ISMS 與 PIMS 整合導入之研究 -以國防部全球資訊網站系統為例

孫天貴、左瑞麟
政治大學資訊科學系、政治大學資訊科學系
albert1725@gmail.com、raylin@cs.nccu.edu.tw

摘要

近年來全球資訊安全事件不斷發生，所肇生的資訊系統損害、資料毀損、個資外洩、財務詐騙事件也不斷增加；個資法實施之後，資訊系統在技術上、管理上、法規遵循上更具複雜性，稍有不慎，將造成單位重大影響與傷害。

為全面性解決資安與個資問題，資訊安全管理系統（ISMS）與個人資訊管理系統(PIMS)整合導入便是一套可有效控制管理之方法。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。

本研究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。

以國防部網站系統為實作目標，運用整合結果進行實作，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，也證明整合確實有效，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

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

Sun Tien-Kuei, Raylin Tso
Computer Science of the NCCU
albert1725@gmail.com
raylin@cs.nccu.edu.tw

Abstract

In recent years, the global information security incidents continue to occur. Information system damage, data corruption, personal data leakage, financial fraud is increasing. After Personal Data Protection Act implementing, information systems on technology, management, legislation follow become more complexity. If the slightest mistake, the company will result in a significant impact and damage.

In order to solve information security and personal data protection, Importing and Integration of ISMS and PIMS is a set of effective management methods. The study tried to lifecycle data, confidentiality, integrity, availability of Information Security PDCA operating model ... and so on point of view to probe on the essence to execute the work of Importing and Integration of ISMS and PIMS.

The study work of integration from the multi-oriented perspective to provide four specific practices that can be integrated effectively. : 1. Inventory of all workflow must include the extension process personal data. 2. Inventory information assets and personal information checking operations on the work processes. 3. Information assets and personal information, risk evaluation operations.4. Establish ISMS and PIMS four level documents structures, output ISO27001 applicability statement shall contain a Personal Data Protection Act.

That is the goal of the World Wide Web for Military of National Defense, Taiwan, R.O.C. which put into practice for this case with the results of this study. This practice has verified this study more efficient and more logic to solve information security and personal data protection problem. In workflow surface to analyze information security and personal data, so that each control point more clear. Finally, generally accepted in various countries ISO standard (ISO 27001 standard including Personal Information Protection Management Processes) to verify this implement which also has proved this study can integrate, works, compliance with the relevant standards and regulations really.

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

壹、 前言

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。

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。但隨著資訊日新月異，網站系統所面臨的資訊安全的威脅與過去相比複雜許多。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，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。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，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。

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，大多藉由導入「資訊安全管理系統」(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。

1.2 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，2012 年 12 月 27 日民視新聞報導，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。

又如 2015 年 6 月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。同月，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，需要資訊安全的協助才行。

又如 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。

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。

1.3 全方面解決策略-ISMS 與 PIMS 整合

ISMS 與 PIMS 管理作法各界都認同可以整合,但是沒有一個可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 與 PIMS,降低管理複雜度,藉由國防部網站實作驗證可行性,達到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。

貳、文獻探討

2.1 資訊安全管理系統-ISMS

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。

資訊安全是一個管理過程而非技術過程,須不斷調整與改善,以「資訊安全管理」為核心加以整合「資訊安全技術」層面並遵循相關「法規要求」,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。

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,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。[6]

2.2 個人資訊管理系統-PIMS

我國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，避免人格權受侵害及促進資料之合理利用，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[7]。因應個資法實施後，普遍相關 PIMS 作法有 BS10012、TPIPAS，以下將針對此兩種作法作研討。

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。。

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。[5]

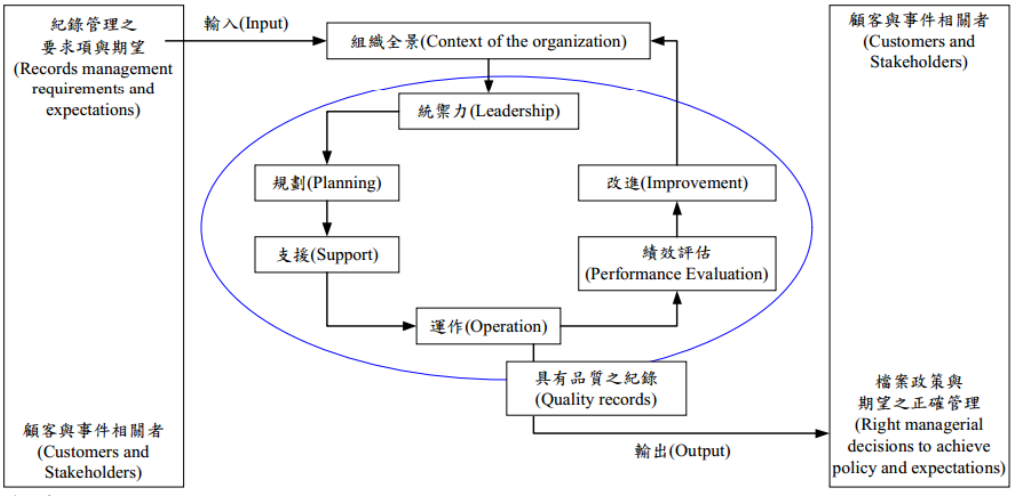
然而，在普遍 PIMS 實務作法中，BS10012 為英國隱私標準，其中個人資料法制規範與環境之不同，相關制度無法直接移植供國內使用。TPIPAS 僅針對本國個資法條文訂定管理制度，難以透過國際標準認證(如：ISO27001)；個人資料相關法制規範主要係維護個人對於其資料的資訊自主，仍需要資訊系統安全之協助。

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

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，自 2000 年起進行管理系統標準(Management System Standards，簡稱 MSS)之標準化工作項目，[8]。於 2001 年先行出版 ISO Guide 72 作為準備[2]，並在 2008 年至 2012 年於能源管理為標的試行[1]。ISO 技術管理委員會於 2010 年已完成第 2 階段之共同用語與核心定義的標準化作業，ISO/IEC 27001 新版亦遵循。[3]

新版管理系統標準 MSS 已由原本 PDCA 模型修正為圖一模型，尤其在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。



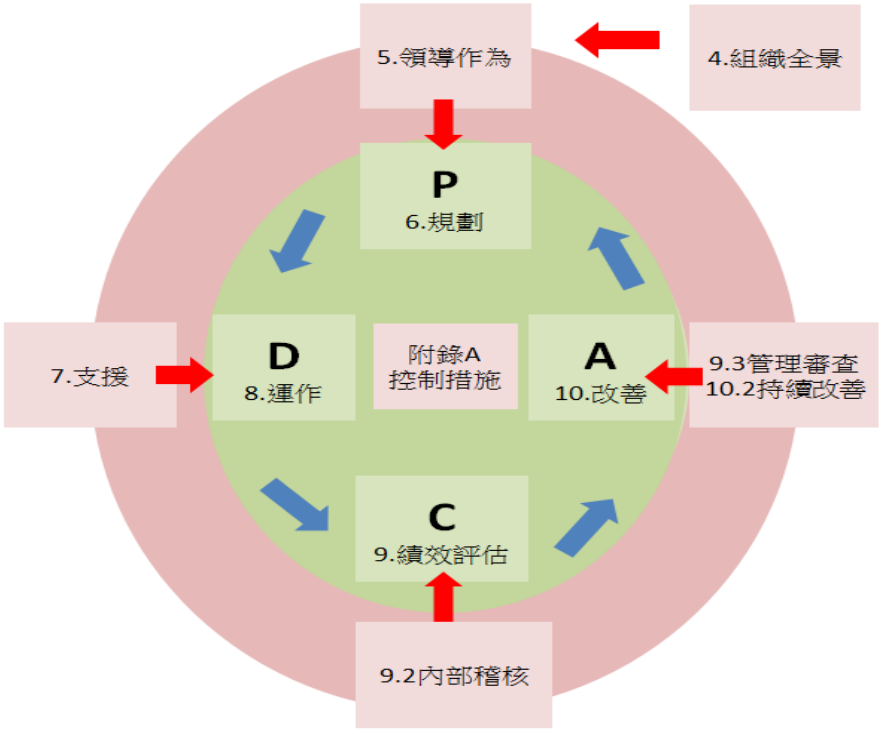
圖一： 根基於過程導向之管理系統的紀錄模型

2.4 新版 ISO 27001:2013 國際標準

ISO/IEC 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。[4]

本研究為使讀者更能了解 ISO 27001:2013，以圖二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。



圖二： ISO 27001:2013 整體架構圖

參、方法

本研究試著在本質上多角度探討 ISMS 與 PIMS 整合可行性，並進行多面向整合工作，最後提出 4 點實務上有效具體作法，並且以國防部網站系統為實作目標，驗證其具體作法可行性、有效性。

3.1 各角度探討整合可行性

本研究從以下 4 個角度探討整合可行性：

3.1.1 從資料生命週期角度：

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」，參考個資法所要求之個人資料各個階段生命週期[蒐集-處理-利用-儲存-銷毀]，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[產生-使用-儲存-傳輸-銷毀]，有異曲同工之妙。

3.1.2 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、完整性、可用性。

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]。

所以個資保護也包含資安的三項特性，後續可延伸在風險評鑑之風險值評等

3.1.3 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。後續如有更好的管理系統來取代，讓整合後更有效。

3.1.4 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。

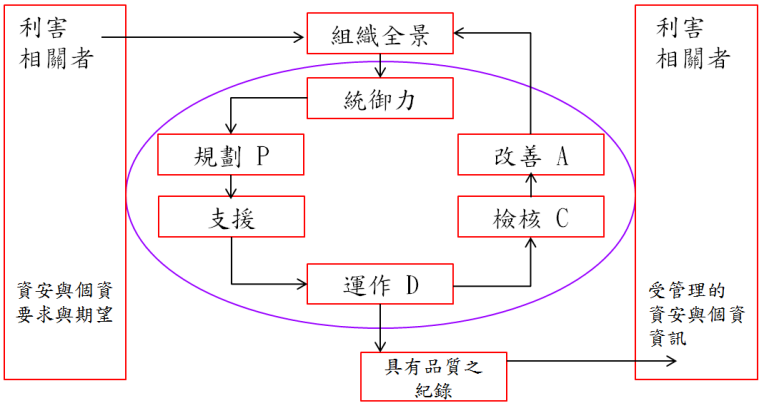
不管在資安上所探討的作業流程上所延伸的資訊流程，或者個資所提及的業務流程上所延伸的個資流程，均屬須在作業流程上去進行相關的風險管理機制。

3.2 進行多面向整合工作

本研究試著以 ISMS 既有作法及各角度探討之延伸整合六大部分：

3.2.1 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，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。



圖三：運用新版 MSS 整合 ISMS 與 PIMS 模型

3.2.2 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。

3.2.3 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。

3.2.4 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。

3.2.5 控制領域部分：

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，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。

3.2.6 四階文件部分：

實務工作上，在 ISMS 運作最後輸出須產出 ISO27001 適用性聲明；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，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。

3.3 整合後有效具體作法

在實務工作上本研究提出四點具體作法，讓有意導入或研究之 IT 人員能快速且有效進行整合導入工作，內容如下：

3.3.1 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，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。

3.3.2 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，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，以作業流程角度完成清查作業。

3.3.3 資訊資產及個人資料風險評鑑作業

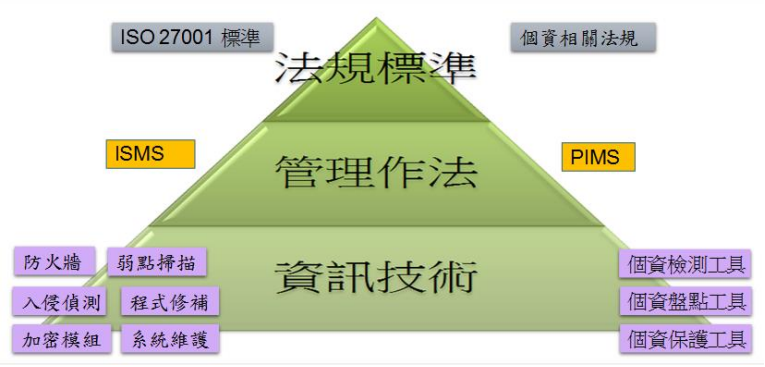
參照現有 ISO27005 風險評鑑作法，利用 CIA 等級及風險評鑑作業，整合資訊資產與個人資料項目，並依個人資料敏感性區分 CIA 等級，如特種個資，列為最高評分數值，產出一致化風險評鑑報告，以利於後續規劃因應及處置措施。

3.3.4 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)。

肆、結論

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，如圖四所示。



圖四：資訊安全三層概念圖

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。

在本文明顯發現 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。

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；本文所提出各面向整合工作與具體作法，以國防部網站系統為實作目標實施，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，經驗證通過(如 103 年 12 月 26 日青年日報報導)，也證明本研究確實有效，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，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，確保民眾權益，並達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。

[誌謝]

本文承蒙政治大學左瑞麟老師、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，方能順利完成，特此致謝。

參考文獻

[1] ANSI, " Justification study for a new work item proposal for a energy management standard ad guidance document," 2007.

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

[3] ISO, "Information and documentation – Management system for records – Fundamentals and vocabulary," *ISO,* ISO DIS 30300:2010-05-21, 2010.

[4] 張文瀞, " ISO27001:2013 和 ISO27001:2005 的主要差異,"*臺灣大學計算機及資訊網路中心,* 發行 ISSN 2077-8813, 2014. http://www.cc.ntu.edu.tw/chinese/epaper/0030/20140920_3003.html

[5] 經濟部商業司, "TPIPAS 臺灣個人資料保護與管理制度規範," 2012. http://www.tpipas.org.tw/model.aspx?no=159

[6] 鄭東昇, "資訊安全管理系統與企業網路安全實作探討," *碩士論文*,交通大學資訊管理所, 2005.

[7] 鄭伊雯, "植基於 ISO 27001 建立符合 BS 10012 之 個人資訊管理自我評鑑模式," *碩士論文*,中原大學, 2012.

[8] 樊國禎, "ISMS 新版實作初探：擴增 MSS 的 ISMS 初論之一," *103 年第 1 季資訊安全管理系統標準化系列討論會*,經濟部標準局, 2014.

[作者簡介]

孫天貴，國防部資訊官，曾擔任八軍團、馬防部、部辦室機房管理軍官，經歷菲律賓攻擊國防部網站 DDOS 事件、洪仲丘事件後駭客攻擊國防部網站、行政院資訊院攻防演練、國際駭客支持學生反課綱活動攻擊國防部網站。

左瑞麟，政治大學資訊科學系副教授，研究興趣為資訊安全與密碼學相關領域。