陸軍核心資訊系統導入 ISO 27701關鍵成功因素之研究

林于令[1] 廖偉明[2]

[1] 國防大學管理學院
[2]國防大學陸軍指參學院

摘要

隨著科技快速發展，網路安全和資料防護成為維護個人資訊安全的重要課題。在陸軍核心資訊系統裡，陸軍官、專校校務系統中，仍具有軍職及學員師生等個人資訊情形，亦肩負防範系統內部個資外洩之責任，本研究藉由汲取資訊安全整合個資管理要求、安全防護實作案例及個人資訊管理系統(PIMS)導入相關運用文獻等現存窒礙問題，期可找出陸軍核心資訊系統導入 ISO 27701關鍵成功因素，經文獻蒐集及專家問卷作業後，獲得「資安及個資政策」4項主準則及「組織個資法規遵循性」計15項次準則，建構了本研究之決策層級架構，再運用層級分析程序法(AHP)問卷調查結果，確認各項準則之權重值，俾作為系統導入規劃之決策優序參考。依分析結果，本研究歸納了「導入個資管理系統，防範資訊洩漏威脅」等三項結論，並據以提出了「強化人員素養評估與教育訓練」等三項具體建議，期可做為爾後陸軍核心資訊系統導入 ISO 27701之決策發展方向，進而強化組織的資訊安全架構和個人資料保護能力，提升系統的防護效能和韌性，應對目前及未來可能面臨的資訊安全威脅為目標。

關鍵詞：陸軍核心資訊系統，資訊安全，個人資訊管理，層級分析程序法

壹、前言

隨著科技的數位化，也伴隨著資安風險增加，在現代戰爭已成為主要趨勢，影響國防安全甚鉅，在近年因網路漏洞導致企業及機關重要資訊遭竊情事，從預防駭客侵害及個資防範角度來看，個人可識別資訊的控制者與處理者，均需要有效方式管制個人資訊及資訊安全。故相關認證標準應運而生，無論是 ISO 27001資訊安全管理系統(Information Security Management System，ISMS)管理標準政策或衍生額外控制措施，來處理個資特定資安威脅、風險及隱私資訊管理之 ISO 27701隱私資訊管理系統又稱為個人資訊管理系統(Personal Information Management System，PIMS)，對於保障個人隱私和資訊安全也在逐步加強資安法令的制定與執行。個人資料保護法的實施，在國際上個資保護意識也隨之提升，特別是2018年歐盟開始實行的《一般資料保護規範》又稱為《通用資料保護規則》(General Data Protection Regulation，GDPR)個資保護法令。這些法令促使組織必須以資訊安全管理為基礎，確保在其運作流程中對個人隱私資訊的處理符合相關法規的要求，從而實現個人資料的保護。[1]衍生出 ISO 27701來強化個資隱私管理，其標準為 ISO 27001 在個資管理上之延伸。

2016年在歐盟推行一般資料保護規範(GDPR)以更新其個資保護法規之後，我國在多次修訂個人資料保護法的過程中，並未設立專門負責個資保護的獨立機構，[2]而 ISO 27701標準源自於 ISO 27001資訊安全管理系統，專注於隱私資訊的妥善管理。該標準雖未直接受到特定法規，如：我國個資法或歐盟一般資料保護規範(GDPR)的影響，卻基於資訊安全管理的原則，有效整合隱私保護措施。在數位化和網際網路的進步，個人資料的處理方式已經從傳統的紙本方式轉變為數位化存儲和處理。這種變化意味著個資不僅可以被他人大量蒐集和利用，而且更容易暴露和被誤用。如此一來個資一旦外洩，不僅容易被不法分子濫用，還可能對當事人造成詐騙風險，引發社會恐慌，甚至影響國家安全。[3]例如在2016至2017年期間一名海軍士官吳姓士官，濫用其在處理人事業務時獲得的資訊。他獲悉國防部、空軍司令部等高層級單位長官的人事系統帳號及密碼，並涉嫌非法使用這些帳號和密碼侵入國軍的人力資源管理和人事管理資訊系統，進行未授權的查探；另一名曾任職於國防部人事單位的陸軍後勤訓練中心鍾姓上尉人事官涉嫌未經授權登入人事資料系統，非法查閱將官的個人資料。[4]上述行為顯示了資訊安全及個人資訊管理中的重大漏洞，特別是在處理敏感的人事和人力資源資訊時。這種未經授權的行為不僅違反了資訊安全的基本原則，還可能危及相關人員隱私和安全，並對組織的整體運作和信譽造成嚴重損害。

而在陸軍核心資訊系統中以陸軍官、專校之校務系統內，仍建有大量軍職及學員師生之個人資訊，更具有風險，雖然已導入 ISO 27001標準，但僅著重於資訊安全管理的整體流程，包括對機構資訊資產的風險管理、安全控制、政策、程序及員工訓練等方面。[5]對於個人資訊管理方面相對有限，主要因為設計重點不在於詳細的個人資料保護控制措施。故本研究以陸軍核心資訊系統導入 ISO 27701關鍵成功因素之研究為探討標的，將權重分析排列優序作為爾後執行陸軍核心資訊系統導入個人資訊管理之參據。

貳、文獻探討

一、陸軍核心資訊系統與個人資料保護

(一)陸軍核心資訊系統概述

國軍依「資安事件通報應變指導要點」及「行政院資通安全管理法施行細則」要求，在資訊資產核心資訊系統依重要性區分作戰指管、戰備訓練、管理資訊及行政教育類等四類說明如下: [6]

1.作戰指管類：直接用於作戰指管系統，包含衡山戰情系統、迅安系統、寰網系統、聯成系統、電子戰、網路戰、情報系統及監偵系統等其他。

2.戰備訓練類：直接用於戰備或演訓系統。

3.管理資訊類：用於作業管理系統，包含政戰、人事、主財、後勤、計畫、行政、醫療及通資電系統等。
4.行政教育類：用於行政作業或一般教育訓練，包含民網、訓練教室等內網電腦、備用資訊資產及其相關管理設備。

在國軍面對嚴峻網路攻擊與挑戰，組織更需要採取全面的政策來管理和保護其核心資訊系統，包括強化資安稽核、配置資安專責人員、即時情資共享回報、職能訓練及資料傳遞安全等機制，[7]定期進行風險評估和安全審查，以及培訓員工提升其對資訊安全的意識。現今陸軍在「國軍資通安全責任等級分級作業指導」要求下，所律定之資通安全責任等級B級以上機關及學術單位，核心資訊系統應導入「CNS27001」或「ISO 27001」等資訊安全管理標準。藉資通系統防護需求分級原則，機密性、完整性、可用性及法律遵循性等四大構面，識別核心資訊系統，並依資通系統防護基準執行控制措施。且陸軍在資通安全維護計畫裡，明確以「系統重要性、業務失效影響程度及最大可容忍中斷時間評估」歸納出核心業務及重要性如表一，訂定資訊安全管理機制，加強資訊系統防護，確保重要資訊之機密性、完整性及可用性。

在陸軍核心資訊系統中陸軍軍官及專科學校校務系統內，所維管軍職、學員師生及畢業校友學籍裡，仍存有個人資訊情形，相對具有風險存在。此外，當個人資訊透過電腦科技及網際網路進行儲存、處理或交換時，這些資料便有具可被長期保存、容易複製、方便使用及快速傳輸之特性。這些特性使得個資更容易被暴露或誤用。在數位時代，確保個資的安全，以及保護資訊隱私權和資訊自主權，亦是全民必須面對的重要且嚴肅的課題。特別是個資外洩後的通知機制，對於政府來說是一項極需重視的個資保護事項。不僅要採取措施保護個資，還需要制定有效的政策及程序來應對可能的資訊洩漏。[8]在個人資料保護法實施後，對於未能有效保護個資的組織，特別是其資訊部門，通常難以逃避責任。因此，確保強化資訊安全措施，並遵循相關法律規範，對於預防個資外洩風險更是重要。然核心資訊系統已是現代支撐組織運作的基礎，其管理和保護個資更是一個持續的過程，不僅需要技術上的創新，更需要全面的風險管理和法律規範意識，確保個資的安全和組織的可持續發展。

表一：陸軍核心業務及重要性統計表

單位	核心系統	重要性說明	業務失效影響說明	最大可容忍中斷時間
陸軍司令部	陸軍全球資訊網站	業務推展重要系統。	系統中斷將影響核心業務推廣。	36小時
	陸軍軍網網站			36小時
陸軍後勤指揮部	後勤資訊系統	提供三軍後勤補保作業。	系統失效將影響三軍單位後勤補保作業運用。	1小時
陸軍軍官及專科學校	教務(校務)自動化系統	維管軍職、學員師生及畢業校友學籍資訊管理。	系統失效將影響校務推展。	24小時

資料來源：本研究整理

(二)個人資料的重要性與風險

隨著個人資料保護法的實施，許多機構和企業需要重新評估他們對個人資料的處理方式，以確保符合法律要求。在我國個資法起源於「電腦處理個人資料保護法」，由於新法的實施代表著個人資料保護的重要，這反映出社會對個人資料重視程度的提升，這不僅是一個法律問題，同時也是資訊安全和隱私權保護的關鍵，在制定個資法時，參考了國際上的多項個人資料保護法條及隱私保護架構，如世界經濟合作暨發展組織(Organization for Economic Cooperation and Development，OECD)的隱私保護指引，[9]是全球隱私保護的基礎，並為跨國境資料傳輸活動的發展提供了指導；[10]亞太經濟合作組織(Asia-Pacific Economic Cooperation，APEC)的隱私保護機制，[11]提升我國隱私保護形象，促進對外跨國境數位貿易發展與合作。[12]

根據國際個資法條及隱私保護架構發展出一系列的個資保護標準和指引，以ISO 國際標準組織於2019年發佈 ISO 27701著重在隱私與個資的保護，利用資訊安全管理基礎延伸，涵蓋隱私保護的個資管理標準，[13]在我國個人資料保護法對於機構與企業在善盡個資告知上都有所規範，特別強調管控個資當事人的權益。這些指引主要集中在隱私權保護、資料安全、個資的適當使用和存取控制等方面，確保個人資料的處理、蒐集與利用等行為保障，也同時保護個人隱私。

現今面對網路安全挑戰及整個產業的轉型改變，將致使整個網路安全領域受到極為重大的潛在衝擊，其面臨的不只是資訊安全作為，更應重視個人隱私資訊安全。然資安事件多數違規行為涉及郵件帳號被利用，寄送社交工程的釣魚郵件，以及惡意程式垃圾郵件。統計近年公務機關個資外洩情形如圖一所示。[14]在陸軍單位經由資通安全責任等級分級屬B級以上之單位，近年陸續藉導入 ISO 27001標準提升資安防護等級，雖然資訊系統有完善防護措施，仍須藉由管理制度整合資訊安全及個資保護，建立適當安全維護措施，來提升其資訊安全管理和個資保護的成熟度，不僅符合法律要求，同時也保護組織內部員工及外部關注方的隱私權。

歷年公務機關個資外洩事件表

時間	事件內容
2023年1月	華航會員資料庫遭駭，國外論壇公布會員資料，包含賴清德、張忠謀、林志玲等人。
2023年1月	健保署前主秘葉逢明、現任承保組科長謝玉蓮、職員李仁輝三人，疑竊取民眾及11情治單位健保資料長達13年，遭調查局偵訊。
2022年12月	部立桃園醫院遭爆採用中國醫療資訊系統(內有簡體中文附註的程式碼)，自2020年8月起遭駭，竊取個資與醫護資料，部桃新聞稿稱案發後即請資安公司鑑識，僅有一台主機資料遭竊，且內無個資。
2022年10月	戶政資料遭駭，並在外國論壇公開兜售，疑為2,357萬餘筆。
2020年5月	美國資安公司Cyble 在暗網發現外洩資料庫，內容稱是全臺戶籍資料，包含超過2千萬筆民眾個資，資料庫來源是內政部戶政司。
2019年6月	銓敘部爆發公務人員個資被置於國外論壇販賣案，外洩資料內含國安局等機敏機關，超過20萬筆公務員資料。
2016年7月	勞動部勞發署發現所屬之「台灣就業通」網站，遭民間債務催收公司駭入，竊取5萬8千多筆求職民眾個資，以賺取催收債務傭金。
2016年5月	中華郵政商城因網站漏洞遭中國駭客侵入，逾1.7萬筆的交易資料遭竊

圖一：歷年公務機關個資外洩事件統計
資料來源：自由時報

二、ISO 27001、ISO 27701整合與應用

(一)ISO 27001資訊安全管理標準定義

ISO 27001是一個國際認可的資訊安全管理系統(ISMS)標準，旨在幫助組織保護和管理其資訊資產，以確保保密性、完整性和可用性。此標準由國際標準化組織(ISO)和國際電工委員會(IEC)共同制定，進一步提供了一個框架，使組織能夠透過有效的風險管理和適當的安全控制措施來應對資訊安全威脅。[15]

核心主要涵蓋建立、實施、運維、監控、審核、維護和改進資訊安全管理系統，是一個持續的過程，要求組織評估其資訊資產所面臨的風險，然後根據這些風險實施適當的管理和技術控制。[16]該標準的一個關鍵元素是持續的改進和周期性的資訊安全管理系統審核，以確保其持續適應不斷變化的威脅環境。實施 ISO 27001不僅僅是技術上的投入，還需要組織文化的變革，組織必須確保員工對資訊安全的重要性有充分的認識，並在日常工作中貫徹這一理念。此外，也強調領導階層的承諾與支持，對於建立與維護有效的資訊安全管理系統至關重要，也涵蓋了廣泛的資訊安全控制領域，包括資產管理、人力資源安全、實體環境安全、運營管理、存取控制、資訊系統的獲取、開發和維護，以及資訊安全事件管理。

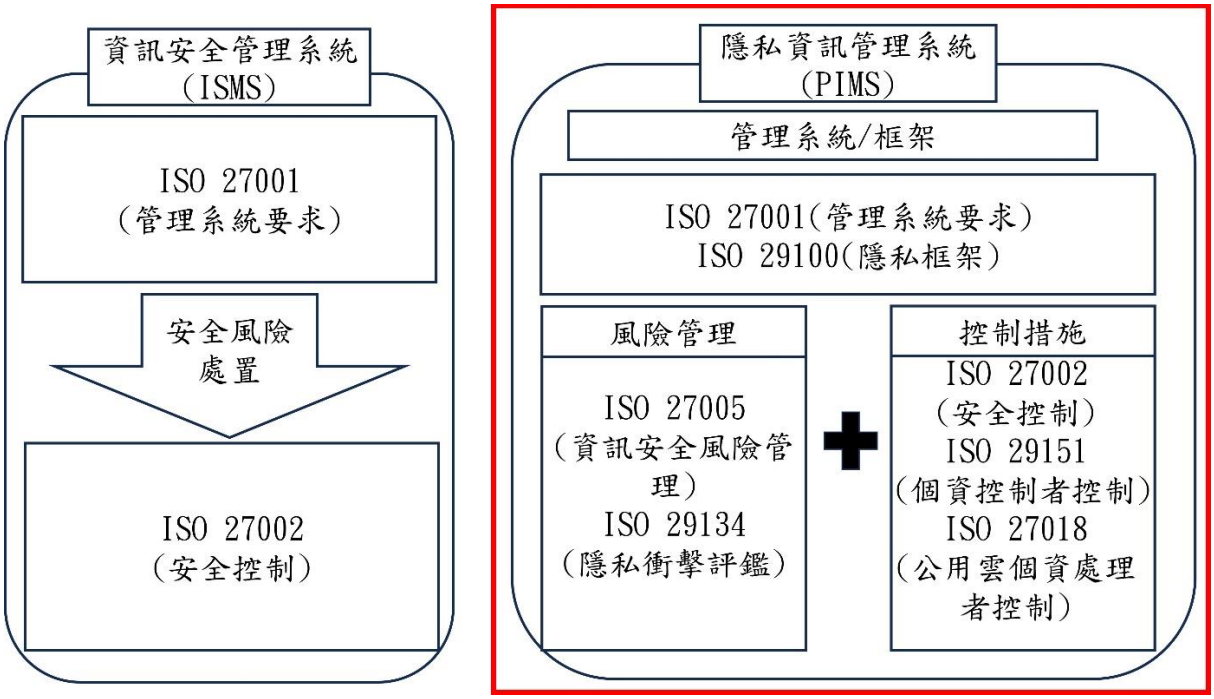
資訊安全管理系統標準在著重於機構整體的資訊安全管理，當涉及到特定的個人資料保護和隱私管理時，ISO 27001顯得不足。因為 ISO 27001主要關注的是保護組織的資訊系統和資產免受安全威脅，並沒有特別強調個人資料的隱私保護。然而，ISO 27701擴展了 ISO 27001的框架，包含了針對個人資料控制者和處理者的額外要求和控制措施，進一步強化了個人隱私數據的保護。[17]

(二)ISO 27701隱私資訊管理標準定義

ISO 27701「隱私資訊管理系統-個人可識別資訊的處理要求」，是針對隱私保護的國際標準。該標準於2019年推出，旨在幫助組織建立、維護並持續改進隱私資訊管理系統(PIMS)。這一標準是基於 ISO 27001資訊安全管理系統和ISO 27002資訊安全控制措施的實踐指南的框架，專門針對個人可識別資訊(PII)的管理進行了擴展和補充。[18]

主要在於幫助組織管理隱私風險，同時確保符合日益嚴格的全球隱私法規，如歐盟的一般資料保護規則(GDPR)、加州消費者隱私法(CCPA)及我國個人資料保護法等。這一標準為組織提供了一個明確的指南，用於管理和保護個人資料，並確保這些資料的合法、公正和透明的處理。[19]

兼顧隱私保護和個資安全管理的ISO 標準，利用原資訊安全風險評鑑程序來識別與處理個資相關的風險，確保評鑑流程能讓資訊安全與個資能適當的被保護管理。識別風險後對潛在影響做分析評鑑及處理，且要求與附錄 A、附錄 B 及 ISO 27001(資訊安全管理系統)的附錄 A 控制措施進行比較，確認必要之控制措施是否有遺漏情形。ISO 27701(隱私資訊管理系統)除包含 ISO 27001(資訊安全管理系統)與 ISO 27002(資訊安全、網路安全和隱私保護—資訊安全控制措施)外，亦整合了 ISO 27005(資訊安全風險管理)、ISO 27018(公用雲個資處理者控制措施)、ISO 29151 (個資控制者控制措施)、ISO 29134 (隱私衝擊評鑑)、ISO 29100 (隱私框架)等現有個資相關標準，是一個整合設計的國際標準如圖二所示。[20]



圖二：PIMS 關係架構圖
資料來源：本研究整理

(三)整合運用效益說明

在資訊安全與隱私保護的領域中，ISO 27701、ISO 27001與個人資料保護法的整合，是實現全面資安治理的關鍵。ISO 27701與 ISO 27001分別代表隱私資訊管理與資訊安全管理的國際標準，而個資法則是具體的法律規範，用以保護個人資料。這三者的整合不僅能提升組織的資訊安全水平，還能確保符合法律要求，從而增強對內部所屬人員與公眾的信任。[21]

ISO 27001聚焦於建立資訊安全管理系統(ISMS)，涵蓋了資訊資產的保護、風險管理及持續改進。而 ISO 27701則是在 ISO 27001的基礎上，增加了隱私資訊管理的要求，尤其是針對個人資料的處理。這使得 ISO 27701成為擴展至隱私保護領域的自然選擇。[22]

與此同時，個資法規範了個人資料的蒐集、處理及利用方式，要求組織必須確保資料的安全與隱私。[23]這不僅要求技術性的資訊安全措施，還包括組織流程與政策的合規性。整合這三者意味著在建立資訊安全管理系統時，同時考慮到隱私保護的要求與遵守相關法律。[24]組織需評估其資訊系統與流程中涉及的個人資料類型、處理方式及其相關的風險。基於此，制定相應的資安政策與流程，並將隱私保護融入其中如表二所示。

保護個人資料不僅是法規遵循的問題，更是國家安全和部隊士氣的關鍵。通過 ISO 27701導入整合是實現全面性資訊安全治理的核心策略，涵蓋資訊資產保護、風險管理與持續改進，並添加了對隱私資訊管理的要求，陸軍單位能夠展示其對保護個人資料的承諾，並在國際上表明其對於高標準隱私保護的堅持。不僅可提升軍隊的聲譽，也強化對內部所屬人員和外部關注方的信任。

表二：整合 ISO 27701、ISO 27001 與個人資料保護法的關係

整合項目	ISO 27001 資訊安全管理系統	ISO 27701 個人資訊管理系統	個人資料保護法
目的與範圍	建立資訊安全管理系統(ISMS)，保護組織的資訊資產	擴展 ISO 27001 以包含隱私資訊管理，特別是針對個人資料的保護	法律規定，保護個人資料免受未經授權的存取和處理
風險管理	識別、評估並處理資訊安全風險	包括針對個人資料處理的風險評估	要求針對個人資料處理活動進行風險評估
管理承諾	管理層必須承諾支持資訊安全政策與程序	同樣要求管理層的支持，並考慮隱私權益	法規要求組織領導層對個資保護負責
政策與程序	制定並實施資訊安全政策和程序	包含隱私保護的政策和程序	法律要求有關個資的處理、存取和保護的政策和程序
人員培訓	對員工進行資訊安全意識和培訓	包括隱私保護的培訓	要求對涉及個資處理的員工進行適當培訓
事故管理	建立和維護資訊安全事件和弱點的管理程序	擴展以包含隱私事件的回應	法規要求適當回應個資洩露或違規處理的事件
持續改進	要求持續評估並改進 ISMS	同樣要求持續改進，特別是隱私資訊管理方面	法律規範也鼓勵不斷改進個資保護措施

資料來源：本研究整理

三、導入 ISO 27701關鍵成功因素探討

運用 ISO 27701個人資訊管理系統(PIMS)導入陸軍核心資訊系統關鍵性成功因素之相關文獻，綜整各專家學者意見，歸納主要評估層面計4項、次要評估要項計16項，相關參考文獻說明如下：

(一)資安及個資政策

透過資訊安全管理系統之標準及個人資料保護法規範要求，結合資訊安全管理系統專業認知與訓練需求，完善個人資料安全防護機制，[25]保護個人資訊、增強當事人等相關利害關係人，對於組織在個人資訊管理上的信心，以符合法律及政策要求，故將「資安及個資政策」納為主要評估層面運用。

1.組織個資法規遵循性

個資法對公務機關和非公務機關在個人資料的蒐集、處理和使用上都有明確規範。公務機關需指派專人負責個資的安全與維運，而非公務機關則受其事業主管機關的監督與檢查。2010年的修正加強了這些要求，並在民事和刑事方面設定了相應的責任。違反法律的重大行為可能導致刑事責任和民事賠償。故組織必須確保其處理個資的過程符合個資法的規範，以避免潛在的法律風險，[26]因此將「組織個資法規遵循性」列為次要評估要項。

2.資安及個資安全風險評鑑

個資安全風險評鑑應該與資安風險評鑑進行整合，以確保資訊資產的全面保護。這包括識別並評估所有個人資料的價值，以及該資料可能面臨的風險。這種整合性的評鑑不僅有助於理解風險的發生機率，還能評估其對組織的影響程度，從而制定更有效的風險管理策略。[27]故透過這種方式，組織能夠更全面地理解並管理其面臨的資訊安全和個資

保護挑戰，確保遵守相關法律規定，同時保障組織和個人的利益，因此將「資安及個資安全風險評鑑」列為次要評估要項。

3.整合資安及個資管理機制

在個資管理系統(PIMS)的建置過程中，必須遵循相關的管理措施和技術指引。這包括了對 ISO 27701與 ISO 27001 標準的合規展現，特別是在進行個資管理系統驗證時。不僅符合資訊安全管理系統的要求，而且增強了含有個資的核心資訊通訊系統的驗證有效性，同時也展現了資訊安全與個資保護的合規性。[28]因此將「整合資安及個資管理機制」列為次要評估要項。

4. 緊急應變演練機制

緊急應變演練機制涵蓋事前安全防護、事中緊急應對和事後恢復作業。這需要制定全面的策略和程序，以確保在發生資安事件時，可以迅速有效地應對。事前安全防護包括風險評估、安全漏洞修補和安全意識培訓，旨在最大限度減少安全威脅。事中緊急應變則涉及實時監控、快速識別攻擊和有效應對策略，以控制損害並迅速恢復正常運作。

透過定期的演練和檢討，可以加強對網路安全威脅的應對能力，從而保護國家的資訊資產，[29]因此將「緊急應變演練機制」列為次要評估要項。

(二)人員素養要求

對於從事個資處理的員工而言，進行嚴謹的背景篩選和審查是不可忽視的一環。組織需要確保員工對於資訊安全的重要性有充分的認識，並具備相應的技術能力來處理個資。這不僅包括了對資料的安全存取和適當使用，也涉及了對任何安全漏洞的識別和回應。對於員工的持續教育和訓練更是重要，通過定期的培訓，員工能夠獲得最新的資訊安全知識和技能，從而能更好地識別和防範潛在的威脅。此外，鼓勵員工參與資安管理，並對其進行適當的賦權，可以提高他們對保護個資的責任感，[30]故將「人員素養要求」納為主要評估層面運用。

1.各類人員個資權責訂定

組織在個人資料管理方面應有明確的權責劃分，確保個資的完整保護與合法使用。這些資料需按何種保護層級進行保護。接著，必須確立個資保護政策，包括隱私權衝擊分析、業務活動資料焦點和關鍵環境的分析。這也涵蓋了確定個資的權責和所有權，評估存放系統的風險，並部署適當的保護與監控工具。[31]此過程在建立一個透明、可追蹤，且符合法律規範的個資管理框架，以保障組織與個人的權益，因此將「各類人員個資權責訂定」列為次要評估要項。

2.各權限人員個資認知教育訓練

確保組織在資料保護方面的持續改進與法規遵循。PDCA 模式的“Do”實施階段尤其重要，因為它涉及實際執行個人資訊管理系統和相關教育訓練。這一階段的核心目標是提高組織中所有員工的個資認知和處理技能。提高員工對個人資訊保護的意識。訓練應涵蓋資料的正確收集、處理、傳輸和保存方法，以及在個資洩露或其他相關安全事件發生時的應對措施。訓練計畫應依據員工的角色和責任進行分層，確保每個人都了解在個資管理中的具體職責，[32]因此將「各權限人員個資認知教育訓練」列為次要評估要項。

3. 制定違反法規處置作為

PDCA 在個人資訊管理系統中，”Act”維持與改善個人資訊管理系統(PIMS)的過程，此階段的是透過預防措施和持續改進來避免違反法規的事件。組織需制定具體策略，以確保所有處理個人資料的活動遵循適用的法律和規範。組織應進行全面的風險評估，識別與個人資料相關的潛在問題和風險。這包括分析數據處理流程中可能出現的安全漏洞，以及可能違反個資法規的行為。根據風險評估結果，制定和實施一系列預防措施，以減少違反法規的風險。這些措施可能包括加強員工培訓、更新內部政策、強化數據保護措施，以及改善數

據存取和處理程序，[33]因此將「制定違反法規處置作為」列為次要評估要項。

4. 委外廠商及組織個資保護

個資風險源自外部侵入及內部人員或委外單位的故意或過失行為。外部侵入風險無法透過內部制度預防，僅能依賴資安技術應對。而內部人員或委外單位所造成的風險，尤其是因過失行為導致的風險，則應透過公司內部制度的建立來降低。這些措施包括管理策略、教育訓練、事前監督、事後稽核及獎懲制度，以強化員工對個資保護的重視。[34]建立員工和委外廠商對法律風險的防火牆，進而對內部員工或委外廠商違反個資行為或資料外洩的情況，從而減少法律責任，因此將「委外廠商及組織個資保護」列為次要評估要項。

(三)系統保護機制

面對不斷進化的資安威脅，我們必須持續升級及完善安全措施，來保護數據和系統免受侵害，強化資訊系統保護機制顯得更為重要。在新的漏洞不斷被發現，也代表著資安攻擊方式不斷演變，所以加強系統弱點修正至關重要，更應建立一個完善的弱點管理機制，包括定期的系統掃描、漏洞評估及快速修補，確保資訊系統安全的基礎。

快速的漏洞修補對於維持系統安全更是重要。延遲修補可能使系統易受攻擊，增加數據泄露或系統損壞的風險。[35]強化系統保護機制應包括定期的系統掃描、評估及有效的漏洞修補，以確保資訊系統的整體安全，故將「系統保護機制」納為主要評估層面運用。

1.系統伺服器弱點檢測

系統伺服器的安全是組織資訊安全的基礎。要維持這一層安全，定期利用弱點掃描器對各種系統進行檢查至關重要。這些掃描器能有效辨識包括郵件、檔案、網頁伺服器及域名系統等在內的系統漏洞，甚至擴及個人工作站和電腦。透過這些掃描，系統管理員能及時發現並修補潛在風險。

系統管理員的角色不僅限於技術操作，還包括對資訊安全的深入理解。他們負責確保防火牆後的工作環境安全無虞，並執行系統掃描，迅速處理發現的安全漏洞。這樣的工作要求他們不僅要有技術知識，還要對資訊安全有全面的認識和實踐能力，[36] 以確保組織的資訊資產安全與完整，因此將「系統伺服器弱點檢測」列為次要評估要項。

2.系統網站滲透測試

網站滲透測試是一個關鍵的步驟，確保資訊安全和防止未經授權的訪問。這個過程涉及一系列謹慎設計的測試，模擬可能的攻擊情景來識別和修復潛在的安全漏洞。滲透測試的目的是最大限度地減少資訊洩漏的風險，增強網站對外部威脅的防禦能力。

定期進行滲透測試能持續監測和強化網站的安全狀態，隨著新威脅的出現和安全技術的發展，持續精進網站的安全，幫助組織在快速變化的資安環境中保持警覺，並對抗日益複雜和精密的網路威脅。[37]不僅保障了網站的安全性，還提高了用戶對網站可靠性的信心，進而支持業務的穩定發展，因此將「系統網站滲透測試」列為次要評估要項。

3.個資重要資訊去識別化

去識別化技術在保護個人資料方面日益成為一種重要且廣泛採用的趨勢。去識別化的目標是通過技術手段從個人資料中去除或修改能夠識別個體身份的資訊，從而在保護個人隱私的同時，仍能允許數據的分析和使用。組織應根據期望達成的特定效用和降低重新識別風險的需求來選擇合適的去識別化技術或機制。 [38]重要的是，組織應評估各種方法的安全性和實用性，以確保個人隱私，以最大限度地利用了數據的價值，因此將「個資重要資訊去識別化」列為次要評估要項。

4.系統存取、備份及加密措施

在系統存取控制的強化，限制並監控對敏感數據的存取，這包括用戶身份驗證、設定存取權限和審查追踪。透過這些措施，僅允許授權人員存取關鍵數

據，並確保所有存取行為均有記錄可供追蹤，提高安全性。落實資料備份是有效對抗數據遺失和安全事件的關鍵。這包括定期備份重要數據並將備份存儲在安全的位置。確保在數據損壞或系統故障的情況下，可以迅速恢復數據，保持業務連續性。資料加密是保護敏感資料的另一重要層面。無論是靜態數據存儲，或者動態數據傳輸，加密都能為個人和機構資料提供額外的保護層。確保即使數據被非法竊取，資料內容也無法輕易被解讀。[39]

這些措施的結合不僅提升了數位資產的安全性，也增強了對機構信譽的保護，為數據安全提供了堅實的基礎，因此將「系統存取、備份及加密措施」列為次要評估要項。

(四)實體及環境安全

增加犯罪阻力的作為涵蓋了改善實體安全環境和強化網路安全控制。這不僅包括保全辦公室、房間和設施的安全強化，也涵蓋了資訊交換的安全性、密碼控制措施及系統檔案的保護。這些措施的目標是透過加強安全控制來防止未授權的存取和犯罪行為。

另一方面，提升犯罪風險的作為著重於增加犯罪者被捕獲的可能性。這包括在犯罪易發生的地區實施有效的監控措施，如監視錄影和網路偵測系統。通過這些系統，能夠及時發現和回應潛在的安全威脅，從而有效地威懾犯罪者。此外，加強對第三方交付的管理、防範惡意碼和自動碼的措施也是關鍵。[40]故將「實體及環境安全」納為主要評估層面運用，透過這些綜合的安全措施，可以大幅提升整體環境的安全性，降低犯罪發生的風險。

1. 防範惡意攻擊或事故

為了有效防範惡意攻擊與事故，組織必須建立全面的資訊安全政策，並進行綜合性的風險評估與安全稽核。這涉及技術層面，有效建置防火牆、防毒軟體等防護措施，同時也要考量非技術面的因素，例如，制定應變可能遭駭客內、外部的資訊系統入侵。除此之外，防範自然災害和人為疏失造成的風險也同樣重要。[41]因此將「防範惡意攻擊或事故」列為次要評估要項。

2. 降低設備環境威脅及危害風險

實施有效的實體與環境安全措施是確保個資安全的重要一環。這些措施的主要目的是保護存儲個人資料的場所，防止未經授權的入侵、存取、洩漏、竊取或破壞。為此，組織必須對其重要基礎設施，如防火/防水設施、溫濕度控制、電力供應、網路傳輸和通訊設備等進行全面的安全評估，根據評估結果實施適當的防護措施，以實時監控和記錄任何可疑活動；以及確保重要的基礎設施如存放伺服器場所具有適當的防災和緊急應對設施。此外，應定期進行安全演練和檢視，以確保安全措施能處於最佳狀態，[42]因此將「降低設備環境威脅及危害風險」列為次要評估要項。

3. 無人看管之設備具備適切保護

在無人看管的設備存管，這可能包括設備存放在受監控的環境中，以防止未經授權的存取。例如，公司規範筆記型電腦及可攜式設備上鎖在指定儲櫃，或將重要伺服器存放至限制出入的機房中，而桌面清空政策是防止敏感資訊外洩的有效方法。這項政策要求員工在離開工作站時，必須清理桌面上的所有敏感文件和數位設備，以防止未經授權的人員查看或存取這些資訊。此外，應進行定期的宣導和訓練，以提高員工對於保護敏感資訊的意識。[43]因此將「無人看管之設備具備適切保護」列為次要評估要項。

4. 減少受侵害或破壞的損失

為了保護個人資料而採取的重要措施，它們的目的在於降低因個資遭受侵害或破壞可能造成的損失，藉隱私衝擊分析確保在個人資料的收集、處理和利用過程中，相關的管理政策、作業流程、人員管理及系統控制技術符合保護個人隱私的基本要求，並以個資風險評鑑識別經過個資盤點確認的個資項目中存在

的安全風險，並分析風險由哪些弱點和威脅造成，以降低個資遭受侵害或破壞可能導致的有形和無形損失，[44]以減少個人資料被不當使用、洩露、遺失或破壞的風險，因此將「減少受侵害或破壞的損失」列為次要評估要項。

參、研究方法與設計

首先，藉由文獻探討建立主要評估層面及次要因素，再透過專家訪談確立層級架構，建立主、次準則，並運用分析層級程序法(Analytic Hierarchy Process , AHP)設計問卷，以產出各準則 之權重。

一、層級架構流程設計

本層級架構流程區分二個階段，第一階段為「層級架構建立」，第二階段為 「主、次準則權重確立」，分述如下：

(一)「層級架構建立」階段

運用文獻探討所發展出的初步主要評估層面及次要因素，設計專家問卷，並針對相關專家進行問卷調查，綜整專家共識，確立關鍵成功因素之層級架構。

(二)「主、次準則權重確立」階段

依前一階段所確立之層級架構，利用層級分析法(AHP)設計問卷，針對任職資訊作業制度及執行系統涉及個資處理之政策、管制及作業等人員，比較各影響因素，以獲得本研究主、次準則權重。

二、層級架構建立

(一)評估要項歸納

本研究經文獻探討，彙整相關主要評估層面計需求規劃釐訂等4項，次要因 素共計16項(如表三)。

(二)專家問卷發展

本研究將專家問卷範圍設定為涵蓋國防部通次室、陸軍司令部通資處、陸勤部及陸軍官、專校等，以前述單位內對資訊安全決策、管理及執行資訊系統維護具有豐富經驗之專家為對象(如表四)。本次專家訪談採「自填式問卷調查」方式執行，為使受訪專家確實瞭解問卷目的，已透過問卷說明、個人基本資料、主層面與次要素定義及層面要素選定欄位等完成問卷設計。

(三)確立層級架構

本次專家問卷調查表於民國112年12月18至22日，針對10位專家透過線上及紙本問卷發送、回收或輔以電話訪談方式進行，共寄送或訪談合計10 份，回收10份。經彙整專家意見後得知，影響陸軍核心系統導入 ISO 27701之關鍵成功因素計有 4 項主準則及 15 項次準則(如圖三)；其中在主、次準則經專家建議(主準則：人員素養評估；次準則：組織人員個資權責訂定、防範惡意攻擊與事故應處、風險管控作為)實施修改，且有1項次準則(制定違反法規處置作為)勾選數過低，顯示對本研究關鍵成功因素較無影響，故將此項刪除。

三、AHP 問卷設計

本階段執行目的，係為確立陸軍核心資訊系統導入 ISO 27701關鍵成功因素研究之主、次準則權重及其次序；首先以前階段綜整專家意見建立之層級架構為基礎，依層級分析法完成 AHP 問卷，問卷發放範圍層級為國防部通次室、陸軍司令部通資處、陸軍後勤指揮部、陸軍軍官及專科學校等單位，實際從事資訊業務之人員為問卷訪談對象，由受訪者針對各主、次準則進行兩兩成對比較。續以 AHP 法應用軟體(Expert Choice 11)實施權重驗證及確立。

表三：主要評估層面與次要因素一覽表

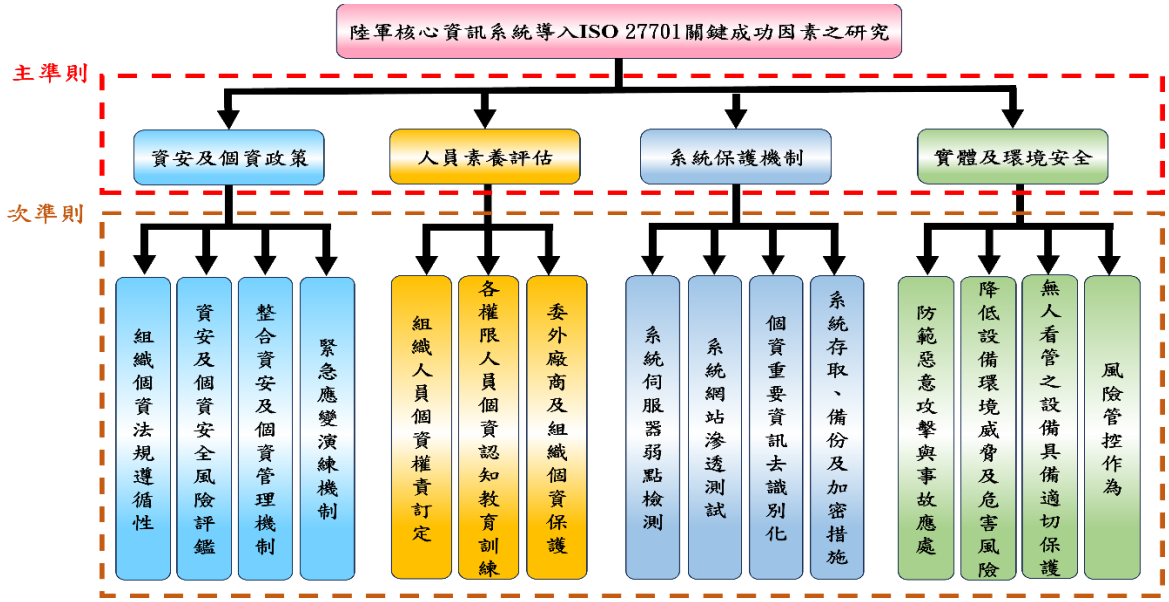
陸軍核心資訊系統導入ISO 27701關鍵成功因素	
主要評估層面	次要因素
資安及個資政策	組織個資法規遵循性
	資安及個資安全風險評鑑
	整合資安及個資管理機制
	緊急應變演練機制
人員素養要求	各類人員個資權責訂定
	各權限人員個資認知教育訓練
	制定違反法規處置作為
	委外廠商及組織個資保護
系統保護機制	系統伺服器弱點檢測
	系統網站滲透測試
	個資重要資訊去識別化
	系統存取、備份及加密措施
實體及環境安全	防範惡意攻擊或事故
	降低設備環境威脅及危害風險
	無人看管之設備具備適切保護
	減少受侵害或破壞的損失

資料來源：本研究整理

表四：專家背景表

項次	單位	級職	學歷	實務經驗年資
1	國防部通次室	上校副主任	博士/戰院(略)教育	24
2	國防部通次室	少校資參官	大學(專科)/正規班	10
3	陸軍司令部	上校副組長	博士/戰院(略)教育	24
4	陸軍司令部	中校電督官	碩士/指參教育	18
5	陸軍後勤指揮部	中校副主任	碩士/指參教育	22
6	陸軍後勤指揮部	上尉資參官	大學(專科)/正規班	8
7	陸軍軍官學校	上校主任	博士/戰院(略)教育	26
8	陸軍軍官學校	中校副主任	碩士/指參教育	21
9	陸軍專科學校	中校主任	碩士/指參教育	25
10	陸軍專科學校	少校副主任	大學(專科)/正規班	17

資料來源：本研究整理



圖三：本研究之層級架構圖
資料來源：本研究整理

肆、研究方結果分析

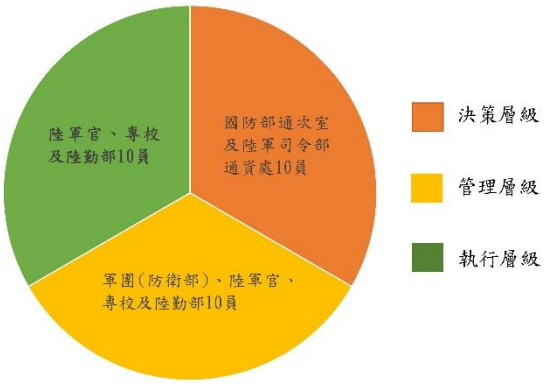
一、問卷資料分析

本次調查使用 AHP 問卷發放，將受訪對象區分為決策、管理和執行三個階層。決策階層受訪對象包括國防部通次室和陸軍司令部通資處資訊政策人員，共計10員；管理階層的受訪對象為軍團(防衛部)、陸軍官、專校及陸勤部資訊系統相關管理人員，共計10員；執行階層對象為陸軍官、專校及陸勤部資訊系統等作業單位人員，共計10員，總計30員。問卷發放30份，回收30份，回收率100%(如圖四)。

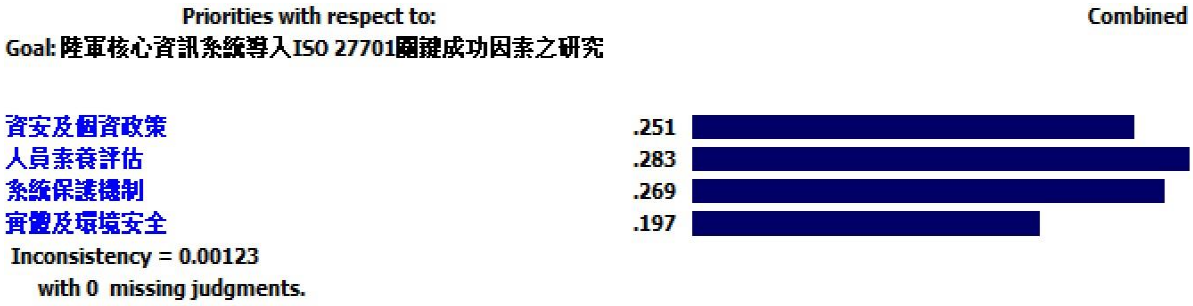
運用 AHP 應用軟體「Expert Choice 11」，對回收的問卷進行一致性檢測，當主準則及次準則的一致性指標(Consistency Index, C.I.)值>0.1時，則不予採用。在回收的30份問卷中，其中3份未能確保優劣或強度關係的遞移性，因此被視為無效問卷；而27份問卷則被視為有效問卷，因此以 27 份有效問卷為本研究決策體依據。

(一)整體主準則權重比序分析

整體評選原30份 AHP 問卷，其中3份 C.I.值均＞0.1不採用，餘27份 C.I.值均＜0.1，經軟體分析主準則之權重值優序為「資安及個資政策」0.251、「人員素養評估」0.283、「系統保護機制」0.269、「實體及環境安全」0.197，表示整體受訪人員認為「人員素養評估」相較於其他主準則重要，權重分析結果如圖五，權重優序表如表五。



圖四：問卷調查對象統計圖
資料來源：本研究整理



圖五：整體評選主準則權重分析結果
資料來源：本研究整理

表五：整體評選主準則權重優序表

主準則	相對權重	優序	一致性指標
資安及個資政策	0.251	3	incon=0.00123 With 0 missing judgment
人員素養評估	0.283	1	
系統保護機制	0.269	2	
實體及環境安全	0.197	4	

資料來源：本研究整理

(二)整體次準則權重比序分析

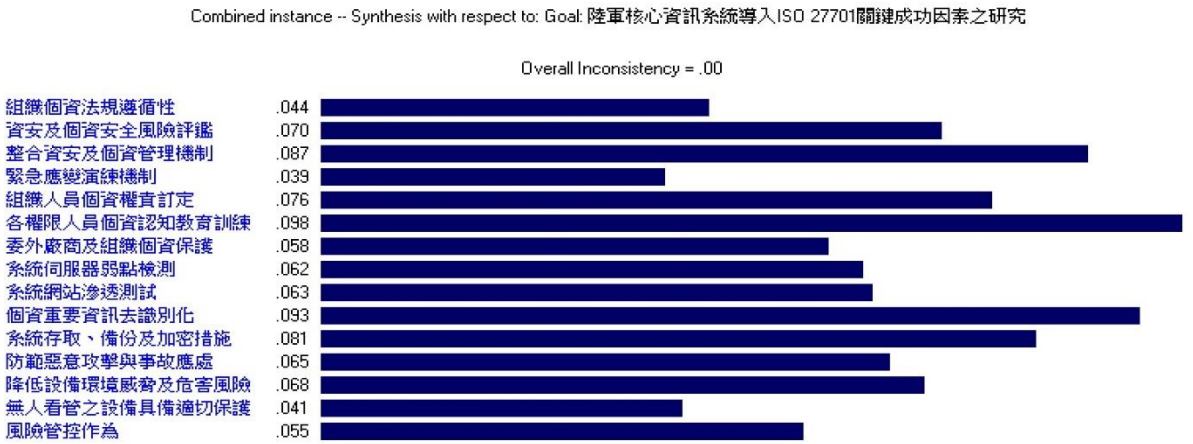
整體次準則權重比序前三優序為「各權限人員個資認知教育訓練」0.098、「個資重要資訊去識別化」0.093、「整合資安及個資管理機制」0.087，表示整體受訪者認為，「人員素養評估」主準則中的「各權限人員個資認知教育訓練」次準則較其它次準則為重要(如圖六)。

二、綜合分析

經問卷資料分析、彙整各階層主、次準則權重及優序分析(如表六)，顯示不同階層存在明顯差異，以下分就主、次準則權重差異分析歸納原因。

(一)主準則分析

綜觀表六可知，各階層受訪者對，針對本研究 4 項主準則權重排序大致相同，在決策階層受訪者認為「資安及個資政策」為首要，而在管理階層以「人員素養評估」為優先，則執行階層著重在「系統保護機制」，整體以「人員素養評估」為最高優序。



圖六：整體評選各次準則權重分析結果
資料來源：本研究整理

表六：各階層主、次準則權重及整體優序分析表

分類	項目	決策階層		管理階層		執行階層		整體	
		權重	優序	權重	優序	權重	優序	權重	優序
主準則	資安及個資政策	0.332	1	0.235	3	0.203	4	0.251	3
	人員素養評估	0.273	2	0.291	1	0.272	2	0.283	1
	系統保護機制	0.218	3	0.277	2	0.302	1	0.269	2
	實體及環境安全	0.177	4	0.198	4	0.223	3	0.197	4
次準則	組織個資法規遵循性	0.064	7	0.040	15	0.045	14	0.044	13
	資安及個資安全風險評鑑	0.111	2	0.067	8	0.055	10	0.070	6
	整合資安及個資管理機制	0.132	1	0.077	6	0.069	7	0.087	3
	緊急應變演練機制	0.039	11	0.050	12	0.048	13	0.039	15
	組織人員個資權責訂定	0.108	4	0.079	4	0.059	8	0.076	5
	各權限人員個資認知教育訓練	0.109	3	0.095	1	0.082	4	0.098	1
	委外廠商及組織個資保護	0.037	12	0.078	5	0.092	3	0.058	11
	系統伺服器弱點檢測	0.030	14	0.089	3	0.051	11	0.062	10
	系統網站滲透測試	0.023	15	0.091	2	0.070	6	0.063	9
	個資重要資訊去識別化	0.087	5	0.059	10	0.103	1	0.093	2
	系統存取、備份及加密措施	0.045	10	0.071	7	0.101	2	0.081	4
	防範惡意攻擊與事故應處	0.063	8	0.057	11	0.056	9	0.065	8
	降低設備環境威脅及危害風險	0.046	9	0.065	9	0.076	5	0.068	7
	無人看管之設備具備適切保護	0.035	13	0.042	13	0.044	15	0.041	14
	風險管控作為	0.071	6	0.042	14	0.049	12	0.055	12

資料來源：本研究整理

就「人員素養評估」而言，在陸軍核心資訊系統導入 ISO 27701過程，應於資訊系統處理個人重要資訊管理過程之人員審慎完成評估，並帶給單位組織對於個人資訊保護的承諾及後續效益通盤納入考量，作為陸軍核心資訊系統導入個人資訊管理(PIMS)之決策指標。其次準則為「組織人員個資權責訂定」、「各權限人員個資認知教育訓練」、「委外廠商及組織個資保護」等3項，在資訊作業人員管理政策支持下，為有效達到組織控制者及處理者在資訊安全內，執行個人資訊管理系統(PIMS)運作上，防範洩漏情事肇生為最終目的及效益，亦在個人資訊管理系統導入過程佔有較高之優序。

在決策階層的受訪人員，認為「資安及個資政策」最為重要，項下次準則計有「組織個資法規遵循性」、「資安及個資安全風險評鑑」、「整合資安及個資管理機制」及「緊急應變演練機制」等項，此階層屬政策決定人員，著重於政策推動與要求，認為確保組織在資訊安全和個人資料保護方面，必須從制度上制定全面的政策和措施。不僅涵蓋了遵守相關法律法規的必要性，也包括了對潛在風險的評估及緊急應變演練機制來提升組織整體的應對能力，為精進組織在面對潛在資安事件時的準備和應變能力為最高優序。

而執行階層的受訪人員，則認為「系統保護機制」最為重要，項下次準則計有「系統伺服器弱點檢測」、「系統網站滲透測試」、「個資重要資訊去識別化」及「系統存取、備份及加密措施」等項，此階層屬系統作業最密切之維護人員，著重於資訊系統的防護，認為防範威脅和保護資料安全有著直接的責任和需求，維護系統安全不僅有助於防範外部攻擊，也能有效地管理內部資源，確保資料安全和系統穩定性。此外，組織能夠有效應對日益複雜的資訊安全威脅為重要關鍵因素。

(二)「資安及個資政策」次準則分析

決策、管理、執行及整體階層在「資安及個資政策」主準則中權重最高優序首重於「整合資安及個資管理機制」次準則。

陸軍核心資訊系統導入 ISO 27701過程中，需在保障資訊系統與個人資訊安全的同時，確保符合國內外日益嚴格的隱私保護法規與標準。隨著個資保護法規的全球化，以及個人資料在國防安全中扮演的關鍵角色，導入 ISO 27701成為確保資訊安全管理系統(ISMS)中，個人資料處理活動符合隱私保護要求的重要性，故各階層受訪人員以「整合資安及個資管理機制」為最高優序次準則。

(三)「人員素養評估」次準則分析

決策、管理階層在「人員素養評估」主準則中權重最高優序皆首重「各權限人員個資認知教育訓練」次準則，執行階層則以「委外廠商及組織個資保護」次準則為優先。以「各權限人員個資認知教育訓練」為整體次準則最高優序，代表受訪者皆認為此項較其它2項為重要。

組織對於員工的選擇與培養為關鍵角色，尤其是在處理個人資料和資訊安全管理的工作中。這要求組織不僅要在聘用前進行嚴格的背景審查，確保員工沒有潛在安全風險，而且還需要考慮到他們的專業技能和對資訊安全的認識程度是否符合職位需求。並強調了持續教育和訓練在提升組織資訊安全和個資保護能力的重要性。此外，也有助於提高員工對資訊安全威脅的警覺性，使他們能夠在日常工作中識別和防範潛在的安全風險，上述乃為次準則「各權限人員個資認知教育訓練」獲得較高權重之原因。

而在執行階層，為了有效管理個人資料風險，組織必須制定一套全面的內部管理規章。這不僅涉及對個人資料的收集、處理、傳輸和儲存的規範，還包

(四)「系統保護機制」次準則分析

決策、執行階層在「系統保護機制」主準則中權重最高優序皆首重「個資重要資訊去識別化」次準則，管理階層則以「系統網站滲透測試」次準則為優先。以「個資重要資訊去識別化」為整體次準則最高優序，代表受訪者皆認為此項較其它3項為重要。

通過技術手段有效移除或變更個人數據中的可識別資訊，從而在保障個人隱私的同時，允許數據進行分析和使用，而不會泄露個人身份。能夠減少個人數據被誤用或非法使用的風險，提高數據處理的安全性，有此可見「個資重要資訊去識別化」為陸軍核心系統有效防護外洩個資威脅之重要關鍵因素。

而在管理階層，對於陸軍核心系統透過網站滲透測試，能夠通過模擬駭客攻擊的方式，有效識別網路系統中存在的安全漏洞和弱點。這種主動的安全評估方式使得管理層能夠在真實攻擊發生之前，及時發現並修復漏洞，從而顯著提高系統的安全性，故此階層受訪者，首重「系統網站滲透測試」次準則最為優序。

(五)「實體及環境安全」次準則分析

管理、執行階層在「實體及環境安全」主準則中權重最高優序皆首重「降低設備環境威脅及危害風險」次準則，決策階層則以「風險管控作為」次準則為優先。以「降低設備環境威脅及危害風險」為整體次準則最高優序，代表受訪者皆認為此項較其它3項為重要。

透過強化實體環境的安全控制和提升網路安全防護，來保障組織的資訊資產和個人資料免受未授權存取、洩露或破壞為重要關鍵，因此對於管理及技術受訪者而言，「降低設備環境威脅及危害風險」不僅可以提升組織對外部和內部威脅的防範能力，還可以增強員工和括對委外廠商的管理和監督。這些規章能夠確保組織免受潛在的安全威脅和法律挑戰，上述乃為次準則「委外廠商及組織個資保護」獲得較高權重之原因。用戶對組織資訊安全管理能力的信心，有此可見「降低設備環境威脅及危害風險」為提高組織系統防禦能力之重要關鍵因素。

而在決策階層，對於通過有效的風險管理措施，組織能夠提前識別潛在威脅，制定緊急應變計畫和復原機制，確保在面臨災難或攻擊時能夠迅速恢復維持正常運作，故此階層受訪者，首重「風險管控作為」次準則最為優序。

(六)整體次準則權重分析

由表六所見各階層主、次準則權重及優序分析，以「各權限人員個資認知教育訓練」、「個資重要資訊去識別化」及「整合資安及個資管理機制」為各階層受訪人員認為在15項次準則中較為重要的前三項，上述結果與主準則優序結果相互乎應，亦顯示不同階層之受訪人員依所處層級經驗與需求會定義不同之系統功能優序，歸納原因分述如後：

1.「各權限人員個資認知教育訓練」：於研討陸軍核心資訊系統導入 ISO 27701 關鍵成功過程中，由各階層受訪人員回饋意見內，以「人員素養評估」為最首要主準則，其中又以「各權限人員個資認知教育訓練」次準則為最高優序；教育訓練重要性在於提升員工的個資保護意識和能力，確保組織能夠有效管理和保護個人資料，達成導入 ISO 27701標準的要求，同時減少法律和潛在風險，實現個資安全管理成功的重要關鍵因素之一。
2.「個資重要資訊去識別化」：在陸軍核心資訊系統存有個人資訊，進而從事蒐集、處理及運用等行為，透過去除或匿名化個人可識別資訊，個人隱私得到有效保護，即使數據被洩漏，也難以追溯到具體個體，從而減少了個人資訊被濫用的風險，以降低個人資訊洩漏風險為重要關鍵因素之一。

3.「整合資安及個資管理機制」：陸軍核心資訊系統在面對日益複雜的資訊安全挑戰，以及嚴格的個資保護要求時能夠有效運作，透過整合資訊安全管理系統(ISMS)與個人資訊管理系統(PIMS)，組織能夠有效地識別、評估和管理資訊安全風險及個資保護的要求。促進組織提升對抗外部威脅(如網路攻擊和數據洩露)和內部風險(如員工過失或不當操作)的能力，確保資訊安全和個資保護措施有效實施及持續改進為重要關鍵因素之一。

伍、結論與建議

綜上研究與分析成果，本章提出以下結論及建議事項等兩節次，以呼應本研究動機與目的，作為陸軍核心資訊系統導入 IOS 27701關鍵成功因素之參據。

一、結論

(一)導入個資管理系統，防範資訊洩漏威脅

蒐集機構及企業組織導入 ISO 27701之相關文獻，隨著數位化和網際網路的發展，個人資料的處理方式已從傳統的紙本轉變為數位化儲存和處理。這種變化不僅提高了資料處理的效率，但同時也增加了資料洩露的風險。有效地主動識別並預防潛在的風險因素，確保陸軍核心資訊系統中的個人資料得到有效保護，已成為目前資訊安全管理的一大挑戰。隨著資訊科技的進步，資料的蒐集、儲存與處理變得更加迅速和廣泛，這使得資料管理和保護變得更加複雜。組織面臨的挑戰不僅在於如何防範外部威脅，也包括如何管理和控制內部人員對敏感資訊的存取，避免因操作不當或違反政策而導致資料洩露。採取資訊安全和個資保護管理，有效地識別個資處理活動中的風險，並採取適當的風險管理措施，以符合法規要求並保護個人隱私。

(二)分析層級架構，掌握關鍵需求

在陸軍核心資訊系統導入 ISO 27701過程中，最重要關鍵就是組織對於員工的人員素養評估，進而達到人員對個資管理的認識和執行能力之目的，並結合資訊安全技術和管理之運用，發掘現行陸軍核心資訊系統在個人資料管理方面之窒礙及不足部分，因此，陸軍核心資訊系統不僅應該對現有的個人資訊處理進行檢討，而且還應該考慮將個人資訊管理的最新發展和法規要求納入系統導入和整合的參考依據。透過嚴謹的風險管理和持續的改進措施，組織能夠有效分析和提升資訊處理的效率、準確性及運作效率，從而最大限度地發揮個資保護的效能。

(三)運用關鍵因素，導入陸軍核心資訊系統整合個資管理

陸軍核心資訊系統雖已建立資訊安全管理系統(ISMS)機制，但在個人資訊管理方面仍顯不足，且未訂定個人可識別資訊控制措施及如何實施和維護個人資料保護原則，導致現有系統無法有效管理個人資訊，增加了資料洩漏的風險，經由本研究問卷分析結果得之「各權限人員個資認知教育訓練」、「個資重要資訊去識別化」及「整合資安及個資管理機制」等3項關鍵成功因素，惟此次受訪者認為在15項次準則中，前3名優序。故陸軍核心資訊系統導入 ISO 27701需參考關鍵成功因素，首要導入過程，著重於提升人員素養和教育訓練，確保所有涉及個資處理的員工充分理解個資保護的重要性和相關法律法規，從而達到提高整體個資安全意識的目標；而次要準則中「個資重要資訊去識別化」及「整合資安及個資管理機制」對於有效個人資訊管理來說，都是有效提升組織的個人資料保護能力，降低數據洩漏的風險，保障個人隱私安全之必要條件。

二、建議

(一)強化人員素養評估與教育訓練：

組織進行人員的資訊安全與個資保護培訓是重要的一個階段，對於陸軍核心資訊系統維護及管理，通過定期的資訊安全與個人資料保護教育訓練，提升人員對於保護個人資料重要性的認識，

同時對人員進行能力評估，確保他們具備必要的知識和技能以安全處理個人資料。此外，教育訓練內容應根據最新資訊安全趨勢和法律法規更新，提升人員能夠應對新興的安全威脅和日益嚴格的法律要求，為導入 ISO 27701標準奠定堅實的基礎。

(二)同步實施資安及個資管理政策：

在陸軍核心資訊系統導入 ISO 27701標準同步實施資訊安全與個人資訊政策尤爲重要。是確保組織在處理個人資訊時，既能滿足資訊安全的需求，又能遵守個人隱私保護法律法規之關鍵。通過政策制定和實施過程中將資訊安全與個人資訊保護政策緊密結合，配合資安及個資管理四階文件整合，組織能夠建立一致的管理框架，有效地識別、評估和處理與個人資訊處理相關的安全風險。組織不僅能夠提高其對資訊安全和個人資訊保護的管理能力，還能增強對外部和內部威脅的防禦能力。

(三)持續更新系統保護機制：

在陸軍核心資訊系統導入 ISO 27701標準整個過程中，持續更新系統保護機制的重要性不容忽視。從啓動到長期維運階段，不斷地投資於最新的資訊安全技術和工具，定期進行系統的安全評估，以及及時發現並修補漏洞，對於系統維護安全性和數據保護至關重要。通過在各個階段實施持續更新系統保護機制，陸軍核心資訊系統能夠建立起一套動態、能夠適應不斷變化的威脅環境防禦體系。這將有助於提高組織整體安全態勢，確保個人數據安全和隱私得到有效保護。

參考文獻：

[1]《資訊安全與個資隱私的認證 － ISO 27001 與 ISO 27701 介紹》，(Medium)，2022/07/124<https://medium.com/kryptogo/資訊安全與個資隱私的認證-iso-27001-與-iso-27701-介紹-217b5a881178>，(檢索日期：2023年10月11日)。

[2]黃彥棻《【2021資安大預測】趨勢7：法規遵循｜臺灣資安法及個資法都面臨修法壓力》，(iThome)，2021年1月12日，<https://www.ithome.com.tw/news/142118>，(檢索日期：2023年10月12日)。

[3]彭文暉，〈數位時代個資外洩事故之通知機制研究〉《立法院法制局專題研究報告》，pp.3，2013年4月。

[4]《國軍人資系統連3年遭內鬼入侵》，(自由時報)，2020年5月28日，<https://news.ltn.com.tw/news/politics/paper/1375817>，(檢索日期：2023年11月27日)。

[5]《徹底詳解「資訊安全控制措施」》，(網管人)，2012年5月7日，<https://www.netadmin.com.tw/netadmin/zh-tw/feature/3F86F1AFBF2648EEA939C7E99400EC57>，(檢索日期：2023年11月27日)。

[6]陸軍司令部，"陸軍資訊資產管理作業規定"，桃園：陸軍司令部，2022

[7]李建鵬、陳保佑，〈淺談國軍網路安全防護作為之研究〉《海軍學術雙月刊》，55卷第1期，pp.129，2021年2月。

[8]李榮耕，〈個人資料外洩及個資外洩通知條款的立法芻議〉《東吳法律學報》，20卷第4期，pp.258，2009年04月。

[9]《經濟合作暨發展組織》，(維基百科)，2023年11月24日，<https://zh.wikipedia.org/zh-tw/经济合作与发展组织>，(檢索日期：2023年11月29日)。

[10] 賴怡秀《世界經濟合作暨發展組織(OECD)修正「隱私保護及個人資料之國傳輸指導指引」》，(科技法律研究所)，2013年11月22日，<https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&i=156&d=6382>，(檢索日期：2023年11月29日)。

[11] 《亞太經濟合作會議》，(維基百科)，2023年11月19日，<https://zh.wikipedia.org/wiki/%E4%BA%9A%E5%A4%AA%E7%BB%8F%E6%B5%8E%E5%90%88%E4%BD%9C%E7%BB%84%E7%BB%87>，(檢索日期：2023年11月29日)。

[12]《我國獲准設立 APEC 跨境隱私保

護規則(CBPR)體系當責機構》，(國家發展委員會)，2011年6月15日，<https://www.ndc.gov.tw/nc_27_35052>，(檢索日期：2023年11月29日)。
[13]黃明達，〈整合資安與個資管理系統的國際標準－ISO/IEC 27701 簡介與應用〉《國土及公共治理季刊》，7卷第4期，pp.92-101，2019年12月。
[14]《盤點公部門8起個資外洩案綠委齊轟：數發部不能消極坐視》，(自由時報)，2023年1月18日，<https://news.ltn.com.tw/news/politics/breakingnews/4188767>，(檢索日期：2023年10月31日)。
[15] 《ISO/IEC 27001》，(維基百科)，2023年10月23日，<https://zh.wikipedia.org/zh-tw/ISO/IEC_27001>，(檢索日期：2023年12月4日)。
[16]林宜隆、陳珮菁、陳高宏、李正元、劉世詳、謝宗翰、羅尹伶，〈整合 ISO 27001與 ISO 27799應用於護理資訊之探討〉《電腦稽核》，30期，pp.1-11，2014年07月。
[17]魏銷志、洪韻茹、陳昇智、祝亞琪，〈隱私資訊管理系統標準 ISO27701於 GDPR 適用性評估〉《電腦稽核》，42期，pp.40-51，2020年8月。
[18]《ISO 27701 – The Standard for Privacy Information Management》，(isms.online)，<https://www.isms.online/iso-27701/>，(檢索日期：2023年12月5日)。
[19] 《全球首批！BSI 頒發 ISO/IEC 27701 隱私資訊管理系統證書》，(bsi)，<https://www.bsigroup.com/zh-TW/about-bsi/media-centre/press-release/2019/201912/first-organizations-to-achieve-ISO-27701/>，(檢索日期：2023年12月5日)。
[20]黃國裕，〈最新個人資訊管理系統(PIMS)國際標準〉《政府機關資訊通報》，第352期，pp.33，2018年4月。
[21]孫天貴、左瑞麟，〈ISMS 與 PIMS 整合導入之研究－以國防部全球資訊網站系統為例〉《資訊安全通訊》，21卷4期，pp.42，2015年10月。
[22]《2020十大資安趨勢8：資安標準】資安產品驗證蔚為風潮，隱私保護有賴ISO 27701整合 ISMS》，(iThome)，2020年1月9日，<https://www.ithome.com.tw/news/135180>，(檢索日期：2023年12月5日)。
[23]《圖解個資法｜個人資料蒐集、處理、利用的原則》，(iThome)，2012年10月25日，<https://www.ithome.com.tw/article/88034>，(檢索日期：2023年12月5日)。
[24]吳錦松、彭紹綸、黃筱珊，〈物聯網之安全規範與隱私權探討〉《NCS 2019全國計算機會議》，第352期，pp.76-80，2019年11月。
[25]孫天貴、左瑞麟，〈ISMS 與 PIMS 整合導入之研究－以國防部全球資訊網站系統為例〉《資訊安全通訊》，21卷第4期，2015年10月，pp.32-43。
[26]林益正，〈以資安保證因應個資法衝擊〉《資訊安全通訊》，16卷第3期，pp.146-147，2010年7月。
[27]魏銷志、祝亞琪，〈資訊安全風險管理在實務面的挑戰〉《資訊安全通訊》，18卷 第4期 ，pp.152～153，2012年10月 。
[28]黃明達，〈整合資安與個資管理系統的國際標準－ISO/IEC 27701 簡介與應用〉《國土及公共治理季刊》，7卷第4期，pp.92-94，2019年12月。
[29]吳嘉龍，〈資訊安全風險管理與電腦緊急應變發展研究探討〉《危機管理學刊》，12卷 第2期 ，pp.51-52，2015年09月。
[30] 陳惟凡、陳振楠、伍台國，〈電子商務平臺之安全風險評估模式：植基於ISO 27001資訊安全管理系統與個人資料保護法〉《電腦稽核》，34期，pp.30-31，2016年08月。
[31]曾志忠，〈教育雲規劃與建置之研究—以國中校園資訊教育為例〉《宜蘭大學多媒體網路通訊數位學習碩士在職專班學位論文》，pp.38，2013年6月。
[32]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〉《中原大學資訊管理學系學位論文》，pp.26，2012年7月。
[33]林淑儀，〈臺灣推動個人資料保護與管理制度(TPIPAS)之研究〉《淡江大學資訊管理學系碩士論文》，pp.51，2014年6月。
[34]蔡朝安，〈個人資料保護實務：以遵法及風險管理為中心〉《資訊安全通訊》，19卷3期，pp.91-9，2013年7月3。
[35]陳仕弘，〈資訊安全威脅與治理政策之探討〉《管理資訊計算》，12卷特刊1，pp.10，2023年7月。
[36]梁華傑，〈網路戰資訊安全探討與省思〉《國防雜誌》，23卷2期，pp.114，2008年4月。
[37]邱泰源，〈軟體安全品質之滲透測試案例分享〉《品質月刊》，50卷9期，pp.12，2014年9月。
[38]樊國楨、羅德興、錢素英、蔡昀臻，〈ISMS 驗證合規初論：根基於管理系統驗證機構資通安全管理法驗證方案特定要求事項〉《電腦稽核》，47期，pp.79，2023年2月。
[39]林芙美，〈博物館資安管理與防護—國立臺灣博物館資安推動與實施經驗分享〉《臺灣博物館季刊》，47期，pp.81-89，2021年9月。
[40]方嘉鴻、林宜隆，〈網路犯罪問題與防範對策之警政五力分析〉《電腦稽核》，30期，pp.137-138，2014年7月。
[41]何寬祥，〈應用層級分析法之資訊安全風險評鑑〉《國立交通大學工學院工程技術與管理學程碩士論文》，pp.9，2014年6月。
[42]邱映曦、劉敏慧、何寶中，〈我國個人資料保護法與個人資料管理制度〉《資訊安全通訊》，19卷1期，pp.59-61，2013年1月。
[43]陳盈成，〈外商銀行業資訊安全管理之研究-以 A 銀行為例〉《淡江大學管理學院資訊管理學系碩士論文》，pp.39，2012年1月。
[44]林茹玉，〈個資安全防護實作建議〉《資訊安全通訊》17卷3期，pp.47-48，2011年7月。

Study on the Key Success Factors for Implementing ISO 27701 in the Army Core Information Systems

Yu-Ling Lin[1], Wei-Ming Liao[2]

[1]College of Management, National Defense University

[2]Army Command and Staff College, National Defense University

Abstract

With the rapid advancement of technology, cybersecurity and data protection have emerged as crucial topics for maintaining personal information security. Within the core information systems of the army, including the systems for army officers and specialized academic institutions, personal information about military personnel and students remains present. These systems also carry the responsibility of preventing the leakage of personal information from within. This study aims to identify the key success factors for the implementation of ISO 27701 in army core information systems by addressing existing challenges in integrating information security and personal information management requirements, security protection implementation cases, and the application of Personal Information Management Systems (PIMS). Following literature review and expert questionnaires, four main criteria for "Information Security and Personal Information Policy" and fifteen sub-criteria for "Organizational Compliance with Personal Information Regulations" were established, forming the decision-making framework of this research. Using the Analytic Hierarchy Process (AHP) to analyze questionnaire results, the weights of each criterion were determined to serve as a reference for prioritizing decisions in system implementation planning. Based on the analysis, the study concludes with three main findings, including "Implementing a Personal Information Management System to mitigate information leakage threats," and offers three concrete recommendations, such as "Enhancing personnel literacy assessment and training." These are intended to guide future decision-making for the adoption of ISO 27701 in army core information systems, thereby strengthening the organization's information security framework and personal data protection capabilities, improving the system's defensive efficacy and resilience, and addressing current and future information security threats.

Key words：Army Core Information Systems, Information Security, Personal Information Management, Analytic Hierarchy Process(AHP)