

致理技術學院

資訊網路技術系 實務專題報告



資訊安全風險管理與評估

指導老師：柯振根

學生：陳慶龍(29434518)

余家榮(29434534)

陳錦儒(29434541)

翁仕誠(29434548)

陳穩在(29434553)

中華民國 96 年 1 月

致理技術學院

資訊網路技術系 實務專題報告

資訊安全風險管理與評估

學生：陳慶龍(29434518)

余家榮(29434534)

陳錦儒(29434541)

翁仕誠(29434548)

陳穩在(29434553)

本成果報告書經審查及口試合格特此證明。

指導老師：_____

評審委員：_____

評審委員：_____

評審委員：_____

中華民國 96 年 1 月

專題研究授權書

本授權書所授權之專題研究為_____

共_____人，在致理技術學院資訊網路技術系 _____學年度第_____學期完成資
網實務專題。

專題名稱：_____

同意 不同意

本組同學共_____人，皆同意著作財產權之論文全文資料，授予教育部指
定送繳之圖書館及本人畢業學校圖書館，為學術研究之目的以各種方法重製，
或為上述目的再授權他人以各種方法重製，

不限地域與時間，惟每人以一份為限。

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

指導教授姓名：

專題生簽名：

學號：

中華民國 _____年 _____月 _____日

致 謝

在這期間，我們不僅得到許多資訊安全上的專業知識，並發揮專業技能來製作本報告，要感謝各方的援助與支持，本報告得以完成，首先要以誠摯的心情感謝資網系系主任兼指導教授柯振根老師的教誨與指導，經由各種方式，知會我們注意報告報告的寫作方式以及報告實作的進度，由於老師不斷的督促與鼓勵，從報告的制訂、研究架構的建立以及在撰寫過程中，提供許多智慧的引導，使我們在研究資訊安全上更增進許多理論的基礎，並提供我們改進的方向與建議，使我們得以正確尋找出與本報告有關的資料與文章，讓本報告從不像專業人士所寫的，變成更有深度和專業的報告，使本報告更趨嚴謹。

我們衷心感謝其他幫助我們完成收集資料與提供解決方法的學生和老師，感謝幫助我們建置資料庫，並且說明我們應該如何建置資料庫的方法，使我們得以克服重重難關。

再來感謝學校圖書館中老師們留下的報告研究資料，因為有他們留下的資料，才能夠找到能配合我們各組員的能力就能夠做出的報告，使的我們才能找到報告的研究題目應該往哪一個方向進行。

最後感謝紐奧良文化事業股份有限公司發行的資安人雜誌，因為有他們所提供的專業專欄文章，本報告各資訊安全問題才得以迎刃而解。

摘 要

隨著資訊科技的發展，組織資訊資產也相對的更需嚴加保護，因而資訊安全成為業界不可乎視的一環。本專題報告的目的主要是了解何謂資訊安全、影響資訊安全的因素、資訊安全的風險，搜集並整理有關資訊安全的趨勢的資訊與發展重點，並探討英國國家標準局資訊安全標準範本 BS7799 規範與條文說明與資訊安全產品技術運用和評估標準，運用資訊安全範本設計應用資訊安全風險管理評估分析網站，本分析網站運用 3D Max 與 Flash 設計互動式按鈕與首頁登入畫面，並建立資訊安全資料庫，主要是分析組織內部是否符合資訊安全並提出相對的分析建議與風險指數圖以供參考，說明何謂 ITDR (IT Disaster Recovery) 災害復原計畫，及其重要性與規劃方式，在結論中說明了本報告資訊安全的重要性，及資訊安全分析網站的重要性，提出了對現今環境資訊安全的幾點建議與本報告未來研究的方向

關鍵詞：資訊安全、資訊安全規範 BS7799、ITDR 災害復原計畫

目 錄

授權書	I
致謝	II
摘要	III
目錄	IV
圖目錄	VI
表目錄	VIII
第壹章 緒論	1
第一節 資訊安全的重要性與發展演進	1
第二節 本報告的動機與目的	9
第三節 本報告範圍與架構	11
第貳章 資訊安全理論與技術	13
第一節 資訊安全定義	13
第二節 影響資訊安全的因素	15
第三節 資訊安全的風險	21
第四節 資訊安全的標準規範	28
第五節 資訊安全產品技術與評估標準	34
第六節 ITDR (IT Disaster Recovery) 災害復原計畫	46

第參章 資訊安全分析網站	60
第一節 資訊安全評估分析網站架構	60
第二節 資訊安全分析網站功能操作流程	64
第肆章 資訊安全分析網站呈現	86
第一節 資訊安全分析網站之各別分析畫面呈現	86
第二節 資訊安全分析網站之整體分析畫面呈現	90
第伍章 結論與建議	93
參考文獻	98
附錄一 資訊安全風險等級表	102
附錄二 文獻探討	105
附錄三 成果光碟	128

圖目錄

圖 1-1 本報告書基本架構概念圖	12
圖 2-1 風險分析、風險評估與風險管理關係圖	34
圖 2-2 我國資訊安全產品驗證體系架構	41
圖 2-3 我國共同準則評估驗證體系	43
圖 3-1 資訊安全評估分析網站架構圖	61
圖 3-2 資訊安全分析評估網站流程圖之安全性政策	64
圖 3-3 資訊安全分析評估網站流程圖之安全組織	66
圖 3-4 資訊安全分析評估網站流程圖之資產分類控制	68
圖 3-5 資訊安全分析評估網站流程圖之人員安全	70
圖 3-6 資訊安全分析評估網站流程圖之實體環境安全	72
圖 3-7 資訊安全分析評估網站流程圖之電腦網路管理	74
圖 3-8 資訊安全分析評估網站流程圖之系統存取控制	76
圖 3-9 資訊安全分析評估網站流程圖之系統開發維護	78
圖 3-10 資訊安全分析評估網站流程圖之業務持續運作	80
圖 3-11 資訊安全分析評估網站流程圖之稽核	82
圖 3-12 資訊安全分析評估網站流程圖之總體分析	84
圖 4-1 資訊安全分析評估網站首頁	86

圖 4-2	資訊安全十個類別(點選安全政策)-----	86
圖 4-3	資訊安全之安全政策相關分析內容-----	87
圖 4-4	資訊安全之安全政策分析結果暨風險等級-----	87
圖 4-5	資訊安全分析評估網站首頁-----	88
圖 4-6	資訊安全十個項目(點選安全組織)-----	88
圖 4-7	資訊安全之安全組織相關分析內容-----	89
圖 4-8	資訊安全之安全組織分析結果暨風險等級-----	89
圖 4-9	資訊安全分析評估網站首頁-----	90
圖 4-10	資訊安全十個項目-----	90
圖 4-11	資訊安全分析項目內容之一-----	91
圖 4-12	資訊安全整體分析暨整體風險等級(1)-----	91
圖 4-13	資訊安全整體分析暨整體風險等級(2)-----	92
圖 4-14	資訊安全整體分析暨整體風險等級(3)-----	92

表 目 錄

表 2-1 國內外對資訊安全的定義	14
表 2-1 國內外對資訊安全的定義(續)	15
表 2-2 影響資訊安全的自然與人為因素	16
表 2-3 影響資訊安全的因素	17



第壹章 緒論

第一節 資訊安全的重要性與發展演進

「資訊」(Information) 是企業的重要資產之一，對組織而言，是具有價值的，因此，必須適切的加以保護。「安全」(Security) 是指結合系統、運用及內部控制，來確保資料及作業程序的完整、真實及隱密。

由於資訊科技的快速進步，從 60 年代的集中式大型主機 (Central Mainframe Computers)，70 年代中期以後的個人電腦、部門運算 (Departmental Computing)、區域網路 (Local Area Networks)，到 90 年代的主從式 (Client-Server)、網際網路 (Internet)、企業內部網路 (Intranet) 與企業間網路 (Extranet) 等。資訊系統的使用者，從只限於組織內部的資訊技術人員的存取資訊設施 (Access Information Facilities)，漸漸增加到組織內部的非資訊技術人員，也需要存取資訊設施，進而再擴大到跨組織的電子交易，連接不同平台的資訊設施，使用者也隨之擴大到組織外部不特定的個人。隨著資訊新科技的快速發展，使用者範圍不斷擴大，組織為資訊系統依賴程度的提高，使得資訊安全面臨更大的挑戰。

換言之，資訊安全日漸重要，係由於資訊系統的環境大幅度的改變，在網際網路的環境中，隨時都有為數可觀來自世界各地的非授權使用者，可能去存取或變更組織的資訊，使組織的資訊面臨空前的威脅；因

此，資訊安全已是當今任何組織為達成有效管理的重要關鍵之一，資訊安全也成為每一個組織的核心業務之一。

層出不窮的各種災害，無孔不入的網路入侵與組織內部的人謀不藏等，不斷的在世界各地上演，確實使各界更加的重視資訊安全，但是現今資訊安全解決方案卻出現：片段而零散的安全功能、缺乏整合的對策、欠缺相互貫通的管理機制、資訊安全專業人才不足等現象 (Clyde,2002)，使得組織無不希望能藉助過去的研究，以作為制定資訊安全策略的參考，但似乎無法令人滿意，所顯示的現象是：(1)資訊安全技術面的研究多，管理面的研究少，更缺乏實證的研究；(2)縱然有少數涉及資訊安全管理的研究，也是片面者多，整體性者少，且像瞎子摸象一樣只摸到一小塊，缺乏較完整的圖像，究竟是其中的哪一塊？(3)實務界出現一些錯誤的觀念，例如：防火牆即是資訊安全，資訊安全只有技術的問題等等...不一而足；(4)直到 1995 年英國國家標準協會 (British Standards Institution, BSI) 制定 BS7799-1 「資訊安全管理實務準則」第一部分 (Information Security Management-Part1 : Code of Practice for Information Security Management)，始出現較完整的資訊安全管理架構。

資訊安全事故一再發生，資訊安全的議題也漸漸受到重視，但普遍存在的現象，是一般人對資訊安全有一些錯誤的觀念：

- (1)防火牆等於資訊安全。
- (2)防毒就是資訊安全。
- (3)SET 及 SSL 加密即是網路安全。
- (4)資訊安全是技術問題。
- (5)資訊安全事資訊部門的責任。
- (6)資訊安全的投資值得嗎？

事實上，防火牆與防毒軟體只是資訊安全的產品或工具之一，而 SET、SSL 是加密技術，只靠加密而未能有其他的網路管理措施及技術的配合，是很難確保資訊安全的。亦即，資訊安全產品本身的使用，並不能表示任何安全防護的效果，必須搭配適當的裝置、設定管理 (Configuration Management)、系統管理與監控稽核；而單憑某一項資訊安全技術的使用，恐難以達到安全保護的效果。資訊安全不僅僅是技術的問題，更是管理的問題，也是內部程序及控制的問題，若將資訊安全限定在技術問題，那是只見樹木，不見森林，以偏概全的偏失，事實上，是無任何一套產品可以為一個組織提供一個完全的安全防護。資訊安全事組織各個階層，所有員工的責任，不是某一單一部門的責任，更不僅僅是資訊部門的責任。資訊安全的投資不能單從有形的成本效益來考量，資訊安全事故所造成對組織的傷害，不只是有形財務上的損失，其

商譽、公司信譽，消費者的信任都會受到嚴重的打擊，甚至損害到企業的競爭能力，危及到組織的生存，因此，資訊安全是企業經營必要的條件，而不是值不值得投資的問題。整體而言，資訊安全需要機密性（Confidentiality）、完整性（Integrity）與可用性（Availability）三者同時考量（行政院研考會,2002）。

從以上這些錯誤觀念的觀察，真正的問題是對資訊安全的範疇不了解，對於究竟有哪些因素會導致組織的資訊安全受到危害，尚缺乏整體而周延的研究所致。對於資訊安全管理的文獻，大多偏重觀念的陳述，架構的建立，尚乏實證的研究，固然學者提出許許多多的程序與步驟，近年來國際標準在此方面有相當的成就，尤其 ISO/IEC17799 及 BS7799-2 公佈之後，為資訊安全管理提供了一個較完整的系統，但是系統中各個管理活動之間的關係，程序的發展，雖然在資訊安全管理的顧問服務受到廣泛的重視，但是尚未能從研究上獲得驗證。

在資訊技術快速的進步，資訊處理架構不斷創新的情況下，資訊安全威脅的型態也不斷變化，資訊安全的軟、硬體亦隨之有更新的技術、更好的產品；而企業的產業別不同，所處的環境不同，組織目標更是有極大的差異，因此，不可能所有的組織都採用完全相同的資訊安全技術，建構一個與技術無關（Technical Independent）的資訊安全管理系統

(Information Security Management System)，以適用於不同資訊技術之組織，而如何評估此一系統的有效可行。

無論從學術研究的角度來看或實務面觀察，組織都需要有資訊安全管理的評估模式，使組織可以檢視其資訊安全的防禦能力，及為資訊安全的策略管理提供一個可以參考的模式，這樣的評估模式相信是資訊安全的學術研究所要努力的方向，也是實務界所期盼的，當然資訊安全評估模式的建立是極度困難的工程，但總是要踏出困難的第一步，未來才能在現有的基礎上修正、發展，始能建構可以長可久的評估模式。

資訊安全今日存在著內憂外患的亂象和危機，情報長期失竊的情況點出資訊安全的重大缺失。駭客和維護資訊安全的工程師皆擴大範圍，將焦點轉向消費者產品，如資訊安全軟體和管理服務軟體等。為因應此一趨勢，業界無不儘速加強內部控管；資訊安全軟體、漏洞管理產品、以及附有異常偵測功能的資訊安全應用軟體，則擔起此一重責大任來補其不足。

今年十大趨勢

(1)內部與外來入侵者將會修補受攻擊網站的安全漏洞。如此一來，不僅可使資訊科技公司湯下戒心，亦可防止其他駭客攻擊此網路，因為攻擊者的目標在於長期竊取情報。附有異常偵測功能得資訊安全應用軟

體將會是針對解決此問題的方案之一。

(2)攻擊者將利用已安裝的間諜軟體和其他惡性程式碼的漏洞。惡性程式碼 (malicious code) 為自行散播病毒的程式碼，而攻擊者每年釋出數以百計的新版本，因此漏洞呈倍數增加也是可預期的。有鑑於此，大量的資訊安全管理產畧，如防毒軟體、反間諜軟體等需求將持續增加；而漏洞管理產品和入侵偵測產品也將成為重要的一環。

(3)Skype 及其他 V OIP 產品，包括附加即時通訊應用軟體，將更受企業界的重視。此情況下，用戶將尋求安全傳遞訊息的解決方案。

(4)使用者將延伸現有規範，建立內部控管機制。目的包括保護智慧財產和防止資料外流。而資訊傳遞、通訊安全、個人資料和存取管理等領域資訊安全市場都將受益。

(5)發展較單純用 PIN 或密碼輸入更為有效的認證方法，以因應高漲的消費者議題。諸如侵犯隱私、偽造身分、個人或公眾的監控疏失、線上金融和商務服務等情況的增加。單獨使用密碼已不足以保護公司資料。除了共用密碼所帶來的危害之外，有心人士亦可透過多種方式輕易破解密碼。此外，不少法案和條例也隨著與日俱增的安全威脅而催生，促使企業建立更有效的辨識系統。目前最完備且最廣為人知的，莫過於 FFIEC(聯邦金融機構檢查委員會)法案，其他法案條例將持續在 2006 至

2007 年間完成。傳統硬體以憑證識別之系統在短期內仍將持續成為主流；但是根據 IDC 的研究報告指出，綜合式及使用 USB 憑證，及其他新興辨識方法皆有成長的趨勢。

(6)攻擊者和資訊安全維護人員將擴大範圍。除了微軟的產品之外，攻擊者及資訊安全維護工程師，皆將其觸角延伸至其他企業及消費性產品上，如資訊安全軟體和管理服務等。應用軟體漏洞測試工具亦將受益於此趨勢。

(7)網路裝置多內建更多安全性功能，市場會轉向主動式管 (proactive management)，以處理日益異質化 (heterogeneous) 的資訊安全環境。新的漏洞管理、安全管理系統將能自動搜尋潛在威脅、蒐集分類資訊、分析客戶環境、發展漏洞管理的策略、提供多階層 (multi-level) 的事件回應策略 (response strategy)；另外也可針對互動資料進行事件分析，這些資料將可運用於日後的風險回應策略中。安全軟體跟漏洞管理產品將因此而受益。

(8)整合威脅管理 (UTM, Unified Threat Management) 將逐漸成為安全性裝置之主流，其他軟體安全產品 (Software Security Products) 將漸漸移往設備為基礎 (Appliance-Based) 的平台。舉例來說，我們相信傳訊及端點裝置 (endpoint appliance) 將可融合許多單點產品，使其成為整

併的平台。即使中階 (midtier) 客戶將因為管理上的便利，而湧向採用這類解決方案，但在另一方面，小型公司和大企業，由於成本與效率的考量，將較偏好單點 (single-point)、單盒 (single-box) 式的解決方案。

(9)消費性產品安全的焦點將由產品轉移到服務。雖然個人消費者安全產品在零售市場中仍維持強勁力道，我們預測管理服務 (managed service) 將漸成氣候；McAfee 是此一領域之先驅，從消費者服務供應商 (consumer service provider) 看來，這趨勢也十分明顯，但我們仍預期微軟跟賽門鐵克能推出新的安全管理服務 (managed security services)，導引市場發展更多的解決方案。

(10)未來五年內，資訊科技安全系統即逐漸融入實體保全設備，如門禁系統、錄影監視等。當奇異 (GE)、思科 (Cisco) 等企業開始進入監視器等實體的安全設備市場之際，我們預期資訊安全及實體保全系統兩領域將更為整合。CA 的指揮中心 (Command Center) 已經提供了一部份此種整合。在大企業中採用整合的比例從 90 年代晚期的 1-2%、2003 年的 5-7% 至 2006 年的 10-12%。當越來越多的監視系統從類比裝置轉變成數位、以 IP 為基礎的網路，我們預期監視系統將加速成為另一種 LAN 應用。(本報告整理，資料來源：IDC 調查)

第二節 本報告動機與目的

本報告的動機，由於資訊系統的發展，由大型電腦時代到個人電腦時代，而現今無疑是到了 Internet 的時代。

Internet 的發展，帶來資訊界許多新的變革，方便並簡化了許多煩雜的問題，但在資訊科技發達的現在，由電腦病毒、蠕蟲、木馬程式，甚至駭客的入侵資訊系統，造成電腦的癱瘓，讓許多組織損失了許多金錢，而「資訊安全」這個重大的問題卻也在資訊界逐漸受到重視，因而許多組織花大錢買高檔的設備，來維護自己公司的資訊資產，難而直到組織又再次被入侵，產生了一個重大的疑惑，「難到之錢花大錢買許多資訊安全設備，一點用也沒有嗎？」，那到未必。

其實都忽略了一個盲點，「入侵真的都是由組織外在而來嗎？」，因而往往都忽略了組織內部的「人」，在加上資訊安全的管理不當，造成無法彌補的損失，根據統計，組織內部人員入侵組織，比外面駭客入侵，高出了八到九成，如最近幾年發生的某銀行客戶基本資料外洩，銀行帳戶金錢被盜領；某銀行的網路銀行網頁被入侵，客戶金錢不易而飛．．．等，這些種種都基於內部人員所為，及組織的控管不當所造成的。

「安全」代表一種穩定的、在一定的程度內可以預期的環境，讓個人或團體可以在追定目標時，不受干擾或傷害，也不必擔心任何動亂或

意外。長久以來，安全(Security)就一直是人類社會追求的一種狀態。就資訊界而言，「資訊安全」，無疑是組織內最重要的工作，因而良好的管理與評估是必要的。

如何管理組織的資訊資產、做好資料的備份，更重要的是，如何在災害發生後做最快的復原計畫等，眼前的這些問題，已成為組織內部資訊安全相當重視的問題。

基於此因素，本組的報告目的著重在下列幾項：

1. 探討資訊安全的最新趨勢。
2. 探討英國國家標準局資訊安全標準範本 BS7799。
3. 資訊安全產品技術與評估標準
4. 設計應用資訊安全風險管理評估分析網站。
5. ITDR (IT Disaster Recovery)災害復原計畫。

有鑑於此，「資訊安全風險管理與評估」，是相當重要的一個課題之一，為了進一步了解我國資訊安全發展趨勢，找出組織發展的問題，本組除了說明英國標準局資訊安全範本及資訊安全產品技術與評估標準外，並探討如何妥善管理資訊的風險及設計資訊安全分析評估網站，及規劃執行 ITDR (IT Disaster Recovery)災害復原計畫等，並提出本組的建議，供為參考。

本報告期望能夠讓個人或組織更加了解何謂資訊安全，並如何妥善應用資訊安全的設備，管理及評估個人或組織內部的資訊安全。

第三節 本報告範圍與架構

研究範圍主要分為二階段：

(一)在收集資料方面：收集國內、外資訊安全相關之議題資料，了解資訊安全最新趨勢，並了解資訊安全未來發展，探討英國國家標準局資訊安全規範，及了解資訊安全產品技術與評估標準，並規劃執行 ITDR (IT Disaster Recovery) 災害復原計畫。

(二)在設計分析評估方面：運用英國國家標準局資訊安全規範，以其為基本架構，設計資訊安全分析評估網站，借以分析個人、及組織內部是否符合資訊安全基本要求，並提供建議。

本報告書的基本架構，如下(如圖 1-1)：

第二章為資訊安全理論與技術的探討，本章探討全球資訊安全定義、影響資訊安全的因素及資訊安全的範本 BS7799，說明其理論基礎，接著探討資訊安全的產品技術，最後規劃執行 ITDR (IT Disaster Recovery) 災害復原計畫的重要性，在當災害發生時，如何去實際啟用。

第三章為資訊安全評估分析網站，本章設計應用資訊安全標準範本為架構，並實際建構資訊安全的分析評估網站，敘述其系統架構與系統

功能操作流程图，評估及分析個人或組織內部是否合乎資訊安全的要求。

第四章為資訊安全評估分析網站畫面呈現，運用 Flash 製作登入畫面，建立資訊安全評估分析資料庫，並提供良好的建議與該個人或組織的风险分析評估等級圖。

第五章資訊安全報告結論與建議。

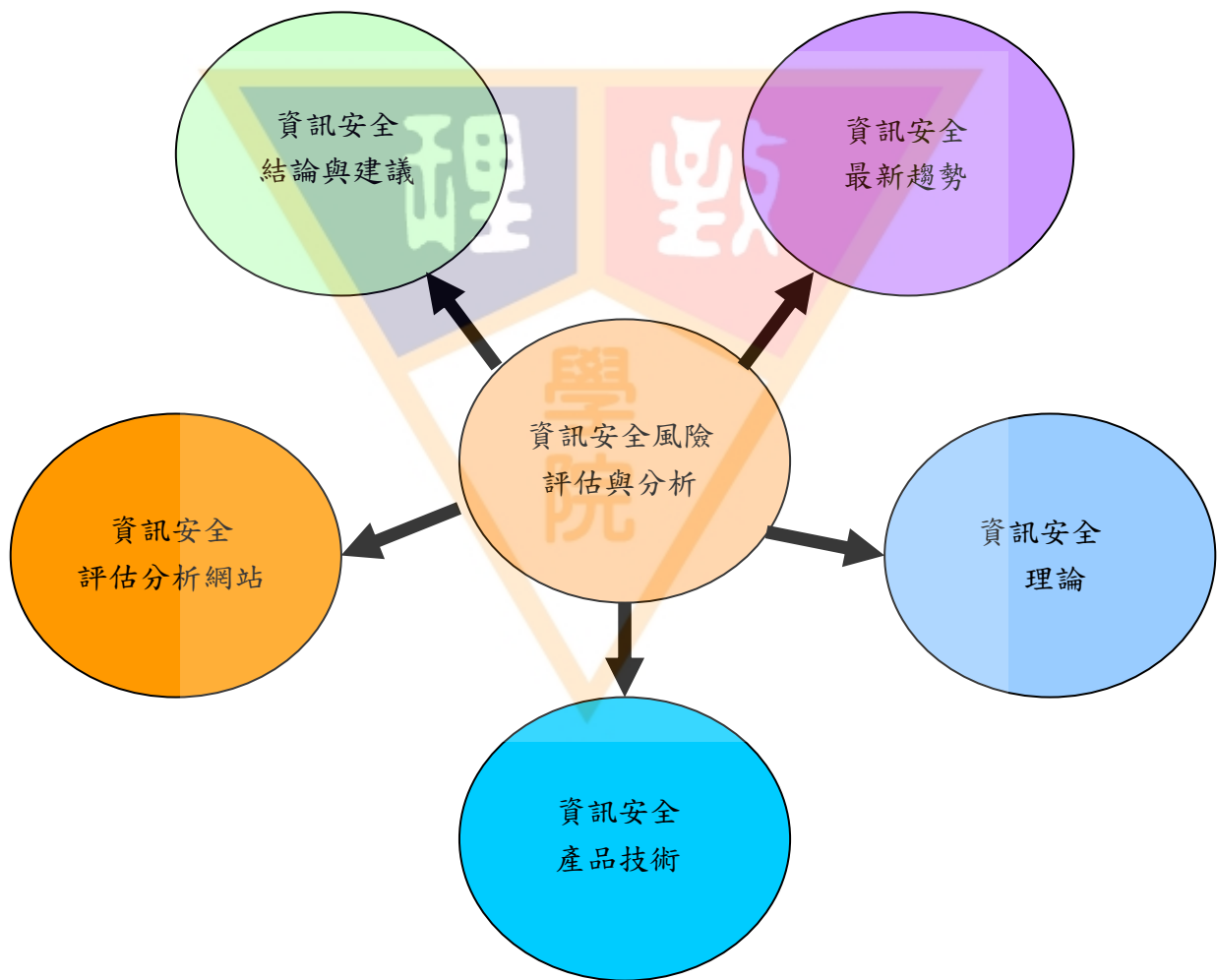


圖 1-1 本報告書基本架構概念圖

第貳章 資訊安全理論與技術

第一節 資訊安全定義

BS7799 對資訊安全之定義為：(資訊安全人雜誌，2004)

- (1)機密性 (Confidentiality)：其目的在防止未經授權的人取得訊息，所考量的是確保通訊的兩端彼此之間，在通訊期間內的訊息傳遞不被截取，因而導致資料外洩。
- (2)完整性(Integrity)：是為確保資料再傳遞過程中，接收者所得到的訊息和發送者所發出的訊息是完全一樣，任何被竊改過的訊息便失去了其本身的意義，成為一個無效的資料，更可能影響其他的資訊，造成資訊系統被破壞。
- (3)可用性(Availability)：是為了確保合法的使用者在需要使用系統資源時可順利使用，無論是利用任何手段造成合法的使用者，若無法順利使用系統資源，則資訊系統的可用性便喪失了。
- (4)不可否認性(Non Contradict)：利用數位簽章的技術，只有文件發送者知道自己的私密金鑰，而且文件具有發送者之數位簽章資訊，使其無法否認發送的事實。

國內外資訊安全定義如表 2-1、表 2-1 續。

年 代	資料來源	資訊安全的定義
1984	IBM	對資訊資產有意或無意的情形下，未經授權的公開、修改、破壞或使之失效等行為的保護。
1992	黃亮宇	就是把管理程序和安全防護技術應用於電腦的硬體、軟體和數據，以確保儲存中或傳遞中的數據免於他人有意或無意的讀取、刪除或修改。
1995	劉國昌	電腦安全的保護範圍包括：機房、電腦主機、終端機、電腦網路線、軟體與資料等有形與無形的電腦相關事務，良好的安全措施維護了這些資料的機密性、正確性、完整性及可用性。
1995	Hutt	資訊安全的威脅分為：潛在的威脅、實體災難、裝備故障、軟體故障、人為錯誤、資料的濫(誤)用及資料遺失等威脅。
1997	Parker	資訊安全的就是對於個人或組織在使用，所有關於言論、印製的及自動化技術等的保護以及保護資訊的產生、處理過程、傳遞、儲存使用、展示及控制等來源。

表 2-1 國內外對資訊安全的定義

年 代	資料來源	資訊安全的定義
2000	Finne	為降低資訊風險所進行的各種量策方法。
2000	ISO17799	機密性：確保只有獲得授權的人才能存取資訊。 完整性：保護資訊及處理方法準確性及完整性。 可用性：確保獲得授權的使用者在需要時可以存取資訊並實用相關資訊資產。
2002	李順仁	資訊安全，是一種管理而非技術。
2006	Microsoft	「資訊」對組織而言就是一種資產，和其它重要的營運資產一樣有價值，因此需要持續給予妥善保護。 資訊安全可保護資訊不受各種威脅，確保持續營運，將營運損失降到最低，得到最豐厚的投資報酬率和商機。

表 2-1 國內外對資訊安全的定義(續)

第二節 影響資訊安全的因素

資訊科技的快速進步，從早期集中式的主機系統到個人電腦、區域網路、進而到了今日的網際網路電子商務時代，電腦使用範圍不斷擴大，資訊安全威脅不斷升高，使資訊安全面臨更大的挑戰：任何可能造成資訊系統損壞的事物都稱「威脅」，而資訊系統可能遭遇的威脅可分為：「人為因素」與「自然因素」兩大類，如表 2-2，這些因素對企業來說都是重要的資訊安全警訊，也是資訊安全政策、資訊安全標準以及安全控管作業程序上所產生的缺失。

問題類別		原因		說明	後果
天然	災害	來自外部的自然現象故障		火災、水災、地震、打雷及溫溼度異常	無法正常
因素	故障	本身系統發生故障		軟體、硬體、網路故障	服務
人為因素	過失	人為錯誤獲 怠慢造成的 故障	疏失	<ul style="list-style-type: none"> ● 操作疏失 ● 維護疏失 ● 管理疏失 	資訊資產濫用
	故意	人為惡意獲 蓄意故障	破壞	<ul style="list-style-type: none"> ● 電腦系統破壞 ● 資訊設備破壞 ● 資料程式破壞 ● 資料程式竄改 	
			不當使用	<ul style="list-style-type: none"> ● 擅自使用電腦設備 ● 未經授權使用，不當使用資料、媒體、程式 	
			隱私權	<ul style="list-style-type: none"> ● 不當蒐集資料 ● 不當使用資料 ● 不當公開資料 	

表 2-2 影響資訊安全的自然與人為因素

資訊安全的問題，固然有科技的因素，但人性的因素還是遠大於科技的因素，且內部員工比外部駭客的威脅還大，在資訊系統所面臨的威脅事件中，屬於「自然因素」僅佔整體的 15%，而「人為因素」則高達 85%，其中又有高達 80%，來自於組織內部員工的無心之過或蓄意破壞，這是企業組織使用再好的資訊技術也無法防範的威脅。

資訊安全的目標在保護資訊資產，包括：硬體、軟體、資料、程序及人員，以防止電腦資源被變更、破壞及未授權使用，所以，影響組織

資訊安全的因素，除了防火牆、防毒軟體、消防系統之外，也必須制定資訊安全政策，做好風險評估及安全稽核，才能確保資訊安全，而影響資訊安全的因素，主要包括「商業上的競爭」、「資訊安全政策的疏失或漏洞」及較難防護的「資訊安全應用層面的疏漏」、「其他影響資訊安全因素」等因素，如表 2-3。

構面	影響資訊安全的因素
商業上的競爭	同業競爭入侵資訊系統
	盜取機密的資訊
資訊安全政策的疏失或漏洞	資訊安全政策的弱點
駭客入侵	內部與外部的入侵與攻擊
	一時興起、好玩等個人因素
	種族、宗教、國與國間的對立
資訊安全的應用層面	資料安全、網路安全
	電腦系統安全、電腦病毒防治
其他影響資訊安全因素	天然災害、人為的疏失

表 2-3 影響資訊安全的因素

(台灣電腦網路危機處理中心，2003、本研究整理)

(一)商業上的競爭

為達成商業上的目的，同業或其他競爭者利用入侵或攻擊對手的資訊系統意圖盜取商業上之秘密，而導致資訊系統被破壞或是機密的資訊落入競爭對手，其他入侵或攻擊的目的為構成財務、商譽之損失進而達成削弱對手之競爭優勢。

(二)資訊安全政策的疏失或漏洞

企業組織在制定資訊安全政策時，因為考慮不周或疏忽而導致資訊安全政策出現了弱點。內部的使用者或外部的入侵者常利用這些弱點進行攻擊、滲透、資訊竊取等行為，或因為措施上的弱點而導致危害企業組織資訊安全事件的發生。

(三)資訊安全應用層面的疏漏

資訊安全相關工作可概分為資料安全、電腦系統安全、網路安全與電腦病毒防治等應用層面，一般較難防護為網路安全。

(四)一般網路安全的防護措施

- (1)網路使用帳號，由權責部門統籌管理設定。
- (2)網路密碼必須定期更換，且不得洩漏他人，並於人員異動及職務異動時，註銷其帳號或調整其使用權限。
- (3)下載資料或程式必須先確認無病毒感染後，再行下載。
- (4)連線設備應使用防毒軟體及合法版權軟體，嚴禁更動原系統設定。
- (5)為防範電腦遭到非法入侵，應該要設置防火牆。
- (6)設定警示訊號，提醒系統管理或使用人員處理突發狀況。

(五)電腦犯罪

電腦或網路系統無法使用或提供正常的服務，原因有很多，從單純的電力中斷到遭受入侵及破壞等都有可能，凡是造成電腦或網路系統無法提供正常服務的，都可以稱為「事件」或「事故」，而在這些「事件」當中，可能造成損害或是危害組織資訊安全的，則稱為「資訊安全性事件」，其共通點都是造成系統服務中斷或無法正常運作。更甚者，當安全性事件造成重大的損害，且是由惡意所造成的，則稱之為「電腦犯罪」，如駭客入侵等。

一般網路犯罪包括：網路恐嚇、網路毀謗與公然侮辱、網路煽惑他人犯罪、網路色情、網路駭客、網路詐欺、網路強暴、而常見的類型有：

- (1)資料竄改：利用非法的手段改變電腦系統中重要的資料。
 - (2)特洛伊木馬：是指在電腦程式中擅自加上一些指令，而使得此程式不但能正常工作，且還能執行一些未經授權的作業。
 - (3)邏輯炸彈：是指一個程式或片段程式，被設計成隨時或在某種特定的時刻，來執行某些未授權的行為。
 - (4)電腦病毒：通常是經由網路下載程式的方式，所傳輸的破壞性程式的行為。
 - (5)電腦蟑螂：專門在網路上登記知名企業的名稱作為網址，然後再以高價向企業兜售牟利的人。
 - (6)軟體盜版：凡是為經過授權的複製或使用電腦程式都算構成犯罪。
- (六)其他影響資訊安全因素

天然災害，如地震、颱風、火災等，或因人禍，如戰爭、人為的疏失而導致危害組織、單位資訊安全事件的發生。

第三節 資訊安全的風險

風險管理在資訊安全的領域內是一個相當重要的議題，風險管理是透過一系列的工作，如：確認、評估並且運用保護的機制來降低風險；務必將風險經由以上的程序，維持在一個組織體能夠接受的層級；也就是說風險發生的次數、影響範圍、造成的損失被降低而不是完全消除，因當在實際運作環境中並沒有完全百分之百安全的環境。風險管理的另外一個目的是建置一些有效而正確的方法和機制來持續不斷地維持風險的層級，所以它同時意味著必須導入一定的管理方法與原則，形成一個風險管理的架構戰策略，成為日常運作的一部分。

由於各個企業與組織體存在的目的和任務不盡相同，所以對於不同的企業或組織體，相同的風險可能會有不同的看法或者是同樣列為風險但其所被定義的危險程度和使用的應變機制也會不同，另外所謂的風險也不全然與電腦運算環境相關，例如：一個組織體它本身的電腦運算系統是正常執行，但是機房所在的位置發生了火災意外，在這樣的情形下，電腦系統就必須被迫在消防系統啟動前停止其運作，要知道一個風險實現時，通常它影響的是一連串的作業，而且它的對應措施，通常也是一連串的程序和步驟。

組織體在確認一個風險時，一般來說必須定義以下四個基本的要素：

- (1)實際的威脅：定義一個威脅的存在，必須考量在實際環境裡；是否合理，例如在離海 1,000 公里遠的城市，定義海嘯帶來的威脅不具有任何意義。
- (2)當威脅發生時可能造成的後果：一個威脅的發生可能會帶來多種的後果，例如：颱風來臨，除了強風以外，可能伴隨著淹水、停電、地震及氣溫異常等不同的影響。
- (3)威脅事件可能發生的次數與頻率：當威脅發生的次數與頻率相當高時，意味著組織體可能必須將這個威脅的影響程度提高，而且需要積極處理預防此種威脅的發生。
- (4)我們如何確定威脅發生的範圍：威脅發生的範圍同樣也會影響威脅程度的定義。例如：地震發生的次數雖然比較之下不一定很高，但一個地區影響的範圍，通常包含相當大的區域。

以上四點的基本要素，可以幫助管理者針對本身環境和組織特性，了解各種威脅的影響，可以讓風險的評估較有一個整體性；由於環境和真實的情況不斷地改變，所以有可能一些威脅在評估的當時被忽略了，風險管理盡可能地降低風險所帶來的影響。

風險管理的過程中包含了許許多多的要素，主要包含下列所列的部分：

(1)執行風險分析：包含保護機制的成本效率分析。

(2)建置：檢閱及維護保護機制。

要進行這些流程，需要決定各種要素的一些特性，像是資訊資產的價值、威脅、脆弱性以及事件發生的可能性，風險管理流程的主要部分為給予威脅一個價值的基準，以及估計它發生的頻率，要做到以上這些評估的結果，需要運用一些公式及針對一些名詞先行做一些定義，我們會在後續談到風險分析時討論這些名詞。

(1)實行風險分析

進行資訊安全風險分析的主要目的，是要定義出潛在威脅發生的影響為何；所以要針對確認營運功能上的停頓，所造成的損失加以估計而後給予一個百分比或是實際的價值估算，風險分析的主要結果有兩個，一是風險的確認，一是證明所採用的資訊安全對策(鑑別、存取控制等)的效益(成本效益比(Cost/Benefit))；風險分析的結果，會直接地影響到風險降低的策略。

(2)建置

進行風險分析能夠建立資訊安全保護機制的成本及價值的比率分

析，同時她也會影響決策的制定；例如：當要保護的資訊資產遠低於保護機制時，通常會採取接受風險(Accept Risk)的決策，另一部分有時組織所重視的資訊保全的特性也會有所不同，例如：軍政系統通常較重視機密性(Confidentiality)，而私人企業則較重視完整性(Integrity)及可用性(Availability)。風險分析能讓組織體將有限的資源集中在對他們有重大影響的風險上，有許多的風險分析可以在後續的決策上直接採取預防措施，如此可避免後續處理時必須承擔較高成本的支出，同時免於較重大的損失。

風險降低，是風險管理的第二大項工作步驟，在進行了一系列的風險評鑑的活動之後，組織體已經可以由風險評鑑報告中清楚地了解本身組織體內有多少的風險存在，同時也了解目前的風險程度在什麼樣的一個位置。風險降低的流程包括了風險程度的排序、風險的評估及經由風險分析的流程去建置適合的風險降低控制的機制，想要把風險完全的消除是不切實際而且幾乎是不可能。想要把風險完全地清除必須花費非常多的人力及時間，而且在現今的企業環境裡電腦應用的環境可說一日三變，每一個環境的調整都會產生新的或不同形勢的資訊風險。

使用最少的成本和建置最適當的控制方法是資深管理者及各部門管理者的責任，進行風險降低的主要目的在於將風險控制在一個企業體可

接受的層級，並控制風險的發生維持在一個最小的負面影響，通常企業體本身都有所謂關鍵的企業功能，風險降低的另一目的是讓風險的發生不致造成企業的關鍵企業功能受到長期的中斷甚至於出現無法恢復的窘境。風險降低是一個有系統的方法論，資深管理者可以運用這些方法論降低風險的影響，而風險的降低可以被達成經由以下所列的方式：

(1)風險承擔

接受潛在風險的存在並讓資訊科技系統在這樣環境下持續運作，或者建置控制的機制將風險降低到可被接受的層級。例如在評估外部的入侵者對內部資訊系統的危害後在連接網際網路(Internet)的主要入口處建立過濾機制來防止不適當的存取活動。

(2)風險迴避

經由清除風險的成因及結果來迴避這個風險(例如：放棄系統的某些功能或是當這個風險被證實影響層面很大時，停止系統的運作，關閉系統)。

(3)風險限制

經由控制機制的建立來限制風險，最小化潛在威脅的負面影響，強化系統中較脆弱的部分(可考慮外部支援的應用、預防、偵測控制方法的使用)。

(4)風險計畫

經由發展一個風險降低的計畫來排序、建置、維護這些控制機制並可進一步的來管理風險。經由風險計畫的建立不但可以管理風險的發生同時也可以確實的擬定當風險發生時所應當進行的對應步驟及關鍵行動為何。

(5)研究與確認

經由確認系統脆弱性及安全漏洞的程序並且研究如何修正這些脆弱性及漏洞的方法，降低風險發生所產生的損失。再選擇修正方法時，同時也會評估實施修正方法所支出的費用成本與此一風險發生所產生的損失之間的比較，防能確保不會因防堵很小的風險而付出太多的成本。

(6)風險轉移

運用其他的選擇方式來轉移風險所帶來的損失，例如可以投保保險的方式來轉移風險造成的損失。通常在進行風險轉移的同時也會進行風險降低的一系列的活動，其原因在於一般的保險業者通常也會對投保人進行一系列風險評估的檢驗程序來確認保險業者本身所承擔的風險層級。

選擇任何一種風險降低的方法時，組織的任務與目標也必須一併考慮，因為不同的組織體所著眼的主要任務也會有所不同，同樣的一個風

險對 A 組織體來說是一個足以讓它作業停頓的重大風險，但對 B 組織體而言也許只是將日常作業改為手動如此地簡單。

組織體也許不會實際去定義所有已確認的風險，所有的威脅與脆弱性都應該依它們潛在造成任務的影響和損害的程度去加以分類，如前所言風險的分類同時也決定了組織體該把有限的資源放在對組織體來說有重大影響的風險，組織體任務及資訊科技系統的保護，會因為每一個組織體獨特的環境與目的，選擇所要降低的風險與建置控制的方法也會不盡相同。



第四節 資訊安全的標準規範

ISO/IEC 17799。國際資訊安全管理規範，是源自於英國標準協會 British Standards Institution (BSI) 在 1995 年所提出的標準--BS7799，2000 年被國際標準組織 (International Organization for Standardization，簡稱 ISO) 接受並於當年 12 月 1 日正式頒佈為 ISO/IEC17799 2000 (E)：Information Technology---Code of Practice for Information Security Management，成為全球通用與遵循之資訊安全管理系統規範。BS7799 標準條文的內容經過多次修訂，主要分成兩個部分：

Part 1-The Code of Practice for Information Security Systems

(資訊安全管理之作業要點)

Part 2-Specification for Information Security Management Systems

(資訊安全管理系統規範)

目前已成為資訊安全應用、管理與稽核所應遵循的架構，包含 10 個章節與 10 個控管重點，它可以來設置應用的時程，並以 10 個控管重點來保證目標的達成。

目前 ISO 為了避免一般組織或企業在實際稽核作業的困擾，計畫將相關重要管理系統，如 9001 品質管理系統及 14000 環境保護管理系統等整合成為可以合併申請驗證程序的標準，且企業或組織通過這些標準後，日後的持續稽核作業亦可合併辦理，以減輕人員實際工作上的負荷，

在 ISO/IEC 17799 資訊安全管理系統方面也已納入整合考量，而 ISO/IEC17799f 已通過的標準有 Part1 部份，Part2 部份 BS7799 Part2：於 2002 年改版完成後，已將相關條文納入審查，且其標準的條文將可併同整合於其他相關管理系統的標準，俟審查通過後，已成為 ISO 之標準，當企業或組織在申請管理系統認證時，可一併辦理多項的標準驗證，省去因單獨個別認證的時間、人力及費用成本。

ISO/IEC 17799 標準的風險評估包括了兩項系統化的考量：

- (1) 資訊技術 (Information Technology, 簡稱 IT) 安全的破壞造成可能的資訊保密性、真確性與可用性失效之後果，將會導致對企業的傷害。
- (2) 對各種威脅的防範與合理的控管部會影響這些破壞發生的實際可能性。

ISO/IEC 17799 是一套比較全面性的資訊安全應用與管理的標準，但不外乎就是控制及稽核 (Control & Audit) 的觀念。定義一套完整的政策、程序、實施與組織化的架構，用來提供合理的保障使企業目標得以達成，並避免要偵測或修正無法預期事件所造成的後果。

條文內容介紹

ISO/IEC 17799 的標準條文內容，主要分成 10 個章節範疇，其內容概述如下：

(一)安全政策 (Security Policy)

「安全政策」的目標包括：提供管理階層對資訊安全的指示與支持

(二)安全組織 (Security Organization)

「安全組織」的目標包括：

- (1)企業內資訊安全的管理。
- (2)維持處理組織安全的相關設施與資訊資產由一個可靠的第三單位所控管。
- (3)維持當資訊處理程序外包 (Outsource) 給其他組織時的安全。

(三)資產分類與控制 (Assets Classification and Control)

「資產分類與控制」是為了維持對企業資產適當的保護及確保資訊資產可得到一個相當程序的保障。

(四)人員安全 (Personnel Security)

「人員安全」為了要降低人為錯誤、竊取、欺騙及濫用相關設施的風險，來確保使用者意識到資訊安全的威脅；為了確保在正常工作程序中資訊的安全與降低安全意外事件的損害並從中習得經驗。

(五)實體與環境安全 (Physical and Environmental Security)

「實體與環境安全」主要是為了避免未授權之存取、破壞與影響企業的建築或資訊；避免損失、或對資產的破壞與阻礙企業活動的進行；避免對資訊及處理設施的破壞或竊取。

(六)電腦與網路管理 (Computer and Network Management)

「電腦與網路管理」要達成：

- (1)確保正確與安全資訊處理設備之運作。
- (2)把系統的失誤降到最低。
- (3)保護軟體和資訊的真確性。
- (4)維持資訊處理與通訊的正確性與可用性。
- (5)確保資訊在網路上的保全與保護支援的基礎建設。
- (6)避免對資產的損害與中斷企業活動。
- (7)避免資訊在組織間傳遞時的中斷、竄改與誤用
- (8)系統存取控制 (System Access Control)

(七)系統存取控制 (System Access Control)

「系統存取控制」要達成：

- (1)資訊存取控制。
- (2)避免資訊系統未授權之存取。
- (3)網路服務的保護。
- (4)避免電腦未授權之存取。
- (5)偵測未授權之活動。
- (6)確保行動運算與電信網路設施的安全。

(八)系統開發與維護 (Systems Development and Maintenance)

「系統開發與維護」要做到：

- (1)確保安全被內建在運作的系統中。
- (2)避免使用者資料在應用系統中被中斷、竄改與誤用。
- (3)保護資訊的授權、機密性與真確性。
- (4)確保所有的 IT 專案與相關支援活動都在安全的考量下進行。
- (5)維護應用系統軟體與資料的安全。

(九)企業持續運作規劃 (Business Continuity Planning)

「企業持續運作規劃」要降低對企業活動的阻礙與防止關鍵企業活動受到嚴重故障或災害的影響。

(十)稽核 (Audit) 則是要：

(1)避免違反民、刑事法律、規範、或任何安全要求契約上的義務。

(2)確保系統運作遵循組織的安全政策與標準。

(3)把系統稽核過程之效能極大化與影響最小化。

例如：協力廠商或公司外部人員存取組織內資訊系資訊處理設施時之安全管理；委外處理時資訊安全管理；如何去減少人為錯誤、惡意欺騙或設備誤用之風險；一旦發生重大系統故障或人為疏失時，如何確保主要的企業活動持續且能保護企業的關鍵作業等等。

訂定適當的資訊安全計畫並落實其管理，已是數位社會各個組織均需面對的課題。每個機構均面臨來個內部和外部不同的風險，這些風險均有必要加評鑑。評鑑風險的先決條件是訂定目標，目標有不同之層級，最高層級的目標就是政策。風險評鑑旨在識別、分析、評估並控制達成目標之悠關風險，其整個程序即為如圖 2-1。由於技術、營運環境、主管機關等不斷的改變，特殊風險又伴隨這些改變而來，所以，識別、分析、評估並控制這些風險的管理機制有建置的必要。

識別與風險分析的過程是一種持續及反覆的程序，包括過程分析 (Process Analysis)、明訂應盡之義務 (Responsibility) 與應負的責任之可歸責性 (Accountability) 等。

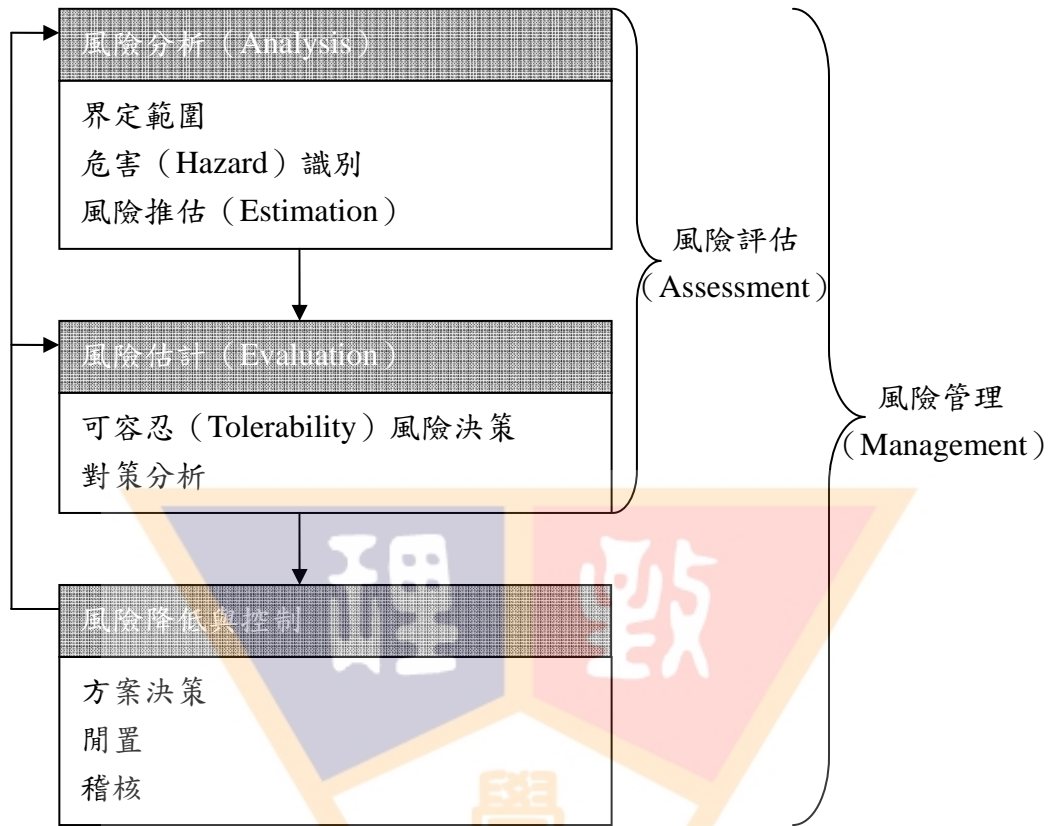


圖 2-1 風險分析、風險評估與風險管理關係圖

第五節 資訊安全產品技術與評估標準

近年來在許多國家都已經看到了電子商務在各個產業的如何改變其商業模式之實例。簡而言之，凡是透過網路所進行的商業活動，都可視為電子商務的範疇，這些活動包括資訊提供、市場情報、商品交易、以及透過網路的其他服務等等。因應這股不可擋的世界科技潮流，本國政府亦提出並開始執行「電子化/網路化政府」的計畫，目的是透過資訊與通信科技，將政府機關、民眾與資訊連在一起，建立互動系統，讓政府資訊及服務更加方便，隨時隨地可得。

然而在此對資訊化、網路化有高度需求的大環境中，資訊產品的安全成為不可缺少的環節。而資訊產品常常在研發的過程中即有意或無意夾雜著安全上的漏洞，而且這些漏洞或是引發出的弱點經常在安裝時甚或是使用一段時間後，才被發現。即使近年在資訊科學及軟體工程的領域都有長足進展，但是類似早期系統的缺失仍不時出現在新的資訊產品中。而有心人士對資訊產品的漏洞故意攻擊的手法，日新月異，防不勝防。

為了要提升採購單位及使用者在購買或使用時對產品的信心，產業界的各式產品自來就有相關的產品檢驗，以確保其功能、效能、可靠度、以及共通性國際標準等符合要求，藉以維持產品水準及安全的穩定性。然而，對資訊產品的檢測，與其他一般的工商產品之檢測則有本質的差異。因為資訊產品之安全功能主要是要保護資訊產品元件中的功能、元件所要達成的效能及所具的可信賴度，因而其複雜度及困難度也就相對的提高。

在諸多需要考量的事項中舉例來說，安全檢驗的目的除了要檢視產品的功能表現是否與所定義的規格一致外，並且還需要確保不想要的表現（包括惡意的，或是預期外的不正常表現）不至於發生。另外，若產品想提供更高的可信賴度，評估安全等級必須要提升，而相對伴隨的檢

測項目及分析亦趨複雜。根據等級的不同，此類的分析有可能需要涵蓋對產品的結構、設計、原始程式碼等詳細的檢視。再者，為使檢測的結果更具公信力，理論上須另行經過稱職且獨立的第三單位做確認（Validation）。亦即，完整的檢測過程，須包括第一階段的檢測單位的測試及評估，以及第二階段另一單位（及第三單位）的確認。

以下列舉現今傳統上一般所使用安全評估方式。

(1)駭客測試

為確定資訊產品的安全功能不至遭到破壞，或是存在有技術上的疏失，一種直接的測試做法是，聘用有經驗或有興趣的專業人士對其結構或功能上可能有的漏洞做探測。然而因為個人的經驗與所遵循的探測原則不盡相同，此種做法亦不依循較全面性、或一致化的檢測原則來確保產品的功能及品質，故此種做法所的的檢測結果僅能提供有限的信賴依據，或是做研發過程中產品檢測的輔助測試。

(2)一般商業測試

此類測試一般是為了提供產品販售商在產品介紹推銷之文宣上所需的依據，故大多只是進行較簡單的，且選擇特定項目式的對安全的部份功能做檢測，而不對安全實作的牢固性做足以提供某種信任等級的評估。

(3)各國政府內部規範

為了能夠對資訊產品之安全特色做一致性的描述，並針對安全特色所能提供的可信賴度定義、並劃分等級，以促進對此類產品完整全面的測試與評估，各先進國家已先後陸續建立了各國資訊產品安全之評估準則與評估架構。最為人之的是全國國防部在所謂的彩虹系列（Rainbow Series）中「白皮書」（The Orange Book），即可信賴的電腦系統評估準則（Trusted Compute System Evaluation Ctiyrtis，簡稱 TCSEC）中對電腦作業系統定義了安全功能及相對保證依次漸增的六個安全等級。後來此評估準則亦延伸到對網路連接設備以及資料庫管理系統之安全等級的定義及評估。

(4)業者自我聲明

有些業者對消費者推薦其所生產之特定資訊產品之安全特色時，常強調其產品的功能可以提供消費者對安全需求的保障。然而這些宣稱若是並無量化的、或是有效的佐證來支援，甚至在其宣稱中夾有模稜兩可或是誤導的字眼，對於不具有足夠專業知識的消費者而言，常常難以判斷其產品的品質是否真正符合需求。消費者對一特定產品的信心至多只能基於對此項產品研發業者原有的商譽、專業能力、以及與業者過去業務往來的經驗。但是這種做法，缺乏可量化的結果，自然不算是客觀的

判斷證據。

(5)良好軟體工程實作

另一種提升對資訊產品安全信心的做法，是在產品研究發展的時期，即確實遵循健全的產品實作（Implementation）準則，對產品架構的設計做嚴格且有固定原則的控管。已有的做法是，對產品的研發者及產品研發之軟體工程之程式進行被認可的功能完善評估（Capability Maturity Assessments），以展示產品研發者製造優良產品的勝任度。經此評估測試過，且顯示具有足夠專業能力的產品研發者，自然能對消費者提供較大的信心基礎。

(6)消費者評估

消費者有可能已具備、或是養成所需的專業技術，可以自行根據特定需求直接自行對產品做評估及測試。或是聘請某些足以信任的評估者、評估單位代為進行產品之評估及測試。不過顯而易見的，這種做法耗費成本較高。

上述各式測試評估的方法皆提供了商業網路及資訊產品場加值的商機，而取決於這些檢測方法的使用範圍及配合措施，或多或少它自也其貢獻；值得注意的是，這些既有的測試評估並不如原本設想的那麼簡單、有效率、或符合經濟原則。

資訊安全產品不斷推陳出新，使用者很難去判斷這些產品所宣稱的安全功能是否能提供所需的保障。且若業者所提供的安全功能無一套國際通用的衡量標準，怎能判斷哪一家廠商的產品最符合消費者的需求？對此國際間已制定跨國性的評估標準，將資訊安全產品的安全性以 7 個不同的等級(EAL1~EAL7)進行分類，並明確的制定出各等級所應具備的防護條件及安全說明，以有效的降低產品設計不良所存在風險及提供各廠牌產品比較的平台。

目前資訊技術安全評估共同準則(Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408, 簡稱 CC), 已成為國際公認的評估標準，各國陸續以此標準作為評估資訊安全產品安全之依據，並相繼建立自主性的資訊安全產品驗證體系及機制，以確保國家整體之資通訊安全。同時搭配國與國之間彼此交互承認，達到通行世界的目標。

就國內所使用的資訊安全產品來說，有高達 82%是自國外引進。試想若無自主性的驗證機構及評估技術去檢測這些資訊安全產品是否能符合其聲稱具備的安全功能，對於企業、機關的整體資訊安全防護，乃至國家安全等，均可能造成難以估計的損失。由於資訊安全產品驗證機制在國外已行之多年，且經證實透過繁雜的安全驗證程序，來檢測產品本

身是否符合 CC 對不同等級的安全要求，的確達到降低產品使用的風險，並進而建立起消費者對於產品的使用信心。

因此，行政院於 2003 年起便開始執行 e-Taiwan 計劃項下的「建立資訊安全產品驗證體系計畫」，目的在於建立我國自主性的驗證體系，如圖 2-2，培養檢測技術人才，籌備加入共同準則國際交互承認(CCRA, Common Criteria Recognition Arrangement)，使我國具有檢測及驗證國內、外資訊安全產品之能力，並與各國建立互信機制，達到「國內一次驗證，全球通關」的目標。在此四年的延續性計畫中，編列預算由經濟部商業司負責執行 2003~2004 年的工作項目，並委由資策會執行初期的體系規劃及市場調查工作。後為因應電信、資訊及傳播科技及產業之匯流，有效運用國家資源，並利後續資訊安全工作之推展，行政院科技顧問組遂於 2004 年 6 月 1 日函示，將 2005~2006 年度的預算改由交通部電信總局編列並執行。電信技術中心因此受委託負責執行本計劃檢測實驗室之建置、人才培訓及協助取得國際相互承認檢測技術及資格。

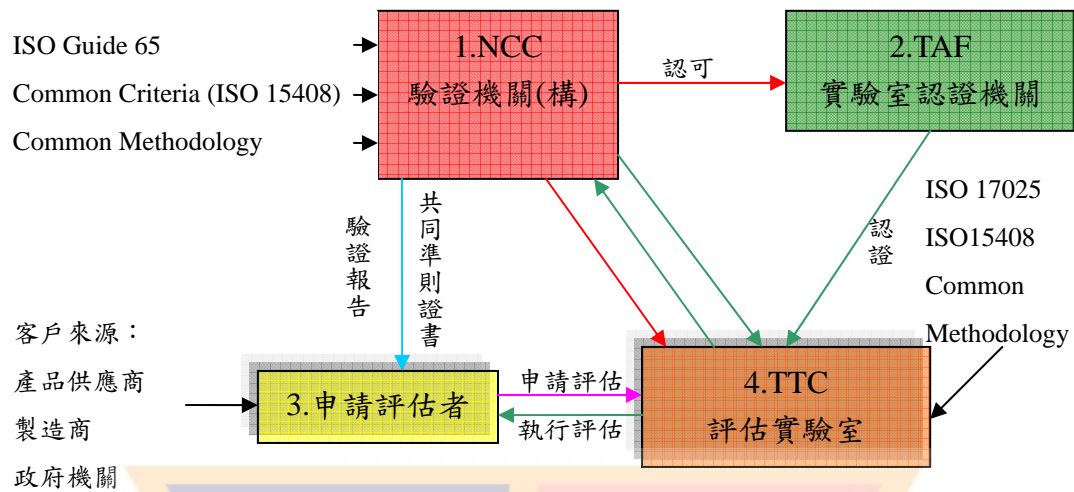


圖 2-2 我國資訊安全產品驗證體系架構

在此之前，礙於資訊安全產品在國內並無完整的驗證機制，以評估產品的安全性。所以廠商往往得花費龐大的檢測費用及冗長的文件往返程序，將產品送交到國外的實驗室進行檢測，以取得產品驗證證書。所幸這些窘況，於 2005 年 11 月國內第一家取得 ISO/IEC17025 資訊安全產品共同準則安全評估實驗室(CCTL, Common Criteria Testing Lab)認證的實驗室完成建置後，已順利得解決。同時也提供國內資訊安全廠商相關的產品檢測、顧問諮詢及教育訓練等服務項目，以縮短與國際間的落差。

就電信技術中心協助政府所規劃的共同準則評估及驗證體系中，如圖 2-3，是由國家通訊傳播委員會(National Communication Commission，NCC)擔任最高主管機關，除代表我國申請加入成為 CCRA 會員、制定相關的資訊安全政策及驗證程序外，同時也必須對認證機構(全國認證基金會，簡稱 TAF)進行認可，並由認證機構對執行檢測業務的實驗室進行認證，來確保實驗室的營運及檢測品質均符合國際規範。評估實驗室在收到送檢廠商的申請文件後，並須依據 CC 的規範逐一對送檢者所提供的文件及產品樣本進行評估，並完成技術評估報告。最後再由驗證機關依據實驗室的評估報告衡量申請廠商是否達到授予證書的標準，若符合則核發證書予申請廠商。

Common Criteria Evaluation Certification Scheme

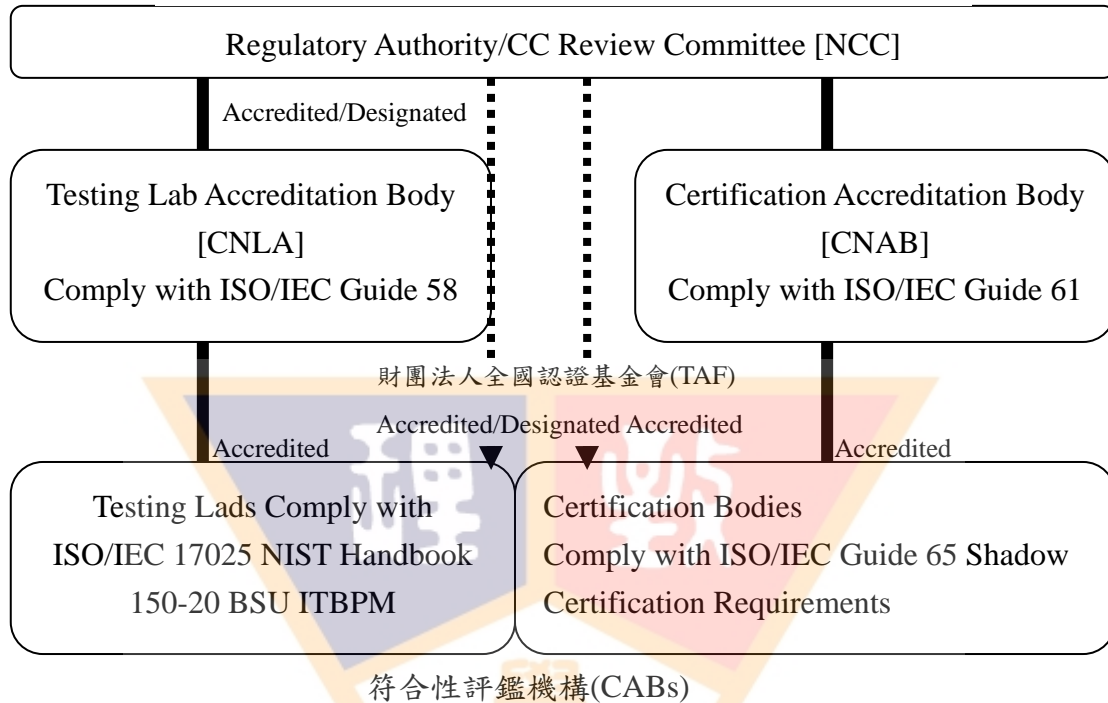


圖 2-3 我國共同準則評估驗證體系

各主要職掌負責的工作內容說明如下：

1. 驗證機構(CB, Certification Body)

- 管理與維護檢測實驗室之資格
- 管理與督導檢測實驗室所從事的活動以符合驗證機構所訂定之政策與程序
- 提供檢測實驗室檢測方法並給予技術指導
- 審核與驗證實驗室所出具的檢測報告書
- 核發與維護檢測結果之驗證證書

- 管理與維護驗證產品項目與所有相關文件
- 公開與驗證活動相關之所有文件

2. 認證機構(AB, Accreditation Body)

- 對國內共同準則評估實驗室提供認證服務以確保實驗室符合 CC 與資訊安全產品認證之規範。

3. 共同準則安全評估實驗室(CCTL, Common Criteria Testing Laboratory)

- 經過認證機構認證及驗證機構驗證的檢測實驗室
- 已具驗證機構提供之檢測規範與程序與共同準則檢測方法
- 執行相關的檢測活動
- 為維護檢測之公正性，實驗室必須有正式文件，申明其檢測活動之政策與程序符合公開、公正與保密立場

4. 產品製造商或供應商(Developer/Sponsor)

- 提供檢測實驗室檢測項目之安全標的、評估標的及相關軟硬體與文件

以國內的資訊安全市場型態來看，主要可分為資訊安全服務及資訊安全產品兩大市場。在資訊安全服務部份，又以提供顧問諮詢及建置或導入 ISO17799 為主，且所執行的工作尚有明訂的標準可依循。但在資訊安全產品部分，則僅能仰賴資訊安全廠商所自訂的安全等級或宣稱，進行硬體設備或是軟體系統的安裝及設定，以達到安全防護的目的。在缺乏一個國際共通的評估介面或標準之下，是難以將抽象的表述量化，甚至進行差異性的比較。

自從 CC 成為資訊安全產品檢測領域共通語言之後，世界主要國家大多已採行此標準並建置技術能量多年。透過對資訊安全產品所進行的檢測及驗證程序，將可以嚴格執行採購資訊安全設備的第一道關卡，並將資訊安全防護的保衛戰由後端的管理、維護及監控機制等拉到最前線。藉由一開始便採用已取得驗證證書的資訊安全產品，來降低後續漏洞或風險發生的機率，以確保整個組織能永續經營下去。若能重視進行資訊安全產品驗證所代表的涵義，將可以提升國內資訊安全廠商對產品安全需求與標準的認知，進而成為一股欲擠身進入極具專業且進入門檻極高的 CCRA 會員的助力。

因國內資訊安全廠商對產品安全需求與標準的認知普遍不足，無法生產符合資訊安全要求之產品，進而拓展國外市場；另一方面，由於國內資訊安全產品之檢測機制尚未建置完成，無法自行確保資訊安全產品能有效達到保護使用者安全，我國該如何利用現有資源與自擁優勢急起直追，建立自我國資訊安全檢測能量，協助推動國內資訊安全檢測機制之建立，進而提升國內資訊安全廠商之國際競爭力是現今不容緩的課題。

第六節 ITDR (IT Disaster Recovery) 災害復原計畫

資訊安全政策的制訂，已成為一個流行的趨勢，隨著 BS7799/ISO17799 等安全規範的被推廣，企業組織開始注意到除了安全防护系統的採購外，安全政策的制訂及完善的管理規章，才是維護整體組織永續經營的重要環節，在整個安全規範下，災害復原 (Disaster Recovery) 被列為評估的重點之一，災害復原的重要性由此可見一斑。

網路安全事件也跟人體健康有異曲同工之妙，可以分為事前及事後的處理方式，防火牆、IDS 等安全軟體的設置是將焦點放於預防；而完善的安全政策、快速的災後復原，則是重視在治療，隨著電子化企業組織的普遍，組織內所有電子資訊是公司的重要資產，如何有效的保護、及快速回復至原始狀態，便是建立災害復原計畫 (Disaster Recovery Plan) 之目的。

企業永續經營 (Business Continuity) 成為越來越多廠商關心的焦點，災害復原計畫是企業永續經營管理下的一項重要環節，災害復原 (Disaster Recovery) 被定義為建立一套作業程序，可以在組織商業機能遭受中斷時獲得快速回應能力的應變計畫，因此，透過規劃及建置災害復原計畫，企業組織可以在受到破壞時，以最短的時間恢復到正常作業狀態，是該計畫的最大目的，其中造成商業機能中斷原因包含了天災、人為災害、系統損害、病毒、系統安全問題等，也因此，災害復原計畫並非僅指於讓電子系統回復到正常狀態下如此簡單，而是更廣泛的涵蓋了整個企業的文化、日常運作機能，範圍擴及整體企業組織。

透過底下建置計畫的步驟可協助您建立復原計畫，隨著所重視的程度不同，您所規劃的內容將不盡相同，請斟酌自己管理環境加以修正。

階段一 蒐集您的資訊

Step1 組織復原專案

Step2 建立企業災害影響分析

Step3 建構風險評估

Step4 發展復原政策

Step5 檢視現場與非現場備份及復原作業程序

Step6 選擇替換設施

階段二 撰寫及測試復原計畫

Step7 發展復原計畫

Step8 測試你的計畫

階段三 建置和審核計畫（持續的）

Step9 建置計畫

Step10 定期演練及審核

事前：復原計畫單位的目標與範圍

開始規劃您的災害復原計畫前，一項重要的認知必須先被瞭解，您必須去界定出進行災害復原計畫單位的目標以及範圍，談論到企業永續經營管理，除了災害復原以外，災害預防計畫（Loss Prevention Plan）是著重於事前的預防，造成商業行為（可解釋為日常運作）嚴重中斷的原因會有以下：天然災害（風、水、火及地震等）、設備失效引起的錯誤、工作程序所以引起的中斷、人為判斷上引起的錯誤及惡意行為（包含了網路攻擊、病毒、入侵等），請記住，災害復原計畫需依附在一完整的災害預防計畫下所建置的快速復原計畫，目的在於儘早恢復正常運作，減少商業損失，因此，所有的動作皆是為了儘早復原所設計，為此，您的計畫必須明確根據不同型態的中斷原因，具體說明所該反應的動作（Action）。

例如，離線進行資料更新、撥打救難電話、聯絡專案負責人、更換網路設備等實際的反應動作，撰寫一套明確的標準作業程序（SOP）會增加反應速度的好方法，因此，如何界定復原計畫單位的目標和範圍您可以根據底下三個原則，來規劃您所採取的反應動作：

- (1)找到可能會嚴重干擾重要運作單元的共同導致中斷干擾因素。
- (2)預期這些運作被干擾所導致結果的影響和效果。
- (3)規劃並且文件化干擾因素回應辦法，促使恢復（Recovery）中斷儘可能快速處理。

建構：組織災害復原專案

共有三個階段能協助您建構此一專案

首先，在第一階段，您必須區隔何謂重要系統、出錯時的影響和風險、可用資源狀態、回復程序和如何取得復原，考量以上因素來規劃適合的災害復原專案。其次，第二階段為實際的考量單位環境及能力，撰寫並且測試所規劃之復原計畫。最後，第三階段為持續的進行計畫的查核及建置計畫於您的企業，並保持計畫隨時皆能運作。

三個階段皆是隨時可逆的發展過程，您必須瞭解，您得隨時回頭審視您目前所規劃的策略或是方法，是否切合實際狀況。

階段一 取得您的資訊

步驟 1 組織復原專案當您的復原計畫範圍及底下的所有涉及的因素，和進行計畫的流程被決定時，最初的階段便是選擇您專案組織的成員，其中包含了協調者，復原計畫所涉及的單位部門廣泛，錯誤的發生，並非僅是簡單的系統錯誤或是設備錯誤所引起，所造成的影響的範圍，也許是跨部門的，因此，協調者的存在將會非常重要，其負責在整個復原計畫組織小組內肩負起協調及掌握小組進度之責，協調者之外，便是各部門的委任者，透過委任者將可瞭解各單位部門之詳細狀態，視部門大小您可以選擇多位或是一位委任者來擔任小組的成員，專案小組確認後，即可著手規劃完整的工作計畫以及工作時程表，而復原計畫小組的成員，也成了日後處理單位錯誤狀態的第一線人員，因此，在選擇上必須針對專業以及對於環境的熟悉程度來進行審慎的評估，並要建立起完整的復原計畫小組的通訊方式，目的在於可以快速的找到該工作負責人。

步驟 2 建立企業災害影響分析

建立工作小組後，企業災害影響分析的步驟將是協助您針對企業弱點進行建檢的動作，包含了企業工作流程、主要工作系統、應用系統、網路設備都需在此階段界定災害影響分析。評估及假設各種中斷行為所造成災害影響，是本階段的重點，您必須根據不同的中斷狀況進行分析，其中需要思考的不僅僅只是單一系統或是工作行為被中斷，您必須去思考到背後所影響的範圍，例如電力的中斷所造成的影響範圍，因漏水所造成的受害範圍等，這些看似雞毛蒜皮的小事，也都是需要去考量並進行分析的，藉由界定影響範圍及受害程度的分析，您將能找出發生錯誤時優先處理的層級，這有助於快速恢復及後續進行選擇合適恢復方法階段時的工作。

步驟 3 建立風險評估

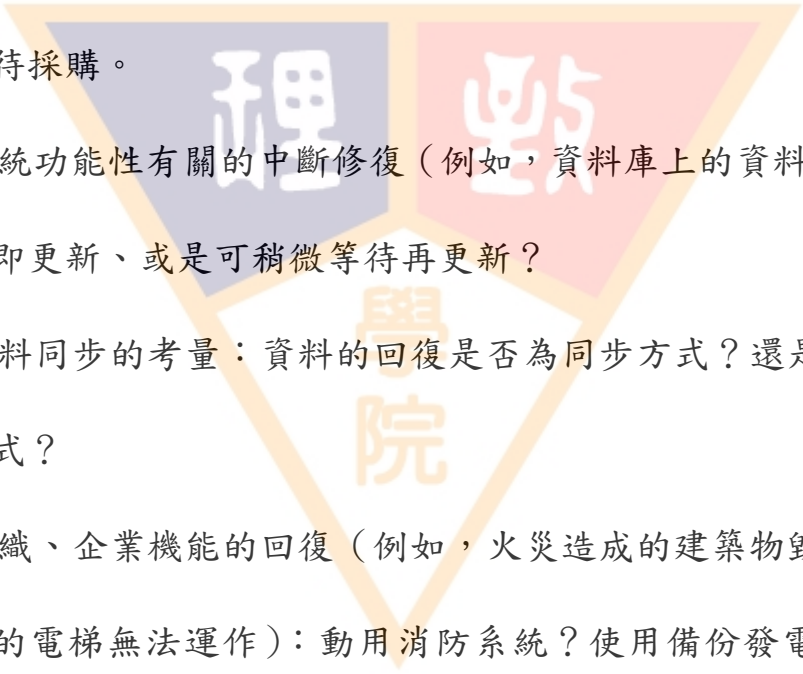
定義並且量化單位裡的實際風險，風險會來自哪些環節？您必須去衡量其間的嚴重性和優先順序，實際的安全問題（包含系統、人事、工作環境），備份程序（或系統）、資料上的安全、甚至是由鄰近災害所導致（水、電、火等其他因素）這些都是會導致重要系統遭受干擾的因素，分辨這些弱點，並分析其背後的風險，是本步驟的重點。透過風險評估的過程不僅是找出上述錯誤發生點的動作，更是需要從企業日常運作經

驗中發覺出最小單位的錯誤徵兆，例如發生電力中斷原因可能來自於電源設備錯誤，也可能是地區停電未通知，更有可能是因為供電設備遭受關閉（如插頭被踢掉），您必須視所處單位和環境來區別出同一種狀況下事件發生的嚴重性與優先處理順序，小至辦公室大至整棟商業大樓等，都是需要去界定和分析所造成的影響，儘管在整個 DRP（Disaster Recovery Project）資料取得的階段中，透過企業災害影響分析的步驟，系統漏洞的界定已經由確認共同風險或是透過減少共同發生的分析方式做了最簡化的粹取，您還是必須針對這些所粹取的系統漏洞（或是安全漏洞）做風險上的評估，包含發生的機率、優先處理順序，修復的成本等。

步驟 4 發展復原計畫的策略大綱

需瞭解復原方法選擇策略的目的在於將運行中斷的影響降至最低，因此復原方法選擇策略的設定上，必需考量那些因素是日常運作中重要的商業機能（如交易、人事、門禁、網路、電腦設備等需要界定），透過企業災害影響分析（步驟 2）可以去找到並且界定其優先順序，接著便可以決定遭受損害時所需動用的恢復資源層級（根據重要程度不同，可以去決定所需要動用的資源，並跟使用資源的使用程度來設定妳的層級）以及這些可用資源扮演的角色（資源函蓋了人、事、物，並非單純僅指

系統)，而復原計畫工作小組則是扮演了協助這些可用資源居中調配，使其能夠適時的發揮其作用，快速回復至正常狀態下，因此，規劃您的復原策略大綱時必須把握底下幾項重要的考量點，透過考量點來決定您所採行的動作，以及需要調配的資源程度，甚至是選擇的替代方案：需要立即回應，如：選擇成本高的回復方式，即隨時備份。

- 
- (1)運作環境有關的中斷修復：可能涉及設備毀損，需要用備品或是等待採購。
 - (2)系統功能性有關的中斷修復（例如，資料庫上的資料遺失）：離線立即更新、或是可稍微等待再更新？
 - (3)資料同步的考量：資料的回復是否為同步方式？還是用離線拷貝方式？
 - (4)組織、企業機能的回復（例如，火災造成的建築物毀損、停電造成的電梯無法運作）：動用消防系統？使用備份發電機？請水電工？
 - (5)過渡時期的方案選擇：用舊系統先頂替？去跟別的部門商借？
 - (6)系統恢復後的後續處理：系統過渡時是否有損耗？備份後的資料是否銷毀再重新備份目前新的狀態？

上述的考量點都是您可以根據資源、錯誤風險嚴重程度可以選擇的錯誤復原方法選擇策略，根據所選的方式，您必須付出的成本將會不同，這也將是您必須腦力激盪的。

步驟 5 檢視現場（線上）與非現場（離線）備份及復原作業程序組織單位所使用的任何系統都需要重要的資料記錄來支援，無論是電子形式或是文件形式的資料，包含商用系統、資料庫作業，透過企業災害影響分析步驟，這些資料及功能的優先權順序都會被界定出來，因此，本步驟則是將重點放置於如何重建這些已經損失或是遭受中斷的資料，您可以選擇的資料恢復辦法有不少選擇，可以利用同步的方式來做到資料的復原，或是使用外部媒體的方式將舊有資料移植回工作平台上，亦有利用人工輸入的方式重建，根據所選擇的方式、資料的嚴重程度、原始資料備份方式，您所花費的時間、成本將會不同。

然而，一項重要的觀點在此必須被提及，以系統來說，企業內部會有許多不同的資料系統存在（包含資料庫型態、函數庫、檔案甚至是文件、程式原始碼等），這些存在的系統經過風險分析後，您必須決定最有效率的資料備份、保存方式，至於備份程度以及備份技術的拿捏，則需視您成本、資料優先權而定，先有備份策略後，才能有復原程序的設計。選擇離線或是即時線上的復原，將是視您系統重要性、技術可行性所做

決定，越是重要的系統，越要求其在線的時間，舉例說明，若同時銀行機構的首頁與網路銀行交易網頁出錯，這時您該選擇何者為優先？一般會選擇讓交易恢復，但若加入時間因素，修復首頁需要 30 分鐘，修復交易網頁需要 45 分鐘，那這時您該如何選擇呢？因此，復原策略的重要性即是在此，是以時間為考量，還是以系統重要性為考量，兩者衝突時，如何選擇，都考驗著復原計畫小組的規劃能力。離線或是在線的備份策略、復原策略，則是在整體原則下所產出的標準程序，為此，還需多多的思考。

步驟 6 選擇替代方案

經由上述的步驟，您將能夠依單位內系統及功能的重要程度來規劃您的備份程序，以及面臨災害時恢復的標準作業程序（SOP），然而，這樣就能完全沒有疑慮了嗎？最後需要思考的，則是復原過渡時期所需要選擇的替代方案，您可以考慮來自於外部的援助或是系統以外的處理方式，替代方案設定的目的在於避免內部無法立即復原時，可以藉由外部來做到支援的工作，例如常提及的異地備援，甚至是由外部技術人員來協助處理無法解決之問題（亦有經驗是採用外部網站方式來取代目前網站癱瘓時的替代做法），或是電子系統遭受癱瘓時，利用人事的人力結構來做到作業的持續執行，這些額外的替代方案，是需要被思考來當作復

原過渡時的處理方案，因災害所影響的範圍，並非是我們可以預測的，雖有完善的回應策略，但中間所面臨的灰色地帶如何處理，這就是替代方案存在的必要性，因此，需將其納入考量的範圍，如此架構的災害復原計畫才能夠全盤且切合實際運作狀況，而非單純紙上談兵，為了應付而規劃。

階段二 撰寫及測試復原計畫

步驟 7 發展復原計畫此階段重點在於將您實際的復原計畫動作文件化，以文件形式來記錄您目前的所有復原動作，不僅只是描述目前環境並且需要仔細去描述在遭受嚴重中斷或是干擾場景下得實際復原動作（建議利用 SOP，如此任何人皆可透過 SOP 來做到復原動作，日後維護、審核上也是相當有助益），本文件裡一項重要的內容則是詳述如何的復原，請考量您在第一階段所做的復原策略，根據所定義的復原方法選擇策略來撰寫您的復原動作，例如，重新安裝系統的步驟、資料庫資料重新匯入的步驟甚至是撥打電話請外部人員處理時，電話號碼以及外部人員的聯絡資料皆須撰寫至您的復原動作說明裡。因此，可想而知，這個復原計畫將會是項非常繁瑣的紙上作業，您必須思考的場景以及復原手法之多，將會大大的考驗工作小組的專業能力及對於組織的熟悉程度。然而，繁瑣的工作背後，將是日後處理災害復原時最大的助力，也是建

立災害復原計畫的最大目的所在，本階段的重要性可想而知。

步驟 8 測試你的計畫

文件化您的災害復原策略/計畫之後，測試計畫的可行性，將是接下來的步驟，您必須去預想可能會遭受的中斷原因，並測試您的復原計畫是否可以快速且正確的完成工作，測試場景的設計必須切合實際狀況，且力求徹底與真正切合，這與近年來許多演習都力求真實是相同道理，組織內需建立對於復原計畫的重視，而非是敷衍，認為僅是形式上的心態來進行測試，透過測試活動，您將找到規劃後尚未能思考的環節，甚至是設計更為流暢的復原活動，降低組織的抗拒性，因此，您的測試計畫將會是需要長期進行且隨時更動的（會演變為定期的演習），以線上人員能夠隨時熟悉作業程序，發生真正狀況時能立即處理，快速反應。

階段三 建置和審核計畫（持續的）

步驟 9 建置計畫

確認計畫可達上線標準後，將計畫導入您的組織中，即是本階段的努力工作，復原計畫的導入勢必會引起陣痛期，因此，足夠的教育訓練與領導階層的協調及高階主管的支持，將會是專案工作小組需要注意的環節，除人事的抗拒外，備份系統及替代系統的導入與整合，也將是需要衡量的因素，若在規劃之初都有將其考量在內，相信建置計畫的過程

將會十分順利，且獲得支持，這也是在期初資料蒐集及策略規劃思考時花費大量時間成本所需要預見的成果，若仍遭受阻礙，那您得再回頭審視是否在規劃時那個環節出錯，需要再重新規劃思考。

步驟 10 定期演練及審核

災害復原計畫就等同於災防演習演習般，力求的是災害發生同時能降低損害程度，儘早回復正常運作，因此，定期的演練以及審核是相當重要，且現代組織追求快速應變，以期具有競爭力，資訊設備的添購與更換，週期改變定會比傳統更為快速，因此，不同系統的導入，復原計畫就需跟上其腳步，才能符合災害復原計畫的目的。而審核上，除針對計畫本身的審核，人員本身的審核也是需要思考的環節，畢竟系統是由人所操作，人為的疏失，會比系統的疏失來的嚴重，透過人事系統也許可以在審核上給與獎懲。

組織文化的相整合 EDS(www.eds.com)負責全球永續經營管理總監

Joyce Repsher 提出了八項永續經營訣竅分別為：

步驟 1：主動規劃勝於被動回應，長久之後下花費也比較低。

步驟 2：不要把所有的蛋放在同一個籃子。

步驟 3：在企業管理文化當中，整合永續營運的管理計畫。

步驟 4：選擇負擔得起的備援方案中，回復速度最快的方案。

步驟 5：定期測試不間斷計畫，確保計畫和現行狀況相符。

步驟 6：永續營運計畫應以最可能發生的威脅為主。

步驟 7：檢查不間斷計畫當中，不同部分彼此間是否協調。

步驟 8：了解地區性災害對優先順序的影響。

災害復原計畫的建立，除了快速解決遭受破壞的組織作業外，更深遠的意義在於維持企業的永續經營，資安政策並非僅是空談或是定期請顧問進行審查時才進行的作業，而是需要思考企業文化，將其融入日常運行中，如此，建立的計畫才能有所發揮，災害復原計畫小組的成員必須體認且親自推行至工作現場，復原計畫不僅是系統上的工作，更重要的它應是個企業活動，與企業生存有著重要關係的作業，相信有這樣的認知，計畫的推行與實踐將會有所意義，且整體計畫會是「可用」的計畫，而非是趕流行的一個護身符，這是應是企業上下全體需要有的認知。

第參章 資訊安全分析網站

第一節 資訊安全評估分析網站架構

以 BS7799 資訊安全管理標準之控制目標及控項目，以其作為風險評估要項，建新立資訊安全風險評估之依循，首先辨認是否為資訊安全風險，建立資訊安全風險管理評估表，並實際分析資訊安全風險的發生，針對組織內部或個人不同的環境設定，做測試與評估其內部資訊安全的風險，並提出報告，達成資訊安全有效的管理。

運用其控制的觀念，建構資訊安全評估分析網站，經由此網站的建立，來確定組織內部或個人資訊是否安全，並提出建議及風險等級指數圖，資訊安全評估分析網站架構，如圖 3-1 所示。

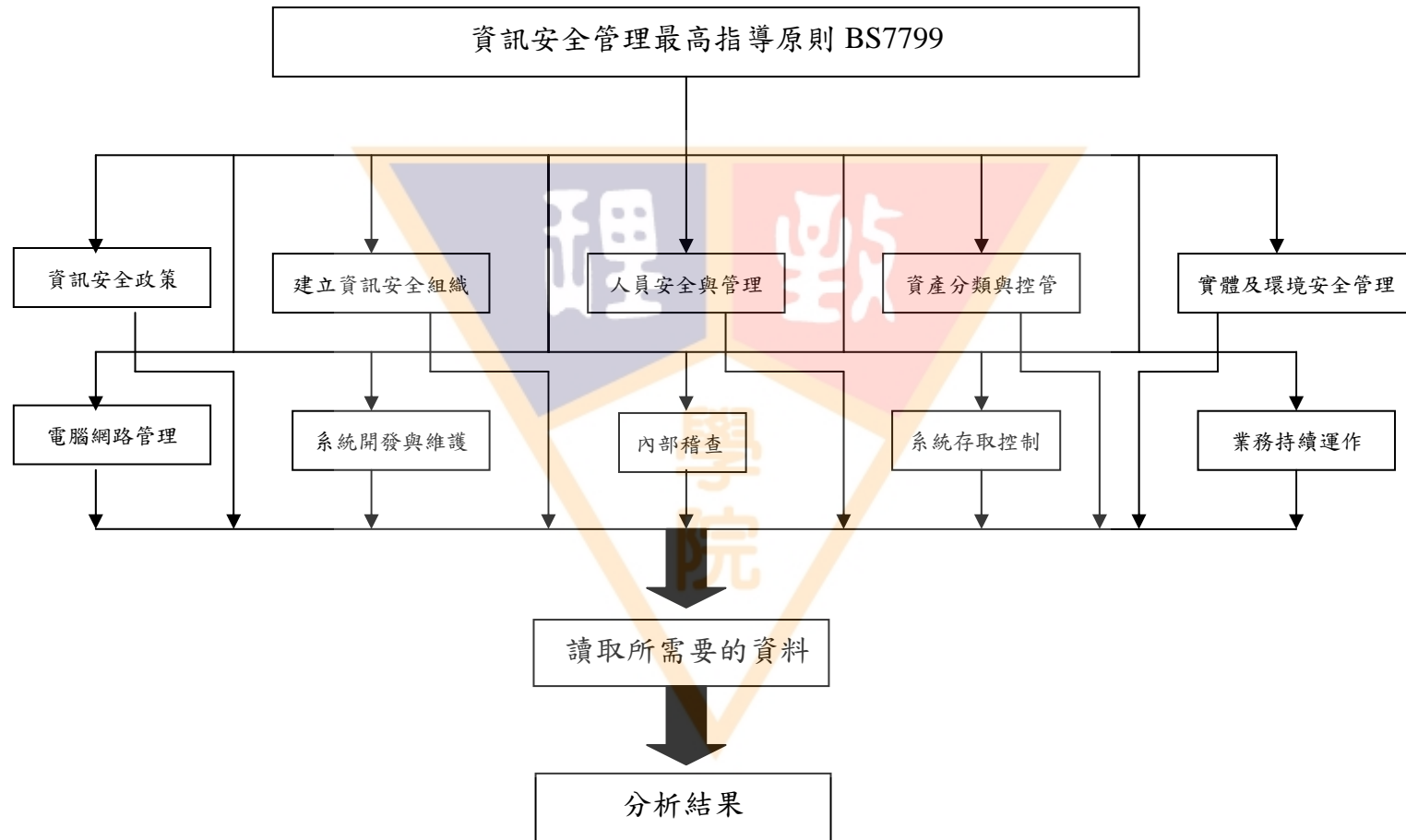


圖 3-1 資訊安全評估分析網站架構圖

本報告資訊安全評估分析網站的架構主要是參考資訊安全規範

BS7799 所建立出來的分析網站，主要的分析類別與重點有：

- (1) 資訊安全政策：主要分析內容是提供並建議管理階層對資訊安全的指示與支持。
- (2) 建立資訊安全組織：主要分析內容是組織內資訊安全的管理、組織安全的相關設施控管、資訊處理委外的安全。
- (3) 人員安全與管理：主要分析內容是降低人為的錯誤、確保使用者意識到資訊安全的威脅。
- (4) 資訊產分類控管：主要分析內容是將組織資產做適當的保護與確保資訊資產可得到保障。
- (5) 實體環境安全：主要分析內容是避免資產的破壞與損失、組織的建築或資訊的破壞與影響。
- (6) 電腦網路管理：主要分析內容是降低系統的失誤率、維持資訊的正確性與可用性、保護軟體和資訊的真確性。
- (7) 系統開發與維護：主要分析內容是確保安全內建於系統、保護資料的授權與機密與真確性、維護應用系統與軟體的安全。
- (8) 系統存取控制：主要分析內容是降低組織活動的阻礙、防止關鍵組織活動受到嚴重的災害或故障。

(9)業務持續運作：主要分析內容是降低組織活動的阻礙、防止關鍵組織活動受到嚴重的災害或故障。

(10)內部稽核：主要分析內容是確保系統運作依循標準、確定遵行契約上的安全規定、確保資訊安全發生時影響最小。

本報告的分析可以分別做十大類別的各別分析，也能做十大類別的整體分析，並且會將使用者或管理員的資料，利用 Access 資料庫做資訊安全的整合分析，並提供相關的建議，及資訊安全風險的指數圖，方便了解該組織的風險等級。



第二節 資訊安全分析網站功能操作流程

本報告資訊安全分析網站各別分析功能操作流程如下：

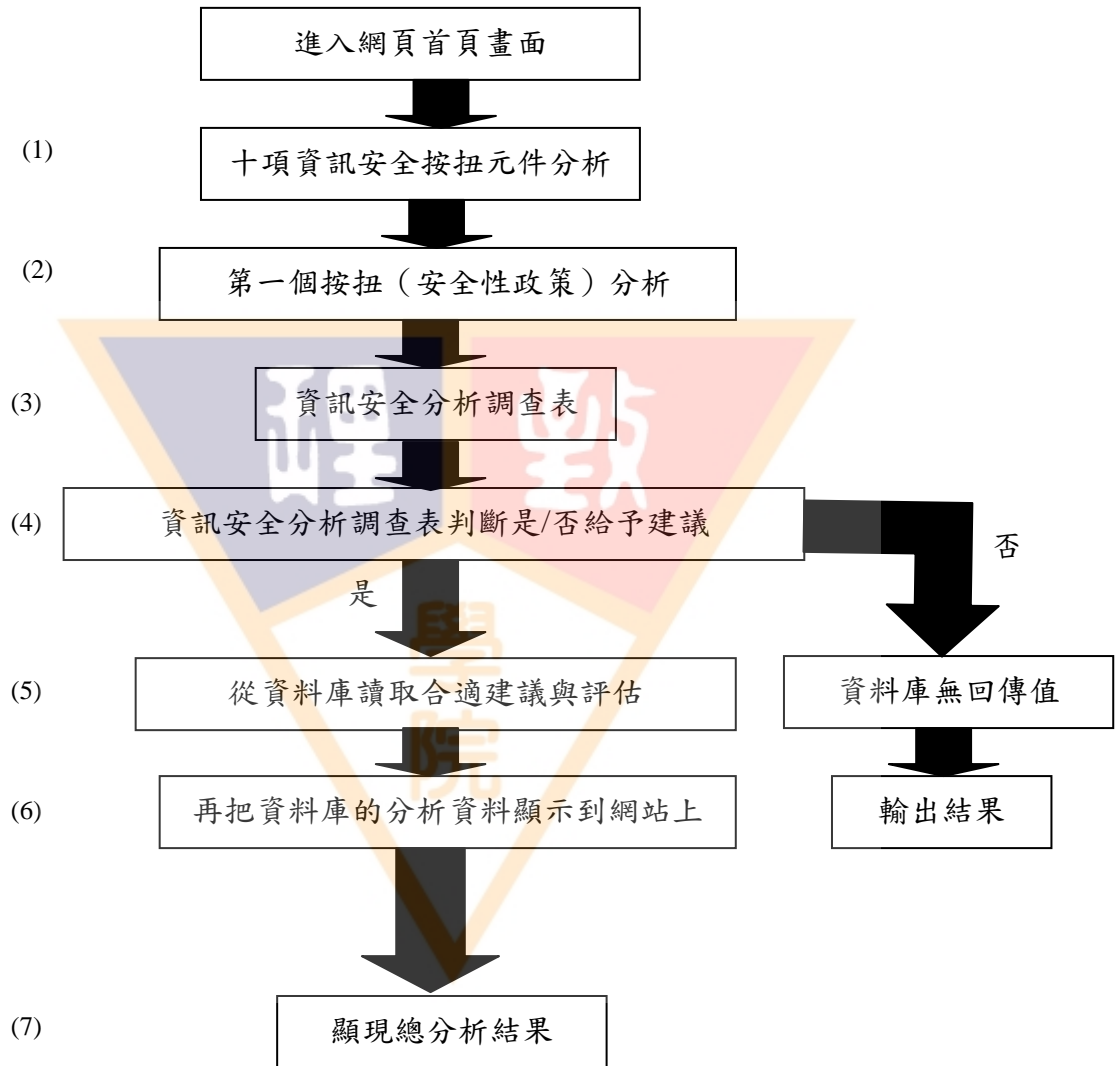


圖 3-2 資訊安全分析評估網站流程圖之安全性政策

第一個按鈕資訊安全分析評估網站之安全性政策功能步驟說明：

- (1)顯示出一個圓餅圖從第一項到第十項的可以連結到下一頁各項的資訊安全分析調查表。
- (2)按下 Flash 互動式按鈕進入資訊安全分析調查表裡面做分析。
- (3)國內外的組織或個人所面臨到一些常見到有關資訊安全的安全性政策的困難。
- (4)建立資料庫與網頁資訊安全調查表的連線請求，由使用者勾選的選項來判斷出資料庫是否給予分析。假如是的話從資訊安全分析調查表請求資料庫裡面所分析，排序，整合所有的問題發現到有需要回應分析資訊安全分析調查表。否的話就沒有顯示網頁上。
- (5)讀取的裡面適合的資料庫分析建議與風險等級圖。
- (6)所有問題的資料分析調查表的建議與補充都會依序問題的輕重排列顯示在網頁上面。
- (7)從資訊安全分析調查表請求資料庫裡面所分析，排序，整合所有的問題無需要回應分析資訊安全分析調查表。

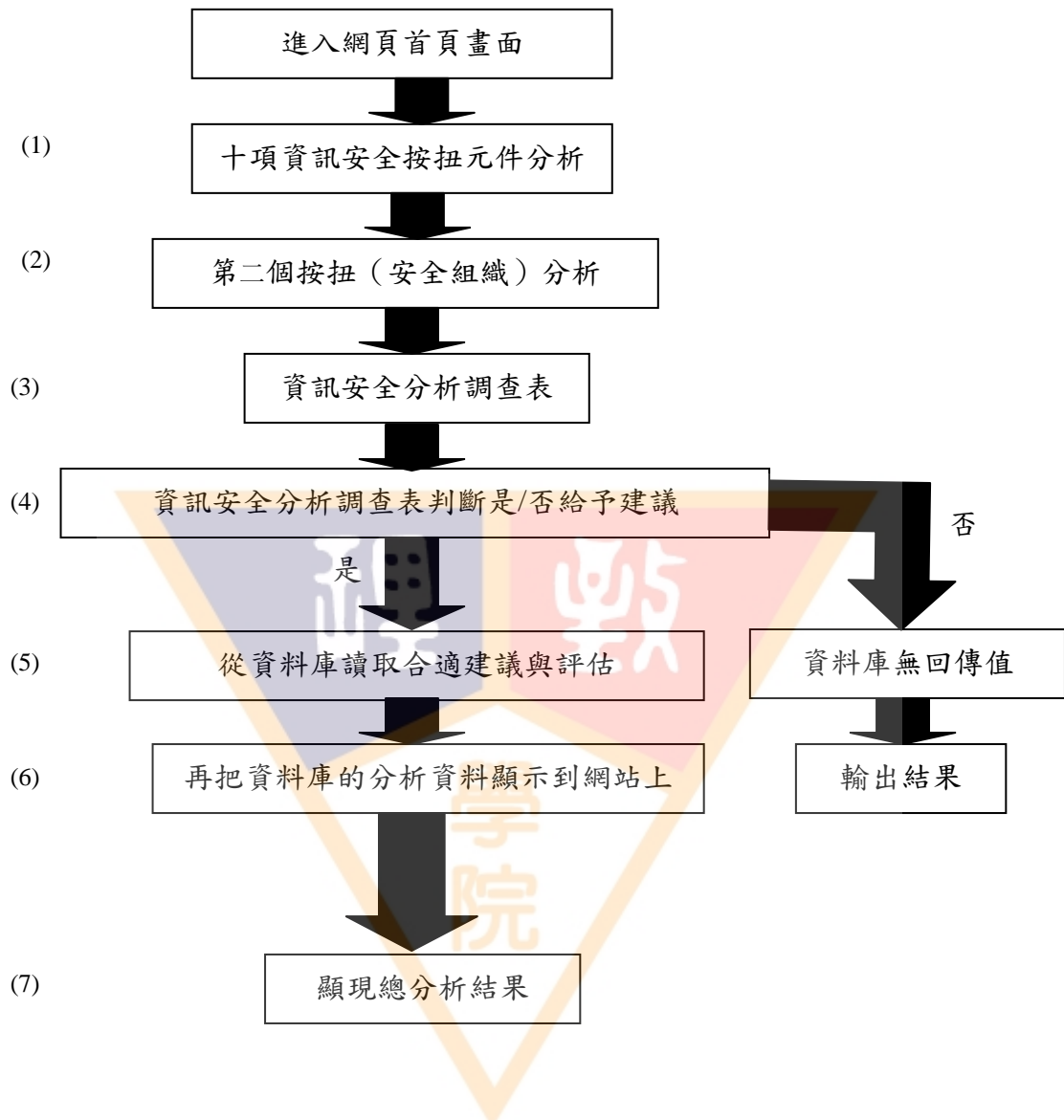


圖 3-3 資訊安全分析評估網站流程圖之安全組織

第二個按鈕資訊安全分析評估網站之安全組織功能步驟說明：

- (1)顯示出一個圓餅圖從第一項到第十項的可以連結到下一頁各項的資訊安全分析調查表。
- (2)按下 Flash 互動式按鈕進入資訊安全分析調查表裡面做分析。
- (3)國內外的組織或個人所面臨到一些常見到有關資訊安全的安全性政策的困難。
- (4)建立資料庫與網頁資訊安全調查表的連線請求，由使用者勾選的選項來判斷出資料庫是否給予分析。假如是的話從資訊安全分析調查表請求資料庫裡面所分析，排序，整合所有的問題發現到有需要回應分析資訊安全分析調查表。否的話就沒有顯示網頁上。
- (5)讀取的裡面適合的資料庫分析建議與風險等級圖。
- (6)所有問題的資料分析調查表的建議與補充都會依序問題的輕重排列顯示在網頁上面。
- (7)從資訊安全分析調查表請求資料庫裡面所分析，排序，整合所有的問題無需要回應分析資訊安全分析調查表。

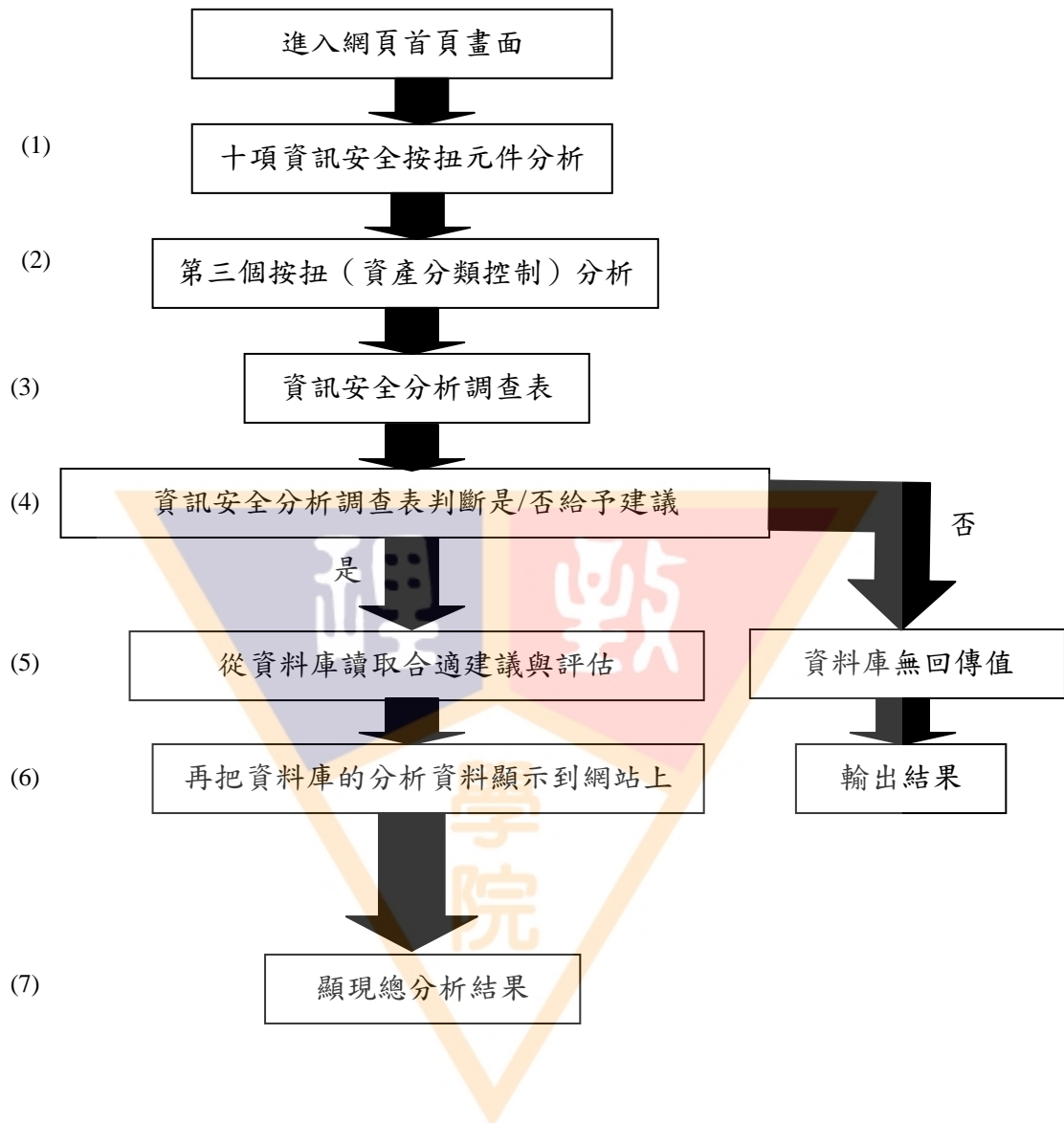


圖 3-4 資訊安全分析評估網站流程圖之資產分類控制

第三個按鈕資訊安全分析評估網站之資產分類控制功能步驟說明：

- (1)顯示出一個圓餅圖從第一項到第十項的可以連結到下一頁各項的資訊安全分析調查表。
- (2)按下 Flash 互動式按鈕進入資訊安全分析調查表裡面做分析。
- (3)國內外的組織或個人所面臨到一些常見到有關資訊安全的安全性政策的困難。
- (4)建立資料庫與網頁資訊安全調查表的連線請求，由使用者勾選的選項來判斷出資料庫是否給予分析。假如是的話從資訊安全分析調查表請求資料庫裡面所分析，排序，整合所有的問題發現到有需要回應分析資訊安全分析調查表。否的話就沒有顯示網頁上。
- (5)讀取的裡面適合的資料庫分析建議與風險等級圖。
- (6)所有問題的資料分析調查表的建議與補充都會依序問題的輕重排列顯示在網頁上面。
- (7)從資訊安全分析調查表請求資料庫裡面所分析，排序，整合所有的問題無需要回應分析資訊安全分析調查表。

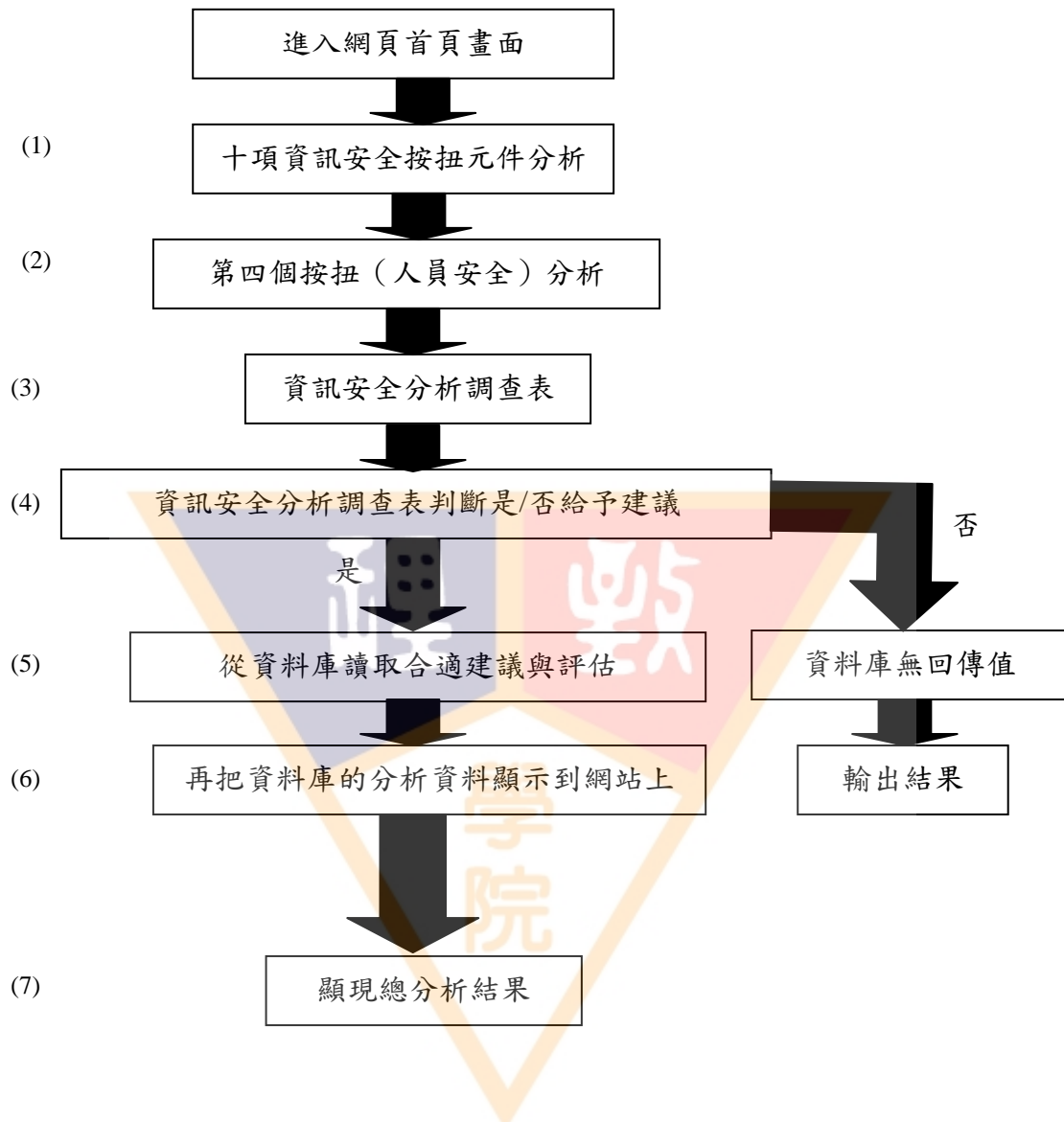


圖 3-5 資訊安全分析評估網站流程圖之人員安全

第四個按鈕資訊安全分析評估網站之人員安全功能步驟說明：

- (1)顯示出一個圓餅圖從第一項到第十項的可以連結到下一頁各項的資訊安全分析調查表。
- (2)按下 Flash 互動式按鈕進入資訊安全分析調查表裡面做分析。
- (3)國內外的組織或個人所面臨到一些常見到有關資訊安全的安全性政策的困難。
- (4)建立資料庫與網頁資訊安全調查表的連線請求，由使用者勾選的選項來判斷出資料庫是否給予分析。假如是的話從資訊安全分析調查表請求資料庫裡面所分析，排序，整合所有的問題發現到有需要回應分析資訊安全分析調查表。否的話就沒有顯示網頁上。
- (5)讀取的裡面適合的資料庫分析建議與風險等級圖。
- (6)所有問題的資料分析調查表的建議與補充都會依序問題的輕重排列顯示在網頁上面。
- (7)從資訊安全分析調查表請求資料庫裡面所分析，排序，整合所有的問題無需要回應分析資訊安全分析調查表。

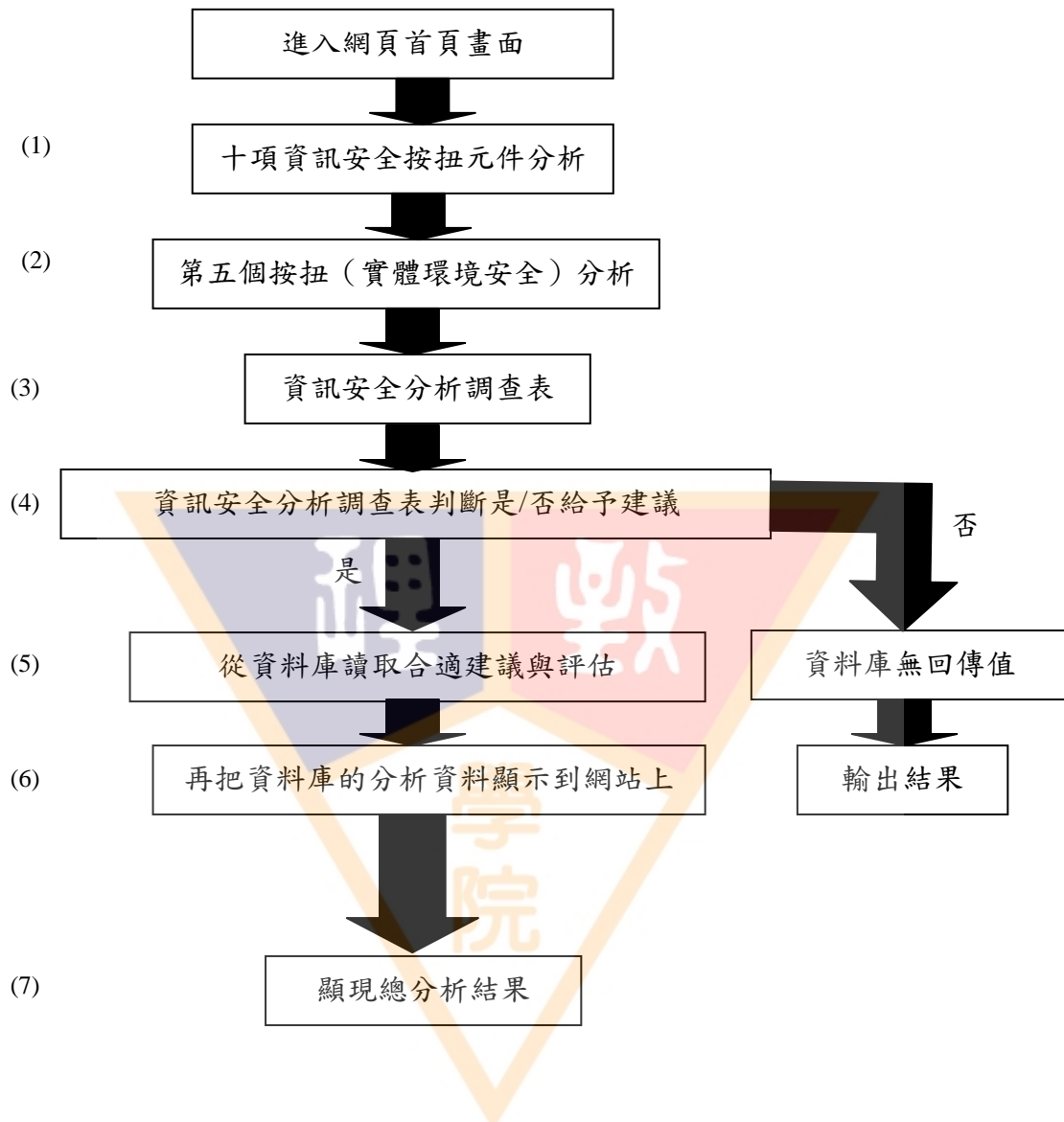


圖 3-6 資訊安全分析評估網站流程圖之實體環境安全

第五個按鈕資訊安全分析評估網站之實體環境安全功能步驟說明：

- (1)顯示出一個圓餅圖從第一項到第十項的可以連結到下一頁各項的資訊安全分析調查表。
- (2)按下 Flash 互動式按鈕進入資訊安全分析調查表裡面做分析。
- (3)國內外的組織或個人所面臨到一些常見到有關資訊安全的安全性政策的困難。
- (4)建立資料庫與網頁資訊安全調查表的連線請求，由使用者勾選的選項來判斷出資料庫是否給予分析。假如是的話從資訊安全分析調查表請求資料庫裡面所分析，排序，整合所有的問題發現到有需要回應分析資訊安全分析調查表。否的話就沒有顯示網頁上。
- (5)讀取的裡面適合的資料庫分析建議與風險等級圖。
- (6)所有問題的資料分析調查表的建議與補充都會依序問題的輕重排列顯示在網頁上面。
- (7)從資訊安全分析調查表請求資料庫裡面所分析，排序，整合所有的問題無需要回應分析資訊安全分析調查表。

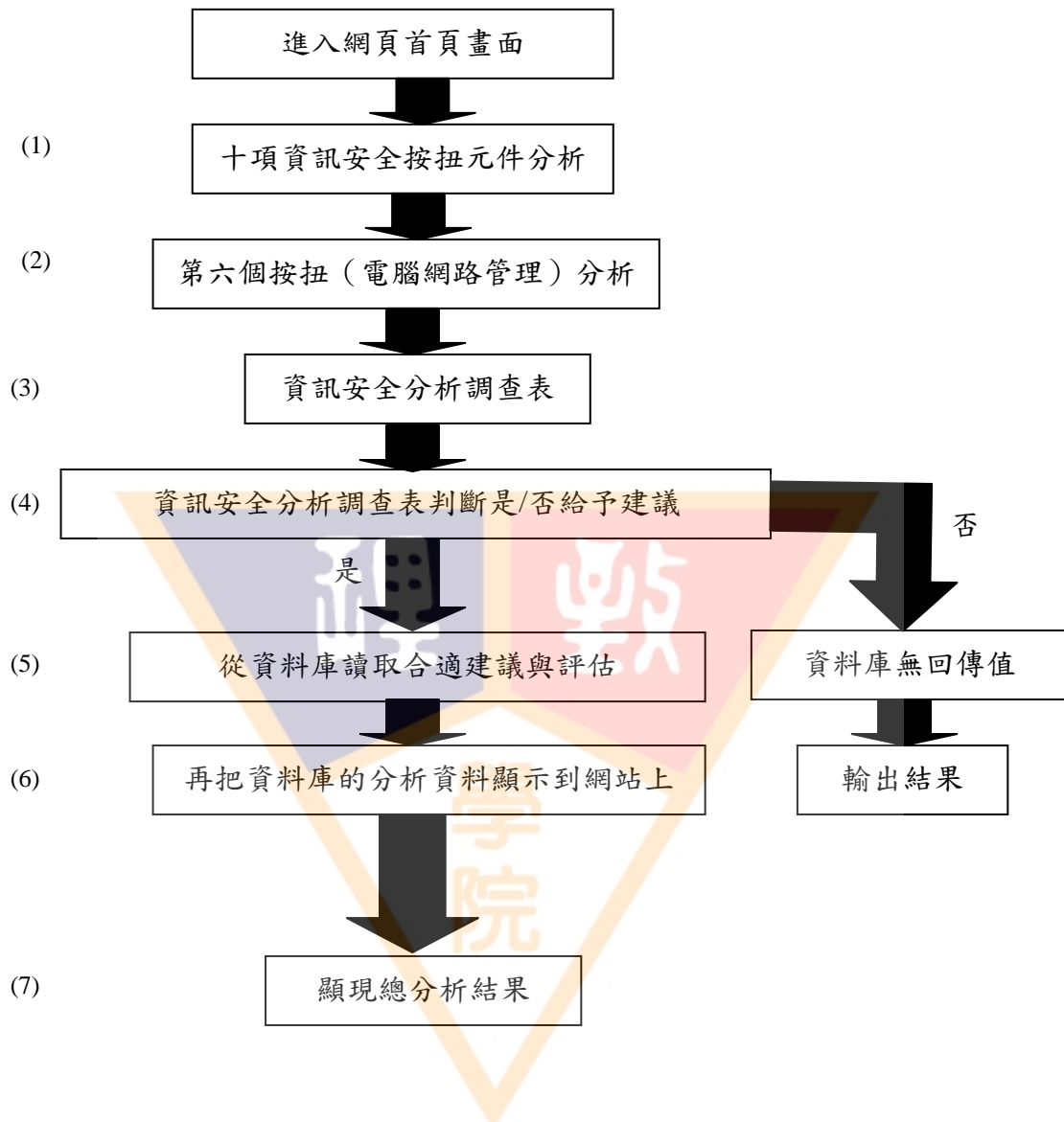


圖 3-7 資訊安全分析評估網站流程圖之電腦網路管理

第六個按鈕資訊安全分析評估網站之電腦網路管理功能步驟說明：

- (1)顯示出一個圓餅圖從第一項到第十項的可以連結到下一頁各項的資訊安全分析調查表。
- (2)按下 Flash 互動式按鈕進入資訊安全分析調查表裡面做分析。
- (3)國內外的組織或個人所面臨到一些常見到有關資訊安全的安全性政策的困難。
- (4)建立資料庫與網頁資訊安全調查表的連線請求，由使用者勾選的選項來判斷出資料庫是否給予分析。假如是的話從資訊安全分析調查表請求資料庫裡面所分析，排序，整合所有的問題發現到有需要回應分析資訊安全分析調查表。否的話就沒有顯示網頁上。
- (5)讀取的裡面適合的資料庫分析建議與風險等級圖。
- (6)所有問題的資料分析調查表的建議與補充都會依序問題的輕重排列顯示在網頁上面。
- (7)從資訊安全分析調查表請求資料庫裡面所分析，排序，整合所有的問題無需要回應分析資訊安全分析調查表。

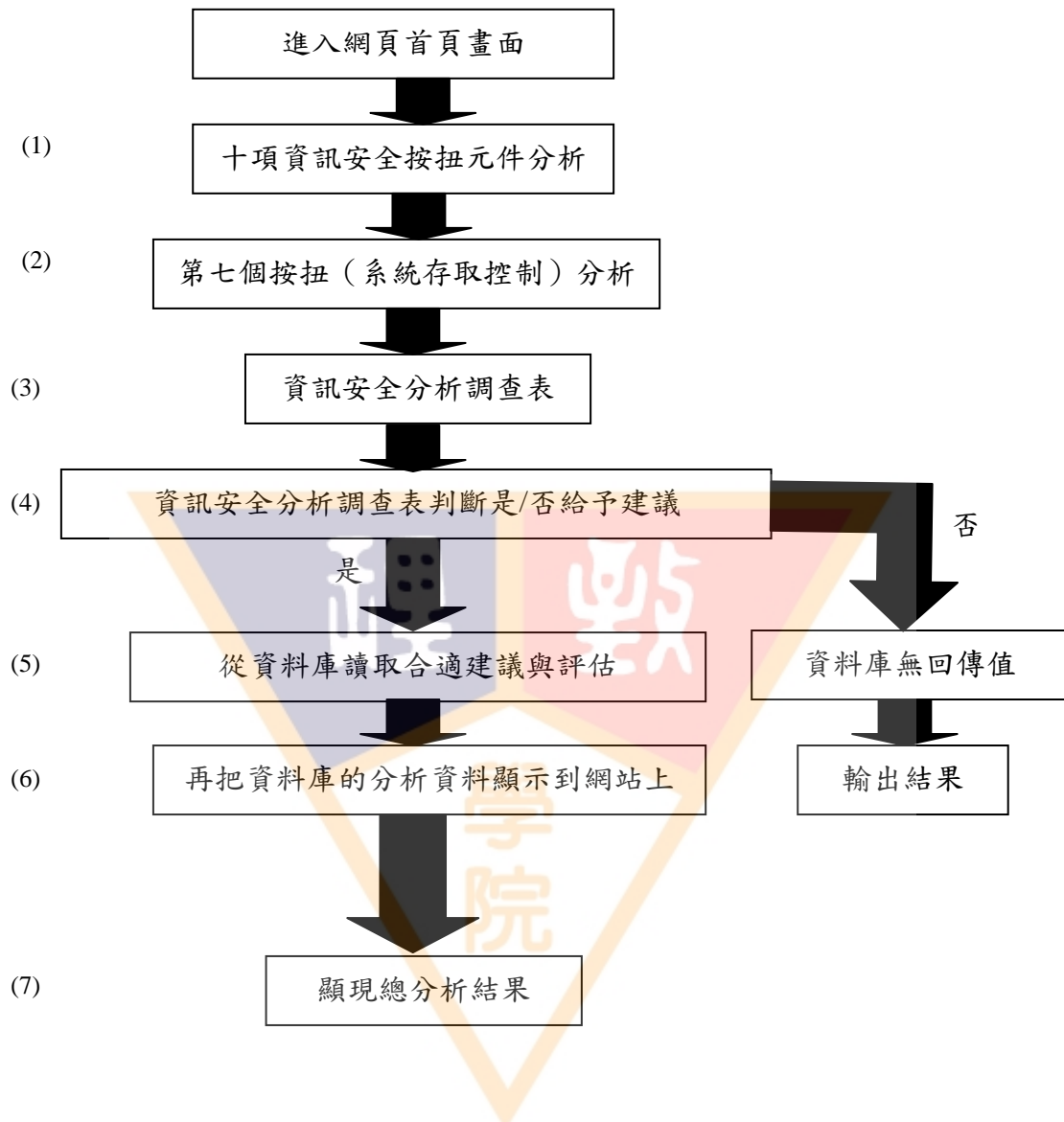


圖 3-8 資訊安全分析評估網站流程圖之系統存取控制

第七個按鈕資訊安全分析評估網站之系統存取控制功能步驟說明：

- (1)顯示出一個圓餅圖從第一項到第十項的可以連結到下一頁各項的資訊安全分析調查表。
- (2)按下 Flash 互動式按鈕進入資訊安全分析調查表裡面做分析。
- (3)國內外的組織或個人所面臨到一些常見到有關資訊安全的安全性政策的困難。
- (4)建立資料庫與網頁資訊安全調查表的連線請求，由使用者勾選的選項來判斷出資料庫是否給予分析。假如是的話從資訊安全分析調查表請求資料庫裡面所分析，排序，整合所有的問題發現到有需要回應分析資訊安全分析調查表。否的話就沒有顯示網頁上。
- (5)讀取的裡面適合的資料庫分析建議與風險等級圖。
- (6)所有問題的資料分析調查表的建議與補充都會依序問題的輕重排列顯示在網頁上面。
- (7)從資訊安全分析調查表請求資料庫裡面所分析，排序，整合所有的問題無需要回應分析資訊安全分析調查表。

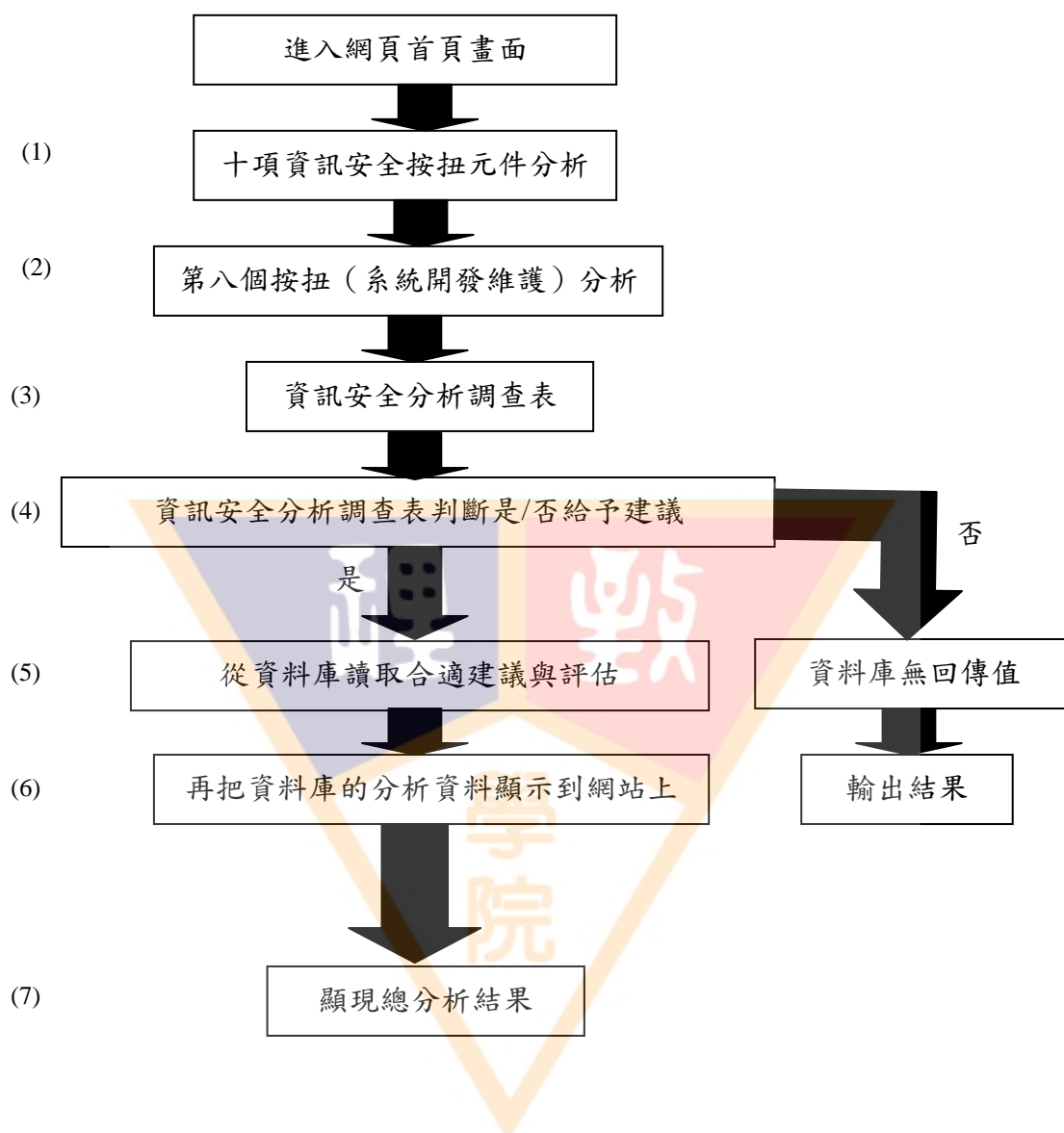


圖 3-9 資訊安全分析評估網站流程圖之系統開發維護

第八個按鈕資訊安全分析評估網站之系統開發維護功能步驟說明：

- (1)顯示出一個圓餅圖從第一項到第十項的可以連結到下一頁各項的資訊安全分析調查表。
- (2)按下 Flash 互動式按鈕進入資訊安全分析調查表裡面做分析。
- (3)國內外的組織或個人所面臨到一些常見到有關資訊安全的安全性政策的困難。
- (4)建立資料庫與網頁資訊安全調查表的連線請求，由使用者勾選的選項來判斷出資料庫是否給予分析。假如是的話從資訊安全分析調查表請求資料庫裡面所分析，排序，整合所有的問題發現到有需要回應分析資訊安全分析調查表。否的話就沒有顯示網頁上。
- (5)讀取的裡面適合的資料庫分析建議與風險等級圖。
- (6)所有問題的資料分析調查表的建議與補充都會依序問題的輕重排列顯示在網頁上面。
- (7)從資訊安全分析調查表請求資料庫裡面所分析，排序，整合所有的問題無需要回應分析資訊安全分析調查表。

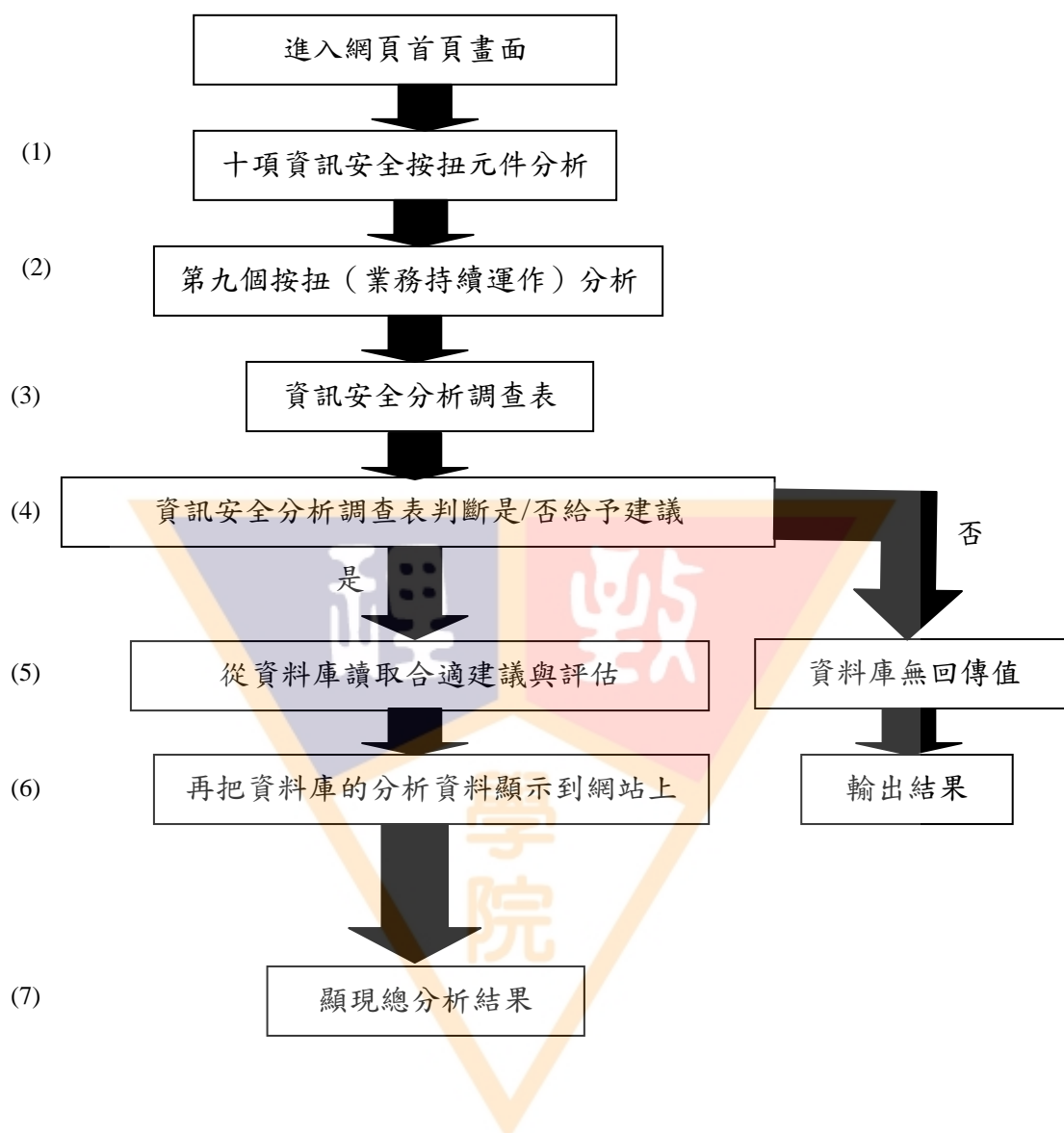


圖 3-10 資訊安全分析評估網站流程圖之業務持續運作

第九個按鈕資訊安全分析評估網站之業務持續運作功能步驟說明：

- (1)顯示出一個圓餅圖從第一項到第十項的可以連結到下一頁各項的資訊安全分析調查表。
- (2)按下 Flash 互動式按鈕進入資訊安全分析調查表裡面做分析。
- (3)國內外的組織或個人所面臨到一些常見到有關資訊安全的安全性政策的困難。
- (4)建立資料庫與網頁資訊安全調查表的連線請求，由使用者勾選的選項來判斷出資料庫是否給予分析。假如是的話從資訊安全分析調查表請求資料庫裡面所分析，排序，整合所有的問題發現到有需要回應分析資訊安全分析調查表。否的話就沒有顯示網頁上。
- (5)讀取的裡面適合的資料庫分析建議與風險等級圖。
- (6)所有問題的資料分析調查表的建議與補充都會依序問題的輕重排列顯示在網頁上面。
- (7)從資訊安全分析調查表請求資料庫裡面所分析，排序，整合所有的問題無需要回應分析資訊安全分析調查表。

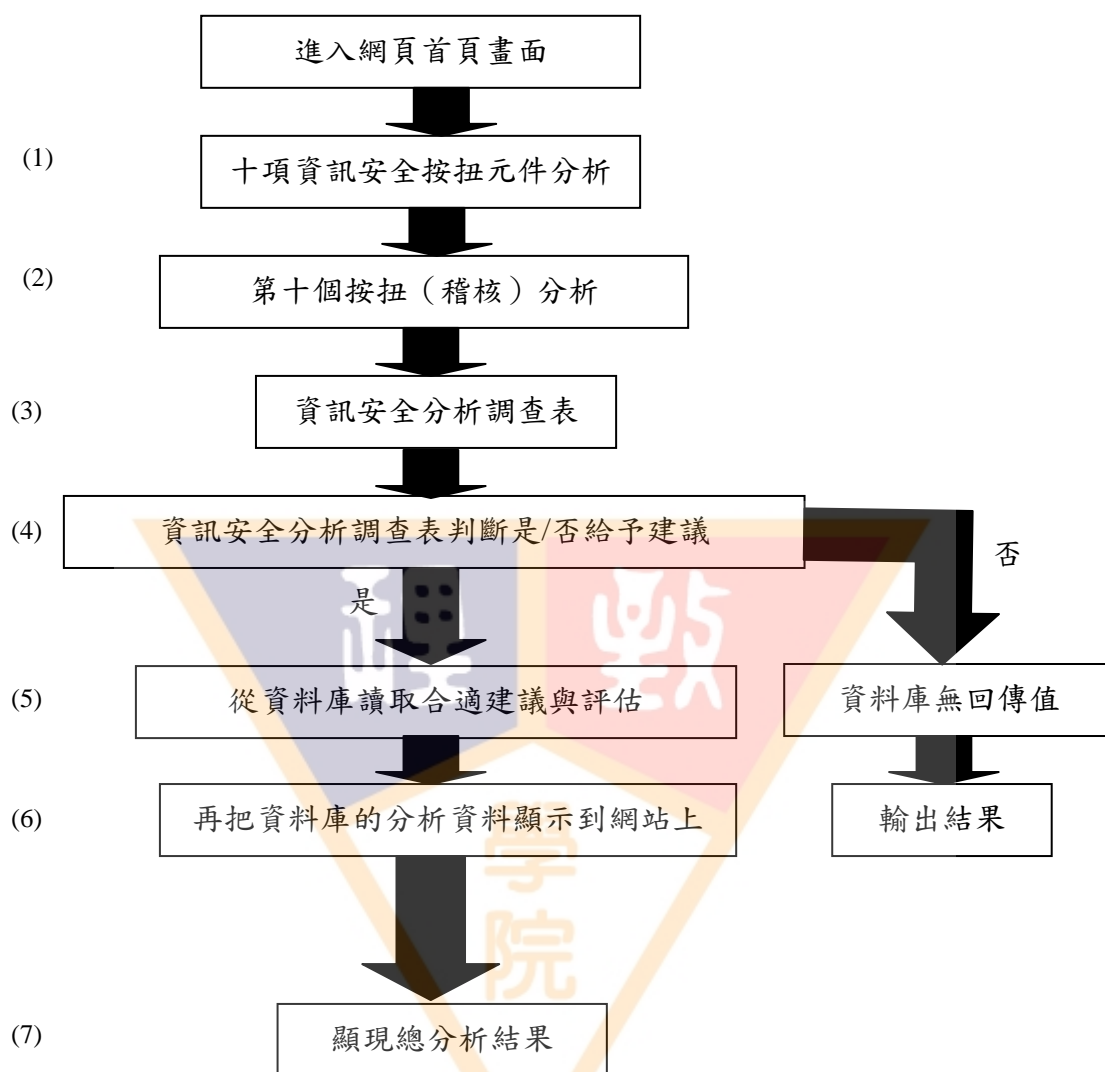


圖 3-11 資訊安全分析評估網站流程圖之稽核

第十個按鈕資訊安全分析評估網站之稽核功能步驟說明：

- (1)顯示出一個圓餅圖從第一項到第十項的可以連結到下一頁各項的資訊安全分析調查表。
- (2)按下 Flash 互動式按鈕進入資訊安全分析調查表裡面做分析。
- (3)國內外的組織或個人所面臨到一些常見到有關資訊安全的安全性政策的困難。
- (4)建立資料庫與網頁資訊安全調查表的連線請求，由使用者勾選的選項來判斷出資料庫是否給予分析。假如是的話從資訊安全分析調查表請求資料庫裡面所分析，排序，整合所有的問題發現到有需要回應分析資訊安全分析調查表。否的話就沒有顯示網頁上。
- (5)讀取的裡面適合的資料庫分析建議與風險等級圖。
- (6)所有問題的資料分析調查表的建議與補充都會依序問題的輕重排列顯示在網頁上面。
- (7)從資訊安全分析調查表請求資料庫裡面所分析，排序，整合所有的問題無需要回應分析資訊安全分析調查表。

本報告資訊安全分析網站總體分析功能操作流程如下：

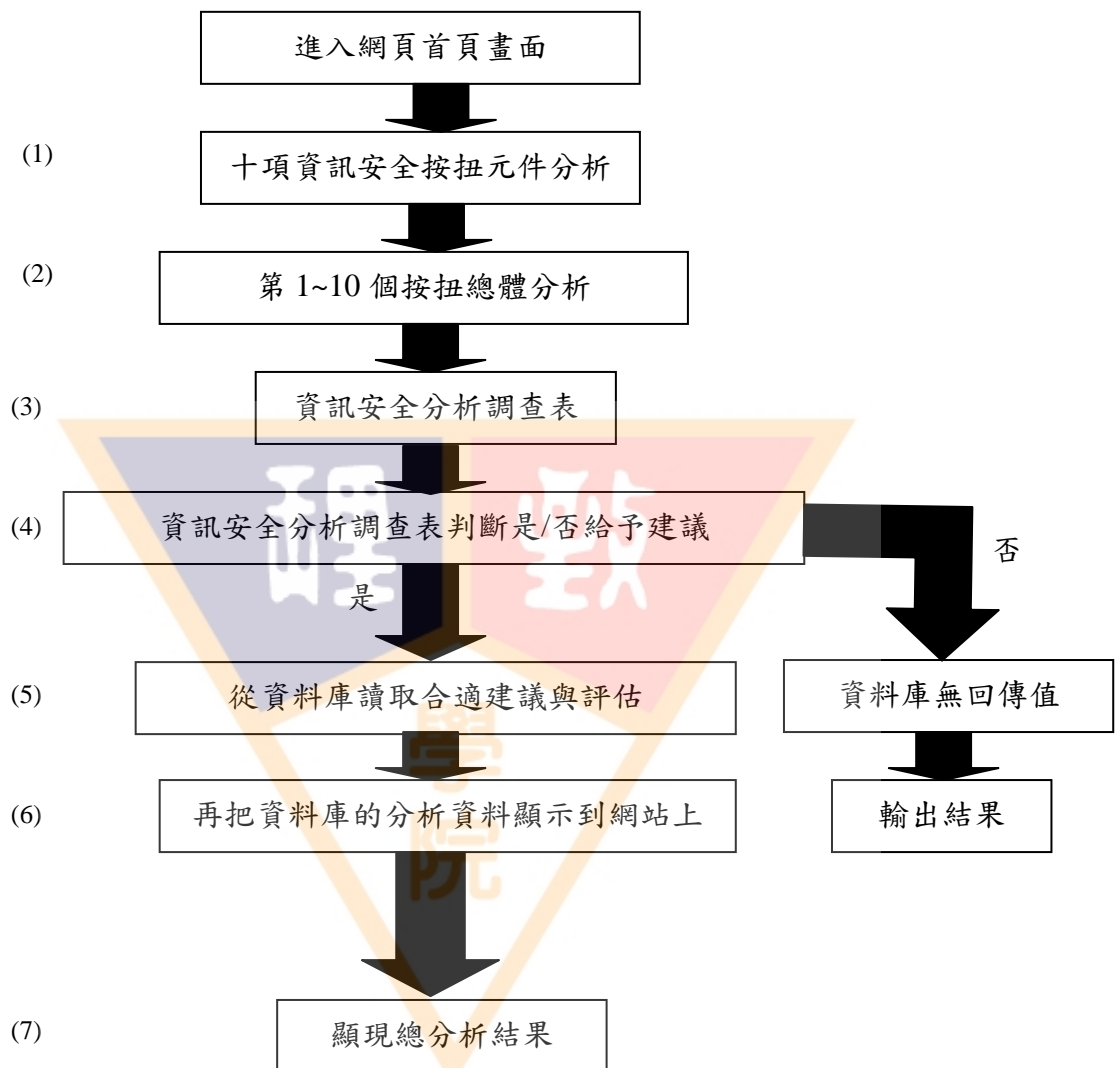


圖 3-12 資訊安全分析評估網站流程圖之總體分析

第 1~10 個按鈕資訊安全分析評估網站之總體分析功能步驟說明：

- (1)顯示出一個圓餅圖從第一項到第十項的可以連結到下一頁各項的資訊安全分析調查表。
- (2)按下 Flash 互動式按鈕進入資訊安全分析調查表裡面做分析。
- (3)國內外的組織或個人所面臨到一些常見到有關資訊安全的安全性政策的困難。
- (4)建立資料庫與網頁資訊安全調查表的連線請求，由使用者勾選的選項來判斷出資料庫是否給予分析。假如是的話從資訊安全分析調查表請求資料庫裡面所分析，排序，整合所有的問題發現到有需要回應分析資訊安全分析調查表。否的話就沒有顯示網頁上。
- (5)讀取的裡面適合的資料庫分析建議與風險等級圖。
- (6)所有問題的資料分析調查表的建議與補充都會依序問題的輕重排列顯示在網頁上面。
- (7)從資訊安全分析調查表請求資料庫裡面所分析，排序，整合所有的問題無需要回應分析資訊安全分析調查表。

第肆章 資訊安全分析網站呈現

本報告資訊安全分析網站呈現如下：

第一節 資訊安全分析網站之各別分析畫面呈現

一、資訊安全分析系統之安全政策畫面呈現

(1)點選首頁的 SKIP 進入資訊安全分析系統，如圖 4-1。

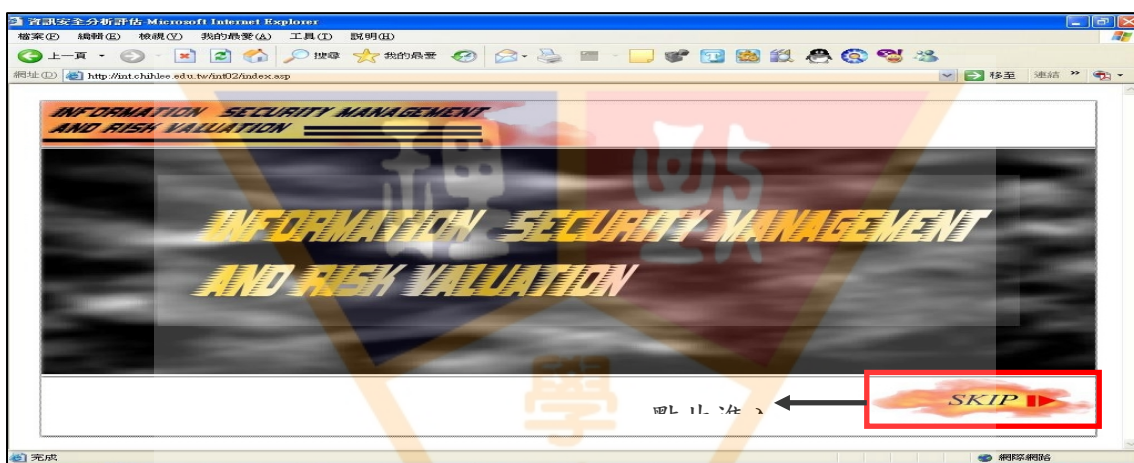


圖 4-1 資訊安全分析評估網站首頁

(2)點選首頁進入後會有十個資訊安全項目點選第一個安全政策，進行該項相關的資訊安全分析，如圖 4-2。

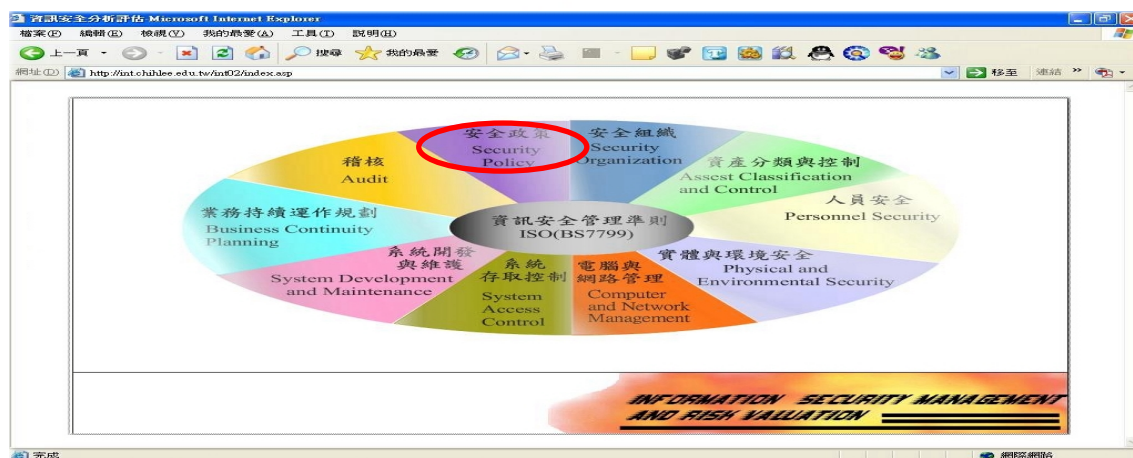


圖 4-2 資訊安全十個類別(點選安全政策)

(3)進入安全政策的分析項目，勾選組織安全政策內所無達成的選項，點選分析該項目按鈕進行分析，如圖 4-3。

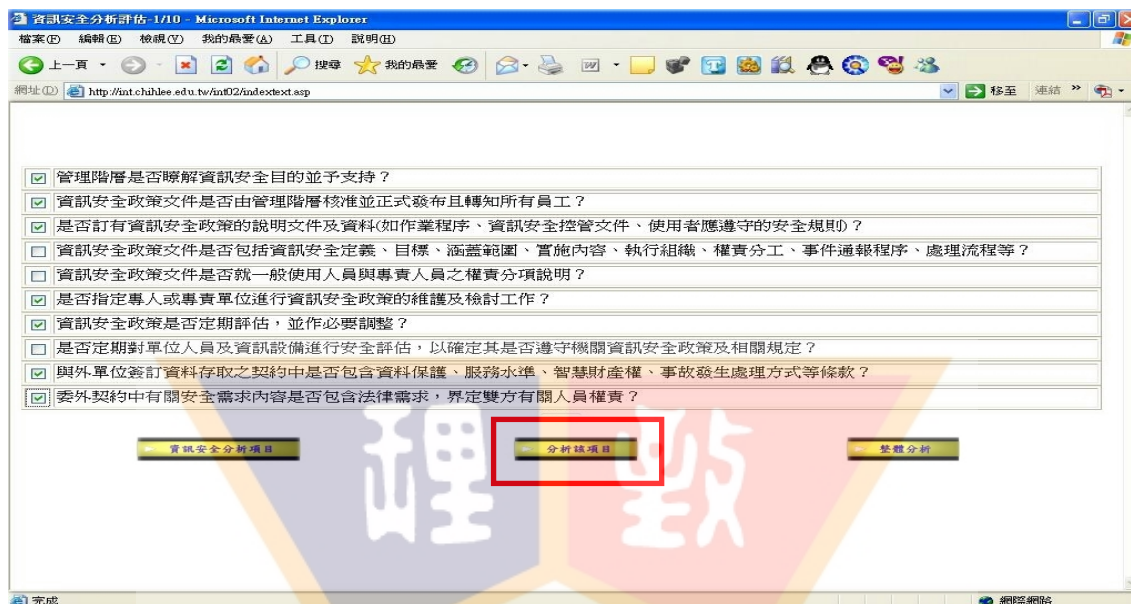


圖 4-3 資訊安全之安全政策相關分析內容

(4)按分析該項目按鈕後，得到分析建議與風險評估圖，如圖 4-4。

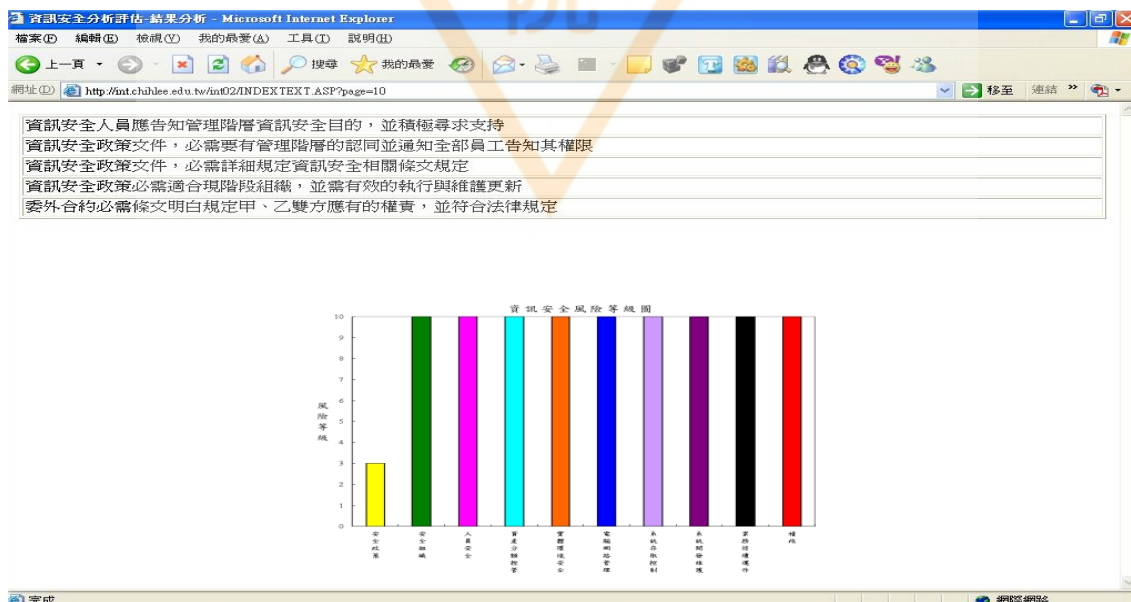


圖 4-4 資訊安全之安全政策分析結果暨風險等級

二、資訊安全分析系統之安全組織畫面呈現

(1)點選首頁的 SKIP 進入資訊安全分析系統，如圖 4-5。



圖 4-5 資訊安全分析評估網站首頁

(2)點選首頁進入後會有十個資訊安全項目點選第二個安全組織，進行該項相關的資訊安全分析，如圖 4-6。

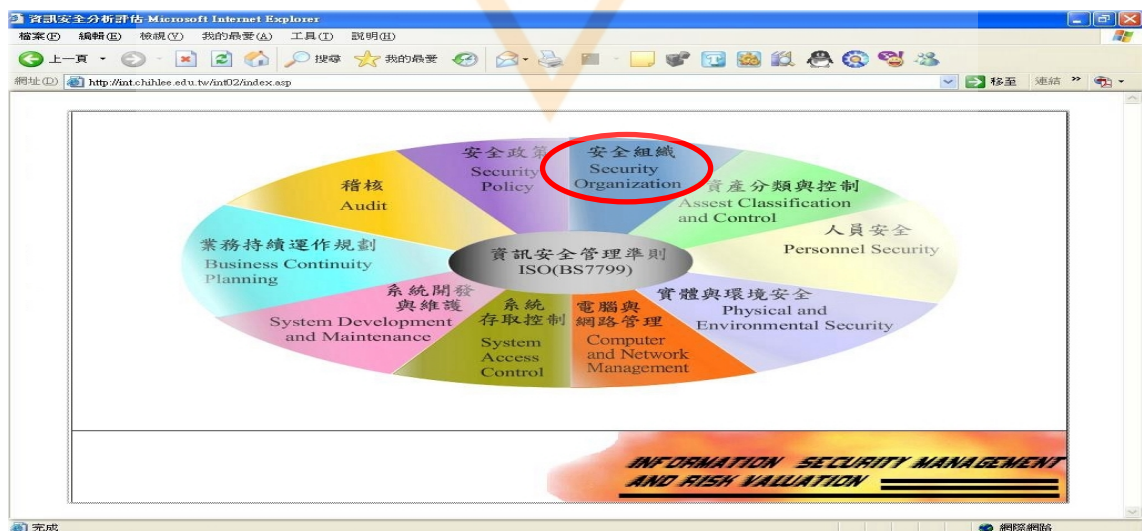


圖 4-6 資訊安全十個項目(點選安全組織)

(3)進入安全組織的分析項目，勾選組織安全政策內所無達成的選項，點選分析該項目按鈕進行分析，如圖 4-7。

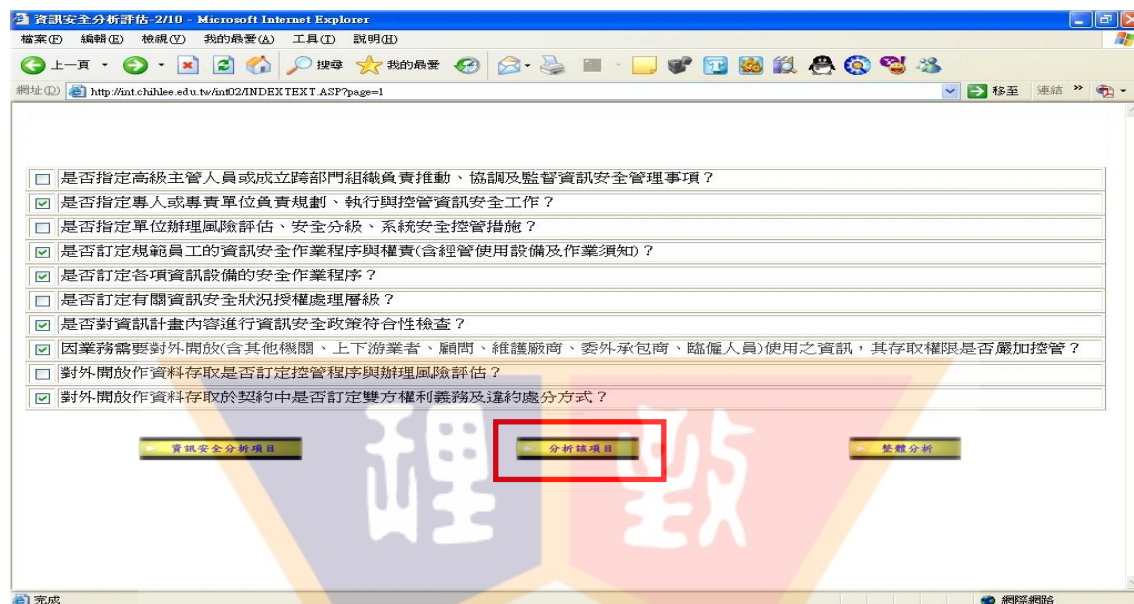


圖 4-7 資訊安全之安全組織相關分析內容

(4)按分析該項目按鈕後，得到分析建議與風險評估圖，如圖 4-8。

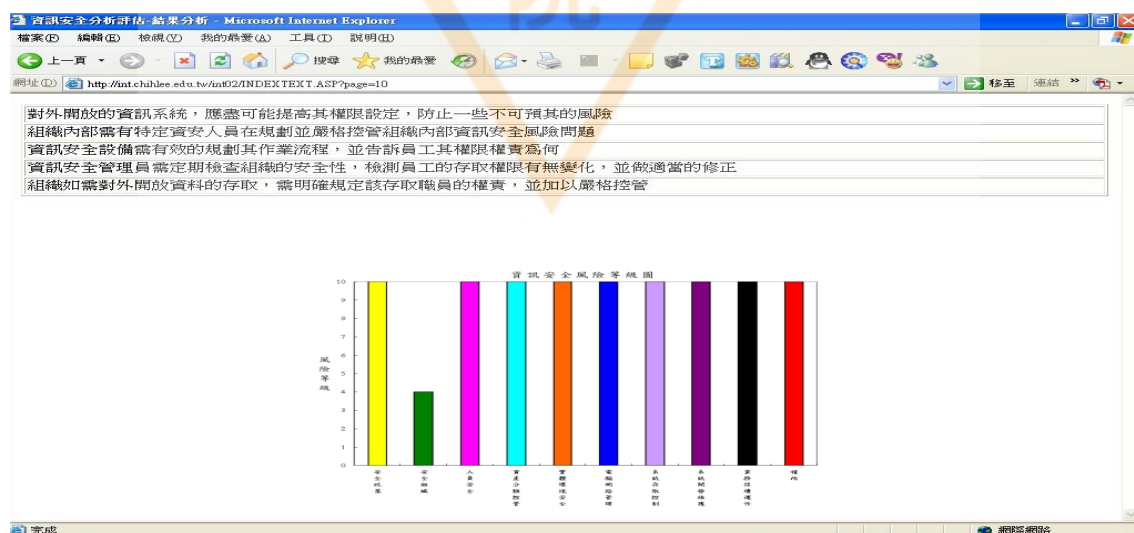


圖 4-8 資訊安全之安全組織分析結果暨風險等級

其於八個項目系統畫面如前兩點所示，在此省略。

第二節 資訊安全分析網站之整體分析畫面呈現

(1)點選首頁的 SKIP 進入資訊安全分析系統，如圖 4-9。



圖 4-9 資訊安全分析評估網站首頁

(2)點選首頁進入後會有十個資訊安全項目依序點選並進行該項相關的資訊安全分析，如圖 4-10。



圖 4-10 資訊安全十個項目

(3)進入各分析項目，勾選組織內所無達成的選項，點選整體分析按鈕進行分析，如圖 4-11。

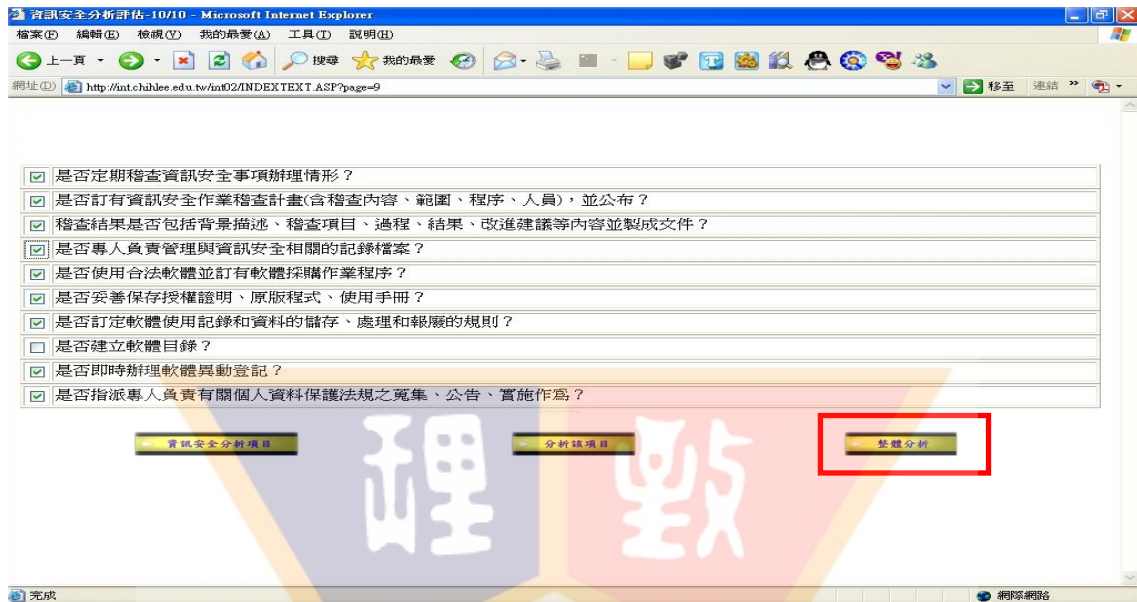


圖 4-11 資訊安全分析項目內容之一

(4)按整體分析按鈕後，得到分析建議與風險評估圖，如圖 4-12~4-14。

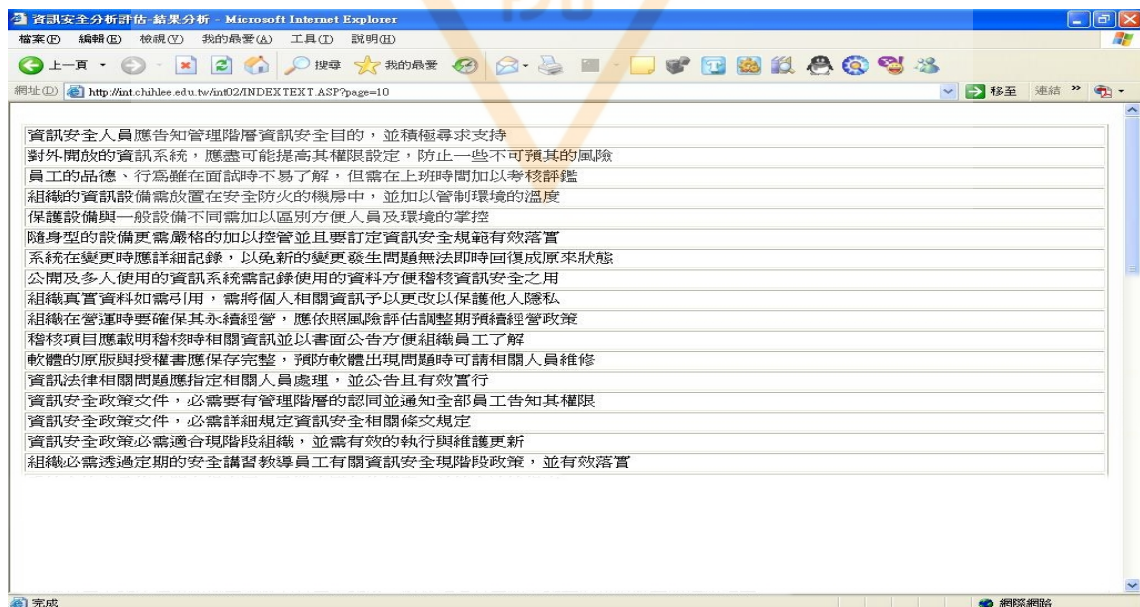


圖 4-12 資訊安全整體分析暨整體風險等級(1)

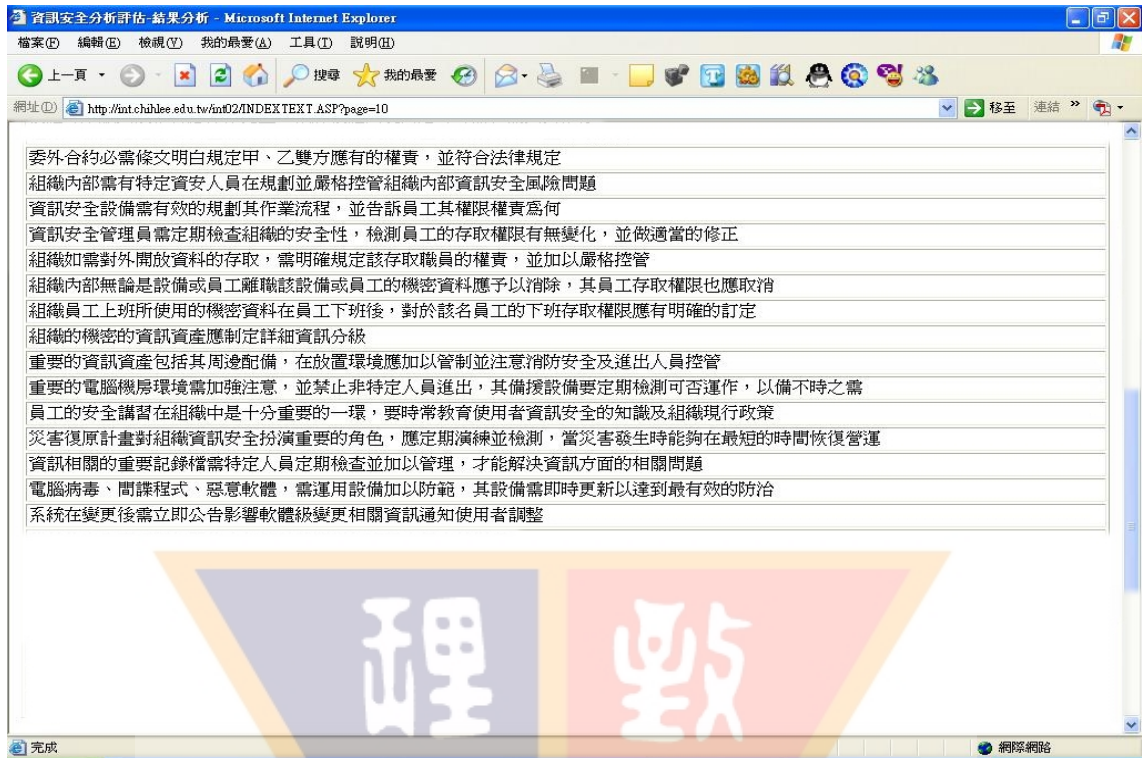


圖 4-13 資訊安全整體分析暨整體風險等級(2)

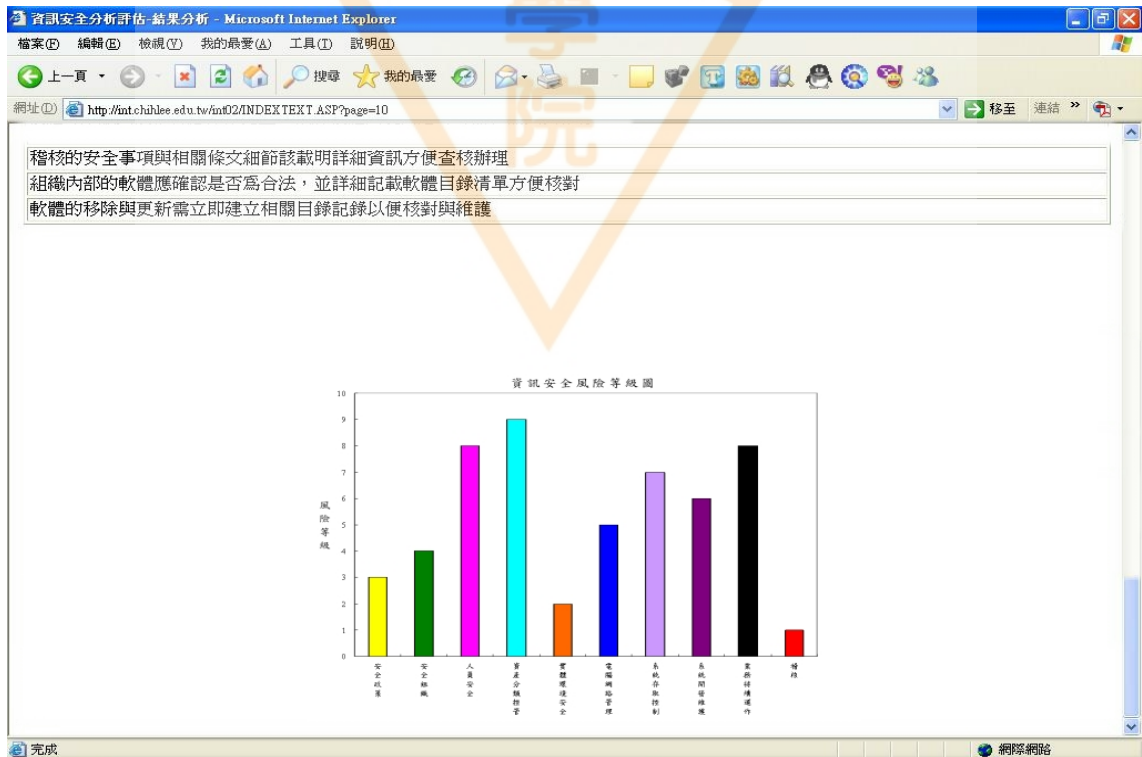


圖 4-14 資訊安全整體分析暨整體風險等級(3)

第五章 結論與建議

鑑於資訊科技的訊速發展，資訊安全的重要性也是日漸重要，然而現今的攻擊模式與攻擊手法較以往先進，並讓許多系統管理人員渾然不知自身已遭受攻擊，等到事件擴大時，通常已造成無法收拾的局面，相對的組織與政府已有相當可觀的損失。

許多資訊安全人員有很多的資訊安全想法，但往往受限於組織主管的不支持，組織其它部門的不配合的狀況下，導致組織有出現資訊安全漏洞，成為一個資訊安全危險環境，因此資訊安全所面對的主要攻擊與入侵並不是外來的攻擊，而是組織內部人員的人為因素，如何控管內部人員，變成是組織資訊安全政策中重要的一環。

由於現今資訊安全發展的趨勢，本報告探討的並不是資訊安全的攻防戰，而是如何預防來襲的資訊安全問題。經由資料的搜集，我們了解現今各國或相關組織，為了維護並具確保組織資訊安全，均訂立有相關的管理規範。經過研究與探討，英國國家標準協會(BSI)所制訂的 BS7799 資訊安全管理規範，其針對現金資訊安全所應注意的事項及曾經發生的事故制訂出標準，包含組織在資訊安全管理所有的層面，因此本報告以 BS7799 為基本架構，與最新資訊安全技術，來完成此報告，希望能對組織資訊安全工作少許的貢獻。

本報告運用資訊安全管理規範 BS7799 為基本架構，與國內資訊安全技术，業界的案例，經過本報告的探討獲得了幾項成果。

一、資訊安全的趨勢與發展重要性

資訊安全的是資訊發達的二十一世紀，不能忽略相當重要的一種觀念與計畫，不管是資訊安全的攻擊或資訊安全的防禦，相互成長沒有極限，雖然不能百分之百的解決資訊安全的問題，因為外在的影響因素太多，但能做的就是預防資訊安全問題發生，並有因應的計畫，爭取時間，將資訊安全影響的程度降到最低。

二、以 BS7799 所建立的分析網站的重要性

英國國家標準局的資訊安全規範 BS7799 基本的了解，並運用 BS7799 的資訊安全規範建立資訊安全分析網站，得知此一規範如何訂定組織與政府的資訊安全，利用相關的十大控制項目來管理資訊安全，使資訊安全能夠達到一定的水準。

三、ITDR(IT Disaster Recovery)災害復原計畫的重要性

許多組織都會有規劃當資訊安全危機發生時，將要如何解決，但並沒有達到一個有效的執行。本報告運用 ITDR(IT Disaster Recovery)災害復原計畫，幫助組織制訂有效的資訊安全復原計畫，並定期演練與測試是否符合現階段的組織環境所需，期望能在組織面對資訊安全危機後，能

在最短的時間恢復正常營運。

四、由資訊安全分析表了解資訊安全執行的困難處

資訊安全的好與壞，在組織與政府中，不是取決於資訊安全人員，而是組織與政府裡的全體人員，主管階層需全面了解資訊安全政策，並全力配合，公司各部門的員工必需隨時提出建議，供資訊安全人員的參考，使其了解公司人員需要的是什麼，但往往這些最基本的，通常都被忽略，只是拼命用金錢築一道資訊安全的牆，終就還是會倒塌。

五、資訊安全風險的重要性

資訊安全問題要如何的預防，取決於之前的風險認定，但風險的認定往往在組織與政府裡都時常上下不同調，要如何界定風險、何為風險，並了解真正的資訊安全的風險，與其發生所帶來的影響與損害，才是資訊安全最根本之道。

資訊安全從以往的微不足道，躍進到今日舉足輕重的地位，實在是要感謝資訊科技的發達，與資訊界兩大勢力的對抗 Black Hacker 與 White Hacker，使資訊安全成為一個廣大的市場，各資訊科技公司相爭之地。

本報告對於資訊安全方面的探討不盡完善，但在資訊安全方面也有相當的了解，因此在報告最後提出幾點建議，與未來報告方向以供參考。

本報告對於資訊安全的建議，有下列幾點：

- (1)對於資訊安全的觀念不要一味只是在探討攻擊手法，其實真正的資訊安全必需注重的是一個良好的規範。
- (2)資訊安全攻擊的日新月異，災害復原計畫雖然不能完全有效的防範新攻擊，但卻可以在第一時間將組織的資訊資產的損失降到最低，並在最短的時間恢復營運。
- (3)資訊安全真正好的防禦，並不是誰了解的攻擊手法比較多，而是當資訊安全發生的時候，能夠用空間換取更多的時間，來處理並解決資訊安全的問題。
- (4)資訊安全真正的主要的攻擊並不是來自於外在，而是來自組織內部人員對資訊安全的不了解，與組織沒有相當的規範來規定資訊安全。
- (5)國內對於資訊安全的法律規定不完全，造成許多資訊安全案件無法得到有效的判決，因此需參考國外的資訊安全相關法律，對資訊安全相關法律條文做更嚴謹的制訂。

本報告未來的研究方向有下列幾點：

- (1)更深入了解 BS7799 規範，探討一個良好的資訊安全規範是如何形成，並比較各國的資訊安全規範。
- (2)資訊安全法律的不完善，組織應如何面對與處理。
- (3)資訊安全的設備與程式各國均有所發展，在專利上將會有明顯的爭取，須適時的了解反托拉斯法來保障自身權益。
- (4)由於資訊科技的發達，未來戰爭不免會有資訊戰的發生，如何預防將成為各國政府資訊安全的重點。
- (5)資訊安全的攻擊手法層出不窮，如何在建立更完善更深入的資訊安全風險管理系統，也是重要課題。

參考文獻

1. ACM SIGSAC (ACM Special Interest Group on Security , Audit and Control) , <http://www.acm.org/sigsac/>
2. ACSA (Applied Computer Security Associates) ,
<http://www.acsac.org/acsa/>
3. AVAR , (Association of Anti Virus Asia Researchers) , 亞洲防毒研究協會 , <http://www.avar.org/>
4. CERT/CC(Coordination Center , CERT 是 Computer Emergency Response Team) , 可直譯為電腦安全緊急應變小組 ,
<http://www.cert.org/>
5. CSI (Computer Security Institute) , <http://www.gocsi.com/>
6. EPIC(Electronic Privacy Information Center) ,
<http://www.epic.org/security/>
7. FIRST(Forum of Incident Response and Security Teams) ,
<http://www.first.org/>
8. IACR and CRYPTO , EUROCRYPT , ASIACRYPT
(International Association of Cryptographic Research) ,
<http://www.iacr.org/>
9. NSI(National Security Institute) , <http://www.nsi.org/>
10. NSS , <http://www.nss.co.uk>
11. SANS(System Administration , Networking and Security) ,
<http://www.sans.org/>

12. UCL Crypto Group , <http://www.dice.ucl.ac.be/Crypto/index.Shtml>
13. CCISA (Chinese Cryptology and Information Security Association) , 中華民國資訊安全協會 , <http://www.cccisa.org.tw>
14. NECRT , 國家資通安全應變中心 , <http://www.ncert.nat.gov.tw/>
15. NICST (National Information & Communication Security Taskforce) , 行政院國家資通安全會報 , <http://www.nicst.sat.gov.tw/>
16. STIC , 行政院國家科學委員會科學技術資料中心 , <http://www.stic.gov.tw/>
17. ACM Transactions on Information and System Security , <http://www.acm.org/tissec/>
18. Computers and Security , <http://www.compseconline.com>
19. Cryptologia , <http://www.dean.usma.edu/math/pubs/cryptologia/>
20. 兩大金控資訊長的危機管理心法 , <http://www.bnext.com.tw/meg/20040515/200405152254.html>
21. 管理技術分析 , <http://www-8.ibm.com/services/tw/strategy/etk/publickey/html>
22. 網路金融資訊犯罪 , <http://www.fisc.com.tw/news/maz/34/p3-5b.asp>
23. 經濟部標準檢驗 , <http://www.bsim.gov.tw/page/security.sp?groupip=5>
24. 行政院文化建設委員會資訊安全政策 , <http://www2.ntcri.gov.tw/rule/secrule.htm>

25. Computer Associates，組合國際電腦股份有限公司
， <http://www.ca.com.tw/news/share/security/sasser 02.asp>
26. 全面杜絕內部網路的安全威脅，
<http://www.isecutech.com.tw/feature/view.asp?fid=234>
27. 台灣電腦網路危機處理中心， <http://www.cert.org.tw/>
28. 保存駭客入侵證據，
<http://www.shoppingguide.ithome.com.tw/interview/interview2004-06-24-001.html>
29. 國土安全計劃帶來的資安效應，
<http://www.isecutech.com.tw/feature/view.asp?fid=172>
30. 資料流程安全，
<http://www.public.boulder.ibm.com/tividd/td/itpme/sc23-1284-00/zhtw/html/p12plmst58.htm>
31. 內政部役政署資訊安全政策，
<http://www.nca.gov.tw/lns.htm>
32. 電腦系統安全管理， http://www.content.edu.tw/primary/info_educvsa/content/5/5-4.htm
33. 教育部資訊網，
<http://www.edu.tw/eduweb/edumgt/e00001/eduion001/private/safe-1.htm>
34. 網路安全認證服務，
<http://www.hitrust.com.tw/newsite/productsecurity.asp>

36.賽門鐵克公司，

<http://www.symantec.com.tw/>

37.趨勢科技股份有限公司，

<http://www.trendmicro.com.tw/home/enterprise.htm>

38.建華銀行資訊處與 BS7799，

<http://www.isecutech.com.tw/feature/view.asp?fid=6>

39.如何建立有效的安全政策，

<http://www.symantec.com/region/tw/enterprise/article/securitypolicy.html>

40.資訊安全管理系統，

<http://asie.bsi-global.com/taiwan+about/bsinews/peter+report/index.xalter>

41.國立交通大學資訊安全計畫，

http://www.cc.nctu.edu.tw/doc/manage_rule/nctu-sec.htm

42.資訊安全技術應用國際研討會，經濟部工業局，2001

43.資通安全概論，張真誠教授，2002

44.資通安全管理系統與稽核，樊國楨博士，2003

27.資訊安全能力評鑑，樊國楨博士，2002

28.資訊安全風險管理，樊國楨博士，2002

29.資訊安全「影響因素與評估模式」之研究，國立政治大學資訊管理學系博士學位論文，洪國興，2003

30.資安人雜誌，28期~35期，2006，紐奧良文化

附錄一 資訊安全風險等級表

風險等級	內容
<p>0 無</p>	<p>(1)組織未考慮安全的弱點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。</p> <p>(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。</p> <p>(3)管理單位不瞭解資訊作業或服務有哪些風險、弱點和威脅。</p>
<p>0~2 初步、特別狀況</p>	<p>(1)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。</p> <p>(2)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。</p>
<p>2~4 可重複，但仍靠直覺</p>	<p>(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，且仍改進中。</p> <p>(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，或有誤導的可能。</p> <p>(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。</p>

風險等級	內容
<p>4~6 已有程序</p>	<p>(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。</p> <p>(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。而非以業務運作為中心。有非常態性的入侵測試。</p> <p>(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雲星部署。重要系統及元件的清單非常嚴謹。</p>
<p>6~8 有管理、且可測量</p>	<p>(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。</p> <p>(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都根據特定的安全基準完成。安全教育簡報、使用者 ID、身份驗證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。</p> <p>(3)已施行服務不間斷的權責劃分及標準。系統備援作部署方法適當。</p>

風險等級	內容
<p>8~10 最適化</p>	<p>(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。</p> <p>(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驗證。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，收集有關新威脅和新弱點的資訊，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。</p> <p>(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。</p>

附錄二 文獻探討

資訊安全定義相關文獻探討

Gollmann (1999)電腦安全的定義：電腦安全在處理電腦系統的使用者之非授權行為的預防與發現。

任何電腦安全政策之廣義目標，必須能保護儲存於資訊系統中資料之機密性 (Confidentiality)、完整性 (Integrity) 與可用性 (Availability)，即所謂「C.I.A.」(Smith,1989；Schultz,2001；ISO/IEC 17799,2000；Chapmsn,1995；鄭信一,1999；Dhillon&Backhouse,2000；Gehrke,1992；Schneider&Gregory,1990；Finne,2000；吳瑞明,1994；陳同孝,1996；林鈴玉,2001；Ettinger,1993；Anderson,2003)：

- (1)機密性 (Confidentiality)：確保「資訊」之能被經過授權的人，才能存取。
- (2)完整性 (Integrity)：保證「資訊」和其「處理方法」的準確性與完整性。
- (3)可用性 (Availability)：確保經過授權的使用者，能存取「資訊」，並使用相關「資訊資產」。

依賴電腦系統的使用者，其軟體運作的表現如期所預期，則該系統即可稱之為「安全」(Simson&Gene,1991)。Von Solms 等 (1994) 認為資

訊安全的範疇包括：資訊安全政策、風險分析、風險管理、權變規劃（Contingency Planning）及災害復原(Disaster Recovery)等。運用可施行於資訊資源（硬體、軟體及資料）上之技術性防護方法及管理程序，期使組織所擁有的資產及個人隱私，均能受到保護(樊國楨與楊晉寧,1996)。

資訊安全就是保護任何與電腦有關的事務之安全，將管理程序與安全防護技術運用在硬體、軟體與資訊之中（黃亮宇,1992；Rusell&Gangemi,1992）。對組織而言，資訊是一種具有價值的重要商業資產，需妥善加以保護，以免受到各種威脅的攻擊，而維持組織營運的持續性，並使其可能發生損失降至最低（ISO/IEC 17799,2000）。

美國國防部發展的可信賴電腦系統評估準則（Trusted Computer System Evaluated Criterion；TCSEC,1985）指出：安全的系統應是藉由使用特別的安全功能，以對資訊的擷取加以控制，如：經過適當授權的個人或處理，才能讀、寫、新增或刪除資訊。美國國防部的「軍事及相關術語國防辭典」，對於資訊安全的定義為：保護資訊及資訊系統，以避免在儲存、處理或傳輸中的資訊遭受未經授權的存取或更改，且避免經授權的使用者遭到服務拒絕（虞金燕與鄭祥勝；2001）。

由於美國將資訊基礎建設中的資訊安全防護，在 Y2K 後納入國家的範圍，亦即成為國防保護的範圍，而美國的資訊安全技術研發，一向由

軍方支持，資訊戰之執行則由美國太空司令部（SPACECOM）負責。足見美軍為負責資訊安全最重要的權責單位，其對資訊安全的定義最具權威性（虞金燕與鄭祥勝,2001）。

「資訊系統安全」乃指一切保護資訊系統資源，包括：硬體、軟體、資料庫，以防止遭受變更、破壞及未授權使用資訊系統資源之控制措施，其範圍包括技術面與組織管理面（吳琮璠,1996）。

資訊安全管理的目的在保護電腦資源，包括：硬體、軟體、資料、程序及人員，以防止電腦資源被變更、破壞及未授權使用（謝清佳與吳琮璠,1999）。

所有涉及到「安全」的問題，基本上再處理下列事項，以確保資訊系統軟硬體資料、資訊的機密性（Confidentiality）、整體性（Integrity）及可用性（Availability）（Pfleeger,1996；Gollmann,1999）：

(1)預防（Prevention）：在防止資產發生危險。

(2)發現（Detection）：當安全問題發生時，要有方法可以在最短時間內發現，並知道確切的危險及其嚴重程度。

(3)反應（Reaction）：要在最短時間內使傷害降至最低，損害減至最少，並恢復到正常的情況。

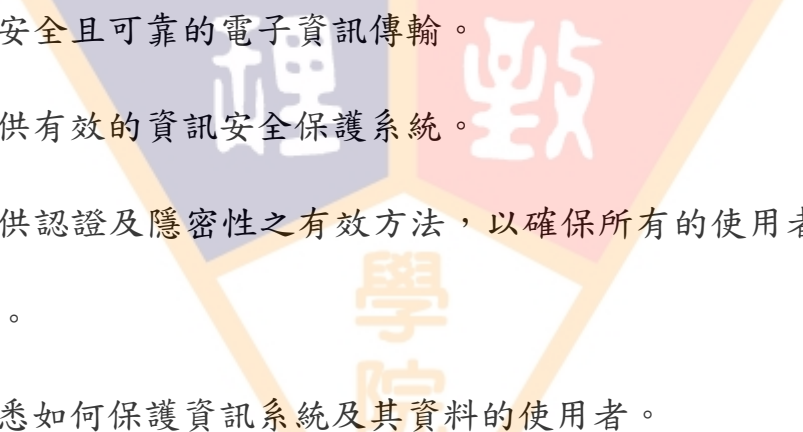
「預防」與「發現」的概念對應到資訊安全即是所謂「防禦性資訊系統安全」，其目標在於：「從確保資訊資源的合法存取，到在所有可能遭受資訊攻擊時，可提供完整（Complete）、不中斷的資訊系統運作。」百分之百的資訊安全是難以做到的，為確保資訊安全基礎建設的安全性，防禦性資訊系統受到先進國家的重視，其功能性典範（Functional Paradigm）採取下列措施（樊國楨等,2001d；Panda&Giordano,1999；樊國楨與時崇德,2000；Ellisort,1999；國家安全局,2000）：

- (1)防護（Resistance）：即防止資訊系統之硬體、軟體與資料遭受外部或內部的威脅。
- (2)識別（Recognition）：即快速且正確的偵測與辨識出惡意的資訊攻擊，以爭取回復的時間與機會。
- (3)回復（Recovery）：即評估損害程度，找出隱藏的惡意程式，關閉入侵者為在次入侵留下的後門與回復資料，快速且完整的回復系統，並維護系統的完整性與可用性。

資訊安全管理的目標，是要減少資訊安全事故發生的機率或頻率，或當發生時，減少其後果的嚴重程度，或使兩者都減少（Solms,1996；Moulton,1991）。

資訊安全需求與原則相關文獻探討

在網際網路的環境下，商業交易的資訊，及人民與政府或政府與政府間公文書的往來，不再只是具有實體的形式，已漸漸轉變成數位的形式，並在網際網路上傳輸或交換，因此，資訊安全的需求以不同於往常，亦即資訊安全必須考量在 Internet、Intranet、Extranet 等 Web base 環境下的需求。其資訊安全的要素（吳琮璠,1999）諸如：

- 
- (1)具安全且可靠的電子資訊傳輸。
 - (2)提供有效的資訊安全保護系統。
 - (3)提供認證及隱密性之有效方法，以確保所有的使用者均係授權使用。
 - (4)熟悉如何保護資訊系統及其資料的使用者。

利用網際網路的商業交易（Commercial Internet Transaction），在資訊安全的需求則包括（Bhimani,1996；Furnell&Karweni,1999；樊國楨,1995）：

- (1)機密性（Confidentiality），以確保使用者的私密性，防止資訊的非法被竊。
- (2)確認性（Authentication），完全確認交易者之間的身分。
- (3)資料完整性（Data Integrity），資料傳輸或儲存的無法被竊改。

(4)不可否認性 (No repudiation)，交易的任何一方，在交易完成後，無法否認交易的事實。

(5)存取控制 (Access Control) 與選擇性服務 (Selective application of Service)，可以在不同的需求情況下，分別限制其存取權限。

1992年11月26日世界經濟合作開發組織(Organization for Economic Cooperation and Development, OECD)，訂定可信賴的資訊系統使用環境，應遵守的九大指導原則。該原則係由24個會員國決定採用1990年起，由資訊、電腦與通訊政策 (Information, Computer and Communication Policy, ICCP)組織的專家小組，訂定之資訊系統安全指導方針(Guidelines for Security of Information Systems)之提議所制定，期間經過20個月，6次會議的評議會 (OECD,1992)。其 OECD 資訊安全指導原則為 (OECD,1992；樊國楨等,2001a)：

(1)責任原則：清楚界定資訊系統之擁有者、提供者、使用者及其他有關組織之職責與責任。

(2)預警原則：資訊系統之擁有者、提供者、使用者及其他有關團體等，對於資訊系統安全之方法、運作方式、程序及其有關知識應具備相當程度，以達成對資訊系統的信任度，及維護其安全。

- (3)倫理原則：尊重他人權利及合法利益，為使用及提供資訊系統及資訊安全之原則。
- (4)多層面紀律原則：應以技術、管理、機構、運作、商業、教育及法律等等，多層面的考量資訊系統安全所用的方法、運作方式及程序步驟，並提出相關條件及不同觀點。
- (5)正比原則：應以組織對一特定的資訊系統的依賴程度、潛在危害的嚴重程度、發生機率等因素，來考量其安全等級、投資成本、使用方法、運作方式及程序步驟，使兩者能成正比。
- (6)整合原則：資訊系統安全的執行、運作、程序與步驟等之間，彼此應相互整合，再進一步與組織相對應的部分加以整合，以建立整體性、一致性的安全體系。
- (7)適時原則：無論政府、民間，須適時與國際間各國之政府、民間，彼此協調運作，並預防及回應有關危害資訊系統安全的任何傷害。
- (8)持續評估原則：資訊系統及其安全之環境及要件經常改變，故須定期重覆的加以評估，以據以修正。
- (9)民主原則：資訊系統應符合、方便民主社會對資料與資訊合法的使用與流通。

OECD 有鑒於美國遭受 911 攻擊事件之後，各會員國的網路遭受網路恐怖份子、網路駭客、電腦病毒等的不斷攻擊，故公佈「邁向安全文化的資訊系統與網路安全指引」(Guidelines for the Security of Information Systems and Networks Towards a culture of Security)，以加強會員國間資訊及網路的安全。其指導原則為 (OECD,2002)：

- (1)意識原則 (Awareness)：對於資訊系統與網路的安全要有充分的
認知與安全警覺的意識。
- (2)責任原則 (Responsibility)：組織要檢視自己的安全政策、執行、
措施與程序規定，評估其是否符合環境需要，並發展、設計與提
供產品與服務，以落實對資訊系統與網路安全的責任。
- (3)回應原則 (Response)：會員國應及時採取行動及相互合作，以防
範、察覺及因應資訊安全事故之發生。
- (4)倫理原則 (Ethics)：會員國應尊重會員間之合法權益。
- (5)民主原則 (Democracy)：資訊系統及組織安全應與民主社會價值
相容。
- (6)風險評估 (Risk Assessment)：會員國應進行資訊系統及網路安全
之風險評估。

(7)安全設計與建置 (Security Design and Implementation)：將資訊系統及網路安全部分納入安全體系。其安全體系的基本組成包括：產品、服務、系統與網路，及系統設計與架構的整合。

(8)安全管理原則 (Security Management)：應採取完整周延的措施，以達成安全管理的目標。安全管理應建立在風險評估，動態、涵蓋各層級的活動，並包括：高瞻遠矚的防禦、偵測與對意外事故的反應，系統恢復，持續的維護，檢討與稽核。對於資訊系統與網路的安全政策、實施、措施與程序應整合貫穿成一個安全系統。

(9)持續評估原則 (Reassessment)：應檢視與在評估資訊系統及網路安全，並適時修正資訊安全政策、措施與程序。

一般公認系統安全原則 GASSP (Generally Accepted System Security Principle) 所揭示的一般功能原則，代表資訊安全的目標，共有十四項 (Ozier, 1997; 樊國楨與時崇德, 2000)：

(1)資訊安全政策：確保發展、維護政策、支持標準、基線水準、程序、指導方針等，以處理資訊安全。

(2)教育及意識：確保所有人員均有效地瞭解安全政策，經常傳達與教育其要求，使其知不遵守之後果。

- (3)承擔責任：要嚴格界定所有人員取得及使用資訊所應負擔之責任，此為組織建立及維持資訊資產支控制基準所必要的。
- (4)資訊資產管理：對資訊資產予以有效管理，依其機密性、敏感性或重要性等獨特程度，予以識別及指定責任歸屬。
- (5)實體環境管理：對於資訊技術資源之支援，資訊資產之儲存、傳送或使用等之內外在實體環境管理，以阻絕自然災害，非故意或故意之安全威脅。
- (6)人員資格條件：資訊資源的運用有賴於具體足夠的知識、技術能力，廉正等資格條件的人員來執行。
- (7)系統整合：確保所有對組織任務為基礎的，或賴以支援組織任務之系統均被建置、保持與保護，使資訊技術資源充分整合。
- (8)資訊系統生命週期：確保安全的控制制度，能與系統生命週期的每一階段充分結合，值得信賴的管制功能，應是持續的融入資訊系統生命週期的每一環節，充分整合。
- (9)存取控制：建立適當的存取控制，以確保資訊資產與資訊技術資源的存取是經過合法授權，而降低資訊安全之風險。

(10)持續營運及應變規劃：為確保資訊資產及資訊資源免於中斷服務，或是在無法避免情況下中斷服務後，能迅速的重新恢復功能運作，始終段服務的損害及衝擊降至最低。

(11)資訊風險管理：找出資訊資產受到的威脅與弱點，針對資訊資產的價值，決定有效的安全基礎，以降低資訊安全風險，使其風險程度在組織可以接受的範圍以內。

(12)網路安全：建立網路安全基準時，應考慮對網路潛在影響，找出可能弱點，及被非法入侵的後果，使資訊資產可依其敏感性或重要性匹配其保護程度。

(13)資訊安全的法律、管理、契約上的要求：組織應遵守與營運相關的法律、管理及契約上的要求。

(14)道德的實踐：組織在制定政策，或選擇、履行安全基準時，應尊重個人的權利和尊嚴，必須是公正、公平、謹慎的。

資訊安全問題已受到全世界的關注，除了之前所指 OECD 公佈「資訊系統與網路安全指引」之外，歐聯（European Union）也提出網路與資訊安全的政策走向，建議各會員國（Pounder，2001）：

(1)資訊安全管理之具體實施，如：執行 ISO/IEC17799 等。

(2)學校教育更強調資訊安全問題。

- (3)分享資訊安全的經驗。
- (4)建立電腦安全緊急處理中心 (Computer Emergency Reponse Teams, CERT)。
- (5)擴大歐聯的 CERT 網路，以連接全世界的類似機制，如 G8 事故報告系統(G8 Incident Reporting System)，何況美國以建立此機制。
- (6)蒐集歐聯現存與浮現的安全威脅。
- (7)資訊安全標準與認證的推動。
- (8)納入有效與可互相操作的資訊安全解決案，其基本需求在於 e 化政府 (e-Government) 與 e 化採購 (e-Procurement)。
- (9)引進電子簽章於線上公共服務。

資訊安全的原則，在傳統上有所謂的 CIA 原則，即機密性 (Confidentiality)、完整性 (Integrity) 和可用性 (Availability)，受到廣泛的重視及認同 (Tudor, 2001; Gollmann, 1999)，而 Dhillon 及 Backhouse 卻認為：此三原則，在彈性鬆散的現今組織結構中是難以適用的，如機密性強調嚴格的存取控制，非正式組織，鼓勵資料存取，較少的規則，及加強授權等之趨勢相違背；而完整性則對資料的正確性與一至性，但忽視了在使用上的解釋。

因此 Dhillon 及 Backhouse 即提出增加 RITE 原則，即人員責任心

(Responsibility)、核心成員完整性 (Integrity)、信賴度 (Trust)、道德性 (Ethicality) 等四項原則。

即使得組織的成員能明確地瞭解自己的職責所在，主動的承擔份內工作，對於核心成員應維持其完整性，注意信任度與道德的規範，才能在動態的環境中，避免指運用嚴密的控制來達成目標。

CIA 原則強調的是制度面的控制，而 RITE 原則強調的是人性面的管理，兩者強調的重點雖有不同，但維護資訊安全的目標卻是一致，故可以相輔相成 (Dhillon& Backhouse, 2000)。

資訊安全可參考的政府法令如：電腦處理個人資料保護法、行政院及所屬各機關資訊安全管理規範、財政部證券暨期貨交易管理委員會所制定的公開發行公司建立內部控制制度實施要點等。國際標準規範，如：BS7799、ISO1799、COBIT、GAPSIT、RFC-2196、FISCAM 等等，如表附錄 1-2 所示。企業之業務需要則應衡量資訊科技對組織營運之需要與必要程度，以及企業之財務、技術能力等因素。

標準名稱及說明	提出單位及網頁
COBIT 資訊技術控制目標架構 (Control Objectives for Information and related technology)	國際電腦稽核協會 (ISACA) http://www.isaca.org/
BS7799 BS7799/c : cure code of practice 1& 2	英國標準組織 (BSI) http://www.bsi-global.com/
ISO17799 ISO17799 (採用 BS7799 code of Practice 1)	國際標準組織 2000 年 3 月東京年會 (ISO) http://Iso.ch/
GAPSIT 一般公認資訊系統技術之安全原則與實務 (General Accepted Principal and Practice for Securing information Systems and technology)	美國國家標準與技術組織 (NIST) http://csrc.Nist.gov/nistpubs/800-14.pdf
RFC-2196 網路服務安全指南 (Site Security Handbook)	網際網路工程任務團隊 (NIST) http://www.ietf.org/rfc2196.txt?number=2196
FISCAM 聯邦政府資訊系統控制與稽核指南 (Federal Information Systems Control & Audit Manual)	美國政府審計總署 (GAO,US Government) http://www.gao.gov/
Sys Trust TM 可信賴之資訊系統認證 (Sys Trust)	美國與加拿大會計師公會 (AICPA & CCA) http://www.aicpa.org/
GASSP 一般公認系統安全原則 (General Accepted Systems Security Principal)	國際資訊安全協會 (ISC2) http://w3.mit.edu/security/www/gassp1.html

表附錄 1-1 資訊安全國際標準表

基於防護、識別與回復的需要，國際標準組織 (International Organization for Standardization, ISO) 提出資訊技術安全保護框架，其相關標準有：COBIT、ISO/IEC TR13335、ISO/IEC 15026、ISO/TR 13569、ISO/IEC 15408、ISO/IEC TR 15504、ISO/IEC 17799、SE-CMM、SSE-CMM 等。

美國國防部所出版「可信任的電腦系統評估標準」(Trusted Computer System Evaluation Criteria)，俗稱橘皮書 (The Orange Book) 中定義四個安全等級：D (最低安全)、C1 (任意性的防護)、C2 (存取控制保護)、B1 (標籤安全保護)、B2 (有組織的保護)、B3 (安全範圍)、A1 (驗證性的防護) 等。橘皮書提出六點基本要求 (尤培麟，2002)：

- (1)安全政策 (Security Policy)：制定完整的安全政策，建立規則用以規範那些主體 (Subject) 可以存取那些客體或物件 (Object)。
- (2)標記 (Marking)：所有客體的資訊資源，必須加以標記，以確定物件的安全等級。
- (3)識別 (Identification)：所有的物件居均可以辨識，當物件被存取時，即可辨別存取者為何人，及存取權限等級。
- (4)責任 (Accountability)：對稽核資料加以保存與保護，以利任何影響資訊安全行為之追蹤。將所有與安全有關的事件 (event) 紀錄在稽核的 log 中。
- (5)保證 (Assurance)：具備獨立評估的機制，以確保可以達到以上四個要求。
- (6)持續保護 (Continuous Protection)：上述的各項機制應持續運作，並加維護，以達成安全目標。

在橘皮書之後，許多組織試圖努力推行新的安全驗證共同通規範，包括（高宏傑，2002）：

(1)加拿大的可信賴電腦產品評估準則（Canadian Trusted Computer Products Evaluation Criteria）。

(2)歐盟的資訊產品評估準則（Information Technology Security Evaluation Criteria，ITSEC）。

(3)美國聯邦標準。

紅皮書即 Trusted Network Interpretation Environment Guideline 提供使用者一個更深入檢視及維護可信任電腦網路的方向。針對不同型態的網路環境，訂定最低限度的安全要求。紅皮書規定，每個網路應該有一個「網路安全架構與設計」（Network Security Architecture and Design，NSAD），並包括通信安全（Communication Security）、實體安全（Physical Security）、人員安全（Personnel Security）及資訊安全（Information Security）等。

資訊安全架構相關文獻探討

資訊安全管理 (Information Security Management) 包括 10 大要項 (BS7799-1, 1999; ISO/ICE17799, 2000; Kwok & Longley, 1999; AS4444, 1996):

- (1)安全政策 (Security Policy)
- (2)安全的組織 (Security Organization)
- (3)資產分類與控制 (Assets Classification and Control)
- (4)人員安全 (Personnel Security)
- (5)實體與環境安全 (Physical and Environmental Security)
- (6)通訊與操作管理 (Communication and Operations Management)
- (7)存取控制 (Access Control)
- (8)系統開發及維護 (Systems Development and Management)
- (9)業務持續運作管理 (Business Continuity Management)
- (10)遵行 (Compliance)

此 10 大要項受到國際間所重視，政府於 2002 年 12 月已將 ISO/IEC17799 轉定為 CNS17799，另 BS7799-2 亦同時轉定為 CNS17800。

資訊安全管理系統需要加以驗證，以知其可行性與適應性，其驗證之準備工作與內涵為（徐鈺宗與樊國楨，2003）：

- (1) 定義資訊安全政策 (Define Security Policy)
- (2) 定義資訊安全管理系統範疇 (Define the ISMS Scope (Boundary))
- (3) 識別資訊資產 (Define Information Assets)
- (4) 執行資訊資產風險評估 (Undertake Information Assets Risk Assessment)
- (5) 識別資訊資產弱點區域 (Identify Information Assets Weak Areas)
- (6) 決定如何管理風險 (Make Decisions to Manage Risk)
- (7) 選擇適當控制措施 (Select Appropriate Controls and Risk Treatment Plan)
- (8) 準備適用性聲明 (Prepare Statement of Applicability)

一般而言，資訊資產分為人員、實體、軟體、文件、檔案、服務、公共設施、商譽 8 類。

資訊安全管理亦可從兩面向著手，即從管理面的程序認證與產品（系統）面的評估，已構成資訊安全管理（Eloff & Von Solms，2000a）。

資訊安全的威脅與弱點相關文獻探討

資訊安全的風險來自外在的威脅 (Threats) 與自身的弱點 (Vulnerabilities)。威脅與弱點會損及資訊資源、系統及網路的機密性 (Confidentiality)、完整性 (Integrity) 或可用性 (Availability)，使資訊安全水準下降 (行政院研考會，2002)。資訊安全的威脅 (Threats) 與弱點 (Vulnerabilities) 包括有 (黃淙澤，2002；Rainer 等，1991；宋鎧等，2001；ISACA，2002)：

- (1)天然威脅：水災、火災、地震等。
- (2)人為疏失：安全意識不足，使用者訓練不夠，員工操作不良等。
- (3)內部弱點：電力供應不穩定，機房未設門禁，網路工作流量負荷過重，系統當機。
- (4)實體威脅 (Physical Threats)：設備損壞、電力中斷、天候、火災、空氣污染、濕氣、人為破壞等。
- (5)未授權的實體或電子存取 (Unauthorized Physical or Electronic Access)：如電腦失竊、資料失竊、資料損毀、揭露或更改、駭客、病毒、電腦炸彈、EDI 詐欺、網路上的幽靈節點、語言信箱詐欺及軟體盜版等。

(6)機授權的實體或電子存取 (Authorized Physical or Electronic

Access)：如資訊系統的陳舊過時，EUC 增加的影響，員工的濫用

以上發生的比例依 Loch 等 (1992) 的研究，係以天然威脅居首。

對於人為的安全威脅，依其來源可區分為自組織內部與外部的威脅

(李東峰，2001)。林傳敏 (2000) 任危網路交易是時代趨勢，資訊安全

威脅則是無國界之分，可以歸納為：

(1)組織內部的威脅：內部威脅佔 80%，包括：承包商與內部員工，

疏忽即犯錯、心懷怨恨及故意舞弊等情況，而稍早 Van Duyn(1985)

認為組織內部的威脅佔 75%，黃慶堂 (1999) 則認為資訊安全問

題 85% 來自於組織的內部因素。

(2)組織外部的威脅：外部威脅佔 20%，包括：Internet 漫遊者、產業

間諜、競爭者、外國政府、地下組織等，電子商務盛行後，財務

詐欺與資訊資產的竊取更加的容易。

層出不窮的駭客入侵事件，其駭客無論是：業餘玩家、職業入侵者、

玩票性質的電腦高手、Hacker 級的 Cracker 等，其入侵的目的也無論是：

好奇心與成就感，當作入侵第三者的跳板，到用系統資源，竊取機密資

料，惡意攻擊或心懷不滿的反應等，都對組織的資訊安全構成極大的威

脅 (宋振華等，2000)。

Loch 等（1992）對於資訊安全的威脅，則更從四個面向來分析：

- (1)威脅來源：來自於組織內部或外部。
- (2)破壞者：人的破壞或非人的破壞。
- (3)意圖：意外或故意。
- (4)後果：資訊揭露、竄改、破壞、拒絕服務等。

電腦犯罪事資訊的嚴重威脅之一，電腦犯罪（Computer Crime）是以使用（use）或存取（Access）電腦系統或電腦的組成（如終端機、網路等）為必要條件的犯罪行為；亦即未使用到電腦則不視為電腦犯罪（劉達餘，1988）。

Cohen and Felson 指出：犯罪的發生必須有三種因素（M-O-P）在時空的聚合（張盛盛與許美玲，1995）：

- (1)Motivation：有動機及能力的犯罪者。
- (2)Object：合適的犯罪標的物。
- (3)Protect：保護犯罪者不在場的理由。

要防止電腦的犯罪，降低資訊安全潛在威脅，亦可從此三者加以思考（許慧珍，2001）：

- (1)Motivation：制定資訊安全政策，建立資訊安全知內部控制制度，加強資訊安全教育。

(2)Object：資訊安全軟硬體的使用，如防火牆等。

(3)Protect：稽核軌跡、各種紀錄檔、監控、偵測的軟硬體設備等。

張慶光（1997）認為網際網路及商業應用的資訊安全威脅有下列四種型態：

(1)網路上的交易資料遭到竊取（Unauthorized Access to Network Transactions）。

(2)伺服器上的資料遭外部駭客的竊取（Unauthorized Access by Insiders to Server Data）。

(3)伺服器上的資料資內部員工的竊取（Unauthorized Access by Insiders to Server Data）。

(4)主從架構的應用系統被竄改（Violation of Client and Server Application Integrity）。

Karen 等（1992）認為安全威脅可為四類：資訊洩漏（Disclosure）、資訊竄改（Modification）、資訊損毀（Destruction）、資訊無法使用（Denial of use）。張偉斌（2000），認為在電子商務的環境下，其安全威脅的型態又有所不同，如：竊聽（Eavesdropping）、連線巧取（Spoofing）、協定錯誤（Protocol Error）、資料竄改（Data Modify）、錯誤傳送（Transit Error）、滲透（Permeate）、病毒（Virus）、拒絕支付（Denial payment）、拒絕服務

等 (Denial Service) 等。

風險分析一向是用來識別最適合的安全控制方式，對維護資訊安全扮演者主要角色，風險分析的目的在識別與評估所有可能的風險，在據於規劃控制方案，以使組織的資訊安全風險降低到一個可以接受的水準，即是風險管理 (Gerber & Von Solms, 2001)。

組織進行風險評估應包括五類資訊資產：

- (1)資料：檔案、程式 (原始碼、目的碼)、公用程式、作業手冊、技術文件、表單、輸出報表、備份資源、資料規格 (Meta data) 等。
- (2)系統：網路系統、資料庫系統、作業系統、應用系統、系統開發之程式庫與工具、安控系統、OA 系統、介面系統、網路服務系統、系統運作等。
- (3)服務：供資訊系統運作，或資訊系統提供服務之對象，以及支援資訊系統提升效能之相關服務。
- (4)設備：包含主機設備、終端機、工作站、個人電腦、儲存媒體、印表機、磁碟機、通訊線路、通訊設備、實體安控設施、機房與設備等。
- (5)人員：使用者、設備/系統管理人員、硬體維護人員、資訊安全人員、系統開發人員、系統維護人員等。

附錄三 成果光碟

