國立政治大學資訊科學系
Department of Computer Science
National Chengchi University

碩士論文

Master's Thesis

ISMS與PIMS整合導入之研究
–以國防部全球資訊網站系統為例

Research on Importing and Integration of ISMS and PIMS – A Case Study of the World Wide Web for Military of National Defense, Taiwan, R.O.C

研 究 生：孫天貴
指導教授：左瑞麟

中華民國一〇四年七月
July 2015

摘要

隨著資訊科技的蓬勃發展，資訊技術可以提昇組織效率與競爭力，資訊系統或網站亦是組織營運重要命脈。而在近年來全球資訊安全事件不斷發生，資訊犯罪手法不斷翻新，所肇生的系統損害、資料毀損、個資外洩、財務詐騙事件近來更是層出不窮，對單位或公司而言風險不斷提高，傷害亦相對嚴重，甚至導致公司信譽破產，面臨倒閉威脅，為保護組織內部資訊相關資產與個人資料，並保持組織持續正常運作，資訊安全管理系統（ISMS）與個人資訊管理系統 (PIMS) 便是一套可有效控制管理之方法；ISMS 與 PIMS 分兩次來導入，造成組織增加工作負荷，有疊床架屋情形，成本有部分重複投資現象。本研究試著以資料的生命週期，資訊安全的機密性、完整性、可用性，PDCA 運作模型...等角度進行本質上探討，來進行整合 ISMS 與 PIMS 的整合工作。

經文獻探討與專家學者建議，本研究突破各項盲點，從各角度分析進行多面向整合工作，並提出 4 點可有效整合具體作法：1. 清查作業流程須包含個人資料所延伸之流程。2. 進行作業流程上資訊資產及個資清查作業。3. 資訊資產及個人資料風險評鑑作業。4. 建立 ISMS 與 PIMS 四階文件，產出 ISO27001 適用性聲明須包含個資法。

本研究以國防部網站系統為例，運用整合結果進行實作，將實作經驗分享給未來有意導入 ISMS 與 PIMS 之 IT 人員，實作結果也證實本研究提出論點確實有效，更有效且更有邏輯性的面對各種資安與個資問題，以作業流程面來分析資安與個資，讓每個控制點更加明確，最後實作運用以各國均能接受的 ISO 標準(ISO 27001 標準包含個資管理流程)來驗證本實作，也證明本研究整合後，在實施（Plan-Do-Check-Act）管理系統確實有效，均能符合相關標準與法規。

關鍵詞: 資訊安全管理系統(ISMS)、個人資料管理系統(PIMS)、MSS、個人資料保護法、ISO27001、TPIPAS、BS10012。

Abstract

With the rapid development of information technology. information technology can enhance the organization efficiency and competitiveness.information system or website is also an important lifeline organizational operations.

In recent years, the global information security incidents continue to occur. Ever-changing information modus operandi, the system damage, data corruption, personal information leakage, financial fraud recent events is endless.The unit or risk companies continue to improve. Also relatively serious injury, and even lead to the company's reputation bankruptcy, faces closure threat within the organization for the protection of personal data and information-related assets, and continued to maintain the normal operation of the organization. Information Security Management System (ISMS) and Personal Information Management System (PIMS) is a set of methods to effectively control management; ISMS and PIMS to import twice, increases the workload, there are needless repetition circumstances, the cost of some duplication of investment phenomenon. The study tried to lifecycle data, information security confidentiality, integrity, availability, PDCA operating model ... were essentially discussed perspectives to integrate the work of integrating ISMS and PIMS.

Through literature review and experts suggested that the research breakthroughs of the blind spots, multi-oriented integration from each perspective, and gives four specific practice can be effectively integrated:

1. Inventory workflow process must include the extension of the personal data.
2. Perform the work flow of information assets and personal information checking operations.
3. Information assets and personal information, risk evaluation operations.

4. Establish ISMS and PIMS four level documents structure, output ISO27001 applicability statement shall contain a personal information protection act.

In this study, the Department of Defense Web site system, for example, the use of integrated solid results for the real experience sharing as the future intention to import ISMS with PIMS of IT staff, implement the results of this study also confirmed that the arguments put forward truly effective, more efficient and more logic in the face of a variety of information security and a financing problem to surface to analyze processes of information security and a funded, so that each control point more clearly, and finally apply to countries implement acceptable to ISO standard (ISO 27001 standard including Personal Information Protection Management Processes) to verify this implement, also proved this study, integration, implementation (Plan-Do-Check-Act) management system really works, can meet the relevant standards and regulations.

Keywords: Information Security Management System (ISMS), personal information management system (PIMS), MSS, Personal Data Protection Act, ISO27001, TPIPAS, BS10012.

誌謝

在政治大學求學過程中，回想這四年光陰，幾乎是擠出時間過日子，不管在工作上的磨練、學業上的考驗、家庭上的照顧，讓我分身乏術，要當個好的部屬、好的老公、好的爸爸，實在不容易；在此特別感謝左瑞麟老師在我工作上與家庭上的體諒，學業上諸多的指導，讓我順利完成碩士學業。

也感謝我的老婆，在這期間生下一女一子可愛的寶寶，以及學業上的督促；「說到作到」是我一貫的作風，答應妳的事，我從沒忘記，未來日子裡，我會更珍惜人生每個時光；也感謝我的家人，無時無刻給我打氣，幫我照顧小孩，讓我有時間可以專心於學業。

最後，感謝嘉義大學王智弘老師、長庚大學許建隆老師、致理技術學院呂崇富老師、華夏科技大學蔡國裕老師給予學術上指導，以及最佳化企管顧問有限公司何銘燁顧問給予實務上之協助，感謝所有在學習期間曾經協助我的同學、朋友、家人、同事，還有 上天，謹致上個人最高的謝意!

未來的日子，我會致力於將所學貢獻於社會，幫助人群，不斷學習，並將我的座右銘時時警惕「待有餘而濟人，必無濟人之日；待有暇而讀書，必無讀書之時」，知難行易一步一步去完成。

孫天貴 謹致

目錄

表目錄

圖目錄

1. 緒論

1.1. 研究背景

1.1.1. 網站系統面臨的資安問題

網站系統是公司營運重要命脈，是對外服務或行銷重要的窗口，但近年來資安事件不斷發生，如南韓所遭遇的大規模病毒攻擊 (癱瘓將近 3 萬 2 千台電腦)、個資外洩 (Sony PSN, LinkedIn, Dropbox, Evernote…等)、關鍵網路機房因電力中斷導致全臺對外網路服務遭受到嚴重影響、菲律賓對台政府機關發動一連串的網路攻擊…等事故，均對政府機關或企業組織的網站系統營運造成了重大的衝擊(本單位網站系統如圖 1-1 所示)。

由於資訊犯罪手法不斷翻新，資訊安全的威脅與過去相比不管在議題的複雜性、管理的難度及範圍的涵蓋面上已經產生了不小的轉變，如: 網路安全 (Cyber security)、智慧型設備所衍生的 BYOD (Bring Your Own Device)，社群媒體 (Social Media)、巨量資料 (Big Data)、雲端 (Cloud)、進階持續性威脅(Advanced Persistent Threat，APT)、個資防護的安全管理等都是不小的挑戰。

網站系統所遭受的系統損害、資料毀損、個資外洩、財務詐騙事件，對單位或公司而言，威脅逐年增加，稍有不慎可嚴重影響公司信譽，甚至面臨倒閉威脅。

圖 1-1：國防部網站系統畫面

從圖 1-2 可以看的到，全球駭客攻擊從不間斷，駭客攻擊手法也不斷翻新，身為網站系統管理人員要如何因應這些問題呢?實在是非常難處理的議題。面對這些駭客攻擊的手法日新月異，倘若與其進行軍備競賽，逐年採購新型高階防禦資安設備，似乎不是一個較好的解決之道；或者運用好幾道資安防護機制，如進入網站需進行圖像驗證，再來進行密碼驗證，再來進行憑證驗證...等眾多資安防護手段，讓民眾或使用者非常不便利；或者消極的面對這些資安事件，等出事再來改進；在此，本研究提出：分配適當的資源進行風險管控，會是大多公司或企業所願意接受的想法。

圖 1-2：全球駭客即時攻防狀況

資料來源：http://map.ipviking.com

然而資訊安全的威脅，不單只是外部威脅(如天然災害、駭客病毒、明文傳輸、連線欺騙...等)，資安事件發生往往內部問題(系統弱點、員工操作不當、內部人員惡意操作、內部網路管理不善、協力廠商問題...等)佔大多比率。

本研究試想有沒有一套方法或管理作法可以全方面進行這些工作，解決眾多資安問

題，研究過程中發現，現今各政府部門及公司為達成資訊安全的目標，藉由導入「資訊安全管理系統」(Information Security Management System，ISMS)，可點線面全方位檢視所有資訊環境，了解自身弱點與威脅，強化資安管理流程，依標準作業程序使用資訊工具，達到良善的資訊及資安管理目的。

1.1.2. 個資法的實施造成的衝擊

但是身為網站管理人員，只要把網站管理好就好了嗎?自從個資法三讀通過實施後，時有所聞某網站或系統因管理不當或駭客入侵造成大量個資外洩，如圖 1-3 所示，2012 年 12 月 27 日新聞報導，屏東縣政府網站因管理不當，公布民眾個人資料在網站上，未符合個資法要求，遭提出告訴賠償 200 萬元，是本國個資法實施後挨告的首例。

環評洩自救會個資 屏縣府挨告

民視新聞 民視－2012年12月27日 下午5:06

屏東有民眾因為反對在高屏溪畔興建殯葬專區，組成自救會，沒想到9月間參加第一次環評會議時，成員留下的身分證字號、地址等個人資料，全部被屏東縣政府公佈在網站上，自救會成員因此對縣長曹啟鴻提出告訴，求償200萬，屏東縣政府也因此成為個資法實施後挨告的首例。

這是今年6月底，屏東縣長曹啟鴻主持殯葬專區的說明會時，混亂的場面，當時自救會成員情緒激動，還一度站上椅子表達意見，隨後9月間，縣政府召開環評說明會。

圖 1-3：2012 年 12 月 27 日新聞報導

資料來源：民視新聞

如圖 1-4 所示，2015 年 5 月 29 日新聞報導，丹堤咖啡網站因駭客入侵，造成 5000 筆會員個資外洩，該公司是將網站委託其他資訊公司代管，然而委外公司未將資訊安全作好，造成公司聲譽損失，是公司與委外資訊廠商雙輸的局面。

丹堤被「駭」 5000筆會員個資外洩

民視新聞 民視 – 2015年5月29日 下午9:02 -A +A

相關內容

丹堤被「駭」 5000筆會員個資外洩

國內知名的丹堤咖啡，傳出駭客入侵，共5000筆會員個資外洩，被PO到俄羅斯不知名的網站，今天（29日）丹堤出面道歉，表示已和俄羅斯網站連絡，請求把資料下架，並說明是代管的鉅潞科技公司把關出了紕漏，丹堤將會對消費者負起責任。

到丹堤吃早餐喝咖啡，想要更優惠，加入會員，以為可以省更多，但沒想到，卻爆發個資外洩，5000筆會員資料全都露，而且資訊還出現在俄羅斯的網站，丹堤後知後覺，19天後才發現！

丹堤咖啡副總徐恒鈞：「針對這次駭客入侵的狀況，我們對於代管網站的公司，沒有辦法在資訊安全上面，為消費者把關，我們表達非常大的歉意。」

圖 1-4：2015 年 5 月 29 日新聞報導

資料來源：民視新聞

如圖 1-5 所示，2015 年 6 月 2 日新聞報導，日本國民年金機構遭駭客社交工程手法，內部員工開啟有毒電子郵件，導致 125 萬筆大量個資外洩。由本新聞顯示個資保護，不單只是網站系統或資料庫，內部員工的行為也佔很大的因素，所以要做好個資保護，需要資訊安全的協助才行。

圖 1-5：2015 年 6 月 2 日 IThome 新聞

資料來源：http://www.ithome.com.tw/news/96364

如圖 1-6 所示， 2015 年 6 月 10 日新聞報導，永豐銀行因人員操作錯誤，寄錯近 2 萬筆客戶個資，嚴重影響客戶權益，遭金管會開罰 400 萬元。所以要做好個資保護，不僅是系統上要做好資安防護，人員更要做好教育訓練，避免因認知不足或操作錯誤，造成公司名譽受損或財務賠償。

圖 1-6：2015 年 6 月 10 日自由時報新聞

資料來源：http://news.ltn.com.tw/news/business/breakingnews/1344275

如圖 1-7 所示，2015 年 7 月 11 日新聞報導，美國人事總局網站系統疑似遭中國大陸駭客入侵，導致 2000 多萬筆個人資料外洩，嚴重影響國家安全，事後局長強調會再加強網路安全。

超大量個資外洩 美國聯邦人事總局長下台

推薦 3

中廣新聞網 – 2015年7月11日 下午2:09

駭客入侵，導致二千多萬件個人資料外洩，美國政府人事總局長、也是歐巴馬的親信阿庫利塔女士今天遞出辭呈，立即得到歐巴馬同意。不過，白宮仍然拒絕承認駭客來自中國大陸。（劉芳報導）

阿庫利塔女士（Katherine Archuleta）領導的美國聯邦人事總局（Office of Personnel Management），不久前遭到駭客入侵，多達420萬筆的個資外洩。接下來再度遭到駭客入侵，外洩的個資更高達2千多萬筆，包括聯邦人員的健康及財務狀況、他們的家人、朋友的資料等。

圖 1-7：2015 年 7 月 11 日中廣新聞

資料來源：http://www.bcc.com.tw/newsView.2607868

從以上案例可知，網站系統因管理不當，或資安防護沒作好，肇生個資外洩情事，影響個資當事人權益。尤其個資法上路後，政府部門或企業若沒有做好資安防護導致個人資料外洩，很可能因此吃上法律責任，資訊部門通常難卸其責。

於是，坊間出現了 PIMS(個人資料管理系統)作法，如 BS10012、TPIPAS…等，但是要面對資安問題又要面對個資問題，分別導入 ISMS 與 PIMS，所花費的時間與經費、人力負荷，是大多組織或企業不願去承擔的難題。

1.2. 研究動機

身為政府部門資訊人員，在組織改造人員精簡的情況下，同時須肩負各項行政業務資訊化工作，以僅有的資訊能量來面對不斷增加的資訊系統維管與資安防護，加上個資法實施，個資管理問題，實難各系統面面俱到，達到資訊安全政策與個資法要求。

本研究試想有沒有一套方法可以完成IT人員宏觀性的面對這些問題?IT人員除了在資訊安全技術上的研究，如：防火牆技術、電子商務安全、資料加解密、系統安全、程式撰寫...等方法，仍須有一個全方面的管理作法，才能提升資訊安全與個資保護水準。

在尋尋覓覓各種管理作法，試找出一套可以真正符合 IT 人員的作業基準，又可以針對本國個資法要求達到良善的資訊安全與個資保護具體作法。從產官學各界發現，在產業界 SGS 全球產品經理呂敏誠提出[1]：PIMS 與 ISMS 的整合其實很簡單，只要找到其中的差異點，再把它加到現有的管理系統中即可；在政府官方行政院研考會主任吳啟文[2]也提出：目前政府 A、B 級單位已經有 80%取得 ISMS 認證，將個資保護相關作法整併至 ISMS 中，會是比較理想的作法；學者黃小玲(99)的個資法及 ISO 27001 共通性與操作概述有提及[3]：現今，在政府大力推動資通安全的策略下，大部分政府機關皆已了解資訊安全之重要性；如何在這個框架下，加強個人資料之保護，可以讓整個資訊安全管理系統(ISMS)更加成熟，且可降低觸法之可能性。

本論文花費 3 年時間，尋尋覓覓尋找可以根本且有邏輯、有方向、全方面解決資安與個資問題,ISMS 與 PIMS 整合便是最好的解決之道。運用 ISMS 與 PIMS 整合後實施，各界也都有相同的看法，可有效管控資訊安全與個人資料，可符合個資法等相關法規要求，可以省下人力負荷與經費，可以保護網站系統永續發展。

1.3. 研究目的

ISMS 與 PIMS 管理作法，各界都認同可以整合，但是沒有一個可具體整合的方法與有效具體作法,本研究也藉由研究手法與試著以資料的生命週期,資訊安全的機密性、完整性、可用性，PDCA 模式...等角度進行本質上探討，與研究方法進行整合 ISMS(資訊安全管理系統) 與 PIMS(個人資訊管理系統)，降低管理複雜度，藉由單位實作驗證可行性，將實作經驗與方法供資訊能量有限之政府機關或中小型企業有所參考，達到最基本資安與個資保護要求，大幅降低個資外洩風險，確保資訊系統機密性、完整性、可用性。

本論文主要價值在於：1.突破先前專家學者研究盲點，如：建議整合但不知怎麼作整合、列舉一些可整合作法但很零碎不知本質、無實際提出有效具體作法與導入…等，首次提出 ISMS 與 PIMS 整合方法。2.整合後提出 4 點有效的具體作法，可有效實施整合工作。3.將整合後方法實際導入現有網站，有效解決資安與個資問題，導入過程可供有意作好資安與個資保護 IT 人員參考。

對產官學各界貢獻：1.產業界可減少重複投資與節省經費。2.政府官方可減少人力工作負荷與遵循法規。3.學術界首次進行 ISMS 與 PIMS 整合之研究，提出整合方法與 4 點有效具體作法。

1.4. 研究範圍與限制

本研究針對國防部網站系統進行ISMS及PIMS整合導入,未涵蓋整個機關或組織，因此適用於資訊能量或經費不足之機關、組織、企業採用其精神藉以參考依循。

1.5. 論文架構

本論文架構共分為五章，各章內容簡述如下：

第一章緒論：說明本研究背景及動機、研究目的、研究範圍與限制、論文架構。

第二章文獻探討：進行文獻探討的回顧，首先了解何謂 ISMS 與 PIMS，以及依循之規範 ISO 27001、本國個資法，了解資安與個資保護的精神與本質。

第三章研究方法：試著從多角度探討整合可行性，並進行多面性整合工作，提出 4 點有效具體作法。

第四章實作：運用 ISMS 與 PIMS 整合後作法，以國防部全球資訊網站系統為個案實作對象，根據第三章整合方法，進行專案整合導入工作，將整個實作過程一一記載，供需求組織或企業參考，最後以現有 ISO27001 標準包含個資管理流程來驗證此作法。

第五章結論與貢獻：發現整合後作法經 ISO 國際標準驗證通過，將研究與實作貢獻進行總結，以及後續研究方向建議。

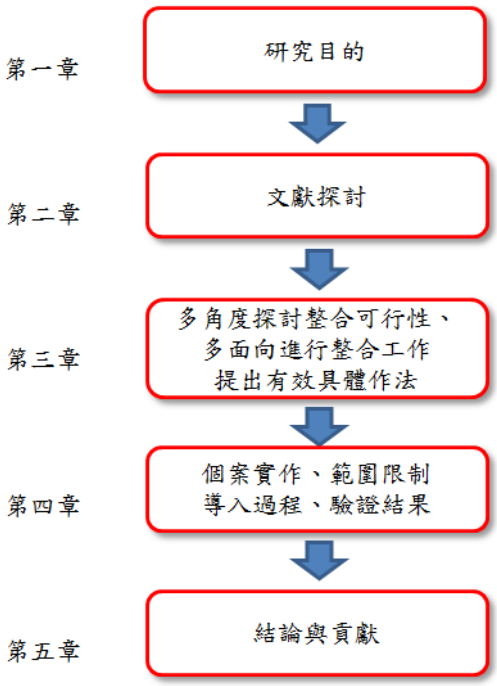

圖 1-8：本研究步驟

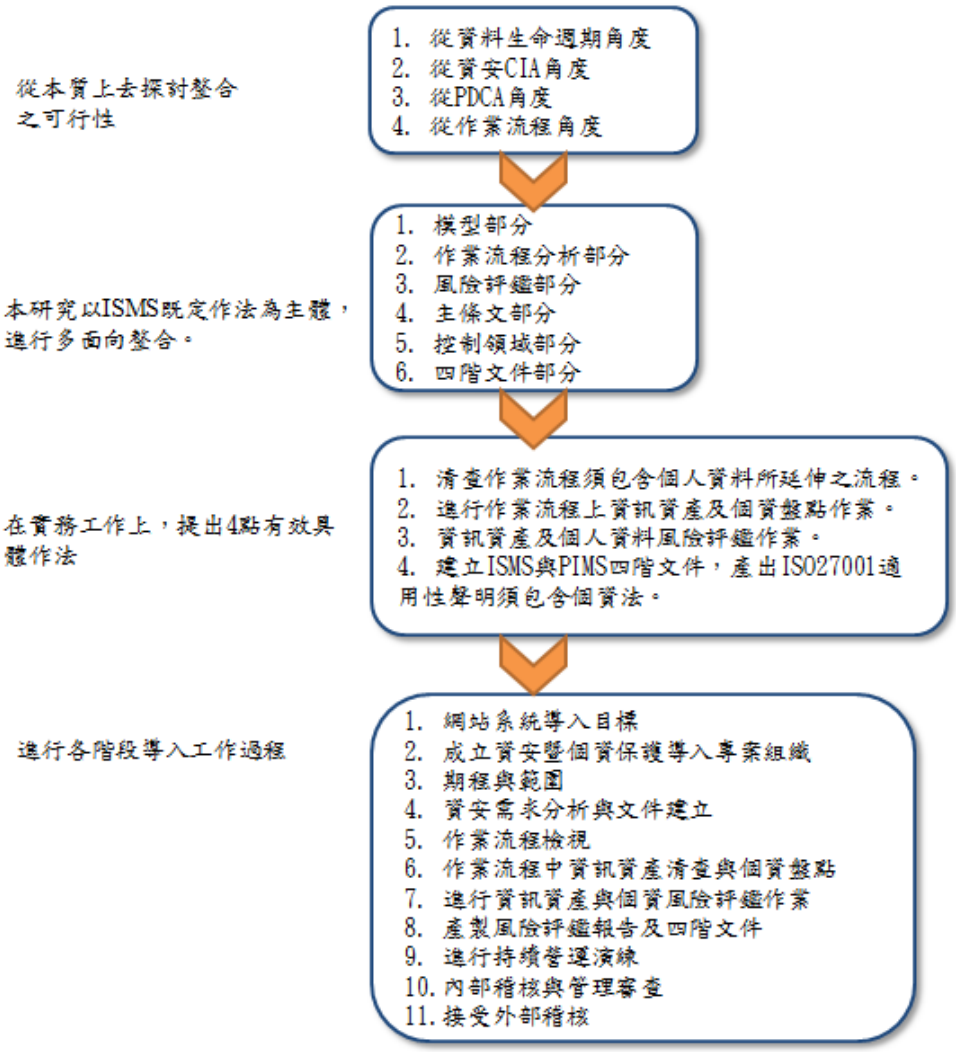
從本質上去探討整合之可行性
1. 從資料生命週期角度
2. 從資安CIA角度
3. 從PDCA角度
4. 從作業流程角度
本研究以ISMS既定作法為主體，進行多面向整合。
1. 模型部分
2. 作業流程分析部分
3. 風險評鑑部分
4. 主條文部分
5. 控制領域部分
6. 四階文件部分
在實務工作上，提出4點有效具體作法
1. 清查作業流程須包含個人資料所延伸之流程。
2. 進行作業流程上資訊資產及個資盤點作業。
3. 資訊資產及個人資料風險評鑑作業。
4. 建立ISMS與PIMS四階文件，產出ISO27001適用性聲明須包含個資法。
進行各階段導入工作過程
1. 網站系統導入目標
2. 成立資安暨個資保護導入專案組織
3. 期程與範圍
4. 資安需求分析與文件建立
5. 作業流程檢視
6. 作業流程中資訊資產清查與個資盤點
7. 進行資訊資產與個資風險評鑑作業
8. 產製風險評鑑報告及四階文件
9. 進行持續營運演練
10. 內部稽核與管理審查
11. 接受外部稽核

圖 1-9：本研究方法論

2. 文獻探討

本章旨在說明本研究主題相關的文獻探討，共分為六節。2.1 節介紹資訊安全管理系統-ISMS；2.2 節介紹個資保護管理系統-PIMS；2.3 節介紹管理系統模型-MSS；2.4 介紹 ISO 27001 國際標準；2.5 節說明風險評鑑；2.6 節進行本章小節。

2.1. 資訊安全管理系統-ISMS

2.1.1. 資訊安全

資訊是一種資產對組織營運而言是不可或缺，面對各種外在威脅與本身脆弱點，需要進行適當保護。

資訊安全是使資訊不受各種廣泛威脅之保護，降低資訊系統營運風險，確保營運的持續性。資訊安全經由實作一套適當的控制措施達成，包括政策、過程、程序、組織結構及軟硬體功能，必要時須建立、實作、監視、審查與改進這些控制措施，以確保達成組織的特定安全與營運目標。

資訊安全主要為確保資訊的以下三項特性：

- 機密性(Confidentiality)：資訊不可被未經授權的個人、實體或流程取得或揭露。
- 完整性(Integrity)：保護資訊及資產的準確度(Accuracy)與完全性(Completeness)。
- 可用性(Availability)：經授權的個體在需要時可以存取或使用資訊及相關資產。

  除此之外，資訊安全亦同時涉及資訊的鑑別性(Authenticity)、可歸責性(Accountability)、不可否認性(Non-repudiation)與可靠度(Reliability)。

對於任何造成資產損害的潛在可能性稱為威脅(Threat)，威脅利用脆弱性造成對資產、組織和系統的傷害和損毀。資訊安全的威脅一般可分為兩大類：

- 環境威脅(天災)：天然災害，例如：火災、颱風和地震等；或是系統故障，例如：網路設備異常、硬碟故障和線路中斷等。

- 人為威脅(人禍)：又可分為人為疏失與蓄意破壞。人為疏失大多來自於內部人員，主要為系統操作不慎、不當使用習慣(濫用電子郵件、任意下載檔案)與管理鬆散等；蓄意破壞則可能來自於內部人員與外部人員，主要為內部人員竊取公司資料、離職員工挾怨報復、駭客入侵與商業間諜等。

資訊安全是一個管理過程而非技術過程，必須永無止境的不斷調整與改善，以「資訊安全管理」為核心加以整合「資訊安全技術」層面，在組織或單位內架構一套專屬且適用的資訊安全管理機制與策略，因應管理資訊系統所面臨的資訊安全風險，以控制與降低資訊安全事件所帶來的威脅與衝擊。[4]

2.1.2. 資訊安全管理系統

資訊安全管理系統（Information Security Management System，簡稱 ISMS）為一套有系統地分析和管理資訊安全風險的方法，要達到100%的資訊安全是一種過高的期望，資訊安全管理的目標是透過控制方法，把需要被保護的資訊資產風險降低到可接受的程度內，並且採用風險管理方法、控制目標、控制方法、以及所需要的安全保證程式。一般常見之實施 ISMS 六大步驟為：(1)定義政策(Define the Policy)；(2)定義範圍(Define the Scope of the ISMS)；(3) 進行風險評估（Undertake a Risk Assessment ）；(4) 風險管理(Manage the Risk)；(5)選擇要實行的控制目標及控制方法(Select Control Objective and Control to be Implemented)；(6)準備適用性聲明(Prepare a Statement of Applicability)等，形成一個程序化的安全管理系統，並運用 PDCA 模式來不斷改善 ISMS，如圖 2-1 所示 [4]。

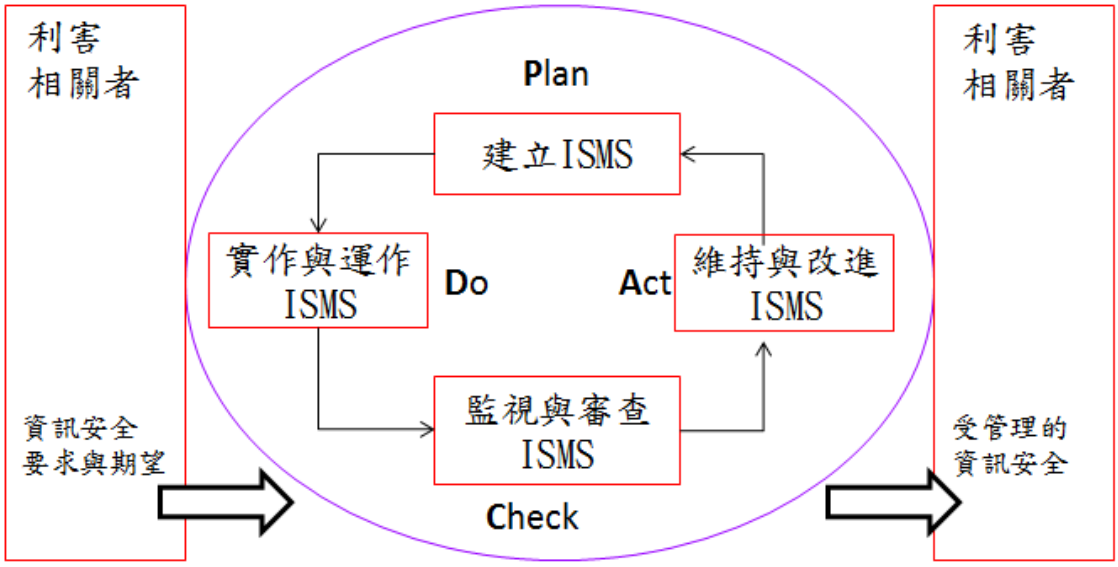

圖 2-1：PDCA 過程模式運用於資訊安全管理系統

資料來源：ISO 27001：2005 Standard

PDCA 模式於資訊安全管理系統所代表的含義如下：

(1) Plan－規劃建立 ISMS：建立與管理風險及改進資訊安全相關的資訊安全管理系統政策、目標、過程及程序，以產生與組織整體政策和目標一致的結果。

(2) Do－實作與運作 ISMS：實作與運作資訊安全管理系統的政策、控制措施及程序。

(3) Check－監督與審查 ISMS：依據資訊安全管理系統政策、目標及實際經驗，評鑑及量測實行績效，並將結果回報給管理階層審查。

(4) Action－維持與改進 ISMS:基於資訊安全管理系統稽核與管理階層審查結果，或其他相關資訊採取矯正與預防措施，以達成資訊安全管理系統的持續改進。又組織應針對可能違反法規的事件，在事先實施預防的行動，並評估可能造成的問題，以決定與採取必要的預防措施。另針對管理階層審查的結果，對於不

符合政策與標準要求的事項，應進行矯正的行動，以將資安風險降至最低。

2.2. 個資保護管理系統-PIMS

2.2.1. 個人資料保護法

我國於民國 84 年 8 月 11 日公布施行「電腦處理個人資料保護法」，此法係參照 OECD 隱私網領的保護資料 8 大基本原則所制定，其立法目的在於避免人格權受侵害及促進資料之合理利用。隨著時代變遷，陸續納入其他與「電腦處理」個人資料相關之非公務機關行業，然而原法規已諸多不合時宜，又缺乏管理及稽核層面足夠的配套措施，因此，法務部為加強保護個人資料之隱私性，並促進資料之合理運用及與國際接軌，自民國 90 年起廣徵各界意見及蒐集國外相關法例，並採認 APEC 隱私保護綱領九大原則，研擬完成修法，並將新法更名為「個人資料保護法」，於 99 年 4 月 27 日於立法院三讀通過，於 99 年 5 月 26 日以總統令公布。另法務部於 101 年 9 月 26 日依「個人資料保護法」第五十五條規定訂定「個人資料保護法施行細則」，於 101 年 10 月 1 日正式施行[5]。

2.2.2. 個資保護管理系統

本研究泛指的 PIMS（Personal Information Management System，PIMS）為廣義針對個資保護的具體管理系統的作法，非專指英國隱私標準 BS 10012：2009 Standard 條文中的 PIMS，在本研究利用現有 BS 10012 的管理框架來介紹，運用 PDCA 循環模式（如圖 2-2）來建立維護個人資訊管理系統（PIMS），讓各組織能維持和改善對資料保護法律及優良實踐的遵循。

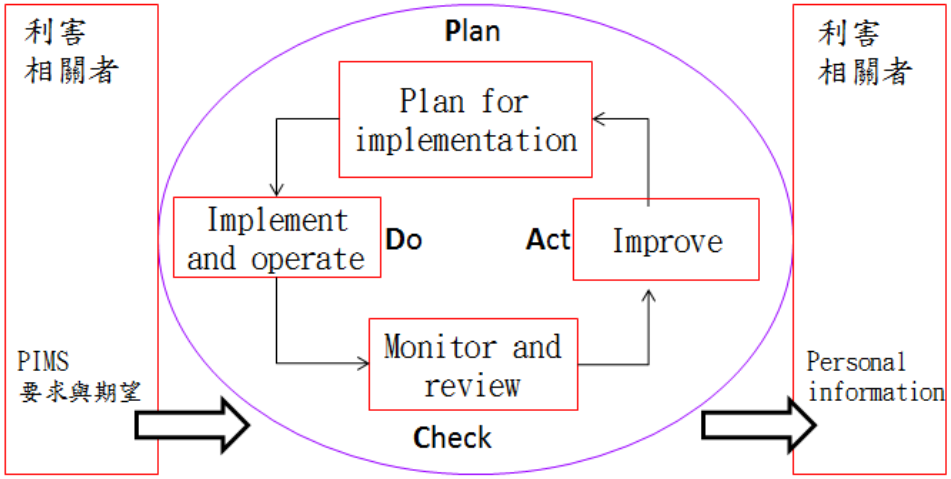

圖 2-2：PDCA 過程模式運用於個人資訊管理系統

資料來源：BS 10012：2009 Standard

PDCA 在個人資訊管理系統所代表的含意如下：

(1) Plan－規劃建置 PIMS：組織必須定義個人資訊管理的範圍和目標，並判斷內部有哪些資料屬於個人資訊，以制訂適合組織運作的個人資訊管理政策。

(2) Do－實作與運作 PIMS：確保組織已指派適當的負責人選推動並執行個人資訊管理制度，並透過各個單位負責代表的協助，進行個人資訊的風險評鑑，以評估目前組織所擁有及處理個人資訊的風險等級。此外，要求組織對員工實施教育訓練，確保個人資訊被公平且合法的處理使用，以及採取適當的資訊安全控制措施，皆為此階段的重點工作。

(3) Check－監督與審查 PIMS：組織除了必須制定稽核計畫，選擇合適的稽核人員依照政策與管理要求定期實施稽核作業外，還須定期舉行管理階層審查會議，了解個資處理的過程是否有任何的變動，並審查稽核後的結果。而對於是否發生和個資相關的資安事件亦應加以了解，以掌握組織推動個資的現況，並適時修訂個資管理政策。

(4) Action－維持與改善 PIMS：組織應針對可能違反法規的事件，事先實施預防的行動，並評估可能造成的問題，採取必要的預防措施；其次則是針對管理階層審查的結果，針對不符合政策與標準要求的事項，進行矯正的行動，以求將個資管理不當的風險降至最低。

2.2.3. 相關個資保護作法

BS10012：英國標準協會（BSI）於 2009 年 6 月公告 BS 10012 個人資訊管理標準。BS 10012 的全名為「資料保護-個人資訊管理系統之要求」（Data protection－Specification for a personal information management system），本標準具體說明了對個人資訊管理系統（Personal Information Management System，PIMS）的各項要求。根據 BS 10012 的規範，不論是國家或企業組織，都應該有一個專責的個資管理單位，負責個資的收集、使用、傳遞、銷毀和保存。且不論是國家或組織，都應該要事先定義出一份「個資類別清單」，清楚定義哪些是單位內所收集的個資範圍，釐清並界定哪些資料該被保護，以及各種個人資料被保護的層級，並對各資訊流清楚掌握，以設置各個控管機制來管控個人資料出入口，為個資保護的框架。BS 10012 的 8 大資料保護原則如下：

(1) 受到公平合法的處理。

(2) 僅限核於特定目的之取得，且不會進行不符合特定目的之後續處理。

(3) 適當、相關且不過度。

(4) 正確且最新。

(5) 保存期限不超過必要期限。

(6) 依據法律授與個人權利進行處理，包含標的存取權 。

(7) 確保安全。

(8) 不會在未受到適當保護的情況下，被移轉到歐洲經濟區以外的國家。

BS 10012 標準共有 7 章，第 0~2 章為標準介紹及適用範圍與名詞定義之說明，

第 3~6 章則為個人資訊管理制度的架構要求。BS 10012 相關條文彙整如表 2-1。

表 2-1：BS 10012 標準條文彙整

編號	條文大綱
0	前言 Introduction
0.1	個人資訊管理系統 Personal information management system
0.2	資料保護原則 Data protection principles
0.3	告知 Notification
1	範圍 Scope
2	名詞、定義與縮寫 Terms, definitions and abbreviations
2.1	名詞與定義 Terms and definitions
2.2	縮寫 Abbreviations
3	規劃個人資訊管理系統(PIMS)Planning for a personal information(PIMS)
3.1	個人資訊管理系統的建立與管理 Establishing and managing the PIMS
3.2	個人資訊管理系統的範圍與目標 Scope and objectives of the PIMS
3.3	個人資訊管理政策 Personal information management policy
3.4	政策內容 Policy content
3.5	職責與責任承擔 Responsibility and accountability
3.6	資源提供 Provision of resources
3.7	將 PIMS 深植於組織文化 Embedding the PIMS in the organization’s culture
4	實行與運作個人資訊管理系統（Implementing and operating the PIMS）
4.1	重要人員之指派 Key appointments

編號	條文大綱
4.2	識別並記錄個人資訊的用途 Identifying and recording uses of personal information
4.3	訓練與意識 Training and awareness
4.4	風險評估 Risk assessment
4.5	維持最新的個人資訊管理系統 Keeping PIMS up-to-date
4.6	告知 Notification
4.7	公平合法地處理 Fair and lawful processing
4.8	為具體指明的目的處理個人資訊 Processing personal information for specified purposes
4.9	適當、相關且不過度 Adequate, relevant and not excessive
4.10	正確 Accuracy
4.11	保留與處置 Retention and disposal
4.12	個人的權利 Individuals’ rights
4.13	安全議題 Security issues
4.14	將個人資訊移轉到國（境）外的地方 Transfer of personal information outside the EEA
4.15	對第三方揭露資訊 Disclosure to third parties
4.16	外包處理 Sub-contracted processing
4.17	維護 Maintenance
5	監督與審查個人資訊管理系統（Monitoring and reviewing the PIMS）
5.1	內部稽核 Internal Audit
5.2	管理階層審查 Management review

編號	條文大綱
6	改善個人資訊管理系統 Improving the PIMS
6.1	預防與矯正措施 Preventive and corrective actions
6.2	持續改善 Continual improvement

資料來源：BS 10012：2009 Standard

TPIPAS：台灣個人資料保護與管理制度（Taiwan Personal Information Protection and Administration System；TPIPAS）緣起於經濟部商業司委託財團法人資訊工業策進會，執行「電子商務個人資料管理制度推動計畫」，規劃並推動「臺灣個人資料保護與管理制度（TPIPAS）」，並於 2013 年起擴大適用至所有行業別，亦適用於公務機關。於 2012 年 09 月 04 日公告 **TPIPAS:2012**。相關條文彙整如表 2-2。

表 2-2：TPIPAS 管理制度條文彙整表

編號	條文大綱	內容
0	**前言**	
0.1	**概述**	臺灣個人資料保護與管理制度規範(Taiwan Personal Information Protection and Administration System, TPIPAS)(以下稱「本制度規範」)是使事業以「PDCA 方法論」，建立一套將個人資料保護與事業營運連結之系統化管理制度。
0.2	**訂定目的**	本制度規範旨在提升事業對於個人資料之保護與管理能力，降低營運風險，並創造可信賴之個人資料保護及隱私環境。
0.3	**用途**	本制度規範係對於事業之個人資料管理制度進行內、外部評量及用以核發事業「資料隱私保護標章」(Data Privacy Protection Mark, DP Mark)之依據。
0.4	**PDCA 方法論**	本制度規範之架構以「計畫-執行-檢查-行動(Plan-Do-Check-Act)，PDCA 方法論」為基礎。說明如下： (1)計畫：建立個人資料保護管理政策、目標及相關程序。 (2)執行：個人資料管理制度之實施。 (3)檢查：依據個人資料保護管理之政策、目標及要求，評估與監督流程及其產出，並將結果回報給最高管理階層加以審查。 (4)行動：採取措施，以持續改善個人資料管理制度之績效。
1	**適用範圍**	本制度規範係針對蒐集、處理、利用及國際傳輸個人資料之事業，訂定相關規範事項，以建立個人資料管理制度，確保個人資料之安全。

2	**版本標示**	事業引用本制度規範，應註明所引用版本。若未註明者，則指使用最新版本。
3.	**用語與定義**	本制度規範用詞，定義如下：
3.1	**個人資料管理制度**	指事業針對所持有個人資料所訂定之政策、內部管理組織及其規則、風險管控措施、應變處理程序及教育訓練計畫之整體管理體系。
3.2	**個人資料**	指包含自然人姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。
3.3	**當事人**	指透過個人資料得以識別之本人。
3.4	**事業**	指法人或非法人團體。
3.5	**個人資料管理代表**	指最高管理階層指派管理階層之一，就事業內部個人資料管理制度之運作具有監督管理權責之人。
3.6	**個資管理人員**	實際推動並確保個人資料管理制度之有效運作之人員。
3.7	**事業人員**	指受事業直接監督，包括正職、派遣及其他與事業保有個人資料之蒐集、處理或利用有關之從業人員。
3.8	**事故**	指事業之個人資料外洩、滅失、毀損、竄改及其他侵害；或其他違反個人資料保護相關法令或本制度規範之情事。
4	**要求事項**	
4.1	**一般要求事項**	事業應依其規模、特性及本制度規範之具體要求，建立、實施與維持其個人資料管理制度，並持續改善，以維護其有效性。
4.2	**個人資料保護管理政策**	事業應將其內部保有及管理個人資料之依據、目的與事業所負責任等基本理念原則，以書面訂定並對事業人員加以公開周知。
4.3	**個人資料保護管理手冊**	事業為建置個人資料管理制度，應製作個人資料保護管理手冊，訂定具體規則，並提出有效方式維持機制運作，供事業依循使用。

		具體規則內容至少包括： (1) 識別法令與其他相關規範。 (2) 識別事業所保有之個人資料。 (3) 事業蒐集、處理或利用個人資料之事宜。 (4) 個人資料相關之風險分析及管控措施。 (5) 事故緊急應變。 (6) 事業各部門以及層級所擁有個人資料管理權限與責任。 (7) 當事人權利之行使。 (8) 維持個人資料正確性。 (9) 安全管理措施。 (10) 事業人員之監督與獎懲。 (11) 委託蒐集、處理或利用個人資料之監督。 (12) 教育訓練。 (13) 個人資料管理制度之文件與紀錄管理。 (14) 當事人申訴及諮詢。 (15) 內部評量。 (16) 矯正及預防措施。 (17) 最高管理階層定期檢視。
4.4	**個別要求事項**	4.4.1 識別法令及其他相關規範事業應識別所須遵循之相關法令，明示其個人資料管理制度與國家個人資料保護相關法規在內容及執行面上之相符性，並依法令之變動進行調整。 4.4.2 納入管理之個人資料範圍事業應識別其保有之個人資料檔案，及蒐集、處理、利用個人資料之流程，劃定其納入個人資料管理制度之範圍，建立並維護個人資料檔案清冊及流程說明。 4.4.3 風險管控措施事業應就納入管理範圍之個人資料，識別事業因蒐集、處理、利用個人資料可能面臨的風險，視需求訂定管控措施。 4.4.4 資源管理事業應提供並維持個人資料管理制度所需之人力及軟硬體資源，確保相關資源管理之實施、維持及改善方式之有效性，並就資源管理事項留存相關紀錄。 4.4.5 權限與責任分工事業應以書面明定個人資料管理

		制度之相關人員之職務、職掌、選任方式、責任層級及權限內容，並向事業內部公開周知。 4.4.6 事故之緊急應變為避免事故可能產生之不利益及影響，事業應訂定事故緊急應變措施。相關措施應至少包括： (1) 查明後以適當方式通知當事人事故發生，並提供後續查詢與處理管道。 (2) 防止事業所受損害擴大之方法。 (3) 避免類似事件再次發生之方法。 (4) 將事故通報授證機關。
4.5	**管理制度之實施**	4.5.1 基本原則事業應確保個人資料之蒐集、處理、利用或國際傳輸，以誠實信用方式進行，出於最小且未逾越特定目的之必要範圍，並與蒐集之目的具有正當合理之關聯。 4.5.1.1 蒐集 事業針對個人資料之蒐集程序應符合下列要求： (1) 確認蒐集時具備特定目的，並符合法律規定之特定情形。 (2) 其他法令規定蒐集時應履行之義務。 (3) 保存前二款相關紀錄。 4.5.1.2 處理 事業為建立或利用個人資料檔案，針對個人資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結及進行內部傳送，其程序應符合下列要求： (1) 確認處理時符合蒐集時之特定目的及特定情形。 (2) 其他法令規定處理時應履行之義務。 (3) 事業應訂定適當且合法程序，處理刪除暨銷毀及業務終止時事業所保有之個人資料。 (4) 保存前三款相關紀錄。 4.5.1.3 利用 事業對於個人資料之利用程序應符合下列要求： (1)於蒐集之特定目的必要範圍之內利用個人資料。 (2)目的外利用個人資料時係屬合乎法律要求。 (3) 保存前二款相關紀錄。 4.5.1.4 行銷

		事業針對利用個人資料進行行銷，其程序應符合下列要求： (1) 提供當事人至少首次免費表示拒絕接受行銷之方式。 (2)當事人可隨時拒絕接受行銷之管道，並於表示拒絕接受後，立即停止利用其個人資料為行銷之用途。 (3) 保存前二款相關紀錄。 4.5.1.5 特種個人資料之蒐集、處理及利用限制 事業針對醫療、基因、性生活、健康檢查、犯罪前科等特種個人資料，其程序應符合下列要求： (1)內部人員原則禁止蒐集、處理及利用特種個人資料之要求。 (2)例外得蒐集、處理或利用特種個人資料時，係屬合乎法律要求。 (3)保存前二款相關紀錄。 4.5.1.6 告知義務之履行 事業針對個人資料保護法規定之應告知事項，應建立告知程序暨免告知之確認程序，其內容至少符合下列要求： (1) 符合個人資料保護相關法律之告知時點。 (2) 適當之告知方式。 (3)針對免告知之理由及其確認方式。 (4) 保存前三款相關紀錄。 4.5.2 當事人之相關權利 4.5.2.1 個人資料之相關權利 事業應訂定當事人申請查詢、閱覽、補充、更正、製給複製本、停止蒐集、停止處理、停止利用、刪除其個人資料，以及申訴與諮詢之規則與流程並保存相關紀錄。 4.5.2.2 當事人行使權利之程序事項 事業為處理 4.5.2.1 之當事人請求之程序，內容至少符合下列要求： (1) 具備當事人提出請求之方式。 (2) 具備確認當事人身分之方式。 (3) 具備確認事業是否得依法拒絕當事人行使其權利。 (4) 具備拒絕請求或發生爭議，當事人得提出申訴之管道與聯繫方式。 4.5.2.3 提供查詢、閱覽、複製本之方式

		事業針對當事人請求查詢、閱覽個人資料或製給個人資料複製本，其程序應符合下列要求： (1) 確保於 15 日內為准駁之決定。 (2) 准駁當事人請求，拒絕時並應附理由以書面通知當事人。 (3) 決定延長 15 日作出准駁之決定時，應附理由以書面通知當事人。 (4) 保存前三款相關紀錄。 4.5.2.4 當事人請求個人資料補充、更正、刪除、停止蒐集、處理及利用程序 事業針對當事人請求補充、更正、刪除、停止蒐集、處理或利用個人資料，其程序應符合下列要求： (1) 確保於 30 日內為准駁之決定。 (2) 准駁當事人請求，拒絕時並應附理由以書面通知當事人。 (3) 決定延長 30 日作出准駁之決定時，應附理由以書面通知當事人。 (4) 保存前三款相關紀錄。 4.5.2.5 申訴及諮詢之處理 針對申訴與諮詢事項，事業應確保迅速有效之處理，其程序應符合下列要求： (1) 適當且迅速回應當事人。 (2) 視申訴與諮詢內容，必要時應通報個資管理代表，並由其決定回應之內容與方式。 (3) 保存前二款相關紀錄。 4.5.3 管理監督 4.5.3.1 維持個人資料之正確性 事業為維持個人資料正確之狀態，應建立符合下列要求之程序： (1) 確保個人資料於處理過程中，正確性不受影響。 (2) 當確認個人資料有錯誤時，應適時更正。 (3) 檢查個人資料之正確性。 (4) 因可歸責於事業之事由，未為更正或補充之個人資料，應訂定於更正或補充後，通知曾提供利用對象。 4.5.3.2 安全管理措施 事業應針對因蒐集、處理及利用個人資料所可能面臨之

		風險，採取防止個人資料外洩、滅失、毀損、竄改及其他侵害之必要且適當之安全管理措施。 必要且適當之安全管理措施應至少包括： (1) 作業面安全管理措施 (2) 物理性安全管理措施 (3) 技術性安全管理措施 4.5.3.3 事業人員之監督 事業應對事業人員就個人資料蒐集、處理及利用採取必要且適當之監督措施。 4.5.3.4 委託蒐集、處理或利用個人資料之監督 事業委託他人蒐集、處理或利用個人資料之全部或一部時，應建立選任受託人之標準及其監督方式，並確認以下事項： (1) 委託人及受託人之權利義務。 (2) 委託蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 (3) 受託人對個人資料之安全管理措施。 (4) 有複委託者，所約定之受託人及複委託之範圍；嗣後複委託者，應得委託人同意。 (5) 向委託人報告關於個人資料處理狀況之內容以及報告週期。 (6) 委託人對受託人保留指示之事項。 (7) 發生事故時向委託人即時報告及採行之補救措施等相關事項。 (8) 委託關係終止或解除時，個人資料載體之返還，及儲存於受託人持有個人資料之刪除。 (9) 受託人僅得於委託人指示之範圍內，蒐集、處理或利用個人資料。受託人認委託人之指示有違反本法或基於本法所發布之命令規定之情事，應立即通知委託人。 委託人應定期確認受託人執行之狀況，並將確認結果紀錄之。
4.6	**教育訓練**	4.6.1 一般要求事業應以適當方式確保事業人員對個人資料管理具有正確的認知及能力。 4.6.2 基本教育訓練事業針對事業人員應提供必要的個人資料管理教育訓練。

		4.6.3 權責人員教育訓練事業應決定個人資料管理制度相關權責人員之必要能力與教育訓練需求，並規劃與執行。 4.6.4 成果維持及改善措施事業應針對事業人員教育訓練成果建立紀錄與改善機制。
5	**管理責任**	
5.1	**最高管理階層**	最高管理階層之責任應包括： (1) 決定個資保護管理政策 (2) 決定資源管理 (3) 決定個資保護管理組織架構及權責劃分 (4) 定期檢視管理制度 (5) 建立有效的溝通機制
5.2	**管理代表**	最高管理階層應指派管理階層成員之一，擔任個人資料保護制度管理代表，其應有之責任與職權包括： (1) 負責維持個人資料管理制度運作之有效性，並建立必要內部人員結構。 (2) 確保職務執行過程之公正性與客觀性。 (3) 確保個人資料管理制度所需的各項程序被建立、實施與維持。 (4) 向最高管理階層報告個人資料管理制度之實施成效與改善措施。
5.3	**個資管理人員**	事業應由取得下列資格之一者，擔任個資管理人員，以實際推動並確保個人資料管理制度之有效運作： (1) 個人資料管理師。 (2) 個人資料內評師。 (3) 個人資料驗證師。 個資管理人員得由個資管理代表兼任。
6	**有效性量測**	事業應針對個人資料管理制度之實施，建立分析量測機制，藉由使用各項方式，使管理代表能判定個人資料管理制度內所建立之程序與機制是否有效，將所進行之分析量測作成紀錄，以確保制度之持續有效運作。
7	**文件及紀錄之控管**	

7.1	**文件及紀錄之範圍**	7.1.1 文件事業應製作及保存下列文件： (1) 個人資料保護管理政策。 (2) 個人資料保護管理手冊，及其相關具體規則。 (3) 個人資料內部管理程序相關表單。 7.1.2 紀錄 事業應製作及保存實施個人資料管理制度之相關紀錄。
7.2	**文件管理**	事業為落實個人資料管理制度，應建立文件管理程序，其程序包含： (1) 文件之製作及修正之相關事項。 (2) 明確標記文件修正時,與前次版本間之關聯及差異。 (3) 文件之儲存位置與保存方式及其存取權限。
7.3	**記錄管理**	事業為落實且證明其已符合本制度所要求之事項，應製作必要之紀錄文件並確立實施相關之管理程序。
8	**內部評量**	事業每年應依其特性規劃執行內部評量，以瞭解個人資料管理制度是否符合下列要求： (1) 符合法規及本制度之要求。 (2) 符合個人資料保護管理政策、手冊及相關具體規則之要求。 事業應規劃內部評量方式及流程，以決定內部評量之準則、範圍、頻率及方法。 事業應將內部評量之規劃、執行、報告、改善、追蹤等事項製作書面之內部評量報告。 內部評量應由具備個人資料內評師或個人資料驗證師資格者執行，並由其出具內部評量報告。
9	**改善**	9.1 定期檢視個資管理代表為落實個人資料保護管理,應每年定期召開檢視會議，召集相關權責人員，檢視個人資料保護管理制度，以書面紀錄檢視結果，並報告最高管理階層。 定期檢視會議應檢視下列事項並提出檢視報告： (1) 個人資料管理制度執行狀況及其分析。 (2) 矯正及預防措施之成效。 (3) 有效性量測之結果。 (4) 個人資料處理之相關法令以及其他相關規範之修改

		狀況。 最高管理階層決策調整個人資料管理制度時，應考量以下事項，並據以調整與修正個人資料管理制度： (1) 檢視報告。 (2) 社會情勢、國民認知、技術發展等各種環境之變遷。 (3) 事業業務領域之變化。 (4) 事業內外部之改善建議。 (5) 其他可能影響個人資料管理制度的任何變更。 9.2 矯正及預防措施事業針對內部評量及本管理制度實施之結果，應規劃矯正措施及預防措施，並確保相關措施之執行。 9.2.1 矯正措施事業針對不符合事項，應規劃及完成執行矯正措施，並完成以下事項： (1) 確認不符合事項之內容並判定其發生原因。 (2) 評估需求並提出矯正方案，以確保不符合事項不再發生。 (3) 訂定合理之執行期限。 (4) 紀錄執行結果。 (5) 檢視所採取的矯正方案成果。 9.2.2 預防措施事業針對潛在不符合事項之風險，應規劃及執行預防措施時，並完成以下事項： (1) 依據事業因持有個人資料可能面臨的風險，確認各項潛在不符合事項之內容及其原因。 (2) 評估需求並提出預防方案，以確保不符合事項不發生。 (3) 訂定合理之執行期限。 (4) 紀錄執行結果。 (5) 檢視所採取的預防方案成果。

資料來源：[6]

在普遍 PIMS 實務作法中，BS10012 為英國隱私標準，其中個人資料法制規範與環境之不同，相關制度無法直接移植供國內使用。

然而 TPIPAS 僅針對本國個資法條文訂定管理制度，難以透過國際標準認證(如：

ISO27001)；個人資料相關法制規範主要係維護個人對於其資料的資訊自主，仍需要資訊系統安全之協助。

但現有資訊安全管理系統，並不完全符合遵循我國個資法之要求，透過本研究將 ISMS 與 PIMS 整合，是較全面性的作法，也可以較低資安與個資管理制度導入成本。

2.3. 新版管理系統標準-MSS

在第三章運作模型整合部分會介紹到 MSS，本章節先介紹 MSS 管理系統標準，讓讀者可以更清楚了解。

國際標準組織(International Standardization for Organization，簡稱 ISO)自 2000 年起即分 3 階段進行管理系統標準(Management System Standards，簡稱 MSS)之標準化工作項目，期能在 2015 年完成各個管理系統要求事項的調合，新版 ISO/IEC 27001 標準系列已遵循 MSS 建立[7]。

國際標準組織為使管理系統要求事項之「一致性」，以符合社會大眾的利益，於 2001 年先行出版 ISO Guide 72 (Guidelines for the justification and development of management system standards)作為準備[8]，並在 2008 年至 2012 年於能源管理(Energy Management)為標的試行[9]。ISO 技術管理委員會(Technical Management Board，簡稱 TMB)主責的管理系統標準(Management System Standards，簡稱 MSS)於 2010 年已完成第 2 階段之共同用語(Term)與核心定義(Core Definitions)的標準化作業，ISO/IEC 27001 新版亦遵循[10][11][12][13][14]。

目前 TMB 提出之 MSS 規範所有管理系統要求事項(例：ISO 9001、ISO 14001、ISO 27001、ISO 28001、ISO 50001 等)的至次節之高階結構(High Level Structure)，其章節如後：

(1) 第 1 章：適用範圍(Scope)。

(2) 第 2 章：引用標準(Normative references)。

(3) 第 3 章：用語釋義(Terms and definitions)。

(4) 第 4 章：組織全景(Context of the organization)。

(5) 第 5 章：統御力(Leadership)。

(6) 第 6 章：規劃(Planning)。

(7) 第 7 章：支持(Support)。

(8) 第 8 章：運作(Operations)。

(9) 第 9 章：績效評估(Performance evaluation)。

(10) 第 10 章：改進(Improvement)。

(11) 資料來源：：ISO/IEC JTC1/SC27 N7616:2009-04-23，附錄 B。

新版管理系統標準 MSS 已由原本 PDCA 模型修正為圖 2-3 模型，已對原本 ISMS 實作性產生直接的衝擊，在實作上統御力佔導入成功關鍵因素，除了領導每位參與同仁，也在溝通協調上佔很大的關鍵因素，尤其在跨部門的溝通與協調，消除本位主義，在實務上是相當困難的工作。

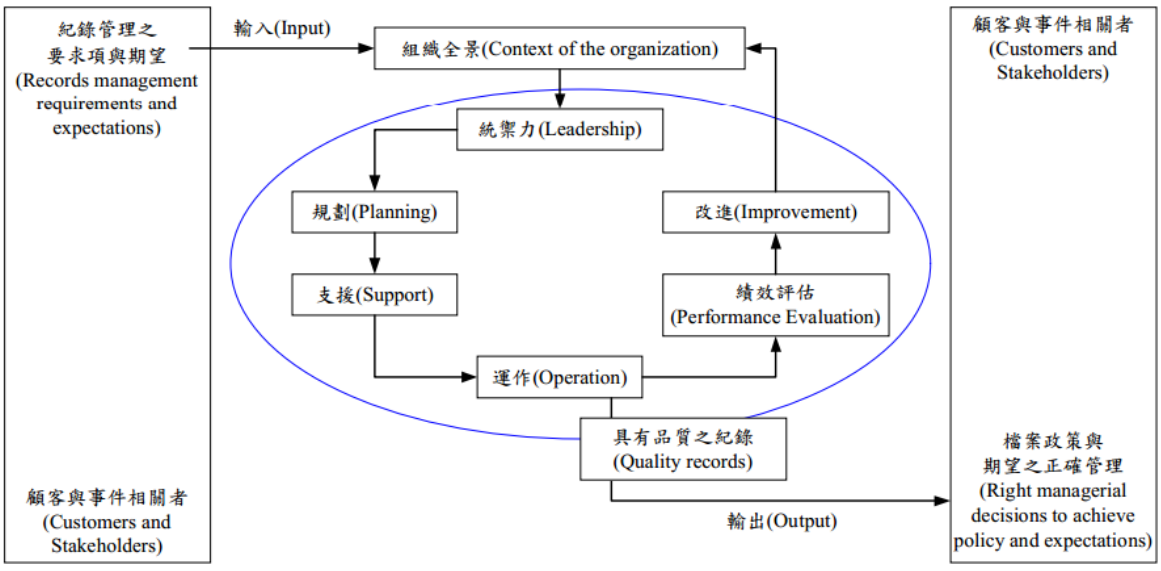

圖 2-3：根基於過程導向之管理系統的紀錄模型

資料來源：[15]

2.4. 新版 ISO 27001:2013 國際標準

ISO/IEC 27001 即本研究主題之 ISO 27001，為資訊安全管理的標準，源自於英國國際標準 BS 7799 Part-2:2002，英國標準協會於 2005 年公布新版之 BS 7799 Part-2:2005，國際標準組織於 2005 年 10 月 14 日將 BS 7799 Part-2:2005 編納為 ISO 27001，是目前國際公認最完整的資訊安全管理標準，其規範安全內容涵蓋：建立、實施、操作、監督、審查、維持與改善資訊安全管理系統(Information Security Management System，ISMS)。國際標準組織於 2013 年 10 月 1 日 ISO 年會中，正式推出新改版的資安認證標準 ISO 27001：2013，這也是 ISO 27001 自從 2005 年正式成為國際標準之後的首次改版。

2005 年版本和 2013 年版本的主要差異，除了內容更加明確律定外，附錄 A 的控制措施更符合實務工作進行，最主要是執行 ISMS 的有效性，特別將管理階層的領導力凸顯出來，並強調設定目標、績效量測與展現。

27001：2013 新版本為了更符合資訊安全的現況及需求，由原先 ISO 27001:2005 的 A.5 至 A.15（11 個領域，39 項目標及 133 項控制措施）變成 A.5 至 A.18（14 個領域，35 項目標，114 項控制措施）控制目標減少了 4 項，控制措施由原本的 133 個變成 114 個。領域變多了，控制目標及控制措施都減少了。且 2013 年版本新增了兩個領域分別是 A.10 密碼(Cryptography)領域與 A.15 供應商關係(Supplier Relationships)領域，並將原本 A.10 通訊與作業管理(Communications and operations management)領域分成 A.12 作業安全(Operations Security)與 A.13 通訊安全(Communications Security)兩個領域[16]。

表 2-3：ISO 27001:2005 與 ISO 27001:2013 比較表

2005 年版本條款			2013 年版本條款		
0.	簡述 Introduction		0.	簡述 Introduction	
1.	範圍 (Scope)		1.	範圍 (Scope)	
2.	引用標準 (Normative references)		2.	引用標準 (Normative references)	
3.	用語釋義 (Terms and definitions)		3.	用語釋義 (Terms and definitions)	
4.	資訊安全管理(Information security management) system	(Plan)	4.	組織全景(Context of the organization)	(Plan)
	-		5.	領導力 (Leadership)	(Plan)
	-		6.	規劃 (Planning)	(Plan)
	-		7.	支援 (Support)	(Plan)
5.	管理階層責任(Management responsibility)	(Do)	8.	運作 Operation	(Do)
6.	ISMS 內部稽核(Internal ISMS audits) (Check)			-	
7.	ISMS 之管理審查（Management review of the ISMS ）	(Check)	9.	績效評估(Performance evaluation)	(Check)
8.	ISMS 之改進 (ISMS improvement)	(Act)	10.	改進(Improvement)	(Act)

資料來源：[17]

ISO 27001 標準條文如表 2-4，分為簡介、適用範圍、引用標準、用語及定義、組織全景、領導作為、規劃、支援、運作、績效評估、改善等 10 節以及附錄 A.5~A.18 控制目標及控制措施，控制措施架構如圖 2-4 所示。

表 2-4：ISO 27001 標準條文彙整

編號	條文大綱
0	簡介
1	適用範圍
2	引用標準
3	用語及定義
4	組織全景
4.1	瞭解組織及其全景
4.2	瞭解關注方之需要及期望
4.3	決定資訊安全管理系統之範圍
4.4	資訊安全管理系統
5	領導作為
5.1	領導及承諾
5.2	政策
5.3	組織角色、責任及權限
6	規劃
6.1	因應風險及機會之行動
6.2	資訊安全目標及其達成之規劃
7	支援
7.1	資源
7.2	能力
7.3	認知
7.4	溝通或傳達
7.5	文件化資訊
8	運作
8.1	運作之規劃及控制
8.2	資訊安全風險評鑑
8.3	資訊安全風險處理
9	績效評估
9.1	監督、量測、分析及評估
9.2	內部稽核
9.3	管理審查
10	改善

編號	條文大綱
10.1	不符合項目及矯正措施
10.2	持續改善
附錄 A	A.5 資訊安全政策~~ A.18 遵循性

資料來源：ISO 27001：2013 Standard

圖 2-4：ISO 27001:2013 控制領域

資料來源：本研究自行整理

本研究為使讀者更能了解 ISO 27001:2013，以圖 2-5 架構來明確指出各條文要求在整個 ISMS 實際運作上 PDCA 所展現的流程位置，在一開始導入 ISMS 時，在第 4 條組織全景部分，組織應了解相關利益團體或個人需求與期望，及決定 ISMS 範圍。外圈為管理階層所要進行之工作項目，內圈為執行編組所要進行之工作項目，均運用 PDCA 循環運作模式；領導階層運用第 5 條領導作為，下定決心進行 ISMS 實施，執行部門進行第 6 條 ISMS 規劃及風險管控之行動，並依規劃進行第 8 條運作，在這之前管理階層需進行第 7 條進行賦予適當權力與支援，透過第 9 條進行組織績效評估，了解組織各項績效與內部缺失與風險所在，最後進行第 10 條各項改善工作，ISMS 進行當中可利用附錄 A 控制目標及控制措施明確了解工作項目並進行控制風險作業。

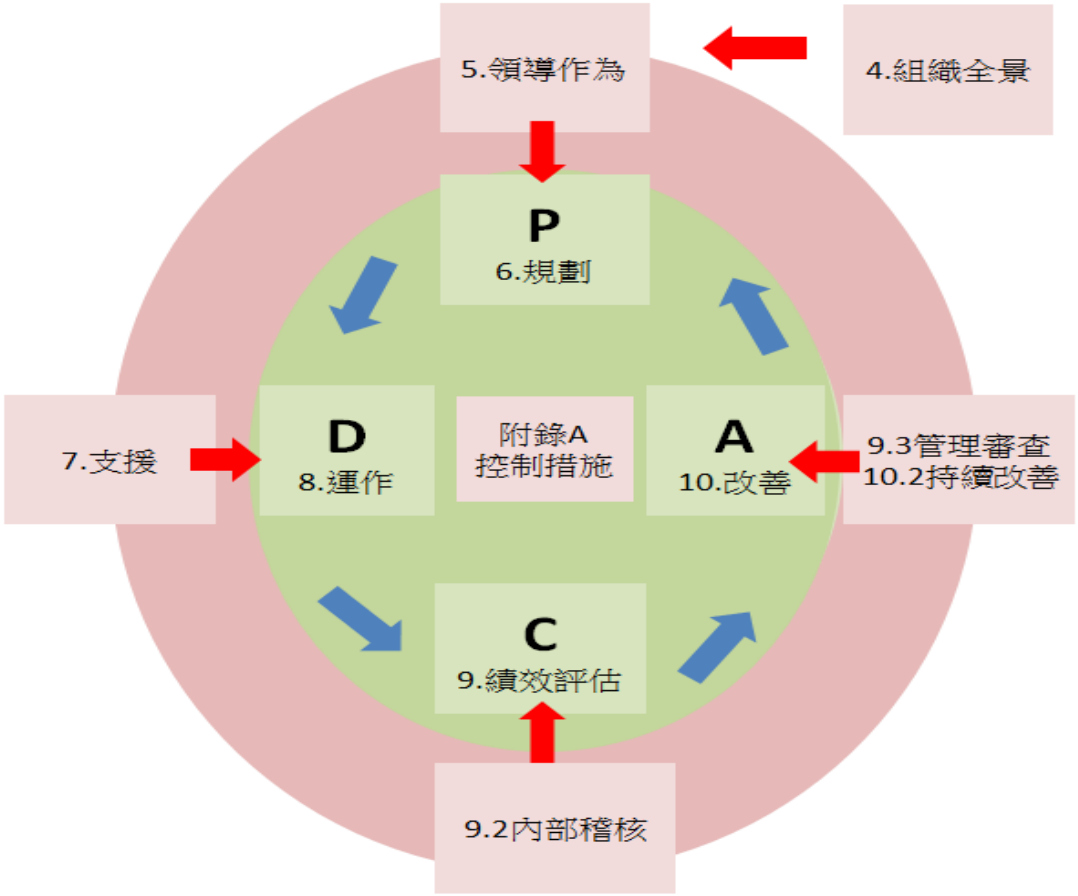

圖 2-5：ISO 27001:2013 架構

資料來源：本研究自行整理

2.5. ISO27005 風險評鑑

在 ISMS 整體運作中，ISO27005 最不可或缺的風險管理方法論，風險評鑑是建構資訊安全管理系統的重要環節，風險管理可以分成兩個部份，第一部份，就是風險評鑑，根據資訊安全管理系統範圍內的資產，評鑑其風險等級。第二部份，就是針對高風險資產作風險處理，降低其風險，使其一旦發生風險時，仍然在可以接受的範圍內。

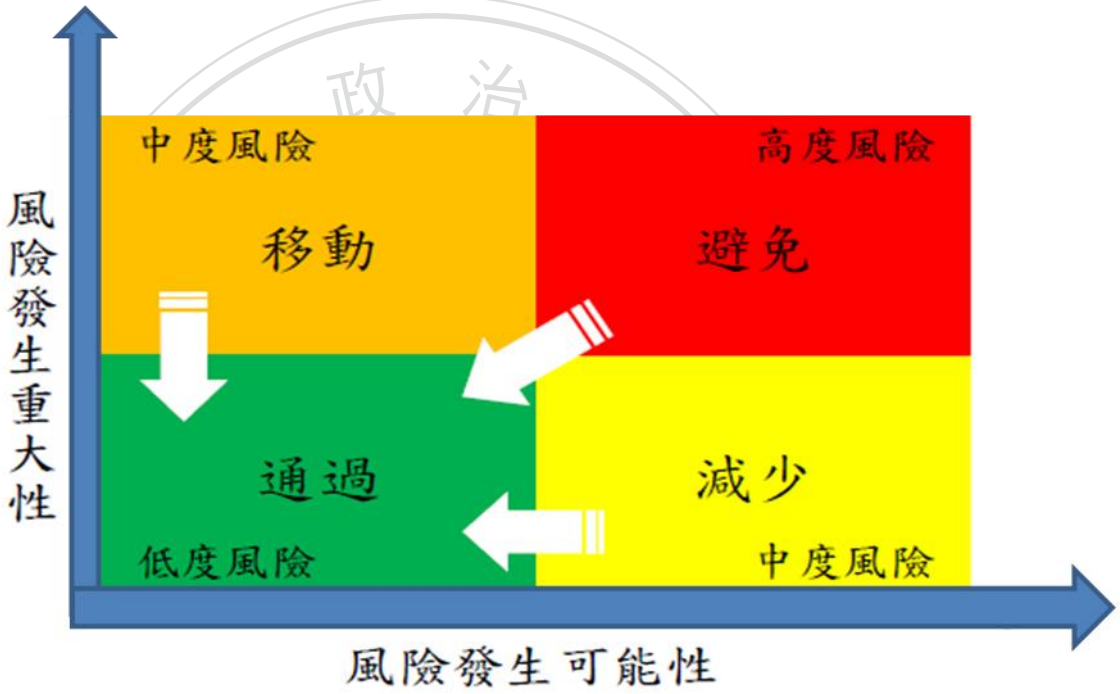

圖 2-6：風險程度關係圖

資料來源：本研究自行整理

2.5.1. 風險評鑑

資訊安全風險評鑑結果，對於 ISMS 的建置有決定成敗重要影響因素，風險評鑑透過分析組織業務流程資訊資產的重要程度(機敏性、完整性、可用性)、潛在的外部威脅、自身可被利用的弱點發生的機率以及現有的控制措施來決定組織的各項資訊資產風險

值，風險評鑑計算方式如下：

- 風險值 = 資產價值 × 破壞事件嚴重程度
- 資產價值 = 機密性評價 + 完整性評價 + 可用性評價
- 破壞事件嚴重程度 = 威脅等級 × 脆弱點等級 × 衝擊等級
- 風險可能性 = 發生機率 / 目前實施狀況

所謂資產價值的評價，就是分別針對機密性評價、完整性評價和可用性評價，加總以求得其總體的資訊資產價值。如以下式子表示:

- 資產價值 = 機密性評價 + 完整性評價 + 可用性評價

機密性、可用性和完整性的評價可以根據標的資產有不同的定義，見表 2-5，但是基本的精神是相同的，以下，我們將就設備資產價值定義為例。

表 2-5：機密性，完整性，可用性評價參照

評價	機密性	完整性	可用性
1	不限制使用之資訊處理設施與系統資源等。	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。	工作日之上班時間至少25%的時間有權限的人可存取資訊系統與資源。
2	非公開使用之非敏感性資訊處理設施與系統資源為者。	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。	工作日之上班時間至少50%的時間有權限的人可存取資訊系統與資源。
3	敏感性資訊處理設施與系統資源，僅開放給必要知道的人使用。	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。	工作日之上班時間有權限的人都可存取資訊系統與資源。
4	敏感性之資訊處理設施與系統資源，僅開放給極少數必要知道的人使用。	不當的損失、破壞資訊處理設施與系統資源，會對業務應用造成很大的衝擊，甚至會造成業務失敗。	工作日(24 小時)，至少95%的時間有權限的人可存取資訊系統與資源者。

資料來源：[18]

要評價破壞事件的嚴重程度，我們就必須要分別對該資產去考量可能的威脅等級評價(系統被攻擊的頻率)，見表 2-6，面對威脅該資產的脆弱點等級評價(系統被攻擊的容易度)，見表 2-7，和該威脅發生時對組織所造成的衝擊等級評價(系統被攻擊所造成的影響程度)，見表 2-8 。同時定義破壞事件嚴重程度如下公式:

● 破壞事件嚴重程度 = 威脅等級 × 脆弱點等級 × 衝擊等級

表 2-6：威脅等級評價表

威脅等級評價	說明(外部威脅有可能危害資訊資產)
1	威脅來源缺乏動機而且能力不足
	防制脆弱性被利用的安全對策有效
	不太可能發生（沒有發生過，但是有發生的可能）
2	威脅來源缺乏動機且能力不足
	防制脆弱性被利用的安全對策有效
	發生頻率低（平均每年發生的次數不到一次）
3	威脅來源有動機也有能力
	防制脆弱性被利用的安全對策有效
	有可能發生（平均每年都可能發生一次以上）
4	威脅來源有強烈的動機與足夠的能力
	防制脆弱性被利用的安全對策無效
	時常發生（平均每月都可能發生一次以上）
5	威脅來源有強烈的動機與足夠的能力
	防制脆弱性被利用的安全對策無效
	發生頻率非常高（平均每週都可能發生一次以上）

資料來源：[18]

表 2-7：脆弱點等級評價表

脆弱點等級評價	說明(本身有弱點，容易遭外部威脅所利用)
1（低）很難被利用	1. 必需運用特殊的方法才能利用脆弱點進行攻擊
	2. 威脅來源必須花費長時間(可能需一個月以上)的資料收集, 突破各層防護, 才能接觸到關鍵資訊
	3. 攻擊成功:可能要1~數個月
2（中）	1. 不需用特殊的方法就能利用脆弱點進行攻擊;

被利用難度適中	2.已實施保護的機制,威脅來源必須花費一段時間(可能是數天)進行資料收集即能接觸到關鍵資訊
	3.攻擊成功:可能是數天以上
3（高） 很容易被利用	1.利用簡易的方法就能利用脆弱點進行攻擊
	2.未實施保護或保護機制無效,威脅來源於短期內即可攻擊成功
	3.攻擊成功:可能是一天內到數天

資料來源：[18]

表 2-8：衝擊等級評價表

衝擊等級評價	說明
0 （可忽略）	1.對於業務執行沒有影響;
	2.可以立即完成復原
1 （微弱）	1.對於業務執行沒有影響;
	2.可以立即完成復原
	3.若持續發生且次數頻繁,對業務執行可能帶來潛在風險
2 （輕微）	1.對於公司整體業務執行影響不大;
	2.造成的損失可能僅影響單一業務或系統;
	3.損失可能影響僅個人或少數幾人;
	4.可以由個人進行復原;
	5.修復或進行復原的措施可以在很短時間(1小時)內完成
3 （嚴重）	1.對於公司整體業務執行造成損害;
	2.造成的損失可能影響多種業務或數個系統;
	3.損失可能影響多個部門或合作夥伴;
	4.復原的措施必須由專業人員才能進行;
	5.復原可能要數個小時~到一天才能完成
4 （癱瘓）	1.公司整體業務執行造成損害;
	2.事件處理不當可能對公司形象造成損害;
	3.造成的損害可能影響全公司;
	4.系統或相關服務停頓或癱瘓,業務無法運作;
	5.合作夥伴或客戶失去信心;
	6.復原的措施僅能由特定專業人員才能進行或修復人員不易取得;
	7.復原無法於一天才能完成;
	8.可能造成人員傷亡

資料來源：[18]

最後將總風險值的最大值和最小值相減再分成四個等分，即可得到 4 個風險等級的級距，在組織管理階層的決議，先進行最高等級風險處理，次高等級風險控管或移轉，並面對可接受的風險等級。

2.5.2. 風險處理

經過前面的步驟，作好資訊安全管理系統範圍內的資產盤點和風險等級評鑑後，可以得到資產的風險等級分佈，針對高風險等級的資產作風險處理。風險處理計劃通常包含了 4 個目的：

(1) 消除風險。

(2) 將無法消除的風險，透過控制機制將其降低到可以接受的程度

(3) 如果決定和風險共存，就必須透過謹慎的控制讓風險的發生仍維持在可以接受的範圍。

(4) 或者，用另一種思維，透過保險或簽定維護合約的方式將風險轉移到其他的協力廠商。

但是在加入控制措施後，我們還必須考慮，加入的控制措施是否能夠移除威脅發生的可能,降低威脅所發生的頻率或是降低威脅所造成的衝擊,再依前面風險評鑑的方法，重新作威脅等級評價，脆弱點評價及衝擊等級評價。再去檢視其殘餘風險等級是否在可以接受的風險程度內。如果，還是高於可接受風險等級，就可以增加控制目標以及對應的控制措施，以降低其風險等級。若增加控制目標無法將風險降到可以接受的等級，或是增加控制措施的成本太高時，可以考慮透過保險，將風險轉嫁給保險公司或是維護合約，將風險轉嫁給協力廠商。

2.6. 小結

在前幾節很清楚了解，資訊安全是需要靠[資訊技術]、[管理作法]、[法規標準]來共同維護，如圖 15 所示，資訊安全三層概念圖。

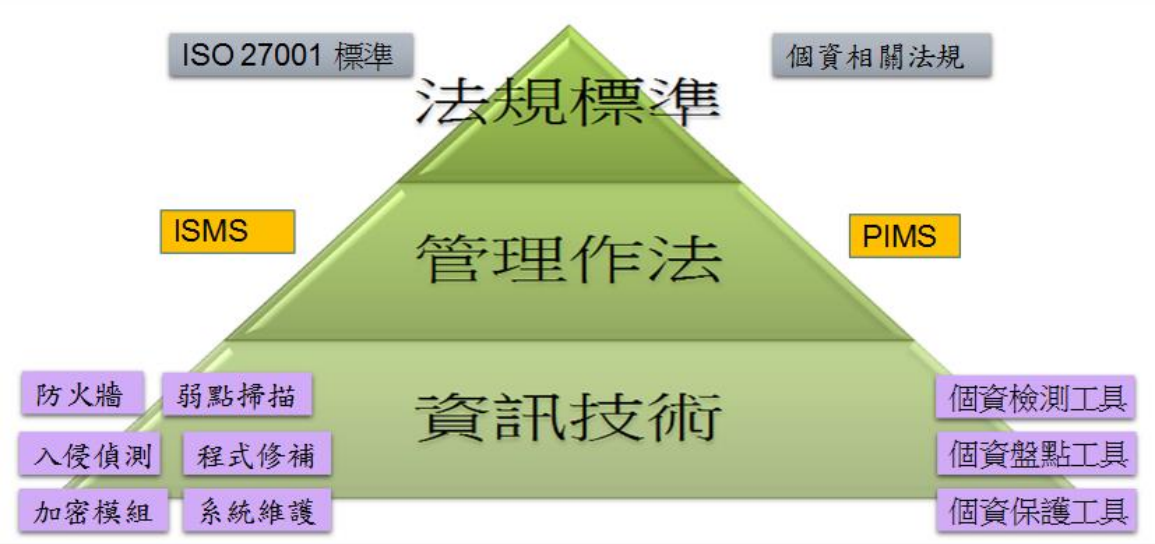

圖 2-7：資訊安全三層概念圖

資料來源：本研究自行整理

以目前國際上最認可的 ISO 27001 標準，及本國政府機關要求的 ISMS 推動，運用各項資訊技術來達到良善控管，是本國現況最能整體提升資訊安全水準的作法。

然而個資法的通過，各式各樣的 PIMS 管理作法出現，ISMS 與 PIMS 分兩次來導入，造成組織增加工作負荷，有疊床架屋情形，成本有部分重複投資現象。

在本章文獻探討，可明顯發現 PIMS 可運用現有的 ISMS 的既定作法，來進行整合，在法規標準方面，ISMS 是採取 ISO27001 標準，PIMS 是採取個資法條文，然而 ISO27001 為組織之一般性資訊安全管理機制，個資法為組織特定性資訊安全管理機制，本研究試著以 ISMS 既有作法將 PIMS 進行整合工作，在法規標準層次，試著以 ISO 27001 國際標準為主體，在條文中法規遵循部分將個資法納入。

3. ISMS 與 PIMS 整合導入之研究

本章旨在說明所採行的研究方法，共分為五節。3.1 節說明各界認同整合之可行性與專家建議；3.2 試從本質上多角度探討整合可行性；3.3 節進行多面向整合工作；3.4 節提出整合後 4 點有效具體作法； 3.5 節進行本章小節。

3.1. 專家認同整合可行性與建議

3.1.1. 認同可整合

現今台灣已經有不少大型公司或政府機關導入 ISMS，為因應個資法實施，這些公司與機關普遍希望將 ISMS 與 PIMS 整合，降低管理複雜度，PIMS 從資料搜集端就開始檢視是否符合法律規範，ISMS 則在資料進入企業後才開始，這是兩者最大的差異，因此，若要在既有 ISMS 作法上整合 PIMS，產業界 SGS 公司呂敏誠先生提出：首要工作就是擬定個資保護的範圍與策略，接下來才是思考如何善用現有的管理系統與機制，將與人有關的資產納入原本 ISMS 作法中。

PIMS 與 ISMS 的整合只要找到其中的差異點，再把它加到現有的管理系統中，舉例來說，ISMS 與 PIMS 都有風險分析作業，然而分析的對象、範圍與深度卻都不相同。’將 PIMS 與 ISMS 整合成一套管理系統，運用其中遵循之標準與條文，結合現今國內個資法，運用 PDCA 流程法驗證，讓管理系統更加符合 IT 部門需求[1]。

3.1.2. 運用既有ISMS作法來整合PIMS

由於新版個資法要求個資保管者應盡善良管理人責任，促使許多企業思考導入個資保護管理制度作為證明，如：BS 10012、ISO 29100、TPIPAS…等，其中 TPIPAS 是經濟部商業司針對 EC 業者而設計，目前尚在起步階段，至於 BS 10012 與 ISO 29100 的差異，TUV NORD 資訊技術事業部經理陳家楨[2]表示，BS 10012 有條文準則與實作框架，唯其參考依據為英國個資法，難免會有在地化差異，而 ISO 29100 並非如此，其強調的

是隱私防護框架，如：角色定義與指派、各角色間的作業互動、如何識別個人資料、隱私保護需求、隱私政策，以及隱私防護原則，如：取得同意、目的、蒐集限制…等。

不過，安侯企管公司協理林義富[2]認為，企業現階段不必急著取得驗證，根據作業流程設計個資管理制度，並加強教育訓練與落實才是重點。無獨有偶地，行政院研考會主任吳啟文[2]也有相同看法，他表示，有沒有取得驗證並不重要，如何落實個資保護才是重點，目前政府 A、B 級單位已經有 80%取得 ISMS 認證，將個資保護相關作法整併至 ISMS 中，會是比較理想的作法。

若只用ISMS既定作法將個資法納入法規遵循，對個人資料保護的深度及廣度而言，仍有所不足。例如，在資產管理目標很重要的一項作業為資訊資產盤點。張芳珍（民93）[19]表示進行資訊資產盤點時必須依據組織及資訊資產的特性決定分類及分級，並在成本效益的考量下，針對各類等級的資訊資產，規劃不同的控管方式。但個人資料於資訊資產盤點作業中，大多歸類於文件及資料，又因目前導入ISMS 之組織，大多以資訊部門及電子資料為範圍，故如非置於資訊部門或書面之個人資料極可能被忽略，而未採取相對應或足夠的保護措施。而又如風險管理，雖劉永禮（民90）[20]強調應建立符合組織的資訊安全風險政策、不斷稽核評估、以適切建立資訊安全風險計畫，不斷循環改正資訊安全環境，但如資產盤點的深度及廣度未涵蓋所有個人資料，則風險評鑑、風險管理計畫等則可能忽略個人資料於各流程中存在的風險，並予以制定適當的管控措施。故本研究試以ISMS 為基礎，進一步就個人資料保護須注意的面向加以強化及整合，則可望以最小成本達事半功倍之效。

3.1.3. 運用ISO 27001 現有框架為基準

專家學者黃小玲(100年)[21]提出個資法與ISO 27001標準有以下幾個共同之重點，值得組織之管理階層考量如何進行整併或解決衝突；1.資產（個資）盤點之實作：如何確認與盤點所有組織內之個人資料。2.背景審查（篩選）之必要性：如何在資訊安全與個

人資料保護兩者之間取得平衡。3.儲存與備份管理：如何確保資料的生命周期已妥善定義與管理。4.存取管理：資料之存取管理如何加強。5.資訊安全事故管理：如何整合事故通報與處置程序。6.遵循性：適法性之必要。

在專家建議上，看的出來，個資法的通過對已取得ISO 27001的驗證者，具有加乘之效。針對涉及個人資料部分可以加強其管理之效度，同時檢視相關之技術配套措施是否足夠。

在鄭伊雯(101年)[5]提及ISO 27001 國際標準乃是為了提供模範以建立、實施、操作、監控、審查、維護及改善ISMS 而準備，而ISMS 之採用必須是組織的策略性決策[20]。因其控制目標包含了資訊安全政策、資訊安全組織、資產管理、人力資源安全、實體與環境安全、密碼學、存取控制、運作安全、通訊安全、供應者關係、資訊系統獲取開發及維護、資訊安全事故管理、營運持續管理之資訊安全層面與遵循性等14 個控制領域，對保護個人資料而言，提供了良好的防護基礎。

3.2. 各角度探討整合可行性

本章節試著從本質上去探討整合之可行性，從資料生命週期角度、資安 CIA 角度、PDCA 角度、作業流程角度來深入了解資訊安全與個資保護之間的相似之處。

3.2.1. 從資料生命週期角度

在本研究試著從資訊作業流程中，資料生命週期來探討與切入，在實務工作上也就能全方面達到資訊安全維護工作，避免只是某角度談論資訊安全；例如 IT 人員只專注在資安設備上的防護，卻往往忽略最機敏資料在老闆電腦，老闆電腦卻遭郵件社交工程被入侵；假設公司的資訊，有 25%資訊以書面文件方式儲存，20%資訊以電子化方式儲存，40%資訊儲存在員工腦袋，那剩下 15%資訊儲存何處?；藉著以作業流程去檢視資訊生命週期各個控制點，較能達到滴水不漏的維護工作。

圖 3-1：資訊作業管理流程資料生命週期

資料來源：本研究自行整理

個人資料保護法的第一章第一條已明定個人資料之蒐集、處理及利用是該法的核心，其實就是組織的「業務流程」中所延伸之「個人資料流程」，參考個資法所要求之個人資料各個階段生命週期(如圖 3-2)，與「業務流程」中所延伸之「資訊作業流程」所產生的資料生命週期(如圖 3-1)，有異曲同工之妙。

圖 3-2：個人資料管理流程個資生命週期

資料來源：本研究自行整理

3.2.2. 從資安 CIA 角度

資訊安全的精神主要為確保資訊的以下三項特性：

- 機密性(Confidentiality)：資訊不可被未經授權的個人、實體或流程取得或揭露。
- 完整性(Integrity)：保護資訊以及資產的準確度(Accuracy)與完全性(Completeness)。
- 可用性(Availability)：經授權的個體在需要時可以存取或使用資訊及相關資產。

然而，個資安全的精神為組織在執行各項工作的[作業流程]中，所延伸出個人資料流程的風險管理機制，包含：

- 保護與維護經授權所限制之個人資料存取及揭發的程度[機密性]。
- 保護個人隱私與私有資訊之手段/方法/工具[機密性]。
- 防範違反不當之個人資料修改/破壞/消滅[完整性]。
- 擔保個人資料之不可否認性與可信賴性[完整性]。
- 擔保個人資料被存取時之及時性與可靠性之程度[可用性]。

3.2.3 從 PDCA 角度

資訊安全管理系統與個人資料管理系統均採 PDCA 管理系統模型，代表在其運作的的原理是相同的，都是利用管理系統的計畫、執行、檢核、改進的程序，不斷改善其管理水準。

3.2.4 從作業流程角度

個人資料保護法的第一章第一條已明定個人資料之蒐集、處理及利用是該法的核心，其實就是組織的「業務流程」中所延伸之「個人資料流程」。

然而，資訊安全的精神為組織在執行各項工作的「作業流程」中，所延伸出資訊流程的風險管理機制，在確保資訊的機密性、完整性、可用性。

不管在資安上所探討的作業流程上所延伸的資訊流程，或者個資所提及的業務流程上所延伸的個資流程，均屬須在作業流程上去進行相關的風險管理機制。

3.3. 進行多面向整合工作

本章節從種種論點，進行多面向整合工作，包含運作模型部分、作業流程分析部分、風險評鑑部分、主條文部分、控制領域部分、四階文件部分去進行整合。

3.3.1 運作模型部分

本研究試著運用新版 MSS 運作模型整合 ISMS 與 PIMS 之 PDCA 運作模型，將資安暨個資管理系統規劃、建置與執行，以遵循「ISO27001 國際標準」及「個人資料保護法」相關規範要求，並輔以 Plan(規劃)、Do(執行)、Check(檢查)、Action(行動)管理循環模式(如圖 3-3)，以企業組織中，所有個人資料蒐集、處理、儲存、使用、銷毀等作業活動與資訊作業流程產生、使用、儲存、傳輸、銷毀作業活動控制點相結合，併同 ISMS 一同進行資訊資產清查時，將個資盤點納入項目之一，進入管理循環模式，評估作業活動中，資訊資產與個人資料之控管風險，建立符合「ISO27001 國際標準」及「個人資料保護法」相關規範之資安暨個資管理制度及文件體系。

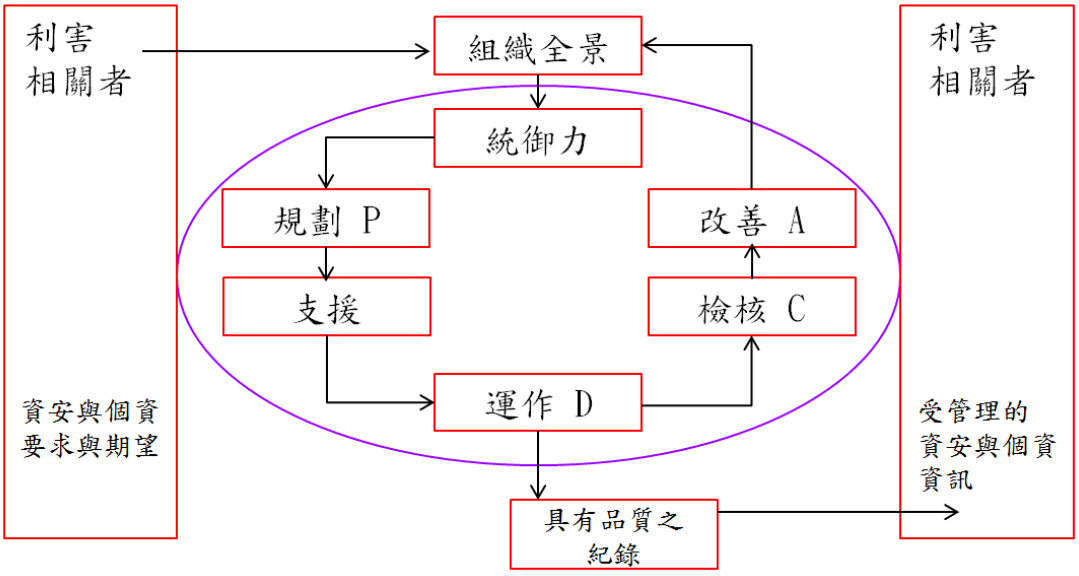

圖 3-3：運用新版 MSS 整合 ISMS 與 PIMS 模型

資料來源：本研究自行整理

3.3.2 作業流程分析部分

從作業流程角度整合切入可以得知，不管在資安上所探討的作業流程上所延伸的資訊流程，或者個資所提及的業務流程上所延伸的個資流程，均屬須在作業流程上去進行相關的風險管理機制。所以組織應在檢視所有作業流程時，須將個資流程納入，避免遺漏,後續資訊資產清查 ISMS 既定作法可結合個資盤點工作,從資料資料生命週期角度，進行各個資料控制點控管，可達滴水不漏的目標。

3.3.3 風險評鑑部分

從資訊安全 CIA(機密性、完整性、可用性)角度切入可以得知，個資安全一樣可以用 CIA 來分級分類。所以運用現有 ISO 27005 風險評鑑作法，鑑別資產價值時，進行 CIA 等級分級分類及風險評鑑作業，整合資訊資產與個人資料項目，並依個人資料敏感性區分 CIA 等級，如特種個資，列為最高評分數值，產出一致化風險評鑑報告，以利於後續規劃因應及處置措施。

表 3-1：資訊資產機密性，完整性，可用性評價參照

評價	機密性	完整性	可用性
1	不限制使用之資訊處理設施與系統資源等。	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。	工作日之上班時間至少25%的時間有權限的人可存取資訊系統與資源。
2	非公開使用之非敏感性資訊處理設施與系統資源為者。	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。	工作日之上班時間至少50%的時間有權限的人可存取資訊系統與資源。
3	敏感性資訊處理設施與系統資源,僅開放給必要知道的人使用。	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。	工作日之上班時間有權限的人都可存取資訊系統與資源。
4	敏感性之資訊處理設施與系統資源,僅開放給極少數必要知道的人使用。	不當的損失、破壞資訊處理設施與系統資源，會對業務應用造成很大的衝擊，甚至會造成業務失敗。	工作日(24 小時)，至少95%的時間有權限的人可存取資訊系統與資源者。

資料來源：[18]

表 3-2：個人資料機密性，完整性，可用性評價參照

評價	機密性	完整性	可用性
1	個人資料所經手之資訊資產喪失機密性後，一旦未經授權存取/使用/進出/洩漏，預計對組織之運作、資產或對當事人影響近可忽略。	個人資料所經手之資訊資產喪失完整性後，一旦資訊不當之修改/改變或破壞/毀滅/消滅，預計對組織之運作、資產或對當事人影響近可忽略。	個人資料所經手之資訊資產喪失可用性後，一旦資訊或資訊系統之存取及使用之崩潰程度，預計對組織之運作、資產或對當事人影響近可忽略。
2	個人資料所經手之資訊資產喪失機密性後，一旦未經授權存取/使用/進出/洩漏，預計對組織之運作、資產或對當事人只有些微不利的影響。	個人資料所經手之資訊資產喪失完整性後，一旦資訊不當之修改/改變或破壞/毀滅/消滅，預計對組織之運作、資產或對當事人只有些微不利的影響。	個人資料所經手之資訊資產喪失可用性後，一旦資訊或資訊系統之存取及使用之崩潰程度，預計對組織之運作、資產或對當事人只有些微不利的影響。
3	個人資料所經手之資訊資產喪失機密性後，一旦未經授權存取/使用/進出/洩漏，預計對組織之運作、資產或對當事人，預計對組織之運作、資產或對當事人有嚴重性或危急性的不利影響。	個人資料所經手之資訊資產喪失完整性後，一旦資訊不當之修改/改變或破壞/毀滅/消滅，預計對組織之運作、資產或對當事人有嚴重性或危急性的不利影響。	個人資料所經手之資訊資產喪失可用性後，一旦資訊或資訊系統之存取及使用之崩潰程度，預計對組織之運作、資產或對當事人有嚴重性或危急性的不利影響。
4	個人資料所經手之資訊資產喪失機密性後，一旦未經授權存取/使用/進出/洩漏，預計對組織之運作、資產或對當事人有劇烈性的或災難性的不利影響。	個人資料所經手之資訊資產喪失完整性後，一旦資訊不當之修改/改變或破壞/毀滅/消滅，預計對組織之運作、資產或對當事人有劇烈性的或災難性的不利影響。	個人資料所經手之資訊資產喪失可用性後，一旦資訊或資訊系統之存取及使用之崩潰程度，預計對組織之運作、資產或對當事人有劇烈性的或災難性的不利影響。

資料來源：[22]

3.3.4 主條文部分

ISMS 既定作法中，所參照的標準(ISO27001 標準)已涵蓋個資法中 11 項安全維護必要措施，只要在最後控制領域 A.18 對法律及契約要求事項之遵循中，納入個資法要求事項即可。

表 3-3：個資法必要措施、個資法、ISO27001、BS10012 對映關係

安全(維護)措施 防止個人資料被竊取、竄改、毀損、滅失或洩漏採取技術上及組織上之必要措施	個資法條文之對應要求	管理面 ISO27001 之對應要求		管理面 BS10012 之對應要求	
一、 配置管理之人員及相當資源。	無	5.1	Leadership and commitment	3.5	Responsibility and accountability
		5.3	Organizational roles, responsibilities and authorities	3.6	Provision of resources
		7.1	Resources	4.1	Key appointments
		A.6.1.1	Information security roles and responsibilities	4.1.1	Senior management
				4.1.2	Day-to-day responsibility for compliance with the policy
				4.1.3	Data protection representatives
二、 界定個人資料之範圍。	第一章 第1條 第一章 第2條	4.1	Understanding the organization and its context	3.2	Scope and objectives of the PIMS
		4.2	Understanding the needs and expectations of interested parties	3.3	Personal information management policy
		4.3	Determining the scope	3.4	Policy content

			of the information security management system		
		5.2	Policy		
		A.5.1.1	Policies for information security		
三、 個人資料之風險評估及管理機制。	無	6.1.1	General	4.4	Risk assessment
		6.1.2	Information security risk assessment	4.13	Security issues
		6.1.3	Information security risk treatment	4.13.1	Security controls
		6.2	Information security objectives and planning to achieve them		
		8.1	Operational planning and control		
		8.2	Information security risk assessment		
		8.3	Information security risk treatment		
			ISO27005		
四、 事故之預防、通報及應變機制。	第一章 第12條	A.16.1.1	Responsibilities and procedures	4.13.6	Managing security incidents
		A.16.1.2	Reporting information security events		
		A.16.1.3	Reporting information security weaknesses		
		A.16.1.4	Assessment of and decision on information security events		
		A.16.1	Response to		

		.5	information security incidents		
		A.16.1.6	Learning from information security incidents		
		A.17.1.1	Planning information security continuity		
		A.17.1.2	Implementing information security continuity		
		A.17.1.3	Verify, review and evaluate information security continuity		
五、 個人資料蒐集、處理及利用之內部管理程序。	第一章 第8條 第一章 第9條 第二章 第15條 第二章 第16條 第三章 第19條 第三章 第20條 第三章 第21條	A.6.2.1	Mobile device policy	4.7.1	Collection and processing of personal information
		A.6.2.2	Teleworking	4.8	Processing personal information for specified purposes
		A.8.1.1	Inventory of assets	4.8.1	Grounds for processing
		A.8.1.2	Ownership of assets	4.13.2	Storage and handling
		A.8.1.3	Acceptable use of assets	4.13.3	Transmission
		A.8.2.1	Classification of information	4.13.4	Access controls
		A.8.2.2	Labelling of information		
		A.8.2.3	Handling of assets		

		A.8.3.1	Management of removable media	
		A.8.3.2	Disposal of media	
		A.8.3.3	Physical media transfer	
		A.9.2.1	User registration and de-registration	
		A.9.2.2	User access provisioning	
		A.9.2.3	Management of privileged access rights	
		A.9.2.4	Management of secret authentication information of users	
		A.9.2.5	Review of user access rights	
		A.9.2.6	Removal or adjustment of access rights	
		A.10.1.1	Policy on the use of cryptographic controls	
		A.13.2.1	Information transfer policies and procedures	
		A.13.2.2	Agreements on information transfer	
		A.13.2.3	Electronic messaging	
		A.14.1.2	Securing application services on public networks	
		A.14.1	Protecting	

		.3	application services transactions		
		A.15.1.1	Information security policy for supplier relationships		
		A.15.1.2	Addressing security within supplier agreements		
		A.15.1.3	Information and communication technology supply chain		
		A.18.1.1	Identification of applicable legislation and contractual requirements		
六、 資料安全管理及人員管理。	無	A.7.1.1	Screening	無	
		A.7.1.2	Terms and conditions of employment		
		A.7.2.1	Management responsibilities		
		A.7.2.2	Information security awareness, education and training		
		A.7.2.3	Disciplinary process		
		A.7.3.1	Termination or change of employment responsibilities		
		A.8.1.4	Return of assets		
		A.9.3.	Use of secret		

		1	authentication information		
		A.11.1.2	Physical entry controls		
		A.11.1.5	Working in secure areas		
		A.12.2.1	Controls against malware		
		A.12.3.1	Information backup		
		A.13.1.3	Segregation in neworks		
		A.13.2.4	Confidentiality or non- disclosure agreements		
		A.18.1.3	Protection of records		
七、 認知宣導及教育訓練。	無	7.2	Competence	4.3	Training and awareness
		7.3	Awareness		
		A.7.2.2	Information security awareness, education and training		
八、 設備安全管理。	無	A.11.2.1	Equipment siting and protection	無	
		A.11.2.2	Supporting utilities		
		A.11.2.3	Cabling security		
		A.11.2.4	Equipment maintenance		
		A.11.2.5	Removal of assets		
		A.11.2	Security of equipment		

		.6	and assets off-premises		
		A.11.2.7	Secure disposal or re-use of equipment		
		A.11.2.8	Unattended user equipment		
		A.11.2.9	Clear desk and clear screen policy		
		A.12.1.3	Capacity management		
		A.12.1.4	Separation of development, testing and operational environments		
		A.12.6.1	Management of technical vulnerabilities		
		A.12.6.2	Restrictions on software installation		
		A.13.1.1	Network controls		
		A.13.1.3	Segregation in neworks		
九、 資料安全稽核機制。	無	9.1	Monitoring, measurement, analysis and evaluation	無	
		A.12.7.1	Information systems audit controls		
		A.15.2.1	Monitoring and review of supplier services		
十、 必要之使用紀錄、軌跡資料及證據之	無	7.5.3	Control of documented information	無	
		A.12.4.1	Event logging		

保存。		A.12.4.2	Protection of log information		
		A.12.4.3	Administrator and operator logs		
		A.12.4.4	Clock synchronisation		
		A.16.1.7	Collection of evidence		
十一、 個人資料安全維護之整體持續改善。	無	9.2	Internal audit	5.1	Internal audit
		9.3	Management review	5.2	Management review
		10.1	Nonconformity and corrective action	6.1	Preventive and corrective actions
		10.2	Continual improvement	6.2	Continual improvement
		A.5.1.2	Review of the policies for information security		
		A.18.2.1	Independent review of information security		
		A.18.2.2	Compliance with security policies and standards		

資料來源：本研究自行整理

3.3.5 控制領域部分

前章節以明確得知，ISO27001 涵蓋個資法對應條文，不足部分，在法規遵循性也可涵蓋。本研究試著將 ISO 27001:2013 之 14 大控制領域擴大解釋，形成包含個資法之控制領域(如圖 3-4)，藉由此控制領域下之控制措施可以確保組織之資訊安全與個資安全。

圖 3-4：ISO 27001:2013 包含個資法控制領域

資料來源：本研究自行整理

3.3.6 四階文件部分

在前章節已明顯分析出，ISO27001 標準已涵蓋個資法中 11 項安全維護必要措施，只要在最後 A.18 對法律及契約要求事項之遵循中，納入個資法要求事項。實務工作上，在 ISMS 運作最後輸出須產出 ISO27001 適用性聲明，如表 3-4；相同地，在 ISMS 與 PIMS 整合後運作輸出必須產出對個人資料保護法適用性聲明，如表 3-5，代表所有文件建立、作業流程、資安管控均符合 ISO27001 及個資法各項要求。

表 3-4：整合後 ISO27001 適用性聲明

ISO/IEC 27001:2013 要求		對應文件	適用性	
			適用	不適用
4	**Context of the organization**			
4.1	**Understanding the organization and its context**	資訊安全風險管理程序	V	
4.2	**Understanding the needs and expectations of interested parties**	資訊安全風險管理程序	V	

4.3	**Determining the scope of the information security management system**	資訊安全手冊	V	
4.4	**Information security management system**	資訊安全手冊	V	
5	**Leadership**			
5.1	**Leadership and commitment**	資訊安全指導委員會	V	
5.2	**Policy**	資訊安全手冊	V	
5.3	**Organizational roles, responsibilities and authorities**	資訊安全指導委員會 各 SOP 之權責要求 職務說明書	V	
6	**Planning**			
6.1	**Actions to address risks and opportunities**			
6.1.1	**General**	資訊安全風險管理程序 資訊資產風險評鑑辦法	V	
6.1.2	**Information security risk assessment**	資訊安全風險管理程序 資訊資產風險評鑑辦法	V	
6.1.3	**Information security risk treatment**	資訊安全風險管理程序 資訊資產風險評鑑辦法	V	
6.2	**Information security objectives and planning to achieve them**	管理階層審查辦法 (年度資安/個資目標)	V	
7	**Support**			
7.1	**Resources**	資訊安全指導委員會	V	
7.2	**Competence**	教育訓練管理程序	V	
7.3	**Awareness**	教育訓練管理程序	V	
7.4	**Communication**	管理階層審查辦法	V	
7.5	**Documented information**			
7.5.1	**General**	文件與紀錄管理程序	V	

7.5.2	Creating and updating	文件與紀錄管理程序	V	
7.5.3	Control of documented information	文件與紀錄管理程序	V	
8	Operation			
8.1	Operational planning and control	所有文件	V	
8.2	Information security risk assessment	資訊安全風險管理程序 資訊資產風險評鑑辦法	V	
8.3	Information security risk treatment	資訊安全風險管理程序 資訊資產風險評鑑辦法	V	
9	Performance evaluation			
9.1	Monitoring, measurement, analysis and evaluation	日常資安工作匯總表 辦公室安全管理辦法	V	
9.2	Internal audit	內部資訊安全稽核程序	V	
9.3	Management review	管理階層審查辦法	V	
10	Improvement			
10.1	Nonconformity and corrective action	矯正與預防程序	V	
10.2	Continual improvement	管理階層審查辦法	V	
A.5	Information security policies			
A.5.1	Management direction for information security			
A.5.1.1	Policies for information security	管理階層審查辦法	V	
A.5.1.2	Review of the policies for information security	管理階層審查辦法	V	
A.6	Organization of information security			
A.6.1	Internal organization			
A.6.1.1	Information security roles and responsibilities	資訊安全指導委員會 各 SOP 之權責要求 職務說明書	V	
A.6.1.2	Segregation of duties	職務說明書	V	
A.6.1.3	Contact with authorities	業務持續運作管理程序	V	

A.6.1.4	**Contact with special interest groups**	行政院資安會報 資安人雜誌 PChome	V	
A.6.1.5	**Information security in project management**	資訊安全風險管理程序 資訊資產風險評鑑辦法	V	
A.6.2	**Mobile devices and teleworking**			
A.6.2.1	**Mobile device policy**	存取控制規範 設備在外地使用的安全管理辦法 使用者註冊管理辦法 資訊處理管理辦法	V	
A.6.2.2	**Teleworking**	存取控制規範 設備在外地使用的安全管理辦法 使用者註冊管理辦法	V	
A.7	**Human resource security**			
A.7.1	**Prior to employment**			
A.7.1.1	**Screening**	員工面談紀錄 承包商及第三方使用者之資料	V	
A.7.1.2	**Terms and conditions of employment**	員工任用相關文件 委外合約	V	
A.7.2	**During employment**			
A.7.2.1	**Management responsibilities**	人事管理規則 各 SOP 中的權責說明	V	
A.7.2.2	**Information security awareness, education and training**	教育訓練管理程序	V	
A.7.2.3	**Disciplinary process**	人事管理規則	V	
A.7.3	**Termination and change of employment**			
A.7.3.1	**Termination or change of employment responsibilities**	人事管理規則	V	
A.8	**Asset management**			
A.8.1	**Responsibility for assets**			

A.8.1.1	**Inventory of assets**	資訊資產風險評鑑辦法	V	
A.8.1.2	**Ownership of assets**	資訊資產風險評鑑辦法	V	
A.8.1.3	**Acceptable use of assets**	軟/硬體及應用系統之購置、使用及維護控制辦法	V	
A.8.1.4	**Return of assets**	使用者註冊管理辦法 程式及資料之存取控制辦法	V	
A.8.2	**Information classification**			
A.8.2.1	**Classification of information**	資訊處理管理辦法	V	
A.8.2.2	**Labelling of information**	資訊處理管理辦法	V	
A.8.2.3	**Handling of assets**	資訊處理管理辦法 軟體使用與管理辦法 硬體使用與管理辦法	V	
A.8.3	**Media handling**			
A.8.3.1	**Management of removable media**	資訊處理管理辦法 辦公室安全管理辦法	V	
A.8.3.2	**Disposal of media**	硬體使用與管理辦法 辦公室安全管理辦法	V	
A.8.3.3	**Physical media transfer**	資訊處理管理辦法 行政事務工作指引 辦公室安全管理辦法	V	
A.9	**Access control**			
A.9.1	**Business requirements of access control**			
A.9.1.1	**Access control policy**	存取控制規範	V	
A.9.1.2	**Access to networks and network services**	存取控制規範	V	
A.9.2	**User access management**			
A.9.2.1	**User registration and de-registration**	使用者註冊管理辦法 程式及資料之存取控制辦法	V	
A.9.2.2	**User access provisioning**	程式及資料之存取控制辦法	V	

A.9.2.3	**Management of privileged access rights**	使用者註冊管理辦法	V	
A.9.2.4	**Management of secret authentication information of users**	使用者註冊管理辦法	V	
A.9.2.5	**Review of user access rights**	使用者註冊管理辦法	V	
A.9.2.6	**Removal or adjustment of access rights**	使用者註冊管理辦法 程式及資料之存取控制辦法	V	
A.9.3	**User responsibilities**			
A.9.3.1	**Use of secret authentication information**	使用者密碼管理	V	
A.9.4	**System and application access control**			
A.9.4.1	**Information access restriction**	使用者註冊管理辦法 程式及資料之存取控制辦法	V	
A.9.4.2	**Secure log-on procedures**	使用者登入管理辦法	V	
A.9.4.3	**Password management system**	使用者密碼管理	V	
A.9.4.4	**Use of privileged utility programs**	使用者註冊管理辦法 程式及資料之存取控制辦法	V	
A.9.4.5	**Access control to program source code**	程式及資料之存取控制辦法	V	
A.10	**Cryptography**			
A.10.1	**Cryptographic controls**			
A.10.1.1	**Policy on the use of cryptographic controls**	資訊處理管理辦法	V	
A.10.1.2	**Key management**			ˇ
A.11	**Physical and environmental security**			
A.11.1	**Secure areas**			
A.11.1.1	**Physical security perimeter**	辦公室及機房 Layout 圖	V	
A.11.1.2	**Physical entry controls**	實體與環境安全管理辦法	V	
A.11.1.3	**Securing offices, rooms and facilities**	辦公室、機房 Layout 圖	V	
A.11.1.4	**Protecting against external and environmental threats**	辦公室及機房設計圖	V	

A.11.1.5	**Working in secure areas**	實體與環境安全管理辦法	V	
A.11.1.6	**Delivery and loading areas**	實體與環境安全管理辦法	V	
A.11.2	**Equipment**			
A.11.2.1	**Equipment siting and protection**	實體與環境安全管理辦法 辦公室、機房 Layout 圖	V	
A.11.2.2	**Supporting utilities**	檔案及設備之安全控制辦法	V	
A.11.2.3	**Cabling security**	檔案及設備之安全控制辦法	V	
A.11.2.4	**Equipment maintenance**	檔案及設備之安全控制辦法	V	
A.11.2.5	**Removal of assets**	實體與環境安全管理辦法 資訊處理管理辦法	V	
A.11.2.6	**Security of equipment and assets off-premises**	存取控制規範	V	
A.11.2.7	**Secure disposal or re-use of equipment**	硬體使用與管理辦法	V	
A.11.2.8	**Unattended user equipment**	使用者登入管理辦法	V	
A.11.2.9	**Clear desk and clear screen policy**	資訊處理管理辦法	V	
A.12	**Operations security**			
A.12.1	**Operational procedures and responsibilities**			
A.12.1.1	**Documented operating procedures**	軟/硬體及應用系統之購置、使用及維護控制辦法	V	
A.12.1.2	**Change management**	軟/硬體及應用系統之購置、使用及維護控制辦法	V	
A.12.1.3	**Capacity management**	軟/硬體及應用系統之購置、使用及維護控制辦法	V	

A.12.1.4	**Separation of development, testing and operational environments**	系統開發作業管理程序	V	
A.12.2	**Protection from malware**			
A.12.2.1	**Controls against malware**	惡意軟體控制辦法	V	
A.12.3	**Backup**			
A.12.3.1	**Information backup**	檔案及設備之安全控制辦法	V	
A.12.4	**Logging and monitoring**			
A.12.4.1	**Event logging**	程式及資料之存取控制辦法 使用者登入管理辦法	V	
A.12.4.2	**Protection of log information**	程式及資料之存取控制辦法	V	
A.12.4.3	**Administrator and operator logs**	檔案及設備之安全控制辦法 實體與環境安全管理辦法	V	
A.12.4.4	**Clock synchronisation**	監督系統使用狀況辦法(調整各系統之時間)	V	
A.12.5	**Control of operational software**			
A.12.5.1	**Installation of software on operational systems**	系統開發作業管理程序	V	
A.12.6	**Technical vulnerability management**			
A.12.6.1	**Management of technical vulnerabilities**	監督系統使用狀況管理辦法 軟/硬體及應用系統之購置、使用及維護控制辦法	V	
A.12.6.2	**Restrictions on software installation**	軟體使用與管理辦法	V	
A.12.7	**Information systems audit considerations**			
A.12.7.1	**Information systems audit controls**	智慧財產使用管理辦法	V	
A.13	**Communications security**			

A.13.1	**Network security management**			
A.13.1.1	**Network controls**	網路通訊作業管理辦法	V	
A.13.1.2	**Security of network services**	網路通訊作業管理辦法 電信公司之服務合約	V	
A.13.1.3	**Segregation in neworks**	網路通訊作業管理辦法	V	
A.13.2	**Information transfer**			
A.13.2.1	**Information transfer policies and procedures**	資訊處理管理辦法	V	
A.13.2.2	**Agreements on information transfer**	資訊處理管理辦法	V	
A.13.2.3	**Electronic messaging**	資訊處理管理辦法	V	
A.13.2.4	**Confidentiality or non- disclosure agreements**	保密協議書	V	
A.14	**System acquisition, development and maintenance**			
A.14.1	**Security requirements of information systems**			
A.14.1.1	**Information security requirements analysis and specification**	系統開發作業管理程序	V	
A.14.1.2	**Securing application services on public networks**	網站管理辦法	V	
A.14.1.3	**Protecting application services transactions**	SSL	V	
A.14.2	**Security in development and support processes**			
A.14.2.1	**Secure development policy**	系統開發作業管理程序	V	
A.14.2.2	**System change control procedures**	應用系統變更作業辦法 網站管理辦法	V	
A.14.2.3	**Technical review of applications after operating platform changes**	軟/硬體及應用系統之購置、使用及維護控制辦法	V	

A.14.2.4	**Restrictions on changes to software packages**	軟/硬體及應用系統之購置、使用及維護控制辦法	V	
A.14.2.5	**Secure system engineering principles**	系統開發作業管理程序	V	
A.14.2.6	**Secure development environment**	實體與環境安全管理辦公室 Layout 圖 資料輸出入之控制	V	
A.14.2.7	**Outsourced development**	系統開發作業管理程序 軟/硬體及應用系統之購置、使用及維護控制辦法 委外合約	V	
A.14.2.8	**System security testing**	系統開發作業管理程序	V	
A.14.2.9	**System acceptance testing**	系統開發作業管理程序 軟/硬體及應用系統之購置、使用及維護控制辦法 委外合約	V	
A.14.3	**Test data**			
A.14.3.1	**Protection of test data**	軟/硬體及應用系統之購置、使用及維護控制辦法	V	
A.15	**Supplier relationships**			
A.15.1	**Information security in supplier relationships**			
A.15.1.1	**Information security policy for supplier relationships**	資訊資產風險評鑑辦法	V	
A.15.1.2	**Addressing security within supplier agreements**	軟/硬體及應用系統之購置、使用及維護控制辦法 委外合約	V	

A.15.1.3	**Information and communication technology supply chain**	資訊資產風險評鑑辦法 委外合約	V	
A.15.2	**Supplier service delivery management**			
A.15.2.1	**Monitoring and review of supplier services**	(承包商及第三方使用者之資料、委外合約)	V	
A.15.2.2	**Managing changes to supplier services**	資訊資產風險評鑑辦法	V	
A.16	**Information security incident management**			
A.16.1	**Management of information security incidents and improvements**			
A.16.1.1	**Responsibilities and procedures**	資訊安全事件管理程序	V	
A.16.1.2	**Reporting information security events**	資訊安全事件管理程序	V	
A.16.1.3	**Reporting information security weaknesses**	資訊安全事件管理程序	V	
A.16.1.4	**Assessment of and decision on information security events**	資訊安全事件管理程序	V	
A.16.1.5	**Response to information security incidents**	資訊安全事件管理程序	V	
A.16.1.6	**Learning from information security incidents**	資訊安全事件管理程序	V	
A.16.1.7	**Collection of evidence**	程式及資料之存取控制辦法 實體與環境安全管理辦法	V	
A.17	**Information security aspects of business continuity management**			
A.17.1	**Information security continuity**			
A.17.1.1	**Planning information security continuity**	業務持續運作管理程序	V	
A.17.1.2	**Implementing information security continuity**	業務持續運作管理程序	V	

A.17.1.3	**Verify, review and evaluate information security continuity**	業務持續運作管理程序	V	
A.17.2	**Redundancies**			
A.17.2.1	**Availability of information processing facilities**	資訊資產風險評鑑辦法	V	
A.18	**Compliance**			
A.18.1	**Compliance with legal and contractual requirements**			
A.18.1.1	**Identification of applicable legislation and contractual requirements**	資訊安全風險管理程序 資訊資產風險評鑑辦法	V	
A.18.1.2	**Intellectual property rights**	智慧財產使用管理辦法	V	
A.18.1.3	**Protection of records**	資訊處理管理辦法	V	
A.18.1.4	**Privacy and protection of personally identifiable information**	存取控制規範	V	
A.18.1.5	**Regulation of cryptographic controls**	MD5	V	
A.18.2	**Information security reviews**			
A.18.2.1	**Independent review of information security**	內部資訊安全稽核程序	V	
A.18.2.2	**Compliance with security policies and standards**	日常資安工作匯總表 辦公室安全管理辦法	V	
A.18.2.3	**Technical compliance review**	監督系統使用狀況管理辦法 智慧財產使用管理辦法	V	

資料來源：本研究自行整理

表 3-5：整合後個人資料保護法適用性聲明

個人資料保護法	對應文件	適用	不適用
第一章　總　　則			
第一條　為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，特制定本法。		V	
第二條　本法用詞，定義如下：			
一、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。	資訊處理管理辦法	V	
二、個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。	資訊處理管理辦法	V	
三、蒐集：指以任何方式取得個人資料。	資訊處理管理辦法 業務流程分析報告	V	
四、處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。		V	
五、利用：指將蒐集之個人資料為處理以外之使用。		V	
六、國際傳輸：指將個人資料作跨國（境）之處理或利用。			V
七、公務機關：指依法行使公權力之中央或地方機關或行政法人。		V	
八、非公務機關：指前款以外之自然人、法人或其他團體。		V	
九、當事人：指個人資料之本人。		V	
第三條　當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：		V	
一、查詢或請求閱覽。	資訊處理管理辦法	V	
二、請求製給複製本。			
三、請求補充或更正。			

四、請求停止蒐集、處理或利用。			
五、請求刪除。			
第四條　受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。			V
第五條　個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。	資訊處理管理辦法 業務流程分析報告	V	
第六條　有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：		V	
一、法律明文規定。		V	
二、公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措施。			
三、當事人自行公開或其他已合法公開之個人資料。			
四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序所為蒐集、處理或利用之個人資料。			
前項第四款個人資料蒐集、處理或利用之範圍、程序及其他應遵行事項之辦法，由中央目的事業主管機關會同法務部定之。			
第七條　第十五條第二款及第十九條第五款所稱書面同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之書面意思表示。		V	
第十六條第七款、第二十條第一項第五款所稱書面同意，指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之書面意思表示。		V	
第八條　公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：		V	
一、公務機關或非公務機關名稱。		V	
二、蒐集之目的。		V	
三、個人資料之類別。		V	
四、個人資料利用之期間、地區、對象及方式。		V	

五、當事人依第三條規定得行使之權利及方式。		V	
六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。		V	
有下列情形之一者，得免為前項之告知：		V	
一、依法律規定得免告知。		V	
二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。		V	
三、告知將妨害公務機關執行法定職務。		V	
四、告知將妨害第三人之重大利益。		V	
五、當事人明知應告知之內容。		V	
第九條　公務機關或非公務機關依第十五條或第十九條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第一項第一款至第五款所列事項。			V
有下列情形之一者，得免為前項之告知：			
一、有前條第二項所列各款情形之一。			V
二、當事人自行公開或其他已合法公開之個人資料。			V
三、不能向當事人或其法定代理人為告知。			V
四、基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。			V
五、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。			V
第一項之告知，得於首次對當事人為利用時併同為之。			V
第十條　公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。但有下列情形之一者，不在此限：	資訊處理管理辦法	V	
一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。		V	
二、妨害公務機關執行法定職務。		V	
三、妨害該蒐集機關或第三人之重大利益。		V	
第十一條　公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。	資訊處理管理辦法	V	
個人資料正確性有爭議者，應主動或依當事人之請求		V	

停止處理或利用。但因執行職務或業務所必須並註明其爭議或經當事人書面同意者，不在此限。			
個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。		∨	
違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。		∨	
因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於更正或補充後，通知曾提供利用之對象。			
第十二條　公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。	資訊安全事件管理程序 業務持續運作管理程序	∨	
第十三條　公務機關或非公務機關受理當事人依第十條規定之請求，應於十五日內，為准駁之決定；必要時，得予延長，延長之期間不得逾十五日，並應將其原因以書面通知請求人。	資訊處理管理辦法	∨	
公務機關或非公務機關受理當事人依第十一條規定之請求，應於三十日內，為准駁之決定；必要時，得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人。		∨	
第十四條　查詢或請求閱覽個人資料或製給複製本者，公務機關或非公務機關得酌收必要成本費用。	資訊處理管理辦法	∨	
第二章　公務機關對個人資料之蒐集、處理及利用			ˇ
第十五條　公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：			
一、執行法定職務必要範圍內。			
二、經當事人書面同意。			
三、對當事人權益無侵害。			
第十六條　公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為		∨	

之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：			
一、法律明文規定。		V	
二、為維護國家安全或增進公共利益。		V	
三、為免除當事人之生命、身體、自由或財產上之危險。		V	
四、為防止他人權益之重大危害。		V	
五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。		V	
六、有利於當事人權益。		V	
七、經當事人書面同意。		V	
第十七條　公務機關應將下列事項公開於電腦網站，或以其他適當方式供公眾查閱；其有變更者，亦同：			
一、個人資料檔案名稱。			
二、保有機關名稱及聯絡方式。			
三、個人資料檔案保有之依據及特定目的。			
四、個人資料之類別。			
第十八條　公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。		V	
第三章　非公務機關對個人資料之蒐集、處理及利用			
第十九條　非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：			V
一、法律明文規定。			V
二、與當事人有契約或類似契約之關係。			V
三、當事人自行公開或其他已合法公開之個人資料。			V
四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。			V
五、經當事人書面同意。			V
六、與公共利益有關。			V
七、個人資料取自於一般可得之來源。但當事人對該			V

資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。			
蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。			V
第二十條　非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：			V
一、法律明文規定。			V
二、為增進公共利益。			V
三、為免除當事人之生命、身體、自由或財產上之危險。			V
四、為防止他人權益之重大危害。			
五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。			V
六、經當事人書面同意。			V
非公務機關依前項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。			V
非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。			V
第二十一條　非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：			V
一、涉及國家重大利益。			V
二、國際條約或協定有特別規定。			V
三、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。			V
四、以迂迴方法向第三國（地區）傳輸個人資料規避本法。			V
第二十二條　中央目的事業主管機關或直轄市、縣（市）政府為執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認有必要或有違反本法規定之虞時，得派員攜帶執行職			V

務證明文件，進入檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料。			
中央目的事業主管機關或直轄市、縣（市）政府為前項檢查時，對於得沒入或可為證據之個人資料或其檔案，得扣留或複製之。對於應扣留或複製之物，得要求其所有人、持有人或保管人提出或交付；無正當理由拒絕提出、交付或抗拒扣留或複製者，得採取對該非公務機關權益損害最少之方法強制為之。			∨
中央目的事業主管機關或直轄市、縣(市)政府為第一項檢查時，得率同資訊、電信或法律等專業人員共同為之。			∨
對於第一項及第二項之進入、檢查或處分，非公務機關及其相關人員不得規避、妨礙或拒絕。			∨
參與檢查之人員，因檢查而知悉他人資料者，負保密義務。			∨
第二十三條　對於前條第二項扣留物或複製物，應加封緘或其他標識，並為適當之處置；其不便搬運或保管者，得命人看守或交由所有人或其他適當之人保管。			∨
扣留物或複製物已無留存之必要，或決定不予處罰或未為沒入之裁處者，應發還之。但應沒入或為調查他案應留存者，不在此限。			∨
第二十四條　非公務機關、物之所有人、持有人、保管人或利害關係人對前二條之要求、強制、扣留或複製行為不服者，得向中央目的事業主管機關或直轄市、縣（市）政府聲明異議。			∨
前項聲明異議，中央目的事業主管機關或直轄市、縣（市）政府認為有理由者，應立即停止或變更其行為；認為無理由者，得繼續執行。經該聲明異議之人請求時，應將聲明異議之理由製作紀錄交付之。			∨
對於中央目的事業主管機關或直轄市、縣（市）政府前項決定不服者，僅得於對該案件之實體決定聲明不服時一併聲明之。但第一項之人依法不得對該案件之實體決定聲明不服時，得單獨對第一項之行為逕行提起行政訴訟。			∨

第二十五條　非公務機關有違反本法規定之情事者，中央目的事業主管機關或直轄市、縣（市）政府除依本法規定裁處罰鍰外，並得為下列處分：			∨
一、禁止蒐集、處理或利用個人資料。			∨
二、命令刪除經處理之個人資料檔案。			∨
三、沒入或命銷燬違法蒐集之個人資料。			∨
四、公布非公務機關之違法情形，及其姓名或名稱與負責人。			∨
中央目的事業主管機關或直轄市、縣（市）政府為前項處分時，應於防制違反本法規定情事之必要範圍內，採取對該非公務機關權益損害最少之方法為之。			∨
第二十六條　中央目的事業主管機關或直轄市、縣（市）政府依第二十二條規定檢查後，未發現有違反本法規定之情事者，經該非公務機關同意後，得公布檢查結果。			∨
第二十七條　非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。			∨
中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。			∨
前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之。			∨

資料來源：本研究自行整理

3.4. 整合後有效具體作法

3.4.1 檢視與清查現有作業流程

清查現況所有作業流程，須包含個人資料所延伸之個人資料流程，可參考圖 3-5，以點線面方式，逐一列舉所有工作項目，並且有邏輯性的分類與調整到每個作業流程，舉凡所有工作點，必定有歸屬之某一程序，程序必定歸屬某一作業流程；先依序進行工作要點分類、檢視，程序前後順序分類與調整，作業流程劃分與凸顯；最後，逆向以作業流程角度來檢視所有程序、步驟是否合宜，需不需要簡化、調整，或有遺漏部分需再補強。

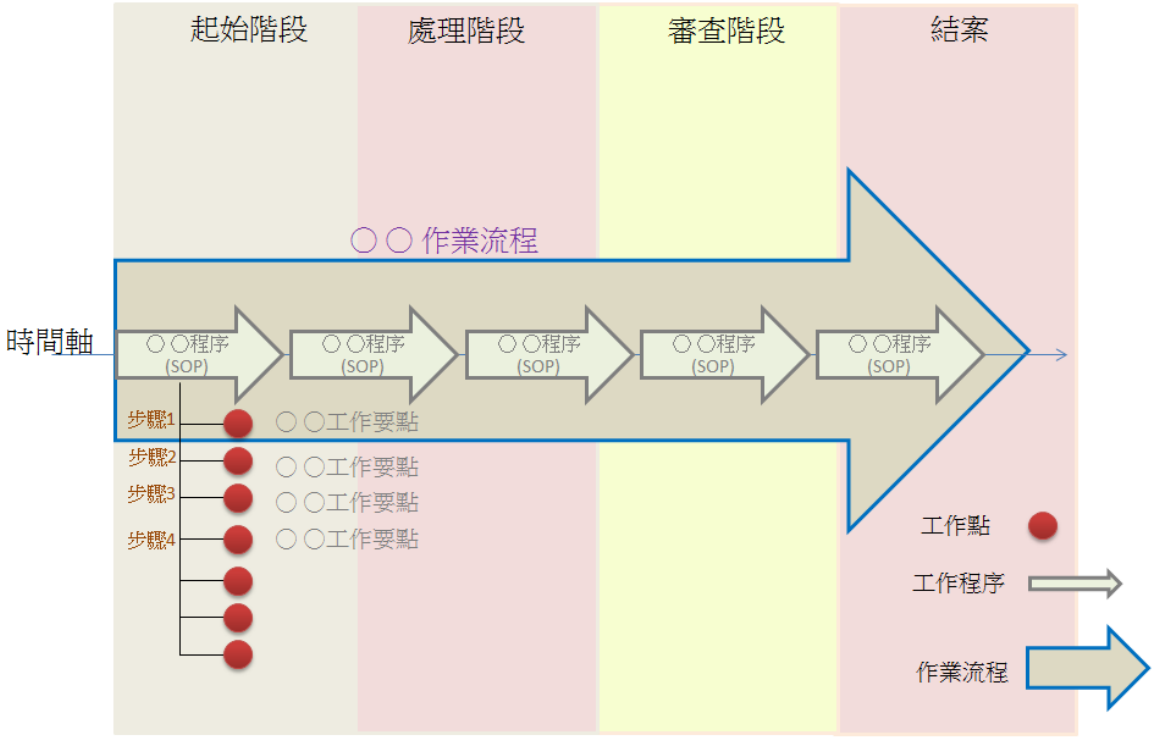

圖 3-5：作業流程點線面分析圖

資料來源：本研究自行整理

3.4.2 進行作業流程上資訊資產及個資清查作業

在所屬作業流程上進行資訊資產清查及分級分類時，可參考整合後風險評鑑前資訊資產與個人資料盤點作業流程圖(如圖 3-6)，在作業流程清查後，進行資訊資產與個人資料盤點，須將個人資料納入，可參考表 3-6 本實作範例，以作業流程角度完成清查作業。

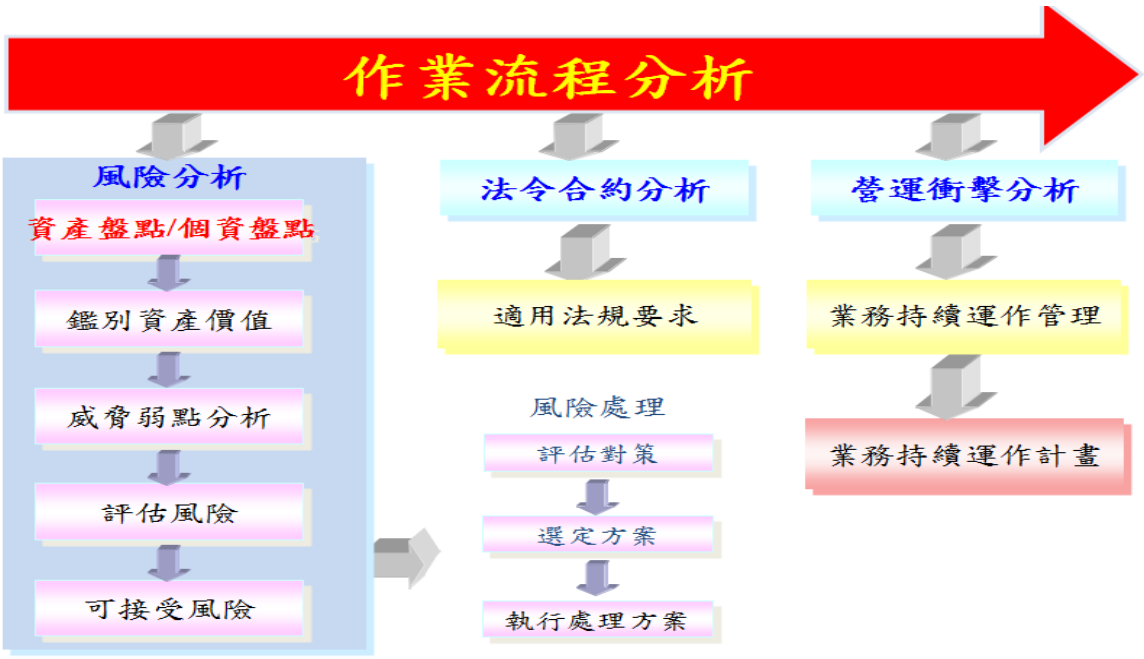

圖 3-6：整合後風險評鑑前資訊資產與個人資料盤點作業流程圖

資料來源：本研究自行整理

表 3-6：整合後風險評鑑前資訊資產與個人資料盤點參考表

作業流程名稱	資源					方法/法令	表單/紀錄(個資紅色)
	管理人員	使用設備	工作區域	電腦系統	服務		
防火牆管理流程	○○○	辦公室 PC1(172.20.1.X)	辦公室	win 7(172.20.1.X)	民網外部	防火牆操作手冊	防火牆異動單
	○○○	辦公室 PC2(172.20.1.X)	機房	win 7(172.20.1.X)	民網內部		
	○○○	機房PC1(172.20.1.X)		win 7(172.20.1.X)	電力		
	○○○	機房PC2(172.20.1.X)		win 7(172.20.1.X)			
	○○○	防火牆(Fortigate 3XX)(172.20.1.254)		Forti (4.0B)(172.20.1.254)			
	○○○	防火牆(Fortigate 3XXA)(172.20.100.X)		Forti (4.0B)(172.20.100.X)			
客服諮詢管理流程	○○○	辦公室 PC1(172.20.1.X)	辦公室	win 7(172.20.1.X)	通訊	後台管理操作手冊	每日工作日誌
	○○○	辦公室 PC2(172.20.1.X)	機房	win 7(172.20.1.X)	民網內部		
	○○○	機房PC1(172.20.1.X)		win 7(172.20.1.X)	電力		
	○○○	機房PC2(172.20.1.X)		win 7(172.20.1.X)			
	○○○	MND-WEBServer(172.20.100.X)		Windows Server 2012(172.20.100.X)			
	○○○			後台管理系統			
	○○○			前台系統			
	○○○	MND-SQLServer(172.20.100.X)		Windows Server 2008 R2 + MS SQl Server 2008 R2(64bit)(172.20.100.189)			

資料來源：本研究自行整理

透過清查、分析作業流程，可針對涉及個資之作業流程，可參考表 3-7 本實作範例，進行個人資料蒐集、處理、利用、銷毀分類，追蹤資料流向，加強適度保護與控管。

表 3-7：作業流程個人資料流向分析表

涉及個資人員姓名	涉及個資流程名稱	涉及個資檔案名稱與型態					涉及個資階段				特定目的代號	類別代號	處理階段之方式與權限									
		檔案名稱	紙檔	電子檔	直接	間接	蒐集	處理	利用	銷毀			記錄	輸入	儲存	編輯	更正	複製	檢索	刪除	輸出	連結	內部傳送
○○○	民意信箱管理流程	民意信箱使用者資料電子檔		o	o		o						o		o				o		o		o
○○○	客服諮詢管理流程	後台系統使用者資料電子檔		o	o		o						o	o	o	o	o		o		o		o
○○○	後台權限管理流程	後台系統使用者資料電子檔		o	o		o						o	o	o	o	o		o		o		o
○○○	退伍令補發申辦管理流程	退伍令申請表單電子檔		o	o		o						o		o				o				o

資料來源：本研究自行整理

3.4.3 資訊資產及個人資料風險評鑑作業

參照現有 ISO27005 風險評鑑作法，利用 CIA 等級及風險評鑑作業，可參考表 3-8，整合資訊資產與個人資料項目，並依個人資料敏感性區分 CIA 等級，如特種個資，列為最高評分數值，產出一致化風險評鑑報告，以利於後續規劃因應及處置措施。

表 3-8：整合後風險評鑑風險分析表

NO.	負責單位/人員	資產名稱	資產類別	數量	機密性	完整性	可用性	防護類別	威脅	脆弱點	威脅等級(安控前)	脆弱等級(安控前)	衝擊等級(安控前)	破壞事件的嚴重性(安控前)	風險值	風險等級
	○○○	前台系統	電腦系統		4	4	4		阻斷服務攻擊	缺乏備援系統。	2	2	3	12	144	B
	○○○	Windows Server 2008 R2 + Acunetix 8.0 + Nexpose 6.0 (172.20.100.220)	電腦系統		4	3	3		作業人員或使用者錯誤	使用者認知不足。	2	2	2	8	80	C
	○○○	Windows Server 2008 R2 + Acunetix 8.0 + Nexpose 6.0 (172.20.100.220)	電腦系統		4	3	3		技術失能	使用者認知不足。	2	2	2	8	80	C
	○○○	MND-DCServer(172.20.100.220)	實體設備		4	2	3		未授權存取資料	對有計畫的破壞行動缺乏懲戒處分。	1	2	2	4	36	D
	○○○	MND-DCServer(172.20.100.220)	實體設備		4	2	3		破壞	對有計畫的破壞行動缺乏懲戒處分。	1	2	2	4	36	D
	○○○	全球資訊網資料庫備份檔	資訊紀錄		4	4	1		未授權存取資料	對有計畫的破壞行動缺乏懲戒處分。	1	2	2	4	36	D
	○○○	全球資訊網資料庫備份檔	資訊紀錄		4	4	1		破壞	對有計畫的破壞行動缺乏懲戒處分。	1	2	2	4	36	D
	○○○	退伍令申請表單電子檔	資訊紀錄		4	3	1		社交工程	缺少資訊諮詢的規範：待釐清詢問者的身份再給予資訊。	1	2	2	4	32	D

資料來源：本研究自行整理

3.4.4 建立 ISMS 與 PIMS 四階文件

運用現有 ISMS 四階文件作法，將 PIMS 納入，如第一階文件資安手冊，可根據個資法建立資安與個資手冊；如第二階文件資訊安全事件管理程序，可整合為資訊及個資安全事件管理程序。整合現有四階文件，在整體資安與個資管理上，文件建立的思維更具縝密。實務工作最後，產出整合後適用性聲明(ISO27001 標準與個資法的結合)。

3.5. 小結

透過本章節進行多角度探討整合之可行性，與進行多面向整合工作，最後提出 4 點整合後有效具體作法，供第 4 章導入實作運用，利用 ISO 27001 擴大解釋包含個資法，來驗證單位 ISMS 與 PIMS 執行成效如何，是否通過驗證，在資安作為與個資保護作為是否達一定水準，降低其資安與個資外洩風險值。

在專家學者黃小玲(99)的個資法及 ISO 27001 共通性與操作概述[17]有提及如果組織已通過 ISO 27001 的驗證，若要強調個資保護議題，似乎較為簡單，至少已有驗證公司之稽核保證。只是 ISO 27001 並不特別強調個人資料，所以若有個人資料出現在非重要業務流程時，可能相關風險就不會被清楚地凸顯；所以本導入實作最後會經過國際驗證，並要求驗證公司將個資管理流程納入驗證範圍，達到整合後雙重保障。

本研究重點摘要 ISMS 與 PIMS 整合後作法：

(1) 檢視與清查現有作業流程：清查現況作業流程須包含個人資料所延伸之個人資料流程。

(2) 進行作業流程上資訊資產及個資清查作業：在所屬作業流程上進行資訊資產清查及分級分類時，須將個人資料納入，並依個人資料敏感性區分 CIA 等級。

(3) 資訊資產及個人資料風險評鑑作業：利用 CIA 等級及風險評鑑作業，整合資訊資產與個人資料項目，產出一致化風險評鑑報告，以利於後續規劃因應及處置措施。

(4) 產出 ISO27001 適用性聲明須包含個資法：利用 PDCA 過程導向，產出之文件及作法須符合 ISO27001 條文與個資法，可藉由本章節之 ISO27001 擴大解釋整合個資法條文來遵循。

4. 個案網站系統 ISMS 與 PIMS 整合導入實作

4.1. 網站系統導入目標

本研究以現行的網站系統為實作目標，國防部全球資訊網站系統為本國在網路世界中相當重要的門面，網站裡面所涵蓋的子系統也隨著網路取代道路資訊化的時代愈來愈多，在眾多程式修改以符合政策所需功能，也衍生出程式控管問題，軟體有無即時更新問題，稍微不注意，漏掉某個網頁程式或模組漏洞，很容易肇生許多資安問題與個資外洩情事發生，在充滿惡意程式的網路世界中，營運指標性網站(中華民國國防部)不得不小心謹慎進行。

本研究尋尋覓覓各種技術面與管理面方法，試藉由 ISMS 與 PIMS 整合導入作法可點線面解決既有資安問題及結合資訊技術防範未來可能發生威脅，同時訂定資訊安全與個資作業相關程序，以降低人為疏失所產生之作業流程風險，提升網站系統資訊安全與個資保護管理水準，讓本網站永續發展。

在導入完成後，如何驗證系統是否符合國際標準各項資安要求，以及資訊系統營運如何不觸及本國個資法各項要求，在前一章節已解釋 ISO27001 為組織之一般性資訊安全管理制度之要求，而個資法為組織之特定性資訊安全管理制度之要求。本實作運用新版 ISO27001:2013 包含本國個資法的驗證方式可達到此項要求。

後續網站系統營運，在不斷的 PDCA 循環中，利用 ISO27001 國際標準為主體架構，涵蓋本國個資法各項要求來不斷改善單位內資安及個資保護管理制度，以達到事先防範與管理風險的功能與機制。

4.2. 成立資安暨個資保護導入專案組織

一個健全有效率的組織，才能將 ISMS 及 PIMS 整合導入順利完成且持續改善，所以在人員組織架構中是工作啟動關鍵因素。

根據新版 ISO27001 特別強調領導力，在此需要找尋上級主管或上上級主管，願意面對問題、處理風險，來擔任專案工作的領導者，並針對相關參與同仁進行任務編組。本專案因涵蓋層面較廣，為使專案執行順遂，多次與長官溝通制度導入，利多於弊，以最易遭受風險之對外服務網站系統為主要範圍，由單位主官展現強烈企圖心，成立專案任務，經單位內專案經理協調長官、顧問老師、協力廠商，爭取預算、時間、人力，透過以下專案編組如圖 4-1，與長官企圖心及領導力，與主辦承辦人不斷地溝通協調，相關人員均能配合執行。在此圖由專案經理不斷地與向上級長官(單位主官、資安暨個資管理委員會、專案負責單位主管、管理代表)報告讓長官了解 ISMS 與 PIMS，並取得相當的支持，與所屬成員(風險評鑑小組、文件編撰小組、稽核小組、相關單位代表)進行相關認知訓練，與輔導顧問群與講師群深入了解導入過程與窒礙問題，與協力廠商簽訂相關契約條文。

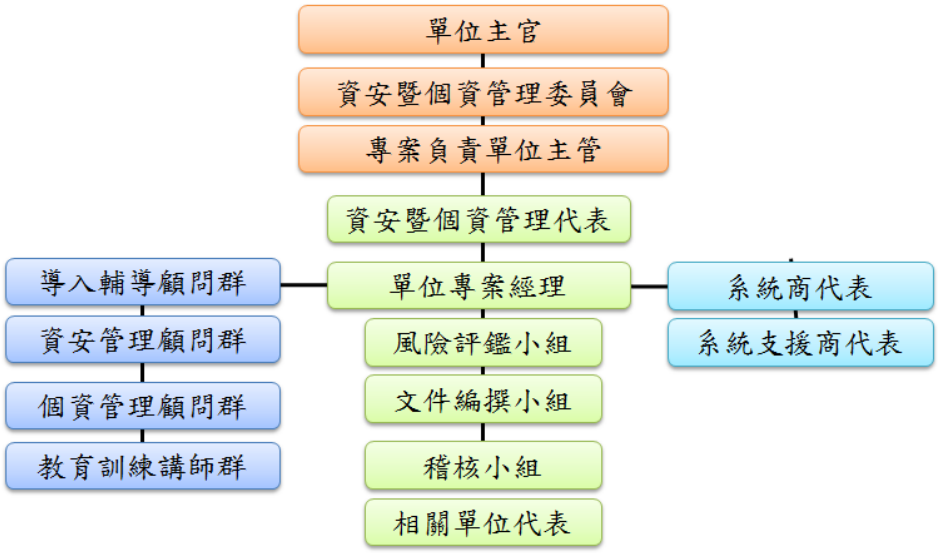

圖 4-1：本實作專案編組人員架構圖

4.3. 期程與範圍

自 102 年底進行導入工作可行性評估，103 年 1 月撰寫導入計畫並經權責長官奉核准，由具實影響力之長官來進行專案啟動會議，進行網站系統導入 ISMS 及 PIMS 之決心，在起始的 1 月份開始透過專家顧問進行資安現況了解與需求分析，執行過程中參與同仁需進行認知教育訓練及一連串的溝通與協調，每週透過專案會議管制各進度執行；過程中歷經安全需求分析、教育訓練、作業流程分析、資訊資產清查、個資盤點、四階文件建立、風險評鑑、風險處理、內部稽核、管理階層審查會議、產製適用性聲明書、系統改善作業、接受第三方稽核公司驗證等主要工作，為時八個月，如圖 4-2 所示。其驗證範圍為本單位重要對外窗口「全球資訊網站系統與機房營運」，執行各作業流程所延伸出資訊流程及個人資料流程之風險管理機制。

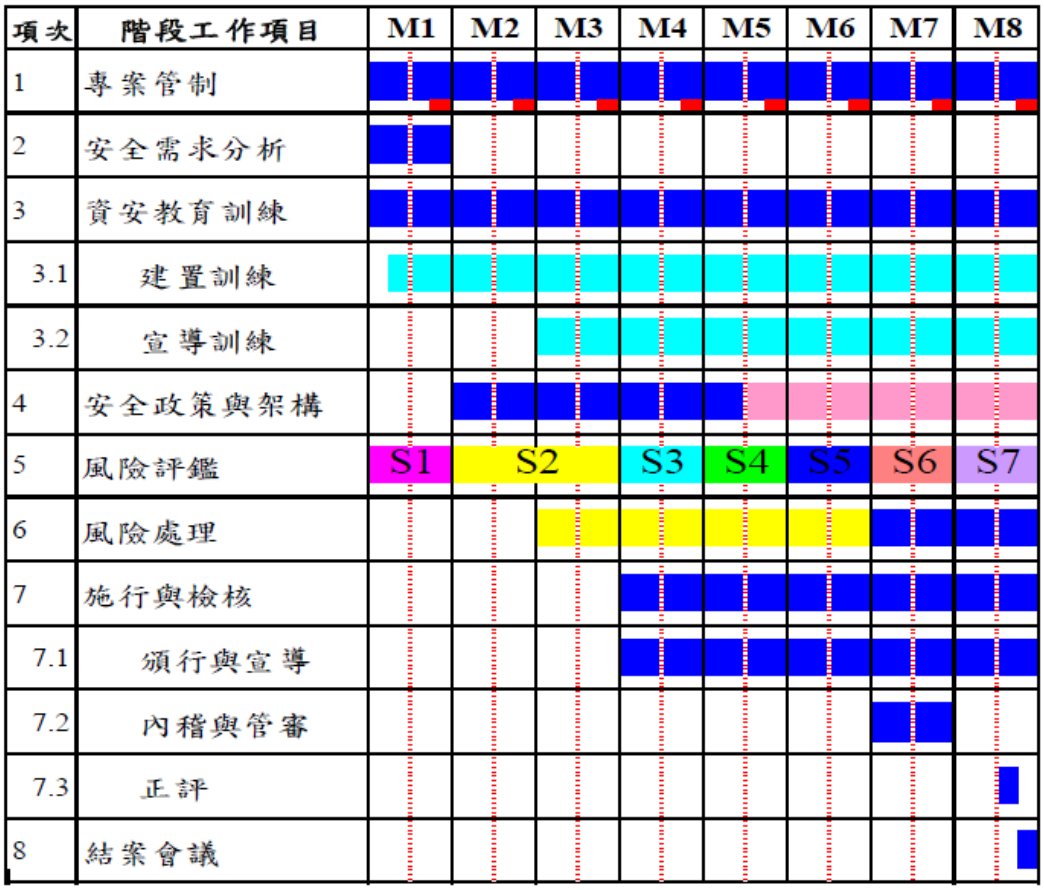

圖 4-2：本實作專案工作期程管制圖

4.4. 資安需求分析與文件建立

首先透過專家顧問對本資訊單位所維運之網站系統與組織全景進行現況了解，透過實地訪談與認知訓練，讓單位資訊主管可以認同觀念，且初步解決明顯之風險因子。

透過四階文件認知教育訓練，讓同仁了解各個法規、政策、程序、作業皆有所來源依據，以下面四階文件概念圖讓同仁可以更加有印象。

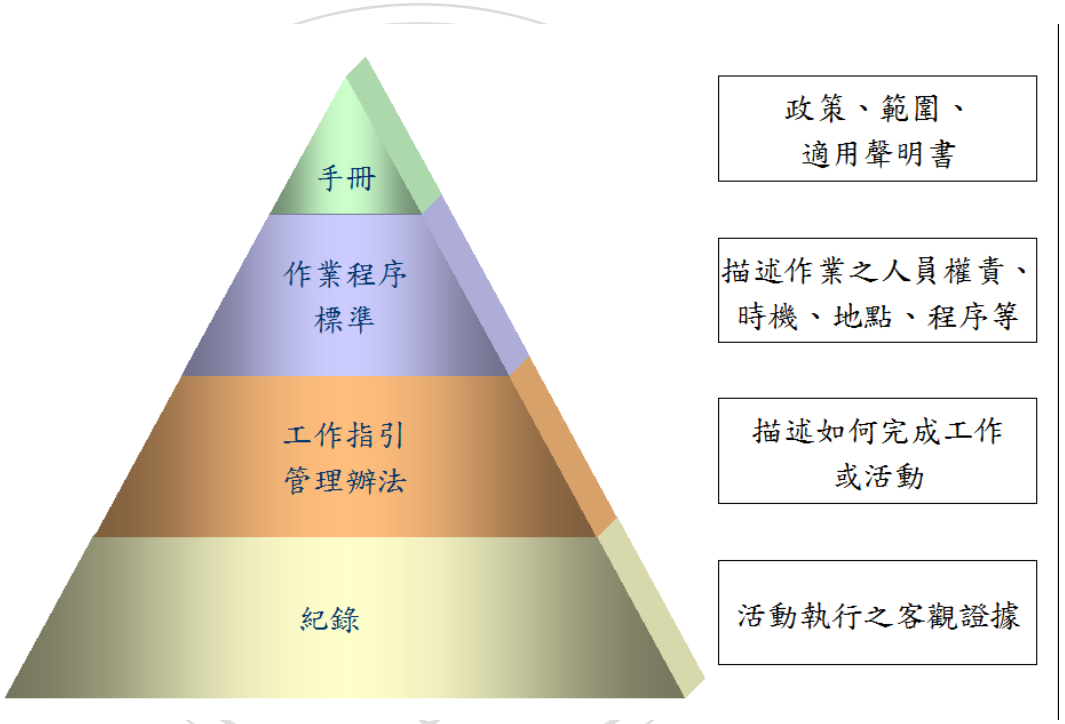

圖 4-3：四階文件概念圖

資料來源：本實作整理

(1) 第一階文件：主要包括全範圍之資安整體實行政策及原則，如：資安政策、管理手冊、適用性聲明等。

(2) 第二階文件：主要包括各領域之執行方向及原則，如：資訊資產、實體環境、人員安全、網路安全、風險評鑑、營運管理、系統開發、事件通報、內部稽核等程序書。

(3) 第三階文件：主要為包括相關業務流程及處理程序之詳細描述，如：人員職權、

帳號及通行碼管理、備份、營運計畫、資料庫管理、委外人員管理等作業程序或辦法。

(4) 第四階文件：主要包括業務運作所採用之表單、合約及其產生之各項紀錄，如：文件記錄、衡量指標表、季報表、名冊、切結書等表單。

建置之文件體系概要範例如下表所示：

表 4-1：四階文件體系概要範例參考表

階層	第一階	第二階	第三階	第四階
類別	手冊	程序	管理辦法	紀錄
名稱	資訊安全政策	資訊安全風險管理程序	資訊資產風險評鑑辦法	訓練計畫與評核
	適用聲明書	文件與紀錄管理程序	辦公室安全檢查管理辦法	風險評鑑報告
	資訊安全手冊	資安事件管理程序	系統監控程序	保密協議書
		內部稽核程序	管理審查程序	資安事件紀錄
		矯正與預防程序	使用者註冊管理	固定資產移動單
		營運持續管理程序	電腦資源管理辦法	軟體借用登錄表
			網站管理辦法	…

資料來源：本實作整理

收集現有之資安與個資保護管理辦法，融入四階文件概念，結合現行網站系統各項管理作為，進行文件與制度的建立，過程中需要不斷的研討，IS027001 標準與個資法各項條文須在文件內容中註記，以利參照源頭。如圖 4-4 所示。

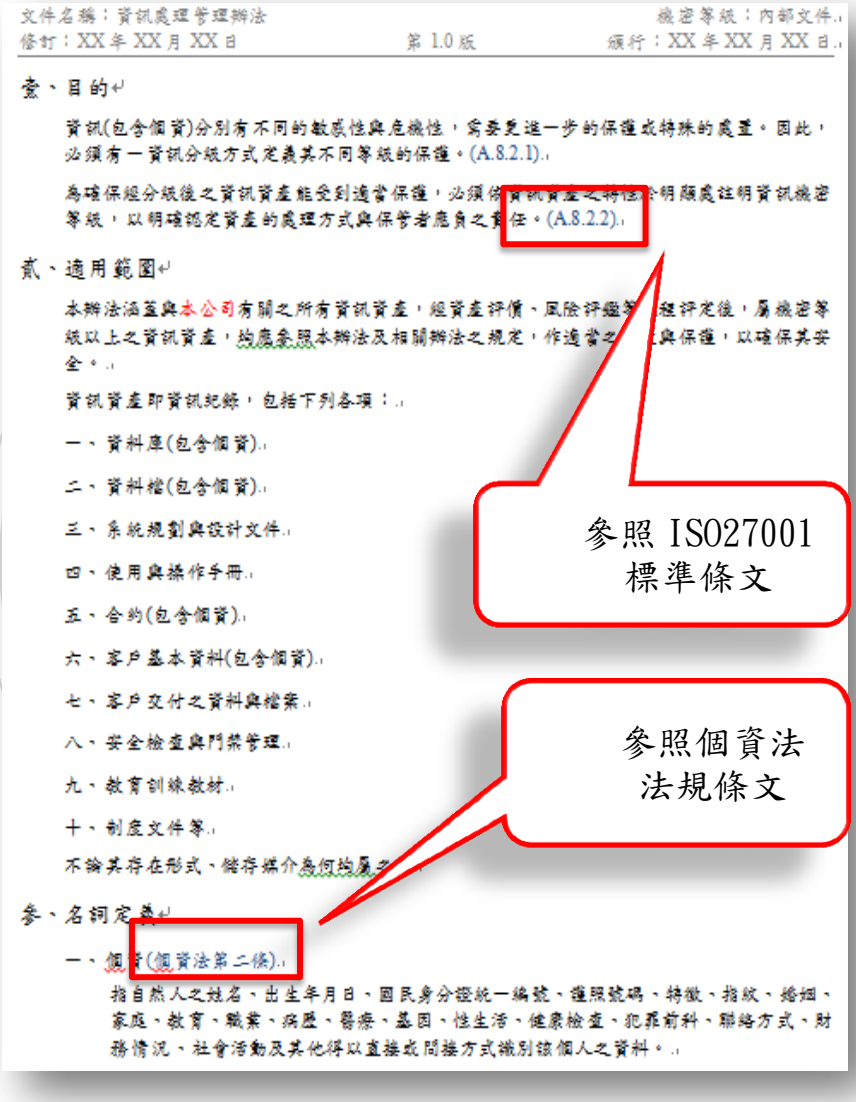

圖 4-4：文件製作參考範例圖

資料來源：本實作整理

在此階段可先檢討既有資訊安全與個資政策相關文件，先建立單位第一階文件-資安與個資政策，依據 ISO27001 標準與個資法之要求，整合現行管理制度並修訂程序及管理辦法，陸續建立第二階文件[作業程序]、第三階文件[管理辦法]、第四階文件[表單紀錄]，並符合 PDCA 持續改進精神，確保相關利害者(管理者與用戶)對資安與個資期望與要求。

4.5. 作業流程檢視

以ISMS管理系統作法為基準，首先檢視管理網站系統所有作業流程，可參考圖3-5：作業流程點線面分析圖。以點線面方式進行各工作點的分類，屬於哪個程序，眾多程序中屬於哪個流程；再以流程的角度檢視還需那些程序，程序中還欠缺那些工作點，使整個作業流程更加完善。

在此階段我們利用作業流程分析，將所有工作點逐一彙整、分類產生出各項作業流程，本實作可分析出：網站伺服器管理流程、資料庫伺服器管理流程、防火牆管理流程、後台權限管理流程、民意信箱管理流程、客服諮詢管理流程、供應商委外管理流程、資安報表管理流程…等 24 項作業流程。

4.6. 作業流程中資訊資產清查與個資盤點

運用現有 ISMS 風險評鑑作法，將個資盤點納入資訊資產清點的項目中，在此可將 PIMS 融入 ISMS 作法，檢視所有作業流程後(可參考圖 4-5：作業流程分析順序圖)，在流程中所經手的資訊資產與個人資料進行分類分級(可參考表 4-2、4-3 範例)。

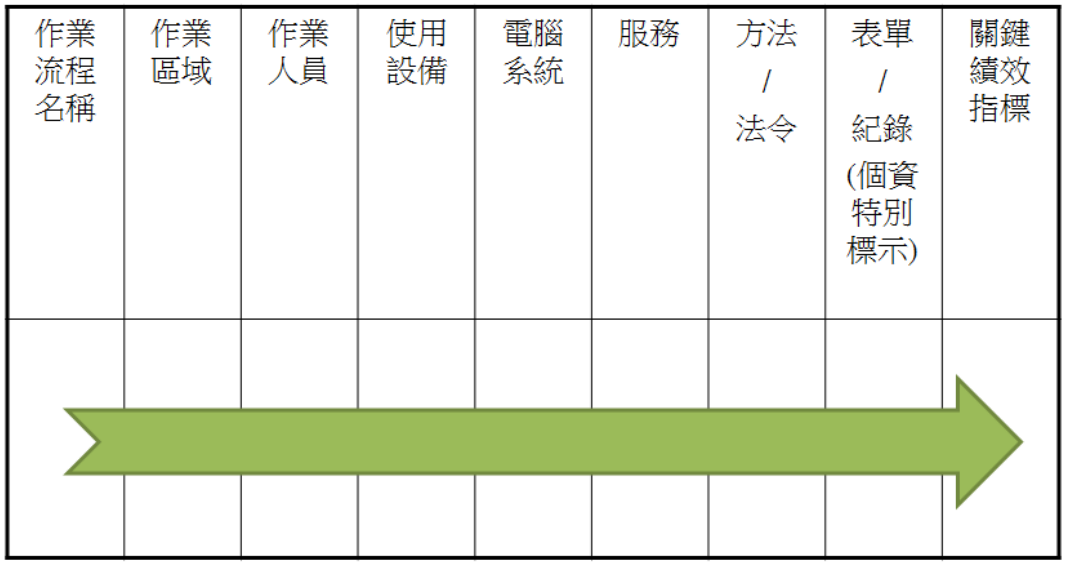

圖 4-5：作業流程分析順序圖

資料來源：本實作整理

表 4-2：作業流程分析參考表

作業流程名稱	資源					方法/法令	表單/紀錄(個資紅色)
	管理人員	使用設備	工作區域	電腦系統	服務		
防火牆管理流程	○○○	辦公室PC1(172.20.1.X)	辦公室	win 7(172.20.1.X)	民網外部	防火牆操作手冊	防火牆異動單
	○○○	辦公室PC2(172.20.1.X)	機房	win 7(172.20.1.X)	民網內部		
	○○○	機房PC1(172.20.1.X)		win 7(172.20.1.X)	電力		
	○○○	機房PC2(172.20.1.X)		win 7(172.20.1.X)			
	○○○	防火牆(Fortigate 3XX)(172.20.1.254)		Forti (4.0B)(172.20.1.254)			
	○○○	防火牆(Fortigate 3XXA)(172.20.100.254)		Forti (4.0B)(172.20.100.254)			
客服諮詢管理流程	○○○	辦公室PC1(172.20.1.X)	辦公室	win 7(172.20.1.X)	通訊	後台管理操作手冊	每日工作日誌
	○○○	辦公室PC2(172.20.1.X)	機房	win 7(172.20.1.X)	民網內部		
	○○○	機房PC1(172.20.1.X)		win 7(172.20.1.X)	電力		
	○○○	機房PC2(172.20.1.X)		win 7(172.20.1.X)			
	○○○	MND-WEBServer(172.20.100.188)		Windows Server 2012(172.20.100.188)			
	○○○			後台管理系統			
	○○○			前台系統			
	○○○	MND-SQLServer(172.20.100.189)		Windows Server 2008 R2 + MS SQl Server 2008 R2(64bit)(172.20.100.189)			

資料來源：本實作整理

表 4-3：涉及個資作業流程分析參考表

涉及個資人員姓名	涉及個資流程名稱	涉及個資檔案名稱與型態					涉及個資階段					類別代號	處理階段之方式與權限									
		檔案名稱	紙檔	電子檔	直接	間接	蒐集	處理	利用	銷毀	特定目的代號		記錄	輸入	儲存	編輯	更正	複製	檢索	刪除	輸出	連結	內部傳送
○○○	民意信箱管理流程	民意信箱使用者資料電子檔		o	o		o						o		o				o		o		o
○○○	客服諮詢管理流程	後台系統使用者資料電子檔		o	o		o						o	o	o	o	o		o		o		o
○○○	後台權限管理流程	後台系統使用者資料電子檔		o	o		o						o	o	o	o	o		o		o		o
○○○	退伍令補發申辦管理流程	退伍令申請表單電子檔		o	o		o						o		o				o				o

資料來源：本實作整理

4.7. 進行資訊資產與個資風險評鑑作業

在此階段可參考本文 2.5 章節風險評鑑作法，將資訊資產與個人資料進行 CIA 評價(機密性，完整性，可用性評價)，本實作可參照表 3-1：資訊資產機密性，完整性，可用性評價參照及表 3-2 個人資料機密性，完整性，可用性評價參照，可計算出資產價值，再運用 XXX 資產本身有 XXX 脆弱點，可能容易被外力 XXX 威脅所攻擊或利用，造成資產有 XXX 衝擊或 XXX 損害的邏輯概念[22]，將脆弱點、外在威脅可能性、衝擊程度、損害程度進行評估，本實作結果如表 4-4、表 4-5。

表 4-4：資安風險評鑑分析參考表

NO.	負責單位/人員	資產名稱	資產類別	數量	機密性	完整性	可用性	防護類別	威脅	脆弱點	威脅等級(安控前)	脆弱等級(安控前)	衝擊等級(安控前)	破壞事件的嚴重性(安控前)	風險值	風險等級
	○○○	網站內容保全軟體管理流程	資訊紀錄		3	2	1		未授權存取資料	對有計畫的破壞行動缺乏懲戒處分。	1	2	2	4	24	D
	○○○	網站內容保全軟體管理流程	資訊紀錄		3	2	1		破壞	對有計畫的破壞行動缺乏懲戒處分。	1	2	2	4	24	D
	○○○	網站內容保全軟體管理流程	資訊紀錄		3	2	1		偷竊	未控制資料及/或軟體複製。	1	2	2	4	24	D
	○○○	網站error log檔	資訊紀錄		3	2	1		破壞	對有計畫的破壞行動缺乏懲戒處分。	1	2	2	4	24	D
	○○○	網站error log檔	資訊紀錄		3	2	1		偷竊	未控制資料及/或軟體複製。	1	2	2	4	24	D
	○○○	電話紀錄單	資訊紀錄		3	3	1		偷竊	未控制資料及/或軟體複製。	1	1	2	2	14	D
	○○○	後台管理系統	電腦系統		4	4	4		作業人員或使用者錯誤	使用者認知不足。	2	1	3	6	72	C

資料來源：本實作整理

表 4-5：個資風險評鑑分析參考表

NO.	負責單位/人員	資產名稱	資產類別	數量	機密性	完整性	可用性	防護類別	威脅	脆弱點	威脅等級(安控前)	脆弱等級(安控前)	衝擊等級(安控前)	破壞事件的嚴重性(安控前)	風險值	風險等級
	○○○	前台系統	電腦系統		4	4	4		阻斷服務攻擊	缺乏備援系統。	2	2	3	12	144	B
	○○○	Windows Server 2008 R2 + Acunetix 8.0 + Nexpose 6.0 (172.20.100.220)	電腦系統		4	3	3		作業人員或使用者錯誤	使用者認知不足。	2	2	2	8	80	C
	○○○	Windows Server 2008 R2 + Acunetix 8.0 + Nexpose 6.0 (172.20.100.220)	電腦系統		4	3	3		技術失能	使用者認知不足。	2	2	2	8	80	C
	○○○	MND-DCServer(172.20.100.220)	實體設備		4	2	3		未授權存取資料	對有計畫的破壞行動缺乏懲戒處分。	1	2	2	4	36	D
	○○○	MND-DCServer(172.20.100.220)	實體設備		4	2	3		破壞	對有計畫的破壞行動缺乏懲戒處分。	1	2	2	4	36	D
	○○○	全球資訊網資料庫備份檔	資訊紀錄		4	4	1		未授權存取資料	對有計畫的破壞行動缺乏懲戒處分。	1	2	2	4	36	D
	○○○	全球資訊網資料庫備份檔	資訊紀錄		4	4	1		破壞	對有計畫的破壞行動缺乏懲戒處分。	1	2	2	4	36	D
	○○○	退伍令申請表單電子檔	資訊紀錄		4	3	1		社交工程	缺少資訊諮詢的規範：待釐清詢問者的身份再給予資訊。	1	2	2	4	32	D

資料來源：本實作整理

在此階段實作過程中，將資安與個資風險評鑑結果(如表 4-6 與表 4-7)中的 AB 等級風險進行適當處理，整個專案過程中，可以先行改善之風險，就馬上修正，資源不足部分，將列到管理審查會議，向主管報告看是否接受風險或申請相當資源降低風險。

表 4-6：本專案針對資安高風險項目

NO.	負責單位/人員	資產名稱	資產類別	機密性	完整性	可用性	威脅	脆弱點	威脅等級(安控前)	脆弱等級(安控前)	衝擊等級(安控前)	破壞事件的嚴重性(安控前)	風險值	風險等級
	○○○	防火牆	實體設備	4	4	4	作業人員或使用者錯誤	使用者認知不足。	2	2	4	16	192	A
	○○○	王○○	人員	4	4	3	誤傳	使用者訓練不足。	2	2	4	16	176	A
	○○○	負載平衡管理流程	資訊紀錄	4	4	2	誤傳	使用者訓練不足。	2	2	4	16	160	A
	○○○	負載平衡交換器	實體設備	4	4	4	作業人員或使用者錯誤	使用者認知不足。	2	2	4	16	192	A
	○○○	前台系統	電腦系統	4	4	4	阻斷服務攻擊	缺乏備援系統。	2	2	3	12	144	B
	○○○	○○○(協力商)	人員	4	4	1	破壞(偷竊,詐欺,竄改)	對有計畫的破壞行動缺乏懲戒處分。	1	3	4	12	108	B
	○○○	負載平衡管理流程	資訊紀錄	4	4	2	破壞	對有計畫的破壞行動缺乏懲戒處分。	1	3	4	12	120	B
	○○○	帳號密碼管制表	資訊紀錄	4	4	1	偷竊	未控制資料及/或軟體複製。	1	1	4	4	36	B
	○○○	後台管理系統	電腦系統	4	4	4	作業人員或使用者錯誤	使用者認知不足。	2	1	3	6	72	C
	○○○	後台管理系統	電腦系統	4	4	4	技術失能	使用者認知不足。	2	1	3	6	72	C
	○○○	後台管理系統	電腦系統	4	4	4	許可權的濫用	離開時，沒有登出終端	1	2	3	6	72	C
	○○○	後台管理系統	電腦系統	4	4	4	誤用	複雜的用戶介面	2	1	3	6	72	C
	○○○	Windows Server 2008 R2 + Acunetix 8.0 + Nexpose 6.0 (172.20.100.220)	電腦系統	4	3	3	作業人員或使用者錯誤	使用者認知不足。	2	2	2	8	80	C
	○○○	Windows Server 2008 R2 + Acunetix 8.0 + Nexpose 6.0 (172.20.100.220)	電腦系統	4	3	3	技術失能	使用者認知不	2	2	2	8	80	C

資料來源：本實作結果

表 4-7：本專案針對個資高風險項目

NO.	負責單位/人員	資產名稱	資產類別	機密性	完整性	可用性	威脅	脆弱點	威脅等級(安控前)	脆弱等級(安控前)	衝擊等級(安控前)	破壞事件的嚴重性(安控前)	風險值	風險等級
	OOO	win 7(172.20.1.X)	電腦系統	2	1	2	入侵	未更新或安裝作業系統/軟體的修補程式。	1	2	1	2	10	D
	OOO	Windows Server 2012+ Mail Server(6.0)	電腦系統	2	2	3	未授權存取資料	對有計畫的破壞行動缺乏懲戒處分。	1	2	2	4	28	C
	OOO	Windows Server 2012+ Mail Server(6.0)	電腦系統	2	2	3	作業人員或使用者錯誤	使用者認知不足。	1	2	2	4	28	C
	OOO	Windows Server 2012+Mail Server(6.0)	電腦系統	2	2	3	破壞	缺少變更管理控制。	1	2	2	4	28	C
	OOO	Windows Server 2008 R2 + MS SQl Server 2008 R2	電腦系統	2	2	3	未授權存取資料	對有計畫的破壞行動缺乏懲戒處分。	1	2	3	6	42	C
	OOO	Windows Server 2008 R2 + MS SQl Server 2008 R2	電腦系統	2	2	3	作業人員或使用者錯誤	使用者認知不足。	2	2	3	12	84	A
	OOO	Windows Server 2008 R2 + MS SQl Server 2008 R2	電腦系統	2	2	3	破壞	缺少變更管理控制。	1	2	3	6	42	C
	OOO	後台管理系統	電腦系統	2	2	2	作業人員或使用者錯誤	使用者認知不足。	1	1	2	2	12	D
	OOO	後台管理系統	電腦系統	2	2	2	技術失能	使用者認知不足。	1	1	2	2	12	D
	OOO	後台管理系統	電腦系統	2	2	2	許可權的濫用	離開時，沒有登出終端	1	2	2	4	24	C
	OOO	後台管理系統	電腦系統	2	2	2	誤用	複雜的用戶介面	2	2	2	8	48	B

資料來源：本實作結果

也在此專案以資安風險角度發現(如表 4-6)，普遍較高風險為網路設備與資安設備，設備均僅有一套，容易因設備故障或韌體更新，影響網站系統正常運作。以個資風險角度發現(如表 4-7)，較高風險為個人資料所存管之資料庫，容易因防護不當或人員操作錯誤，影響個資當事人權益，在這部分已針對人員操作，製作對應之標準作業程序供人員遵循，並加強人員個資法認知訓練，以及對該台伺服器進行適當保護與存取限制。

本專案也因風險評鑑過程中發現主要問題，如圖 4-6，原網路架構沒有備援機制，時常因某設備故障，影響系統中斷；經改善後(如圖 4-7)，不僅系統運作相當穩定，且可面臨較多資安威脅。

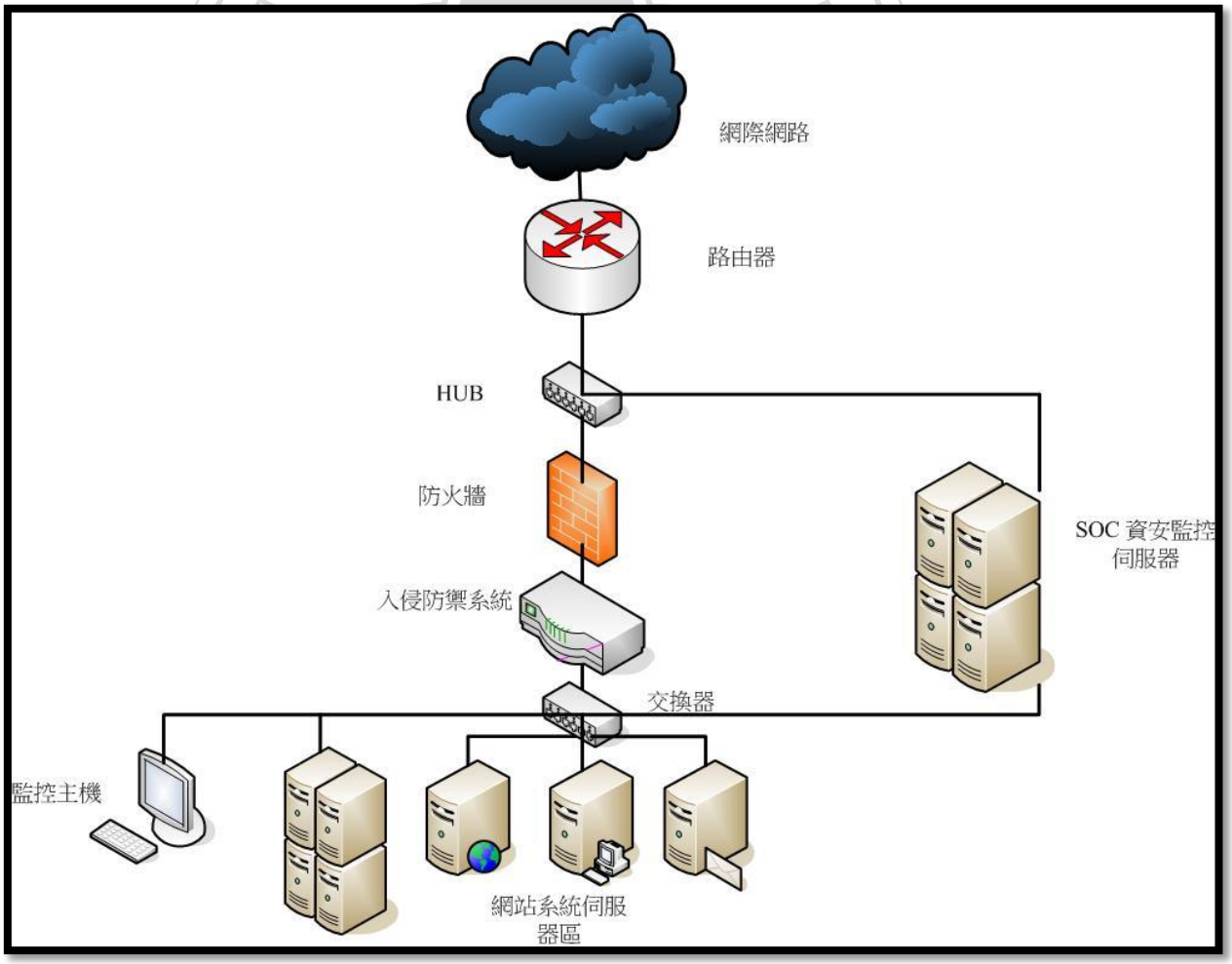

圖 4-6：導入前網路架構圖

資料來源：本實作整理

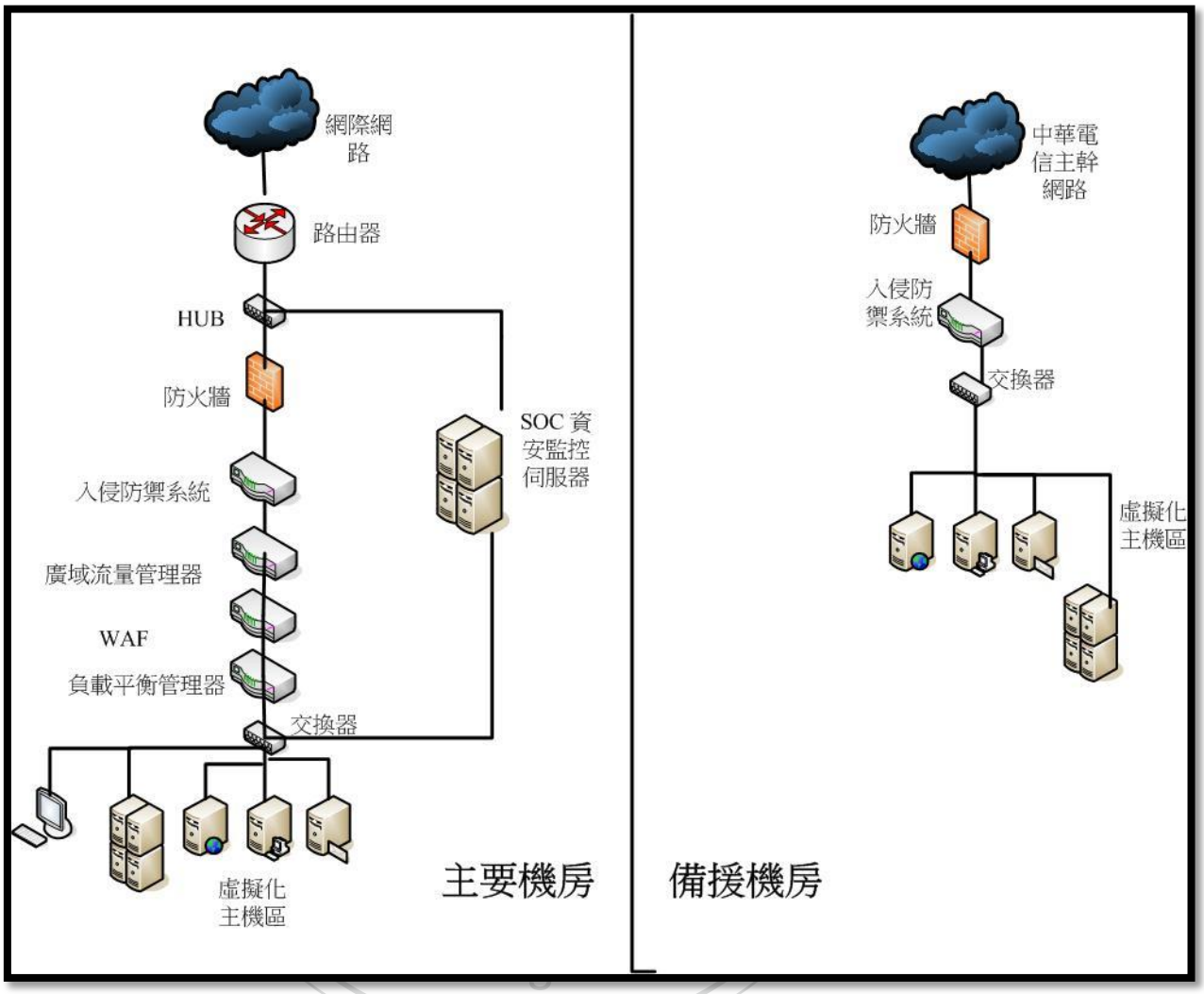

圖 4-7：導入後網路架構圖

資料來源：本實作整理

4.8. 產製風險評鑑報告及四階文件

最後產生風險評鑑報告，透過呈文方式與管理審查會議告知管理階層高中低風險，由主管決定處理順序與風險承受程度，在此風險評鑑報告須有所使用風險評鑑方法、風險評鑑結果(以量化方式呈現)、風險處理計畫(須包含解決方案之選擇)、風險安控後承受程度(有管理階層承受風險之批核)等內容，可參考行政院國家資通安全會報技術服務中心 100 年資訊系統風險評鑑參考指引實務導入報告寫法[23]。

在此階段各類四階文件陸續依據組織全景、單位特性，考量相關法律、規定，以及合約之要求，於適度評估風險及應對措施後，訂出經由管理階層核准之 ISMS 與 PIMS 整合導入之政策與四階文件，並擬定一份適用性聲明書文件。

4.9. 進行持續營運演練

為防範本部「全球資訊網站系統」資訊資產因遭受破壞或不當使用時，導致營運中斷或效率降低影響系統正常運作時，特辦理「全球資訊網站系統」營運持續運作演練；使本部業管資訊同仁能正確判斷受影響範圍及損害程度，且依擬定步驟採取正確之應變處理措施，針對核心系統服務，進行狀況演練，使該系統服務能在所訂定目標回復時間（RTO）、資料回復點（RPO），及最大可容忍中斷時間（MTD）等要求下回復正常並持續運作。

4.10. 內部稽核與管理審查

在此階段，各類文件與管控措施已達到一定水準，為落實單位實施資安與個資保護之成效，透過內部稽核方式，來檢驗其實施績效，藉以掌握單位內可能缺失，適時執行矯正行動及追蹤確認，符合 PDCA 模式之 C(Check)之要求。由內部同仁(非受檢小組)獲得相當稽核能力，根據現行標準與法規(如個資法、ISO27001 條文要求)、內部規定(如資安政策)、管理辦法(四階文件)，驗證是否說寫作一致，並且符合法規、規定要求。

將稽核結果報告與需呈報之相關量測資料，利用管理階層審查會議，由高階主管主持，以確保 ISMS 與 PIMP 持續有效運作，並管制持續加以改善；本實作審核項目內容包含：近期資安/個資事件、內部稽核結果與矯正措施、系統監控與量測之結果、相關利益團體對資安/個資要求與期望之回饋討論、改進 ISMS 及 PIMP 之技術、產品或程序之結果、內外部溝通之回饋討論、抱怨之處理、風險評鑑之結果及風險處理計畫、改進之建議。在管理審查會議中，盡可能將與管理階層相關訊息告知，讓管理階層對資訊系統 ISMS 與 PIMS 運作有所了解，並給予相當資源與支持。

4.11. 接受外部稽核

為驗證本實作 ISMS 與 PIMS 整合後實施有效性，透過第三方國際 ISO 驗證機構來驗證是否符合國際標準 ISO27001 條文要求及本國個資法要求；本專案邀請英國國際品質驗證有限公司（NQA）臺灣分公司蒞部實施文件驗證及實地稽核，並依檢核結果，辦理缺失改正及文件修正，也在 2014 年 10 月 17 日通過驗證，由英國國際品質保證協會（NQA）臺灣分公司授予本部「ISO 27001：2013 暨個人資料保護管理流程認證」國際證書(如圖 4-8)。證明本單位 ISMS 與 PIMS 在執行與維持（Plan-Do-Check-Act）管理系統均能符合相關標準與法規，也證明可運用最具國際公信力 ISO 標準來驗證 ISMS 與 PIMS 整合後作法。

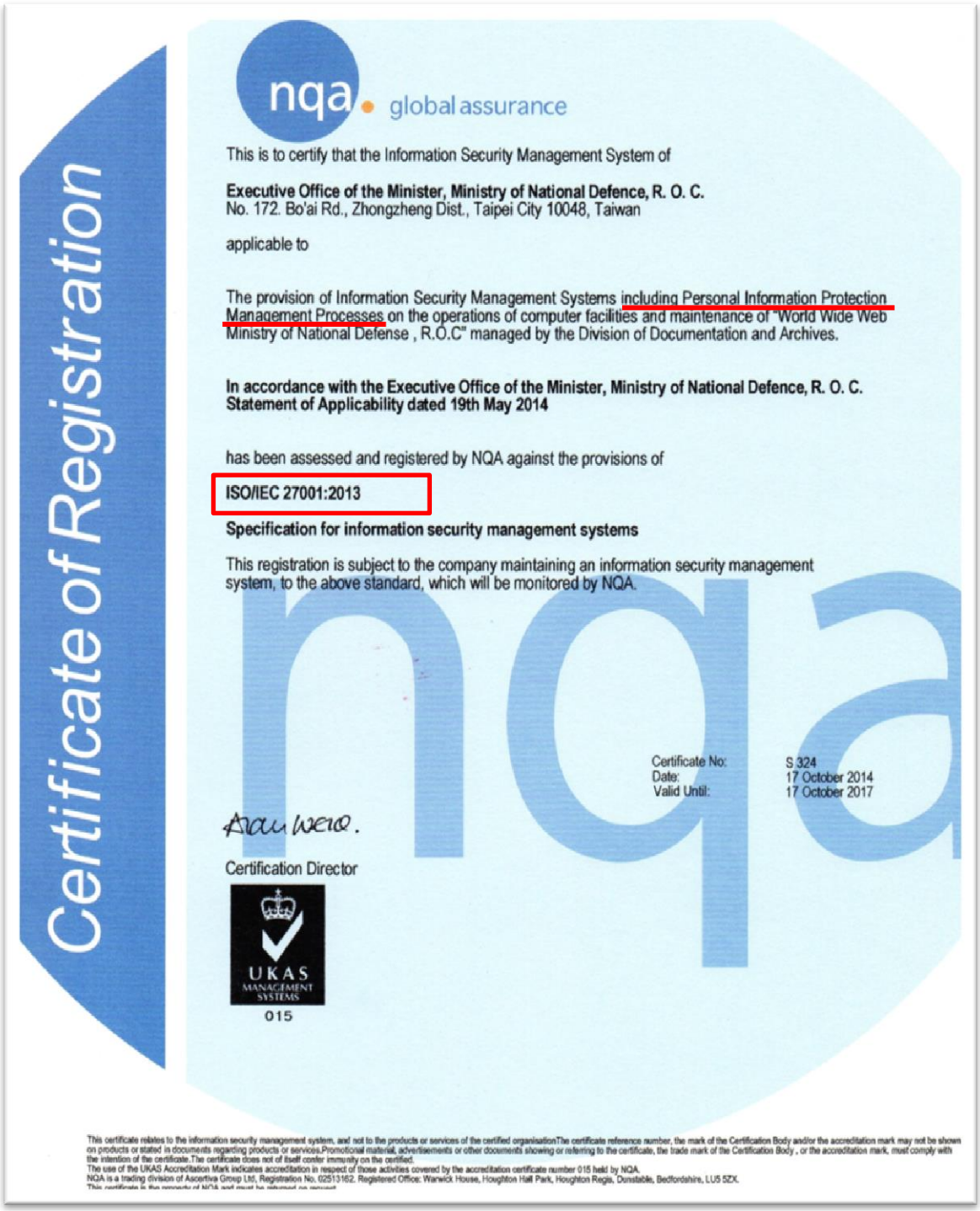

圖 4-8：通過驗證國際 ISO 證書

5. 結論與貢獻

在本研究第二章可以很清楚了解，ISMS 與 PIMS 本質上是很相近的，以資料的生命週期，資訊安全的機密性、完整性、可用性進行探討，運用現有的 ISMS 的既定作法，來進行整合 PIMS；在第三章很明確指出整合後具體作法，不管在作業流程面、四階文件產製、風險評鑑作業等面向，透過這些具體作法，讓需要導入 ISMS 與 PIMS 組織或單位可以更有效；在第四章藉由第三章所具體作法，運在本單位實施，發現在整個 ISMS 與 PIMS 導入，不再是分兩次導入、造成人力負荷、部分成本重複投資等現象，而是更有效且更有邏輯性的面對各種資安與個資問題，以作業流程面來分析資安與個資，讓每個控制點更加明確，也透過文件製作與 SOP 訂定，讓人員大幅降低因操作錯誤，造成資訊與資安風險，最後實作運用 ISO 27001 標準包含個資管理流程來驗證本實作，也證明本研究 ISMS 與 PIMS 整合後，在實施（Plan-Do-Check-Act）管理系統確實有效，均能符合相關標準與法規。

在本單位尚未導入 ISMS 與 PIMS 前，面對各種資安與個資法通過必須因應措施，毫無有效方法，面對外來未知的威脅，充滿許多徬徨，僅能就已知的防護方法，運用許多資訊技術手段，卻無法切確且有效達到安全目標；然而，透過 ISMS 與 PIMS 整合導入，完成主要成效：(1)分析、簡化、修訂 39 項作業流程，及編製各類 SOP，供作業人員遵循，減少人員作業疏失風險，並完成點、線、面整體考量與資安縱深防禦佈局。(2)完成 649 項資訊資產及個人資料風險評鑑作業及風險處理計畫，以降低單位內潛在之資訊威脅，進而保障本單位資訊資產及個人資料之機密性、完整性及可用性。(3)完成 35 份符合 ISO 27001:2013 標準及個資法之作業程序，強化資安暨個資保護管理作業規範，建立符合國際規範之資安暨個資保護管理制度，提升本部網站資安防護水準，以符合行政院資安及個資法之各項要求；最後，(4)通過「ISO 27001：2013 暨個人資料保護管理流程認證」，並獲英國國際品質保證協會（NQA）臺灣分公司授予本部「ISO 27001：2013

暨個人資料保護管理流程認證」國際證書(新聞報導如圖 5-1)。自從導入後，單位資訊同仁對資訊安全與個資保護有更明確了解，除利用資訊技術防範外，在管理作法上更加精進，也透過認知教育訓練，提昇單位資訊同仁與管理階層資安與個資的觀念，認同其重要性，並樂於執行相關程序作業，透過 ISMS 及 PIMS 整合導入工作，主動挖掘潛在風險因子並事先防範，確保系統上個人資料獲得保護，同時保護個人資料不外洩，確保本部重要對外國防政策推廣窗口「國防部全球資訊網」永續營運之目標。本研究可供有心導入 ISMS 與 PIMS 的資訊人員參考，或對這方面有興趣的 IT 人員研究。

圖 5-1：網站個資保護獲國際標準 ISO 認證

參考文獻

[1] 避免多頭馬車管理 PIMS與ISMS踏上整合之路,Information Security 資安人科技網,網址：http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=5910。

[2] 從管理與組織角度一探個資法因應之道,Information Security 資安人科技網,網址：http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=7221#ixzz3UQvFndy3。

[3] 黃小玲(2010)，清流月刊中華民國九十九年十一月號，網址：http://www.mjib.gov.tw/cgi-bin/mojnbi?/d2/9911/4-1.htm。

[4] 鄭東昇(2005),「資訊安全管理系統與企業網路安全實作探討」,交 通 大 學,碩士論文。

[5] 鄭伊雯(2012),「植基於 ISO 27001 建立符合 BS 10012 之 個人資訊管理自我評鑑模式」中原大學，碩士論文。

[6] 經濟部商業司TPIPAS臺灣個人資料保護與管理制度規範，網址：http://www.tpipas.org.tw/model.aspx?no=159 。

[7] 樊國禎博士(2014),「ISMS新版實作初探：擴增MSS的ISMS初論之一」,台灣網路防護協會，經濟部標準局103年第1季資訊安全管理系統標準化系列討論會。

[8] ISO (2001) Guidelines for the justification and development of management system standards,ISO Guide 72:2001(E).

[9] ANSI et al. (2007) Justification study for a new work item proposal for a energy management standard ad guidance document.

[10] ISO/TMB (2009) Request for feedback and comment on proposed identical sub-classes titles for management system standards, 2009-04-10.

[11] ISO/TMB (2009) Request for feedback and comment on proposed common terms and core definitions for management system standards, 2009-04-20.

[12] ISO/IEC JTC 1/SC 27 (2010) Text for ISO/IEC 4th WD 27001 – information technology – Security techniques – Information security management systems – Requirements, 2010-11-15.

[13] ISO/IEC JTC 1/SC 27 (2010) Whitepaper future of ISO/IEC 27001 and management system standards (MSS), ISO/IEC JTC 1/SC 27 N8662, 2010-07-15.

[14] ISO (2009) Risk management –principles and guidelines, ISO 31000:2009(E).

[15] ISO (2010) Information and documentation – Management system for records – Fundamentals and vocabulary, ISO DIS 30300:2010-05-21, Figure 3, p. 7.

[16] 徐弘昌(2009),「以ISO 27001為基礎評估電信業資訊安全管理- 以第一類電信業者

為例」，交通大學，碩士論文
[17] 張文瀞(2014) ，「 ISO27001:2013和ISO27001:2005的主要差異」，臺灣大學計算機及資訊網路中心程式設計組副理張文瀞2014.09.20發行ISSN 2077-8813，網址：http://www.cc.ntu.edu.tw/chinese/epaper/0030/20140920_3003.html
[18] 李慧蘭(2006)，「國際資訊安全標準ISO 27001之網路架構設計–以國網中心為例探討風險管理」，國家實驗研究院國家高速網路與計算中心，期刊
[19] 張芳珍(2004) ，「以BS7799 落實資訊安全管理-管理類資訊資產分類與控管」，碩士論文
[20] 劉永禮(2001) ，「以BS7799 資訊安全管理規範建構組織資訊安全風險管理模式之研究」，碩士論文。
[21] 黃小玲(2011)，「個資法與國際隱私管理標準、規範之分析與應用」，資訊安全通訊，3(7)，21-36
[22] 最佳化企管顧問有限公司何銘燁講師資訊安全/個資法風險管理(ISO27005) 實務訓練課程
[23] 行政院國家資通安全會報技術服務中心100年資訊系統風險評鑑參考指引實務導入報告，網址：https://www.icst.org.tw/CommonSpecification.aspx?lang=zh。