南華大學

資訊管理學系

碩士論文

基於ISO 27001:2013轉版建置資訊安全管理系統程序探討－以某大學為例

Discussion on Establishing Information Security Management System Based on ISO 27001: 2013 Revolving Edition - Taking a University as an Example

研 究 生：蔡伶宜

指導教授：王昌斌

中華民國 107 年 1 月 11 日

南　華　大　學

資訊管理學系

碩 士 學 位 論 文

基於 ISO 27001:2013 轉版建置資訊安全管理系統程序探討－以某大學為例

Discussion on Establishing Information Security Management System Based on ISO 27001: 2013 Revolving Edition - Taking a University as an Example

研究生：蔡伶宜

經考試合格特此證明

口試委員：

指導教授：

系主任(所長)：

口試日期：中華民國 107 年 1 月 11 日

南 華 大 學 碩 士 班 研 究 生

論 文 指 導 教 授 推 薦 函

資訊管理 系碩士班 蔡 伶 宜 君所提之論文

基於 ISO 27001:2013 轉版建置資訊安全管理系統程序探討－以某大學為例

係由本人指導撰述，同意提付審查。

指導教授 _____

107 年 1 月 11 日

南華大學資訊管理學系碩士論文著作財產權同意書

立書人：蔡伶宜之碩士畢業論文

中文題目：基於 ISO 27001:2013 轉版建置資訊安全管理系統程序探討

－以某大學為例

英文題目：Discussion on Establishing Information Security Management System Based on ISO 27001: 2013 Revolving Edition - Taking a University as an Example

指導教授：　王昌斌　　博士

學生與指導老師就本篇論文內容及資料其著作財產權歸屬如下：

■ 共同享有著作權

□ 共同享有著作權，學生願「拋棄」著作財產權

□ 學生獨自享有著作財產權

學　　生：蔡伶宜（請親自簽名）

指導老師：（請親自簽名）

中　華　民　國　107　年　1　月　11　月

誌　謝

在南華資管碩士班學習期間,感謝這一路陪伴支持我走下去的家人、朋友與同事們，因為你們的鼓勵與扶持讓我有勇氣堅持下去。

感謝系上諸位師長與 105 年級資訊管理碩士專班全體同學們，在我學習過程中無私的指導與相互激勵，讓我碩士修業期間知識增長與充滿美好回憶。

感謝恩師王昌斌教授願意以他豐富的學養指導我，在我論文寫作過程中不厭其煩的循循善誘，教導我許多觀念與知識，讓我在論文研究上獲益良多。承蒙陸海文教授、中正大學阮金聲教授，在百忙之中願意前來擔任我的論文口試委員,在論文口試期間對論文詳加審閱與細心指導，針對論文的不足之處給予寶貴意見，使論文能夠更臻完善，藉此致上本人最真誠的感謝。

最後，謹以此篇研究獻給上帝，願一切頌讚都歸我主，願上帝祝福您們。

蔡伶宜 謹誌

中華民國一〇七年一月

基於 ISO 27001:2013 轉版建置資訊安全管理系統程序探討－以某大學為例

學生:蔡伶宜　　指導教授:王昌斌 博士

南 華 大 學 資訊管理學系碩士班

摘要

現今資訊科技應用發展快速，如何避免網路應用時重要資訊與個人隱私不會遭到竊取或竄改、如何強化組織的資訊安全以及當資安事件發生時的衝擊損害程度能夠降低，導入資訊安全管理系統即為首要工作。

教育部於 105 年 8 月 15 日提出新版「教育體系資通安全暨個人資料管理規範」,並以此規範為基礎建立驗證機制。本研究以個案研究的角度，從組織在既有資通安全管理規範下為何願意再進行轉版的動機、新舊規範的差異分析、執行資安資產盤點與風險評鑑、制定組織新版資通安全管理規範，到通過第三方驗證，深入探討轉版建置新規範所面臨的困難及解決方法、導入效益以及成功因素，期望能提供給有意轉版資通安全管理規範的組織有個實作參考步驟，能迅速有效的完成新版資通安全管理規範。

關鍵詞: ISO 27001:2013、轉版、資訊安全管理系統、教育體系資通安全管理規範、教育體系資通安全暨個人資料管理規範

Discussion on Establishing Information Security Management System
Based on ISO 27001: 2013 Revolving Edition
- Taking a University as an Example

Student: Tsai,Ling-Yi Advisors: Dr.Wang,Chang-Bin

Department of Information Management
The M.I.M. Program
Nan-Hua University

ABSTRACT

Nowadays, due to the rapid development of information technology, the application of Information Security Management System (ISMS) to the internet usage has become a primary task. With the monitoring of ISMS, we can keep our personal and private information confidential. Otherwise, personal information could be stolen, pirated or tampered. Moreover, ISMS can improve the information security for the organizations, and reduce the damage in the security events.

The Ministry of Education released the new “Information Security Management and Personal Information Management Practices for Education System” in August 15, 2016, and took it as the core of the verification mechanism. This case study aims to investigate the motivation to adopt the new version of ISMS, the differences between the previous and new versions, the execution of the information assets and the risk assessment, the establishment of new ISMS standard and the authentication of the third- party. This study makes further interpretations of the difficulties, solutions, benefits, and the succeeding factors of implementing the new “Information Security Management Practices for Education System”. Hopefully, the study can provide the practical suggestions for any organizations willing to adopt the new Information Security Management Practices for Education System” .

Keyword: ISO 27001:2013, Version of the Converion, Information Security Management System (ISMS), Information Security Management Practices for Education System, Information Security Management and Personal Information Management Practices for Education System

目錄

表　　目　　錄

圖　　目　　錄

第一章、緒論

第一節　研究背景

網際網路發展蓬勃今日，改變了人類食、衣、住、行的消費者行為，企業利用網路平台創造了無限商機利潤，龐大利益卻也因此遭到覬覦，網路犯罪行為層出不窮，因此如何維持資訊安全，導入資訊安全管理系統即為首要議題，近年資安問題引發的網路犯罪案件層出不窮，如下幾個案例:

壹、TREDN LABS 於 2017 年 2 月 20 日公布的「2016 年十大重大網路資安事件」中顯示， Distributed Denial of Service (簡稱 DDoS 分散式阻斷服務攻擊)，造成美國一家域名服務器管理機構 Dynamic Network Service(簡稱 Dyn)底下的客戶網站因而無法瀏覽；駭客發動最大規模的 DDoS 攻擊，據說曾經一度中斷非洲國家利比亞的網路。

(資料來源:https://blog.trendmicro.com.tw/?p=45442)。

貳、The News Lens 於 2017 年 5 月 13 日發表的「『勒索病毒』癱瘓全球 99 國網路，專家建議：不明『電子發票、訂單』信件勿開」文章中指出，勒索病毒 WannaCry 正在全球網路肆虐，BBC 報導指出，已有 99 個國家地區傳出感染事件，包括英、美、中國大陸、俄羅斯、西班牙、義大利及台灣。

(資料來源:https://www.thenewslens.com/article/68259)。

參、TechNews 於 2016 年 3 月 27 日公布的「史上最大銀行竊案，孟加拉央行損失逾 20 億」文章中指出，嫌犯企圖從孟加拉央行在紐約聯邦儲蓄銀行的帳戶偷走將近 10 億美元（約台幣 32.8 億元），此竊案最特別的地方在嫌犯利用網路犯案，準確地掌握各個銀行的空窗期，

事後更逃得無影無蹤。

(資料來源: https://technews.tw/2016/03/27/the-mystery-of-bangladeshs-missing-millions/)。

肆、The News Lens 於 2016 年 4 月 26 日發表的「烏克蘭電力系統遭駭原因是網路釣魚，如何加強資安防護引討論」文章中指出，2015 年 12 月 23 日，烏克蘭電力網路受到駭客攻擊，導致伊萬諾-弗蘭科夫斯克州大停電，1 個月後安全專家證實這起停電是駭客惡意攻擊所造成，成為全世界第一起駭客攻擊造成電力網路大規模停電事件。

(資料來源:
https://technews.tw/2016/04/26/ukraine-power-system-phishing-information-security-protection/)。

伍、自由時報(Liberty Time Net)於 2017 年 10 月 7 日發佈的 [遠東商銀遭駭 刑事局證實駭客來自外部]新聞中指出，遠東商銀於 10 月 3 日發現 SWIFT(環球銀行間金融電訊網路)系統遭駭客入侵，盜走 6000 萬美元(約 18 億元)，刑事局表示，目前確認駭客來自外部且為最新的病毒，現該銀行已封存遭駭電腦，刑事局科技研發科協助數位鑑識還原工作，釐清駭客入侵手法及途徑，反向追查駭客來源及身分。

(資料來源:http://news.ltn.com.tw/news/society/breakingnews/2216009)。

陸、Trend Micro 於 2017 年 3 月 7 日發佈的「趨勢科技 2016 年資訊安全總評報告出爐 勒索病毒家族數量飆升 7 倍 台灣受勒索病毒的攻擊次數排名全球前 20%」指出，勒索病毒造成全球企業損失金額高達 10 億美元，且勒索病毒新家族數量較 2015 年相比成長 7 倍，而台灣遭受此攻擊次數更排名全球前 20%，顯現駭客攻擊對企業的影響幅度有加劇之趨勢。

(資料來源:
http://www.trendmicro.tw/tw/about-us/newsroom/releases/articles/20170315064246.html)。

以上這些真實案例讓我們了解，網路犯罪影響層面已不再單只是個

人，也不單是一家企業，現在影響層面已擴大到全球性的企業、甚至是國家安全，因此資通安全的保護已是全球所重視的議題，如何建置一個全方位的資訊安全防護機制，更是全球各國家、各組織及企業所重視的工作。

第二節　研究動機

全球重視資通安全防護機制的趨勢下，台灣在民國 90 年 1 月通過「建立我國通資訊基礎設施安全機制計畫」，並成立「行政院國家資通安全會報」，積極推動我國資通安全基礎建設工作。民國 105 年 8 月行政院成立「資通安全處」，成為台灣政院資安專責機構，並提出「資通安全管理法」草案送交立法院院會審查，未來將賦予各機關資通安全維護義務之法律基礎，以及提升國家公務機構之資安防護水準。

現行資通安全規定，是遵循行政院於民國 104 年 1 月 20 日公告「政府機關（構）資通安全責任等級分級作業規定」，該作業規定中將資安責任等級分為三類:政府機關、學術機構、國(公)營事業/醫療機構及其他，再由這三類中依重要性等級區分為 A、B、C 三級。

教育部為學術機構之主管機關，負責規劃校園資訊安全管理系統(Information Security Management System, 簡稱 ISMS)，推動及落實校園資訊安全業務，依教育部於民國 104 年 7 月 13 日發佈「教育部與所屬機關(構)及學校資通安全責任等級分級作業規定」，資通安全責任等級亦區分為 A、B、C 三級，而本研究個案為私立大學，依規定列屬於 B 級單位。

在教育部規劃與執行的「教育部提昇校園資訊安全服務計畫」中，工作目標其一為 「規劃教育機構資安驗證機制」，該機制是以教育部於民國 96 年 6 月 11 日公佈之「教育體系資通安全管理規範」為驗證標準，

針對教育機構內符合政府機關（構）資訊安全責任等級分級中的 A、B 級教育機構，規劃其資安驗證稽核制度，用以確保教育體系各單位、學校落實資訊安全管理系統的有效性。然而，隨著資通訊科技發展快速，資通訊科技進步與廣泛使用，為因應資通訊環境之變化，並考量我國個人資料保護法之修正與實施，以及最佳國際實務標準之發展與普及，教育部自民國 104 年起著手「教育體系資通安全管理規範」修訂，於民國 105 年 8 月 5 日提出新版「教育體系資通安全暨個人資料管理規範」。

針對組織導入資訊安全系統、資安驗證等以往已有許多學者做過相關研究，但尚無以「教育體系資通安全管理規範」轉版「教育體系資通安全暨個人資料管理規範」為基礎來建置資訊安全管理系統程序探討。本研究以研究新舊規範的差異性，對於組織推動建置新版資通安全管理規範可能面臨的困難點與阻力進行個案研究，以提供給未來欲建置新版資通安全管理規範程序之單位參考，期望建置程序能夠較為順利。

第三節　研究目的

本研究之研究者為本研究個案單位之職員，負責處理資訊安全相關工作，藉由校內簽呈取得個案單位鈞長同意，而進行以下個案之研究。

本研究主要針對組織在既有的資通安全管理規範下，如何進行新版資通安全管理規範轉版建置，進而取得第三方認證機構的驗證機制，期望提供相關研究資料，給其他有意取得相同的資安驗證組織作為參考依據。故期望此研究能達到以下具體目的：

壹、 瞭解組織在已建立資通安全管理規範，仍願意再進行轉版的動機。

貳、 在轉版建置新規範的過程中，組織面對困難時的解決方法。

參、 探討組織獲得新資通安全規範驗證的成功因素。

肆、 探討組織導入新資通安全規範後所獲的效益。

第四節　研究流程

本研究共分為五章，論文之研究流程，如圖 1.1 研究流程圖，各章摘要說明如下:

第一章緒論：

說明本研究的研究背景、研究動機、研究目的與研究流程。

第二章文獻探討：

本章將探討資訊安全管理系統、ISO 27001:2013 資訊安全管理國際標準、教育體系資通安全暨個人資料管理規範、教育機構資通安全驗證轉版流程，及其相關探討的論文期刊資料。

第三章研究方法：

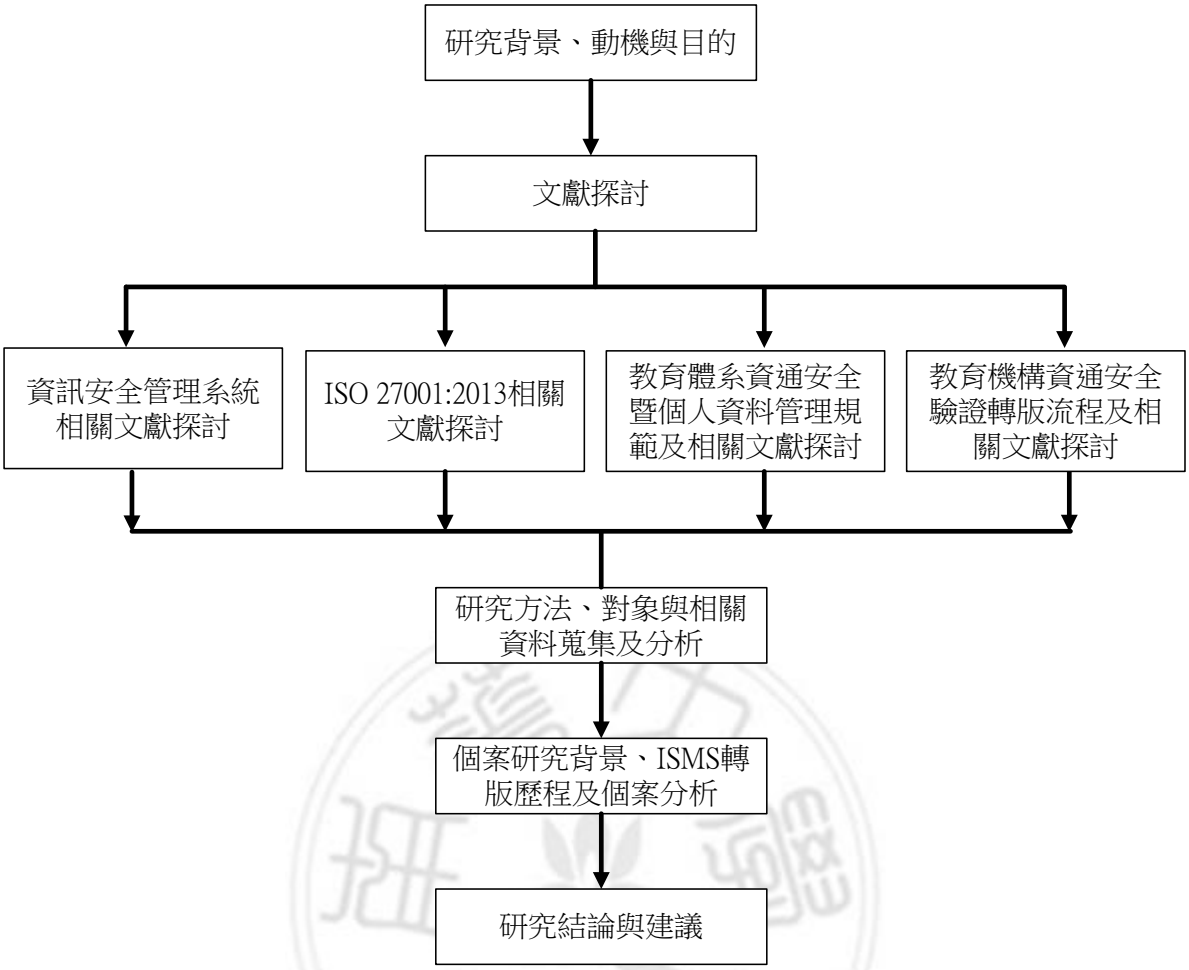
說明本研究的研究方法、研究對象與相關資料蒐集及分析方法。

第四章研究過程與結果分析：

用以探討個案研究背景、ISMS 轉版歷程與個案分析研究。

第五章結論與建議：

為本研究的最後一章，說明本研究的結論及提出未來建議。



▲圖 1.1：研究流程圖
資料來源 ： 本研究整理

第二章 文獻探討

本章節是以資訊安全管理系統、ISO 27001:2013、教育體系資通安全管理規範...等議題，彙整相關文獻資料，由資訊安全管理系統的定義及目標、ISO 27001:2013 資訊安全管理國際標準內容介紹、教育體系資通安全暨個人資料管理規範及教育機構資訊安全驗證轉版流程...等，進行逐一探討。

第一節 資訊安全管理系統

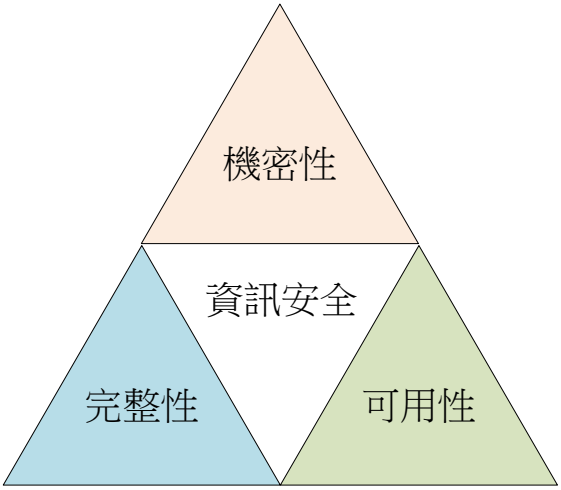
資訊科技發達的現代，資料以電腦處理、傳遞和儲存的過程，可能會遭受到內部或外部的攻擊、入侵或攔截，造成資料被破壞或不當揭露，而造成單位的重大損失，因此資訊安全不論在政府部門、企業機構、學校單位，或小至個人，都已是熱門的討論議題。

資訊安全的三個要素為機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)，簡稱 CIA(林祝興、張明信，2015)，如圖 2.1: 資訊安全三要素，其定義說明如下:

壹、機密性(C):確保資料傳遞、儲存時的私密性，不會被未經授權的使用者有意或無意揭露資料。

貳、完整性(I):在文件傳送或儲存過程中，須確保內容未經非授權的使用者或處理程序所竄改。

參、可用性(A):資料須即時並可靠的提供給企業內部使用，並確保資料能保持可用狀態或系統不能中斷服務。



▲圖 2.1: 資訊安全三要素
資料來源 : 林祝興、張明信，2015

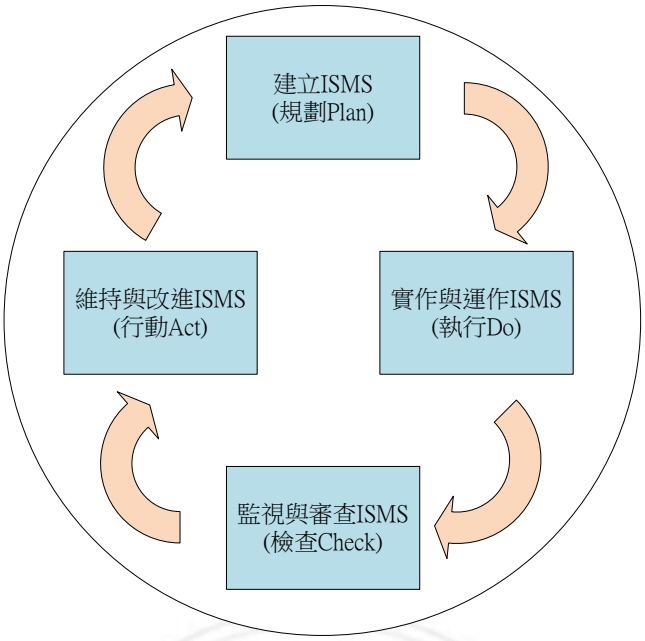
企業組織遵照國際標準 ISO/IEC 27001，建立一套以風險管理為基礎，協助企業組織控管資訊安全風險，確保組織能持續營運的系統，稱為資訊安全管理系統(Information Security Management System，簡稱 ISMS)。資訊安全管理系統是永續經營的工作，它以美國學者愛德華茲.戴明所提出的 PDCA 循環為流程導向，將資訊安全管理系統進行品質管理工作，藉由 PDCA 四個階段不斷循環，週而復始，以確保資訊安全管理系統符合組織的需求與持續有效性，如圖 2.2: ISMS 的 PDCA 循環(潘天佑，2008)，四階段說明如下:

壹、規劃(Plan)：依據組織全景與利害關係團體之要求，建立資訊安全相關的政策、目標、控制措施及程序，達成組織政策程序一致的效果。

貳、執行(Do)：施行與操作資訊安全政策與程序。

參、檢查(Check)：監視與審查資訊安全政策，以適當的量測方法進行測量評估，提報評估結果報告供給管理階層審查，並授權矯正、改善行動。

肆、行動(Act)：依據管理審查結果之矯正措施進行資訊安全改善動作。

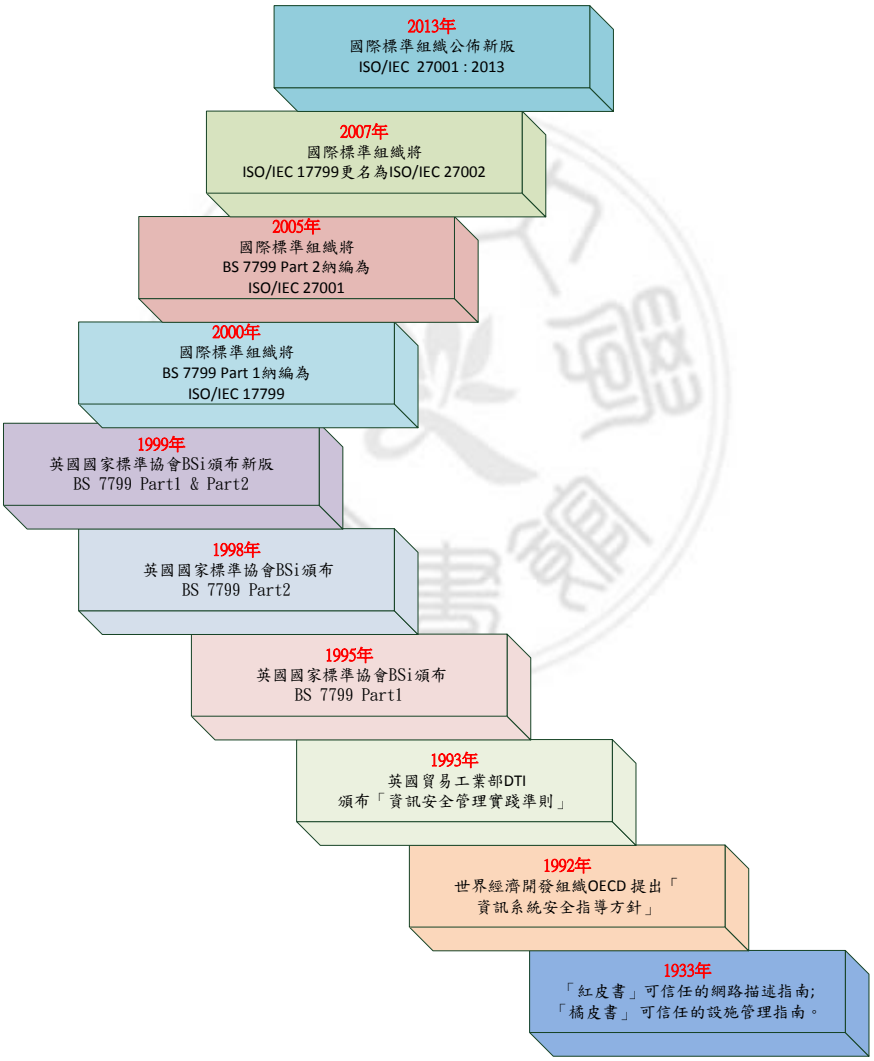


▲ 圖2.2: ISMS的PDCA循環
資料來源：潘天佑，2008

第二節　ISO 27001：2013 資訊安全管理國際標準

ISO 27001 的發展史最早可追朔到 1933 年美國公佈的「紅皮書」可信任的網路描述指南;「橘皮書」 可信任的設施管理指南。1992 年世界經濟開發組織(OECD)提出的資訊系統安全指導方針。1993 年英國貿易工業部(Department of Trade and Industry，DTI)頒布「資訊安全管理實踐準則」(PD0005 Code of Prctice)。1995 年英國國家標準協會(British Standards Institution，BSi)公佈 BS 7799 Part 1「資訊安全管理實務準則」(Code of Practic for Information Security Management)，內容明確建議資訊安全控管實施指南，詳細說明執行的建議;於 1998 年公佈 BS 7799 Part 2「資訊安全管理規範」(Specification for Information Security Management Systems)，主要陳述驗證的依據，如要取得 BS7799 驗證及證書，須遵守的規範要求;BSi 又於 1999 年發佈新版 BS 7799 Part 1 & Part 2。BS 7799 原為英國國家標準，因廣泛涵蓋許多資訊安全的議題，且適用於各種產業與組織，

因此被許多國家採用為國家標準，如:台灣、挪威、捷克、芬蘭、巴西、澳洲和紐西蘭...等國家。在 2000 年國際標準組織(International Organization for Standardization)將 BS 7799 Part 1 納編為 ISO/IEC 17799; 又於 2005 年將 BS 7799 Part2 納編為 ISO/IEC 27001。在 2007 年將 ISO/IEC 17799 更名為 ISO/IEC 27002，並將資訊安全管理標準全部納為 ISO 27000 系列，如圖 2.3: ISO 27001 演進歷史(劉勝雄，2010)。



▲圖 2.3: ISO 27001 演進歷史
資料來源 :劉勝雄，2010

ISO 27001 自 2005 年公佈，經過 8 年後考量資訊科技的快速發展，組織架構與運作模式皆已轉變，管理規範有必要重新檢視與調整，於 2013 年公佈 ISO/IEC 27001:2013，此標準規定於組織全景內建置、實作、維持與持續改善資訊安全管理系統之要求事項，亦包含依組織需要而建立之安全風險評鑑與處理的要求事項，要求事項為通用的，適用於各種形式、規模或性質的組織，而當組織宣稱符合 ISO/IEC 27001:2013 標準時，該組織需遵守標準裡的第 4 到第 10 條款所規定的任何要求事項。以 PDCA 循環來解釋說明第 4 到第 10 條款內容所需執行的工作項目，如表 2.1: ISO/IEC 27001:2013 框架。

表 2.1 : ISO/IEC 27001:2013 框架

PLAN(規劃)				DO(執行)	CHECK(檢查)	ACT(行動)
4 組織全景	**5 管理階層**	**6 規劃**	**7 支援**	**8 運作**	**9 績效評估**	**10 改善**
4.1 瞭解組織及其全景	5.1 領導及承諾	6.1 因應風險及機會的行動	7.1 資源	8.1 運作之規劃及控制	9.1 監督、量測、分析及評估	10.1 不符合事項及矯正措施
4.2 了解關注方之需求及期望	5.2 政策	6.2 資訊安全目標及其達成之規劃	7.2 能力	8.2 資訊安全風險評鑑	9.2 內部稽核	10.2 持續改善
4.3 決定資訊安全管理系統範圍	5.3 組織角色、責任及權限		7.3 認知	8.3 資訊安全風險處理	9.3 管理審查	
4.4 資訊安全管理系統			7.4 溝通或傳達			
			7.5 文件化資訊			

資料來源： NII 產業發展協進會，2016

ISO/IEC 27001 附錄 A 的控制領域 2005 年版與 2013 年版的差異包含有 A.10 通訊與作業安全管理拆分為 A.12 運作安全與 A.13 通訊安全；增列 A.10 密碼學(加密控制)及 A.15 供應者關係，如表 2.2: ISO 27001 控制

領域 2005 年版與 2013 年版的差異分析。

表 2.2: ISO 27001 控制領域 2005 年版與 2013 年版的差異分析

資料來源：陳伯榆，2013

ISO 27001:2013 附錄 A，共包含 14 項控制領域、35 項控制目標、114 項控制項目。14 項控制領域分別為資訊安全政策、資訊安全組織、人力資源安全、資產管理、存取控制、密碼學、實體及環境安全、運作安全、通訊安全、系統獲取、開發及維護、供應者關係、資訊安全事故管理、業務永續運作管理、遵循性，詳細內容如表 2.3：ISO 27001:2013 之控制領域、控制目標及控制項。

表 2.3 : ISO 27001:2013 之控制領域、控制目標及控制項

控制領域	控制目標	控制項目
A.5 資訊安全政策	A.5.1 資訊安全之管理指導方針	A.5.1.1 資訊安全政策
		A.5.1.2 資訊安全政策之審查
A.6 資訊安全之組織	A.6.1 內部組織	A.6.1.1 資訊安全之角色及責任
		A.6.1.2 職務區隔
		A.6.1.3 與權責機關之聯繫
		A.6.1.4 及特殊關注方之聯繫
	A.6.2 行動裝置及遠距工作	A.6.2.1 行動裝置政策
		A.6.2.2 遠距工作
A.7 人力資源安全	A.7.1 聘用前	A.7.1.1 篩選
		A.7.1.2 聘用條款及條件
	A.7.2 聘用期間	A.7.2.1 管理階層責任
		A.7.2.2 資訊安全認知、教育及訓練
		A.7.2.3 懲處過程
	A.7.3 聘用之終止及變更	A.7.3.1 聘用責任之終止及變更
A.8 資產管理	A.8.1 資產責任	A.8.1.1 資產清冊
		A.8.1.2 資產擁有權
		A.8.1.3 資產之可被接受的使用
		A.8.1.4 資產之歸還
	A.8.2 資產分級	A.8.2.1 資產之分級
		A.8.2.2 資產之標示
		A.8.2.3 資產之處置
	A.8.3 媒體處理	A.8.3.1 可移除式媒體之管理
		A.8.3.2 媒體之汰除
		A.8.3.3 實體媒體傳送
A.9 存取控制	A.9.1 存取控制之營運要求事項	A.9.1.1 存取控制政策
		A.9.1.2 對網路及網路服務之存取
	A.9.2 使用者存取管理	A.9.2.1 使用者註冊及註銷
		A.9.2.2 使用者存取權限之配置
		A.9.2.3 具特殊存取權限之管理
		A.9.2.4 使用者之秘密鑑別資訊的管理
		A.9.2.5 使用者存取權限之審查
		A.9.2.6 存取權限之移除或調整
	A.9.3 使用者責任	A.9.3.1 秘密鑑別資訊之使用
	A.9.4 系統及應用存取控制	A.9.4.1 資訊存取限制

		A.9.4.2 保全登入程序
		A.9.4.3 通行碼管理系統
		A.9.4.4 具特殊權限公用程式之使用
		A.9.4.5 對程式源碼之存取控制
A.10 密碼學	A.10.1 密碼式控制措施	A.10.1.1 使用密碼式控制措施之政策
		A.10.1.2 金鑰管理
A.11 實體及環境安全	A.11.1 安全區域	A.11.1.1 實體安全周界
		A.11.1.2 實體進入控制措施
		A.11.1.3 保全之辦公室、房間及設施
		A.11.1.4 防範外部及環境威脅
		A.11.1.5 於保全區域內工作
		A.11.1.6 交付及裝卸區
	A.11.2 設備	A.11.2.1 設備安置及保護
		A.11.2.2 支援之公用服務事業
		A.11.2.3 佈纜安全
		A.11.2.4 設備維護
		A.11.2.5 財產之攜出
		A.11.2.6 場所外設備及資產的安全
		A.11.2.7 設備汰除或再使用之保全
		A.11.2.8 無人看管之使用者設備
		A.11.2.9 桌面淨空及螢幕淨空政策
A.12 運作安全	A.12.1 運作程序及責任	A.12.1.1 文件化運作程序
		A.12.1.2 變更管理
		A.12.1.3 容量管理
		A.12.1.4 開發、測試及運作環境之區隔
	A.12.2 防範惡意軟體	A.12.2.1 防範惡意軟體之控制措施
	A.12.3 備份	A.12.3.1 資訊備份
	A.12.4 存錄及監視	A.12.4.1 事件存錄
		A.12.4.2 日誌資訊之保護
		A.12.4.3 管理者及操作者日誌
		A.12.4.4 鐘訊同步
	A.12.5 運作中軟體之控制	A.12.5.1 運作中系統之軟體安裝
	A.12.6 技術脆弱性管理	A.12.6.1 技術脆弱性管理
		A.12.6.2 對軟體安裝之限制
	A.12.7 資訊系統稽核考量	A.12.7.1 資訊系統稽核控制措施
A.13 通訊安全	A.13.1 網路安全管理	A.13.1.1 網路控制措施
		A.13.1.2 網路服務之安全

		A.13.1.3 網路之區隔
	A.13.2 資訊傳送	A.13.2.1 資訊傳送政策及程序
		A.13.2.2 資訊傳送協議
		A.13.2.3 電子傳訊
		A.13.2.4 機密性或保密協議
A.14 系統獲取、開發及維護	A.14.1 資訊系統之安全要求事項	A.14.1.1 資訊安全要求事項分析及規格
		A.14.1.2 保全公共網路之應用服務
		A.14.1.3 保護應用服務交易
	A.14.2 於開發及支援過程中之安全	A.14.2.1 保全開發政策
		A.14.2.2 系統變更控制程序
		A.14.2.3 運作平台變更後，應用之技術審查
		A.14.2.4 軟體套件變更之限制
		A.14.2.5 保全系統工程原則
		A.14.2.6 保全開發環境
		A.14.2.7 委外開發
		A.14.2.8 系統安全測試
		A.14.2.9 系統驗收測試
	A.14.3 測試資料	A.14.3.1 測試資料之保護
A.15 供應者關係	A.15.1 供應者關係中之資訊安全	A.15.1.1 供應者關係之資訊安全政策
		A.15.1.2 於供應者協議中闡明安全性
		A.15.1.3 資訊及通訊技術供應鏈
	A.15.2 供應者服務交付管理	A.15.2.1 供應者服務之監視及審查
		A.15.2.2 管理供應者服務之變更
A.16 資訊安全事故管理	A.16.1 資訊安全事故及改善之管理	A.16.1.1 責任及程序
		A.16.1.2 通報資訊安全事件
		A.16.1.3 通報資訊安全弱點
		A.16.1.4 資訊安全事件評估及決策
		A.16.1.5 對資訊安全事故之回應
		A.16.1.6 由資訊安全事故中學習
		A.16.1.7 證據之收集
A.17 業務永續運作管理之資訊安全層面	A.17.1 資訊安全持續	A.17.1.1 規劃資訊安全持續
		A.17.1.2 實作資訊安全持續
		A.17.1.3 查證、審查及評估資訊安全持續
	A.17.2 多重備援	A.17.2.1 資訊處理設施之可用性
A.18 遵循性	A.18.1 對法律及契約要求事項之遵循	A.18.1.1 適用之法規及契約的要求事項之鑑別
		A.18.1.2 智慧財產權
		A.18.1.3 紀錄之保護

		A.18.1.4 個人可識別資訊之隱私及保護
		A.18.1.5 密碼式控制措施的監管
	A.18.2 資訊安全審查	A.18.2.1 資訊安全之獨立審查
		A.18.2.2 安全政策及標準之遵循性
		A.18.2.3 技術遵循性審查

資料來源： 教育機構資安驗證中心，2016

第三節　教育體系資通安全暨個人資料管理規範

教育部於民國 96 年 5 月 30 日發佈「教育體系資通安全管理規範」，供教育體系機關(構)與各級學校據以建立其資通安全管理系統，綜合考量其重要性、急迫性及可分配資源…等因素，建立其資通安全管理規範的設計與施測，透過持續改善的管理機制運行，大幅強化其資通安全的有效性。

「教育體系資通安全管理規範」於 96 年實施至今已逾九年，期間資通安全環境快速變遷，資通訊科技進步快速，且網路普及應用也更為廣泛。另外，我國於民國 99 年將電腦個人資料保護法修改為個人資料保護法，擴大保護標的，不限於經電腦處理之個人資料，凡以任何形式存在之個人資料皆由該法適用之；其次，擴大適用範圍，舉凡涉及個人資料蒐集、處理、利用之個人、法人或團體皆適用該法；第三，新增個人資料蒐集、處理與利用之行為規範，如:告知義務之履行，並提高損害賠償額度且導入團體訴訟機制。此外，我國於民國 104 年修正個人資料保護法，因應實務運作之需求，完成第二次修法，修法內容包括:將病歷納入特種個人資料之範圍，新增當事人書面同意為特種個人資料之蒐集、處理與利用依據…等。有鑑於個人資料保護法對於教育體系造成相當程度之影響，且教育體系發生個人資料遭不當揭露或利用之情形時有見聞，是以維護資通安全之際，尤必要再考量個人資料安全之維護。

教育部自民國 104 年起著手「教育體系資通安全管理規範」之研修，當中考量資通訊環境之變化、我國個人資料保護法之修正與施行，以及最佳國際實務標準之發展與普及，如:ISO 27001:2013、ÍSO 27002:2013、ISO 29100:2011、BS 10012:2009…等，歷經數次之專家討論與諮詢教育體系意見，於民國 105 年完成修訂，並於同年 8 月 15 日發佈新版「教育體系資通安全暨個人資料管理規範」 (以下簡稱本規範)。

本規範結合 ISMS 與 PIMS，其一因應國際標準規範 2013 年之改版，新增資訊安全管理系統之相關控制措施建議，期能夠協助教育體系機關(構)與各級學校有能力因應資通訊科技應用所衍生之新興資通安全議題。同時因應個人資料保護法之修正與施行，新增個人資料管理系統(Personal Information Management System，以下簡稱 PIMS)之相關要求，期望以 PDCA 策略協助教育體系機關(構)與各級學校完善其個人資料安全維護之工作，達到個人資料保護之目的，降低個人資料遭不當揭露或利用之風險。

本規範期望對教育體系機關(構)與各級學校之資通安全或個人資料管理產生引導作用，協助其有效率地建置與運行資通安全與個人資料管理系統，發揮「事前預防、事後抑制」之效果，有效落實個人資料保護法令之施行，並達到維護資通安全之目的。是以建置本規範時，得衡酌組織規模、業務特性、所欲達成之資通安全維護或個人資料保護目的…等因素，選擇適當之實施範圍，配置適當之資源與人員，規劃適宜之管理系統，持續有效地運作該系統，並定期檢視與改善該系統。此外，本規範另有規定，選擇單獨建置 ISMS 之單位，無須執行關於 PIMS 之要求，反之亦然；選擇建立「資通安全暨個人資料管理系統」，應同時符合兩項管理系統之要求。

有鑑於教育體系機關(構)與各級學校之層級、組織規模、業務特性差異極大，為避免其因組織特性無法執行部分要求，本規範爰參考行政院國家資通安全會報訂定之「政府機關(構)資通安全責任等級分級作業規定」與教育部頒定之「教育部與所屬機關(構)及學校資通安全責任等級分級作業規定」，將適用機關(構)及學校分為 A、B、C 三級，並依等級建議不同適用範圍與適用對象(教育機構資安驗證中心，2016)，詳細說明如下:

- A 級:

◆ ISMS:應至少包含組織內所有資訊管理作業與流程，全部核心業務應用資訊系統與網路系統，以及受委託執行國家安全與機密資訊或技術研究單位，或試務管理單位。

◆ PIMS:應包含組織內全部所有涉及個人資料蒐集、處理與利用之流程。

◆ 適用對象

- 教育部本部、各國立大學醫學院附設醫院。
- 承接具國家安全機密性或敏感性業務或技術研究之學院或系所，其研究領域涉及國家安全資訊、國家機密資訊、國家安全技術、國家機密技術領域等。
- 辦理大學、技專校院及高級中等學校等入學考試、甄選、招生等工作之常設試務機構。

- B 級:

◆ ISMS:應至少包含資訊管理單位、學術網路系統、核心業務資訊系統。

◆ PIMS:應至少包含涉及核心業務之個人資料蒐集、處理與利用流程之行政單位，及資訊管理單位。

◆ 適用對象

- 以教育部所屬機關(構)、專科學校與十二年國教入學試務機構/學校、各大學、臺灣學術網路各區域網路中心與各直轄市、縣(市)教育網路中心等為主。

➢ C 級:

◆ ISMS:應至少包含資訊管理單位校務行政資訊系統。

◆ PIMS:應至少包含組織內涉及個人資料處理蒐集、處理與利用流程之行政單位，及資訊管理單位。

◆ 適用對象

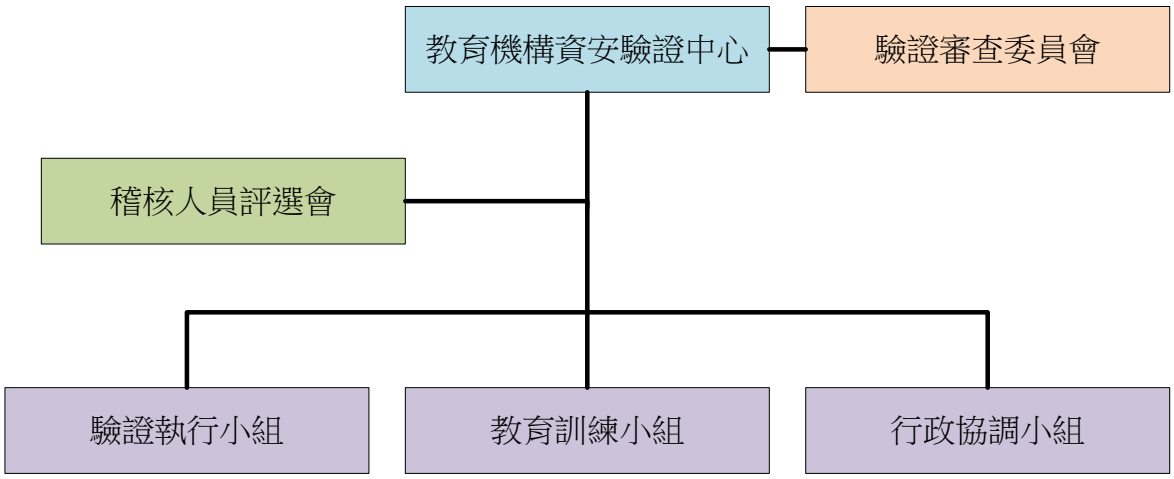
- 第一類：各公私立專科學校、各公私立學院。
- 第二類：各公私立高級中等學校。

【備註】欲建立「資通安全暨個人資料管理系統」之機關(構)與學校，得分別定義兩項管理系統之適用範圍，惟 PIMS 適用範圍所涉及之資通安全管理議題，應完整包含於 ISMS 適用範圍內。

第四節　教育機構資訊安全驗證轉版流程

「教育機構資安驗證中心」於民國 98 年 1 月成立，為教育部授權之資安驗證單位,負責執行並落實教育機構資訊安全管理作業的驗證制度，並配合教育部資安管理與驗證策略規劃，確保教育體系各單位、學校落實資訊安全管理系統的有效性。該中心目前辦理之業務包含有「教育機構資安稽核驗證及追查作業」、「教育機構資安稽核換證作業」、「教育機構資安驗證稽核團隊遴選、培訓、管理業務」、「教育機構資安驗證相關課程辦理」、「教育機構資安驗證研討會辦理」…等，且轄下包含驗證執行小組、教育訓練小組、以及行政協調小組，並設立驗證審查委員會。

如圖 2.4: 教育機構資安驗證中心組織架構圖。



▲圖 2.4: 教育機構資安驗證中心組織架構圖
資料來源 : 教育機構資安驗證中心，2016

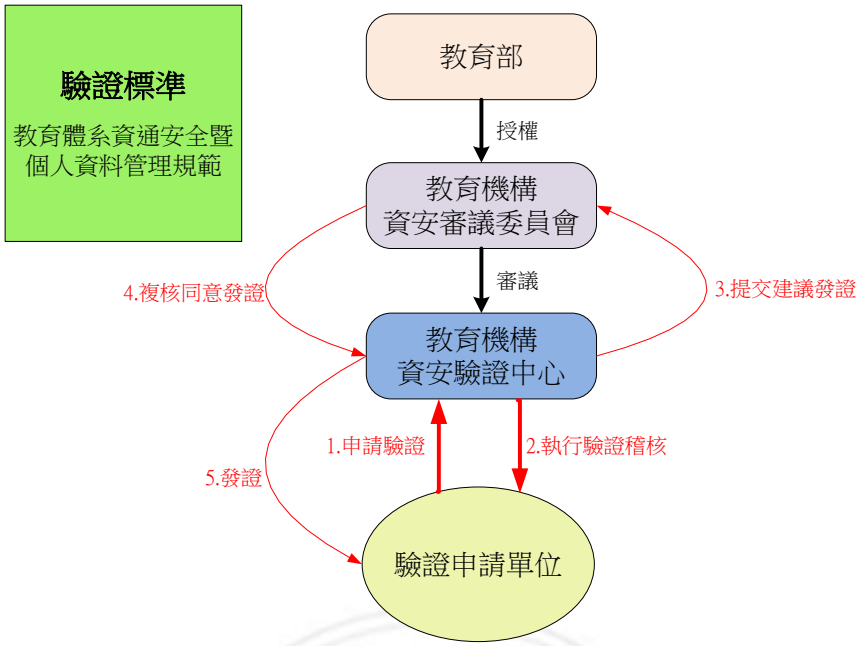
教育體系單位或學校向教育機構資安驗證中心(簡稱:驗證中心)提出驗證申請後，驗證中心將於收到申請案件後 5 個工作天內就申請表內容完整性加以審查，審查結果符合規定之案件即受理申請，並通知單位繳交驗證費;驗證中心將依申請單位所在地，遴派稽核員組成稽核小組，並指派其中 1 名擔任主導稽核員，負責小組的管理工作，稽核小組所有成員(包含稽核觀察員)須簽署「個案利益迴避與保密聲明書」，方能執行驗證稽核作業；稽核小組依申請單位之驗證範圍複雜度進行發證稽核、追查稽核及重新驗證稽核作業時間安排,如有五項驗證範圍複雜度要件，其中四項(含)以上達到判斷值表示複雜度高，複雜度不同安排的稽核人天數也有所不同，如表 2.4: 驗證範圍複雜度判斷要件表。發證稽核作業分二階段，第一階段為文件審查，以不到現場稽核為原則、第二階段為現場稽核，於申請單位所提出的資訊安全管理系統驗證範圍所在地進行稽核;稽核小組評估建議發證的主要依據為，稽核過程中發現其與「教育體系資通安全管理規範」要求無不符合事項，或有少數次要不符合事項且

無主要不符合事項，即可建議發證或有條件的建議發證。如圖 2.5: 教育機構資安驗證架構。

表 2.4: 驗證範圍複雜度判斷要件表

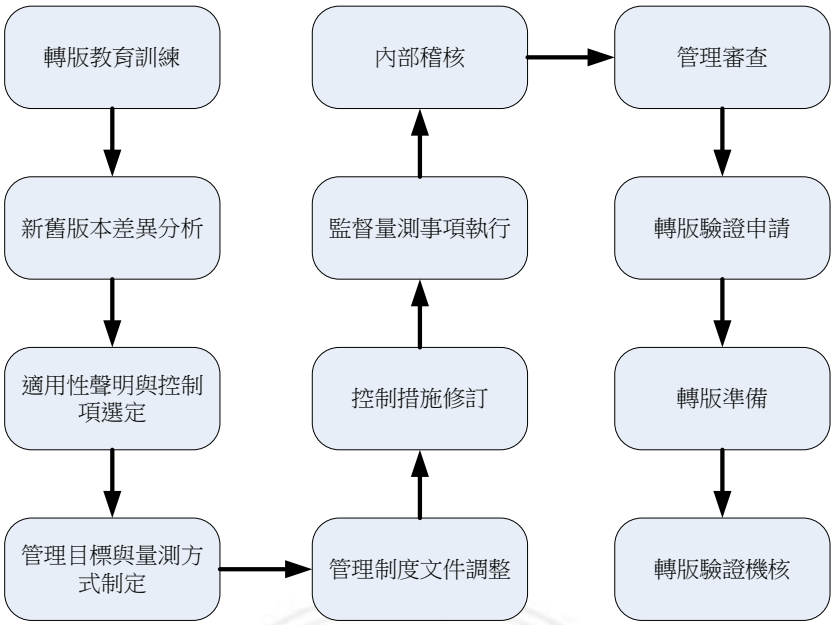
驗證範圍複雜度要件	**判斷值**
1.驗證範圍內人數	≧8 人
2.驗證範圍主要場區數目	2 區
3.驗證範圍內伺服器數目	≧10 台
4.驗證範圍內個人電腦數目(含工作站、筆記型電腦)	≧10 台
5.應用系統使用者	驗證範圍有包含資訊服務/應用系統使用者端維運作業
[**備註**] 四項(含)以上達到各項要件之判斷值，則發證稽核及重新驗證稽核以 4 人天為稽核人天數、追查稽核為 2 人天；若非上述狀況，則發證稽核及重新驗證稽核將安排 2 人天稽核人天數、追查稽核為 1 人天。	

資料來源：教育機構資安驗證中心，2016



▲圖 2.5: 教育機構資安驗證架構
資料來源 : 教育機構資安驗證中心，2016

教育機構轉版驗證稽核是指機構原已通過資安驗證，即以 96 年版「教育體系資通安全管理規範」為基礎的資通安全驗證稽核，後續為達到 105 年 8 月 15 日發佈的新版「教育體系資通安全暨個人資料管理規範」為基礎的資通安全驗證稽核，所進行的轉版教育訓練、分析新舊版差異、適用性聲明與控制項選定、管理目標與量測方式制定...等動作，詳細的執行步驟如圖 2.6: 教育機構轉版執行步驟。



▲圖 2.6: 教育機構轉版執行步驟
資料來源 : 教育機構資安驗證中心，2016

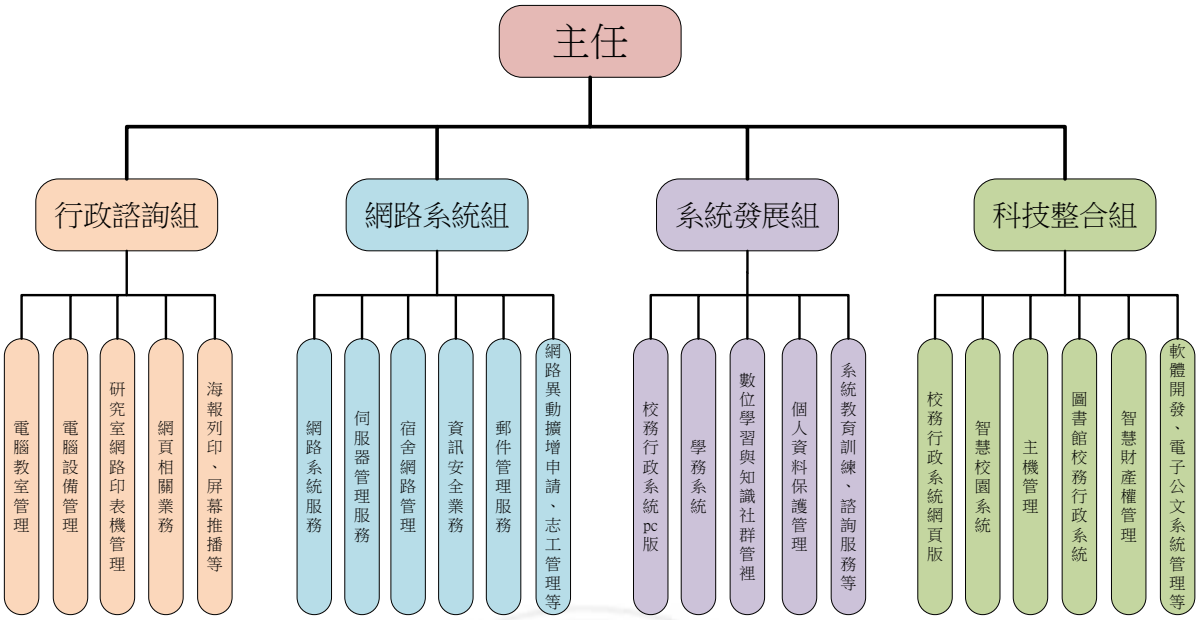
第三章 研究方法

第一節 研究方法

本研究旨在基於 ISO 27001 轉版建置 ISMS 程序探討，瞭解組織願意進行轉版的動機、轉版建置新規範可能面的困難、導入新資通安全規範驗證的成功因素及效益，故採用「質性研究法(Qualitative Research)」，以敘述、瞭解及闡述...等方式，整合與建立本研究所有知識，並依據本研究的研究動機、研究目的，參考相關的標準、較具代表性的期刊論文、書籍、技術報告與新聞報導…等的做法，去觀察、探索找出有意義的關聯和影響，以確保本研究的論述資料的可信度。

第二節 研究對象

本研究以南部某私立大學實施教育體系資通安全管理規範之資訊中心作為研究範圍，該單位組織成員包含主任、行政諮詢組、網路系統組、系統發展組、科技整合組。主任負責中心管理與規劃；「行政諮詢組」負責電腦教室管理、電腦設備維護、研究室網路印表機管理、網頁相關業務、協助電腦報廢審查、海報列印及 LED 屏幕推播...等業務；「網路系統組」負責網路系統服務、伺服器管理服務、宿舍網路管理、資訊安全業務、郵件管理服務、校內有線與無線網路異動擴增申請及服務教育志工管理...等業務；「系統發展組」負責校務行政系統 PC 版、學務系統、數位學習與知識社群管理、個人資料保護管理、系統教育訓練及諮詢服務...等業務；「科技整合組」負責校務行政系統 Web 版、智慧校園系統、主機管理、圖書館校務行政系統、智慧財產權管理、軟體開發及電子公文系統管理...等業務，如圖 3.1: 資訊中心組織架構圖。



▲圖 3.1: 資訊中心組織架構圖
資料來源 : 研究個案單位網頁，本研究整理

研究個案的資安政策聲明書中指出，其導入資訊安全管理制度的目標為:

壹、「落實資安管理，確保持續營運」:

由全體同仁貫徹資訊安全管理制度，落實 PDCA 的執行，持續進行監控、審查及稽核各式資訊系統，確保其機密性、完整性及可用性。保護資訊資產免於因外在之威脅或內部人員不當的管理，遭受洩密、破壞或遺失…等風險，並以『風險管理』為中心，瞭解資產威脅與弱點，選擇適切的保護措施，將風險降至可接受程度，建構安全網路環境，達持續營運之目標。

貳、「加強資安訓練，提升服務品質」:

每年持續進行適當的資訊安全訓練，建立「資訊安全，人人有責」的觀念，提高同仁資訊安全意識與智能，加強應變能力，以提升服務品質。

參、 「做好緊急應變，迅速災害復原」：

訂定重要資訊資產及關鍵性業務之緊急應變計畫及災害復原計畫，並定期執行各項緊急應變流程的演練，以確保資訊系統失效或重大災害事件發生時能迅速復原，確保關鍵性業務持續運作，並將損失降至最低。

第三節 資料蒐集及分析

Yin, R.K 曾指出大多數較好的個案研究倚賴廣泛的不同來源，採用多重證據來源可以具有高度的互補性，也就是使用三角檢定法(Triangulation)。三角檢定法又稱多元檢證法，藉由多方的資料來源來研究同一個現象，來提升質性研究結果的可信性(高淑清，2008)。

依 Yin, R.K 所寫的「個案研究法」書中所述個案研究的證據可能有六種來源:文件、檔案紀錄、訪談、直接觀察、參與觀察、以及實體的人造物(Yin, R. K.著、尚榮安譯，2010)。以下針對此六種個案研究可能的證據來源之優點與缺點進行整理比較，如表 3.1: 六種證據來源:其優點與缺點。

表 3.1 六種證據來源:其優點與缺點

證據來源	優點	缺點
文件 (Documents)	◆ 穩定-可以重複地檢視 ◆ 非涉入式-並不是個案研究所創造的結果 ◆ 確切的-包含確切的名稱、參考資料及事件的細節 ◆ 範圍廣泛-長時間、許多事件，和許多的設置	◆ 可檢索性-可能低 ◆ 如果收集不完整，會產生有偏見的選擇 ◆ 報告的偏見-反應出作者的(未知的)偏見 ◆ 使用的權利-可能受到有意的限制
檔案紀錄 (Archival records)	◆ 同以上文件部分所述	◆ 同以上文件部分所述

	◆ 精確的和量化的	◆ 由於個人隱私權的原因而不易接觸
訪談 (Interviews)	◆ 有目標的-直接集中於個案研究的主題 ◆ 見解深刻-提供了對因果推論的解釋	◆ 因問題建構不佳而造成的偏見 ◆ 回應的偏見 ◆ 因無法回憶而產生的不正確性 ◆ 反射現象-受訪者提供的是訪談者想要的答案
直接觀察 (Direc observation)	◆ 真實-包含即時的事件 ◆ 包含情境的-包含事件發生的情境	◆ 消耗時間 ◆ 篩選過的-除非涵蓋的範圍很廣 ◆ 反射現象-因為事件在被觀察中，可能會造成不同的發展 ◆ 成本-觀察者所需花的時間
參與觀察 (Participant-observation)	◆ 同以上直接觀察部分所述 ◆ 對於人際間的行為和動機能有深刻的認識	◆ 同以上直接觀察部分所述 ◆ 由於調查者操弄事件所造成的偏見
實體的人造物 (Physical artifact)	◆ 對於文化特徵能有深刻的理解 ◆ 對於技術的操作能有深刻的理解	◆ 篩選過的 ◆ 可取得性

資要來源：Yin, R. K.著、尚榮安譯，2010

依據上述六種證據來源所述，本研究之個案研究是採用了:文件、直接觀察及實體的人造物三項，期望以多元化的資料來源來提升本研究的信度，而資訊安全管理系統適用於各種機關(構)組織，因此本研究的發現亦可推論到具有相同管理特性與運作模式的各學校或單位組織，藉此說明了本研究的效度。以下就本研究的證據資料來源相關內容，說明如下:

壹、 文件蒐集:包含個案學校 ISMS 相關的手冊、程序書、標準書及表單資料、官方網站、會議議程和紀錄報告，以及各管理規範與作業規定...等。

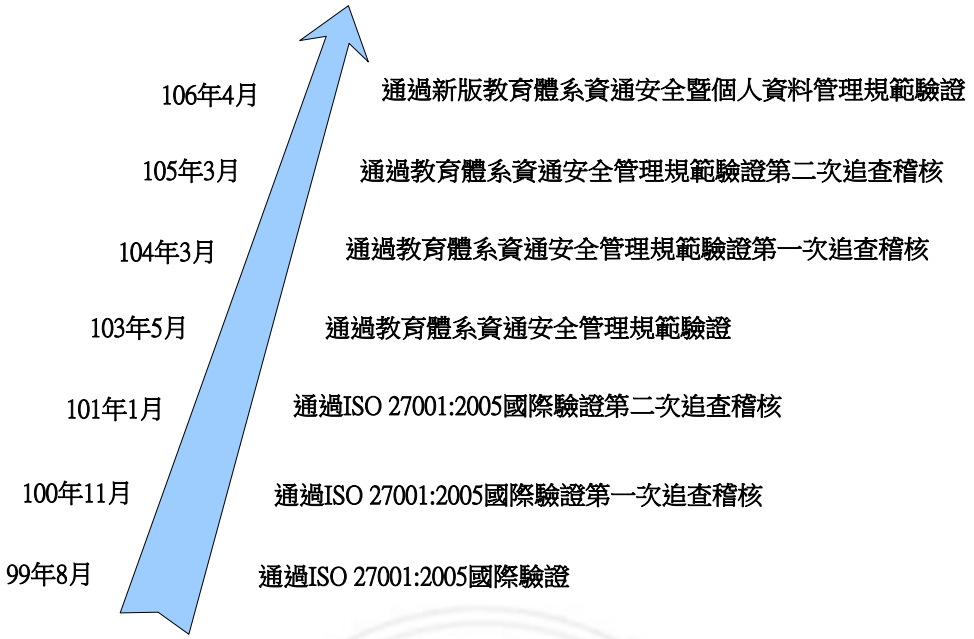
貳、 直接觀察:實際觀察 ISMS 轉版、驗證稽核執行狀況以及如何成功取得教育體系資通安全管理規範驗證證書。

參、 實體的人造物:對個案 ISMS 轉版工作實際參與其中,執行新版 ISMS 制定、審查會議、申請驗證及外部稽核...等。

第四章 研究過程與結果分析

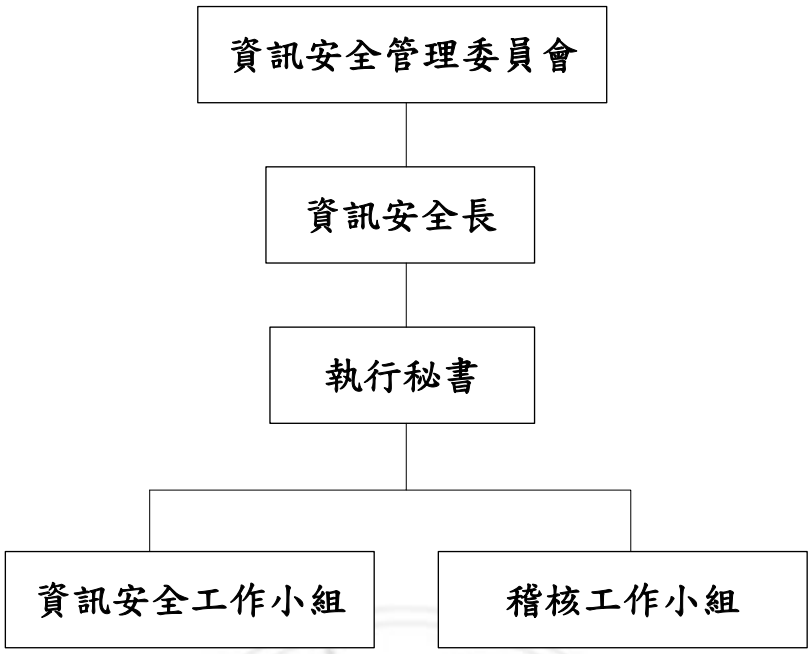
第一節 個案研究背景

個案資訊安全管理系統自民國 99 年導入，於民國 99 年 8 月通過 ISO 27001:2005 國際驗證；於民國 100 年 11 月通過 ISO 27001:2005 國際驗證第一次追查稽核；於民國 101 年 1 月通過 ISO 27001:2005 國際驗證第二次追查稽核。民國 102 年 2 月該單位新主管上任，考量「教育體系資通安全管理規範」是教育部所頒佈的規範，適用於教育體系機關(構)與各級學校，因此將校內運行的資訊安全管理系統改版為教育體系資通安全管理規範，於民國 103 年 5 月通過教育體系資通安全管理規範驗證；於民國 104 年 3 月通過教育體系資通安全管理規範驗證第一次追查稽核；於民國 105 年 3 月通過教育體系資通安全管理規範驗證第二次追查稽核。教育部於民國 105 年 8 月 15 日發佈新版「教育體系資通安全暨個人資料管理規範」，個案為符合教育部新規範之要求，自民國 105 年 6 月起著手進行教育體系資通安全管理規範改版動作，於民國 106 年 4 月通過新版教育體系資通安全暨個人資料管理規範驗證。如圖 4.1: 個案資安驗證演進史。



▲圖 4.1: 個案資安驗證演進史
資料來源 : 研究個案，本研究整理

個案研究的資安驗證範圍為「資訊中心辦公區域環境、資訊機房及校務行政系統運作及維護之安全管理」，其「資訊安全管理委員會」組織架構，是依據該校資訊安全暨個人資料保護推行委員會設置辦法所建立，明確規範資訊安全管理作業人員之權限與責任，協調事務及推動資訊安全管理相關事宜，確保資訊安全各項管理規範能有效持續地執行，並達成資訊安全之政策與目標，如圖 4.2: 資訊安全組織架構圖。



▲圖 4.2: 資訊安全組織架構圖
資料來源 : 研究個案網頁，2016

「資訊安全管理委員會」組織架構最上層為「資訊安全長」，由校長指派學術副校長擔任，下層設有「執行秘書」，由資訊中心主任擔任，最下層設有「資訊安全工作小組」及「稽核工作小組」。「資訊安全工作小組」及「稽核工作小組」的小組成員由執行秘書召集業務相關人員若干名組成，資訊安全組織架構中成員及小組的權責分別說明如下:

壹、「資訊安全長」:

負責決議資訊安全管理制度相關事項、定期主持資安各項會議、協調資安管理制度所需相關資源分配及跨部門資安工作協調與運作。

貳、「執行秘書」:

代理資訊安全長召集資安管理委員會成員，參加各項資安會議及監督、執行資安管理制度各項工作、協調資安工作小組執行資安作業、對資安管理提出改善建議、協助執行資安自我檢核及對資安狀況進行預警、監控，並對資安狀況與事件進行處置。

參、「資訊安全工作小組」:

執行資安例行業務及處理緊急資安事件、制定資安政策、資安目標與各項標準作業程序、界定與檢討資安管理系統之範圍與控制措施、各項資安管理文件與記錄之建立和管制、制定風險管理制度與執行風險管理作業、建立資安事件緊急應變暨復原措施、持續不斷評估與檢討風險管理之具體措施、監督、紀錄和調查資安事件、執行稽核缺失之矯正及預防措施改善建議，並追蹤缺失事項執行情形、執行「資訊安全管理委員會」所決議之事項。

肆、「稽核工作小組」:

制定資安內部稽核作業管理程序、訂定相關稽核計畫、內部稽核及協助進行外部稽核作業、檢核資安業務是否落實、撰寫稽核報告、複查追蹤稽核發現不符合事項矯正措施、評估與檢討資安內部稽核成效。

第二節 ISMS 轉版歷程

壹、研究個案參與聯合輔導轉版簡介

新版「教育體系資通安全暨個人資料管理規範」發佈前，教育機構資安驗證中心於民國 105 年 6 月發函各公私立大專校院、學術網路區網中心及教育部所屬機關...等單位，提出「教育體系資通安全暨個人資料管理制度聯合輔導」案，徵求有意願之學校/單位提出申請，最後全省選出可參與「輔導教育機構資通安全管理制度轉版」案共 35 個單位、可參與「輔導教育機構實施個人資料管理制度」案共 28 個單位，其中有 17 個單位同時獲選參與資通安全管理制度輔導案與個人資料管理制度輔導案，而本研究個案為 17 個獲選兩項的單位之一。

教育機構資通安全管理制度轉版輔導，課程內容包含資安規範轉版實務課程三天、資安內部稽核課程一天，當全部課程訓練結束後，接受輔導之學校/單位須填寫資通安全自評表，回覆給驗證中心以供進行第二次資格審查用，截錄自評表內容如表 4.1: 教育機構資安驗證中心教育體系資通安全暨個人資料管理規範實施自評表(資通安全)。驗證中心統整聯合輔導案之各學校/單位所填寫的自評表內容，再次進行審查稽核工作，如該學校/單位審查稽核通過，將可獲得驗證中心免費的教育體系資通安全驗證稽核，但研究個案之資通安全自評表未獲選，因而改以請購招標方式招聘外部專業輔導顧問公司投標，各專業輔導顧問公司之投標文件再經由校內採購單位辦理開標及評審會議後，選出最適合學校之最佳顧問公司協助進行轉版驗證工作。

表 4.1: 教育機構資安驗證中心

教育體系資通安全暨個人資料管理規範實施自評表

(資通安全)

條款章節	條文		自評結果			相關參考文件 / 說明
			符合	不符合	不適用	
柒、	建置步驟及需求					
一、	組織全景					
	(一)施行機關(構)或學校應依據相關法令要求、行政院及教育主管機關所下達之重要決定或指導(包括但不限於主管機關之行政指導、重要會議決議事項等)、組織透過相關會議所做成之決議(包括但不限於主管會報、行政會議或校務會議等之決議)，針對資通安全或個人資料安全之維護需求進行評估，並據此建立或調整資通安全與個人資料管理範圍與目標。		□	□	□	
A5	資訊安全政策					
A.5.1	資訊安全之管理指導方針					
A.5.1.1 (I/P)	資訊安全政策	資訊安全政策應由管理階層定義並核准，且對給所有員工及相關外部各方公布及傳達。	□	□	□	
A.5.1.2 (I/P)	資訊安全政策之審查	資訊安全政策應依規劃之期間或發生重大變更時審查，以確保其持續的合宜性、適切性及有效性。	□	□	□	

資料來源：教育機構資安驗證中心，2016

貳、顧問團隊介紹

該顧問公司輔導資安實績，包含教育單位、政府單位及醫療體系...等多達 50 家以上，是家擁有相當豐富的資安輔導經驗的公司。為執行研究個案的「資安暨個資保護規範和驗證委外服務專案」，該公司特別成立專案輔導團隊共七人小組，以協助研究個案之新版 ISMS 訂定與驗證服務工作。專案輔導成員的職責分工說明，如下表 4.2: 專案角色與工作職掌表。

表 4.2: 專案角色與工作職掌表

No	角色/職掌	工作執掌
1	計畫主持人	1.負責計畫成敗權責並擔任專案計畫協商之負責人。 2.建置及服務工作品質之管控。 3.建置進度及服務工作進度之查核。 4.執行流程之指導、諮詢與協調。 5.負責策定本專案之目標、與學校溝通、專案人力與資源之規劃、督導及管制。
2	專案經理	1.負責本專案之各項工作管理與進度控管、品質管制。 2.一般性事務及行政聯繫事宜。 3.成立專案小組，協助每項工作順暢進行。 4.與貴校保持最佳報告機制，隨時掌控專案的即時狀況。
3	品質管理小組	1.負責本專案之服務品質、工作進度以及行政作業流程文書等之管　理與監督。 2.資訊安全諮詢服務與客戶服務窗口。 3.服務流程追蹤與品質控管。 4.服務績效及滿意度調查與檢討。 5.控管本專案相關行政作業流程與文書作業。
4	輔導顧問小組	1.依據「教育體系資通安全暨個人資料管理規範」修訂 ISMS 及落實資訊安全管理相關作業。 2.依據「教育體系資通安全暨個人資料管理規範」修訂 ISMS 及落實個資保護管理相關作業。 3.辦理資安與個資保護教育訓練，提昇員工資安及個資保護觀念與能力。 4.協助修訂 ISMS 及 PIMS 並分別通過「教育體系資通安全暨個人資料管理規範」稽核驗證。
5	個人資料管理法律顧問	1.協助進行 ISMS & PIMS 內部稽核作業。 2.提供個資法法律諮詢服務。 3.辦理個資教育訓練，提昇員工資安與個資保護管理觀念與應變處理能力。

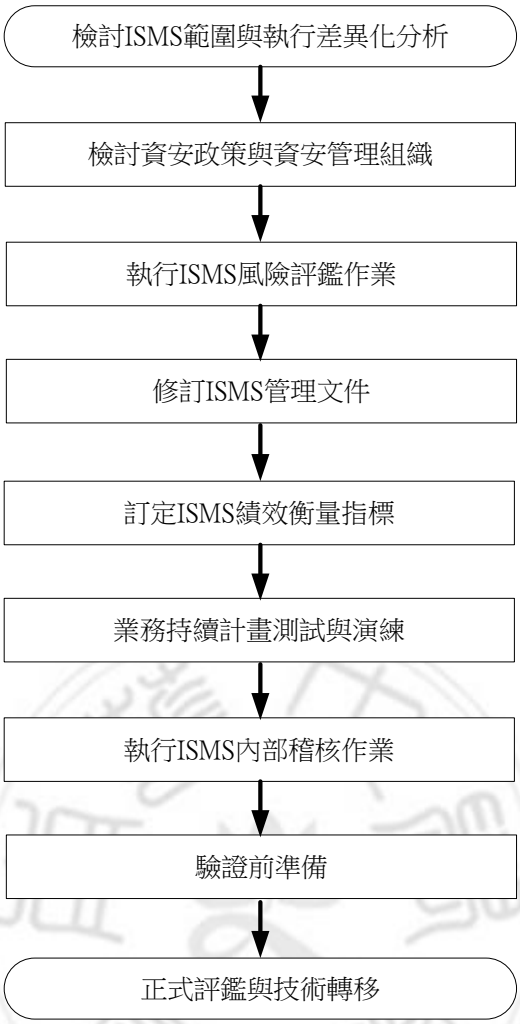
6	行政支援小組	1.提供及支援本專案所需各項文書工作。 2.ISMS & PIMS 各項紀錄之彙總、ISMS & PIMS 四階文件流程圖之繪製。 3. ISMS & PIMS 四階文件之繕打、校稿與格式調整。

資料來源：研究個案之專案工作計畫書，2016

參、資通安全管理規範轉版及驗證歷程

研究個案以現有資通安全管理規範為基底，加入「教育體系資通安全暨個人資料管理規範」之新版要素來進行轉版工作，並以通過「教育機構資安驗證中心」的資通安全管理規範驗證為目標，期望讓資通安全管理規範更切合單位組織需求，進而提升全校資安意識與智能，增強災害應變及復原能力，確保資訊持續營運並提升服務品質。

因此，研究個案的 ISMS 轉版歷程，以教育機構資安驗證中心建議之轉版執行步驟為原則，與顧問公司就學校現行資訊安全管理制度、組織架構現況、關注方要求...等議題進行討論協商後，設計出以下的轉版驗證流程，如圖 4.3: ISMS 驗證流程與步驟。



▲圖 4.3: ISMS驗證流程與步驟
資料來源 : 研究個案ISMS專案工作計畫書，2016

以研究個案之 ISMS 驗證流程與步驟中，各項步驟的執行方法與工作內容，摘要說明如下:

一、檢討 ISMS 範圍與執行差異化分析

輔導顧問至驗證單位進行訪談及診斷，透過討論瞭解學校營運目標是否會影響 ISMS 執行成果之內外部議題與挑戰，鑑別與學校營運相關之利害關係人以及這些利害關係人的資安要求與期許，來判斷學校 ISMS 範圍是否需要修正及調整，並根據校內現行資訊安全管理制度之現況與「教育體系資通安全暨個人資料管理規範」標準及學校需遵循之法令法規進行差異性分析

與評估，發覺出需改善及調整之處，以作為補強控制措施之依據，並制訂現行資訊安全管理制度之修訂方針。

經由評估後，針對附錄 A 的控制項目刪除以下六項，內容說明如下:

(一)、 A.10.1.2 金鑰管理:因資料交換中未使用金鑰之需求。

(二)、 A.11.1.6 交付及裝卸區:本校無設置裝卸區。

(三)、 A.11.2.6 場所外設備及資產的安全:本校無駐外設備。

(四)、 A.11.2.8 無人看管之使用者設備:本校沒有無人看管的資訊設備。

(五)、 A.14.1.3 保護應用服務交易:本校無應用系統服務交易之業務。

(六)、 A.18.1.5 密碼式控制措施(加密控制措施的監管):本校目前所提供之資訊系統服務，未啟用加密控制措施。

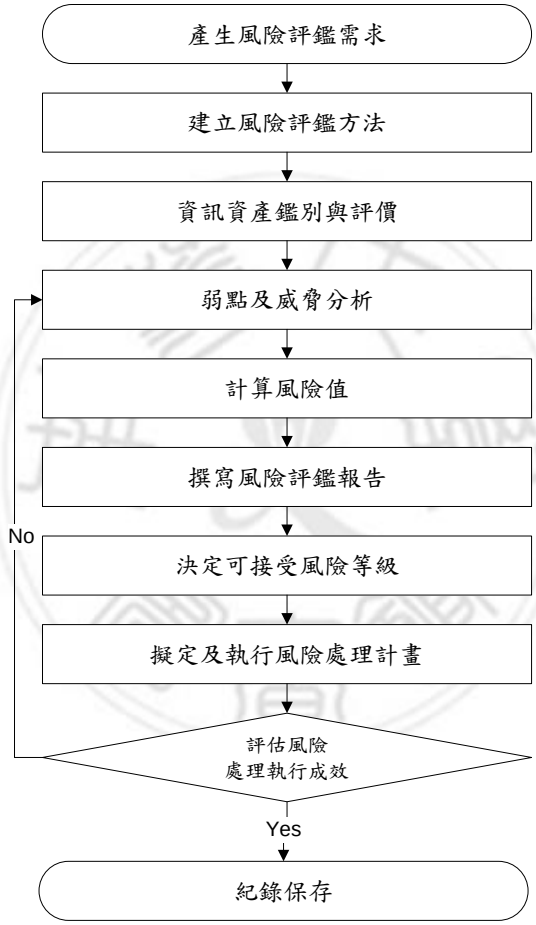
二、檢討資安政策與資安管理組織

(一)、檢討及修正現行之資訊安全政策，將組織全景之鑑別依新規範要求加註說明，以確保資訊資產之機密性、完整性及可用性，並符合相關法令法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，以保障內部同仁之權益。

(二)、檢視現有資訊安全組織於資訊安全事件處理、資訊安全跨部門推動及專責組織之工作流程…等運作之現況，提出相關改善意見及調整現行之資通安全組織架構，使資訊安全組織能有效運作並確保資訊安全管理制度能有效持續執行，達成既定的資訊安全政策與目標。

三、執行 ISMS 風險評鑑作業

(一)、辦理 ISMS 相關資產之年度風險審查作業,協助釐清資訊資產鑑價條件之建議,並協助進行資訊資產鑑別與評價後之複審作業,及相關資產年度風險評鑑後之複審,以產出「風險評鑑報告」及「風險處理計畫表 」文件,如圖 4.4: 資訊安全風險管理流程圖。



▲圖 4.4: 資訊安全風險管理流程圖
資料來源 : 研究個案ISMS程序書，本研究整理

(二)、 資訊資產鑑別與評價工作,首先須建立 ISMS 範圍內的資訊資產，並評估資產價值，還須定期進行盤點動作，當資訊資產發生新增、異動、報廢時，修正資訊資產清單

內容，以供風險評鑑使用。資訊資產依照性質不同，可分為六大類，如表 4.3: 資訊資產分類表；依資訊資產之特性，分為人員與非人員兩大類，對其所對應之機密性(C)、完整性(I)及可用性(A)進行評估量化，再將三者相加即為資訊資產價值(P)，如表 4.4: 資訊資產價值評估標準表。研究個案「資訊資產清冊」截錄內容如圖 4.5: 資訊資產清冊。

表 4.3: 資訊資產分類表

大分類	小分類	範例
人員類	管理者	教職員工、約聘人員、學生、研發人員、管理人員、維護人員、MIS 人員、臨時工作人員、訪客、委外維護人員、委外保全人員、包商或供應商。
	使用者	
	委外廠商	
文件類	作業文件	資料庫與資料檔案、備份資料、網路架構圖、系統文件、使用者手冊、教育訓練教材、ISMS 管理文件、緊急應變計畫、營運持續計畫、稽核日誌、合約與協議、報表、表單記錄...等。
	系統文件	
	合約	
	電子資料紀錄	
	系統紀錄(Log)	
服務類	內部服務	網路服務(Internet)、電話諮詢服務、委外維護服務、一般網路連線設施服務、一般電腦資訊服務。
	外部服務	
硬體類	個人電腦	包含電腦設備(伺服器、筆記型電腦、個人電腦、工作站)、CD/DVD 燒錄器、CD/DVD 光碟機、磁帶機、軟碟機、投影機、PDA(個人數位助理)、印表機、集線器、橋接器、網路交換器、路由器、網路纜線、防火牆、入侵偵測系統、視訊會議設備、傳真機、手機、硬碟(無資料)、磁片(空白)、磁帶(空白)、移動式硬碟(空白)、錄音/影帶(無資料)、絕緣安全電纜、不斷電系統、穩壓器、機櫃.....
	可攜式電腦	
	伺服器	
	資安設備	
	網路設備	
	可攜式儲存媒體	
	電腦保護設施	
	其他硬體	
軟體類	作業系統	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.....
	應用系統	
	套裝軟體	
	軟體開發工具	
	資訊安全系統	
建築與保護類	一般辦公區域	機房、異地備援地點、電腦教室、會議室、監控室、交貨區/裝載區、監視攝影、門禁刷卡、第二電力供應迴路、避雷裝置、UPS、警報系統、備用發電系統、環境控制系統(火偵測、熱偵測、水偵
	特殊辦公區域	
	資訊機房	
	倉庫/庫房	

大分類	小分類	範例
	建築保護設施	測、溫濕度偵測、自動消防滅火系統)、.....

資料來源：研究個案 ISMS 程序書，本研究整理。

表 4.4: 資訊資產價值評估標準表

人員類資產			
機密性評估 (C)	等　級	量化值	內 容 說 明
	高	3	其工作執掌可存取限定資料（含機密、密及普通等三類）。
	中	2	其工作執掌可存取密類資料及普通類資料。
	低	1	其工作執掌僅可存取普通類資料。
完整性評估 (I)	高	3	▪ 未正確執行業務而造成資料不完整，會對業務造成很大的衝擊，甚至造成業務中斷失敗。 ▪ 可能影響全組織對外所提供的服務作業。
	中	2	▪ 未正確執行業務而造成資料不完整，可能對業務運作不造成中斷，但降低運作效率及影響。 ▪ 可能影響單一部門運作。
	低	1	▪ 未正確執行業務而造成資料不完整，可能對業務運作不會造成中斷或雖降低效率但不會造成影響。 ▪ 僅僅影響少數承辦人的作業。
可用性評估 (A)	高	3	▪ 欲維持業務正常運作，在該等人員無法持續提供服務時，可容忍替換時間為 4 小時。 ▪ 業務高度仰賴該員，且一旦該員無法作業時，將影響本校對外所提供的服務作業。
	中	2	▪ 欲維持業務正常運作，在該等人員無法持續提供服務時，可容忍替換時間為 12 小時以內。 ▪ 業務仰賴該員，且一旦該員無法作業時，將影響本校多數部門作業。
	低	1	▪ 欲維持業務正常運作，在該等人員無法持續提供服務時，可容忍替換時間為 24 小時以上。 ▪ 業務仰賴該員，且一旦該員無法作業時只影響少數承辦人員作業，其工作可暫時委由他人替代。
非人員類資產			
機密性評估 (C)	高	3	▪ 機密性資訊處理設施與系統資源，僅開放給必要知道的人使用。 ▪ 資料內容若洩漏會影響本校聲譽及師生權益。

	中	2	▪ 密等級資訊處理設施與系統資源僅開放給內部人員使用。 ▪ 資料內容若洩漏會對本校造成有形或無形的損害，此損害為組織可承受之範圍（註一）。
	低	1	▪ 不限制使用資訊處理設施與系統資源等。 ▪ 資料內容若流傳至組織以外，不會對本校造成任何有形或無形的傷害（註一）。
完整性評估 (I)	高	3	▪ 不當的損失、破壞資訊處理設施與系統資源，會對業務應用造成顯著的衝擊。 ▪ 資訊系統服務若不完整，將導致本校作業受影響。
	中	2	▪ 不當的損失、破壞資訊處理設施與系統資源，會對業務應用造成輕微的衝擊。 ▪ 資訊系統服務若不完整，將造成單一部門作業受影響。
	低	1	▪ 不當的破壞或竄改資訊、資訊處理設施與系統資源，所造成的業務衝擊可以忽略者。 ▪ 資訊系統服務若不完整，將造成少數或個別承辦人作業受影響。
可用性評估 (A)	高	3	▪ 僅容許短暫時間（4 小時內）無法使用，作業停頓期間極易產生客訴事件，使本校受到損害者。 ▪ 作業完全仰賴資訊資產，且一旦服務中斷時將影響全組織對外所提供的服務作業。
	中	2	▪ 容許較長時間（8 小時內）無法使用，會造成部份人員之抱怨，使本校受到輕微損害者。 ▪ 作業仰賴資訊資產，且一旦服務中斷時將影響部門運作。
	低	1	▪ 容許長時間（1 天以上）無法使用，作業停頓期間可利用其他替代方案，不致造成本校之損失。 ▪ 作業仰賴資訊資產，且一旦服務中斷時將影響少數承辦人作業。
註一: 有形的傷害如：財務上的賠償、主管機關的懲處 無形的傷害如：形象上的受損、組織內部員工士氣的低落			

資料來源：研究個案 ISMS 程序書，本研究整理。

資 訊 資 產 清 冊

紀錄編號：資訊-程序-03-01-____-____

NO.	登錄日期	資產群組名稱	資產名稱	數量	資產類別		基本資料				資產價值			
					大類	小類	風險擁有者(部門)	使用者(部門)	存放位置	資產說明/備註	機密性	完整性	可用性	總計

▲ 圖 4.5: 資訊資產清冊

資料來源 ：研究個案 ISMS 程序書，本研究整理。

(三)、 風險值計算需使用資訊資產價值(P)，再依據風險評鑑作業程序識別弱點之脆弱度(V)、威脅之發生機率（T）以及衝擊影響程度（IM），將此四項評分進行相乘，求出該資訊資產之單項風險值，進而求出該資訊資產所有弱點與威脅之總風險值，公式為資訊資產總風險值 $=\Sigma\{P \times V \times T \times IM\}$。研究個案「風險評鑑工作表」截錄內容如圖 4.6: 風險評鑑工作表。

風險評鑑工作表

紀錄編號：資訊-程序-04-01-___-___

資產辨識與分類				風險評鑑											
資產群組名稱	資訊資產名稱	資產類別		資產價值評估				弱點評估		威脅評估		衝擊分析	風險評估	
		大類	小類	機密性 (C)	完整性 (I)	可用性 (A)	合計	弱點名稱	脆弱度 (V)	威脅名稱	威脅發生機率 (T)	衝擊程度 (IM)	風險值小計	風險總值

▲ 圖 4.6: 風險評鑑工作表

資料來源 ：研究個案 ISMS 程序書，本研究整理。

(四)、「風險評鑑報告」結果參閱「資訊資產清冊」及「風險評鑑工作表」，將風險評鑑工作表之評鑑結果給資訊管理委員會審查。研究個案 106 年度共 335 項資訊資產之風險值均在 100 以下，有 3 項超於 100(含)以上。資訊安全工作小組針對風險值超過 100(含)以上需降低風險等級之資訊資產擬訂風險處理計畫，以期將風險降至可接受之程度，研究個案「風險處理計畫表」截錄內容如圖 4.7: 風險處理計畫表。

風險處理計畫表　紀錄編號：資訊-程序-04-03-___-___

資產識別暨風險說明								處理措施		處理進度追蹤					
資產群組名稱	資產名稱	資產類別(大類)	C	I	A	風險說明	資產殘風險值	風險處理型式	改善活動/控制措施	負責人	預定完成日期	實際完成日期	覆核人	風險減緩預期效益	風險處理進度
								□接受風險 □避免風險 □轉移風險 □降低風險							
								□接受風險 □避免風險 □轉移風險 □降低風險							
								□接受風險 □避免風險 □轉移風險 □降低風險							

▲ 圖 4.7: 風險處理計畫表

資料來源：研究個案 ISMS 程序書，本研究整理。

(五)、風險處理計畫於預訂完成日期結束後，資訊安全工作小組須針對進行風險處理動作之資訊資產，實施風險重新評鑑工作，並將評鑑結果紀錄於「殘餘風險評鑑工作表」，以確認風險處理計畫之執行達到風險減緩預期效益之目標，並將風險重新評鑑之結果提報資訊安全管理委員會。研究個案「殘餘風險評鑑工作表」截錄內容如圖 4.8: 殘餘風險評鑑工作表。

紀錄編號：資訊-程序-04-04-___-___

殘餘風險評鑑工作表

資產辨識與分類				風險評鑑											
資產群組名稱	資訊資產名稱	資產類別		資產價值評估				弱點評估		威脅評估		衝擊分析	風險評估	
		大類	小類	機密性 (C)	完整性 (I)	可用性 (A)	合計	弱點名稱	脆弱度 (V)	威脅名稱	威脅發生機率 (T)	衝擊程度 (IM)	風險值小計	風險總值

▲ 圖 4.8: 殘餘風險評鑑工作表

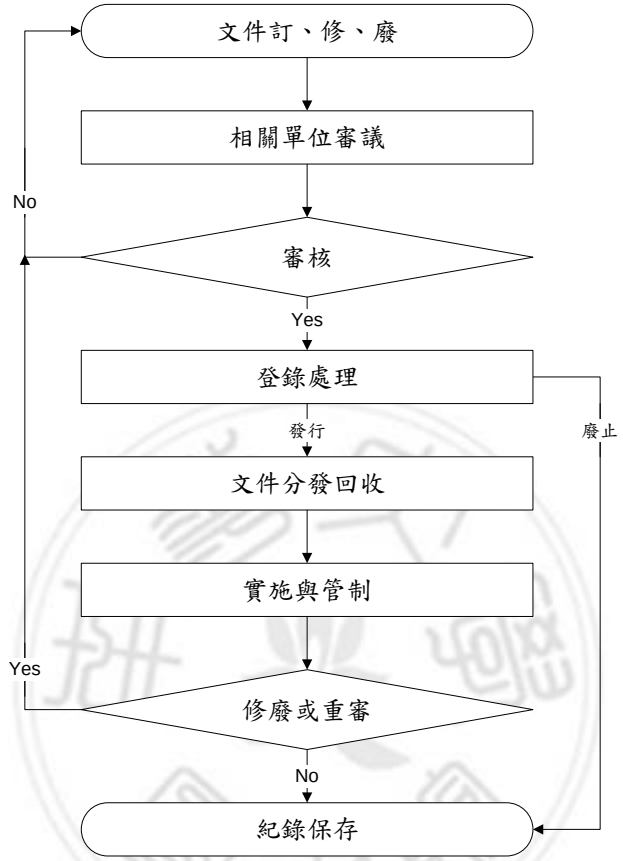
資料來源：研究個案 ISMS 程序書，本研究整理。

研究個案資訊資產盤點內容，早期以服務類、硬體類、軟體類、服務類、文件類...等為盤點主軸，因而忽略掉人員類才是組織推動與執行 ISMS 成敗的關鍵因素，所以在新規範中特別針對人員類進行盤點，將個案單位的人力狀況進行列表與評估其資產價值，評估結果資產價值總計為 7，人員部分皆具有資安素養故脆弱度部分列為 2，資料可能遺失或外洩的問題可能會因工作疏失而發生，所以威脅發生率列為 2，資料外洩後造成的衝擊程度列為 2，最後計算出的風險總值為 56，屬於可控制範圍。

四、修訂 ISMS 管理文件

依據驗證單位之稽核缺失、資安事件發生後之矯正措施、內部稽核缺失矯正及預防措施及「教育體系資通安全暨個人資料管理規範」標準，參考學校現有的資訊安全管理需求來設計，以完成符合「教育體系資通安全暨個人資料管理規範」標準之 ISMS 四階管理文件，並落實執行 ISMS 管理文件中之各項規定以完成驗證。研究個案 ISMS 文件訂、修、廢流程圖如圖 4.9: ISMS 文件訂、修、廢流程圖。研究個案新版資通安全管理規範共分為: 一階手冊 2 份，分別為資訊安全政策及適用性聲明書，

是資訊安全最高指導原則；二階程序書共 19 份；三階標準書共 8 份；四階表單共 66 份，新版 ISMS 規範架構如表 4.5: ISMS 文件架構。



▲圖 4.9: ISMS 文件訂、修、廢流程圖
資料來源 : 研究個案ISMS程序書，本研究整理

表 4.5: ISMS 文件架構

一階手冊	二階程序	三階標準	四階表單
資訊安全政策	文件與紀錄管理程序書	Microsoft Visio 流程圖製作作業標準書	文件標準格式頁
適用性聲明書	組織全景評鑑管理程序書	個人電腦及網路服務使用規範	管制文件訂修廢履歷表
	資安組織與權責管理程序書	資訊安全風險評鑑量化表	管制文件一覽表
	資訊資產管理程序書	網路連線中斷緊急應變作業標準書	文件報表資料調閱申請單
	資訊安全風險管理程序書	外力入侵事件緊急應變作業標準書	外部標準文件一覽表
	資訊安全目標管理程序書	天然災害事件緊急應變作業標準書	文件報表資料銷毀紀錄表
	業務持續管理程序書	校務行政系統異常緊急應變作業標準書	組織全景評鑑表
	資訊安全稽核管理程序書	校務行政系統業務持續計畫	資訊安全管理委員會人員名冊
	矯正及預防管理程序書		外部單位聯絡清單
	資訊安全事件管理程序書		會議記錄單
	人力資源安全與訓練管理程序書		ISMS 有效性量測表
	實體與環境安全管理程序書		資訊資產清冊
	網路安全管理程序書		風險評鑑工作表
	帳號密碼及存取控制管理程序書		風險評鑑報告
	系統發展與維護管理程序書		風險處理計畫表
	資訊備份管理程序書		殘餘風險評鑑工作表
	資訊設備維護與管理程序書		資訊安全目標設定表
	軟體使用管理程序書		資訊安全目標檢討表
	委外作業管理程序書		關鍵營運流程分級表
			業務持續計畫\災害復原演練暨處理報告單
			內部稽核計畫單
			內部稽核檢查單
			矯正及預防處理單
			資訊安全事件報告單
			資訊安全事件報告彙總表

			人員工作職掌表
			員工保密切結書
			工讀生保密切結書
			教育訓練計畫及彙總表
			教育訓練上課紀錄表
			資訊機房門禁卡管制登記表
			資訊機房進出管制登記表
			資訊機房檢查表
			資訊機房系統主機安全查檢表
			辦公區域安全檢查表
			個人電腦安全檢查表
			防火牆通訊埠申請單 (電子)
			資訊設備重大弱點補強紀錄表
			有線網點及無線網路 AP 異動擴增申請單 (電子)
			教職員校務行政系統暨電子郵件使用申請單 (電子)
			密碼變更紀錄單
			系統主機授權申請單
			系統帳號審查紀錄單
			資訊系統開發與變更申請單 (電子)
			資訊系統訪談記錄表
			資訊系統驗收單 (電子)
			應用系統巡檢表
			資訊系統資料異動申請單 (電子)
			資訊系統資料需求單
			資訊系統測試紀錄單
			資訊系統備份計畫表
			系統備份回復紀錄表
			備份作業查檢表
			可攜式設備及儲存媒體管理清冊
			資訊系統變更維護工作紀錄單
			設備借用清單

			資訊設備送修紀錄單
			可攜式設備及儲存媒體使用查核表
			儲存媒體報廢銷毀紀錄表
			軟體使用申請書
			電腦設備合法軟體使用調查表
			委外廠商保密切結書
			委外廠商人員保密切結書
			委外廠商資訊安全要求查核表
			外部人員資訊設備網路連接申請單
			外部人員使用可攜式儲存媒體資料攜出申請單

資料來源：研究個案 ISMS 程序書，本研究整理。

五、訂定 ISMS 績效衡量指標

(一)、為查核資訊安全控制措施的有效性,以確保各項管理品質及運作效率能持續不斷提升進步，以及展現學校能持續且有效地保護重要資訊資產及個人資料之決心，各組承辦人員須每年依據「ISMS 有效性量測表」之項目進行評量，並留下紀錄呈管理審查會議審查，如表 4.6: ISMS 有效性量測表。當評量結果未達預期，或預測未來之趨勢可能造成無法達到績效標準時，應立即採取矯正及預防措施。

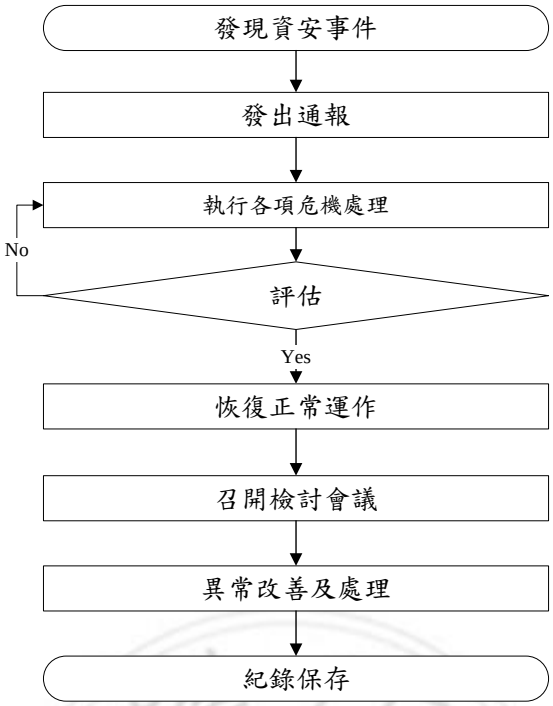
表 4.6: ISMS 有效性量測表

項次	量測項目		目標水準	量測方式	量測結果	差異說明
A.5	資訊安全政策	(1)資訊安全政策審查次數	≧1 次/年	召開審查會議	□ 符合 □不符合	
		(2)資訊安全政策宣導次數	≧1 次/年	會議、教育訓練	□ 符合 □不符合	
A.6	資訊安全組織	(1)有否確實簽署保密協議	不符≦2 件	稽核結果	□ 符合 □不符合	
		(2)管理審查會議召開次數	≧1 次/年	審查會議紀錄	□ 符合 □不符合	
		(3)委外廠商遠端連線造成資安事件次數	≦0 次/年	稽核結果	□ 符合 □不符合	
A.7	人力資源安全	(1)檢查資通安全受訓時數	主管≧ 3 小時 資訊人員≧12 小時 一般人員≧ 3 小時	教育訓練紀錄	□ 符合 □不符合	
		(2)離退人員帳號確實刪除	不符≦2 件	稽核結果	□ 符合 □不符合	
A.8	資訊管理	(1)資訊資產清單是否定期更新	≧1 次/年	更新紀錄	□ 符合 □不符合	
		(2)資訊資產清單符合分級與標示規定	不符≦2 件	稽核結果	□ 符合 □不符合	
A.9	存取控制	(1)定期審查重要系統存取權限（帳號清查）	≧1 次/年	清查紀錄	□ 符合 □不符合	
		(2)管理帳號申請是否依規定填寫表單	不符≦2 件/年	稽核結果	□ 符合 □不符合	
		(3)系統稽核日誌是否已開啟	不符≦1 件	稽核結果	□ 符合 □不符合	
A.10	密碼	(1)管理者密碼長度及複雜度應符合規範	不符≦0 件	稽核結果	□ 符合 □不符合	
A.11	實體與環境安全	(1)檢查有否遵守機房門禁規定	不符≦2 件	稽核結果	□ 符合 □不符合	
		(2)檢查消防器材與 UPS 有否定期保養	不符≦1 件	稽核結果	□ 符合 □不符合	
A.12	作業的安全	(1)惡意程式造成的資安事件次數	不符≦1 件	稽核結果	□ 符合 □不符合	
		(2)定期備份重要系統資料	不符≦3 件	稽核結果	□ 符合 □不符合	
		(3)安裝未授權軟體造成的資安事件次數	不符≦0 件	清查紀錄、稽核結果	□ 符合 □不符合	
A.13	通訊安全	(1)定期監控重要伺服器執行作業之系統容量（例如 CPU、RAM、硬碟）	不符≦2 件	稽核結果	□ 符合 □不符合	
		(2)定期監控網路資源使用率（例如連外頻寬）	不符≦ 2 件	稽核結果	□ 符合 □不符合	
		(3)病毒爆發次數（年）	不符≦3 次/半年	事件紀錄	□ 符合 □不符合	
		(4)檢查病毒碼是否即時更新	不符≦2 件	稽核結果	□ 符合 □不符合	
		(5)檢查重要系統時間是否同步	不符≦2 件	稽核結果	□ 符合 □不符合	
		(6)檢查防火牆設定是否與防火牆進出規則申請表資料相符	不符≦3 件/年	稽核結果	□ 符合 □不符合	
		(7)弱點掃瞄次數	≧1 次/年	掃瞄報告	□ 符合 □不符合	
A.14	資訊系統獲	(1)重要系統更新/上線前經測試	不符≦1 件	稽核結果	□ 符合 □不符合	

	取、開發及維護	(2)重要系統開發或變更時應更新系統文件	不符≦3 件	稽核結果	□ 符合 □不符合	
		(3)重要系統上線具有緊急復原機制	不符≦1 件	稽核結果	□ 符合 □不符合	
A.15	供應商關係	(1)有否確實簽署保密協議	不符≦2 件	稽核結果	□ 符合 □不符合	
		(2)委外廠商資安查核次數	≧1 次/年	稽核結果	□ 符合 □不符合	
A.16	資訊安全事故管理	(1)發生資安事件未依規定通報之件數	不符≦2 件	稽核結果	□ 符合 □不符合	
A.17	營運持續管理的資訊安全層面	(1)執行風險評鑑與營運衝擊分析	≧1 次/年	稽核結果	□ 符合 □不符合	
		(2)檢討營運持續運作計畫演練執行情形	≧1 次/年	稽核結果	□ 符合 □不符合	
A.18	遵循性	(1)合法軟體之安裝	不符≦0 件	清查紀錄、稽核結果	□ 符合 □不符合	
		(2)矯正預防措施於規定時間內改善完成	逾期≦3 件	稽核結果	□ 符合 □不符合	
		(3)是否定期執行資安稽核	≧1 次/年	稽核結果	□ 符合 □不符合	

資料來源：研究個案 ISMS 程序書，本研究整理。

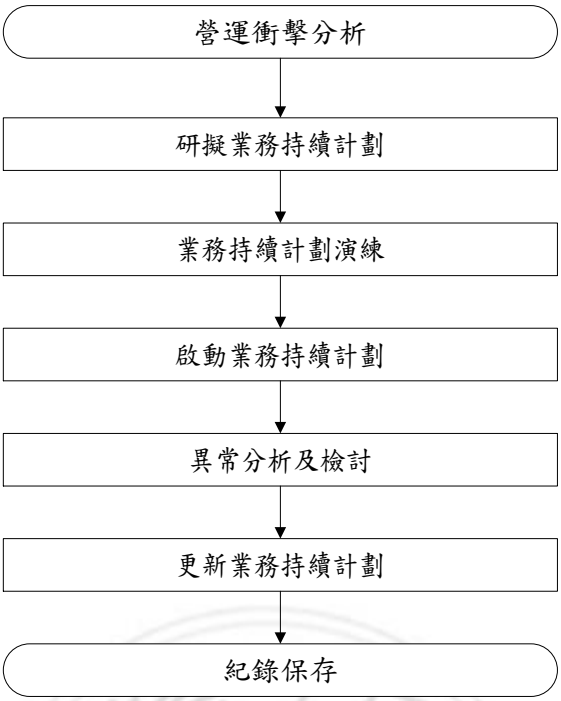
(二)、資訊安全事件管理，舉凡學校與資訊安全相關作業環境中之資訊安全事件，制定明確之處理規範，將安全及失效事件所造成的損害降到最低,並且建立事件學習機制，以識別重複發生的安全或失效事件。如圖 4.10: 資訊安全事件通報及危機處理流程圖。



▲圖 4.10: 資訊安全事件通報及危機處理流程圖
資料來源 : 研究個案ISMS程序書，本研究整理。

六、業務持續計畫測試與演練

(一)、為防止學校業務活動中斷,保護關鍵性業務流程不受重大故障或災害的影響,擬定關鍵性業務流程當遭受重大故障或災害時,可執行之替代方案,以確保員工安全與業務的持續運作,降低事件所造成的損失,並作為業務持續計畫(BCP)發展與維護的依據。研究個案的業務持續計畫執行流程,如圖 4.11: 業務持續管理流程圖。



▲圖 4.11: 業務持續管理流程圖
資料來源 ： 研究個案，本研究整理

(二)、 關鍵營運流程在進行分析前,尚須判斷最大可容忍中斷時間(MTPD)、復原目標時間(RTO)及資料回復點目標(RPO)，若因不可抗力及人為因素，造成服務中斷，應立即採取緊急應變措施及復原程序,而進行以維持日常業務之持續運作，降低對業務活動的衝擊。關鍵營運流程鑑別等級的方法，是參考關鍵營運流程鑑定表，如表 4.7: 關鍵營運流程鑑定表。

表 4.7: 關鍵營運流程鑑定表

識別因子	鑑別等級	鑑別說明(單位：小時)
最大可容忍中斷時間(MTPD)	高	最大可容忍中斷時間小於 4
	中	最大可容忍中斷時間介於 4-12
	低	最大可容忍中斷時間大於 12

資料來源：研究個案 ISMS 程序書，本研究整理。

(三)、關鍵營運流程分析，須檢視負責之營運業務流程，依業務之重要性，鑑別並分別給予「高」、「中」或「低」之關鍵等級，「高」關鍵等級流程即為學校之關鍵性業務流程，營運衝擊分析之結果紀錄於「關鍵營運流程分級表」。研究個案「關鍵營運流程分級表」截錄內容如圖 4.12: 關鍵營運流程分級表。

關鍵營運流程分級表

分級	關鍵流程	單位名稱	負責人	依賴流程/系統	衝擊影響程度	最大可容忍中斷時間	復原目標時間（RTO）	緊急應變措施	復原步驟	資源

▲ 圖 4.12: 關鍵營運流程分級表

資料來源：研究個案 ISMS 程序書，本研究整理。

(四)、業務持續計畫(BCP)須每年進行測試與演練，高危險等級項目由危機處理分組負責規劃，並由相關業務單位擬訂執行計畫，進行測試與演練過程並將結果填寫於「業務持續計畫＼災害復原演練暨處理報告單」，如圖 4.13: 業務持續計畫＼災害復原演練暨處理報告單。測試與演練項目得

依實務需求得採用下列任一方式進行：

1. 結構化測試 （Structural walk-through tests）：召集相關單位與人員進行書面模擬處理方式進行討論。
2. 檢查表測試 （Checklist tests）：發展檢查表，以便相關人員能夠利用此檢查表做測試。
3. 模擬測試 （Simulation tests）：建立一個模擬的環境進行測試。
4. 完全測試 （Full interruption tests）：在實際作業環境中進行測試。。

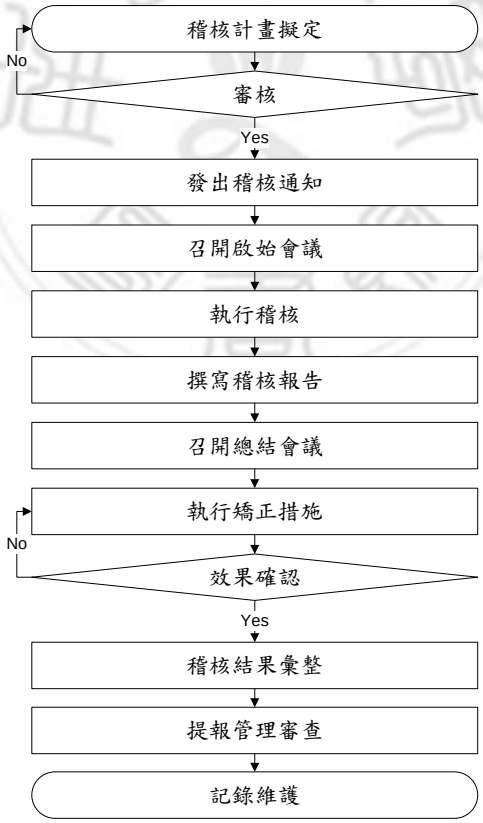
業務持續計畫＼災害復原演練暨處理報告單			
演　練　規　劃　表			
承 辦 人		協辦單位	
規劃日期		填表日期	
演練規劃項目		規劃內容	
1.	規劃演練目標與範圍		
2.	規劃演練腳本		
3.	規劃演練所需設備		
4.	規劃演練所需系統		
5.	規劃演練所需參與人員		
6.	規劃演練時程及完成時限（完成時限參考衝擊分析）		
7.	規劃演練測試方式與測試資源(如：僅測試資料復原 / 異測資料復原與系統復原 / 僅資訊處相關承辦參與測試 / 使用者參與測試)		
8.	規劃演練成果的檢討時程		
9.			
10.			
11.			
承辦人員		主管	
代理人			

▲ 圖 4.13: 業務持續計畫＼災害復原演練暨處理報告單

資料來源：研究個案 ISMS 程序書，本研究整理。

七、執行 ISMS 內部稽核作業

(一)、 對於資訊安全管理系統運作情形予以查驗,以判定系統之各項活動與其相關結果,是否符合預定計畫及計畫事項是否有效執行,並能適切達到資訊安全目標。內部稽核區分為定期稽核與不定期稽核兩類。定期稽核,應每年執行一次,依據定期頒佈之稽核計畫內容,對單位進行內部稽核;不定期稽核,於必要時(如單位業務重大變動時、內部稽核完畢後的跟催及其他非定期性稽核時機),對特定單位資訊安全管理系統之運作,所執行之內部稽核。執行內部稽核管理的流程,如圖 4.14: 資訊安全稽核管理流程。



▲圖 4.14: 資訊安全稽核管理流程圖
資料來源 : 研究個案,本研究整理

(二)、 內部稽核小組，是由執行秘書遴選適當合格之內部稽核人員所組成，以執行內部稽核作業。內部稽核人員應針對負責部分，先了解各相關規定程序及標準，並詳讀上次稽核之缺點報告，以研擬此次稽核之重點，並編寫於「內部稽核檢查單」上，呈核後影印一份給受稽核單位主管，做為對受稽單位稽核通知使用。研究個案「內部稽核檢查單」截錄內容如圖 4.15: 內部稽核檢查單。

內部稽核檢查單							
稽核項目		受稽單位		稽核員		稽核日期	

章節	稽核要點	稽核結果			稽核發現
		符合	不符合	不適用	
4.	**組織背景**				
4.1	**了解組織與其背景** 組織應決定與其目的相關，且會影響其 ISMS 預期結果的達成能力之外部與內部問題。				
4.2	**了解利害相關團體的需求與期望** 組織應決定： a) 與 ISMS 有關的利害相關團體；以及 b) 與資訊安全有關的這些利害相關團體之要求。				
4.3	**決定資訊安全管理系統的適用範圍** 組織應決定ISMS的界線與適用性，以建立其適用範圍。當決定適用範圍時，組織應考量： a) 4.1 所提到的外部與內部問題； b) 4.2 所提到的要求；以及 c) 在組織與其他組織執行的活動之間的接合與互賴關係。				
4.4	**資訊安全管理系統** 組織應依據本標準的要求，以建立、實施、維持和持續改進ISMS。				
5.	**領導力**				
5.1	**領導力與承諾** 高階管理者應展現領導力，以及與 ISMS 有關的承諾，藉由： a) 確保資訊安全政策與目標已建立，並且和組織的策略方向是相容的； b) 確保 ISMS 的要求已融入組織過程中； c) 確保 ISMS 所需的資源可取得； d) 傳達有效資訊安全管理的重要性，並且遵守 ISMS 的要求； e) 確保 ISMS 達成其預期效果； f) 指導與支援人員，使其對 ISMS 的有效性做出貢獻； g) 促進持續改進；以及				

▲ 圖 4.15: 內部稽核檢查單

資料來源：研究個案，本研究整理。

(三)、 受稽部門應尊重及支持稽核人員，誠實答覆稽核人員所提問題，並接受調閱相關的紀錄、報告及文件資料；稽核人員於稽核後應收集客觀證據，將發現之缺失及與受稽單位研討之改善措施撰寫於「矯正及預防處理單」，並

請受稽單位提出改善期限並簽名確認後呈核，而各受稽單位則應於改善期限前完成矯正措施，以維持資訊安全管理系統正常運作。研究個案「矯正及預防處理單」內容如圖 4.16: 矯正及預防處理單。

矯　正　及　預　防　處　理　單			
發生日期	年　月　日	提出者	
問題來源	□內部稽核□外部稽核□風險評鑑□資安事件□個資事件□自行提出□其他_____		
問題點描述 (請依人、事、時、地、物詳述)			
原因分析 (RCA)			
※ 1.提出者填寫完成後，送交權責人員「登錄列管」，權責人員將正本送交該業務單位主管，進行原因分析及改善之 Plan / Do / Check / Act。 2.業務單位須將執行結果提交權責人員審核。			
研擬改善對策(PLAN)			
矯正措施	預防措施	執行者	
		完成期限	
審核改善對策適合與否			
單位主管			
執行情形			
對策實施經過(Do)	效果確認(Check)	對策處置(Act)	承辦人
		□ 陳請結案 □ 重新對策	
完成後審核			
主管		□准予結案 □重新對策	
		結案日期	
※經權責主管核准結案後，由資訊中心保存正本，並影印交業務單位備查。			

▲ 圖 4.16: 矯正及預防處理單

資料來源 ：研究個案，本研究整理。

八、驗證前準備

(一)、 依照教育機構資安驗證中心所公告的教育機構資安驗證申請說明，申請驗證共需須備妥八項文件，分別為「教育機構資安驗證申請書」、「教育機構資安驗證服務權利與義務聲明書」、「資訊安全政策書面文件」、「適用性聲明書書面文件」、「適用法規清單」、「資訊安全管理系統文件一覽表書面文件」、「教育體系資通安全管理規範實施自評表」及「申請單位的地理位置圖」。將所有文件填寫完成並交由主管簽章後，正本寄送到教育機構資安驗證中心，驗證中心收到驗證申請表及必備文件後 5 個工作日，對於符合規定之申請案件即受理申請，並通知申請單位以匯款方式繳交驗證費。

(二)、 就前次外部稽核次要缺失及觀察事項、內部稽核缺失，重新檢視矯正及預防處理單之執行狀況，確保已完成矯正工作與預防修正工作，如有尚未修正之缺失則應盡速予以修正及補強，以及 ISMS 文件表單資料是否有依據各項表單工作時程內完成，以確保外部驗證前備妥所有 ISMS 紙本文件與完成所有矯正工作。

九、正式評鑑與技術轉移

正式評鑑工作共分為兩個階段，第一階段稽核為文件初審，由驗證中心提供驗證申請單位之「資訊安全政策書面文件」、「適用性聲明書書面文件」、「適用法規清單」、「資訊安全管理系統文件一覽表書面文件」、「教育體系資通安全管理規範實施自評表」給予稽核員審查，以了解申請單位的資訊安全管理系統文

件架構及實施現況，並規劃現場稽核作業提供重點；第二階段稽核為現場稽核，主要目的為觀察驗證申請單位資訊安全管理系統實作情形，透過人員面談、檢視紀錄表單、人員實地操作等方式，評估確認申請單位是否遵守資安政策、目的及程序。現場稽核流程為啟始會議、人員訪談、實地審查、產生稽核發現、稽核小組內部會議及總結會議。

教育機構資安驗證中心依據研究個案之申請項目複雜度、驗證範圍、場區及員工數量，決定現場稽核過程共需 2 人天；第一天稽核議程共包含啟始會議、管理階層訪談、適用性聲明書版本確認、驗證範圍瀏覽、文件審查與實地審查；第二天稽核議程為文件審查、實地審查、稽核小組內部會議及總結會議。稽核小組利用訪談、文件與記錄審閱、以及實地觀察...等方式執行驗證稽核作業，其驗證稽核作業的目標為確認單位的資訊安全管理制度是否有符合「教育體系資通安全暨個人資料管理規範」條件、確認單位有無落實改善前一次驗證稽核的稽核發現、確認單位的管理制度足以達成單位的管理政策要求，並將稽核結果製作成稽核報告。

總結會議中由主導稽核員提出稽核發現與稽核結論，申請針對稽核報告所列不符合項目若有不同意見，得當場提出澄清或補正相關資料，經充分討論後達成共識時，申請單位得於稽核報告之申請單位代表簽名欄簽名。申請單位及主導稽核員簽名過後的書面稽核報告為一式兩份，於總結會議後一份由申請單位留存，一份由稽核員攜回驗證中心審查。研究個案的稽核報告內容中，共發現 4 項次要不符合事項，其相關矯正及預防處理

於稽核完畢後 2 周內提送給驗證中心，經主導稽核員查驗後，開立有條件建議發證追蹤處理單，由資安驗證中心驗證審查委員會進行審核並做出驗證判斷，再報請教育機構資安審議委員會進行複核。複核結果研究個案通過「教育體系資通安全管理規範驗證」，並獲得核發的中文證書乙份。

總結以上流程，針對研究個案因應新規範要求，所進行之修改內容其考量因素說明如下:

(一)、 一階資安政策部分增加對組織全景之鑑別，鑑別出對本校提供服務相關之利害關係者，並就利害關係者之需求與期望值，讓資訊安全長知悉並取得共識。

(二)、 二階程序書中，「資訊-程序-01 文件與紀錄管理程序書」就外來文件部分將其範圍明確界定以利管控;「資訊-程序-02 資安組織與權責管理程序書」將資安工作小組、稽核工作小組之權責明定在程序書中，以符合新規範中角色、責任及權限之規定;「資訊-程序-03 資訊資產管理程序書」在資訊資產鑑別以 ISMS 三要點機密性、完整性、可用性進行高、中、低等級分類以便於進行量化分析;「資訊-程序-04 資訊安全風險管理程序書」將風險值計算流程加註說明，便於進行資安評鑑時之參考用;「資訊-程序-06 業務持續管理程序書」於名詞定義中將營運持續計畫、最大可容許中段期間、復原目標時間、資料回復點目標…等重點名詞做說明，研究個案之高等級關鍵營運流程，以系統運作重要性及相關設備之備援狀況為考量因子，將其最大可容忍中斷時間定義為中等

級；「資訊-程序-07 資訊安全稽核管理程序書」在內部稽核部分，因應新規範要求人員需進行相關能力訓練，故增列內稽人員需受過至少 6 小時(含)以上之專業訓練且領有證書或上課證明者，始可任用為資安內部稽核人員；「資訊-程序-08 矯正及預防管理程序書」修改單位所提出之矯正預防措施內容應制定相關管理文件以維持對策持續有效；增訂「資訊-程序-19 組織全景評鑑管理程序書」因應新規範規定，就 ISMS 之施行須透由組織之相關會議作成決議、ISMS 文件須保存文件化紀錄以供關注方確認、ISMS 鑑別與分析應每年至少進行一次審查評估，以確保 ISMS 適用範圍是否有調整之必要。

(三)、三階標準書中，「資訊-標準-02 個人電腦及網路服務使用規範」針對內、外部人員使用可攜式資訊設備(如:筆記型電腦、平板電腦、智慧型手機…等)、可攜式儲存媒體(如:USB 隨身碟、可攜式硬碟、數位相機記憶卡…等)之使用方法進行管制，以防止資訊外洩或中毒問題發生，並就外部人員增設兩項表單「資訊-標準-02-01 外部人員資訊設備網路連接申請單」、「資訊-標準-02-02 外部人員使用可攜式儲存媒體資料攜出申請單」，以確保網路及資訊安全。

(四)、 四階表單中，將原有 58 項表單刪除資料內容與屬性重疊性過高的「資訊資產變更申請單」，保留「資訊系統變更維護工作紀錄表」;「系統主機授權清冊」與「系統主機授權申請單」填寫之欄位內容重複，故予以簡化僅

保留「系統主機授權申請單」;因應新規範之要求增加「組織全景評鑑表」、「ISMS 有效性量測表」、「文件報表資料銷毀紀錄單」、「系統帳號審查紀錄單」、「資訊系統資料需求單」、「資訊系統測試紀錄單」、「儲存媒體報廢銷毀紀錄單」、「委外廠商資訊安全要求查核表」...等 8 項表單。

第三節 個案分析

在了解研究個案轉版建制新版「教育體系資通安全暨個人資料管理規範」的整個程序後，研究個案建置 ISMS 的重點獲得如下的分析內容:

壹、組織全景與資安範圍界定

研究個案依照「教育部與所屬機關(構)及學校資通安全責任等級分級作業規定」中 B 級單位 ISMS 推動作業要求，應至少包含資訊管理單位、學術網路系統、核心業務資訊系統，因此將驗證範圍定義為「資訊中心辦公區域環境、資訊機房及校務行政系統運作及維護之安全管理」，並依據學校決議事項確認其關注方(如:教育部、區域網路中心、中心人員、教職員生家長)的要求事項，透由高階主管(如:副校長)的支持聲明，清楚揭示資訊安全目標及完成組織全景與資安範圍界定。

貳、資訊資產價值判斷

資訊資產共分為六大類，分別為人員類、文件類、服務類、硬體類、軟體類、建築與保護類，資產價值越高代表該資產的重要性越高，相對威脅發生時對組織的衝擊性也越高，因此需考量相對應的控制措施，以確保只有經過授權的人才能存取資訊，以保持資產價值的

機密性；保護資訊及其處理方法的準確性，確保資料不會遭到任意竄改，以保持資產價值的完整性；確保經授權的使用者，在需要時可以隨時存取資訊並使用相關資訊資產，也就是維持資產價值的可用性。

參、風險評鑑報告與風險處理計畫訂定

風險評鑑為計算資訊資產風險值之程序，用以決定風險處理之優先順序，而風險評鑑則會因為營運組織變更、作業流程或服務範圍改變、資訊資產新增或變更、發生重大資安事件、相關利害團體反映或相關法令法規變更而影響到學校...等因素而變動，所以每年至少需執行一次風險評鑑，將現行的資訊資產風險等級計算出來，完成「風險評鑑報告」；針對風險評鑑報告中須降低風險等級之資訊資產，擬定適當之處理措施、處理進度追蹤、預定完成日期...等資料，製成「風險處理計畫表」，並於預定完成日期結束後，再針對進行風險處理之資訊資產實施風險重新評鑑，以確認風險處理計畫之執行達到風險減緩預期效益之目標。

肆、資訊安全指標選擇

為了查核資訊安全控制措施的有效性，研究個案以 ISO 27001:2015 控制領域 A.5 到 A.18 為量測項目，制定量化的目標水準每年進行評量，確保 ISMS 執行結果與資訊安全政策相符及確保控制措施是否有落實執行，評量完成的「ISMS 有效性量測表」呈報管理審查會議審查，使高階主管了解 ISMS 是否持續有效。

伍、聘用外部專業顧問團隊進行輔導

有道是「工欲善其事，必先利其器」，研究個案聘用的外部專業顧問團隊具有豐富的輔導資安實績，且雙方在民國 99 年 ISO 27001:2005

導入初期就合作過，因此顧問公司對於研究個案組織及業務狀況相當熟悉，且對既有資安政策、組織架構、人員權責、資訊資產及作業流程...等熟悉度也相當足夠，所以能將現行 ISMS 依據「教育體系資通安全暨個人資料管理規範」進行轉版，建置適合個案的新版 ISMS。

陸、單位人員有效溝通與資源整合

研究個案的驗證範圍所包含的人員有資訊安全長、執行秘書、資訊安全工作小組、稽核工作小組及資安顧問團隊。內部溝通所需的人員是資訊中心所有同仁，外部溝通部分則是資訊中心與顧問團隊間的溝通，而資訊中心與顧問團隊兩者皆有專業的資安背景，與早期的合作經驗，因此在資安議題上的溝通不會有知識不足、知識落差問題或內容討論上的障礙問題，顧問團隊給予的專業建議，中心人員也都能全力配合以使資源整合及順利完成各項工作。

柒、透過教育訓練增強員工資安素質

針對轉版建置 ISMS 的各階段過程中，資安顧問團隊提供相對應的教育訓練，包含新舊規範控制領域差異性分析、資產管理教育訓練、風險評鑑教育訓練、內部稽核教育訓練以及全校性資訊安全認知教育訓練...等，不僅讓中心人員更加了解新版「教育體系資通安全暨個人資料管理規範」，同時也增強了全校教職人員的資訊安全素質。

第五章 結論與建議

第一節 研究結論

現今資訊科技應用發展快速，網路應用範圍廣大，所面臨的威脅也更為嚴重，所以如何提升資訊安全以及訂定資訊安全規範並加以落實執行，是組織裡各層面所有的人都應遵守與執行。本研究為基於 ISO 27001 轉版建置 ISMS 程序探討，試圖瞭解組織在既有的資通安全管理規範下還願意進行轉版的動機，找尋出轉版建置新規範可能面臨的困難點及如何解決問題，最後分析出導入新資通安全規範驗證的成功因素及效益，提供給未來有意取得相同資安驗證之組織單位、管理階層及後續研究者參考用。

壹、組織在導入資通安全規範的驗證範圍，應包含組織的關鍵核心業務，本研究個案的關鍵核心業務是依照行政院國家資通安全會報訂定之「政府機關(構)資通安全責任等級分級作業規定」與教育部頒定之「教育部與所屬機關(構)及學校資通安全責任等級分級作業規定」之 B 級單位建置 ISMS 範圍，應包含資訊管理單位、學術網路系統、核心業務資訊系統，故本研究個案驗證範圍為「本校資訊中心辦公室環境、資訊機房及校務行政系統運作及維護之安全管理」，這些項目也是本研究個案導入資通安全規範動機中所重視與積極保護的資產，另外，組織在既有的資通安全規範下仍願意再進行轉版的動機，還包含遵循教育部法令法規的要求、達到關注方的要求、保護組織的重要資料、提供穩定的服務、達到持續營運的目的、提升組織形象及強化組織的競爭力。

貳、組織在轉版建置新規範的過程中，會面臨的困難點與解決方法，包含:

一、 組織人員對新規範的不熟悉，而對新規範的推動產生畏懼或抗拒的心理，此時就需要透過教育訓練加強對新規範的宣導，讓人員了解新規範的要求並非加重大家的原工作量，而是因應現行資安環境所進行的改善動作，使資安工作的推動與執行更符合現行環境。

二、 組織單位主管的支持度，影響著組織能否順利推動轉版建置新規範的成敗因素，因此要讓單位主管了解新規範是因應教育主管機關所下達的重要決定，且新規範的推動較原規範所能達成的效益更大,如此才能取得相對應的財力、人力及物力的支援，使新規範的推動及宣導更為順暢。

三、 資訊安全管理制度的合理性，須因著學校類型、組織特性、領導作為而有所調整，本研究個案資訊安全管理制度的推動以資訊中心為主，並期望在新規範的要求下能夠取得創新性、便利性及安全性的資訊安全管理制度，因此尋求專業顧問公司的協助,就組織全貌、領導作為重新規劃管理目標及風險處理程序，並要求不加重單位組織現行工作量為原則，制定出適當且合理的資訊安全管理制度。

參、組織導入新資通安全規範並通過驗證的成功因素，在於高階主管協助制訂出明確的資訊安全政策，藉由「組織全景評鑑表」將組織之使命、核心價值、願景及營運目標…等資訊條列於表單中，讓組織成員清楚地了解到學校執行資通安全規範轉版的決心，以激發成員之工作使命感，使得組織成員能了解資安管理工作要落實執行才能

確保組織持續營運，並配合單位要求積極參與資安教育訓練，以學習如何制定有效風險管理制度，做出正確識別可能的威脅並降低風險及監控風險，再透由資安量測指標，讓組織可以有效的量測 ISMS 推動狀況，幫助組織審視 ISMS 各項流程與控制措施是否需要再進行修改或加強…等工作。

肆、當組織導入新資通安全規範後所獲的效益，包含:

一、 利用新規範規定之資產類別重新盤點出的資訊資產進行的風險管理制度，有效鑑別出高風險的資產，使組織能夠在有限資源下針對高風險的資產進行相關的改善工作。

二、 透由 ISMS 有效性量測表，再審視組織執行 ISMS 狀況，並因應環境變化與考量關注方要求、組織願景、內部稽核及管理審查會議...等要求，使組織真正落實資訊安全管理系統的 PDCA 循環，獲得持續改善的能力。

三、 更新資安通報流程，強化組織處理災害事故的應變能力，並增加主管危機意識，進而有助於組織單位爭取資安維運設備預算的佐證資料，以達到關鍵業務不中斷的目的。

四、 獲得教育部核可的新版資通安全管理規範驗證，以顯示學校對資訊安全保護工作的重視，及成功打造安全可靠的網路資訊環境，並提升學校的資安專業形象。

第二節 研究建議

依據研究結果，對於未來想導入新版資訊安全管理系統之組織或研究資訊安全管理議題之研究者，提供以下建議:

壹、資訊安全導入範圍的選擇，除考量法令或規範之要求外，可再擴展到核心業務資訊系統之主要使用行政單位，更甚者推展到學術單位以及全校，因為資安之推動與執行絕非單一單位之工作，應是全面性的防護工作，如此才能以制度面進行更寬廣角度的資安管控，由各單位自行評鑑出自己單位可能之風險因子，對風險進行管控以降低其發生率，或當期發生時能夠降低其損害率，如此才能更完整、更全面性的解決組織內部資安問題。

貳、現今網路資安事件發生同時，往往伴隨個資外洩事件發生，如:台視新聞於 2017 年 11 月 22 日報導「驚! 全球 5700 萬筆個資外洩 Uber 隱瞞遭駭，1 年前遭駭客攻擊傳 Uber 付 10 萬美元贖金，Uber 稱信用卡資料未遭竊，遭竊個資已銷毀，資安長丟飯碗! Uber 供用戶免費監控軟體」(https://www.ttv.com.tw/news/view/10611220014300I/568)，造成全球共 5,000 萬名乘客及 700 萬名司機的個資遭竊。而我國近年來對「個人資料保護法」進行相關修法，並於民國 105 年 3 月 2 日公布「個人資料保護法施行細則」，所以未來研究資訊安全議題時，建議將個人資料保護議題進行一同研究。

參、對於資訊安全管理議題之研究，未來可再考量立法院審議中的「資通安全管理法」。目前資訊安全管理是依循行政院「政府機關（構）

資通安全責任等級分級作業規定」，未來加入具法律強制效力的「資通安全管理法」，是否能加速組織單位執行資安管理工作的意願與成效，將是值得探討的議題。

參考文獻

一、 中文部分

1. Yin, R. K.著、尚榮安譯，個案研究法，弘智文化，初版，台北市，139 頁、142~143 頁、158 頁，2001。
2. 方仁威(民 93)，「資訊安全管理系統驗證作業之研究」，交通大學資訊管理研究所博士論文。
3. 王振鴻(民 98)，「全組織導入資訊安全管理系統的個案研究」，長庚大學資訊管理研究所碩士論文。
4. 金天翼(民 100)，「以個案研究探討組織 ISMS 之導入」，中央大學資訊管理學系碩士論文。
5. 林祝興、張明信，資訊安全導論，旗標出版股份有限公司，初版，台北市，10-3~10-4 頁，2015。
6. 周楷智(民 103)，「教育機構個人資料保護稽核機制之研究-以某國立大學為例」，中正大學會計與資訊科技研究所碩士論文。
7. 柳望君譯 MARK S. Merkow & Jim Breithaupt.著，資訊安全，台灣培生教育出版股份有限公司，初版，台北市，2006。
8. 高淑清，質性研究的 18 堂課-首航初探之旅，麗文文化事業股份有限公司，初版，高雄市，70 頁，2008。
9. 郭瑞祥(民 101)，「資訊安全管理系統及個人資料管理系統整合之研究」，中山大學資訊管理學系研究所碩士論文。
10. 張正宏(民 101)，「探討銀行業 ISO/IEC 27001:2005 資訊安全管理現況-以 T 銀行為例」，中央大學資訊管理學系碩士論文。
11. 張瑞琛(民 99)，「運用教育體系資訊安全管理規範於國軍某指揮參謀學院之資訊安全管理探討」，元智大學資訊管理學系碩士論文。
12. 許瑋麟、郭仁宗、何玉菁，「台灣企業實施資訊安全管理系統關鍵成功因素調查」，慈濟技術學院院報，22 期，95-108 頁，民 103。
13. 章語彤(民 105)，「導入資訊安全管理系統及個人資料保護法之研究-以 H 大學為例」，華梵大學資訊管理學系碩士論文。
14. 黃郁育(民 103)，「資訊安全管理系統版本差異之導入流程整合」，中山大學資訊

管理學系碩士論文。

15. 詹前隆、黃依賢、黃慶裕,「組織導入資訊安全管理制度之效益探討」,資訊傳播研究,3 卷 1 期,73-92 頁,民 101。

16. 鄭秀珠(民 104),「雲端數位學習平台之有效因素研究-以電信業『資訊安全及個人資料保護宣導』」,東吳大學資訊管理學系碩士論文。

17. 潘天佑,資訊安全概論與實務,碁峰資訊,初版,台北市,14-14~14-15 頁,2008。

18. 教育體系資安規範稽核員轉版訓練課程,教育機構資安驗證中心,初版,7~8 頁、35 頁、A-61~A-88 頁,2016。

19. 教育體系資安規範新版實務課程,NII 產業發展協進會,初版,46 頁,2016。

二、 西文部分

1. ISO/IEC 27001:2005, Information technology - Security techniques – Information security management systems – Requirements.
2. ISO/IEC 27001:2013, Information technology - Security techniques – Information security management systems – Requirements.

三、 其他文獻

1. ISO 27001:2005 資訊安全管理系統—要求-經濟部標準檢驗局，http://www.bsmi.gov.tw/wSite/public/Data/f1223529524000.ppt ，擷取時間 2017/8/26。

2. 政府機關(構)資通安全責任等級分級作業規定，http://www.nicst.ey.gov.tw/News_Content.aspx?n=626B7A2643794AB0&sms=C43ECA251722A365&s=EAB1BC3FBEF78C99 ，擷取時間 2017/9/2。

3. 陳伯榆，新版 ISO/IEC 27001:2013 升級背景說明與考量，精品科技，http://www.fineart-tech.com/index.php/ch/90-fineart-express/coverstory/394-coverstory-2014-q2-1 ，圖 4:A5-A18，14 領域變化圖，擷取時間 2017/9/5。

4. 教育部與所屬機關(構)及學校資通安全責任等級分級作業規定，http://ic.nhu.edu.tw/files/archive/461_04f9bf71.doc，擷取時間 2017/9/2。
5. 教育機構資安驗證中心 https://www.iscb.edu.tw/iscb/vcinfo，擷取時間 2017/9/2。
6. 教育機構資安驗證中心教育機構資安驗證作業手冊，https://www.iscb.edu.tw/isdata/doc/EDU-ISCB-A-02_manual_v4.1.pdf，擷取時間 2017/9/2。
7. 教育體系資通安全管理規範 https://cissnet.edu.tw/Home/rule_edu，擷取時間 2017/9/2。
8. 教育體系資通安全暨個人資料管理規範 https://www.iscb.edu.tw/isdata/doc/1-ediisms-1050704.pdf，擷取時間 2017/9/2。
9. 劉勝雄著，資訊安全稽核人員訓練與政大實例探討，政治大學電子計算機中心，http://slidesplayer.com/slide/11594159/ ，3 頁，擷取時間 2017/9/16。