私立東海大學資訊工程研究所

碩　　士　　論　　文

指導教授：呂芳懌　博士

資訊安全風險評估之執行差異分析與原因探討

—以中部地區兩學術單位為例

The Differential Analyses of Information Security Risk Assessment

Using Two Academic Units in central Taiwan as Examples

研究生：吳秀娟

中 華 民 國 一 ○ ○ 年 六 月 三 十 日

摘　　要

網路與資訊蓬勃發展，除帶來眾多便利亦伴隨著日益嚴重的資訊安全問題。各組織為能確保營運持續，紛紛投注相當資源來建立資訊安全管理系統，以保護重要資訊資產避免遭受各種威脅。有效的資訊安全管理系統並非消弭所有的風險，而是協助組織去辨識與評估所有的威脅與弱點，進而即早採取適當的方法來管理風險。

風險的存在性是不變的，但每個人對風險的認知與容忍程度都不盡相同，即使採用相同的方法論亦可能產生不同的風險評估結果。本研究將資訊安全風險評估之差異因素分成三大層面以進行分析，分別是驗證範圍層面、資訊特性層面與資訊類別層面，並用層級分析法（Analytic Hierarchy Process,AHP）所提的層級架構，建立研究架構的模式，最後並以實際案例說明其個別執行或相結合應用的程序。

本文探討應用相同風險評估模式於背景類似之組織時，其風險評估結果的差異原因，希望能找出風險評估方法與組織特質影響的關聯，以作為未來學術單位執行資訊風險評估之重要參考依據。

關鍵字：風險評估、資訊安全、威脅、弱點、層級分析法

Abstract

Recently, network and information have been vigorously developed, and have truly brought us much convenience for our every life. However, they also bring forth an increasingly serious security problem. Many organizations have invested considerable resources to establish their information security management systems to protect their critical information assets against threats and ensure the safety and security of their business continuity.

The main task of an information security management system is not eliminating all risks, but assisting the organizations to identify and evaluate all threats and vulnerabilities, and then help them to take appropriate and immediate methods for risk management.

Risks always exist in our surrounding. But a person's perception on risk and the degree of risk tolerance are different. Even with the same methodology, they may produce different risk assessment results. In this study, we compare the assessment results of two identical organizations. The information security risk assessment factors to be analyzed are divided into three levels, including the levels of risk verification, information characteristics and information category We use a hierarchical structure proposed by the Analytic Hierarchy Process (AHP for short) to establish our research model. Two actual implementation cases are employed to describe their processes on individuals and a combined application.

This study also explores the key reasons of the different results generated by two organizations of similar background which deployed the same risk assessment model, and try to find the reasons for differences in the risk assessment results. The purpose is to identify the impact of organizational characteristics associated with academic institutions. Someday, when organizations with the similar characteristics and background wish to perform their risk assessment, the research results can be a valuable and important reference.

Key Word: Risk Assessment, Information Security, Threat, Vulnerability,AHP

目　　錄

表 目 錄

圖 目 錄

第1章　緒論

1.1 研究背景與動機

風險評估是執行資訊安全管理中相當重要的環節，也一直是風險管理的基礎，更是組織確認資訊安全要求的途徑。但風險評估程序常由單一人員憑藉著過去經驗的累積，加上自我隨機腦力激盪直覺式地判斷評估結果。因為每個人對風險的認知與容忍度不盡相同，且容易就單一層面判斷問題，即便採用相同的方法評估，亦會產生不同的風險結果，導致評估結果過於主觀偏頗，進而做出錯誤的風險處理決策。

過去對於資訊風險評估之相關研究，大部分僅提出資訊安全風險評估之方法論，少有探討可能導致風險評估結果差異之相關因素分析。有鑑於此，本研究主要方向為探討「資訊安全風險評估結果差異原因」，透過層級分析法(Analytical Hierarchy Process，AHP) 分析組織人員執行資訊安全風險評估方法與過程會影響風險結果的相關因素與權重。本研究個案所提出的風險評估方式為一半量化評估方式，首先依照驗證範圍(關鍵營運)進行流程中資訊資產盤點，再依據各項資訊資產之機密性、完整性、可用性與適法性等四項特性因子，評估資產價值，再進一步考量文件類、軟體類、實體類、人員類與服務類等五項資產類別，各類別所面臨之弱點與可能發生之威脅的機率，最後產生組織的資訊資產風險值，用以決定風險處理之優先順序。

本研究探討兩間背景相似之學術單位，於相同時間導入 ISO27001 資訊安全制度，並採用同樣的風險評估方式，卻有不同的風險優先順序差異結果。本研究期能探討其差異原因，以作為未來學術單位執行資訊風險評估之重要參考依據。

1.2 研究目的

本研究之目的有三：

1. 探究資訊安全風險管理與評估方式。
2. 探討背景相似之組織使用相同之風險評估方式，其評估結果差異程度與原因，並以兩所學術單位實例說明。
3. 利用 AHP 層級分析法，探討兩所學術單位，由不同人員評估風險考量之因子與分析各因素權重，對風險評估之影響。
4. 提供一客觀之群體風險評估權重方法，讓組織進行風險評估程序時，能找出最迫切需處理的風險因素。

1.3 研究範圍

本研究範圍在於資產風險評估結果，不包括風險評估後之風險處理措施與與殘餘風險計算。主要研究單位為學術機構，其研究結果可能不適用於其他產業。

1.4 研究流程

本研究流程之步驟如圖 1-1 所示。首先確定研究的方向與範圍後進行相關文獻探討，其內容分別為：資訊安全管理、資訊安全相關國際標準、風險管理、層級分析法等；經完整文獻資料蒐集，再針對研究目的進行資料蒐集。同時根據個案風險評估方法與結果，建構出風險評估結果差異原因之三項評估層面，並進行問卷調查。最後將問卷調查結果輸入 Expert Choice 軟體計算，得到「驗證範圍層面」、「資產特性層面」、「資產類別層面」之三個層面的評估要素及評估準則之權重。層級分析的目的是藉由風險結果關聯之總向量權，亦可由各目標向量權重值，找出個案之影響風險評估結果差異相關因子之優先順序。

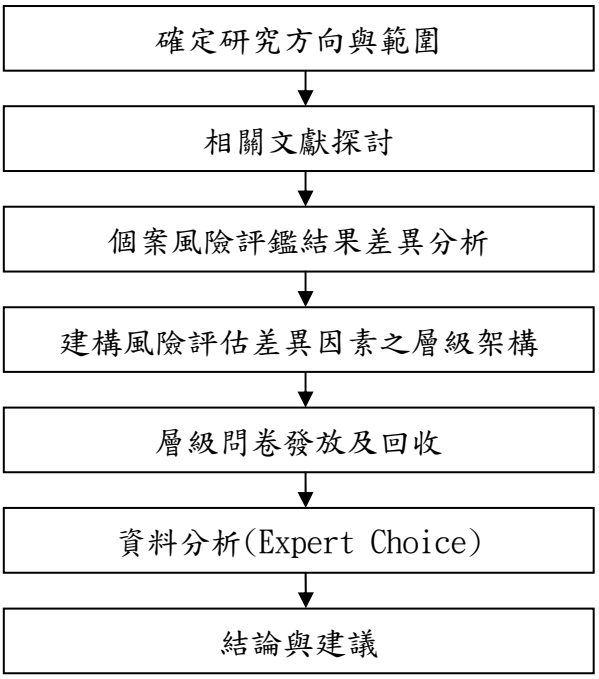

確定研究方向與範圍
相關文獻探討
個案風險評鑑結果差異分析
建構風險評估差異因素之層級架構
層級問卷發放及回收
資料分析(Expert Choice)
結論與建議

圖 1-1 研究步驟示意圖

第2章　文獻探討

2.1 資訊安全管理

資訊安全的定義，資訊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（Gollmann, 1999）。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、完整性與可用性，即所謂「C.I.A」。而近年來智慧財產權與個人資料保護法議題備受重視，應再加上資料之適法性，各項所欲達成的目標分別說明如下：

1. 機密性（Confidentiality）：確保只有經過授權的人才能存取資訊資產。
2. 完整性（Integrity）：保護各項資訊資產的完整度，確保其能準確地被運用。
3. 可用性（Availability）：確保經過授權的用戶在需要時，可以存取資訊資產，並使用相關資訊資產。
4. 適法性（Law）：確保資訊與其處理方式過程，須遵守的法律、規定、合約義務或是組織內部之政策、章程之規範要求。

2.2 資訊安全相關國際標準

國際標準化組織（International Organisation for Standardisation, ISO）是一個非官方國際組織，與國際電工技術委員會（International Electrotechnical Commission, IEC）和國際電信聯盟（International Telecommunication Union, ITU）合作，以制定 information and communications technology（ICT）標準。以下是幾項常見的 ISO 資訊安全標準：

表 2-1　常見的 ISO/IEC 資訊安全標準

標準名稱	內涵說明
ISO/IEC 27000	資訊安全管理系統之原則與詞彙 ISMS fundamentals and vocabulary
ISO/IEC 27001	資訊安全管理系統要求事項

ISO/IEC 27002	資訊安全作業規範 Code of practice for information security management (controls)
ISO/IEC 27003	資訊安全管理系統實作指引 ISMS implementation Guide
ISO/IEC 27004	資訊安全管理之測度與測量 Measurement and metrics
ISO/IEC 27005	風險管理之原則與實作的通用指導綱要 Risk management
ISO/IEC 27006	ISMS驗證/登錄機構之認證指導綱要 Requirements for the accreditation of bodies providing certification of ISMS
ISO/IEC 27007	資訊安全管理系統稽核指導綱要

2.2.1 ISO/IEC 27001:2005

ISO/IEC 27001 是 International Organization for Standardization(ISO)和 International Electrotechnical Commission(IEC)在 2005 年 10 月所公布的資訊安全管理認證標準，其前身是在 90 年代所發表的英國標準 BS7799，目前全球發出的認證張數已超過六千多張，是目前資訊安全管理領域中，最具公信力的認證標準。避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等資訊安全情事發生加上政府近年來大力推動，國內各組織已經開始將資訊安全管理視為不可或缺的一環，也開始願意針對資訊安全管理投入更多的資源來推動符合 ISO/IEC 27001 標準規範之制度及文件，該標準協助組織降低資訊脆弱點所造成的損失及預防潛在風險的衝擊。

此標準透過建立、實施、操作、監測、審查、維護機制來改進資訊安全管理系統，並利用 Plan-Do-Check-Act (PDCA)循環來達到確實的效果。此標準的結構分成八個章節和一個附錄，附錄包含 11 個領域、39 個控制目標和 133 條控制項。我國經濟部亦於 95 年間將其內容翻成中文變成國家標準 CNS27001[1]，該內容提供欲實作資訊安全的組織一個相當完整的參考依據和實行的方向。

一般討論資訊安全缺乏一套系統性的分析工具，ISO27001 標準的作業程序是將資訊資產列表，依據這些資產本身所存在的弱點，預測會面臨的威脅，進而評估該風險是否為組織可承受。而 ISO27001 的核心就是建立 ISMS，以提供一個資訊安全作業準則的平台，藉由這個平台，各個單位可以透過完整而綿密的資訊資產風險評估，建立一套量身訂作風險降低政策以降低資產的風險，透過管理層面的完善規範，可以確保資安事件的發生在可以容忍的風險程度內。ISO/IEC 27001 資訊安全管理規範涵蓋 11 項管理事項如下：

1. 資訊安全政策制定及評估。
2. 組織的資訊安全與分工。
3. 資產管理。
4. 人力資源的安全。
5. 實體與環境安全。
6. 通訊與作業管理。
7. 存取控制。
8. 資訊系統取得、開發及維護。
9. 資訊安全事故管理。
10. 營運持續管理。
11. 遵循性。

2.2.2 ISO/IEC 27002:2005

ISO/IEC 27002:2005 起源於 BS7799-1 的國際標準，而 BS7799-1 原本是由英國標準協會（BSI）提出，於 2007 年 4 月取代 ISO/IEC 17799:2005。ISO/IEC 27002:2005 可被視為資訊安全管理的作業實務守則，我國經濟部亦於 2007 年 10 月 24 日將其內容翻譯變成國家標準 CNS27002[2]，其為發展組織安全標準和有效管理實踐的共同原則與最佳實務指引。該標準包含 10 項安全領域的指引和最佳作業實務建議：（a） 安全政策；（b）資訊安全組織；（c）資

產管理；(d) 人力資源安全；(e) 實體和環境安全；(f) 通訊和操作管理；(g) 接達控制；(h) 資訊系統的採購、發展和維護；(i) 資訊安全事故管理；(j) 持續業務運作管理；(k) 法規遵循。在這 10 項安全領域當中，建議給機構 39 項控制目標和數百件最佳資訊安全控制措施的最佳作業實務，以達到控制目標和保護資訊資產免受保密性、完整性和可用性上的威脅。

2.2.3 ISO/IEC 27005:2008

ISO/IEC 27005 風險管理之原則與實作的通用指導綱要，由 ISO/IEC 13335-2 轉定。其內容說明資訊風險管理的概念是持續的處理過程，明確的指導企業或組織如何有計畫的規律進行資訊安全風險管理作業。

經濟部標準檢驗局配合行政院國家資通安全會報政策，依據 ISO/IEC 27005 於 2008 年 2 月 8 日制定公告 CNS 27005[3]「資訊技術－安全技術－資訊安全風險管理」提供各界參考依循，以強化資通訊環境的安全性。所謂風險管理理論係指組織透過風險分析（Risk Analysis）與風險估計（Risk Evaluation），以確認資訊安全威脅（Threats）與弱點（Vulnerabilities），及估計其發生之可能性，再進行風險評估（Risk Assessment），以規劃組織資訊安全需求風險控制在可以接受的水準，而達成組織資訊安全之目標。樊國楨[4]等人亦提出：風險管理步驟，(1) 風險分析（Risk Analysis）；(2) 風險評估（Risk Assessment）；(3) 改善計畫或管理控制（Improvement Plan or Management Control）；(4) 控制績效審查（Review of Control Performance）；持續改善、週而復始，以達成降低風險、促進資訊安全的目的。

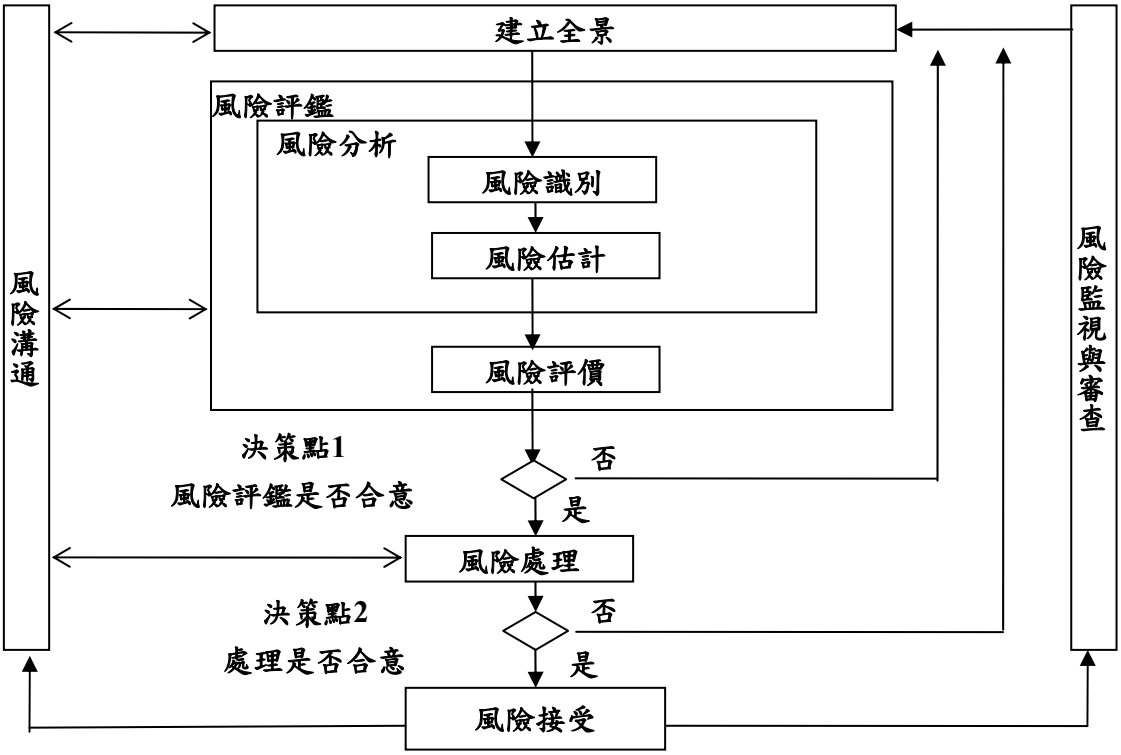


圖 2-1　資訊安全風險管理過程示意圖

資料來源：CNS 27005，2010 年[3]

ISO/IEC 27005:2008，有六個風險管理的步驟如圖 2-1 所示，各步驟分別說明如下[5]：

1. 建立全景(Context Establishment)：制定與組織有關的資訊安全風險管理基本規則，內容必須持續符合 ISMS 的規範，詳細說明組織的資訊資產及精確定義組織的風險管理範圍與機制。
2. 風險評估(Risk Assessment)：針對已制定之組織風險管理機制，列出組織內資產的擁有人、資產置放的位置及資產的功能等，加入威脅事件的識別，列出所有可能遭受威脅事件的資產清單，並找出可能產生威脅事件的弱點，對這些弱點、 脆弱性及威脅事件加入風險發生時的後果推論及判斷，並依序列出風險的等級及劃分可接受風險值的範圍，找出可能即時解決的方法，以降低風險發生時的危害狀況。

3. 風險處理(Risk Treatment)：依據風險評估所列風險等級的優先順序加以處理，處理的方法包括降低風險的產生及檢視組織內的活動項目，若活動易引起某些異 常狀況而產生風險時，應加以避免或做風險的移轉，例如為活動項目加入保險機 制，或者簽訂保障合約書，當風險產生時，可以申請理賠。
4. 風險接受(Risk Acceptance)：依據組織決策者劃分之可接受的風險，做定期的文件紀錄檢視，因風險的可接受度不是絕對的是或否，仍需依照風險事件發生時 的情況做評估，對於某些不符合組織的正常風險的驗收標準（例如某些可接受風 險的降低成本過高）等，必須列出接受此風險的理由。
5. 風險溝通(Risk Communication)：持續蒐集風險資訊，以獲得新的資訊安全知識，對組織的風險管理結果提供保證，並支持組織的決策，分享組織風險管理的結果。
6. 風險監控與審查(Risk Monitoring and Review)：組織目前所制定之風險管理制度並非固定不變，風險的發生會隨著外在環境因素而改變，隨時會因新的弱點及 威脅事件的產生而有所更動，因此必須持續監控組織環境的異常現象，隨時掌握 新的弱點及威脅事件，並且更新，以維持組織風險管理機制的正常運作，保護組織的資訊安全。

2.3 風險評估

風險是由威脅(Threats)、弱點(Vulnerabilities)與資產價值(Assets Value)三要素所構成，風險是資產所受到的威脅、存在的薄弱點及威脅利用薄弱點所造成的潛在影響三方面共同作用的結果，其關係如圖 2-2 所示。以 ISO 27001 標準定義風險一詞為可能對一個或群組資產可能之弱點產生威脅，以致產生損失或傷害資產。威脅是指資訊資產遭受外來安全衝擊的影響，如火

災、水災及駭客入侵。弱點是指資訊資產的安全管控不足所帶來的影響，如人為疏失、網路漏洞。因此，風險評估之意義在分析組織所面臨的威脅存在的弱點。

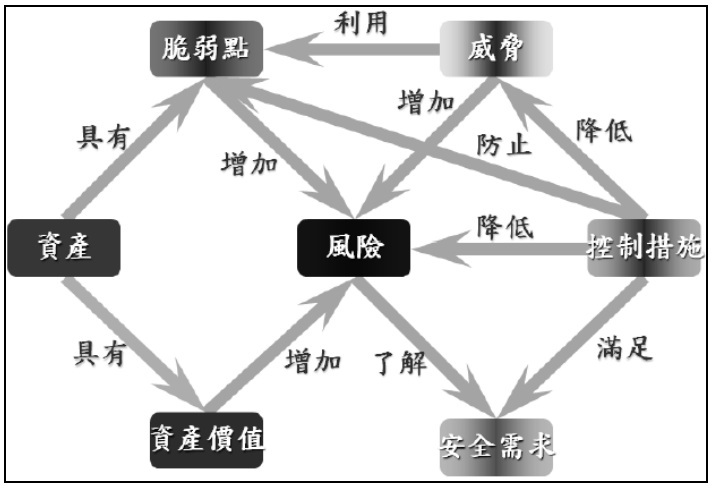


圖 2-2 資產、威脅、脆弱點、風險關係圖

CNS 27005 於其附錄 C 中，亦提供非常多的威脅範例清單，如表 2-2，例如天災類的洪水、暴風雨、地震、雷擊，人為類的人員短缺、錯誤維護、使用者錯誤，科技類的網路故障、流量超過負荷、硬體故障等等，可使威脅審查的範圍更加明確，並且更容易操作。

表 2-2 威脅類別範例

型式	威脅
物質損害	火災
	水災
	汙染
	重大意外
	設備或媒體的破壞
	灰塵、腐蝕、結凍
自然事件	氣候現象
	地震現象
	火山現象
	氣象現象
	水災
喪失基礎服務	空調或水供應系統故障
	電力供應喪失
	電信設備故障
輻射擾亂	電磁輻射
	熱輻射

	電磁脈衝
資訊之破壞	破解干擾訊號之攔截
	遠端間諜
	竊聽
	媒體或文件之失竊
	設備之失竊
	由回收或廢棄媒體之資料擷取
	揭露
	來自不受信賴來源之資料
	竄改硬體
	竄改軟體
	位置偵測
技術上之失效	設備故障
	設備機能失常
	資訊系統飽和
	軟體機能失常
	資訊系統可維護性之破壞
未經授權之行動	未經授權的使用設備
	軟體之詐欺複製
	使用偽造或複製之軟體
	資料毀損
	非法之處理資料
功能之危害	使用錯誤
	濫用權限
	偽造權限
	行動之否認
	人為可用性之破壞

資料來源：CNS 27005 附錄 C

脆弱點指的是組織資訊安全的弱點或漏洞，也就是資產本身的弱點。脆弱點一直與資產共存，本身並不會造成資產的傷害，但是脆弱點卻是可能是威脅影響資產的一種或多種情況，如果脆弱點沒有妥善的處理，可能會形成威脅。CNS 27005 提供了一些脆弱點的範例，例如關鍵人物的缺席、不穩定的動力、未受保護的電纜線、安全意識的缺乏、密碼權限的錯誤分配、安全訓練不足、未安裝防火牆、未上鎖的門等等，如表 2-3、表 2-4 所示。

表 2-3 硬體、軟體與網路類別之脆弱點範例

型式	脆弱性之範例	威脅之範例
硬體	儲存媒體之維護不足／錯誤安裝	危害資訊系統可維護性
	缺乏定期更換方案	設備或媒體之破獲
	對濕度、灰塵、髒污的感受度	灰塵、腐蝕、結凍
	對電磁輻射的敏感性	電磁輻射
	缺乏有效的組態變更管理	使用錯誤
	對電壓變化的感受性	電壓供應喪失
	對溫度變化的感受性	氣象現象
	為保護之儲存體	媒體或文件之失竊
	汰除時不小心	媒體或文件之失竊
	未控制之複製	媒體或文件之失竊
軟體	無或不充分之軟體測試	濫用權限
	軟體上熟知之缺點	濫用權限
	離開工作站時未”登出”	濫用權限
	汰除或再使用儲存媒體未適當地消磁	濫用權限
	欠缺稽核存底	濫用權限
	錯誤之存取權限配置	濫用權限
	廣泛散佈之軟體	資料毀損
	以時間而言，將應用系統程式應用至錯誤之資料	資料毀損
	複雜之使用者介面	錯誤使用
	欠缺文件	錯誤使用
	不正確之參數設定	錯誤使用
	不正確之日期	錯誤使用
	欠缺識別與鑑別機制，像是使用者鑑別	偽造權限
	未保護之通行碼	偽造權限
	不良之通行碼管理	偽造權限
	啟動不必要服務	非法處理資料
	不成熟或新的軟體	軟體機能失常
	對開發者不清楚或不完整之規格	軟體機能失常
	欠缺有效的變更控制	軟體機能失常
	未控制之下載與使用軟體	竄改軟體
	欠缺備份副本	竄改軟體
	欠缺對建築物、門窗之實體保護	媒體或文件之失竊
	產生管理報告失敗	未經授權之使用設備
網路	欠缺寄送或接收訊息之證明	行動之否認
	未受保護之傳輸線	竊聽
	未受保護之敏感性訊務	竊聽
	不良之電纜接合	電信設備故障
	單點故障	電信設備故障
	欠缺寄送者或接收者之識別與授權	偽造權限
	不安全之網路架構	遠端間諜
	以明文傳送通行碼	遠端間諜
	不適當之網路管理(選路之彈性)	資訊系統飽和
	未受保護之公用網路連線	未經授權的使用設備

表 2-4 人員、場域與組織類別之脆弱點範例

型式	脆弱性之範例	威脅之範例
人員	缺人人員	人員可用性之違反
	不適當之招募程序	設備或媒體之破壞
	不足的安全訓練	使用錯誤
	不正確去使用硬體或軟體	使用錯誤
	缺乏安全認知	使用錯誤
	欠缺監視機制	非法處理資料
	欠缺正確使用電信介質和送訊息的政策	未經授權的使用設備
場域	對建築物與房間部適當或草率之實體存取控制	設備或媒體之破壞
	位置位於億餘有水災的區域	水災
	不穩定之電力網	電力供應喪失
	欠缺對建築物、門窗之實體保護	設備之失竊
組織	欠缺使用者註冊予註銷註冊之正式程序	濫用權限
	欠缺存取權限審查(監督)之正式程序	濫用權限
	與客戶及／或第三方之契約中(關於安全)之條款欠缺或不足	濫用權限
	欠缺監視資訊處理設備之正式程序	濫用權限
	欠缺定期之稽核(監視)	濫用權限
	欠缺風險識別與評估之程序	濫用權限
	欠缺紀錄於管理員與操作員日至之錯誤報告	濫用權限
	不適當之服務維護回應	危害資訊系統可維護性
	欠缺或不充分之服務等級協議	危害資訊系統可維護性
	欠缺變更控制程序	危害資訊系統可維護性
	欠缺 ISMS 文件控制之正式程序	資料毀損
	欠缺 ISMS 記錄監督之正式程序	資料毀損
	欠缺公開可用資訊授權之正式程序	來自不可信賴來源的資料
	欠缺資訊安全責任之適當配置	行動之否認
	欠缺持續計畫	設備故障
	欠缺電子郵件使用政策	使用錯誤
	欠缺引進軟體至運作中之系統的程序	使用錯誤
	欠缺管理員與操作員日誌之紀錄	使用錯誤
	欠缺機密資訊處理之程序	使用錯誤
	工作說明中欠缺資訊安全責任	使用錯誤
	員工契約中(有關資訊安全)的條款欠缺或不足	非法處理資料
	欠缺以定義之資訊安全事故懲處過程	設備之失竊
	欠缺使用行動電腦之正式政策	設備之失竊
	欠缺場所外資產之控制	設備之失竊
	欠缺或不足之"桌面淨空和螢幕淨空"政策	媒體或文件之失竊
	欠缺資訊處理設備之授權	媒體或文件之失竊
	欠缺以建立的安全危害監視機制	媒體或文件之失竊
	欠缺定期之管理階層審查	未經授權之使用設備
	欠缺通報安全弱點之程序	未經授權之使用設備
	欠缺遵循智慧財產權規定之程序	使用偽造或複製之軟體

資料來源：CNS 27005 附錄 D

風險評估方法須為一系統化之方法論，經過資訊安全專家確認後均可應用，並不加以限定用某一種方式。常見之風險評估分析方法包含專家討論、群體決策之德菲法(Delphi)、因素分析(Factor Analysis)、錯誤樹分析(Fault Tree Analysis，FTA)、失敗模式與影響之關鍵分析(Failure Mode and Effect Criticality Analysis，FMECA)等；常用的分析工具為「風險評估矩陣法」。風險評估可區分為定性(Qualitative)與定量(Quantitative)兩類方式。定量與定性方法之優缺點比較說明如表 2-5 所示。CNS 27005 之 8.2.2.1 風險估計方法論亦提出兩項風險評估法：

1. 定性評估法則：使用量度尺標，針對重要的推論區分為低、中、高評等，及這些推論可能發生的機率。
2. 定量評估法則：使用數值法則定義推論結果與發生機率，此方法依賴正確與完整的數值資料做為分析依據，數值的來源來自影響組織資產與運作意外事件的歷史資料。

表 2-5 定性與定量風險評估優缺點比較表

	定量方式	定性方式
優點	■ 以財務角度定價較為精準 ■ 結果可用簡單易懂之數據表示 ■ 隨著組織建立數據的歷史紀錄，其精準度將隨時間的推移而提昇 ■ 容易分析決策具調理	■ 易於風險排序 ■ 更容易達到一致意見 ■ 無須量化威脅頻率 ■ 無須確定資產的財務價值 ■ 便於非安全與 IT 人員參與
缺點	■ 某些資訊資產不易以數字呈現 ■ 主觀資產的成本不易衡量 ■ 給定風險的影響值以參與者的主觀意見為基礎 ■ 調查分析數值非常耗時間與成本 ■ 結果只用財務術語來表示，對非技術性人員而言可能難以理解	■ 易受人員主觀意識影響 ■ 在重要的風險之間沒有足夠的區別 ■ 難以證明投資控制措施實施是正確，因為沒有成本效益分析為基礎 ■ 結果取決於建立的風險管理小組評估專業素質

資料來源：陳冠彰，2005 年 [7]

2.3.1 定性風險

定性風險是指對已界定出的風險評估其發生的機率與衝擊，決定其對企業營運影響的優先等級。定量風險分析是指以計量方式分析每一項風險對企業營運影響的程度。(范淼，2002)。定量分析其主要目的是建立順序尺度以衡量風險權值，採用概念模式或機率模式以計算出風險值， 風險評分(R)=發生機率(P) X 衝擊(L)，最後針對個別風險作加總，求出整體風險值。

定性風險分析是指對已界定出的風險評估其發生的機率與衝擊，決定其對企業營運影響的優先等級。輸入項目為原始資料、已界定之風險、機率與衝擊的順序尺度，進行分析各項風險事件，產出項目為整體風險評等、風險優先等級清單及定性風險分析結果之趨勢。

2.3.2 定量風險

定量風險分析經常使用方法為專家的深度訪談、敏感度分析、群體決策的德菲法(Delphi)、決策樹分析與模擬。 學術度，其為一整合性專家群體意見的分析方法，可將一個複雜的系統從風險類別層級加以拆解成細部風險屬性，例如資訊系統風險、人員管制風險、技術風險等，建立一個系統風險的整體架構，以決定系統風險水準與風險事件可控制程度。在執行風險分析時，必須詳細考量定性與定量分析之優缺點，定量分析的優點在於可以提供風險的機率或數值。定性分析的優點在於可對風險做排序，以往定量方式在資訊安全管理中佔據了主流地位，但隨著組織規模與營業項目大幅增高，以定量計算風險實在相當耗費人力與成本，所以許多組織開始採用定性方式以迅速找出高風險資產，再搭配定量方式詳細計算其風險變動[7]。

2.3.3半定量風險

在半定量風險中，係用實際數值表示上述的定性分析等級。但是所敘述的數值並不直接相當於實際的影響程度與機率，半定量分析之目的只是提供一個比定性分析更精確的數字以便進行風險優先順序，並不決定風險的實際價值。

2.4 層級分析法

層級分析法（Analytic Hierarchy Process,AHP）是 1971 年由 Thomas L. Saaty（匹茲堡大學教授）所發展提出的一套決策方法[11]，為主觀評估下的定量分析法。利用關聯的架構建立具有相互影響關係的階層結構(Hierarchical Structure)，運用在將複雜的問題作出有效的決策，或在風險不確定的清況下作有效的決策，或為了在分歧的判斷中尋求一致性。主要應用於不確定情況下及具有多數評估準則之決策問題。層級分析法促使複雜的決策問題系統化，由技術、社會、經濟與政治等層面予以層級分構，藉由量化的判斷來綜合評估，以提供決策的充分資訊，並降低決策的風險。

層級分析法具有理論簡單、易於操作且富彈性之特性，可有效整合專家與決策者意見，獲致嚴謹並具可行性之決策結果；此外並可結合主觀的決策者意見及客觀之決策相關資訊，充分納入主、客觀面向的考量。

2.4.1AHP的優點與應用

AHP 多年來應用於經濟、社會、及管理科學等領域，並利用階層結構幫助決策者對事物作更深的瞭解，進而處理複雜的決策問題。階層系統方式的發展，已在社會及行為科學上被廣泛的應用，能夠使複雜的問題簡化，Narasimhan(1983)曾經歸納出 AHP 的優點如圖 2-3，其主要效益為[8]：

(1) 可將主觀的決策模式化，提供較為準確的判斷參考。

(2) 有相關軟體協助，可進一步作敏感度分析。

(3) AHP 數量化的結果可以供作群體決策的基礎，做為彼此溝通的工具。

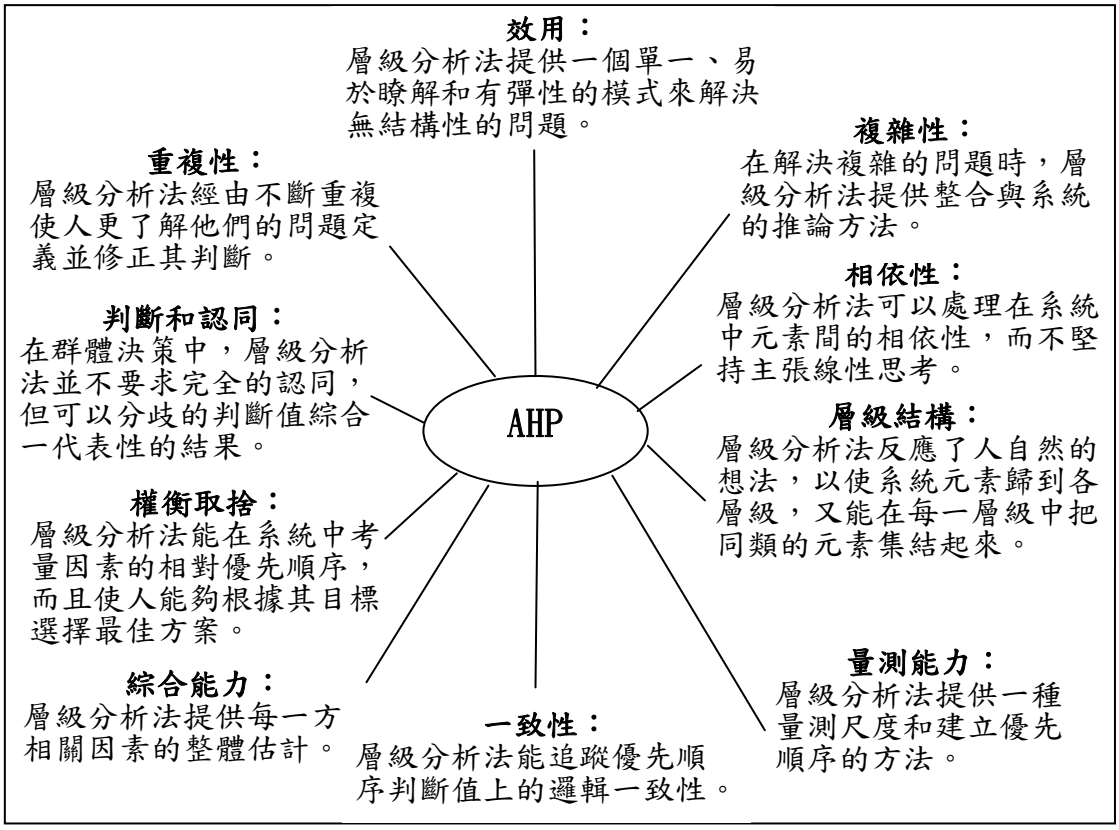


圖 2-3 層級分析法優點說明圖

層級分析法與其他評估方法的比較，層級分析發具有高信度、高效度與高研究廣度等優點，但其執行方式亦較為複雜，其與其他方法比較如表 2-6：

表 2-6 層級分析法與其他研究方法之比較表

比較構面	複雜度	效度	信度	研究廣度
層級分析法	高	高	高	高
德菲爾法	高	低	高	低
權數評估法	高	低	低	高

資料來源：曾雪卿（2009）

2.4.2 AHP 執行步驟

AHP 方法在進行之前，鄧振源、曾國雄[9]提出必須先進行假設，而在制定假設條件時，主要包括下列七項：

(1) 一個系統或問題可被分解成許多被評比的種類或成分(Components)，形成具方向性之網路的層級結構。

(2) 層級結構中，每一層級的要素均假設具獨立性(Independence)。並且可以用上一層級內的某些或所有的要素為基準，進行評比。

(3) 評比時，可將絕對數值尺度轉換成比例尺度(Ratio Scale)。例如 A1 比 A2 重要比值則為 5/1。

(4) 成對比較(Pairwise Comparison)後之矩陣倒數對稱於主對角線，可用正倒值矩陣(Positive Reciprocal matrix)處理。

(5) 偏好關係滿足遞移性(Transitivity)，但完全具遞移性不容易，因此容許不具遞移性質，但必須測試其一致性(Consistency)的程度，藉以測試不一致性的程度若干。

(6) 要素的優勢比重，係經由加權法則求得。

(7) 任何要素只要出現在層級結構中，不論其優勢比重為多少，均被認為與整個評比目標結構有關。

層級建立在 AHP 方法的進行中是相當重要的一個部分，在進行假設後，即必須開始建立層級結構，用意在將複雜的問題簡化，使決策者更容易做出正確的決定。AHP 的每一個層級皆表示對原問題的一個重要部分。建立層級的優點可歸納出以下幾點：(Saaty,1980)[11]

(1) 提供一個有意義的整合系統，而整合是將一個複雜的系統轉換成簡單的成分。

(2) 很清楚的說明上一層內的各因子之優先權重發生變動時,將會如何影響下一層次內各因子的優先權重。

(3) 將元素分成不同層級的集合,易於達成工作。且比直接評估整體系統有效率。

(4) 對整個系統更詳細的劃分層級結構,以更深入的瞭解層級結構的目標。

(5) 發展自然系統以層級的方式是相當迅速及有效的。

(6) 層級具有可靠性(Reliable)及彈性(Flexibility);也就是說局部的改變不會影響整體的結構。

(7) 對於人類的認知而言,層級式的關係是容易被接受的,而且具備易於溝通的特色。

AHP 方法在進行評估上,主要是分為兩大階段,第一是層級的建立,第二是層級評估。AHP 首先是將複雜之系統,匯集專家學者及決策者之意見評估,以簡明之要素層級結構加以表示,並將評估的項目來做成要素的成對比較且建立矩陣,據以求得特徵向量,代表層級要素的優先順位;並衍生最大特徵值,用以評定成對比較矩陣一致性的強弱,供作決策資訊取捨與否或再評估之參考指標。AHP 法進行各步驟說明如下[10]:

2.4.2.1 確定評估問題

對問題所處的系統應儘量擴大,並將可能影響問題的要因納入問題中。同時成立規劃群,對問題的範圍加以界定,問題界定可分為澄清問題與分解問題。

2.4.2.2 影響要素分析

在此階段有收集資訊及確認問題和所需方案兩步驟;前者可採用文獻分

析、腦力激盪等方法，蒐集可供確認問題性質、範圍、影響因素、可用資源等資訊；後者係確定問題和分析目的並視需要而構思可能選用方案。

2.4.2.3 將問題建立層級式的架構

層級為研究問題之骨架，用以探討因素間及因素對方案之影響力。利用前面所歸納出影響問題決策的評估準則要素予以層級化。根據Saaty的定義此種結構乃是將我們對問題所認定之要素(Entities)組合成幾個互斥的集合，而形成上下『隸屬』的層級關係，並假設：

1. 每一層的任一集合僅受上一層集合的影響
2. 同層中的集合彼此互斥
3. 集合中元素與元素之間相互獨立

2.4.2.4 建立成對比較矩陣

成對比較矩陣之建立，在於求取要素間相對的重要程度。在某一個層級之要素，以上一層級某一個要素為評估準則下，進行要素間的成對比較。若有n 個要素，則必須進行C_n^2 次的比較。

AHP 是採用比率尺度做為衡量成對比較矩陣的衡量尺度，所謂比率尺度就是尺度的數值是可以加減乘除的，且有固定的原點，在自然科學方面最常應用。基本上劃分為五項：同等重要、稍重要、頗重要、極重要和絕對重要，再加上另外的四個尺度，介於每兩者之間的強度，總共可以區分為九個尺度，而分別給予 1 至 9 之比重(Saaty, 1990)。AHP 評估的名義尺度的內容與意義如表 2-7。

表 2-7 AHP 評比尺度表

評估尺度	定義	解釋
1	同等重要(Equal importance)	兩事件的貢獻度具同等重要性
3	稍重要(Moderate importance)	經驗與判斷顯示稍微喜歡哪一方案
5	頗重要(Essential importance)	經驗與判斷顯示強烈喜歡哪一方案
7	極重要(Very strong importance)	實際非常強烈喜歡哪方案
9	絕對重要(Extreme importance)	有足夠證據肯定喜愛哪一方案
2,4,6,8	中間值(Intermediate values)	折衷值介於之前評估尺度間

資料來源：Saaty，1990

2.4.2.5 一致性的檢定

由於各層級間的重要性不同，所以要測試整體層級結構是否具有一致性。一致性指標值，不論在決策者判斷的評量或是整個層級結構的測試，Saaty 建議宜在 0.1 左右(一般採 C.R.<0.1)，評估的結果要能通過一致性檢定才可顯示填答問卷者的判斷前後一致，且具合理性。若每一成對比較矩陣的一致性程度皆符合所需，則尚須檢定整個層級結構的一致性。如果整個層級結構的一致性程度不符合要求，顯示層級的要求關聯有問題，必須重新進行要素及其關聯性分析。計算最大特徵值($\lambda_{\max}$)與特徵向量(W)來檢定成對比較矩陣是否具有一致性，根據 Saaty 建議以一致性指標(Consistency Index, C.I.)與一致性比例(Consistency Ratio, C.R..)，檢定成對比較矩陣的一致性。

(1)一致性指標(Consistency Index, C.I.)，其公式如下[8][9]：

$$C.I. = \frac{\lambda'_{\max} - n}{n-1}$$

當 $C.I. = 0$ ，表示前後判斷完全一致。當 $C.I. = 1$，表示前後判斷不一致。

而 $C.I. \leq 0.1$，為可容許偏誤。

(2)隨機指標(Random Index, R.I.)：此值可藉由查隨機指標 R.I.值對照表獲得。一致性指標(C.I.)的大小又受矩陣 A 階數及評估尺度數的影響，矩陣在階數及評估尺度數皆已知情況下，所產生的 C.I.值稱為隨機指標 (Radom Index, R.I.)。

(3)一致性比率(Consistency Ratio, C.R.)：其公式如下

$$C.R. = \frac{C.I.}{R.I.}$$

在相同階數的矩陣下，若 $C.R. \leq 0.1$ 表示矩陣的一致性程度令人滿意。

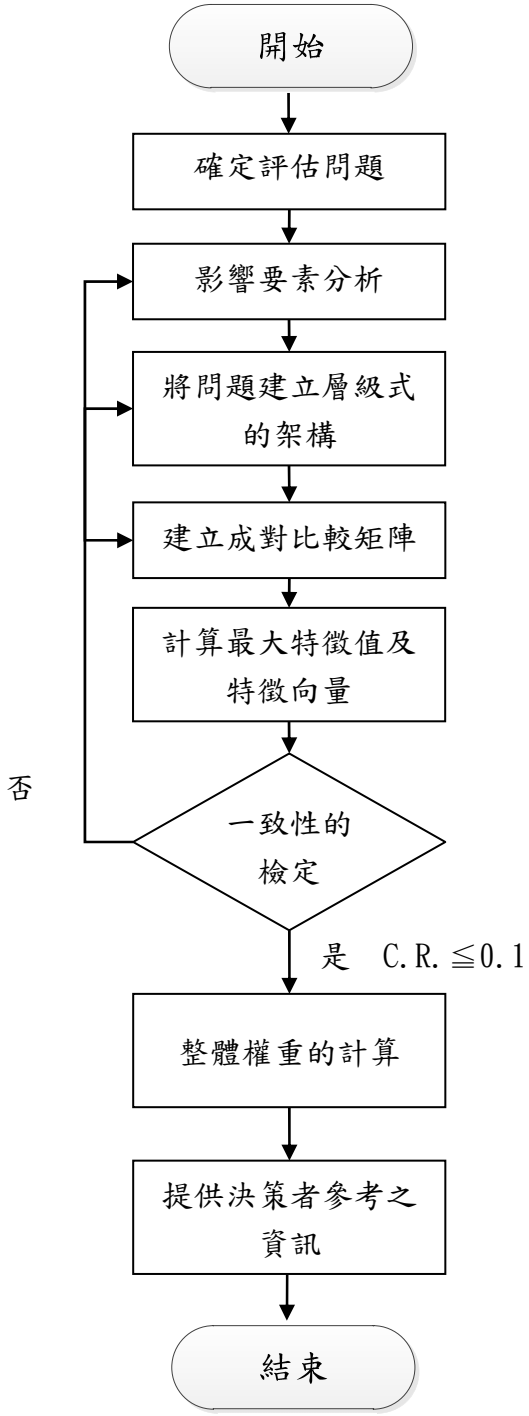


圖 2-4 層級分析法流程圖

第3章　個案研究

本研究主要分析中部地區兩學術單位，兩校規模皆為大學體系，組織內部亦成立獨立資訊部門，其工作內容除了校務系統開發與維護外，還包含網路管理、電腦維修問題排解。此兩個案的背景相同之處很多，如：

(1)　校風與學校歷史沿革，皆為中部歷史悠久之教會學校。

(2)　資訊單位分工與業務，皆由電算中心統籌全校資訊建設與發展。

(3)　導入 ISO 27001 時間，皆於 95 至 96 年間導入 ISO27001 國際認證。

(4)　風險評估方法，皆由同一間顧問輔導公司提供之方法。

因此非常適合作為本研究之個案。

3.1　個案之風險評估方法

兩個個案導入ISO27001 時間相近，亦找同家顧問公司輔導資訊安全制度建置，故使用同一套風險評估方法。風險評估方式，分述如下：

3.1.1 資產分類與鑑價

依據 ISO/IEC 27005:2008 附錄 B，建議將業務程序與活動，及活動所產生之資訊列為主要資產，將硬體、軟體網路、人員、場所及組織架構等視為支援性資產，著重點於機關之施政業務活動。本研究所用之風險評估方法依資訊資產之價值、對組織運作的關鍵程度、及其機密性、可用性和完整性並參考 ISO27005 分類方式加以調整，而將資產類別分為 5 大類，包含人員類、文件類、實體類、軟體類及服務類。其分類方式說明與範例如表 3-1 所示。

表 3-1　資產類別說明表

資產分類	包含	範例
人員類	內部人員 外部人員	正式聘用人員、試用人員、研發人員、管理人員、維護人員、DP 人員、客服人員、人力發展人員、MIS 人員、臨時工作人員、訪客、受訓人員、委外維護人員、委外保全人員、包商或供應商
文件類	電子類文件 紙本類文件	資料庫檔案、備份資訊、網路架構圖、系統文件、使用手冊、教育訓練教材、操作或支援程序、緊急應變計畫、合約、報表、報告、通訊錄、表單…等
實體類	一般硬體 電訊 電腦媒體 電腦保護設施	包含電腦設備(伺服器、主機、筆記型電腦、個人電腦、工作站)、CD 燒錄器、CD-ROM / DVD 放映機、磁帶機、 軟碟機、光碟機、PDA（個人數位助理）、印表機、印刷機橋接器、集線器、路由器、網路交換器、數據機、電話自動交換機、網路纜線、防火牆、視訊會議設備、傳真機、手機 CD-ROM / DVD、硬碟、磁片 、磁帶、移動式硬碟、錄音/影帶、絕緣安全電纜、不斷電系統、穩壓器、機櫃
軟體類	商用軟體 內部發展軟體	套裝應用軟體、系統軟體、開發工具、套裝軟體、防火牆軟體、防毒軟體、驗證軟體、資料庫管理系統（DBMS）、加密軟體、文件管理系統、內部開發程式、內部發展系統
服務類	內部服務 外部服務 基礎架構 建築 建築保護設施	設備借用服務、內部訊息交換服務、技術支援維護部門、網路服務（ISP）、電話服務、外部維護服務、外部安全服務（巡邏）、水電公用設施服務、不斷電系統、穩壓器、機櫃、災害復原地點、網管中心、開發室、電腦室、操作中心、伺服器室、火偵測、熱偵測、水偵測系統、滅火系統、溫濕度計

3.1.2 資訊資產衝擊評價

為量化各資訊資產之價值與重要度，依資產之機密性（Confidentiality，簡稱

C)、完整性(Integrity,簡稱I)、可用性(Availability,簡稱A)、適法性(Legislation,簡稱L)等四項因子,並根據損害程度給予分數:7(極高)、5(高)、3(中)、1(低)、0(不適用) 。

3.1.3 資訊資產群組

為降低風險評估負擔,減少弱點、威脅的重複識別,個案依下列原則進行資訊資產群組,並以群組後之資訊資產進行風險評估作業。

1. 資訊資產價值相同
2. 存在於相同的實體、邏輯環境
3. 遭遇弱點、威脅相同

3.1.4 識別威脅與弱點

對於威脅的定義,是指宣告意圖造成損害、痛苦或不幸。威脅可能形成一個有害的事件,且該事件對於系統、組織或資產會造成傷害,它有可能是蓄意或者是意外,也有可能是人為或者是天災。資訊安全管理制度認為資產容易受到許多威脅,而這些威脅來自於資產之脆弱性。若由Spruit等人的分類狀況來剖析,威脅到資訊安全的因素可歸納至兩個方向:天然因素與人為因素,並將其歸納如表 3-2 所示[13]。

表 3-2 資訊安全威脅分析表

問題類別		原因	說明		後果
天然因素	災害	外部來的自然現象故障	火災、水災、地震、打雷及溫濕度異常		無法正常服務
	故障	本身系統發生故障	硬體、軟體、網路故障		
人為因素	過失	人為錯誤或怠慢造成的故障	疏失	●操作疏失 ●維護疏失 ●管理疏失	資訊資產濫用

人為因素	故意	人為惡意或蓄意造成之故障	破壞	●電腦系統破壞 ●資訊設備破壞 ●資料程式破壞 ●資料程式竄改	資訊資產濫用
			不當使用	●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	●不當蒐集資料 ●不當使用資料 ●不當公開資料	

資料來源：黃慶堂 1999 與本研究整理

3.1.5 鑑別風險

鑑別風險係依資訊資產弱點之脆弱度及威脅之發生機率進行評分，以鑑別各項威脅對資訊資產所造成之機密性、完整性、可用性及適法性之衝擊。資訊資產之弱點係指資訊安全的脆弱點，其本身不會造成傷害，但是可能產生一種或多種威脅，對資產造成影響。資訊資產之脆弱度即在評估資訊資產弱點的嚴重程度，亦即容易被威脅所利用的程度，我們將以個案輔導顧問公司提供兩個案之弱點評分等級，如表 3-3 所示，以進行風險鑑別。

表 3-3 弱點評分等級說明表

評分	等級	說明
7	非常容易被利用(嚴重)	招致威脅發生的可能性 75%(含)或需要於月內解決
5	經常會被利用(高)	招致威脅發生的可能性 74%~50%(含)或需要於半年內解決
3	有時可能會被利用(中)	招致威脅發生的可能性 49%~25%(含)；需要於年內解決
1	不容易被利用(低)	招致威脅發生的可能性 24%~1%或可以長時間存在
0	不適用	N/A

資訊資產之威脅則係指可能會對系統或組織及其資訊資產造成傷害的事件，資產通常都會面臨許多不同的威脅。威脅必須利用資產的弱點才能對資產造成傷害。本項目即在評估資訊資產威脅可能發生的機率，其評估等級方式見表 3-4 所示。

表 3-4 威脅評估等級說明表

評分	等級	說明
7	發生可能性極高	每月至少發生兩次(MAX：∞次/年；MIN：24 次/年)
5	發生可能性高	每月發生一次以上(MAX：23 次/年；MIN：12 次/年)
3	發生可能性中度	每季發生一次以上(MAX：11 次/年；MIN：4 次/年)
1	發生可能性低或無	每年發生三次以下(MAX：3 次/年；MIN：0 次/年)
0	不適用	N/A

3.1.6 風險計算範例

風險計算係根據風險評估結果進行資訊資產評價，識別弱點之脆弱度、威脅之發生機率，並將此三項評分進行相乘，再依威脅對機密性、完整性、可用性、適法性所造成之衝擊影響進行風險值加總，此即求出該資訊資產之風險值，以下為所用參數及其說明：

C：資產價值之機密性

I：資產價值之完整性

A：資產價值之可用性

L：資產價值之適法性

CI：機密性之衝擊影響

II：完整性之衝擊影

AI：可用性之衝擊影響

LI：適法性之衝擊影響

V：弱點脆弱度

T：威脅發生機率

資訊資產總風險值 = Σ {（CI×V×T×C）+（II×V×T×I）+（AI×V×T×A）+（LI×V×T×L)}，圖 3-1 為資訊資產風險計算示意圖。

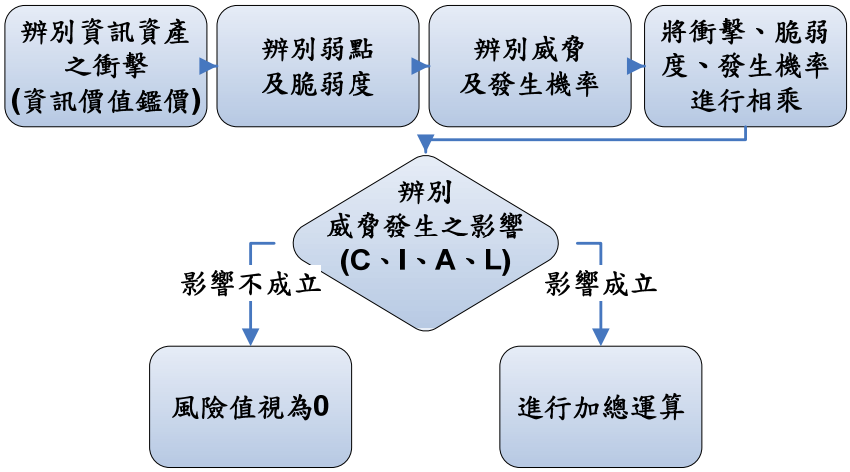


圖 3-1 風險計算示意圖

(1) 以個人電腦為例

以個人電腦為例之風險計算流程如圖 3-2 所示，其各步驟計算說明如下：

1. 依等級進行評分：0-不適用、1-低、3-中、5-高、7-極高。
2. 此資訊資產之鑑價結果為 C:3、I:3、A:3、L:1。
   - ■ 辨別有不明確的責任要求之弱點及嚴重度，其評分等級為 3。
   - ■ 辨別有人員的錯誤之威脅及發生機率，其評分等級為 3。
   - ■ 人員的錯誤之威脅會影響機密性(C)與可用性(A)。

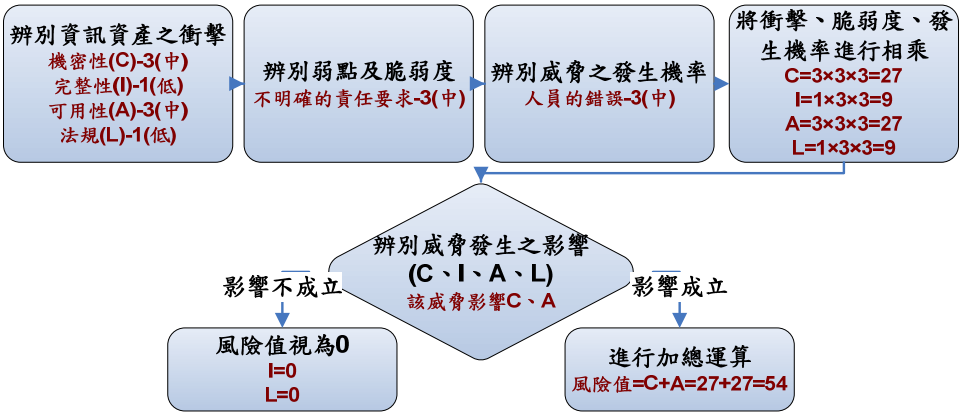


圖 3-2 個人電腦風險計算示意圖

3.2 個案風險評估結果：P大學

3.2.1 個案背景說明

P 大學為天主教大學，設有外語學院、人文暨社會科學院、理學院、管理學院、資訊學院等 5 大學院、22 個學系、19 個碩士班、2 個博士班、5 個碩士在職專班、1 個進修學士班及 3 個教學中心。於 96 年開始導入 ISO 27001 資訊安全管理系統。資訊部門分組為計算機及通訊中心分為行政教學組、網路通訊組、系統支援組、軟體開發組。其資安組織架構如圖 3-3 所示[12]。

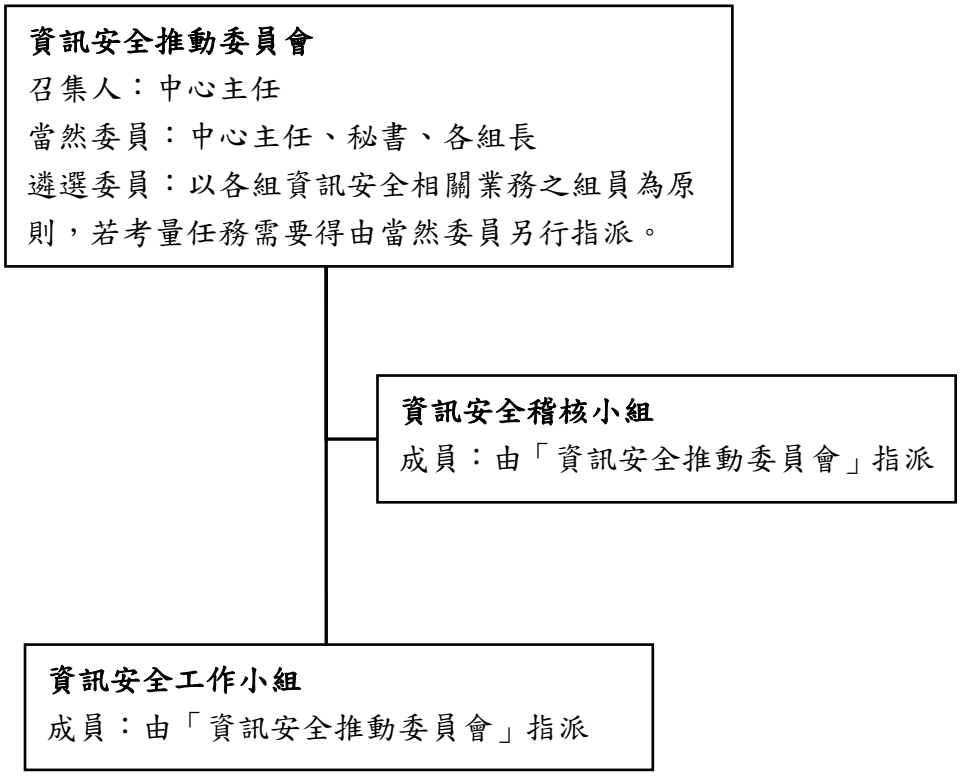


圖 3-3　P 大學資訊安全組織架構圖

3.2.2 P 大學風險評估結果

因資訊資產與風險評估結果內容具有機敏性，故刪除資產名稱，P 大學群組後之風險評估請參閱附錄二所示。表 3-5 及表 3-6 分別為其之資訊資產統計表及風險值統計表。

表 3-5　P 大學群組資訊資產統計表

文件類		軟體類		實體類				服務類					人員類		小計
電子文件	紙本文件	商用軟體	內部發展軟體	一般硬體	電訊	電腦媒體	電腦保護設施	內部服務	外部服務	基礎架構	建築	建築保護設施	內部人員	外部人員	
6	7	22	2	21	11	1	5	0	2	1	2	4	18	4	106

表 3-6　P 大學風險值統計表

分類 / 風險值	文件類	軟體類	硬體類	服務類	人員類	小計
100 以下	8	1	18	7	8	42
101-200	3	1	11	1	4	20
201-300	1	6	3	1	2	13
301-400	0	6	3	0	1	10
401-500	0	2	3	0	6	11
501-600	0	1	0	0	0	1
601-700	0	5	0	0	0	5
701-800	0	1	0	0	1	2
801-900	1	1	0	0	0	2
小計	13	24	38	9	22	106

3.3 個案風險評估結果：T大學

3.3.1 個案背景說明

T 大學為基督教大學，設有文學院、理學院、工學院、管理學院、社會科學學院、農學院、創意設計暨藝術學院及法律學院等八個學院，目前約有學生一萬七千多名，專任教師 550 人。於 95 年開始導入 ISO 27001 資訊安全管理系統。資訊部門分組為網路技術組、系統發展組、教學及研究支援組。資安組織架構如圖 3-4 所示：

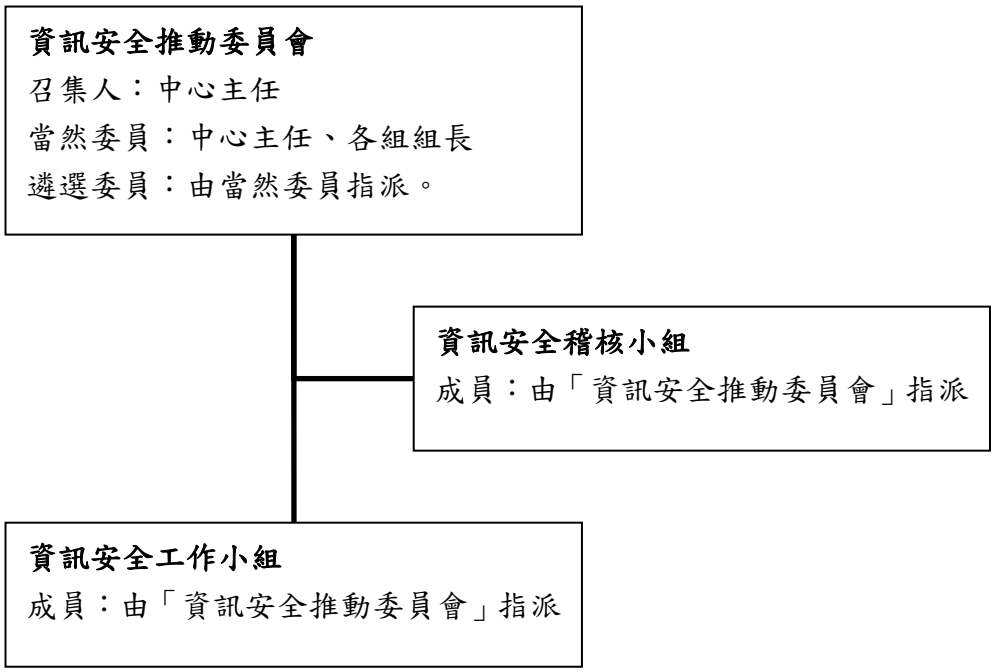


圖 3-4　T 大學資訊安全組織架構圖

3.3.2 T 大學風險評估結果

因資訊資產與風險評估結果內容具有機敏性，故刪除資產名稱，T 大學群組後之風險評估請參閱附錄三所示。表 3-7 及表 3-8 分別為其之資訊資產統計表及風險值統計表。

表 3-7　T 大學群組資訊資產統計表

文件類		軟體類		實體類			服務類				人員類		小計
電子文件	紙本文件	商用軟體	內部發展軟體	電腦保護設施	一般硬體	電訊	建築保護措施	外部服務	基礎架構	建築	外部人員	內部人員	
10	4	22	3	2	25	10	3	2	4	1	6	5	97

表 3-8　T 大學風險值統計表

分類 / 風險值	文件類	軟體類	硬體類	服務類	人員類	小計
100 以下	3	0	6	8	1	18
101-200	4	4	16	0	1	25
201-300	5	7	9	1	3	25
301-400	0	5	2	1	4	14
401-500	1	1	0	0	1	3
501-600	1	1	0	0	1	3
601-700	0	2	2	0	0	4
701-800	0	0	0	0	0	0
801-900	0	1	0	0	0	1
901~1000	0	1	0	0	0	1
1001 以上	0	3	2	0	0	5
小計	14	25	37	10	11	97

3.4 個案差異說明

兩個案之風險評估結果差異部分，分項次方式說明如後：

1. P大學群組後的資產數量共有 106 項，T大學群組後的資產數量共有 97 項。得知，兩校之資產數目差異不大。
2. P大學最高風險值為 884，最低風險值為 1；T大學最高風險值為 1625，最低風險值為 7。得知，T大學評估過程中識別出的弱點脆弱度與威脅發生機率較P大學高。
3. P大學高風險資產多屬校務行政系統驗證範圍，其中以軟體類最多；T大學之高風險資產多屬於網路管理驗證範圍之實體類與校務行政系統驗證範圍之軟體類。

第4章　研究方法與資料分析

本研究利用第三章所提之風險評估方式，採用層級分析法AHP方法探討上述兩個中部大學個案之風險評估實施的結果之差異原因。問卷的發放對象為個案之資訊部門有參與風險評估的資訊業務同仁與主管，實際的問卷回收數為 13 份。

4.1 層級分析架構

本研究所建構之評估目標主要是資訊安全風險評估之差異影響因子與項目彼此之間的重要程度。依Saaty的研究指出，因成對比較次數為C_2^n，n為項目數目，當n>7，人腦在評比思考過程容易產生錯亂與不一致的情形，因此盡可能使n<7。整個評定的層級架構係依據AHP方法所必須具有的層級結構，並以第三章風險評估個案研究中所提之風險評估方法，將之拆解為各層級之風險評估相關影響因素。本研究之層級階層架構如圖 4-1 所示，共分成三個層級：總目標、評估構面及評估準則。**總目標**的主要目的是計算資訊安全風險評估差異之影響因子項目彼此之間的權重；**評估構面**是探討影響風險評估之相關項目；**評估準則**是根據驗證範圍流程盤點資訊資產、評鑑資產價值的資產特性，及評估各類別資訊資產所可能面臨的威脅與弱點。其中第二層評估構面依照評估所需又分成「驗證範圍層面」、「資產特性層面」與「資產類別層面」。之後，再依照不同的屬性劃分出十四項的子項目以為第三個層級，其中在驗證範圍層面項目下劃分出五個子項目，在資產特性層面項目下劃分出四個子項目，在資產類別層面項目下劃分出五個子項目。

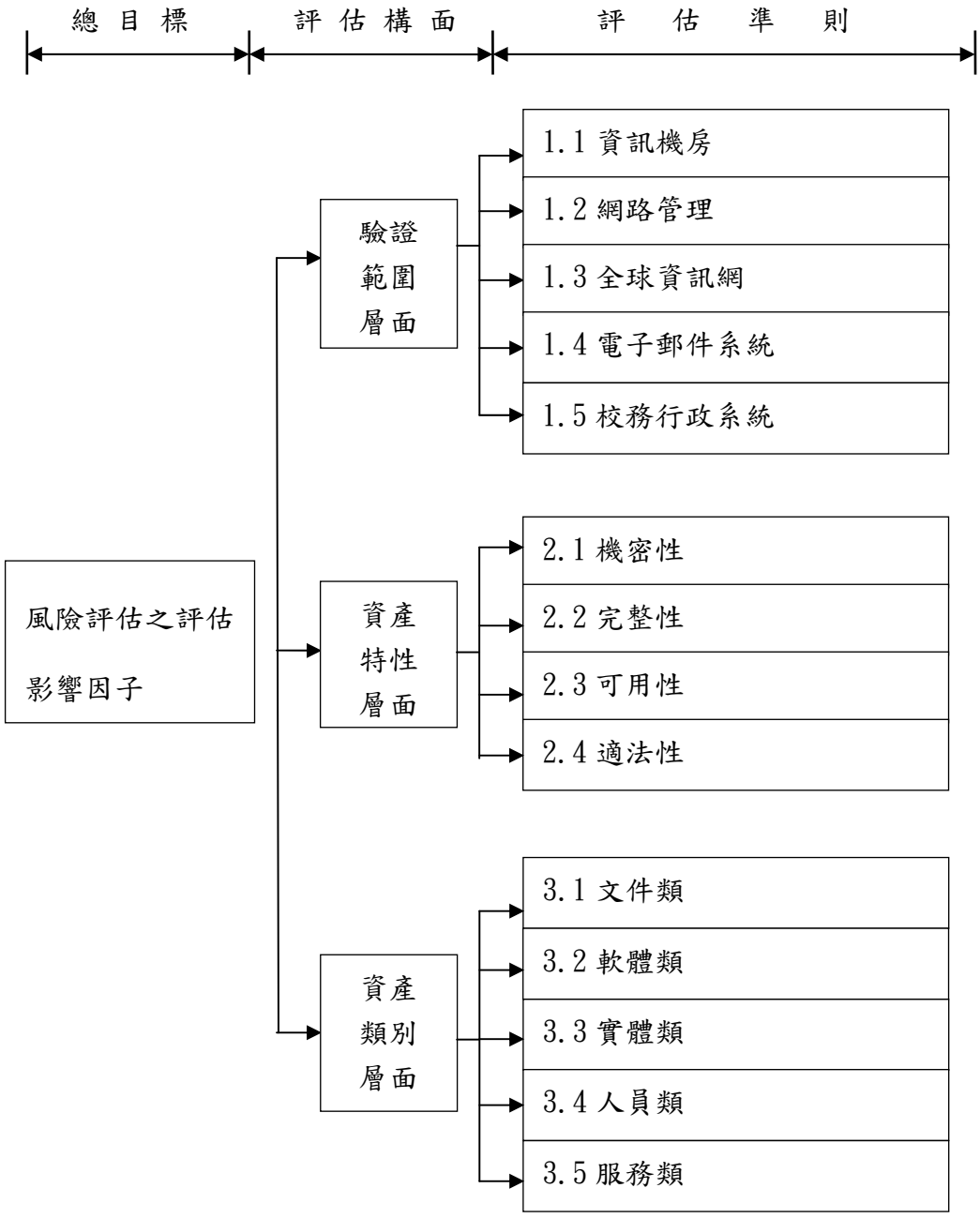


圖 4-1 資訊安全風險評估之影響因子層級架構圖

資料來源：本研究整理

茲將研究架構中所評估項目分類詳細條列如下：

一、驗證範圍層面

本層面所分成之五個子項目說明如下：

1.1 資訊機房：評定資訊機房維運之重要性。

1.2 網路管理：評定網路管理維運之重要性。

1.3 全球資訊網：評定全球資訊網維運之重要性。

1.4 電子郵件系統：評定電子郵件維運之重要性。

1.5 校務行政系統：評定校務行政系統維運之重要性。

二、資產特性層面

本層面所分成之四個子項目說明如下：

2.1 機密性：考量資訊資產分級、資訊資產洩露傷害程度、人員業務性質等機密特性之重要度。

2.2 完整性：考量資訊資產不完整時會造成損失影響範圍、正確性及完整性的要求程度等特性之重要度。

2.3 可用性：考量資訊資產可忍受服務中斷時間長度、仰賴系統程度、仰賴員工程度等特性之重要度。

2.4 適法性：考量資訊資產須遵守之法令、規範、合約義務或是組織內部之政策、章程要求等特性之重要度。

三、資產類別層面

本層面所分成之五個子項目說明如下：

3.1 文件類：考量紙本文件、電子文件之重要性。

3.2 軟體類：考量商用軟體、內部發展軟體之重要性。

3.3 實體類：考量一般硬體、電訊、電腦媒體、電腦保護設施之重要性。

3.4 人員類：考量內部人員、外部人員之重要性。

3.5 服務類：考量網路服務、主機服務、電話服務、建築、保護設施、一般公共設施(冷氣、電力、空調、照明) 之重要性。

4.2 問卷設計

AHP是以成對比較的方式進行，換言之是以對偶方式進行比較，而評估尺度的劃分則如表 4-1 所示，A1、A2、A3、A4 即分別代表評估的各個項目，並將兩兩比較的項目放置在比較表格的左右兩端，依作答者的權重衡量認定兩因素的重要關係。而其中A1 必須先與A2、A3、A4 進行兩兩比較，A2 則再與A3、A4 兩兩比較、A3 最後再和A4 進行比較，由強弱度的不同給予分數。

問卷依照 2.4 節AHP的方法說明，進而規劃出本研究的問卷形式，評估構面成對比較如表 4-2 所示；評估準則成對比較如表 4-3 及表 4-4 所示。一般成對比較程序是匯集專家學者的群體評估以取得一致評估觀點；但若有不同的觀點，亦允許同時並存，只需要在計算時將成對比較矩陣的數字採用幾何平均數綜合之。問卷以AHP成對比較評估表作答，將所欲評估的要素置於兩邊，評估尺度放置於要素之間。假設若有n個要素要進行評估，則需要評比n(n-1)/2 次。

表 4-1 問卷成對比較範例表

評估要素	絕對重要		極重要		頗重要		稍微重要		相同重要		稍微重要		頗重要		極重要		絕對重要	考量因子
	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
A1	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	**A2**
A1	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	**A3**
A1	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	**A4**
A2	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	**A3**
A2	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	**A4**
A3	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	**A4**

表 4-2　本研究問卷評估構面成對比較表

考量因子	重要程度																	考量因子
	絕對重要		極為重要		頗為重要		稍微重要		同等重要		稍不重要		頗不重要		極不重要		絕不重要	
	9:1	8:1	7:1	6:1	5:1	4:1	3:1	2:1	1:1	1:2	1:3	1:4	1:5	1:6	1:7	1:8	1:9	
1. 驗證範圍層面																		2. 資產特性層面
																		3. 資產類別層面
2. 資產特性層面																		3. 資產類別層面

表 4-3　本研究問卷評估準則成對比較表(一)

考量因子	重要程度																	考量因子
	絕對重要		極為重要		頗為重要		稍微重要		同等重要		稍不重要		頗不重要		極不重要		絕不重要	
	9:1	8:1	7:1	6:1	5:1	4:1	3:1	2:1	1:1	1:2	1:3	1:4	1:5	1:6	1:7	1:8	1:9	
1. 資訊機房																		2. 網路管理
																		3. 全球資訊網
																		4. 電子郵件系統
																		5. 校務行政系統
2. 網路管理																		3. 全球資訊網
																		4. 電子郵件系統
																		5. 校務行政系統
3. 全球資訊網																		4. 電子郵件系統
																		5. 校務行政系統
4. 電子郵件系統																		5. 校務行政系統

表 4-4　本研究問卷評估準則成對比較表(二)

考量因子	重要程度																	考量因子
	絕對重要		極為重要		頗為重要		稍微重要		同等重要		稍不重要		頗不重要		極不重要		絕不重要	
	9:1	8:1	7:1	6:1	5:1	4:1	3:1	2:1	1:1	1:2	1:3	1:4	1:5	1:6	1:7	1:8	1:9	
1. 機密性																		2. 完整性
																		3. 可用性
																		4. 適法性
2. 完整性																		3. 可用性
																		4. 適法性
3. 可用性																		4. 適法性

4.3 問卷對象與回收

填寫本研究問卷之受訪者皆係參與過組織風險評估過程之資訊安全工作。兩個案之受訪者背景資料如表 4-5 所示。

表 4-5 兩個案專家問卷受訪者背景資料表

受訪問卷編號	工作年資	資安/職能身分								
		程式設計師	備份系統管理員	資料庫管理員	機房管理人員	網路管理人員	資訊安全工作小組	校務行政系統管理者	電子郵件系統管理者	全球資訊系統管理人員
P1	**12**					✓	✓			
P2	**10**		✓				✓		✓	
P3	**15**		✓	✓			✓	✓	✓	
P4	**10**	✓					✓			
P5	**5**	✓					✓			✓
P6	**2**					✓	✓			
P7	**12**				✓		✓			
P8	**13**						✓			
T1	**15**			✓		✓	✓		✓	
T2	**1**	✓					✓			✓
T3	**16**				✓		✓			
T4	**8**	✓	✓				✓	✓		
T5	**9**	✓					✓			

本研究之專家問卷請參閱附錄四。問卷調查採用實地進行發放。受訪對象當場填寫完畢立即回收之方式。取得問卷後將內容逐一輸入基礎之客觀決策支援軟體Expert Choice中進行統計，建立單一問卷之各層級的相對權重，並求取各層級中評估構面與評估要素間之要素比重。

層級的相重權重中的區域優先權重(Local Prority)，或稱為局部優勢，為每一層級間準則的相對比較權重，亦即該層級內之相互比較結果；另一為全域優先權重(Global Prority)，亦稱為整體優勢，則係以上一層級之權重值乘以本層級各準則相對權重值之結果，藉以顯示該層級之權重值在整體層級中的權重值。Expert Choice會依據 2.4 節所述之運算方式及檢定，計算出各層之區域優先權重，及各層之區域優先權重相乘後之全域優先權重。Expert Choice的相關操作過程，包含層級建構(見圖 4.2)、構面計算結果(見圖 4.3)及區域優先權重計算結果(見圖 4.4)。

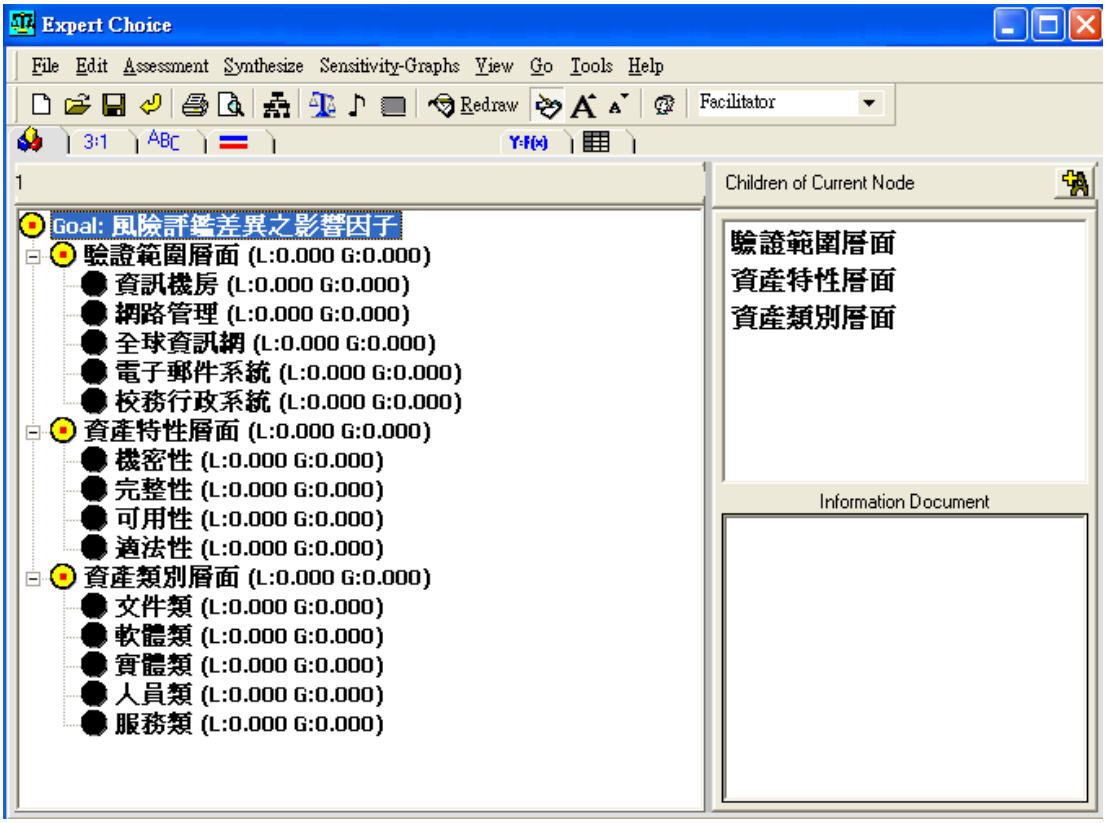


圖 4-2　Expert Choice 層級架構

資料來源：本研究整理

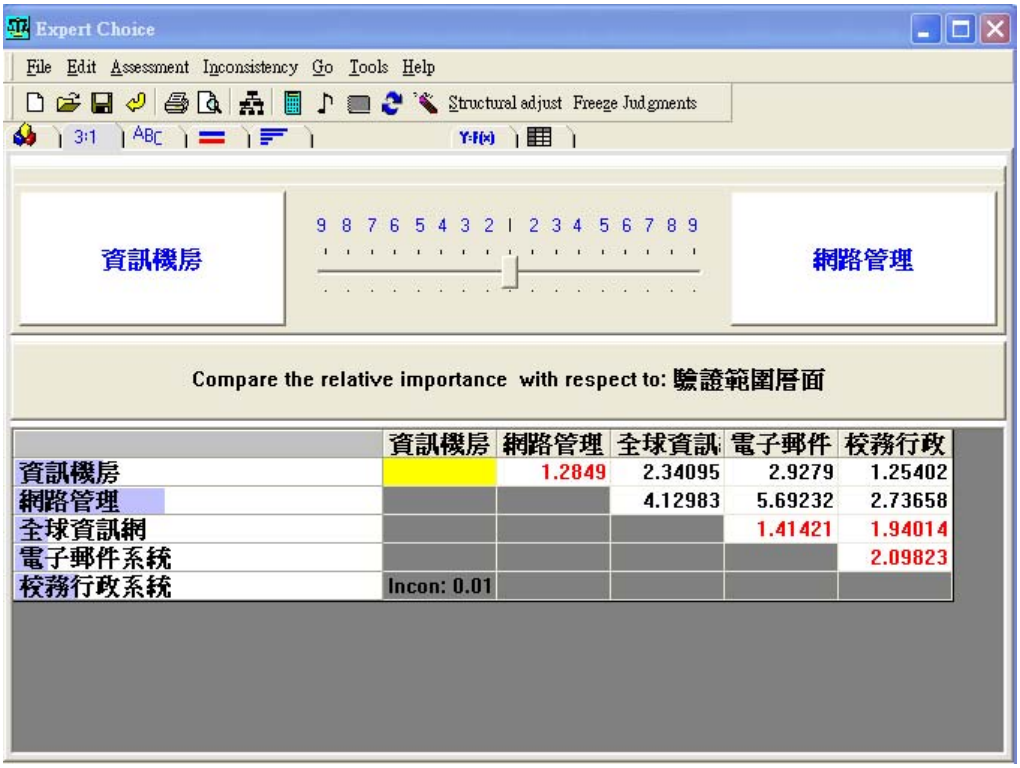


圖 4-3　Expert Choice 第二層級構面計算結果

資料來源：本研究整理

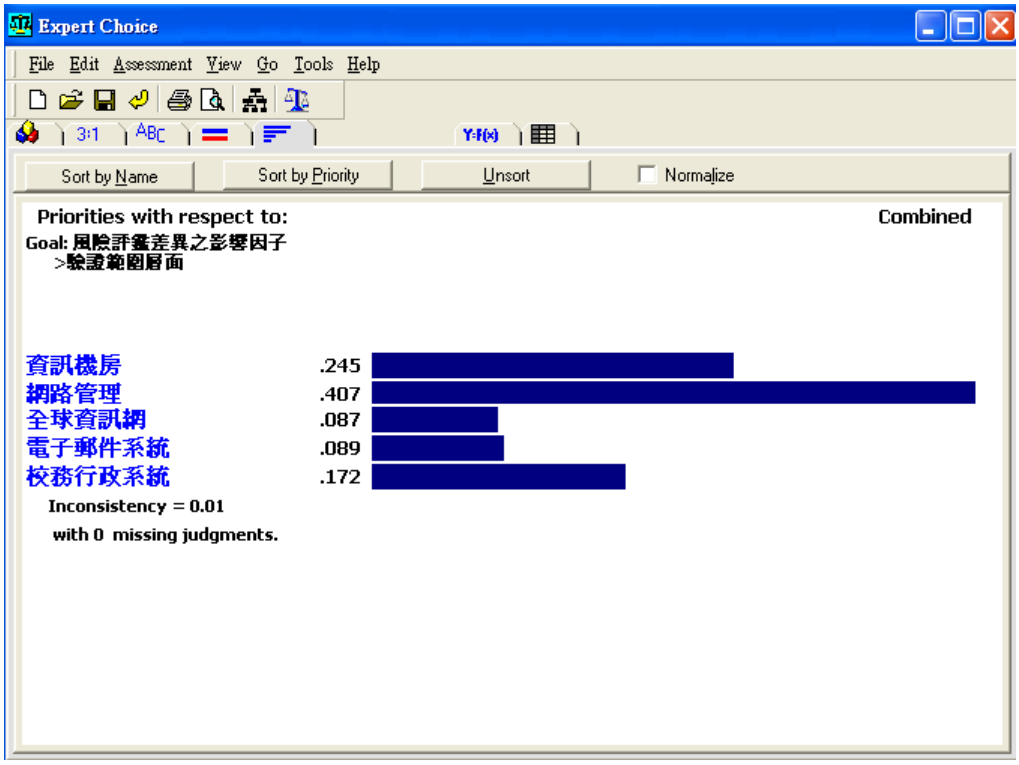


圖 4-4　Expert Choice 第二層級區域優先權重計算結果

資料來源：本研究整理

4.4 信度說明

信度即可靠性(Trustworthiness)，在層級分析法中係指一份問卷所測分數的一致性(Consistency)。在採用問卷調查方式的分析中，為了達到確認調查結果的準確能夠可靠地呈現受驗者的狀況，所獲得的資料必須具有一致性，才能算是一份品質良好且具有足夠信度的問卷。本研究的信度分析係依據Satty(1980)在分析層級架構法中定義的計算各層級一致性比率(Consistency Ratio，簡稱C.R.)作為衡量問卷的可信程度。當其值小於或等於 0.1 時，表示該問卷具有高度一致性，然而大於 0.1 時，表示問卷的一致性較差，建議不採用。

本研究共發放 13 份專家問卷，P大學 8 份，T大學 5 份。問卷受訪者在填寫問卷比較矩陣時，可能會有潛在不一致性的評估誤差存在，影響評估結果之準確性，Expert Choice軟體可逐一檢定單一問卷及累計所有問卷之值，其用不一致比率(Inconsistency Ratio，簡稱I.R.) 來表示一致性比率，所以在此I.R.即為C.R.。當I.R.≤0.1 者始符合標準，而I.R.>0.1 者，則列為無效問卷而予以刪除。透過軟體運算檢定出P大學有 2 份問卷不一致性比率(I.R.)大於 0.1。其中，有效數為 11 份，無效數為 2 份，有效回收率為 85%。其問卷回收統計如表 4-6 所示。

表 4-6　AHP 問卷回收情形

問卷區分	P 大學	T 大學	合計
回收數	8	5	13
無效數(I.R.>0.1)	2	0	2
有效數(I.R.≤0.1)	6	5	11

資料來源：本研究整理

4.5 個案風險評估差異原因探討

本研究兩個案之受訪者根據第三章之風險評估方式，經過資訊資產鑑價、威脅與脆弱性評估、風險值計算等步驟，將風險定性化轉換為數值，以辨識組織之資產風險優先順序。首先請兩個個案參與風險評估之相關人員，針對各層級評估準則進行問卷填寫，並計算一致性檢驗，再根據問卷結果加以分析差異原因。透過AHP工具軟體Expert Choice輸入每位受訪者對於風險評估影響因子的權重關係。使用Expert Choice計算權重分布，取得各別受訪者之評估影響因子(準則)權重，後進一步剖析原先風險評估結果之差異原因。圖 4-5 為Expert Choice計算受訪者T1 之層級權重示意圖。

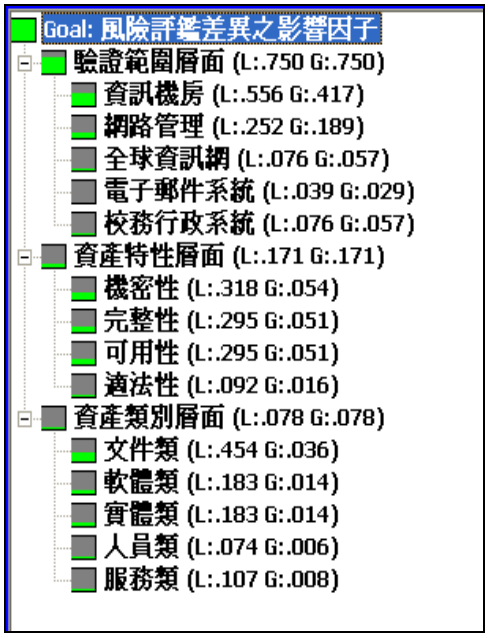


圖 4-5　受訪者 T1 之各層級權重示意圖

資料來源：本研究整理

4.5.1 P 大學風險評估原因分析

P大學之前十名高風險之詳細資產資料如表 4-7 所示。透過Expert Choice軟體可計算出P大學每位受訪者之層級權重與排序之彙整表如表 4-8 所示。

表 4-7　P 大學前十名高風險資產列表

驗證範圍	資產名稱	資產類別	資產價值				風險值					排序	受訪者
			C	I	A	L	C	I	A	L	總風險值		
校務行政	Solaris	軟體類	3	7	7	3	108	315	350	111	884	1	P3
校務行政	校務系統資料庫資料	文件類	7	5	7	3	525	30	84	225	864	2	P3
校務行政	軟研組委外維護人員	人員類	7	0	1	3	511	0	28	219	758	3	P3
校務行政	EIP 應用軟體	軟體類	3	5	3	3	150	250	171	156	727	4	P3
全球資訊	apache	軟體類	1	7	5	3	45	287	220	141	693	5	P5
校務行政	印表計費系統	軟體類	3	5	7	5	54	190	301	100	645	6	P3
電子郵件	Linux 系統	軟體類	1	7	7	3	30	231	280	93	634	7	P2
全球資訊	Solaris	軟體類	1	7	7	3	30	217	266	93	606	8	P5
校務行政	Sybase ASE	軟體類	1	7	7	3	30	217	266	93	606	9	P3
校務行政	Bind9	軟體類	3	7	7	3	78	196	217	84	575	10	P3

表 4-8 P 大學各受訪者層級權重表

評估因子	P1		P2		P3		P4		P5		P6	
	區域權重	區域排序	區域權重	區域排序	區域權重	區域排序	區域權重	區域排序	區域權重	區域排序	區域權重	區域排序
資訊機房	0.324	3	0.556	1	0.142	3	0.158	3	0.048	5	0.341	2
網路管理	0.486	1	0.241	2	0.552	1	0.366	1	0.126	3	0.432	1
全球資訊網	0.077	4	0.033	5	0.040	5	0.068	4	0.450	1	0.042	5
電子郵件系統	0.077	4	0.045	4	0.073	4	0.068	4	0.079	4	0.096	3
校務行政系統	0.036	2	0.122	3	0.194	2	0.339	2	0.297	2	0.088	4
機密性	0.116	3	0.192	3	0.294	2	0.168	3	0.467	1	0.444	1
完整性	0.348	2	0.295	2	0.462	1	0.384	1	0.277	2	0.341	2
可用性	0.441	1	0.397	1	0.156	3	0.384	1	0.160	3	0.137	3
適法性	0.095	4	0.116	4	0.088	4	0.064	4	0.095	4	0.078	4
文件類	0.040	5	0.437	1	0.107	5	0.049	5	0.054	5	0.040	5
軟體類	0.486	1	0.260	2	0.373	1	0.065	4	0.207	2	0.118	3
實體類	0.302	2	0.141	3	0.140	3	0.179	3	0.080	4	0.506	1
人員類	0.112	3	0.088	4	0.139	4	0.430	1	0.135	3	0.076	4
服務類	0.060	4	0.074	5	0.241	2	0.277	2	0.524	1	0.260	2
I.R.	0.03		0.09		0.1		0.02		0.02		0.1	

P大學之風險評估結果原因說明，茲分述如下：

1. P大學高風險資產多屬校務行政系統驗證範圍，其中以軟體類最多。
2. 由受訪者背景得知，校務行政系統流程主要資訊資產風險評估人員為P3 受訪者。該受訪者對【驗證範圍層面】優先排序為網路管理＞校務行政系統＞資訊機房＞電子郵件系統＞全球資訊網；對於【資產特性層面】優先排序為完整性＞機密性＞可用性＞適法性；對於【資產類別層面】優先排序為軟體類＞服務類＞實體類＞人員類＞文件類。
3. 高風險資產在校務行政系統之軟體類，計有Solaris(排名 1，軟體類)、EIP應用軟體(排名 4，軟體類)、印表計費系統(排序 6，軟體類)、Sybase ASE(排名 9，軟體類)、Bind9(排名 10，軟體類)。推論P3 受訪者因個人業務負責校務行政系統，故對於相關資產之完整性與機密性損害程度給予較高分數。且據個人主觀經驗判斷P大學之軟體類有教育訓練不足與缺乏有效變更控管等弱點，如碰到人員離職、使用者失誤等威脅衝擊性大，因此該資產風險分數較高。
4. 高風險資產中校務行政系統驗證範圍之文件類，為校務行政系統資料庫資料(排名 2，文件類)，其風險評估人員亦為P3 受訪者，推論高風險原因除個人職務導致給予較高分數外，且據其個人主觀經驗判斷P大學之文件類有缺乏監督機制之弱點碰到資料外洩威脅，對組織衝擊性較高。
5. 高風險資產中校務行政系統驗證範圍之人員類，為軟研組委外維護人員(排名 3，人員類)，其風險評估人員亦為P3 受訪者，據其個人主觀經驗判斷P大學之人員類(外部人員)有缺乏人員安全審核程序之弱點碰到資料外洩之威脅，對組織衝擊性較高。

4.5.2 T 大學風險評估原因分析

T大學之前十名高風險之詳細資產資料如表 4-9 所示。將T大學每位受訪者問卷輸入Expert Choice軟體可計算出每位受訪者之層級權重與排序之結果，T大學每位受訪者之層級權重與排序彙整如表 4-10 所示。

表 4-9 T 大學前十名高風險資產列表

驗證範圍	資產名稱	資產類別	資產價值				風險值					排序	受訪者
			C	I	A	L	C	I	A	L	總風險值		
網路管理	Cisco Catalyst 6506	實體類	5	5	7	1	345	418	832	30	1625	1	T1
網路管理	Cisco Catalyst 6509	實體類	5	5	7	1	345	313	832	30	1520	2	T1
校務行政	個人帳號管理中心(USSC)	軟體類	5	5	5	1	280	540	532	60	1412	3	T4
校務行政	識別資料交換管理應用系統	軟體類	5	7	3	1	225	679	444	47	1395	4	T4
校務行政	LDAP 軟體	軟體類	5	7	5	1	215	511	560	47	1333	5	T4
校務行政	資料庫管理系統	軟體類	5	7	5	1	125	357	410	27	919	6	T4
電子郵件	Mail 2000 電子郵件系統	軟體類	3	5	3	1	285	275	186	105	851	7	T1
網路管理	HP SureSstore Tape Library	實體類	1	1	5	1	6	3	670	8	687	8	T1
網路管理	Maxxan SA100f	實體類	1	1	5	1	6	3	670	8	687	9	T1
校務行政	Solaris 作業系統	軟體類	5	5	5	1	175	195	265	37	672	10	T4

表 4-10 T 大學各受訪者層級權重表

評估因子	T1		T2		T3		T4		T5	
	區域權重	區域排序	區域權重	區域排序	區域權重	區域排序	區域權重	區域排序	區域權重	區域排序
資訊機房	0.556	1	0.503	1	0.514	1	0.435	1	0.468	1
網路管理	0.252	2	0.277	2	0.136	3	0.167	3	0.250	2
全球資訊網	0.076	3	0.031	5	0.033	5	0.028	5	0.044	5
電子郵件系統	0.039	4	0.067	4	0.055	4	0.067	4	0.134	3
校務行政系統	0.076	3	0.121	3	0.261	2	0.303	2	0.104	4
機密性	0.318	1	0.113	3	0.544	1	0.136	3	0.554	1
完整性	0.295	2	0.536	1	0.108	3	0.509	1	0.072	4

可用性	0.295	2	0.289	2	0.293	2	0.309	2	0.242	2
適法性	0.092	3	0.062	4	0.055	4	0.045	4	0.132	3
文件類	0.454	1	0.332	2	0.040	5	0.039	5	0.043	5
軟體類	0.183	2	0.445	1	0.118	3	0.478	1	0.082	4
實體類	0.183	2	0.031	5	0.506	1	0.300	2	0.504	1
人員類	0.074	5	0.067	4	0.076	4	0.128	3	0.278	2
服務類	0.107	4	0.119	3	0.260	2	0.055	4	0.093	3
I.R.	0.09		0.09		0.08		0.09		0.08	

透過表4-5受訪者背景資料與表4-11個案曾有之威脅弱點與資安事件列表分析，T大學之風險評估結果原因說明，茲分述如下：

1. T大學之高風險資產多屬於網路管理驗證範圍之實體類與校務行政系統驗證範圍之軟體類。
2. 由表4-3受訪者背景資料得知，網路管理流程主要資訊資產風險評估人員為T1受訪者。該受訪者對於【驗證範圍層面】優先排序為資訊機房＞網路管理＞校務行政系統≧全球資訊網＞電子郵件系統；對於【資產特性層面】優先排序為機密性＞完整性≧可用性＞適法性；對於【資產類別層面】優先排序為文件類＞軟體類≧實體類＞服務類＞人員類。
3. 高風險資產在網路管理驗證範圍之實體類，計有Cisco Catalyst 6506 (排名1)、Cisco Catalyst 6509 (排名2)、HP SureSstore Tape Library (排名8)、Maxxan SA100f(排名9)。推論T1受訪者因個人業務負責網路管理與備份系統，故對於相關資產之機密性、完整性與可用性損害程度給予較高分數。且據T1受訪者個人主觀經驗判斷，T大學之實體類有缺乏有效變更控制與缺乏監督機制等弱點，如碰到未經授權使用網路設備與硬體失效等威脅之衝擊性大，因此該資產風險分數較高。
4. 校務行政系統流程主要資訊資產風險評估人員為T4受訪者。該受訪者對於【驗證範圍層面】優先排序為資訊機房＞校務行政系統＞網路管理＞電子郵件系統＞全球資訊網；對於【資產特性層面】優先排序

為完整性＞可用性＞機密性＞適法性；對於【資產類別層面】優先排序為軟體類＞實體類＞人員類＞服務類＞文件類。

5. 高風險資產在校務行政系統驗證範圍之軟體類，計有個人帳號管理中心USSC(排名 3)、識別資料交換管理應用系統(排名 4)、LDAP Server(排名 5)、資料庫管理系統(排名 6) 。推論T4 受訪者因個人業務負責校務行政系統，故對於相關資產之機密性、完整性與可用性損害程度給予較高分數。且據個人主觀經驗判斷，T大學之軟體類有人員角色定義不明與教育訓練不足等弱點，如碰到人員離職與軟體失效等威脅之衝擊性大，因此該資產風險分數較高。

表 4-11 個案曾有之威脅、弱點與資安事件列表

	P大學						T大學				
	P1	P2	P3	P4	P5	P6	T1	T2	T3	T4	T5
弱點											
系統漏洞	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
教育訓練不足	✓			✓	✓	✓		✓	✓		✓
人員缺乏						✓	✓	✓	✓	✓	✓
實體環境不良			✓			✓					✓
軟體之安全機制不足		✓	✓		✓	✓	✓	✓	✓		✓
角色定義不明					✓	✓	✓		✓	✓	✓
威脅											
天然因素災害	✓		✓	✓	✓	✓			✓		
天然因素故障		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
人為過失	✓		✓	✓	✓	✓	✓	✓		✓	✓
人為故意											
資安事件											
病毒感染	✓		✓	✓	✓	✓	✓	✓	✓		✓
入侵及跳板	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
阻絕服務	✓	✓	✓	✓	✓	✓	✓	✓	✓		
垃圾郵件			✓	✓	✓	✓	✓	✓	✓		✓

資料或實體竊取											
資料竄改											
操作不當	✓		✓	✓	✓	✓		✓		✓	✓
系統失效	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
溫濕度因素或電源供應不良	✓		✓		✓	✓	✓				
火、水災或地震等天然災害											

資料來源：本研究整理

4.6 個案群體權重分析

透過 4.5 節探討各受訪者層級分析權重，研究得知，兩個個案之風險評估結果差異，主要受個人主觀與個案過往經驗影響。本節將繼續使用 Expert Choice 軟體進一步計算兩個個案群體之**客觀風險評估層級權重**，並對結果進行說明。

4.6.1 層級評估構面之區域權重分析

研究結果顯示 P 大學與 T 大學評估構面區域權重順序不相同。P 大學優先排序如圖 4-6 所示，為驗證範圍層面＞資產特性層面＞資產類別層面。T 大學優先排序如圖 4-7 所示，為資產特性層面＞驗證範圍層面＞資產類別層面。兩個個案之評估構面區域權重分析如表 4-12 所示。

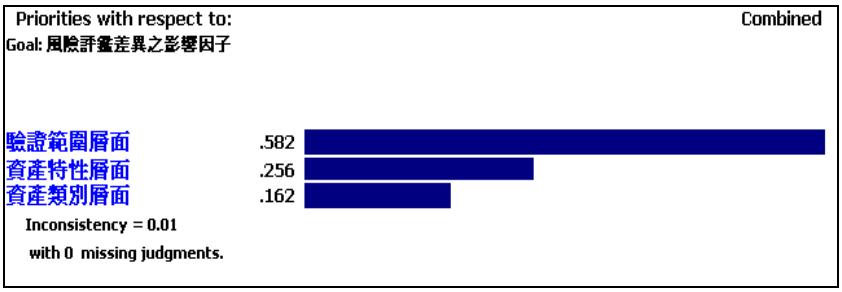


圖 4-6　P 大評估構面區域權重計算結果

資料來源：本研究整理

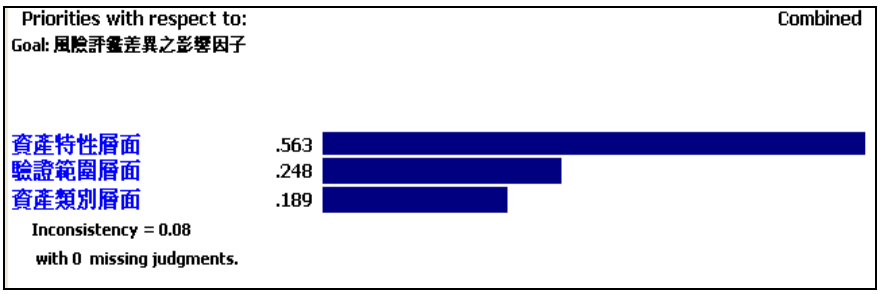


圖 4-7　T 大評估構面區域權重計算結果

資料來源：本研究整理

表 4-12 兩校評估構面之區域權重比較表

評估構面 (第一層)	P 大學		T 大學	
	區域優先權重	排序	區域優先權重	排序
驗證範圍層面	0.582	1	0.248	2
資產特性層面	0.256	2	0.563	1
資產類別層面	0.162	3	0.189	3
I.R.	0.01		0.08	

資料來源：本研究整理

P 大學認為【驗證範圍層面】對風險評估結果具有最大影響程度，推論其原因為 ISO27001:2005 條款 4.2.1 有規範組織須為資訊安全管理系統訂定範圍，P 大學執行 ISO27001 導入前先確認關鍵業務流程，後續再針對關鍵流程盤點相關資訊資產、鑑價與風險評估，因此 P 大學認為驗證範圍層面影響風險評估結果最大。而 T 大學認為【資產特性層面】對風險評估結果具有最大影響程度，推論其原因為 T 大學認為資產的完整性所面臨的威脅與脆弱點較常發生於該組織中，故資產特性層面對風險結果具最大影響。

4.6.2 層級各評估準則之區域權重分析

4.6.2.1 驗證範圍層面之區域權重分析

調查發現 P 大學與 T 大學區域權重順序稍有差異。P 大學之重要性依序為網路管理＞資訊機房＞校務行政系統＞全球資訊網＞電子郵件系統，如圖 4-8 所示。而 T 大學之重要性依序為資訊機房＞網路管理＞校務行政系統＞全球資訊網＞電子郵件系統，如圖 4-9 所示。評估【驗證範圍層面】構面各準則分析結果如表 4-13 所示。

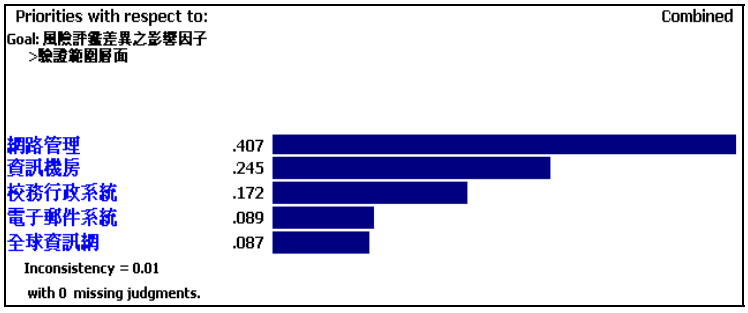


圖 4-8 P 大驗證範圍層面區域權重計算結果

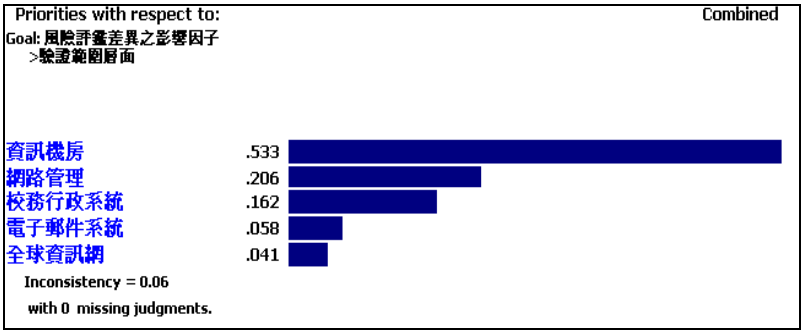


圖 4-9　T 大驗證範圍層面區域權重計算結果

資料來源：本研究整理

表 4-13　兩校驗證範圍層面各準則之區域權重比較表

評估準則	P 大學		T 大學	
	區域權重	排序	區域權重	排序
資訊機房	0.245	2	0.533	1
網路管理	0.407	1	0.206	2
全球資訊網	0.087	5	0.041	5
電子郵件系統	0.089	4	0.058	4
校務行政系統	0.172	3	0.162	3
I.R.	0.01		0.06	

資料來源：本研究整理

資訊機房與網路管理為組織資訊之核心營運關鍵，如遭受風險常會導致其他營運中斷或受損。由表 4-13 可知，P大學群體意見認為網路管理為最重要風險，T大學則將資訊機房視為最重要風險。推論其原因為P大學在風險評估前已完成資訊機房環境重整，因此認為已將資訊機房可能發生之風險機率降低。而T大學在風險評估時，資訊機房線路與電路配置尚未整理，實體環境較為凌亂，易產生電路誤用等風險，因此認為可能風險較大。

4.6.2.2 資產特性構面之區域權重分析

兩個個案之評估風險影響程度區域權重順序皆是完整性＞可用性＞機密性＞適法性，如圖 4-10 及圖 4-11 所示。表 4-14 顯示P大學與T大學之區域優先權重順序在【資訊特性層面】構面中一致。

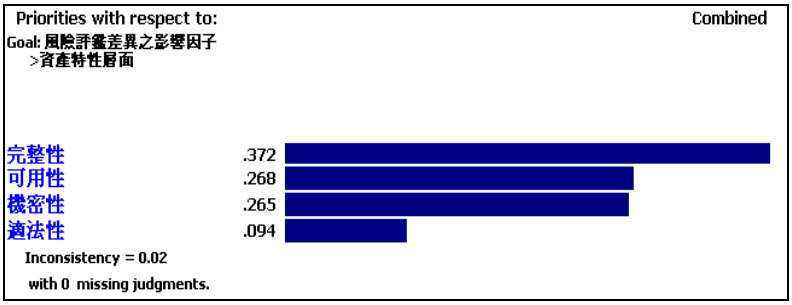


圖 4-10　P 大資訊特性層面區域權重計算結果

資料來源：本研究整理

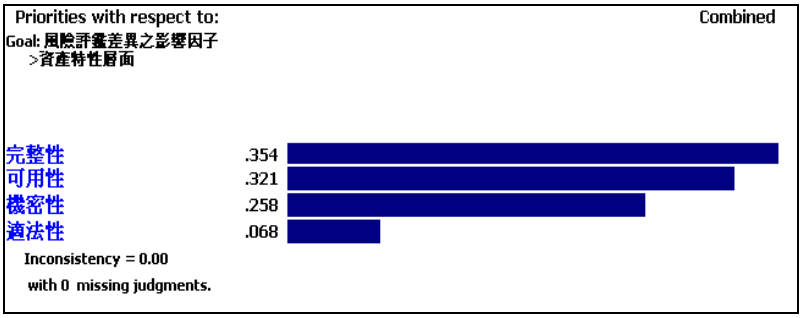


圖 4-11　T 大資訊特性層面區域權重計算結果

資料來源：本研究整理

表 4-14　兩校資產特色層面各準則之區域權重比較表

評估準則	P 大學		T 大學	
	區域權重	排序	區域權重	排序
機密性	0.265	3	0.258	3
完整性	0.372	1	0.354	1
可用性	0.268	2	0.321	2
適法性	0.094	4	0.068	4
I.R.	0.02		0	

資料來源：本研究整理

在資料特性層面，對P大學與T大學而言，資訊資產之完整性是最重要，其次為可用性。除表示兩個案之群體意見認為資訊資產之準確與完整最為重要外。推論個案組織重視資訊資產與營運能即時被使用，且中斷時間忍受度較低。

4.6.2.3 資產類別構面之區域權重分析

P大學之重要性如圖 4-12 所示，依序為實體類＞服務類＞軟體類＞人員類＞文件類；T大學之重要性如圖 4-13 所示，依序為軟體類＞實體類＞文件類＞服務類＞人員類。評估【資訊類別層面】構面各準則分析結果如表 4-15 所示。

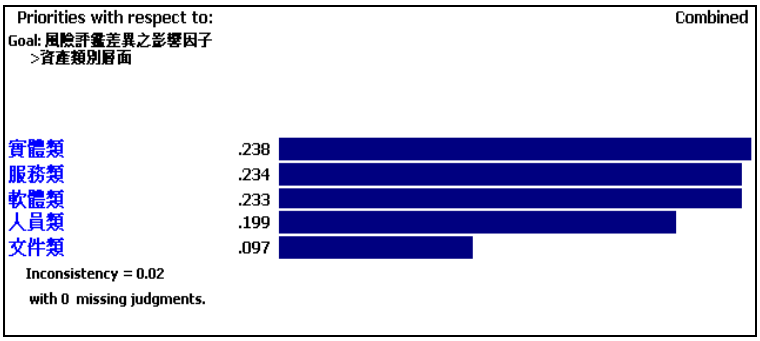


圖 4-12　P 大資訊類別層面區域權重計算結果

資料來源：本研究整理

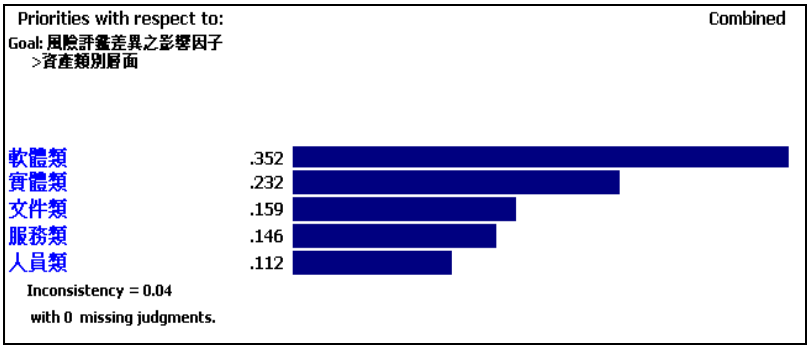


圖 4-13　T 大資訊類別層面區域權重計算結果

資料來源：本研究整理

表 4-15 資產類別層面各準則之區域權重比較表

評估準則	P 大學		T 大學	
	區域權重	排序	區域權重	排序
文件類	0.097	5	0.159	3
軟體類	0.233	3	0.352	1
實體類	0.238	1	0.232	2
人員類	0.199	4	0.112	5
服務類	0.234	2	0.146	4
I.R.	0.02		0.04	

資料來源：本研究整理

在資料類別層面，對於P大學而言，實體類重要度高於其他資訊資產類別。推論其原因為P大學較多實體類資訊資產年代較久，硬體損壞情況較多，因此認為遇到之風險可能機率較高。而對T大學而言，軟體類重要度高於其他資訊資產類別。推論其原因為T大學多數軟體類之安全訓練不足與缺乏有效變更管控，因此認為遇到之風險可能機率較高。

4.7 研究發現

透過本研究建構之層級分析方式與問卷探討比較兩個案之研究發現，並分析其原因，而此分項次方式說明如後：

4. 本研究中兩個個案使用之風險評估法為，可將個人之認知之權重化為風險數值，進行風險優先排序。

5. 由兩個個案之風險評估彙整表(附錄二與附錄三)中可以發現，相同產業與背景之組織，資訊資產項目大部分相似。

6. 因個人主觀經驗與判斷不同，每位風險評估人員所重視之評估項目亦

不盡相同。兩個案雖組織背景相似且使用相同標準的風險評估方式，但因組織內部人員面臨風險與過往經驗之不同，評估出來的風險分布亦有明顯差異。

第5章　結論與建議

5.1 結論

ISO27001 強調資訊安全管理的核心其實就是風險評估。ISO 27001 對於風險評估的步驟與流程是用ISO 27005 的方法。本研究所使用之資訊資產評鑑皆考量到其適法性問題，目的在因應個人資料保護法議題。

本研究主要是利用層級分析法評估影響資訊安全風險差異因子的權重，並且利用中部兩個學術單位作為實際案例探討的對象。根據本研究的論述，可以看出層級分析法的系統性、有效性，因為它可以將複雜的問題利用層級的方式，進行有系統的分析，並可利用層級的架構將問題簡化，增加問題評估的有效性，並且經由層級分析法的評估，得到具體的數值，而呈現結果，而讓分析者據以從事其分析工作。

本研究除利用層級分析法剖析個人主觀之評估因子權重外，更進一步提出整合之群體風險評估權重方式。未來建議可透過與個案主管、顧問專家訪談，利用腦力激盪方式列出最客觀之評估要素及評估準則，進行相關風險評估時可使用群組決策將主觀轉為客觀，確實分析所有重要資產之CIAL弱點與威脅等，為組織評估出最迫切需處理的風險因素，以達營運持續之目的。

5.2 未來研究建議

本研究提出幾點建議，希望可供後續研究之用：

1. 組織進行風險評估前，依各自組織特性，利用層級分析法先評估群體意見了解組織之風險評估因素之全域權重，並透過風險溝通會議，讓組織成員在執行風險評估時，更能得到一致的結果，俾明確地顯示最符合組織內部所面臨且急待處理之風險。
2. 立法院已於 2010 年 4 月 27 日通過個人資料保護法案，對於文件類與個人資料相關之蒐集、利用及保管等明定相關責任。建議後續進行風險評估時，應以更嚴格的標準評估適法性與文件類之相關威脅與弱點等風險問題，俾降低個資外洩對組織的損害程度。
3. AHP方法已被廣泛的應用，但對於專家學者的人數及其人選是一個主要的限制，人數過多或人選認定標準有所偏差，將影響分析結果的一致性。因此有關專家學者及評估人員決定的問題，將是未來研究的方向之一。

5.3 研究限制

1. 本研究僅限於學術單位之風險評估因子權重分析，其他產業因特性差異，其相關因子權重也會有所不同。
2. 本研究採用實地訪查方式，研究者至個案之資訊部門訪談相關人員，並請其立即填寫問卷，可能會因受訪對象工作忙碌匆促填寫而產生無效問卷。

第6章　參考文獻

1. 中華民國國家標準，資訊技術－安全技術－資訊安全管理系統－要求事項（CNS 27001），經濟部標準檢驗局，2006 年。
2. 中華民國國家標準，資訊技術－安全技術－資訊安全管理之作業規範（CNS 27002），經濟部標準檢驗局，2007 年。
3. 中華民國國家標準，資訊技術－安全技術－資訊安全風險管理（CNS 27005），經濟部標準檢驗局，2010 年。
4. 樊國楨、黃健誠、王演芳、楊中皇。重要民生基礎建設資訊安全管理標準化初探－以台灣地區為例。第十四屆海峽兩岸資訊管理發展策略研討會，2008 年。
5. 傅雅萍、樊國楨、楊中皇，ISO/IEC 27005 風險管理標準整合 CORAS 之可行性研究：以電力公司為例，2008 年。
6. 劉興華，資訊安全風險管理(ISO/IEC FDIS 27005)議題初探，堅實我國資訊安全管理系統稽核作業相關標準系列討論會之 25，2008 年。
7. 陳冠彰，論資訊安全風險分析之謬誤，淡江大學資訊管理系研究所碩士論文，2005 年。
8. 鄧振源、曾國雄（1989），層級分析法（AHP）的內涵特性與運用（上），中國統計學報，第 27 卷第 6 期，頁 5~22。
9. 鄧振源、曾國雄（1989），層級分析法（AHP）的內涵特性與運用（下），中國統計學報，第 27 卷第 7 期，頁 1~19。
10. 王志斌，結合層級分析法與德菲法發展資訊安全認知評量法之研究，世新大學資訊管理學系碩士論文，2010 年。
11. Saaty Thomas L.,（1980）,The Analytic Hierarchy Process, New York: McGraw-Hill.
12. 顏鳳伶，靜宜大學導入 ISO 270012005--資安管理系統經驗分享，2006 年。
13. 洪國興、趙榮耀，資訊安全管理理論之探討，產業論壇，頁 17~47，2005 年。

附錄一：資產弱點威脅衝擊對應表

資產類別	弱點	威脅	威脅衝擊			
			C	I	A	L
文件類(電子文件)	安全訓練不足	使用者錯誤	●	●	●	●
文件類(電子文件)	儲存媒體維護不夠/安裝失敗	儲存媒體的劣化		●	●	
文件類(電子文件)		維護錯誤			●	
文件類(電子文件)	缺乏複製備份	地震/颱風			●	
文件類(電子文件)		火災		●	●	
文件類(電子文件)		惡意的軟體		●	●	
文件類(電子文件)	缺乏小心地處置	失竊	●	●	●	●
文件類(電子文件)	缺乏有效變更控制	軟體失效		●	●	
文件類(電子文件)		在未經授權的方式下使用網路設備	●		●	●
文件類(電子文件)		在未經授權的方式下使用軟體	●	●	●	●
文件類(電子文件)	識別與認證機制的不足(如使用者認證)	偽裝成使用者身份	●	●	●	●
文件類(電子文件)		在未經授權的方式下使用網路設備	●		●	●
文件類(電子文件)		在未經授權的方式下使用軟體	●	●	●	●
文件類(電子文件)	缺乏監督機制	空調失效			●	
文件類(電子文件)		通訊滲透	●			●
文件類(電子文件)		通訊服務的失效(例如：網路服務)			●	
文件類(電子文件)		硬體失效			●	
文件類(電子文件)		非法使用軟體	●	●	●	●
文件類(電子文件)		惡意的軟體		●	●	
文件類(電子文件)		軟體失效		●	●	
文件類(電子文件)		在未經授權的方式下使用網路設備	●		●	●
文件類(電子文件)		在未經授權的方式下使用軟體	●	●	●	●
文件類(電子文件)	缺乏安全意識	使用者錯誤	●	●	●	●
文件類(電子文件)	缺少密碼管理	非法使用軟體	●	●	●	●
文件類(電子文件)		偽裝成使用者身份	●	●	●	●
文件類(電子文件)	未控制複製	失竊	●	●	●	●

資產類別	弱點	威脅	威脅衝擊			
			C	I	A	L
文件類(電子文件)	未保護密碼表	偽裝成使用者身份	●	●	●	●
文件類(紙本文件)	建築物、房間的實體進出控制不足或粗心使用	資源的錯誤使用	●	●	●	●
文件類(紙本文件)		失竊	●	●	●	●
文件類(紙本文件)		未經授權的使用媒體	●	●	●	●
文件類(紙本文件)	安全訓練不足	使用者錯誤	●	●	●	●
文件類(紙本文件)	缺乏小心地處置	失竊	●	●	●	●
文件類(紙本文件)	缺乏有效變更控制	軟體失效		●	●	
文件類(紙本文件)		在未經授權的方式下使用網路設備	●		●	●
文件類(紙本文件)		在未經授權的方式下使用軟體	●	●	●	●
文件類(紙本文件)	缺乏安全意識	使用者錯誤	●	●	●	●
文件類(紙本文件)	未控制複製	失竊	●	●	●	●
文件類(紙本文件)	未保護密碼表	偽裝成使用者身份	●	●	●	●
文件類(紙本文件)	缺乏對外部或清潔人員的監視工作	失竊	●	●	●	●
軟體類(商用軟體)	不正確的使用軟體和硬體	非法使用軟體	●	●	●	●
軟體類(商用軟體)		在未經授權的方式下使用網路設備	●		●	●
軟體類(商用軟體)		在未經授權的方式下使用軟體	●	●	●	●
軟體類(商用軟體)		使用者錯誤	●	●	●	●
軟體類(商用軟體)	安全訓練不足	使用者錯誤	●	●	●	●
軟體類(商用軟體)	儲存媒體維護不夠/安裝失敗	儲存媒體的劣化		●	●	
軟體類(商用軟體)		維護錯誤			●	
軟體類(商用軟體)	缺乏複製備份	地震/颱風			●	
軟體類(商用軟體)		火災		●	●	
軟體類(商用軟體)		惡意的軟體		●	●	
軟體類(商用軟體)	缺乏有效變更控制	軟體失效		●	●	
軟體類(商用軟體)		在未經授權的方式下使用網路設備	●		●	●
軟體類(商用軟體)		在未經授權的方式下使用軟體	●	●	●	●
軟體類(商用軟體)	識別與認證機制	偽裝成使用者身份	●	●	●	●

資產類別	弱點	威脅	威脅衝擊			
			C	I	A	L
軟體類(商用軟體)	的不足(如使用者認證)	在未經授權的方式下使用網路設備	●		●	●
軟體類(商用軟體)		在未經授權的方式下使用軟體	●	●	●	●
軟體類(商用軟體)	缺乏監督機制	空調失效			●	
軟體類(商用軟體)		通訊滲透	●			●
軟體類(商用軟體)		通訊服務的失效(例如：網路服務)			●	
軟體類(商用軟體)		硬體失效			●	
軟體類(商用軟體)		非法使用軟體	●	●	●	●
軟體類(商用軟體)		惡意的軟體		●	●	
軟體類(商用軟體)		軟體失效		●	●	
軟體類(商用軟體)		在未經授權的方式下使用網路設備	●		●	●
軟體類(商用軟體)		在未經授權的方式下使用軟體	●	●	●	●
軟體類(商用軟體)	缺乏安全意識	使用者錯誤	●	●	●	●
軟體類(商用軟體)	離開工作站時沒有”登出”	在未經授權的方式下使用網路設備	●		●	●
軟體類(商用軟體)		在未經授權的方式下使用軟體	●	●	●	●
軟體類(商用軟體)	沒有軟體測試或軟體測試不夠	軟體失效		●	●	
軟體類(商用軟體)		在未經授權的方式下使用軟體	●	●	●	●
軟體類(商用軟體)	缺少密碼管理	非法使用軟體	●	●	●	●
軟體類(商用軟體)		偽裝成使用者身份	●	●	●	●
軟體類(商用軟體)	未控制軟體的使用和下載	非法使用軟體	●	●	●	●
軟體類(商用軟體)		惡意的軟體	●	●	●	
軟體類(商用軟體)	軟體知名的瑕疵	惡意的軟體		●	●	
軟體類(商用軟體)		軟體失效		●	●	
軟體類(商用軟體)	存取權限指派錯誤	資源的錯誤使用	●	●	●	●
軟體類(商用軟體)		未經授權的使用媒體	●	●	●	●
軟體類(商用軟體)		在未經授權的方式下使用網路設備	●		●	●
軟體類(商用軟體)		在未經授權的方式下使用軟體	●	●	●	●

資產類別	弱點	威脅	威脅衝擊			
			C	I	A	L
軟體類(自行發展軟體)	不正確的使用軟體和硬體	非法使用軟體	●	●	●	●
軟體類(自行發展軟體)		在未經授權的方式下使用網路設備	●		●	●
軟體類(自行發展軟體)		在未經授權的方式下使用軟體	●	●	●	●
軟體類(自行發展軟體)		使用者錯誤	●	●	●	●
軟體類(自行發展軟體)	安全訓練不足	使用者錯誤	●	●	●	●
軟體類(自行發展軟體)	儲存媒體維護不夠/安裝失敗	儲存媒體的劣化		●	●	
軟體類(自行發展軟體)		維護錯誤			●	
軟體類(自行發展軟體)	缺乏複製備份	地震/颱風			●	
軟體類(自行發展軟體)		火災		●	●	
軟體類(自行發展軟體)		惡意的軟體		●	●	
軟體類(自行發展軟體)	缺乏有效變更控制	軟體失效		●	●	
軟體類(自行發展軟體)		在未經授權的方式下使用網路設備	●		●	●
軟體類(自行發展軟體)		在未經授權的方式下使用軟體	●	●	●	●
軟體類(自行發展軟體)	識別與認證機制的不足(如使用者認證)	偽裝成使用者身份	●	●	●	●
軟體類(自行發展軟體)		在未經授權的方式下使用網路設備	●		●	●
軟體類(自行發展軟體)		在未經授權的方式下使用軟體	●	●	●	●
軟體類(自行發展軟體)	缺乏監督機制	空調失效			●	

資產類別	弱點	威脅	威脅衝擊			
			C	I	A	L
軟體類(自行發展軟體)		通訊滲透	●			●
軟體類(自行發展軟體)		通訊服務的失效(例如：網路服務)			●	
軟體類(自行發展軟體)		硬體失效			●	
軟體類(自行發展軟體)		非法使用軟體	●	●	●	●
軟體類(自行發展軟體)		惡意的軟體		●	●	
軟體類(自行發展軟體)		軟體失效		●	●	
軟體類(自行發展軟體)		在未經授權的方式下使用網路設備	●		●	●
軟體類(自行發展軟體)		在未經授權的方式下使用軟體	●	●	●	●
軟體類(自行發展軟體)	缺乏安全意識	使用者錯誤	●	●	●	●
軟體類(自行發展軟體)	離開工作站時沒有”登出”	在未經授權的方式下使用網路設備	●		●	●
軟體類(自行發展軟體)		在未經授權的方式下使用軟體	●	●	●	●
軟體類(自行發展軟體)	沒有軟體測試或軟體測試不夠	軟體失效		●	●	
軟體類(自行發展軟體)		在未經授權的方式下使用軟體	●	●	●	●
軟體類(自行發展軟體)	缺少密碼管理	非法使用軟體	●	●	●	●
軟體類(自行發展軟體)		偽裝成使用者身份	●	●	●	●
軟體類(自行發展軟體)	開發者的規範不清楚或不完整	軟體失效		●	●	
軟體類(自行發展軟體)	未控制軟體的使用和下載	非法使用軟體	●	●	●	●
軟體類(自行發展軟體)		惡意的軟體	●	●	●	

資產類別	弱點	威脅	威脅衝擊			
			C	I	A	L
軟體類(自行發展軟體)	軟體知名的瑕疵	惡意的軟體		●	●	
軟體類(自行發展軟體)		軟體失效		●	●	
軟體類(自行發展軟體)	存取權限指派錯誤	資源的錯誤使用	●	●	●	●
軟體類(自行發展軟體)		未經授權的使用媒體	●	●	●	●
軟體類(自行發展軟體)		在未經授權的方式下使用網路設備	●		●	●
軟體類(自行發展軟體)		在未經授權的方式下使用軟體	●	●	●	●
硬體類(一般硬體)	沒有適當刪除就處置或重覆使用儲存媒體	資源的錯誤使用	●	●	●	●
硬體類(一般硬體)	極端氣候	地震/颱風			●	
硬體類(一般硬體)		停電水			●	
硬體類(一般硬體)	網路管理不足	通訊滲透	●			●
硬體類(一般硬體)		流量超過負載			●	
硬體類(一般硬體)		在未經授權的方式下使用網路設備	●		●	●
硬體類(一般硬體)	建築物、房間的實體進出控制不足或粗心使用	資源的錯誤使用	●	●	●	●
硬體類(一般硬體)		失竊	●	●	●	●
硬體類(一般硬體)		未經授權的使用媒體	●	●	●	●
硬體類(一般硬體)	維護回應服務不足	通訊服務的失效(例如：網路服務)			●	
硬體類(一般硬體)		硬體失效			●	
硬體類(一般硬體)	不正確的使用軟體和硬體	非法使用軟體	●	●	●	●
硬體類(一般硬體)		在未經授權的方式下使用網路設備	●		●	●
硬體類(一般硬體)		在未經授權的方式下使用軟體	●	●	●	●
硬體類(一般硬體)		使用者錯誤	●	●	●	●
硬體類(一般硬體)	安全訓練不足	使用者錯誤	●	●	●	●
硬體類(一般硬體)	儲存媒體維護不夠/安裝失敗	儲存媒體的劣化		●	●	

資產類別	弱點	威脅	威脅衝擊			
			C	I	A	L
硬體類(一般硬體)		維護錯誤			●	
硬體類(一般硬體)	缺乏複製備份	地震/颱風			●	
硬體類(一般硬體)		火災		●	●	
硬體類(一般硬體)		惡意的軟體		●	●	
硬體類(一般硬體)	缺乏小心地處置	失竊	●	●	●	●
硬體類(一般硬體)	缺乏有效變更控制	軟體失效		●	●	
硬體類(一般硬體)		在未經授權的方式下使用網路設備	●		●	●
硬體類(一般硬體)		在未經授權的方式下使用軟體	●	●	●	●
硬體類(一般硬體)	識別與認證機制的不足(如使用者認證)	偽裝成使用者身份	●	●	●	●
硬體類(一般硬體)		在未經授權的方式下使用網路設備	●		●	●
硬體類(一般硬體)		在未經授權的方式下使用軟體	●	●	●	●
硬體類(一般硬體)	缺乏監督機制	空調失效			●	
硬體類(一般硬體)		通訊滲透	●			●
硬體類(一般硬體)		通訊服務的失效(例如：網路服務)			●	
硬體類(一般硬體)		硬體失效			●	
硬體類(一般硬體)		非法使用軟體	●	●	●	●
硬體類(一般硬體)		惡意的軟體		●	●	
硬體類(一般硬體)		軟體失效		●	●	
硬體類(一般硬體)		在未經授權的方式下使用網路設備	●		●	●
硬體類(一般硬體)		在未經授權的方式下使用軟體	●	●	●	●
硬體類(一般硬體)	缺乏定期置換體系(缺乏週期性替換方案)	儲存媒體的劣化		●	●	
硬體類(一般硬體)	缺乏安全意識	使用者錯誤	●	●	●	●
硬體類(一般硬體)	離開工作站時沒有”登出”	在未經授權的方式下使用網路設備	●		●	●
硬體類(一般硬體)		在未經授權的方式下使用軟體	●	●	●	●
硬體類(一般硬體)	缺少密碼管理	非法使用軟體	●	●	●	●
硬體類(一般硬體)		偽裝成使用者身份	●	●	●	●

資產類別	弱點	威脅	威脅衝擊			
			C	I	A	L
硬體類(一般硬體)	單點失效	通訊服務的失效(例如：網路服務)			●	
硬體類(一般硬體)	未保護通訊線路	通訊滲透	●			●
硬體類(一般硬體)		損害到線路			●	
硬體類(一般硬體)		竊聽	●			●
硬體類(一般硬體)	缺乏對外部或清潔人員的監視工作	失竊	●	●	●	●
硬體類(一般硬體)	存取權限指派錯誤	資源的錯誤使用	●	●	●	●
硬體類(一般硬體)		未經授權的使用媒體	●	●	●	●
硬體類(一般硬體)		在未經授權的方式下使用網路設備	●		●	●
硬體類(一般硬體)		在未經授權的方式下使用軟體	●	●	●	●
人員類(內部人員)	人員缺乏	人員短缺			●	●
人員類(內部人員)	不正確的使用軟體和硬體	非法使用軟體	●	●	●	●
人員類(內部人員)		在未經授權的方式下使用網路設備	●		●	●
人員類(內部人員)		在未經授權的方式下使用軟體	●	●	●	●
人員類(內部人員)		使用者錯誤	●	●	●	●
人員類(內部人員)	安全訓練不足	使用者錯誤	●	●	●	●
人員類(內部人員)	缺乏安全意識	使用者錯誤	●	●	●	●
人員類(外部人員)	人員缺乏	人員短缺			●	●
人員類(外部人員)	不正確的使用軟體和硬體	非法使用軟體			●	
人員類(外部人員)		在未經授權的方式下使用網路設備			●	
人員類(外部人員)		在未經授權的方式下使用軟體	●	●	●	●
人員類(外部人員)		使用者錯誤	●		●	●
人員類(外部人員)	安全訓練不足	使用者錯誤	●	●	●	●
人員類(外部人員)	缺乏安全意識	使用者錯誤	●	●	●	●
服務類(服務相關)	安全訓練不足	使用者錯誤	●	●	●	●
服務類(服務相關)	缺乏安全意識	使用者錯誤	●	●	●	●
服務類(服務相關)	未保護通訊線路	通訊滲透	●			●
服務類(服務相關)		損害到線路			●	

資產類別	弱點	威脅	威脅衝擊			
			C	I	A	L
服務類(服務相關)		竊聽	●			●

資料來源：本研究整理

附錄二： P大學風險評估結果彙整表

資產類別		資產價值				風險值				
大類	小類	機密性	完整性	可用性	適法性	機密性	完整性	可用性	適法性	總風險值
軟體類	商用軟體	3	7	7	3	108	315	350	111	884
文件類	電子文件	7	5	7	3	525	30	84	225	864
人員類	外部人員	7	0	1	3	511	0	28	219	758
軟體類	商用軟體	3	5	3	3	150	250	171	156	727
軟體類	商用軟體	1	7	5	3	45	287	220	141	693
軟體類	內部發展軟體	3	5	7	5	54	190	301	100	645
軟體類	商用軟體	1	7	7	3	30	231	280	93	634
軟體類	商用軟體	1	7	7	3	30	217	266	93	606
軟體類	商用軟體	1	7	7	3	30	217	266	93	606
軟體類	商用軟體	3	7	7	3	78	196	217	84	575
人員類	內部人員	7	0	3	3	266	0	93	114	473
人員類	內部人員	7	0	3	3	266	0	93	114	473
人員類	內部人員	7	0	3	3	266	0	93	114	473
人員類	內部人員	7	0	3	3	266	0	93	114	473
實體類	電訊	1	1	7	7	17	6	329	119	471
實體類	電訊	1	1	7	7	16	4	315	112	447
實體類	電訊	1	1	7	7	17	6	287	119	429
軟體類	內部發展軟體	3	5	7	5	60	90	161	110	421
軟體類	商用軟體	1	5	3	3	25	175	138	81	419
人員類	內部人員	7	0	1	3	266	0	33	114	413
人員類	外部人員	3	0	1	3	195	0	20	195	410
實體類	電訊	1	1	7	3	17	5	322	51	395
軟體類	商用軟體	1	5	5	3	25	125	140	81	371
軟體類	商用軟體	1	5	3	3	19	170	108	63	360
實體類	電訊	1	1	7	3	17	5	280	51	353
軟體類	商用軟體	1	3	3	3	23	123	129	75	350
軟體類	商用軟體	1	5	3	3	21	135	114	69	339
人員類	內部人員	5	0	1	3	190	0	33	114	337
實體類	電訊	1	1	7	1	17	5	280	17	319
軟體類	商用軟體	1	5	1	3	30	155	38	93	316
軟體類	商用軟體	1	3	3	3	21	99	114	69	303
軟體類	商用軟體	1	5	3	3	19	115	102	63	299

軟體類	商用軟體	1	5	5	5	17	85	100	95	297
軟體類	商用軟體	1	3	3	3	21	81	114	69	285
實體類	一般硬體	1	1	5	3	14	7	210	54	285
軟體類	商用軟體	1	5	5	3	17	95	105	57	274
軟體類	商用軟體	1	5	5	3	17	85	100	57	259
軟體類	商用軟體	1	5	5	3	17	85	95	57	254
服務類	外部服務	1	1	7	7	12	3	147	84	246
實體類	電訊	1	1	5	3	18	6	165	54	243
人員類	外部人員	3	0	1	3	99	0	27	108	234
人員類	內部人員	3	0	1	1	144	0	29	48	221
實體類	電訊	1	1	3	3	17	5	138	51	211
文件類	電子文件	1	1	1	1	85	11	17	90	203
文件類	紙本文件	3	5	3	7	36	20	27	112	195
文件類	紙本文件	3	5	3	7	36	20	27	112	195
實體類	電訊	1	1	5	1	15	5	155	16	191
實體類	電訊	1	1	3	3	17	5	114	51	187
文件類	紙本文件	7	5	3	7	84	0	12	84	180
實體類	一般硬體	1	1	7	5	6	3	126	40	175
實體類	一般硬體	1	1	7	3	8	3	140	24	175
實體類	一般硬體	1	1	7	5	6	3	119	40	168
人員類	內部人員	3	0	1	3	69	0	29	69	167
人員類	內部人員	3	0	1	3	69	0	29	69	167
服務類	外部服務	1	1	3	7	12	3	63	84	162
實體類	電訊	1	1	3	1	17	5	102	17	141
實體類	一般硬體	1	1	5	5	6	3	80	40	129
實體類	一般硬體	1	1	5	5	6	3	75	40	124
人員類	內部人員	7	0	3	3	56	0	30	27	113
人員類	內部人員	1	0	1	1	36	0	36	39	111
實體類	一般硬體	1	1	3	1	8	3	90	8	109
軟體類	商用軟體	1	1	1	3	15	16	29	48	108
實體類	電腦媒體	1	1	3	1	28	4	42	28	102
實體類	電腦媒體	1	1	3	1	28	4	42	28	102
文件類	電子文件	3	1	1	3	39	5	7	48	99
人員類	內部人員	7	0	1	3	63	0	8	27	98
人員類	內部人員	5	0	3	3	40	0	30	27	97
人員類	內部人員	5	0	3	3	40	0	30	27	97
人員類	外部人員	3	0	3	3	33	0	24	39	96

實體類	一般硬體	1	1	3	1	6	3	72	8	89
文件類	紙本文件	3	1	1	3	30	4	11	42	87
實體類	一般硬體	1	1	3	3	6	3	48	24	81
人員類	內部人員	3	0	3	3	24	0	30	27	81
實體類	一般硬體	1	1	3	3	6	3	48	24	81
服務類	建築	1	1	7	5	4	0	56	20	80
服務類	建築	1	1	7	5	4	0	56	20	80
人員類	內部人員	3	0	3	3	24	0	24	27	75
實體類	電腦媒體	1	1	1	1	28	4	14	28	74
服務類	基礎架構	1	1	5	3	0	2	65	6	73
軟體類	商用軟體	1	1	1	1	17	17	20	19	73
實體類	一般硬體	1	1	1	1	16	5	26	20	67
實體類	一般硬體	1	1	1	1	6	13	26	18	63
人員類	內部人員	1	0	1	1	20	0	20	21	61
實體類	一般硬體	1	1	1	3	6	3	25	24	58
實體類	電腦媒體	1	1	1	1	18	4	14	20	56
實體類	電腦媒體	1	1	1	1	18	4	14	20	56
實體類	一般硬體	1	1	1	3	8	3	20	24	55
實體類	一般硬體	1	1	1	3	8	3	20	24	55
文件類	紙本文件	1	1	1	3	12	0	4	36	52
實體類	電腦保護設施	1	1	3	7	2	1	21	21	45
文件類	紙本文件	1	1	1	1	12	4	9	16	41
文件類	電子文件	1	1	1	1	13	5	7	16	41
文件類	紙本文件	1	1	1	1	10	4	12	14	40
實體類	一般硬體	1	1	1	1	8	3	20	8	39
實體類	一般硬體	1	1	1	1	8	3	20	8	39
實體類	一般硬體	1	1	1	1	8	3	20	8	39
實體類	一般硬體	1	1	1	1	8	3	20	8	39
服務類	建築保護措施	1	1	7	3	0	2	21	6	29
實體類	一般硬體	1	1	1	1	6	1	14	6	27
實體類	一般硬體	1	1	1	1	6	1	13	6	26
人員類	內部人員	1	0	1	1	8	0	8	9	25
服務類	建築保護措施	1	1	5	3	0	2	15	6	23
服務類	建築保護措施	1	1	3	3	0	2	9	6	17
服務類	建築保護措施	1	1	3	3	0	2	9	6	17
文件類	電子文件	1	1	1	1	0	0	2	0	2
文件類	電子文件	1	1	1	1	0	0	1	0	1

附錄三： T大學風險評估結果彙整表

資產類別		資產價值				風險值				
大類	小類	機密性	完整性	可用性	適法性	機密性	完整性	可用性	適法性	總風險值
實體類	電訊	5	5	7	1	345	418	832	30	1625
實體類	電訊	5	5	7	1	345	313	832	30	1520
軟體類	內部發展軟體	5	5	5	1	280	540	532	60	1412
軟體類	商用軟體	5	7	3	1	225	679	444	47	1395
軟體類	商用軟體	5	7	5	1	215	511	560	47	1333
軟體類	商用軟體	5	7	5	1	125	357	410	27	919
軟體類	商用軟體	3	5	3	1	285	275	186	105	851
實體類	一般硬體	1	1	5	1	6	3	670	8	687
實體類	一般硬體	1	1	5	1	6	3	670	8	687
軟體類	商用軟體	5	5	5	1	175	195	265	37	672
軟體類	商用軟體	5	3	5	1	295	105	190	61	651
文件類	電子文件	7	7	7	3	161	63	273	84	581
人員類	外部人員	7	0	1	3	357	0	38	183	578
軟體類	商用軟體	1	3	5	1	83	117	225	85	510
文件類	電子文件	5	7	7	1	105	63	273	26	467
軟體類	商用軟體	5	3	1	1	185	141	72	39	437
人員類	內部人員	7	0	3	1	224	0	144	37	405
實體類	一般硬體	1	1	5	1	6	3	380	8	397
軟體類	商用軟體	5	1	1	7	135	19	22	203	379
服務類	建築	1	1	7	2	106	0	56	212	374
軟體類	內部發展軟體	5	5	5	1	110	100	125	24	359
人員類	外部人員	5	0	1	1	255	0	38	61	354
人員類	外部人員	5	0	1	1	255	0	38	61	354
軟體類	商用軟體	5	3	3	1	125	81	114	27	347
實體類	電訊	1	1	7	1	15	5	308	17	345
人員類	內部人員	7	0	5	1	56	0	280	9	345
軟體類	商用軟體	5	3	3	1	105	87	120	23	335
人員類	內部人員	5	0	1	3	180	0	36	117	333
軟體類	商用軟體	5	1	1	7	110	18	23	168	319
服務類	外部服務	1	1	5	1	42	15	195	42	294
實體類	一般硬體	1	1	5	1	12	5	260	16	293

實體類	一般硬體	1	1	5	1	12	5	260	16	293
實體類	一般硬體	1	1	5	1	12	5	260	16	293
人員類	內部人員	7	0	7	1	56	0	224	9	289
實體類	一般硬體	1	1	5	1	24	9	220	32	285
實體類	電訊	1	1	5	1	17	7	240	19	283
實體類	電訊	1	1	5	1	17	7	240	19	283
軟體類	商用軟體	5	3	5	1	85	51	120	19	275
軟體類	商用軟體	5	3	5	1	85	51	120	19	275
軟體類	商用軟體	3	3	3	1	75	81	90	27	273
實體類	電訊	1	1	5	1	15	5	230	17	267
人員類	外部人員	1	0	1	1	89	0	76	99	264
軟體類	商用軟體	5	3	3	1	85	57	102	19	263
實體類	一般硬體	1	1	5	1	12	5	230	16	263
文件類	紙本文件	3	1	3	5	60	8	51	140	259
文件類	紙本文件	3	1	3	7	48	6	45	154	253
文件類	電子文件	7	7	7	3	91	35	77	48	251
實體類	電訊	1	1	5	1	17	7	200	19	243
人員類	內部人員	7	0	3	1	98	0	114	15	227
文件類	電子文件	7	7	7	1	91	35	77	16	219
文件類	電子文件	7	7	7	1	91	35	77	16	219
軟體類	商用軟體	1	3	5	1	17	51	130	19	217
軟體類	商用軟體	1	3	5	1	17	51	130	19	217
軟體類	商用軟體	1	3	5	1	17	51	130	19	217
人員類	外部人員	1	0	1	1	67	0	54	77	198
軟體類	商用軟體	1	3	5	1	17	51	110	19	197
軟體類	商用軟體	1	3	5	1	17	51	110	19	197
實體類	一般硬體	1	1	5	1	6	3	170	8	187
軟體類	商用軟體	3	3	3	1	51	51	60	19	181
實體類	電訊	1	1	3	1	15	5	138	17	175
實體類	電訊	1	1	3	1	15	5	138	17	175
實體類	電訊	1	1	3	1	15	5	138	17	175
實體類	一般硬體	1	1	3	1	8	5	150	10	173
文件類	電子文件	3	1	3	5	39	5	27	80	151
實體類	一般硬體	1	1	5	1	6	3	130	8	147
實體類	一般硬體	1	1	5	1	6	3	130	8	147
實體類	一般硬體	1	1	5	1	6	3	130	8	147
實體類	一般硬體	1	1	5	1	6	3	130	8	147

文件類	電子文件	5	5	5	1	65	25	35	16	141
文件類	電子文件	5	5	5	1	65	25	35	16	141
實體類	一般硬體	1	1	5	1	6	3	120	8	137
實體類	一般硬體	1	1	5	1	6	3	120	8	137
實體類	一般硬體	1	1	3	1	6	3	114	8	131
實體類	一般硬體	1	1	3	1	6	3	114	8	131
實體類	一般硬體	1	1	5	1	6	3	110	8	127
文件類	紙本文件	1	1	1	7	10	4	11	98	123
實體類	一般硬體	1	1	5	1	6	3	90	8	107
實體類	一般硬體	1	1	5	1	6	3	90	8	107
軟體類	內部發展軟體	1	1	1	1	20	24	37	22	103
實體類	一般硬體	1	1	3	1	6	3	78	8	95
實體類	一般硬體	1	1	3	1	6	3	78	8	95
文件類	紙本文件	3	1	1	1	51	4	10	21	86
服務類	建築保護措施	1	1	1	1	0	24	31	24	79
服務類	基礎架構	1	1	5	1	0	2	75	2	79
服務類	基礎架構	1	1	5	1	0	2	75	2	79
人員類	外部人員	5	0	1	1	55	0	8	13	76
服務類	基礎架構	1	1	5	1	0	2	55	2	59
實體類	一般硬體	1	1	1	1	12	5	26	16	59
文件類	電子文件	1	3	1	1	13	15	11	16	55
文件類	電子文件	1	3	1	1	13	15	11	16	55
服務類	外部服務	1	1	7	3	4	1	35	12	52
服務類	基礎架構	1	1	3	5	0	2	33	10	45
實體類	一般硬體	1	1	1	1	6	3	16	8	33
服務類	建築保護措施	1	1	3	1	0	2	9	2	13
服務類	建築保護措施	1	1	1	1	0	2	3	2	7
實體類	電腦保護設施	1	1	1	1	0	2	3	2	7
實體類	電腦保護設施	1	1	1	1	0	2	3	2	7

附錄四：資訊安全風險評估之差異因素架構案例問卷

各位長官、專家、先進：您好!

這是一份學術性之問卷調查，主要探討資訊安全風險評估結果之差異原因。希望透過問卷調查形式探討風險評估時各項因素的影響權重，並了解貴組織在執行風險評估時評估之準則，以作為本研究之差異原因依據。

本此調查問卷純為學術研究之用，不另作其他用途，亦不對外公開，因此懇請您依個人感受安心作答，您的幫助將是此論文研究計畫成功與否的關鍵，佔用您寶貴的時間，在此衷心感謝您的支持與協助致上十二萬分謝意！

敬祝

身體健康　萬事如意！

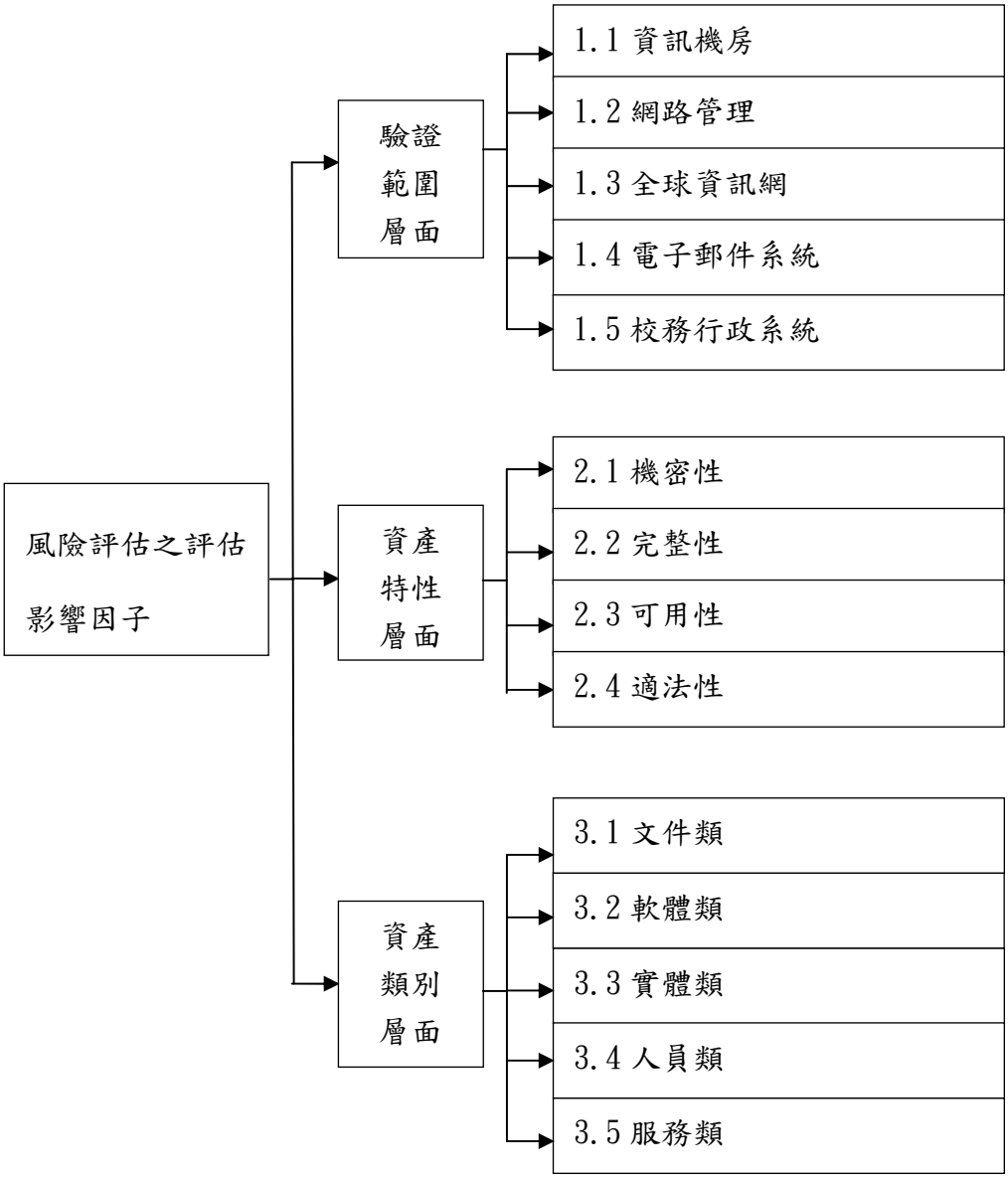
東海大學資訊工程研究所
指導教授：呂芳懌 博士
研究生：吳秀娟 敬上
連絡電話：0963-014150
電子信箱:ada.taiwan@gmail.com

【問卷目的】

本研究乃是利用**層級分析法**(Analytic Hypothesis Process, AHP)作為研究方法，以資訊安全風險評估為範疇，衡量影響貴單位風險評估各**因子間權重**之關係，影響層面包含驗證範圍層面、資產特性層面、及資產類別層面。藉以分析出影響風險評估的風險值之重要要素。

本問卷主要目的透過問卷蒐集各位專家先進之意見，希望了解您於貴單位執行資訊安全風險評估的估算方式與各層面因子之相對權重關係，以便了解貴組織風險評估結果與各因子的影響關聯。

【資訊安全風險評估之差異因素架構】



【資訊安全風險評估影響因素各項說明】

層面	準則	評估準則意義
1. 驗證範圍層面	1.1 資訊機房	資訊機房維運之重要性。
	1.2 網路管理	網路管理維運之重要性。
	1.3 全球資訊網	全球資訊網維運之重要性。
	1.4 電子郵件系統	電子郵件維運之重要性。
	1.5 校務行政系統	校務行政系統維運之重要性。
2.資產特性層面	2.1 機密性	請考量資訊資產分級、資訊資產洩露傷害程度、人員業務性質等機密特性之重要度。
	2.2 完整性	請考量資訊資產不完整時會造成損失影響範圍、正確性及完整性的要求程度等特性之重要度。
	2.3 可用性	請考量資訊資產可忍受服務中斷時間長度、仰賴系統程度、仰賴員工程度等特性之重要度。
	2.4 適法性	請考量資訊資產須遵守之法令、規範、合約義務或是組織內部之政策、章程要求等特性之重要度。
3.資產類別層面	3.1 文件類	請考量紙本文件、電子文件之重要性。
	3.2 軟體類	請考量商用軟體、內部發展軟體之重要性。
	3.3 實體類	請考量一般硬體、電訊、電腦媒體、電腦保護設施之重要性。
	3.4 人員類	請考量內部人員、外部人員之重要性。
	3.5 服務類	請考量網路服務、主機服務、電話服務、建築、保護設施、一般公共設施(冷氣、電力、空調、照明) 之重要性。

填寫說明

甲、本問卷為層級分析（AHP）問卷，請先按所列因子之重要性排序，以提高勾選時之一致性（按：一組因子間的邏輯一致性是填寫 AHP 問卷之必要條件，如 Z>X>Y，則 Y<Z 必須成立，否則將導致該份問卷無效。）；再請就兩個因子進行比較，依其比值全依**個人專業經驗之主觀判定**。

乙、在進行重要性排序及相對重要性勾選前，請先參閱「問卷目的」及「資訊安全風險評估影響因素各項說明」之內容，再進行因子相對重要性判斷。

（一） 因子排序：假設您購買車輛的三個考量因子為：1. 價格、2.性能、3.外型，如果您認為其重要性程度為「外型」≧「價格」≧「性能」，則**請填寫（3）≧（1）≧（2）**。

（二）因子相對重要性勾選：以上項所舉選擇車輛的三個考量因子為例，如您認為下表左邊的因子「價格」相對於右邊的因子「性能」之重要性為 6：1，則請在左邊 6：1 欄內打「v」，依此類推（依上項排序，如您認為「價格」≧「性能」，則此時如勾選右邊的比值，在邏輯上就有衝突矛盾之處。）反之，若您認右邊的因子相對重要性較高，則請在右邊比值欄內打「」，尺度數字愈大者表示重要性愈高。

考量因子	重要程度																	考量因子
	絕對重要		極為重要		頗為重要		稍微重要		同等重要		稍不重要		頗不重要		極不重要		絕不重要	
	9:1	8:1	7:1	6:1	5:1	4:1	3:1	2:1	1:1	1:2	1:3	1:4	1:5	1:6	1:7	1:8	1:9	
1. 價格				v														2. 性能
										v								3. 外型
2. 性能														v				3. 外型

問卷由此開始:

一、「風險評估之評估影響因子」考量三項層面分別為：1.驗證範圍層面 2.資產特性層面　3.資產類別層面。

1-1.請按其重要程度將三大因子層面之代號**依序填入括號內**：(　)≧(　)≧(　)

1-2.請依據上項順序比較下表中左右各因子之相對重要性，並勾選之：

考量因子	重要程度																	考量因子
	絕對重要		極為重要		頗為重要		稍微重要		同等重要		稍不重要		頗不重要		極不重要		絕不重要	
	9:1	8:1	7:1	6:1	5:1	4:1	3:1	2:1	1:1	1:2	1:3	1:4	1:5	1:6	1:7	1:8	1:9	
1. 驗證範圍層面																		2. 資產特性層面
																		3. 資產類別層面
2. 資產特性層面																		3. 資產類別層面

二、「驗證範圍層面」考量五項層面分別為： 1. 資訊機房 2.網路管理 3.全球資訊網 4.電子郵件系統 5.校務行政系統

2-1. 請您依據經驗判斷重要程度將五大考量因子之代號依序填入括號內：(　) ≧ (　) ≧ (　) ≧ (　) ≧ (　)

2-2. 請依據上項順序比較下表中左右各因子之相對重要性，並勾選之：

考量因子	重要程度																	考量因子
	絕對重要		極為重要		頗為重要		稍微重要		同等重要		稍不重要		頗不重要		極不重要		絕不重要	
	9:1	8:1	7:1	6:1	5:1	4:1	3:1	2:1	1:1	1:2	1:3	1:4	1:5	1:6	1:7	1:8	1:9	
1. 資訊機房																		2. 網路管理
																		3. 全球資訊網
																		4. 電子郵件系統
																		5. 校務行政系統
2. 網路管理																		3. 全球資訊網
																		4. 電子郵件系統
																		5. 校務行政系統
3. 全球資訊網																		4. 電子郵件系統
																		5. 校務行政系統
4. 電子郵件系統																		5. 校務行政系統

三、在「資產特性層面」應考量之因子分別為：1.機密性 2.完整性 3 可用性 4.適法性

3-1. 請您依據經驗判斷重要程度將四大考量因子之代號依序填入括號內：(　) ≧ (　) ≧ (　) ≧ (　)

3-2. 請依據上項順序比較下表中左右各因子之相對重要性，並勾選之：

考量因子	重要程度																	考量因子
	絕對重要		極為重要		頗為重要		稍微重要		同等重要		稍不重要		頗不重要		極不重要		絕不重要	
	9:1	8:1	7:1	6:1	5:1	4:1	3:1	2:1	1:1	1:2	1:3	1:4	1:5	1:6	1:7	1:8	1:9	
1. 機密性																		2. 完整性
																		3. 可用性
																		4. 適法性
2. 完整性																		3. 可用性
																		4. 適法性
3. 可用性																		4. 適法性

四、在「資產類別」應考量之因子分別為：1.文件類 2.軟體類 3.實體類 4.人員類 5.服務類。

4-1. 請您依據經驗判斷重要程度將五大考量因子之代號依序填入括號內：(　) ≧ (　) ≧ (　) ≧ (　) ≧ (　)

4-2. 請依據上項順序比較下表中左右各因子之相對重要性，並勾選之：

考量因子	重要程度																	考量因子
	絕對重要		極為重要		頗為重要		稍微重要		同等重要		稍不重要		頗不重要		極不重要		絕不重要	
	9:1	8:1	7:1	6:1	5:1	4:1	3:1	2:1	1:1	1:2	1:3	1:4	1:5	1:6	1:7	1:8	1:9	
1. 文件類																		2. 軟體類
																		3. 實體類
																		4. 人員類
																		5. 服務類
2. 軟體類																		3. 實體類
																		4. 人員類
																		5. 服務類
3. 實體類																		4. 人員類
																		5. 服務類
4. 人員類																		5. 服務類

五、請您依照經驗勾選，貴組織過去曾面臨過之威脅、弱點與資安事件。

(一) 弱點：

- ☐ 系統漏洞：如網路、作業、應用系統開發時所產生的漏洞。
- ☐ 教育訓練不足：對於資安的不重視或是故意忽略，認為危機不會發生。
- ☐ 人員缺乏：原來開發或維護人員離職，導致有系統持續運作而無人負責。
- ☐ 實體環境不良：電力、空調、伺服器及環境等，未依據標準或法規進行施作或施作不完全。
- ☐ 軟體之安全機制不足：對於軟體開發時，無提供更新或是安全的操作機制。
- ☐ 角色定義不明：對於組織、權限、所有人角色的定義不明。

(二)威脅：

- ☐ 天然因素災害：指火災、水災、地震、打雷及溫濕度異常等。
- ☐ 天然因素故障：指系統自然耗損發生故障，硬體、軟體、網路故障等。
- ☐ 人為過失：指人為錯誤或怠慢造成，如操作疏失、維護疏失、管理疏失等。
- ☐ 人為故意：指人為惡意或蓄意造成之故障，如人為破壞、濫權、犯罪等。

(三)資安事件：

- ☐ 病毒感染：外來病毒造成系統不正常或中斷運作。
- ☐ 入侵及跳板：駭客入侵竊取資料或是利用合法的服務主機去非法攻擊他人服務。
- ☐ 阻絕服務：利用外來合法主機或多方攻擊方式，導致網路或服務中斷運作。
- ☐ 垃圾郵件：利用垃圾郵件，阻塞訊息傳遞服務或是利用大量的垃圾郵件，造成郵件主機需額外投資大量成本在防制垃圾郵件上。
- ☐ 資料或實體竊取：電子資料、文件或資訊設備，因人為竊取，要成資料外洩或無法正常服務。
- ☐ 資料竄改：以駭客手法或是內賊將原有電子資料、文件進行內容竄改，造成提供之資訊錯誤。
- ☐ 操作不當：因人為因素操作系統，造成設備、資料服務中斷、異常。
- ☐ 系統失效 (硬體系統、作業系統、應用系統、網路系統)：系統因故障，導致無法正常運作，對於服務中斷所造成損失衝擊。
- ☐ 溫濕度因素或電源供應不良：因天候因素，造成溫度或濕度大量提高或因電力供應失效，導致系統、硬體設備無法正常運作甚至於設備毀損。
- ☐ 火、水災或地震等天然災害：因天然災害，導致系統運作的環境毀損，進而造成系統無法正常運作。

感謝您百忙之中撥冗填寫問卷，請惠於留下您的相關資料：

1.請問您的資安/職能身份是 (可複選) ：

☐程式設計人員　☐備份系統管理者　☐資料庫管理者

☐機房管理人員　☐網路管理人員　☐資訊安全工作小組

☐校務行政系統管理人員　☐電子郵件系統管理人員

☐全球資訊系統管理人員　☐其他_____

2.請問您於貴校工作時間約有_____年。

3.如尚有寶貴之指正意見，煩請您詳填於下，我們將會參考改正，以提升本研究之深度與廣度，再次謝謝您！

本問卷到此結束，**請確認上述問題已全數填寫完畢**。並再次謝謝您的協助！

敬祝　心想事成 萬事如意！