與應用，包括傳輸中的資訊之安全。
	10.6.2	網路服務安全：
		應識別所有網路服務的安全特性、服務等級、及管理需求，並納入不論是內部或外包的任何網路服務協議。
	10.7	處理媒體
	10.7.3	資訊處理程序：
		應建立資訊的處理及儲存程序，以保護資訊不被未經授權的揭露或誤用。
	10.8	資訊交換
	10.8.1	資訊交換政策與程序：
		應有適當的正式交換政策、程序、及控制措施，以保護經由使用所有型式通訊設施的資訊交換。
	10.8.2	交換協議：
		組織與外部團體間資訊與軟體的交換應建立協議。
	10.8.3	運送過程中的實體媒體：
		應保護運送中在組織實體界限之外、包含資訊的媒體，不被未經授權的存取、誤用或毀損。
	10.8.4	電子傳訊：
		應適當地保護涉及電子傳訊的資訊。
	10.8.5	營運資訊系統：
		應發展與實施政策及程序，以保護與營運資訊系統互連有關的資訊。
	10.9	電子商務服務
	10.9.1	電子商務：
		應保護在公用網路上傳輸、涉及電子商務的資訊，使不受詐欺行為、合約爭議、及未經授權的揭露與修改。
	10.9.2	線上交易：
		應保護涉及線上交易的資訊，以防止不完整的傳輸、錯誤的路由、未經授權的訊息交替、未經授權的揭露、及未經授權的訊息複製或重送。

	10.9.3	公開可取得的資訊
		應保護在公眾開放系統上可取得資訊的完整性，以防止未經授權的修改。
	10.10	監控
	10.10.3	保護日誌資訊：
		應保護記錄日誌設施與日誌資訊，不受竄改及未經授權的存取。
七	11.1	存取控制的營運要求
	11.1.1	存取控制政策：
		應建立、文件化、及依據存取的營運與安全要求審查存取控制政策。
	11.3	使用者責任
	11.3.2	無人看管的資訊設備：
		使用者應確保無人看管的資訊設備有適當保護措施。
	11.4	網路存取控制
	11.4.2	外部連線的使用者鑑別：
		應使用適當的鑑別法以控制遠端使用者的存取。
	11.4.4	遠端診斷與組態埠保護：
		應控制對診斷與組態埠的實體與邏輯存取。
	11.4.5	網路區隔：
		應區隔在網路上的資訊服務、使用者、及資訊系統群組。
	11.4.6	網路連線控制：
		應限制使用者連線至共享網路，特別是穿越組織界限的能力與存取控制政策與營運應用的要求一致。
	11.4.7	網路路由控制：
		應實施網路路由控制，以確保電腦連線與資訊流不破壞企業應用系統之存取控制政策。
	11.5	作業系統存取控制
	11.5.1	安全登入程序：
		應由安全登入程序控制作業系統的存取。
	11.5.5	連線階段逾時：
		一定時間的不活動後，應關閉不活動的連線階段。
	11.5.6	連線時間限制
		對高風險的應用系統，應使用連線時間限制以提供額外的安全性。
	11.6	應用與資訊存取控制
	11.6.1	資訊存取限制：
		應根據已定義的存取控制政策限制使用者與支援人員對資訊及應用系統功能之存取。
	11.6.2	敏感性系統的隔離：
		敏感性系統應有專屬（ 隔離） 的電腦作業環境。
	11.7	行動式電腦作業與遠距工作：
	11.7.1	行動式電腦作業與通訊：
		應制訂正式政策及採取適當的安全量測，以防止使用行動式電腦與通訊設施的風險。

	11.7.2	遠距工作：
		應發展與實施遠距工作活動的政策、作業計畫、及流程。
八	12.4	系統檔案的安全
	12.4.2	系統測試資料的保護：
		應小心地選擇測試資料，並保護及控制。
	12.4.3	程式原始碼的存取控制：
		應限制對程式原始碼的存取。
	12.5	開發及支援作業的安全
	12.5.1	變更控制程序：
		變更的實施應使用正式變更控制程序予以控制。
	12.5.2	作業系統變更後的應用系統技術審查：
		作業系統變更時，應審查與測試重要營運應用系統，以確保對組織作業或安全無不利的衝擊。
	12.5.4	資料洩漏：
		應防止資訊洩漏的機會。
	12.5.5	軟體開發委外：
		組織應監督與監控軟體開發委外。
	12.6	技術脆弱性管理
	12.6.1	技術脆弱性控制
		應取得及時的使用中資訊系統之技術脆弱性資訊、評估組織對該脆弱性的暴露、及採取適當的量測，以處理有關的風險。
九	13.1	通報資訊安全事件與弱點
	13.1.2	通報安全弱點
		應要求資訊系統與服務的所有受雇人員、承包商及第三方使用者記錄與通報明顯的或可疑的系統或服務之任何安全弱點。
十	14.1	營運持續管理的資訊安全層面
	14.1.3	發展與實施包含資訊安全的持續計畫：
		應發展與實施計畫，在重要營運過程中斷、或失效後，維持或恢復作業，並確保所要求等級資訊在所要求時間級別之前的可用性。
十	15.1	遵守法規要求
	15.1.5	防止資訊處理設施的誤用：
		應制止使用者以未經授權的目的使用資訊處理設施。
	15.3	資訊系統稽核的考量
	15.3.2	資訊系統稽核工具的保護
		應保護資訊系統稽核工具之存取，以防止任何可能的誤用或危害。

▼表 3.13：企業檢測結果統計

項目	CNS 17799:2005 控制措施各項合計	企業評核符合總計	符合率	評核結果
安全政策	2	2	100%	良好
組織資訊安全	11	8	73%	普通
安全政策資產管理	5	4	80%	良好
人力資源安全	9	7	78%	普通
實體與環境安全	13	10	77%	普通
通訊與作業管理	32	16	50%	待加強
存取控制	25	11	44%	待加強
資訊系統取得、開發、及維護	16	9	56%	待加強
資訊安全事件管理	5	4	80%	良好
營運持續管理	5	4	80%	良好
營運持續管理符合性	10	8	80%	良好
合計	133	83		

在上述「待加強」項目所造成之風險，最常被舉證的攻擊形式是病毒以及人員對網路的存取濫用。由於資訊科技之一日千里、個人電腦的普及、網路通信結構之改進與全球資訊網的風行，網際網路以驚人之速度成長，使得資訊傳播無遠弗屆。每天都有數以萬計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中；雖然大部分之使用者都是合法地存取資料，但仍常有非法入侵與存取其他電腦中的事件發生，而老練之駭客更經常苦心鑽研弱點，藉以侵入資訊系統。Klez、Nimda 等病毒和蠕蟲以及 SQL Slammer，都是利用軟體中的安全性弱點攻擊電腦，然後再對其他電腦發動新的攻擊。而這些弱點也提供了攻擊者機會，透過拒絕合法使用者的存取、啟用提高的特殊權限，以及暴露資料致使未經授權的檢視及篡改，而使得資訊及資產受到危害。

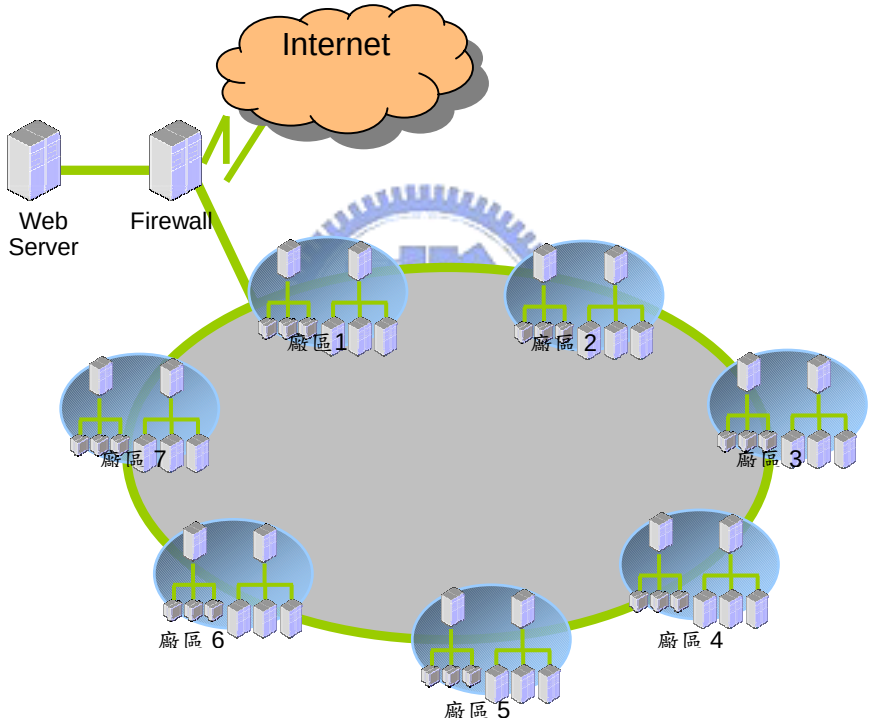
弱點攻擊技術日新月異防不勝防，而防範之道必須建立滴水不漏的基礎架構之上。本研究將在下一章提出一可行之企業安全性修補程式之架構設計，以及利用實作之方式證明該架構是可用以支援可信賴資訊安全使用環境之解決方案。

第四章 企業安全性修補程式架構之設計與實作

4.1. 基礎架構環境檢視

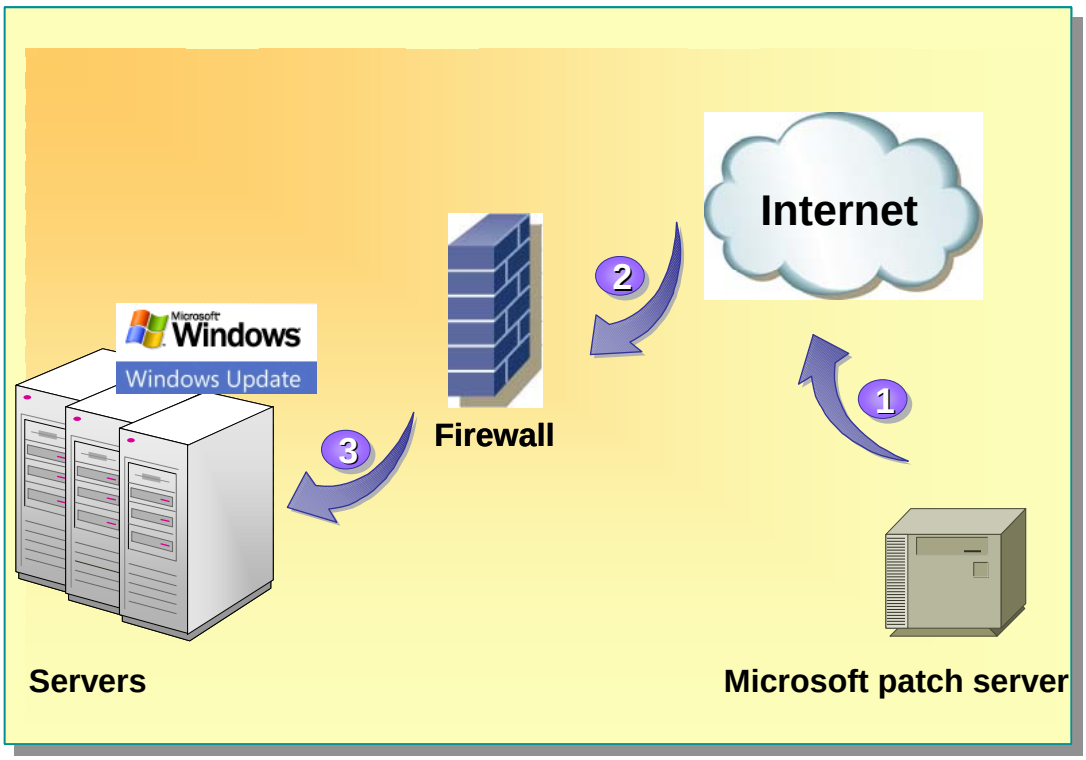
如圖 4.1 所示為該企業的基礎架構圖之實例，其依功能性不同將檢視的項目分成兩個部分：

1. 辦公使用者：在辦公區，依作業系統不同可以分成兩個部分來檢視。
   工作站(包含 NT4/2000)總數量約 12000 台
   伺服器(Windows NT4/2000/2003)總數量約 1100 台
2. 遠距工作使用者：這二者均被視為辦公區的一部分，因為他們可在自己的辦公室或家中透過撥接或是寬頻的方式連上中連結到公司的網路。



▲圖 4.1：企業網路基礎架構圖

目前如圖 4.2 所示是目前該企業的伺服器端更新電腦安全性修補程式之基礎架構，每一台伺服器均安裝 Windows Update，透過網際網路自動取得最新之安全性修補程式；工作站端則由工程師透過網際網路取得安全性修補程式後逐一手動執行安裝。



▲圖 4.2：伺服器端更新電腦安全性修補程式基礎架構圖

4.2. 目前架構對於網路安全管理上不足處之分析

1. 無法確知目前網路上哪些主機具有安全性弱點：

   在發行新的安全性佈告欄時才掃描整個環境以尋找遺失更新的電腦，經過事實證明，是非常耗時的，而這點對於大型環境更是如此。在理想狀態下，應該發展並實行一套機制來自動收集並分析在弱點掃描過程中所產生的資訊，並針對安全性警訊作出回應，以有效維護作業中基準線的安全。

2. 沒有足夠的時間可以安裝或部署安全性修補程式：

   依目前架構，每一台伺服器均自行透過網際網路自動取得最新之修補程式，若遇上網路頻寬使用率較高時便會發生安全性修補程式更新失敗的問題(經實際評估失敗率約為 15%)。另外由於工作站總數量多達 12269 多台，如表 4.1 所示若要所有工作站完成安全性修補程式更新時間約為 1394 人/天，可能會發生安全性修補程式尚未更新完成前就已經遭受攻擊的問題。

▼表 4.1：工作站更新電腦安全性修補程式預估時間

安全性修補程式	數量	每一台工作站檢查時間(分鐘)	預估檢查作業完成時間(人/天)	每一台工作站部署時間(小時)	預估部署作業完成時間(人/天)	修補程式更新作業時間(人/天)
MS03-026/007	7,000	15	219	0.5	540	759
MS03-039	7,000	15	219	0.5	574	792
MS03-041~44	8,000	15	250	0.5	615	865
MS04-040	9,800	15	306	0.5	772	1078
MS04-011	10108	15	316	0.5	823	1138
MS04-022	9,600	15	300	0.5	769	1069
MS04-023	9,700	15	303	0.5	536	839
MS04-025	12,269	15	383	0.5	1011	1394

計算方式說明：

1. 人/天＝總時間/60（分鐘）/8（每日工時）。
2. 預估檢查作業完成時間(人/天)＝每一台工作站檢查時間(15 分鐘)x數量/60/8。
3. 預估部署作業完成時間（人/天）＝每一台工作站部署時間（0.5 小時）x數量/60/8。
4. 修補程式更新作業時間（人/天）＝預估檢查作業完成時間（人/天）＋預估部署作業完成時間（人/天）。

資料來源：本研究整理

3. 有些系統無法自動安裝安全性修補程式：

某些獨立電腦或不受控制的非網域成員電腦由於沒有這些不受管理用戶端的本機系統管理員權限，故難以收集電腦名稱及 IP 位址之外的系統資訊並用以識別完成安全性修補程式需要。

4. 有些系統無法自動安裝安全性修補程式：

訪客、行動和遠端使用者，如同辦公區中一般的客戶端一樣，這對於企業來說，這些客戶端也是潛在的攻擊來源，需另行處理。

4.3. 企業安全性修補程式之架構設計

4.3.1. 企業安全性修補程式之管理需求

1. 當採用新的硬體或軟體而造成環境的變更時，通常會執行設定，設定活動是支援順利且有效的安全性修補程式管理所必需的。包括：
   - □ 取得庫存及建立環境的基準線：作業基準線包含的是讓生產環境中不同類型電腦皆能安全運作的所有必要軟體。
   - □ 訂閱安全性警訊及其他資訊來源：安全性佈告欄會識別新的產品缺點、過去佈告欄的重要更新，以及已被其他人發現的新病毒。
   - □ 建立安全性報告以協助識別問題：識別環境中的病毒或入侵，可指出需要儘速解決之進行中的攻擊。
   - □ 設定及維護修補程式管理基礎架構：無論是任何大小的組織，都應利用自動化工具，讓系統管理員得知可用的更新，並部分掌控安全性修補程式的安裝情形。

2. 以每天或每週為執行基礎，定期檢閱網站、安全性通知以及安全性報告，以識別新的軟體更新及安全性問題，並判定更新與環境中問題的關聯性。
   - □ 識別：判定環境是否需要修補程式，以及其來源是否有效。
   - □ 關聯性：判定修補程式對於組織的 資訊技術（Information Technology，簡稱 IT）基礎架構環境是否有意義。
   - □ 隔離觀察：在一個或多個修補程式中查出可能會影響組織 IT 基礎架構的病毒或其他惡意程式碼時，隔離任何與修補程式相關的檔案。

3. 識別環境中新安全性弱點，並擬定發行安全性修補程式或相關的對策，包括：
   - □ 變更管理：瞭解問題、將變更分類及排定優先順序，以及取得對生產環境進行變更之核准的程序。
   - □ 發行管理：計畫、開發、測試，以及在生產環境中部署變更的程序。
   - □ 檢閱變更：因為負面的商業影響或其他影響品質的原因而需要時，此步驟可以包括復原。

4. 對於組織環境中一些分散的系統管理層級 (例如，多個擁有系統管理權限的群組或是在本身電腦上擁有系統管理權限的一般使用者)、不受限或是不存在的基準線電腦安裝標準，或是不受管理的電腦 (例如，實驗室電腦或是「地下伺服器」)。均要確實執行安全性原則，其中包括：
   - □ 安裝標準，描述所支援的安裝位置及方法。
   - □ 網路及網域標準，指出如何命名和設定網路協定資訊，以及電腦應加入哪些網域。
   - □ 作業系統安全性選項及原則設定，包括根據必要服務減少開放的連接埠數目。
   - □ 相容的最小版本服務套件以及安全性修補程式，並以每次的安全性發行進行更新。
   - □ 相容的防毒軟體。
   - □ 系統管理員帳戶標準，例如，重新命名或停用帳戶以及設立虛擬帳戶。

5. 定義安全性修補程式之強制方式及相關的時間表。若缺點仍無法在要求的時間之內成功解決，須採用更強烈的策略，例如：在違規者的組織中呈報這個問題、停用存取此電腦的主帳戶、在網路裡移除此電腦的網路實體連線，或是重新設定網路硬體

以達到相同的效果。

4.3.2. 企業安全性修補程式之系統架構

1. 高階設計（high-level design）：

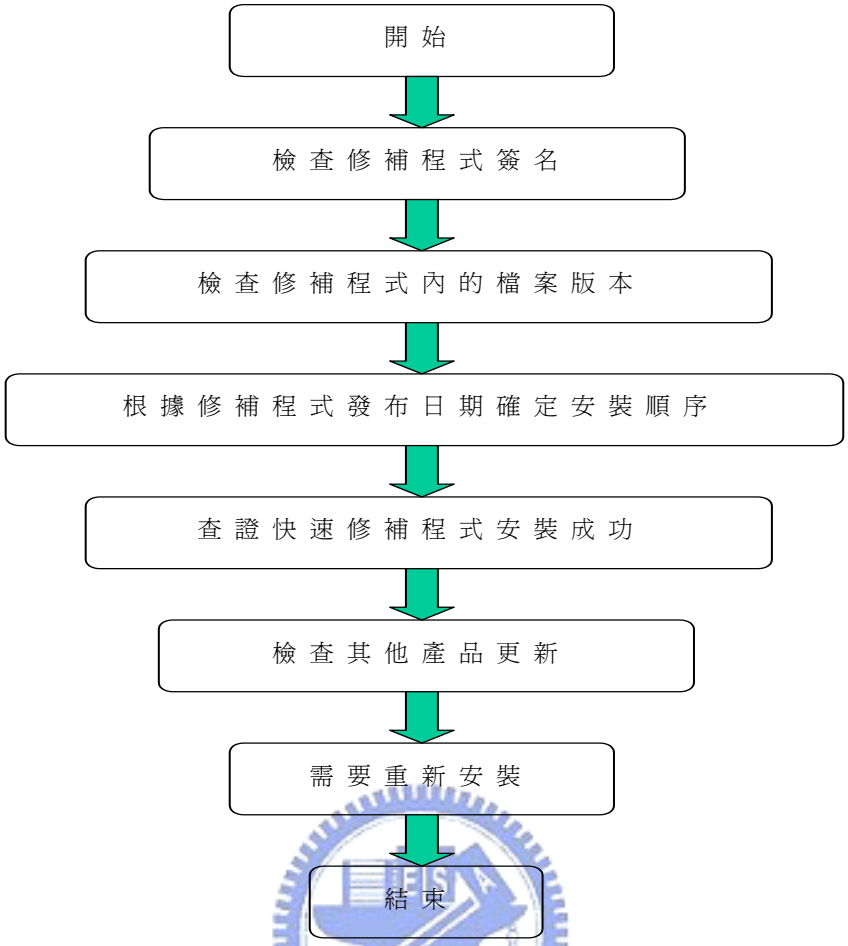
2002 年 2 月，資訊技術安全評估共同準則(Common Criteria for Information Technology Security Evaluation，簡稱 CC)公布缺點修補之評估方法增列（Supplement）。共同準則定義的缺點修補安全保證之目的在於要求發展者追蹤與更正所發現的安全缺點，包括配發缺點更正措施之需求。缺點修補程序宜描述所遇到的型式缺點處理之方法，某些缺點可能是無法立即可修復的，可能有無法修復之缺點而必須採取諸如程序的措施之情況。缺點修補程序，包括提供修補解法（Fix）予運作場所及提供缺點修補解法延遲時，在過渡期間該做什麼的資訊或當修補解決是不可能時該如何處理之資訊。

資訊技術安全評估共同準則將資訊產品/系統之缺點修補程序的要求如表 4.2 所示，共同準則評估員於確認受驗之產品與系統所提供之資訊符合表中不同階層的證據之內容和表現的所有需求後，方能建議於產品與系統之共同準則證書上註明其通過缺點修補的驗證。換言之，資訊產品/系統之缺點修補於資訊安全管理系統中之控制措施宜有不同的要求，於等級 1 時宜增加缺點修補衍生新缺點之控制措施，等級 3 須建立如圖 4.3~圖 4.5 所示的「缺點修補管理系統」以提昇成效。

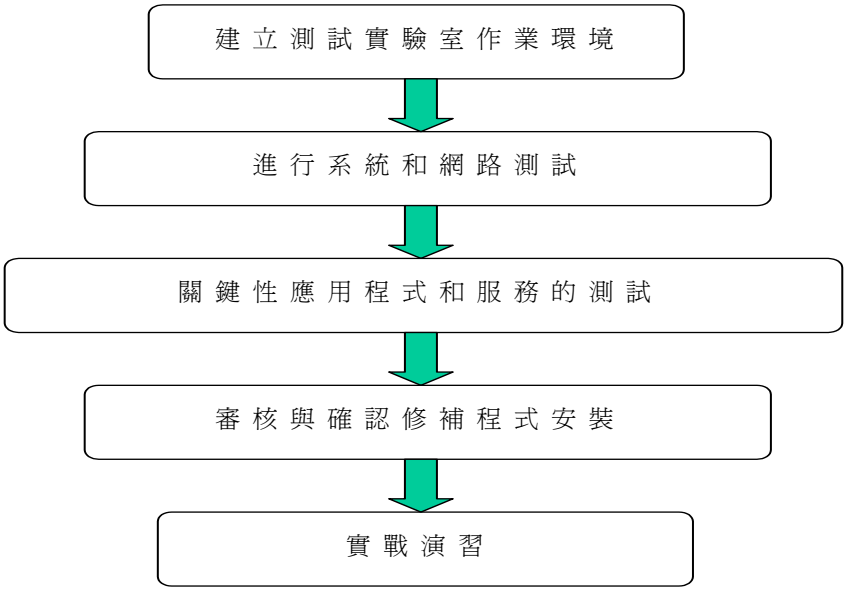
▼表 4.2：共同準則要求之缺點修補程序的證據內容和表現元件

等級 1	1. 缺點修補程序文件應描述用來追蹤在每一版本 TOE 所有報告的安全缺點的程序。 2. 缺點修補程序應需要提供描述每一安全缺點的本質和效應，以及發現校正的狀態到有缺點。 3. 缺點修補程序應需要針對每一安全缺點識別更正措施。 4. 缺點修補程序文件應描述用來為更正動作提供 TOE 使用者缺點資訊、更正措施和指引的方法。
等級 2	等級 1 之所有證據內容和表現元件再加上： 5. 處理所報告之安全缺點的程序，應確保改正任何已報告的缺點，並發出更正措施予 TOE 使用者。 6. 處理所報告之安全缺點的程序，應提供對這些安全缺點的任何更正措施不衍生任何新缺點之安全警衛。
等級 3	等級 2 之所有證據內容和表現元件再加上： 7. 缺點修補程序應包括程序需要自動分配安全缺點報告的及時回應，和已登記而可能受缺點影響的使用者的相關更正措施。

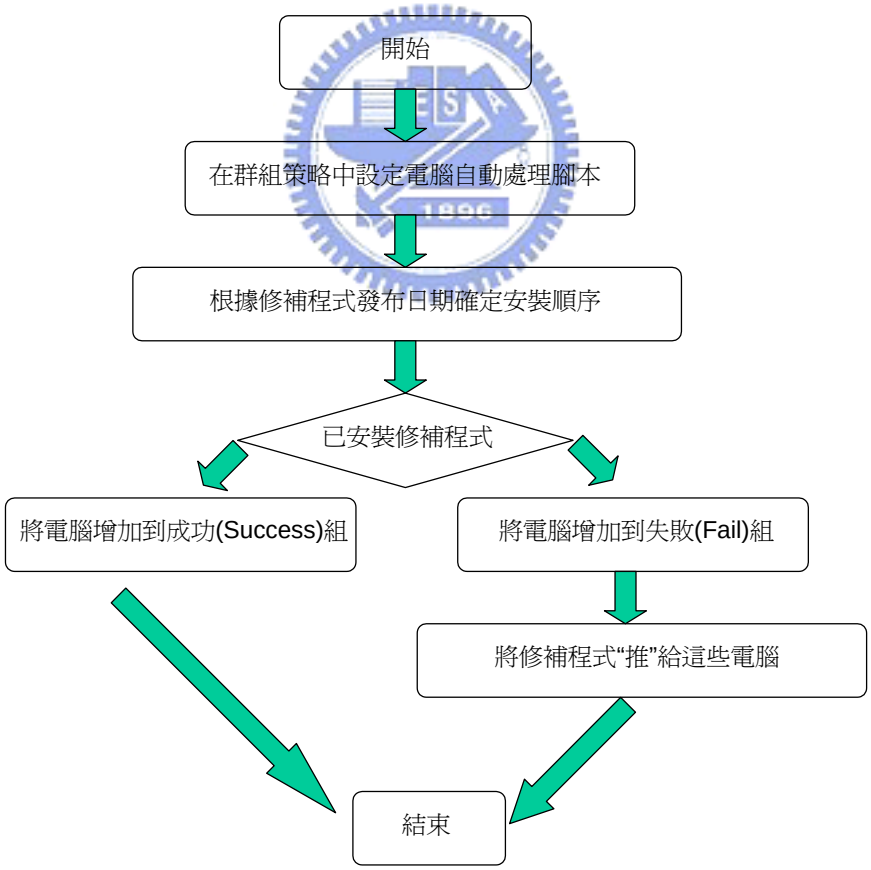
資料來源：本研究整理



▲圖 4.3：資訊系統組態管理流程設計－以修補程式安裝為例（一）



▲圖 4.4：資訊系統組態管理流程設計－以修補程式安裝為例（二）



▲圖 4.5：資訊系統組態管理流程設計－以修補程式安裝為例（三）

以下詳細說明各流程及系統設計方式。

2. 企業安全性修補程式部署時間範圍：

當確認要部署的重要補充程式時，識別環境中最容易受弱點影響的資源，以及在其中哪些是影響環境正常作業的重要資源，是非常重要的步驟。Microsoft 安全性回應中心 (Microsoft Security Response Center，簡稱 MSRC) 會在其發行的安全性佈告欄中提供了弱點的等級，以協助企業針對本身的特定情況，決定要套用哪些補充程式，或是需要多快採取行動。如表 4.3 所示是該企業依弱點安全性層級經過重新設計的電腦安全性修補程式之部署時間範圍。

- 重大、重要層級：由於該企業之基礎架構包含辦公區、機台用途設備與多種作業系統使得測試環境較為複雜，且考慮多部電腦部署修補程式時將使網路效能降低，進而對整個環境的正常作業造成負面影響。新架構宜優先採取網路存取監控措施，對於異常電腦進行監控並於必要時予以隔離；並在不影響整個環境的正常作業下於 1 個月內完成修補程式部署。
- 中度、輕微層級：根據可用性而定，在 1 年之內部署新的服務套件，或是更新包含了此弱點修復程式的積存，或是選擇完全不要部署。

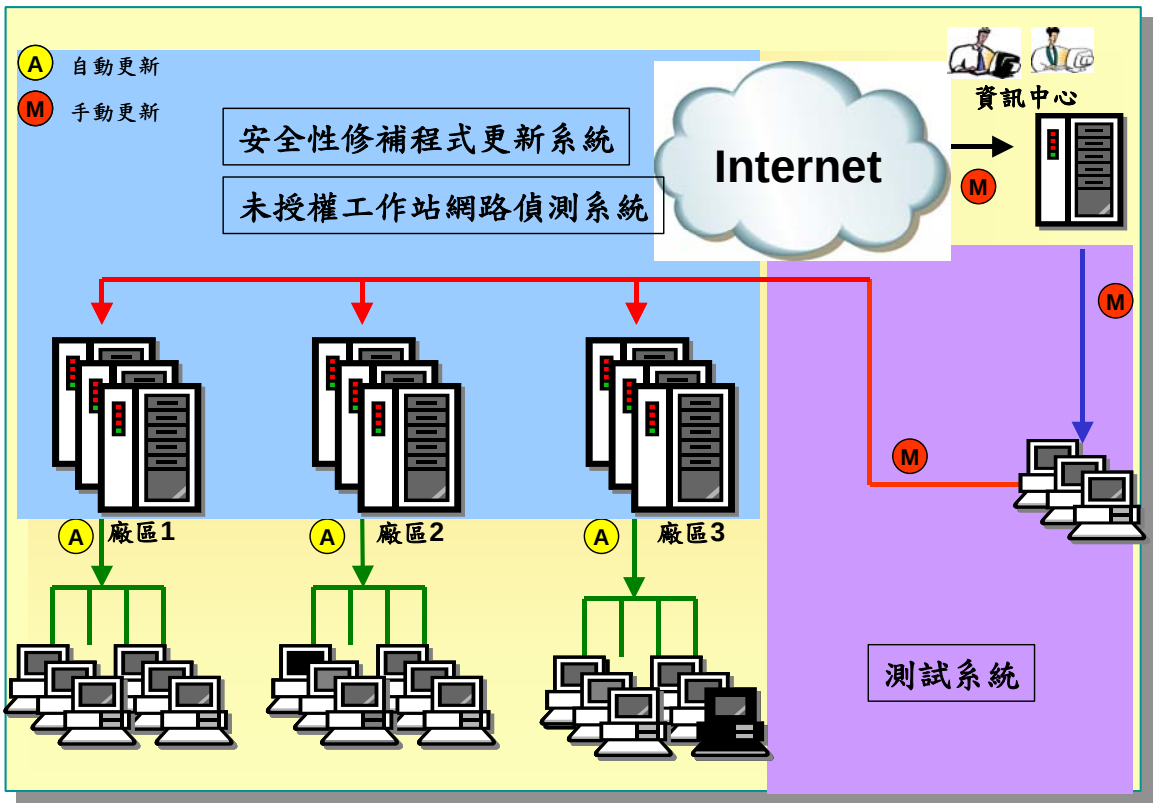
▼表 4.3：企業安全性缺點回應策略

弱點安全性層級	定義	Microsoft 安全性回應中心建議修補程式部署時間範圍	企業安全性缺點回應策略
重大	可被利用來不透過使用者的動作，即可傳播網際網路蠕蟲的弱點。	2 個星期內	優先採取網路存取監控措施，並於1 個月內完成修補程式部署。
重要	可能導致危害使用者資料機密性、整體性或可用性，或程序資源整體性或可用性的弱點。	2 個月內	優先採取網路存取監控措施，並於1 個月內完成修補程式部署。
中度	因為預設組態、稽核或難以利用等因素而顯著減少被利用的機會。	在 6 個月內部署軟體更新	根據可用性而定
輕微	非常難以利用，或影響極小的弱點。	在 1 年內部署軟體更新，或是選擇完全不要部署。	根據可用性而定

資料來源：本研究整理

3. 工作站端更新電腦安全性修補程式系統架構：

如圖 4.6 所示是該企業經過重新設計的工作站端更新電腦安全性修補程式之系統架構。該架構分為三個系統：測試系統、安全性修補程式更新系統、未授權工作站網路偵測系統。第一個系統是測試系統，管理者使用此系統來驗證網際網路所取得之安全性修補程式；第二個系統是安全性修補程式更新系統，管理者將經過驗證之安全性修補程式利用此系統完成工作站端之程式部署；第三個系統是未授權工作站網路偵測系統，對於不受管理或是非標準網域的電腦，利用此系統移除此工作站的網路連線。



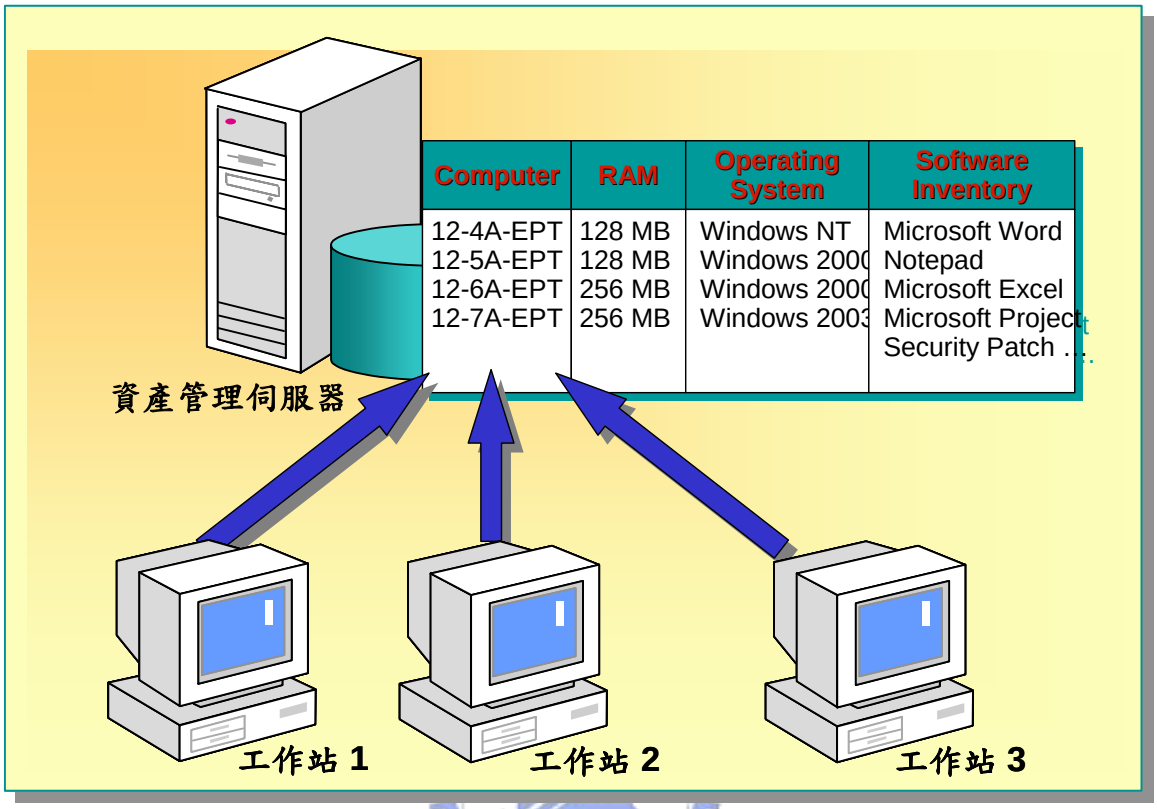
▲圖 4.6：工作站端更新電腦安全性修補程式系統架構圖

以下詳細說明各系統元件及系統運作方式。

- 測試系統
  1. 訂閱安全性警訊及其他資訊來源，安全性佈告欄會識別新的產品缺點、過去佈告欄的重要更新，以及已被其他人發現的新病毒。
  2. 仔細地檢閱補充程式，但不需要立即決定是否必須將之部署到環境中。因為有如此多種不同種類的軟體會使用如此多種的修補程式，當確定已徹底分析所有修補程式與環境之間的關聯性，才下載任何相關的檔案測試。
  3. 將檔案隔離於生產環境網路之外，以便確保這些檔案不會對組織的 IT 基礎架構造成負面的影響。
- 安全性修補程式更新系統
  1. 個人電腦代理程式：為安裝於各被控電腦之程式，依管理功能區分為「資產管理代理程式」、「軟體派送代理程式」。
     - 資產管理代理程式：根據管理者所訂定之資產收集項目及時程執行收集作業，並將資產回報至資產管理伺服器。
     - 軟體派送代理程式：當接收到安裝任務時，軟體派送代理程式根據管理者之設定開始安裝，並將安裝結果回報資軟體派送伺服器。
  2. 資產管理模組：如圖 4.7 所示建立企業整體資產管理中心，在這裡集中所有資產資訊，使得管理者可以匯總企業內所有資產設備及軟體等資訊。此種集中收集作業是透過代理程式來完成，代理程式根據管理者之設定時程將各廠區內之資產資料複製回來。當發現硬體遭變更時，根據事先所定義之機制，送出警訊或訊息至企業資訊中心來通知管理者。
     - 透過自動化資產管理的機制，收集所有電腦設備資產的清單（Hardware：CPU 數量、速度，RAM、Disk、網路卡數量及類型。Software：OS，Application），並針對資產生命週期進行更有效的管

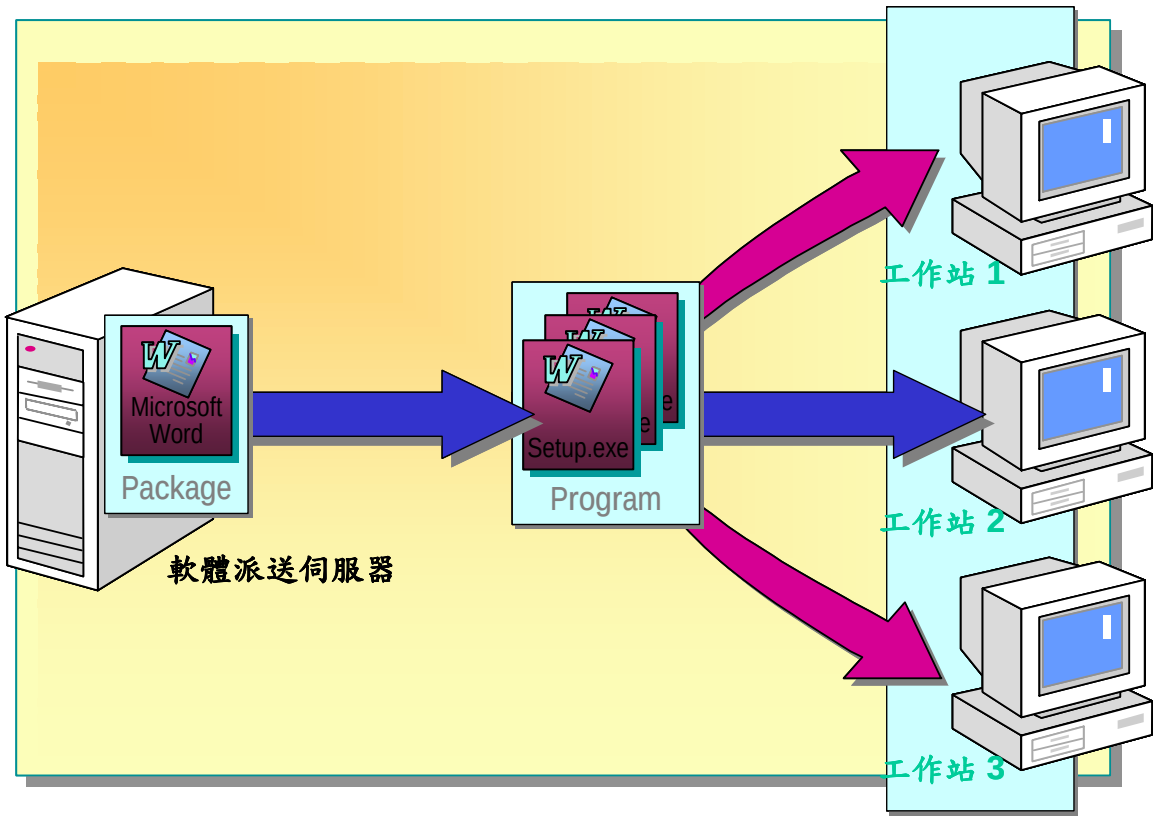
理。

- 將資產管理定義 Policy 或是 Query 條件所產生的群組與軟體派送整合。



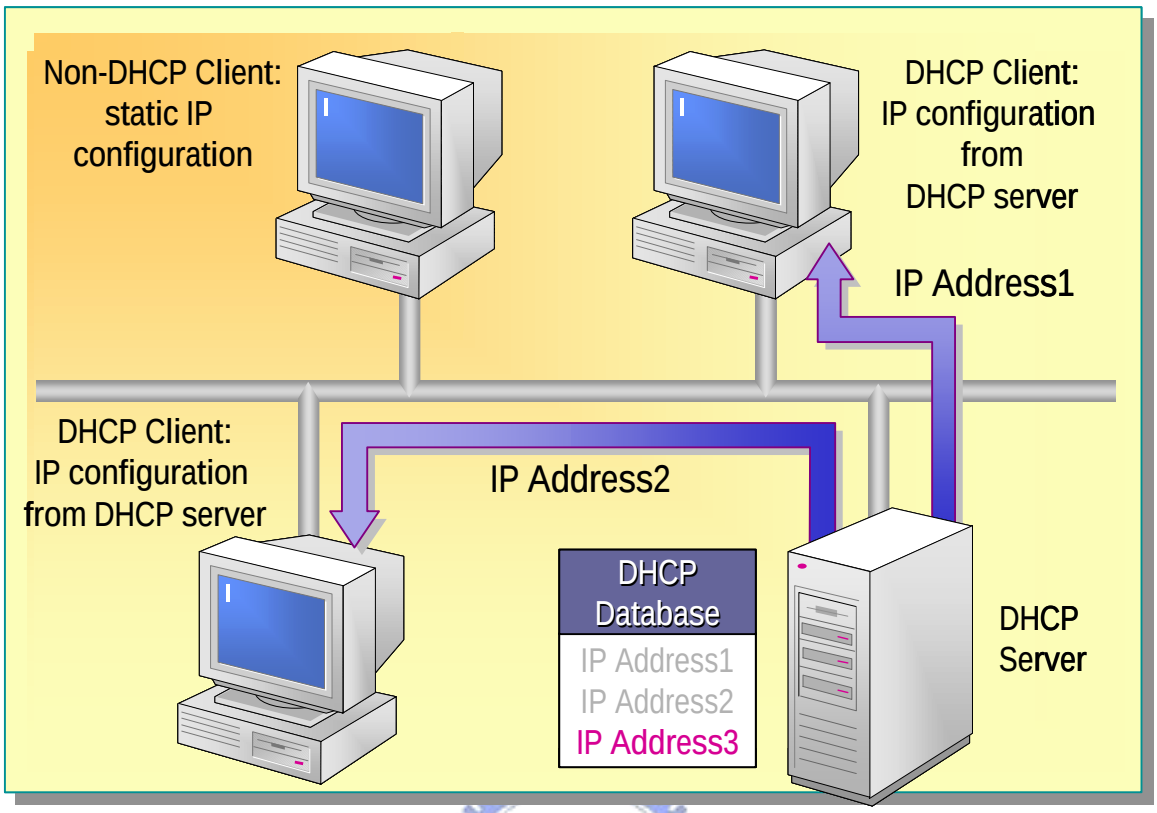
▲圖 4.7：安全性修補程式更新系統之資產管理模組

3. 軟體派送模組：如圖 4.8 所示建立企業整體軟體派送管理中心，管理者維護一共同之程式庫，減少軟體重複包裝，也可以透過管理介面，當軟體的派送成功或失敗時，會送出警訊或或訊息至至企業資訊中心來通知管理者。
   - 透過軟體自動派送的機制，配合自動化資產管理，快速篩選出需要安裝軟體的電腦，利用群組的方式，即可在短時期間內快速有效將軟體安裝成功。
   - 設定派送時程並可於設定之時間執行自動安裝或設定不同階段之安裝。以及保存並維護一個被安裝軟體相關資料之中央記錄檔。



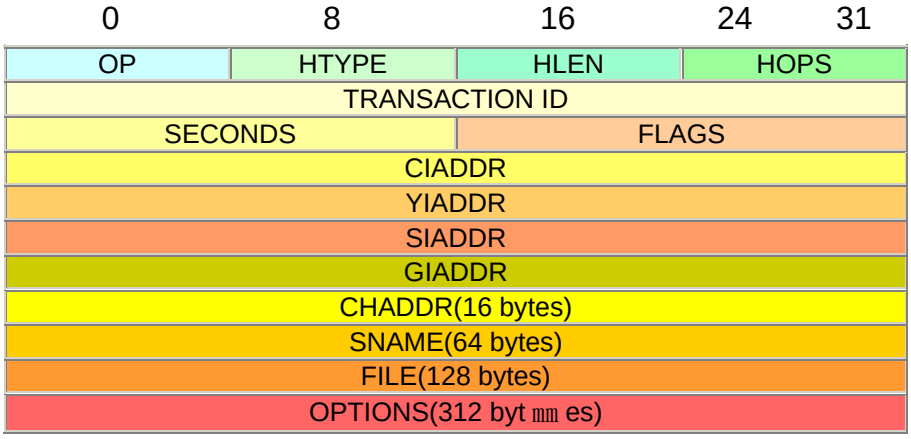
▲圖 4.8：安全性修補程式更新系統之軟體派送模組

- 未授權工作站網路偵測系統
  1. 動態主機設定協定（DHCP）模組：大型企業因為工作站的數量眾多，為了減少網管人員的負擔均會使用 DHCP 以靈活 IP 位址的使用。DHCP 全名是動態主機規劃配置協定（Dynamic Host Configuration Protocol），如圖 4.9 所示它的主要功能是讓工作站能夠透過自己的 Ethernet Address 廣播，向 DHCP 伺服器取得有關 IP 位址、Netmask、Default gateway、DNS…等設定。
     - 當 DHCP 用戶端第一次登錄網路的時候（本機上沒有任何 IP 資料設定），它會向網路發出一個 DHCPDISCOVER 封包。因為用戶端還不知道自己屬於哪一個網路，所以封包的來源位址會為 0.0.0.0 ，而目的位址則為 255.255.255.255 ，然後再附上 DHCPDISCOVER 的信息，向網路進行廣播。
     - 由於用戶端在開始的時候還沒有 IP 位址，所以在 DHCPDISCOVER 封包內會帶有其 MAC 位址訊息，並且有一個 XID 編號來辨別該封包，DHCP 伺服器回應的 DHCPOFFER 封包則會根據這些資料傳遞給要求租約的工作站。根據伺服器端的設定，DHCPOFFER 封包會包含一個租約期限的訊息。
     - DHCP 伺服器會保留一段 IP 範圍,當 DHCP 伺服器聽到網路上有 DHCP 用戶發出廣播時，伺服器就從該段 IP 範圍中挑一個還沒有使用的 IP，並在資料庫中找有關的相關設定值，將其回傳給這個工作站。
     - 如果用戶端收到網路上多台 DHCP 伺服器的回應，只會挑選其中一個 DHCPOFFER 而已（通常是最先抵達的那個），並且會向網路發送一個 DHCPREQUEST 廣播封包，告訴所有 DHCP 伺服器它將指定接受哪一台伺服器提供的 IP 位址。



▲圖 4.9：DHCP 運作原理

2. 認證模組：DHCP 用戶端除了接受 DHCP 伺服器的 OFFER，可以用 DHCPREQUEST 向伺服器提出 DHCP 選擇，如圖 4.10~圖 4.11 所示這些選擇會以不同的號碼填寫在 DHCP Option Field 裡面。
   - □ 當 DHCP 用戶端第一次登錄網路的時候會向網路發出一個 DHCPDISCOVER 封包向網路進行廣播。在 DHCPDISCOVER 封包內會帶有其 MAC 位址訊息，以及在 DHCP Option Field 會帶有主機名稱（Host Name）的識別訊息。
   - □ 如圖 4.12~圖 4.13 所示當認證伺服器收到 DHCP 用戶端所發出的 DHCPDISCOVER 網路廣播封包時，判斷 MAC 與 Host Name 與註冊資訊是否相同，如果相同則視為已授權工作站並由 DHCP 伺服器將 IP 與有關的相關設定值回傳給這個工作站。
   - □ 若 MAC 與 Host Name 與註冊資訊並不相同則視為未授權工作站，如圖 4.14 所示先提示該工作站警告訊息，並由認證伺服器將 MAC 位址訊息傳送至網路設備並採取移除此工作站的網路連線方式來阻絕風險。

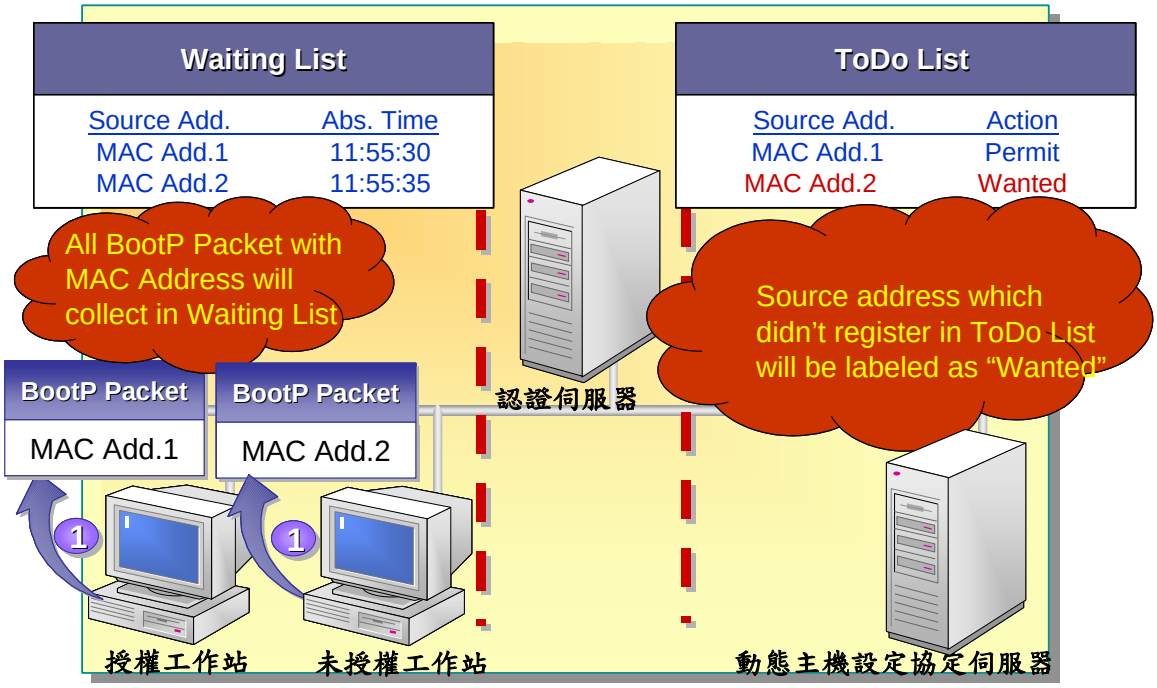


Op Code (OP)	若是 1，表示這個 Packet 是從 Client 送出的 Request (BOOTREQUEST)，若為 2，表示此 Packet 是由 DHCP Server 回應 (BOOTREPLY)
HTYPE	硬體類別，Ethernet 為 1
HLEN	硬體位址長度， Ethernet 為 6
HOPS	若封包需經過 router 傳送，每站加 1 ，若在同一網內，為 0
TRANSACTION ID	DHCPREQUEST 時產生的數值，以作 DHCPREPLY 時的依據
SECONDS	Client 端啟動時間(秒)
FLAGS	從 0 到 15 共 16 bits ，最左一 bit 為 1 時表示 server 將以廣播方式傳送封包給 client ，其餘尚未使用
CIADDR	要是 client 端想繼續使用之前取得之 IP 位址，則列於這裡
YIADDR	從 server 送回 client 之 DHCPOFFER 與 DHCPACK 封包中，此欄填寫分配給 client 的 IP 位址
SIADDR	若 client 需要透過網路開機，從 server 送出之 DHCPOFFER、DHCPACK、DHCPNACK 封包中，此欄填寫開機程式碼所在 server 之位址
GIADDR	若需跨網域進行 DHCP 發放，此欄為 relay agent 的位址，否則為 0
CHADDR	Client 之硬體位址
SNAME	Server 之名稱字串，以 0x00 結尾。
FILE	若 client 需要透過網路開機，此欄將指出開機程式名稱，稍後以 TFTP 傳送
OPTIONS	允許廠商定議選項(Vendor-Specific Area)，以提供更多的設定資訊(如：Netmask、Gateway、DNS、等等)。其長度可變，同時可攜帶多個選項，每一選項之第一個 byte 為資訊代碼，其後一個 byte 為該項資料長度，最後為項目內容

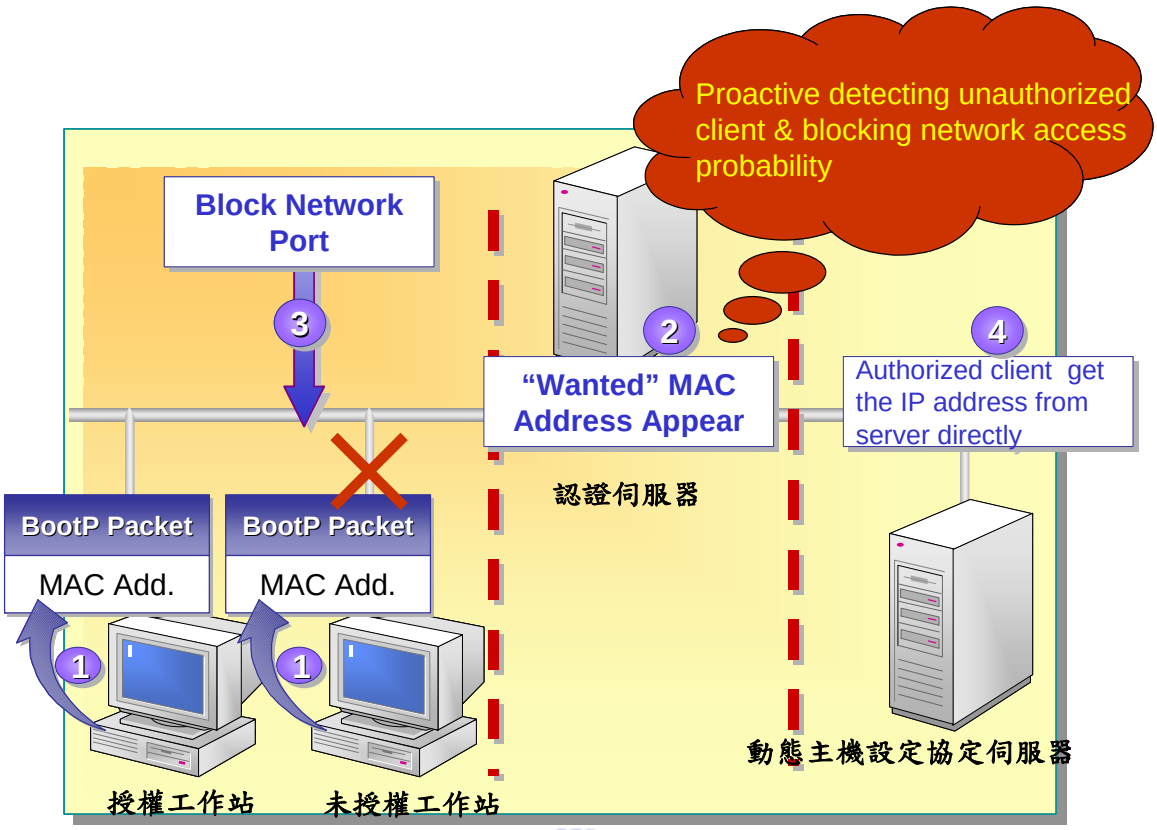
▲圖 4.10：RFC 2131 DHCP Message 封包格式與各欄位的意義

```
 Code   Len                    Host Name
+-----+-----+-----+-----+-----+-----+-----+-----+--
|  12 |  n  |  h1 |  h2 |  h3 |  h4 |  h5 |  h6 |  ...
+-----+-----+-----+-----+-----+-----+-----+-----+--
```

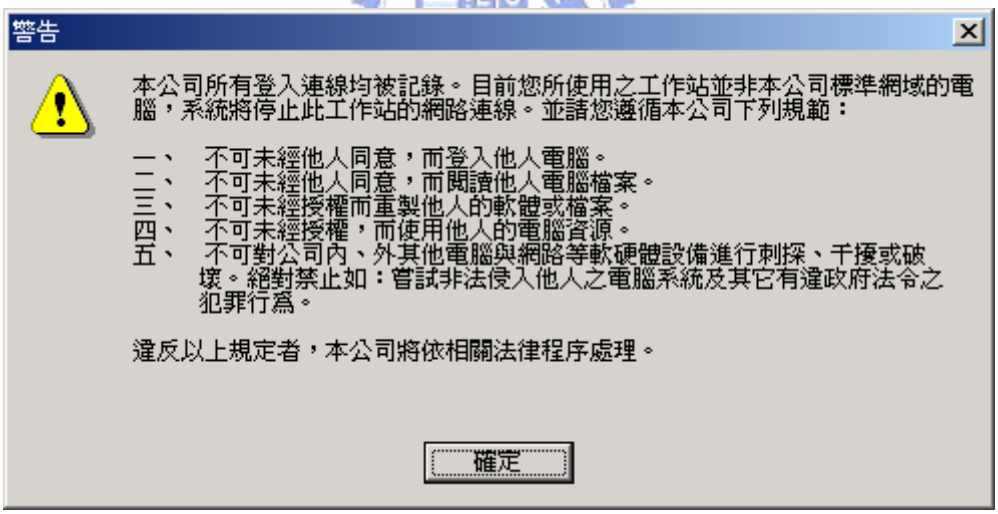
▲圖 4.11：RFC 1533 DHCP Option



▲圖 4.12：未授權工作站網路偵測原理之一



▲圖 4.13：未授權工作站網路偵測原理之二



▲圖 4.14：對未授權工作站之警告訊息

4. 伺服器端更新電腦安全性修補程式系統架構：

如圖 4.15 所示是該企業經過重新設計的伺服器端更新電腦安全性修補程式系統架構。該架構分為兩個系統：測試系統、安全性修補程式更新系統。第一個系統是測試系統，管理者使用此系統來驗證網際網路所取得之安全性修補程式；第二個系統是安全性修補程式更新系統，管理者將經過驗證之安全性修補程式利用此系統完成伺服器端之程式部署。

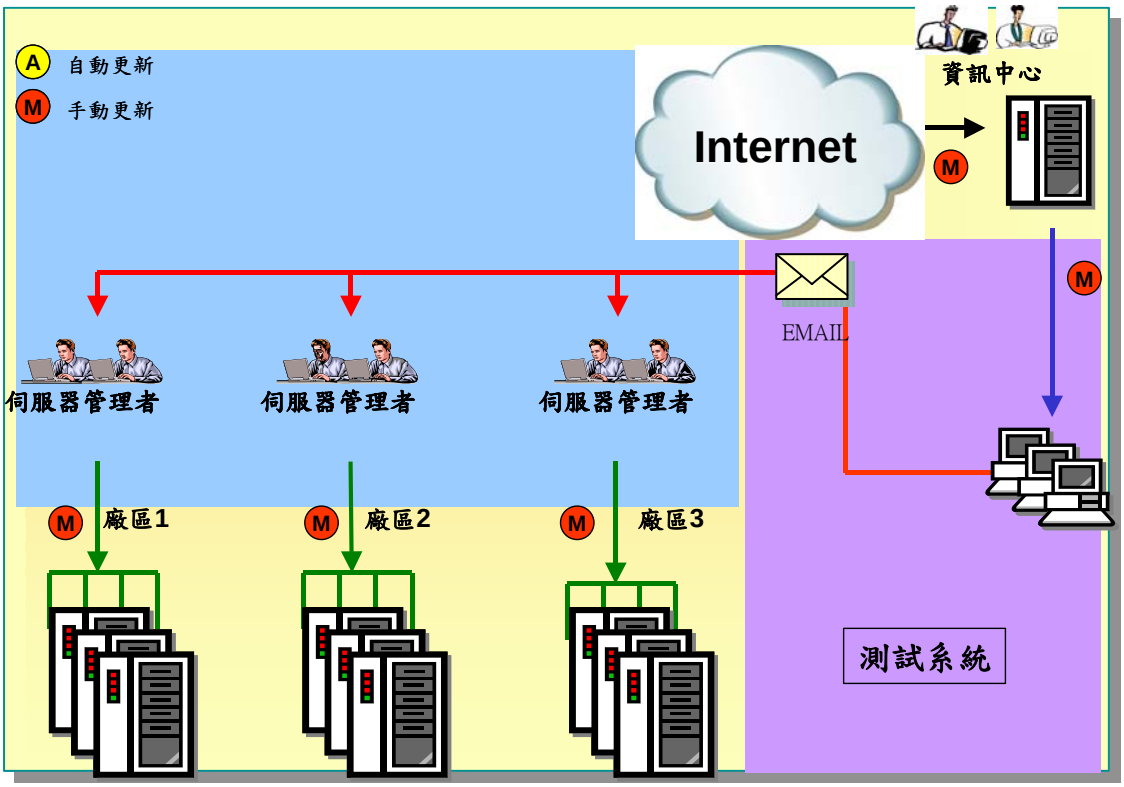
以下說明各系統元件及系統運作方式。

□ 測試系統

1. 訂閱安全性警訊及其他資訊來源，安全性佈告欄會識別新的產品缺點、過去佈告欄的重要更新，以及已被其他人發現的新病毒。
2. 仔細地檢閱補充程式，但不需要立即決定是否必須將之部署到環境中。因為有如此多種不同種類的軟體會使用如此多種的補充程式，當確定已徹底分析所有補充程式與環境之間的關聯性，才下載任何相關的檔案測試。
3. 將檔案隔離於生產環境網路之外，以便確保這些檔案不會對組織的 IT 基礎架構造成負面的影響。

□ 安全性修補程式更新系統

1. 經資訊中心人員確認所有修補程式與環境之間的關聯性並完成隔離測試後，經由訊息系統主動通知伺服器管理者下載修補程式進行個別伺服器端之手動程式部署。
2. 伺服器管理者於完成修補程式之部署後主動回覆資訊中心。資訊中心並且負責伺服器管理者未回報時之追蹤管理。



▲圖 4.15：伺服器端更新電腦安全性修補程式系統架構圖

4.3.2 成效評估

如圖 4.6~圖 4.15 所示的企業安全性修補程式架構之實作後，如表 4.4 所示經實際伺服器進行測試，原伺服器安全性修補程式更新成功率為 85%，改以新架構後安全性修補程式更新成功率為 99%（提昇 14%）。在工作站完成安全性修補程式更新時間方面，如表 4.5 所示從 1394 人/天減少為 32 人/天。

▼表 4.4：改善後伺服器電腦安全性修補程式更新效益評估表

安全性修補程式	數量	更新數量(先前)	成功比例	更新數量(之後)	成功比例
MS03-026/007	1,200	1,014	84.5%	1,194	99.5%
MS03-039	1,200	1,022	85.2%	1,180	98.3%
MS03-041~44	1,200	1,034	86.2%	1,190	99.2%
MS04-040	1,200	1,017	84.8%	1,180	98.3%
MS04-011	1,200	1008	84.0%	1189	99.1%
MS04-022	1,200	1,022	85.2%	1,193	99.4%
MS04-023	1,200	1,018	84.8%	1,196	99.7%
MS04-025	1,200	1,024	85.3%	1,190	99.2%

▼表 4.5：改善後工作站電腦安全性修補程式更新效益評估表

安全性修補程式	數量	先前更新作業時間(人/天)	自動部署作業完成時間(人/天)	節省部署作業時間(人/天)
MS03-026/007	7,000	759	30	729
MS03-039	7,000	792	15	777
MS03-041~44	8,000	865	10	855
MS04-040	9,800	1078	15	1063
MS04-011	10,108	1138	25	1113
MS04-022	9,600	1069	10	1059
MS04-023	9,700	839	12	827
MS04-025	12,269	1394	32	1362

計算方式說明：

1. 人/天＝總時間/60（分鐘）/8（每日工時）。
2. 預估檢查作業完成時間(人/天)=每一台工作站檢查時間(15 分鐘)x數量/60/8。
3. 預估部署作業完成時間（人/天）＝每一台工作站部署時間（0.5 小時）x數量/60/8。
4. 修補程式更新作業時間（人/天）＝預估檢查作業完成時間（人/天）＋預估部署作業完成時間（人/天）。

資料來源：本研究整理

從表 4.4 與表 4.5 可知此企業安全性修補程式架構設計能大幅提昇對抗惡意軟體的控制措施之有效性。

第五章 研究結論與建議

5.1.研究結論

電腦系統安全之演進至今已經有三十幾年以上的歷史且獲得長足之進步。儘管如此，在數以萬計的電腦系統當中安全性仍意味著這是件麻煩的事。有心人與駭客可以輕易竊取或破壞大部份系統上的有用資訊，甚至於在一次的行動中可以攻擊數以萬計的系統。在網際網路盛行之後使得電腦安全的防護愈來愈困難，約在二十年前只有少數的人使用電腦，而今，全世界約有五億人口連結網際網路，任何人來自於任何地方都可能因此對安全造成影響。許多組織仰賴 IT 資源，並且相信它們是可靠的，一旦公司資產的安全性受到危害而導致災難性後果，數天停機所帶來的損失將會難以估算，並且因為公司的安全性缺口，以及其所導致的信用、客戶、夥伴喪失，將使組織本身面臨相當大的險境。

本論文提出以國際上已標準化之方式來評估企業資訊安全防護能力與改善方案，其成果如下：

1. 評估資訊安全之防護能力可確立企業資訊安全發展方向：

   網路安全問題會隨著時間變得更加錯綜複雜，影響也將會不斷擴大，但是企業對於資訊科技的投資卻逐漸走緩而形成強大的對比。「知己知彼，百戰不殆」，企業利用評估資訊安全之防護能力，一方面可以瞭解自身「罩門」之所在，亦可當作企業資源分配上之參考依據。

2. 資訊產品/系統安全性修補程式管理系統能可提昇對抗惡意軟體的控制措施之有效性：

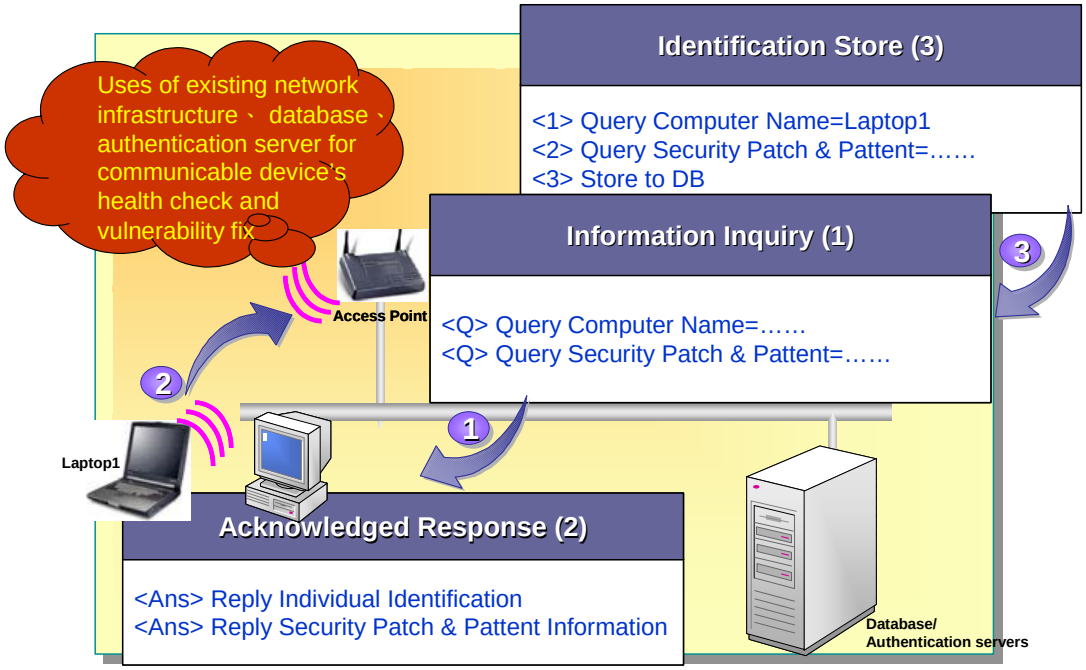
   弱點攻擊技術日新月異防不勝防，而防範之道必須建立滴水不漏的基礎架構之上。資訊產品/系統安全性修補程式管理系統可以緩和系統因為安全性修補程式尚未更新完成前就已經遭受攻擊的問題，藉由實例規劃亦驗證改善方法之可行性，進而產生之明顯之效益改善。

5.2.後續研究建議

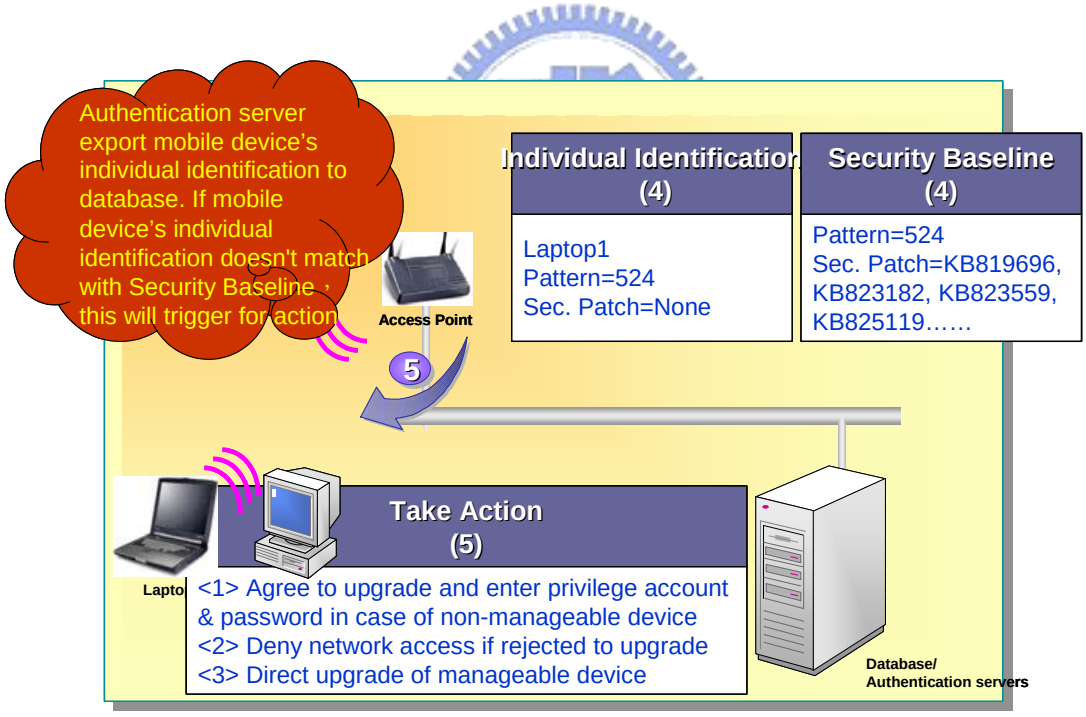
CNS 17799（ISO/IEC 17799）資訊安全管理之作業要點，已是資訊安全管理廣為接受之最佳實務與指引廣為接受的標準，原作業要點中所不足之諸如「資訊產品/系統缺點修補作業」與「技術脆弱性控制」等控制措施【17~25】亦在新版 ISO/IEC FDIS 17799:2005(E)中增列。在未來的研究上，筆者認為由於電腦的普及和網路的持續快速發展，使用資訊科技必將成為日常生活的一部份且未經授權存取與病毒感染所造成之危害勢必更加頻繁，如何減少使用者與管理者之操作負擔是維持控制措施有效性之最佳途徑。以下是對於後續研究者之建議：

- 未授權工作站自動化缺點修補作業：

  訪客、行動和遠端使用者，對於企業來說這些用戶端是潛在的攻擊來源，除此之外某些獨立電腦或不受控制的非網域成員電腦由於沒有這些不受管理用戶端的本機系統管理員權限，故難以收集電腦名稱及 IP 位址之外的系統資訊並用以識別完成安全性修補程式需要。本研究對於不受管理或是非標準網域的電腦，僅採取移除此工作站的網路連線方式來阻絕風險。因此如圖 5.1~5.2 所示，亦可設計一種針對未授權工作站自動化缺點修補作業方法及系統以主動完成缺點修補作業。



▲圖 5.1：未授權工作站自動化缺點修補作業原理之一



▲圖 5.2：未授權工作站自動化缺點修補作業原理之二

參考文獻

【1】 Robert D. Austin; Christopher A.R. Darby, "The Myth of Secure Computing", Harvard Business Review, June 1, 2003.

【2】 Nicholas G. Carr, "IT Doesn't Matter", Harvard Business Review, May 1, 2003.

【3】 洪國興、趙榮耀（2002）資訊安全管理理論之探討，資管評論，第 12 期，頁 17~47。

【4】 樊國楨、徐鈺宗（2003）數位社會資訊安全管理系統驗證規範初探，資訊安全論壇，第 10 期，頁 39-50。

【5】 林禎吉、賴溪松（2000）資訊安全國際標準制定之現況，網路通訊，第 111 期，頁 90~97。

【6】 ISO, Banking- Approved algorisms for message authentication- Part 1: DEA, ISO 8731-1:1987(E), ISO, 1987.

【7】 ISO, Banking –Approved algorithms for message authentication- Part 2: Message authenticator algorithm, ISO 8731-2: 1987(E), ISO, 1987.

【8】 馬正維，資訊安全國家標準之研訂現況，資訊安全通訊，第四卷，第四期，頁 19~28，1998。

【9】 http://www.nicst.nat.gov.tw (2004 年 11 月 21 日)。

【10】http://www.icst.org.tw (2004 年 11 月 21 日)。

【11】國家資通安全會報技術服務中心（2002）2001 年資通安全報告書，2001 年 12 月。

【12】行政院國家資通安全會報技術服務中心（2002）九十一年執行成果彙編，2002 年 12 月。

【13】行政院國家資通安全會報技術服務中心（2003）九十二年執行成果彙編，2003 年 12 月。

【14】行政院國家資通安全會報（2004）建立我國通資訊基礎建設安全機制計畫(九十四年至九十七年)，2004 年 3 月。

【15】戚難先（2003）我國資通安全的推手－建立我國通資訊基礎建設安全機制計畫，資安季刊，第 1 期，頁 4~10。

【16】ISO, Information technology – Code of practice for information security management, ISO/IEC 17799:2005-06-15, ISO, 2005。

【17】經濟部標準檢驗局（2002）資訊技術－資訊安全管理之作業要點，CNS17800。

【18】經濟部標準檢驗局（2002）資訊技術－資訊安全管理之作業要點，CNS17900。

【19】Microsoft Corp.（2003）The Microsoft Guide to Security Patch Management，July 2003。

【20】Brykczynski, B. and R.A. Small（2003）Effective security patch management，IEEE Computer，Vol. 20，No.1，pp. 50 －57。

【21】British Standards Institution（2002）Information security management systems－Specification with guideance for use，BS 7799-2：2002。

【22】Plate, A（2004）Hot off the press－Revision of version of ISO/IEC 17799，ISMS Journal，Issue 5，pp. 2~3，Nov. 2004。

【23】Mell, P. and M. Tracy（2002）Procedures for Handling Security Patches－Recommendations of the National Institute of Standards and Technology（NIST），NIST Special Publication 800-40，NIST。

【24】ISO（2004）Information technology－Security techniques－Information security incident management，ISO/IEC：2004（E）。

【25】Kaplan, R. S. and D. P. Norton(1996)The Balanced Scorecard：Translating Strategy into Action，Harvard Business School Press。