圖書資訊學研究18：2 (June 2024)：1-47
DOI:10.30177/JLISR.202406_18(2).0001

文檔系統資安意識評估架構及其實務運用之探討

Discussion on the Assessment Framework of Cybersecurity Awareness on Electronic Record Management System and Its Practical Application

林巧敏*

Chiao-Min Lin

國立政治大學圖書資訊與檔案學研究所教授
Professor
Graduate Institute of Library, Information and Archival Studies
National Chengchi University

劉穎芝

Yin-Chih Liu

桃園市政府警察局書記
Associate Clerk
Taoyuan Police Department

【摘要 Abstract】

在資訊安全問題日益重要的環境下，職司電子公文及檔案管理資訊系統（簡稱文檔系統）的相關人員對於系統的資安意識相形重要。本研究採用疊慧法統整學者專家意見，建立「資安意識評估問卷」，並透過Cronbach's α係數值及驗證性因素分析，確立達到良好的信效度。接續以該問卷調查桃園市一級機關之文檔人員及資訊人員，對於文檔系統資安之認知及其實務達成情形。研究結果顯示不同背景專家對於資安意識評估題項具有高共識，總

*通訊作者：林巧敏 cmlin@nccu.edu.tw
投稿日期：2023年5月21日；接受日期：2023年8月21日

計訂出10個構面之資安意識評估問卷，並經機關人員填答資安意識問卷統計後，發現機關人員資安意識偏正向且趨於一致，而資訊人員之認知高於文檔人員，檢驗「認知重要性」與「機關達成程度」之間也有正相關。

In an era where information security issues are increasingly critical, the awareness of information security holds significant importance for individuals responsible for Electronic Records Management Systems (ERMS). This study aimed to develop an Information Security Awareness Assessment Questionnaire by employing the Delphi method to integrate the perspectives of scholars and experts. The questionnaire's reliability and validity were evaluated using the Cronbach's α coefficient and confirmatory factor analysis, indicating satisfactory results. Subsequently, the questionnaire was utilized to examine the perception of information security among personnel involved in electronic record management and information-related roles within official agencies in Taoyuan City. The research findings demonstrated a high level of consensus among experts from diverse backgrounds regarding the assessment items for information security awareness. A comprehensive Information Security Awareness Assessment Questionnaire consisting of 10 dimensions was developed. The survey outcomes concerning information security awareness within Taoyuan government agencies revealed a generally positive and consistent level of awareness among personnel. However, it was observed that information personnel exhibited a higher level of awareness compared to record management personnel. Furthermore, a positive correlation was observed between the perceived importance of information security and the agency's level of achievement.

【關鍵詞 Keywords】

資安意識；電子檔案；文檔系統；資訊人員；文檔人員

Cybersecurity Awareness; Electronic Records; ERMS; Information Staff; Record Management Staff

壹、前言

臺灣政府機關因應科技趨勢推動數位轉型，機關文書及檔案作業資訊化則是推動電子化政府發展的重要里程碑。至2019年臺灣政府機關已完成「電子化政府計畫」，各機關已使用電子公文及檔案管理資訊系統（簡稱文檔系統）總數達3,108個，占政府機關99.36%，顯見臺灣文書檔案資訊化的比例相當高。隨著電子文書及檔案數量的不斷產生及累積，資訊時代的資安問題對於文檔系統的威脅也與日俱增。因此，不論是基於政府資訊安全維護的角度，抑或是對於文書檔案內容真實性的捍衛，資通安全已然是政府機關必須審慎應對的重要議題（國家發展委員會，2016；國家發展委員會檔案管理局，2020a）。

然而，資安威脅卻是無孔不入，除了仰賴資通科技做好防護措施之外，機關人員對於資安的認知及履行程度更加重要（Kruger & Kearney, 2008; Wall & Palvia, 2022）。每個人依其職務身分之不同，可接觸到不同程度的資訊，並承擔不同輕重的資安責任，亦即資通安全，人人有責。在文檔系統當中，不僅是資訊人員肩負起機關資通安全整體規劃的責任，但凡是負責文書及檔案的管理人員（簡稱文檔人員）亦是串聯系統資安維護的關鍵角色。可知機關除了依資通安全責任等級持續優化系統之外，各機關人員的資安意識培養尤為重要。

機關文檔人員包含機關文書單位及檔案單位之工作人員，文書人員的權責為收發文、登記桌、公文時效管制等業務；檔案人員則負責檔案點收、立案編目、檢調、清理、保管、安全維護等業務。此外，因機關文檔系統之資安問題，亦屬資訊人員權責，故本研究也將資訊人員併同納入調查，此處資訊人員是指職司機關文檔系統之管理者，或是機關資通安全負責人等。

雖然已有不少文獻探討促進員工資安認知之相關文獻，然而針對文檔系統相關人員之資安意識探討，卻相對缺乏。再者，針對文檔系統資安意識的評估指標，也缺乏權威性之評估問卷。因此，本研究先透過疊慧法建立資安意識評估問卷，接續進行個案機關之實務調查，以瞭解運用文檔系統之文檔及資訊人員的資安意識程度，並探究不同人員之間是否有差異，可藉此釐清對於機關人員進行資安教育的需求，進而提供機關檔案管理政策修正或是資安訓練課程規劃之參考。

因此，本研究目的在於：

一、探討文檔系統資安意識層面，提出可供機關評估文檔人員及資訊人員資安意識之調查問卷。

二、運用資安意識問卷調查機關文檔人員及資訊人員，對於文檔系統資安意識認知現況以及機關達成程度。
三、分析機關人員資安意識認知與機關達成程度之關連，並探討文檔人員及資訊人員資安意識之差異。

貳、文獻探討

一、資通安全及資安意識之推動

參考美國國家標準技術協會（National Institute of Standards and Technology, NIST）詞彙表、ISO/IEC 27035-3: 2020及ISO/IEC 27100: 2020對於「資訊安全」（information security）的定義是「防止資訊和資訊系統受到未經授權的存取、使用、揭露、破壞或竄改，可提供機密性、完整性和可用性維護」。廣義的資訊安全事件可能涉及資訊及通訊科技（information and communications technology, ICT）。因而有「資通安全」（information and communications technology security, ICT security）一詞，適用層面更廣，包括資料及資訊的擷取、儲存、檢索、處理、顯示、陳述、組織、管理、安全、傳輸和交換（International Organization for Standardization [ISO], 2018, 2020a, 2020b）。

我國行政院《資通安全管理法》對於「資通安全」的定義，是「指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。」（資通安全管理法，2018）顯見我國對於「資通安全」的範圍亦是包含資訊（information）及通訊（communication）兩個面向。

資安意識（cybersecurity awareness或ICT security awareness）係指認知到資安的重要性，以及瞭解資安問題發生時，可能會帶來的後果，因而可對資安議題產生時，做出相應的行為，目的在於建立使用者對於資通安全的注意力，也是後續進行資安訓練的先備條件（Wilson, de Zafra, Pitcher, Tressler, & Ippolito, 1998; Wilson & Hash, 2003）。Hansche（2001）指出資安意識的建立，主要目標在於提高對於資訊系統安全的認識，並瞭解資安漏洞可能帶來的負面影響。

Kruger與Kearney（2008）說明一個組織的資通安全良窳，除了仰賴資通科技加以防護，人員的資通安全活動更是同等重要，但反而是最容易被忽略的一環，例如在資安攻擊手段當中的網路釣魚（phishing），顯然與人員的資安意識極為相關，然而卻是經常發生的資安問題。

資安社群（system administration, networking and security, SANS）於2011年發表安全意識成熟度模型（security awareness maturity model），此模型列出資訊安全意識成熟度模型指標矩陣，將組織的資安意識成熟度由低至高，分為五個階段，（一）是毫無意識階段，（二）是遵守專注階段，（三）是推廣意識和行為改變階段，（四）是長期維持和文化變革階段，一直到最後（五）的成熟指標框架。每個階段提供對於人員行為表現的判斷指標，此模型可協助組織判別現階段組織內資安意識的成熟度，作為邁向下一階段設定目標的參考（SANS, n.d.-a）。透過此模型（表1），可評估現行組織人員的資安行為表現，瞭解目前組織的資安意識正處於何種成熟度階段，提供組織進行資安政策調整的建議。此

表1

人員於不同階段之資安意識成熟度行為表現指標

資安意識成熟度	人員行為表現指標
1. 毫無意識階段	員工從不討論安全或表現出安全行為。
2. 遵守專注階段	• 員工具有「讓我們解決這個問題」的態度。 • 員工認為安全是資訊科技單位必須負責，而不是個人的問題。 • 員工覺得安全是個人必須參與的。 • 員工對於安全議題和／或安全團隊，存有消極的看法。
3. 推廣意識及行為改變階段	• 員工瞭解安全僅靠技術無法完全保護，個人有責任保護自己和組織的資產。 • 員工會在資安事件或懷疑攻擊時，提出報告。 • 當安全團隊推出資安資訊時，員工會加以詢問。 • 員工表現出來的行為是有接受過培訓的反應。 • 員工在家中也能遵守安全行為。
4. 長期維持及文化變革階段	• 良好的安全實踐是瞭解自己的角色以及需要做什麼。 • 員工會教育他人具備良好的安全行為。 • 員工會提供如何提升組織安全性的想法或建議。 • 員工或部門會主動要求安全簡報或更新，並產生積極尋求更多資訊的行為。 • 單位主管和團隊定期要求安全審查。 • 單位會要求競爭或比較組織內，誰擁有最好的資安表現。 • 組織安全團隊及其維護安全的工作，被視為是一件積極的事。
5. 成熟指標階段	• 單位會主動要求並使用安全意識指標，以衡量組織內或比較跨組織單位的進展情形。

資料來源：SANS（n.d.-b）。

指標關注的面向，比較是偏重由人員的行為與態度，瞭解機關資安意識推動的成熟度，可知建立組織人員的資安意識需要先瞭解人員的認知程度，並建立組織內評比機制。惟有根據人員資安意識成熟度並擬定人員訓練計畫，藉由長期持續的推動，才能提升組織人員的資安意識，進而有效提升組織整體的資安成效（SANS, n.d.-b）。

二、資安意識探討的內涵

〈NIST Special Publication 800-16〉提出「ABC's of Information Technology Security」作為資訊安全的基本概念，是以英文字母A到Z排列以利於記憶，總計26項的資安概念內容包括：資產（assets）、備份（backups）、對策與控制（countermeasures and controls）、指定委派專家與其他人員（DAA and other officials）、道德標準（ethics）、防火牆與責任區分（firewalls and separation of duties）、目標（goals）、駭客（hackers/crackers）、個人責任（individual accountability/responsibility）、工作職責說明（job description/job function）、資安事件防範重點（keys to incident prevention）、法規（laws and regulations）、模式架構（model framework）、須知（need to know）、責任歸屬（ownership）、政策與程序（policies and procedures）、品質保證與控制（quality assurance/quality control）、風險管理（risk management）、安全訓練（security training）、威脅（threats）、單一識別碼（unique identifiers）、弱點（vulnerabilities）、浪費、詐欺及濫用（waste, fraud and abuse）、預期與非預期事件（expect the unexpected）、自己本身（you）以及分區隔離（zoning/compartmentalization）（Wilson et al., 1998）。

此外，〈NIST Special Publication 800-50〉也提到，資安意識所關心的問題，包含對於密碼的使用和管理、防範病毒、蠕蟲、木馬程式和其他惡意程式、對於不明電子郵件及使用網路的監控、資料備份和儲存要求、事故發生的聯繫及處理通報、環境變化對於系統風險的增加、資料和管理權限的移轉、實體和線上所衍生的安全議題、作業系統和軟體版權問題、存取控制議題、機密文件的特殊管理、個人資安維護責任等（Wilson & Hash, 2003）。

國家發展委員會檔案管理局（2019）根據文檔系統資安措施的角度，提出四個資安管理的建議，包括：文檔系統主機管理、文檔系統程式防護、文檔系統危機處理、文檔系統資訊安全宣導等必要措施。綜合國內文獻，對於我國文檔系統所面臨的資安問題探討經歸納統整後，可

分為下列面向說明（吳倩萍，2006；張文熙，2004；曹明玉，2006；歐芳伶，2008）：

（一）傳送安全：以文檔系統而言，指公文電子交換安全，各機關在上傳檔案資訊時，皆須採取加密動作。

（二）人員安全：人員管制是整體資訊安全最基本的環節，人員異動的管理作業亦是帳號管理的基本要務。當人員是在單位內異動時，人員帳號應即時異動。退休人員帳號應予停用，切忌讓後續承接業務人員沿用舊帳號，以免權責混淆。對於機關人員之資訊安全認知應加強基本操作，主管層級則加強管理層面之觀念，如異地備援、定期稽核、通報程序等，而主管的資安態度對於資通安全有立竿見影之效。

（三）設備安全：機房門禁系統應維護設備實體安全，建立異地備援機制是確保設備持續運作以及危機管理的有效方式。

（四）網路安全：面對各種網路攻擊手法不斷翻新的環境，資安技術必須不斷更新、填補漏洞。

（五）檔案產生及傳送過程的安全：技術可以防堵部分問題，但無法完全避免人為錯誤和洩密，因此，在資料傳送的每個作業環節，都應避免發生人為操作不慎的漏洞。

（六）應用安全：應用安全包含應用內容及應用程式和操作，應用內容部分可透過防毒軟體、過濾系統等方式把關；而應用程式部分可透過包含網頁存取控制（web access control）、資料庫存取控制（database access control）及檔案系統存取控制（file system access control）達到目的；操作安全部分可透過對系統暨網路非法入侵偵測、系統暨網路行為的掃描以及系統暨網路行為監控作業予以把關。

因此，對於資安意識的宣導，通常也是以上述的資安議題為核心。在國內探討資安意識的相關研究當中，對於資安意識評估工具的設計，主要是參考國際資安標準或過往學者所設計的架構，邀集國內專家學者參與發展符合本地情境需求之評估工具。例如吳倩萍（2006）在探討政府機關個人資訊安全認知與行為的研究中，是以計畫行為理論為基礎，結合資訊安全管理實務經驗主管層級人員及業界顧問人員之建議，歸納出「事件通報」、「電子郵件」、「密碼管理」、「資料保護」、「實體安全」、「清空作業」、「其他」等資安議題，並從中延伸實質的資安認知評估題項。

曹明玉（2006）的研究則是以〈NIST Special Publication 800-16〉當

中的「ABC's of Information Technology Security」項目為基礎，採用疊慧法設計資訊安全認知評量表，區分為「法律與規範」、「組織與資訊安全」、「系統互聯與資訊分享」、「敏感性」、「風險管理」、「管理控制」、「系統生命週期控制」、「作業控制」、「技術控制」等構面予以評量。

歐芳伶（2008）曾以Drevin、Kruger與Steyn（2007）所設計的資安意識評估架構為依據，並透過國內專家訪談，發展出個人資訊安全認知量表的題目，共分為六大類別，分別為「極大化資訊完整性」、「極大化資訊機密性」、「有效及有效率使用電子通訊資源」、「極大化資訊及硬體設備可用性」、「極大化接受對行動的責任感」、「極大化使用資源」等，側重以個人資訊安全認知的角度提出量表。

比較前述研究對於資安意識評估的題項，雖然不盡相同，但也反映出資安意識所涉層面的多樣性及複雜性。對於資安意識之評估，通常是根據已制訂之評估項目，基於大環境需求加以編修，以符合本地資安關注的議題。因此，在基礎構面上首先必須歸納出基本的共通需求，例如：針對資料的完整性、機密性及可用性，皆會提到帳戶密碼管理、系統防護措施、人員行為、備份要求、管理政策、事件通報等事項。雖然，國內已有學者曾提出資安認知量表或是評估問卷設計，但所投射和關心的皆為一般資訊系統，比較無法反映針對文檔系統的資安管理問題，由於文檔系統包含檔案本體內容以及檔案電子目錄，無論是原生電子檔案或是紙本檔案，皆同樣是時時刻刻會面臨檔案資訊的資安問題。加上政府機關對於文檔系統的資通安全問題日益重視，若能針對文檔系統特性提出資訊安全評估工具，勢必能促進文檔人員及資訊人員的資安意識，進而提升文檔系統的資安維護。

三、國內外文檔系統資訊安全之研究

文檔系統資訊安全的相關議題，可從政策面、組織面、人員面、文化面及系統面等多面向切入探討，探討議題相當多元，亦可依據不同理論提出假設。洪國興、季延平與趙榮耀（2003）曾以資訊安全管理「整合系統理論」為基礎，經由因素分析的程序，匯集專家意見，建構「資訊安全評估準則層級結構」，共分9個評估構面，37項評估準則，提供組織建立資訊安全策略之參考。

此外，對於建構資訊安全認知評估量表之研究，國內尚有曹明玉（2006）以疊慧法設計出評估企業人員資訊安全認知的評量表，進而以問卷調查法評估此量表之適用性。而歐芳伶（2008）則是以Drevin等人

（2007）所設計的資安意識評估架構為基礎，修整文字和題項，發展出適用本地情境之資訊安全認知量表內容。此外，林巧敏（2020）曾對於電子檔案風險評估問題，運用疊慧法評核電子檔案風險管理之共識項目，建立機關檔案進行電子檔案風險自我檢核的指標，並進行個案實證研究，以驗證風險檢核表之適用性，進而提出機關電子檔案風險管理策略。

國外探討資訊安全認知量表之研究，有Dhillon與Torkzadeh（2006）係以組織的角度根據組織內部人員對於資訊系統安全的理解，彙整內部人員認知資訊安全管理的重要問題，此研究採用訪談法對於103名管理人員進行資訊安全價值觀的意見蒐集，研究獲得可分為25類的86項管理目標，並邀請7名資訊安全專家進行分析結果驗證，最終認為資訊安全的維護是超越技術的考慮，最重要的管理工作是需要以組織為基礎，發展評估原則和人員價值觀，才是核心的管理議題。

至於進行機構人員資訊安全認知和態度調查的相關研究，國內有吳倩萍（2006）因關注政府機關人員對於資訊安全認知程度，採用計畫行為理論為基礎，利用問卷調查方式，分析政府機關人員對於資訊安全認知、態度及其行為之關係。蕭瑞祥、羅雅萍與鄭哲斌（2012）是以問卷調查方式瞭解非營利組織資訊科技能力、員工資訊安全認知現況，並探討非營利組織的員工的資訊能力，對於個人資訊安全認知之影響。林天生、蔡侑庭與侯禹賢（2015）則是探討雲端企業資源規劃系統（enterprise resource planning, ERP）的安全防護機制問題，並對於企業資源的實體安全及虛擬安全管理問題，提出加強維護的建議。

國外有關資訊安全認知調查之相關研究，有Drevin等人（2007）因有感於建立人員資安意識對於降低人為錯誤很重要，故而進行學術環境人員的資安意識價值評估，結果顯示在一般公認的資安目標，例如：機密性、完整性和可用性之外，機關人員認為資安問題的發生，往往有相當高的比例，是發生在社會和管理層面的問題上（例如：人員行動和有效的資源管理責任），因此，各機構可根據自身情境，運用評估資訊安全意識的工具，進行人員認知和行為態度的分析，提供本機構資訊安全的體檢和改善評估。Wall與Palvia（2022）認為現行少有解釋性或批判性的研究，是探討員工對於組織內資訊安全議題涉及的權力和控制觀點，故而採用定性研究訪談和訪談紀錄分析，探討機構員工在組織環境中，基於資訊安全管理要求，衍生出對於身分權限控制及其價值觀問題之探討。

統整前述國內外對於資訊安全認知、資訊系統安全及資安意識評估等相關文獻之探討，可知目前國內外探討資安意識的議題，研究對象主要集中在企業組織的員工，鮮少對於政府機關中的文書、檔案或資訊

人員等職務身分之資安認知進行探討。然而，政府機關所有施政及決策紀錄幾乎全數典藏於文檔系統，文檔系統的安全涉及政府資訊安全的問題，尤其，負責文檔系統的相關人員，更是扮演維護政府資安問題最舉足輕重的角色。因此，本研究希望進行政府機關中文檔人員及資訊人員的資安意識探討，不僅試圖建構符合本地實務情境的評估指標，並以個案機關為例，分析檔案機關人員資安意識現況以及不同職務人員之間認知的差異。

參、研究設計與實施

一、研究方法

本研究為發展適合評估臺灣機關文檔系統人員的資安意識問卷，首先統整國內外文獻彙整為資安意識認知題項，藉由疊慧法徵詢學者與專家意見，完成「資安意識評估題項」。繼而採個案調查研究，根據前階段提出之資安意識評估問卷，進行機關文檔系統資安意識調查，以瞭解個案研究機關文檔人員及資訊人員的資安意識認知以及機關的達成程度。採用研究方法包括：

（一）疊慧問卷調查

本研究進行資安意識評估問卷設計，因過往文獻探討之資安評估面向與分析重點不盡相同，且個別文件對於資安觀念陳述之文字龐雜，無法直接適用於機關文檔人員。本研究以我國資安法規為基礎，參考《資通安全管理法》（2018）及其子法、《機關檔案管理作業手冊》、《國家發展委員會檔案管理局公文處理作業要點》、《機密檔案管理辦法》（國家發展委員會檔案管理局，2020b），加上國外相關標準，包括Drevin等人（2007）的資安意識評估架構、NIST（2018）的網路安全框架（cybersecurity framework, CSF）、ISO（2018）所訂之27000系列標準（含ISO/IEC 27001: 2013、ISO/IEC 27003: 2017及ISO/IEC 27005: 2011）以及ISO（2019）所訂之ISO/IEC 27701: 2019關於隱私密碼管理部分。採用題項的考量，根據下列原則判斷：

1. 在不同標準重複出現，而題旨雷同的評估項目。
2. 文字不同但題意概念類似，擷取概念綜合陳述。
3. 適合臺灣檔案管理環境的資安問題考量。

本研究綜合汲取相關文獻重要的文意之後，將敘述改寫為較一致的形式，可供填答疊慧問卷的專家，針對這些題目是否適用於臺灣環境

做出可靠的判斷。彙整編修過程，儘量減少術語或專業詞彙的描述、避免語意混淆或模稜兩可的描述、避免雙重否定的描述以及注意題項內容的互斥性等編修原則。最終，將所有資安意識題目分為「帳戶管理」、「存取控制」、「系統防護」、「行動安全」、「上網行為」、「電子交換」、「實體安全」、「備份機制」、「遵守政策」及「事件通報」等10個構面，共計68題。

初步編修完成題目採用疊慧法，邀請檔案管理領域4名及資訊管理領域（含資安議題專家）4名參與疊慧問卷，以綜合檔案學者及資訊學者意見，發展符合我國情境之題項。疊慧問卷調查過程填答者彼此不相溝通，可以避免附和或盲從權威的心理，總計8名受訪者之背景如表2。

為獲得穩定的資安意識調查工具，採用李克特五點量表計分，請學者專家評估各題項內容對於資安評估是否具有重要性，5表示「非常同意」、4表示「同意」、3表示「沒意見」、2表示「不同意」、1表示「非常不同意」。

（二）個案調查分析

個案研究是進入研究現象場域，對問題進行主觀與全面的理解，採用個案研究是為瞭解導致個人或機關狀態、行為的因素。本研究之問卷前經檔案或資訊領域專家進行二回合疊慧法問卷修正後，完成實施機關文檔及資訊人員資安意識之「個案機關調查問卷」，問卷填答分為二大部分，一為「資安意識評估題項」，另一為「個人基本資料」（問卷內容詳如附錄）。

其中「資安意識評估題項」係瞭解人員認為資安議題的重要性以及機關達成程度的評估，分為「認知重要性」及「機關達成程度」兩個向

表2

疊慧法問卷調查對象背景及配置說明表

調查對象專業領域	配置人數	背景及配置說明
檔案管理專業領域		
學術研究	2	檔案學相關之專任教師。
實務領域	2	具有電子檔案管理實務工作經驗者。
資訊管理專業領域		
學術研究	2	資訊領域相關之專任教師。
實務領域	2	具有長期資訊管理經驗之實務工作者，且從事與文檔系統相關管理工作。

度，填答採用李克特五點量表計分，請填答者根據資安議題問卷內容，分別勾選符合情形之選項，數字越大代表符合情形越高。「個人基本資料」部分，在於瞭解填答者職務、服務年資、教育訓練等背景資訊，不含可辨識之個資及機關名稱，放置於問卷最後，以降低填答干擾。

本研究以採用文檔系統達10年之桃園市政府為個案調查對象，因機關人員已具備系統使用經驗，適合進行資安意識分析。桃園市政府所屬機關共26局、5處及1委員會，共計32個子機關，以各機關文檔人員及資訊人員為調查對象，預估母群樣本約500至600人左右。參考Raosoft（2004）對於樣本數量計算，本研究採大樣本抽樣（$n \geq 30$），且希望樣本數占母群體數的10%以上，容許誤差範圍在10%以內，如果樣本數達到100份，則容許誤差範圍預估在5.32 ~ 8.13%之間，故樣本數至少應達100份較為理想。

二、資料蒐集與分析

（一）疊慧法問卷部分

在第一回合疊慧法問卷回收後，觀察結果並進行資料描述統計分析，疊慧分析之描述統計說明如表3。

第二回合問卷內容是彙整第一回合問卷收到的資料中，根據各專家勾選的題項以及建議新增的題項，計算各題項的平均數、中位數、眾數、四分位數以及標準差，決定題項的適切性和共識性，將相關分析結

表3

疊慧法常用之描述性工具

描述性統計	統計項目	統計方式說明
集中量數	平均數（mean）	將所有專家填答的值相加除以專家人數所得之數值。
	中位數（mean）	所有專家填答值經高低排序後的中間值。
	眾數（median）	專家群中最多人選填的意見選項。
變異量數	標準差（standard deviation）	表現專家意見的離散程度。
	四分位差（quartile deviation）	將專家意見劃分為25%、50%及75%三切點，Q = (Q3-Q1)/2，表現出中間50%專家意見的離散程度。

果於下一回合回饋給學者專家，做為新回合的填答參考，第三回合問卷內容以此類推，為使問卷達到一致性及穩定性，本研究採用的題項審選標準如下（陳龍田、林巧敏，2021；McKemmish, Cumming, Acland, Reed, & Ward, 2017）：

1. 刪除題項之依據：第一回合填答後原則上不刪除題項，分析內容回饋在第二回合，第二回合填答後，則將平均數 < 3.0的題項刪除，前述平均數過低者，亦即該題項不具適切性，因而予以刪除；最後一回合填答後，則將屬於低共識，四分位差 ≥ 1.0的題項刪除。
2. 適切性程度之依據：採用以眾數為主，平均數為輔的判斷方式，藉此解決受極端意見影響以及同一題項存有多個眾數的情況。眾數為5或平均數 ≥ 4.5的題項代表適切程度很高。反之，眾數為3或4.0 > 平均數 ≥ 3.5的題項代表適切程度較低。
3. 共識性方面：採用四分位差判斷。高共識為四分位差 < 0.6。中共識則為 0.6 ≤ 四分位差 < 1.0，低共識題項於最後一回合刪除。
4. 結束問卷調查之時機：當該題項小於或等於前一回合問卷結果之標準差時，即達收斂度，而當收斂項目達到全體總項目的75%，代表專家群意見已達一致性，可結束問卷調查。

（二）個案機關問卷部分

進行個案機關調查前，先邀請10位受測者實施第一次前測，徵詢前測對象對於問卷內容是否利於填答，並以Cronbach's α係數值進行信度分析，以次數統計確認變異性，並評估正式問卷最低樣本數。正式問卷回收後進行整理，以SPSS進行資料處理及分析，統計方法如下：

1. 信效度分析（reliability and validity analysis）：於前測問卷及正式問卷回收後，將題項當中的「認知重要性」及「機關達成程度」，分別採用Cronbach's α係數值進行內部一致性的信度分析，以再次驗證題項是否妥適。在效度方面，則於正式問卷回收後，採用SEM-PLS進行驗證性因素分析。
2. 描述性統計（descriptive statistics）：填答資料分為「認知重要性」及「機關達成程度」兩個向度，以次數分配、平均數及標準差進行分析。
3. 獨立樣本*t*檢定（independent sample *t*-test）：以獨立樣本*t*檢定分析資訊人員和文檔人員在「認知重要性」及「機關達成程度」兩個向度的平均值是否達到顯著差異（$p < .05$）。
4. 相關分析（correlation analysis）：以皮爾森積差相關（Pearson correlation）分析「認知重要性」及「機關達成程度」之間的關聯程度。

肆、研究結果分析

一、資安意識評估之疊慧問卷分析

本研究綜整文獻探討之資安意識評估重點，將問卷題項分為「帳戶管理」、「存取控制」、「系統防護」、「行動安全」、「上網行為」、「電子交換」、「實體安全」、「備份機制」、「遵守政策」、「事件通報」等10個問題構面，徵詢8位兼具理論與實務背景的檔案管理或資訊管理學者專家。每一回合皆發放與回收8份研究問卷，進行次回問卷時，會附上前回問卷的整體填答狀況，提供填答者瞭解前一回合問卷的平均數、眾數、標準差、四分位差，作為填答參考。

分析專家填答問卷結果，在「帳戶管理」、「行動安全」、「上網行為」、「備份機制」等構面，眾數為5，平均數在4.70以上，顯示專家群判定本構面整體適切性程度高；四分位差為0.00，顯示專家群判定本構面整體達高共識性，故收斂度達100%，代表此類構面題項在專家意見上，很快達成一致性。

在「存取控制」構面分析，眾數為5，平均數為4.55，代表專家群判定本構面整體適切性高；四分位差為.50，標準差為.77，因題項當中有1題為中共識性，但整體構面題項已達高共識性，且所有題項第二回合均小於或等於前一回合問卷結果之標準差，已達100%收斂度，顯示專家意見達成一致性。

在「系統防護」構面分析，呈現眾數5，平均數高達4.69，代表本構面整體適切性高；四分位差為.00，標準差為.77，雖在個別題項中，有1題為中共識性，但整體仍達高共識性。8個題項當中，僅有1個題項未達收斂，係有關於系統版本控管機制，但兩回合後其適切性高且達高共識性，故題目仍予以保留，本構面收斂度達87.5%，達成一致性。

在「電子交換」構面分析，眾數為5，平均數為4.60，判定本構面整體適切性高；四分位差.50，標準差.68，雖然題項當中有1題為中共識性、1題為低共識性，但整體仍達高共識性。但在8個題項當中，有1個題項未達收斂，此題是關於機關憑證之注意事項，最後刪除低共識性的題項2，本構面整體收斂度達83.3%，專家意見達成一致性。

在「實體安全」構面分析，眾數為5，平均數為4.68，判定本構面整體適切性高；四分位差.00，標準差.64，在個別題項中有1題為中共識性，有2個題項未達收斂（題項編號3、13），題項3的內容係有關於收文人員之注意事項；題項13係關於資訊機房環境管控，但此2個題項在第二

回合後，也達適切性高且為高共識性，故仍予以保留，本構面整體收斂度達85.7%，專家意見達成一致性。

在「遵守政策」構面分析，眾數為5，平均數為4.71，本構面整體適切性高；四分位差.00，標準差.58，判定整體達高共識性，6個題項當中，有2個題項未達收斂（題項編號3、4），題項3內容係有關於人員對於機關資安政策認知，題項4係關於人員對於資安訓練認知，雖然未達收斂，但2個題項經兩回合後，也達到適切性高且高共識性，故予以保留，本構面整體收斂度雖為66.7%，但最終整體構面仍屬於適切性高且高共識性。

在「事件通報」構面分析，眾數為5，平均數為4.42，判定整體適切性高；四分位差.50，標準差.72，判定本構面整體達高共識性，但3個題項當中，有1個題項未達收斂（題項編號3），但仍為適切性高且達中共識性，故該題項予以保留，本構面整體收斂度達66.7%，雖然低於整體收斂度，但最後整體構面仍屬於適切性高且達高共識性（表4）。

問卷統計在第一、二回合均呈現適切性高且達高共識性結果，問卷在第二回合達成平均89.6%的收斂度，故於第二回合後結束調查。

在第一回合當中，有專家針對「帳戶管理」、「系統防護」、「行動安全」、「上網行為」及「實體安全」等5個構面之題項共13題提出文字修正或補充意見，修正幅度占整體題項的19.1%；在第二回合當中，有

表4

各構面題項之適切性、共識性與收斂度統計表

資安意識評估構面	眾數	平均數	四分位數	標準差	收斂題數	適切性	共識性	收斂度（%）
帳戶管理	5	4.71	.00	.58	6	很高	高	100.0
存取控制	5	4.55	.50	.77	10	很高	高	100.0
系統防護	5	4.69	.00	.77	8	很高	高	87.5
行動安全	5	4.94	.00	.25	2	很高	高	100.0
上網行為	5	4.82	.00	.47	7	很高	高	100.0
電子交換	5	4.60	.50	.68	4	很高	高	83.3
實體安全	5	4.68	.00	.64	12	很高	高	85.7
備份機制	5	4.83	.00	.45	5	很高	高	100.0
遵守政策	5	4.71	.00	.58	4	很高	高	66.7
事件通報	5	4.42	.50	.72	2	很高	高	66.7

專家針對「存取控制」、「行動安全」及「事件通報」等3個構面共3題提出文字修正意見，修正幅度占整體題項的4.41%，然而二回合的修正內容均以協助題項語意明確為主，未偏離原設計題項之意旨，故本問卷皆予以採納修正。各構面總題數、專家提出意見之修正題數及收斂題數統計，詳如表5。

綜合上述，本研究經由文獻整理綜整各項標準內容，並藉由二回合疊慧法問卷，有效凝聚不同學者專家共識，發展出適用機關文檔人員及資訊人員之資安意識評估問卷，再經問卷前測驗證評估題項之信效度後，確認本問卷可供後續個案研究問卷調查的適切工具，本問卷研訂過程各階段重要結果，歸納說明如表6。

二、文檔系統資安意識調查結果

問卷調查對象為桃園市政府一級機關負責文檔系統相關職務者，調查範圍包括26局、5處及1委員會，共計發出148份問卷，回收100份問卷，回收率為67.56%；填答設計Google表單檢查提示，可避免漏填，故

表5

各構面二回合及最終問卷題數說明

	第一回合		第二回合		最終版本	
回合構面	總題數	修正題數	總題數	修正題數	總題數	收斂題數
帳戶管理*	6	1	6	0	6	6
存取控制*	11	0	11	1	10	10
系統防護	8	6	8	0	9	8
行動安全*	2	1	2	1	2	2
上網行為*	7	1	7	0	7	7
電子交換	6	0	6	0	5	4
實體安全	14	4	14	0	14	12
備份機制*	5	0	5	0	5	5
遵守政策	6	0	6	0	6	4
事件通報	3	0	3	1	3	2
合計	68	13	68	3	67	60
百分比	修正幅度	19.10	修正幅度	4.41	收斂度	89.6

註：*表示收斂度達100%之構面。

表6

資安意識評估問卷各階段研訂結果說明表

研訂階段	實施重點	完成問卷題項
文獻及標準彙整分析	綜合相關文獻與標準中所提列的文意，將敘述改寫為較一致的形式，整併意旨接近及雷同的題項，並保留切合臺灣情境之文字。	完成歸納出「帳戶管理」、「存取控制」、「系統防護」、「行動安全」、「上網行為」、「電子交換」、「實體安全」、「備份機制」、「遵守政策」及「事件通報」等10個構面，共68個題項。
疊慧法專家意見調查	請8位學者專家評估各題項對於資安意識評估是否具有重要性。	第一回合未刪除題項，依據專家意見，在不影響原意旨下，予以酌修部分題項之文字描述，包含在「帳戶管理」構面題項5補充有關帳號安全管理機制之內容。在「系統防護」構面題項3、4、5、6、7及8註明「機關」字樣，以明確指涉範圍限縮於公務系統環境；題項4另補充有關連接外網時，防火牆防護措施之內容。在「行動安全」構面題項2修正有關安全控管之內容。在「上網行為」構面題項5修正有關安全控管之內容。在「實體安全」構面題項5、9、10及12補充有關指涉之實體範圍內容。 第二回合依據專家意見，將「存取控制」及「系統防護」構面之題項異動，並刪除「電子交換」構面共識性低的1題，刪除的題項內容為「郵件信箱不會開啟預覽功能。」其餘題項均呈現適切性高及高共識性，並達成89.6%的收斂度，故保留原有設計的10個構面，修正文字後留存67個題項。
問卷初稿前測	為測試問卷內容的可行性，從符合條件之研究對象中，以便利抽樣方式，邀請10位受測者實施前測，並以訪談方式，瞭解問卷內容適切性及一致性，經確定信效度後，完成正式問卷。	調整文字，提升文字流暢性及清晰度。維持原有10個構面，67個題項。並將題項當中的「認知重要性」及「機關達成程度」，分別以Cronbach's α 係數值進行驗證，Cronbach's α 係數值在 .983 ~ .985之間，均屬高信度係數，修正後項目相關性亦無負值，代表內部一致性高，不須刪除任何題項。

100份皆為有效問卷。將題項中的「認知重要性」及「機關達成程度」兩個向度，分別採用Cronbach's α係數值進行內部一致性的信度分析，在「認知重要性」向度，問卷總係數值為 .982，各構面係數值在 .739至 .955之間，屬可信至很可信範圍。在「機關達成程度」之信度分析，問卷總係數值為 .975，各構面係數值在 .709至 .914之間，均屬可信至很可信範圍。

100份有效問卷填答者背景，在職務方面，以文書人員最多，計36人，其次為檔案人員，計34人，資訊人員（不含委外）計19人，文檔單位主管4人，委外人員7人。在電腦及文檔系統的使用頻率上，所有人每天會使用到電腦，至於使用文檔系統的頻率，則是有81人是每天使用，其餘為經常使用或是偶爾使用者。

（一）資安意識各構面評估統計

本資安意識評估問卷共計10個構面67題，分析機關人員填覆問卷結果分項說明如下（表7）：

1. 帳戶管理

本構面內容含個人帳戶資料密碼管理、自然人憑證、人員異動帳戶權限處理。「帳戶管理」構面的「認知重要性」，平均數為4.77，標準差為0.47；認知重要性當中的題項6「對於完成離職或異動之員工帳

表7

文檔系統資安意識調查結果統計分析表

構　面	認知重要性		機關達成程度	
	平均數	標準差	平均數	標準差
帳戶管理構面	4.77	.47	4.49	.69
存取控制構面	4.68	.59	4.53	.69
系統防護構面	4.75	.48	4.59	.66
行動安全構面	4.78	.45	4.50	.67
上網行為構面	4.77	.45	4.53	.65
電子交換構面	4.77	.50	4.61	.62
實體安全構面	4.76	.45	4.64	.60
備份機制構面	4.70	.52	4.37	.82
遵守政策構面	4.70	.49	4.61	.64
事件通報構面	4.82	.40	4.70	.49
整體構面	4.74	.49	4.57	.66

號，應停用或異動其帳戶權限」，該題的平均數最高，標準差最小（*M* = 4.84, *SD* = .37）；題項2「定期（約3 ~ 6個月）更換個人帳戶密碼並採用高強度密碼（8碼以上，且由英文數字及符號混合組成），發覺有洩漏之虞時，則立即更換」的平均數最低，標準差最大（*M* = 4.67, *SD* = .57）。代表機關人員對於職務異動進行帳戶管理的認同度高，但對於密碼採高強度組成，並定期更換的認同度比較低。

至於「機關達成程度」的平均數為4.49，標準差為.69，其中題項6「對於完成離職或異動之員工帳號，應停用或異動其帳戶權限」的平均數最高且標準差最小；反之，題項4「不會採用生日、身分證字號或電話號碼等個人資料來設定重要密碼」以及題項1「自行管理電腦及各項系統之個人帳戶資料及密碼，不提供他人使用或與他人共用」的平均數比較低。顯示機關人員對於密碼設定和管理的觀念亟待加強，甚至可採取強制規範。

2. 存取控制

本構面內容含電腦及系統的使用者權限控制、線上簽核控制及文件開放格式等。「存取控制」構面的「認知重要性」整體平均數為4.68，標準差為.59。其中以題項4「委外人員或廠商，不可未經授權遠端存取個人電腦或登入文檔系統」的平均數最高，且標準差最小（*M* = 4.86, *SD* = .38）；但題項8「機關應採用開放性標準格式存取檔案，例如ODF、PDF等」平均數最低，且標準差最大（*M* = 4.31, *SD* = .88）。

至於「機關達成程度」的平均數為4.53，標準差為.69，達成程度最高與最低的題項與「認知重要性」一樣，皆為委外人員或廠商不可未經授權遠端存取的平均數最高；也同樣是題項8的採用開放性標準格式存取檔案的平均數最低。

本構面中，雖然整體「認知重要性平均數」大於「機關達成程度平均數」，但其中題項7「保存年限超過10年之公文或機密公文，不採線上簽核方式處理」。是當中唯一呈現「機關達成程度平均數」大於「認知重要性平均數」，可知機關人員對於機密公文不採線上簽核的資安要求，在實務作業中完成實踐的程度很高。

3. 系統防護

本構面內容含防毒軟體、系統版本控制、系統標準驗證及開發階段注意事項等。在「系統防護」構面的「認知重要性」，平均數為4.75，標準差為.48；認知重要性中，以題1「在電腦、行動設備及伺服器應安裝防毒軟體，定期掃描並更新病毒碼及修補系統漏洞」的平均數最高（*M* = 4.84）；但題項5「機關的應用系統於開發或維護階段，不提供正

式資料測試」以及題項9「文檔系統應符合相關國內外技術標準／協定較有保障」的平均數最低（*M* = 4.64）。

至於「機關達成程度」的平均數為4.59，標準差為.66，其中題項7「廠商參與機關資訊系統開發、建置、資料轉置及資訊系統維護人員均應簽訂保密切結書」平均數最高且標準差最小（*M* = 4.79, *SD* = .47）；但對於題項2「使用外接式硬碟或隨身碟時，應先執行病毒掃描」的平均數最低（*M* = 4.21），顯示機關對於委外廠商的資安防護意識很高，但對於人員在系統防護出現的缺口，往往是在儲存媒體的管理上，比較容易出現漏洞。

4. 行動安全

本構面內容為使用行動裝置的安全管理，對於「行動安全」構面的「認知重要性」，平均數為4.78，標準差為.45。本構面題項2「從手機、平板等行動裝置連入機關內部網路，要執行身分辨識作業，或使用防火牆代理伺服器進行安全控管」的平均數較高（*M* = 4.81）；題項1「手機、平板等行動裝置應避免裝置來路不明或不需要的行動應用程式（App）」的平均數較低（*M* = 4.74）。此外，分析「機關達成程度」方面，平均數為4.50，標準差為.67。其中題項2的平均數也是高於題項1的平均數。代表機關人員對於使用行動裝置進入機關內部網路，必須進行安全控管要求的意識與達成度都很高，但是容易輕忽以行動裝置下載應用程式該有的警戒。

5. 上網行為

本構面內容為公務機關連線及網頁網站瀏覽安全注意事項。對於「上網行為」構面的「認知重要性」，平均數為4.77，標準差為.45。其中題項4「具機密或有敏感性之資料，不會存放於對外開放之系統中」的平均數最高且標準差最小（*M* = 4.87, *SD* = .34）；但是題項1「瀏覽網頁時發現可用資料，會先判斷來源，不會直接下載使用」的平均數為最低且標準差最大（*M* = 4.64, *SD* = .58）。

在「機關達成程度」方面，平均數為4.53，標準差為.65，其中題項5「當要從遠端登入內部網路系統之資通服務，要執行身分辨識作業（如使用動態密碼辨識系統）及使用防火牆等方式進行安全控管」的達成程度平均數最高（*M* = 4.78）；而題項1的瀏覽網頁問題也是機關達成程度最低的題項，可知機關人員對於資料儲存的安全性以及登入系統的身分驗證，有比較高的認知與警戒，但對於下載網頁資料的安全性卻容易輕忽，顯然未來需要加強人員對於網路資訊正確性的判斷與宣導。

6. 電子交換

本構面內容為電子郵件及公文電子交換安全管理事項；在「電子交換」構面的「認知重要性」，平均數為4.77，標準差為.50，其中題項5「電子交換須使用有效期之機關憑證，機關憑證應妥善保存，並於效期過期前更新，以免交換異常」以及題項1「收到來源不明之電子郵件或特殊標題之郵件，會先判斷郵件的安全性，不會輕易點開」的平均數皆為最高（M = 4.82）；但題項3「使用者停職或離職後，應刪除其公務郵件帳號」以及題項4「機關收文人員收到電子來文於辨識解簽章後，應即儲存，如發現資料遭竄改，應立即通知原發文機關處理，並通報機關資訊」的平均數最低（M = 4.72）。

在「機關達成程度」方面，平均數為4.61，標準差為.62，達成度較高的題項與認知重要性的題項一致，皆為題項5，但達成度偏低的是題項2「具機密或敏感性之資料，不以電子郵件傳送，如有電子郵件傳送之必要時，應經單位主管核准並加密處理」的平均數最低（M = 4.38）。可知機關人員對於使用憑證以及判斷電子郵件的安全意識和達成度都比較高，但對於職務交接程序的郵件帳號管理或是機敏內容的郵件管理觀念比較缺乏，是需要加強人員教育的部分。

7. 實體安全

本構面內容為收文至歸檔流程當中實體環境的安全管理、庫房安全管理；在「實體安全」構面的「認知重要性」，平均數為4.76，標準差為.45；其中題項10「機關之機敏資料未經允許不得攜出機關」的平均數最高且標準差最小（M = 4.85, SD = .59）；題項6「使用電腦時，若離開座位，會確保鎖定使用環境，確保他人無法使用我的文檔系統或開啟我的檔案」的平均數最低且標準差大（M = 4.60, SD = .58）。

在「機關達成程度」方面，平均數為4.64，標準差為.60，其中的題項12「各類形式之檔案均應依保存年限妥善保管，機密檔案則應由機關首長指定專人或由檔案管理單位主管管理，並應與一般檔案分別存放」的平均數最高且標準差小（M = 4.81, SD = .40）；反之，題項6「使用電腦時，若離開座位，會確保鎖定使用環境，確保他人無法使用我的文檔系統或開啟我的檔案」平均數最低且標準差大（M = 4.19, SD = .40）。代表機關人員對於機敏資料保密管理的意識和達成度皆很高，但是容易忽略離開電腦時設定畫面鎖定的功能。

8. 備份機制

本構面內容為個人及機關的備份機制、災害復原演練；在「備份機

制」構面的「認知重要性」，平均數為4.70，標準差為.52，其中題項1「機關應訂定完整備援機制」的平均數最高（*M* = 4.80, *SD* = .44）；但題項5「公文檔案管理系統要定期執行災害復原演練」平均數最低且標準差大（*M* = 4.60, *SD* = .59）。

在「機關達成程度」方面，平均數為4.37，標準差為.82；達成程度最高的是題項2「資料建置後，應定期執行資料及系統軟體備份」；而題項3「備份資料至少製作2份為宜，除存放在主要的作業場所外，應另存放在離機關有一段距離的場所」的平均數為最低。顯示機關人員對於系統有比較高的備援機制認知，也能定期執行資料及系統軟體備份，但對於災害復原演練以及異地備份的要求，在實務執行上比較不足。

9. 遵守政策

本構面內容為資通安全相關政策內容及配合行為；在「遵守政策」構面的「認知重要性」，平均數為4.70，標準差為.49，其中題項1「機關應訂有資通安全計畫」的平均數最高且標準差最小（*M* = 4.76, *SD* = .45）；而題項5「各機關每年辦理1次通報演練及2次電子郵件社交工程演練」的平均數最低，且標準差大（*M* = 4.64, *SD* = .56）。

在「機關達成程度」方面，平均數為4.61，標準差為.64，其中題項5「各機關每年辦理1次通報演練及2次電子郵件社交工程演練」的平均數最高（*M* = 4.78, *SD* = .53）；但題項3「人員應清楚知道所屬機關的資安等級及資安政策」的平均數最低且標準差大（*M* = 4.36, *SD* = .77）。本構面中題項5「各機關每年辦理1次通報演練及2次電子郵件社交工程演練」是唯一在「機關達成程度」平均數大於「認知重要性」的題項。顯示機關多數已有訂定資通安全計畫的觀念，但對於進行演練的認知較為不足，而且人員對於所屬機關的資安等級及資安政策瞭解程度有待加強。

10. 事件通報

本構面內容為資通安全事件發生時的通報程序，在「事件通報」構面的「認知重要性」，平均數為4.82，標準差為.40，認知重要性最高的是題項1「當電腦的資料外洩或遭入侵時，應立即主動通報」以及題項2「當發現電腦有中毒跡象時，應立即主動通報」，平均數皆為4.85；反之，題項3「機關在知悉資通安全事件後，應於1小時內依主管機關指定之方式及對象，進行資通安全事件之通報」的平均數最低（*M* = 4.75）。

在「機關達成程度」方面，平均數為4.70，標準差為.49；機關達成度平均數最高的是題項3「機關在知悉資通安全事件後，應於1小時內依主管機關指定之方式及對象，進行資通安全事件之通報」；但題項1「當電腦的資料外洩或遭入侵時，應立即主動通報」的平均數最低。顯示機

關人員對於發生資料外洩以及電腦中毒等資安事故，需要進行通報已有清楚的認知，但是對於通報時限以及通報對象比較不瞭解，需要加強此部分之資安教育宣導。

綜合前述各項統計構面之平均數介於4.68 ~ 4.82之間，標準差介於.40 ~ .59之間，其中以「事件通報」構面的平均數最高（M = 4.82, SD = .40），「存取控制」構面的平均數最低（M = 4.68, SD = .59）（圖1）。

（二）認知重要性與達成度之相關分析

以皮爾森積差相關分析「認知重要性」及「機關達成程度」兩個向度之相關程度，兩個向度整體構面及各構面均呈現顯著正相關，其中「帳戶管理」呈現低度正相關（$r < 0.4, p < .001$），其餘向度整體構面及各構面之間呈現中度正相關（$r \geq 0.4, p < .001$）（表8）。亦即認知重要者則機關達成度也比較高，兩者為正相關。

（三）文檔人員及資訊人員資安意識之差異

根據問卷填答者職務身分，分為「資訊人員」及「文檔人員」兩個組別，「資訊人員」是指填答勾選職務身分為資訊人員者，「文檔人員」則包含文書人員及檔案人員。其中資訊人員有少數為委外廠商駐點人員，因其非屬機關聘任者，故將資訊人員中屬於委外的7人加以排除，採獨立樣本t檢定進行機關內資訊人員與文檔人員對於機關文檔系統資安意識之差異分析。

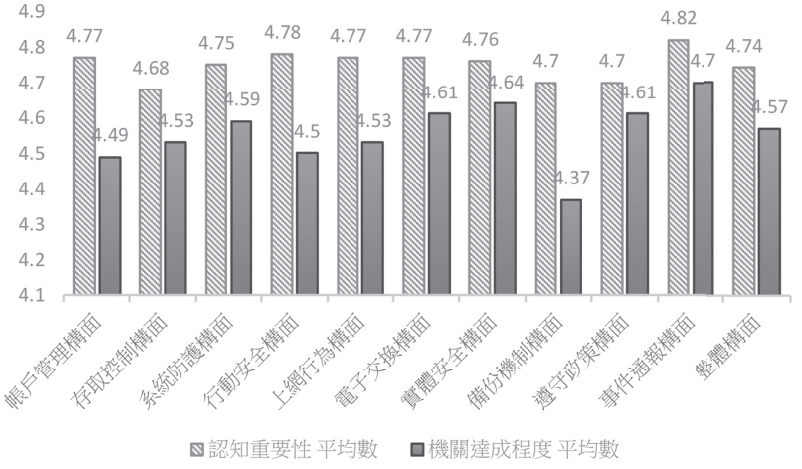

圖1　認知重要性與機關達成程度平均數之比較圖

表8

認知重要性及機關達成程度構面Pearson積差相關分析表

構　面	「認知重要性」／「機關達成程度」相關係數
帳戶管理	.388**
存取控制	.529**
系統防護	.553**
行動安全	.436**
上網行為	.428**
電子交換	.400**
實體安全	.648**
備份機制	.517**
遵守政策	.632**
事件通報	.475**
整體構面	.565**

註：** $p < .001$。

分析統計如表9，在「認知重要性」方面，僅「事件通報」（$t = 4.04, p = .000 < .001$）構面達顯著水準，其餘構面及整體構面均未達統計上顯著水準，代表資訊人員和文檔人員在資安「認知重要性」向度，大多數意見表達一致，唯獨在「事件通報」構面，資訊人員比文檔人員重視「事件通報」，且達到統計的顯著差異。在「機關達成程度」方面，僅「遵守政策」構面達顯著差異（$t = 2.28, p = .026 < .05$），其餘構面及整體構面均未達顯著水準，代表資訊人員和文檔人員對於機關資安作業上的符合程度，大多數意見有一致性，唯獨在「遵守政策」構面，資訊人員認為本機關達成資安要求的認同程度，比文檔人員高，且達到統計的顯著差異。

伍、結論與建議

綜合前述疊慧問卷與機關問卷調查結果分析，歸納以下結論。

一、不同背景的學者專家對於資安意識有高度共識，可建構出評估資安意識的10個構面67個題項

本研究的疊慧問卷調查在第二回合即達成89.6%的收斂度，且在第

表9

不同組別資安意識認知重要性與機關達成度*t*檢定

構面	組別	個數	認知重要性				機關達成程度			
			平均數	標準差	*t*值	顯著性	平均數	標準差	*t*值	顯著性
帳戶管理	資訊人員	19	4.82	.29	0.73	.466	4.50	.48	-0.07	.944
	文檔人員	74	4.76	.33			4.50	.41		
存取控制	資訊人員	19	4.65	.41	-0.77	.445	4.52	.51	-0.49	.624
	文檔人員	74	4.72	.36			4.57	.37		
系統防護	資訊人員	19	4.85	.26	1.39	.173	4.68	.41	0.78	.438
	文檔人員	74	4.75	.38			4.59	.46		
行動安全	資訊人員	19	4.82	.51	0.24	.810	4.47	.66	-0.43	.667
	文檔人員	74	4.79	.38			4.54	.60		
上網行為	資訊人員	19	4.89	.21	1.70	.095	4.51	.52	-0.34	.732
	文檔人員	74	4.78	.39			4.55	.44		
電子交換	資訊人員	19	4.86	.26	1.06	.292	4.60	.56	-0.09	.933
	文檔人員	74	4.77	.35			4.61	.37		
實體安全	資訊人員	19	4.80	.26	0.46	.644	4.65	.35	-0.24	.810
	文檔人員	74	4.76	.36			4.67	.33		
備份機制	資訊人員	19	4.78	.36	0.91	.367	4.29	.98	-0.58	.563
	文檔人員	74	4.68	.45			4.39	.63		
遵守政策	資訊人員	19	4.81	.33	1.28	.209	4.79	.30	2.28	.026**
	文檔人員	74	4.69	.44			4.57	.55		
事件通報	資訊人員	19	4.98	.76	4.04	.000*	4.84	.41	1.62	.117
	文檔人員	74	4.79	.38			4.67	.45		
整體構面	資訊人員	19	4.81	.24	0.94	.354	4.60	.42	1.00	.923
	文檔人員	74	4.75	.34			4.58	.34		

註：$^{*}p < .001$，$^{**}p < .05$。

一、二回合均呈現適切性高並達高共識性，可知對於文檔系統的資安議題，在檔案及資訊背景的學者專家之間存在高度共識。最終提出10個構面67個題項，包含「帳戶管理」6題、「存取控制」10題、「系統防護」9題、「行動安全」2題、「上網行為」7題、「電子交換」5題、「實體安全」14題、「備份機制」5題、「遵守政策」6題及「事件通報」構面3題，並透過Cronbach's α係數值及驗證性因素分析確立達到良好的信效度，可作為後續機關進行人員資安意識評估之運用。

二、機關文檔及資訊人員整體資安意識偏正向，且多數意見趨於一致，其中多數人最重視且對於機關達成程度最具信心的為「事件通報」構面，而最不重視的是「存取控制」構面，但對於機關的達成程度最不具信心的則為「備份機制」構面

在「認知重要性」向度，整體構面平均數為4.74，標準差為.49，代表整體意見認為各資安構面介於重要到非常重要之間。若將10個構面進行比較，是以「事件通報」構面的平均數最高，「存取控制」構面的平均數最低。而「存取控制」構面的題項8「機關應採用開放性標準格式存取檔案，例如ODF、PDF等」的平均數最低且標準差最大，代表文檔及資訊人員雖然整體呈現正向意見，而相較於其他構面及題項，對於採用開放性標準格式存取檔案的作法認同度偏低且存有認知歧異。

在「機關達成程度」向度，整體構面平均數為4.57，標準差為.66，代表整體意見認為各資安構面的機關達成度介於大部分符合到完全符合之間。若將10個構面進行比較，同樣呈現「事件通報」的機關達成度最高，「備份機制」構面的達成平均數最低。而「備份機制」構面的題項5「公文檔案管理系統要定期執行災害復原演練」的平均數最低且標準差最大，代表文檔及資訊人員雖然整體呈現正向意見，而相較於其他構面及題項，對於公文檔案管理系統要定期執行災害復原演練的機關達成度偏低且可能存在歧異。

整體而言，對於資安意識大部分為正向評價，且多數具一致性。在「認知重要性」及「機關達成程度」兩個向度，均有超過60%的人認為非常重要或非常符合，僅1%以下的人員認為非常不重要或完全不符合。兩個向度的各構面平均數皆在4.30以上，標準差皆小於.82，代表機關當中不論何種背景身分，大多數對於各項資安作業都具有正向認知，且認為服務機關的資安作業能符合標準。

三、機關文檔及資訊人員的資安意識程度，「認知重要性」向度略高於「機關達成程度」向度，兩向度及構面之間達顯著正相關

在「認知重要性」向度，各個構面呈現中度至高度正相關，在「機關達成程度」向度，各個構面呈現低度至中度正相關，而「認知重要性」及「機關達成程度」兩個向度之間呈現低度至中度正相關，代表各構面之間互有關連性，整體而言，「認知重要性」向度的分數均高於「機關達成程度」，顯示「機關達成程度」仍然需要繼續努力提升。

四、資訊人員的資安意識程度相對較高，而文檔人員的資安意識程度相對較低

將填答背景區分為資訊人員和文檔人員兩個組別時，呈現資訊人員在「認知重要性」的「事件通報」構面，資訊人員比文檔人員更加重視，在「機關達成程度」的「遵守政策」構面，資訊人員比文檔人員對於機關的達成程度更具信心。在「認知重要性」的「事件通報」構面，資訊人員顯著高於文書人員，可見資訊人員確實在不同職務身分當中，較關注「事件通報」的重要性。在「機關達成程度」向度，不同職務身分的整體及個別構面都無顯著差異。

資訊人員因其業務屬性，而持有較高的資安意識程度，並對於機關資安作業的達成程度較具信心，是可預期的結果，並不讓人意外，而文書人員、委外人員相對是較低的資安意識程度，經常是對於部分資安政策或是作業細節，比較不瞭解，亦即需要統整教育訓練內容，以凝聚不同職務人員之間的共識。

基於前述研究結果，提出對於文檔資訊系統相關人員改善資安意識之建議：

（一）優先加強文檔人員在「事件通報」的資安教育訓練，其次是「存取控制」、「備份機制」的資安教育訓練

本研究發現不同職務人員對於「事件通報」的重要性認知程度差異大，而其中資訊人員不但在整體資安意識最高，且對於「事件通報」的認知重要性顯著高於文檔人員。故建議對於文檔人員，可優先加強有關「事件通報」的資安教育訓練。有鑑於問卷分析結果，在「認知重要性」的「存取控制」平均數最低，在「機關達成程度」的「備份機制」整體平均數最低，可優先加強人員在認知偏低題項的教育訓練。

（二）定期對於機關內不同人員評估資安意識各構面認知，以瞭解認知差異，制訂貼近需求之資安演練及訓練計畫

本研究結果雖然機關人員的資安意識整體偏正向，且多數意見趨於一致，但在機關內不同背景的人員，在個別構面仍存有部分歧異，實因不同職務人員所涉業務不同，必然產生認知上的些微差異，而持續弭平歧異並取得最大共識，是資安議題永遠追求的目標。若一昧針對「已知」的資安內容進行重複無變化的教育訓練，而未找出「未知」的部分，容易淪於形式並欠缺彈性。建議可參考本研究提出的10個資安意識構面及相關題項，定期對於機關不同背景人員評估資安意識認知及需求，可作為建立機關資訊教育訓練內容的基礎。

參考文獻

吳倩萍（2006）。政府機關個人資訊安全認知與行為之探討（未出版之碩士論文）。國立臺北大學公共行政暨政策學系，新北市。【Wu, C.-P. (2006). *The study of governmental employees' personal cognition and behavior toward IT security* (Unpublished master's thesis). National Taipei University, New Taipei. (in Chinese)】

林天生、蔡侑庭、侯禹賢（2015）。雲端ERP安全機制之研究。蘭陽學報，*14*，78-87。doi:10.6665/JLYIT.2015.14.78【Lin, T.-S., Tsai, Y.-T., & Hou, Y.-S. (2010). A study of cloud ERP security mechanism. *Journal of Lan Yang Institute of Technology*, *14*, 78-87. doi:10.6665/JLYIT.2015.14.78 (in Chinese)】

林巧敏（2020）。電子檔案風險評估指標之建構及其應用實例分析。圖書資訊學刊，*18*(1)，69-96。doi:10.6182/jlis.202006_18(1).069【Lin, C.-M. (2020). Establishing the risk assessment indicators of electronic records and empirical analysis of an institution. *Journal of Library and Information Studies*, *18*(1), 69-96. doi:10.6182/jlis.202006_18(1).069 (in Chinese)】

洪國興、季延平、趙榮耀（2003）。資訊安全評估準則層級結構之研究。圖書館學與資訊科學，*29*(2)，22-44。【Hong, K.-S., Chi, Y.-P., & Chao, L. R. (2003). A study of hierarchical structure of information security valuation criteria. *Journal of Library and Information Science*, *29*(2), 22-44. (in Chinese)】

張文熙（2004）。檔案資訊安全之探討。在國家發展委員會檔案管理局（編），檔案資訊資源管理（頁449-458）。臺北市：編者。檢自https://pearl.archives.gov.tw/Publish.aspx?cnid=104425&p=4587【Chang, W.-H. (2004). The study of archives information security. In National Archives Administration, National Development Council (Ed.), *Dang an zi xun zi yuan guan li* (pp. 449-458). Taipei: Editor. Retrieved from https://pearl.archives.gov.tw/Publish.aspx?cnid=104425&p=4587 (in Chinese)】

曹明玉（2006）。資訊安全認知評量表之研究（未出版之碩士論文）。淡江大學資訊管理學系，新北市。【Tsao, M.-Y. (2006). *A study of the development of information security awareness scale* (Unpublished master's thesis). Tamkang University, New Taipei. (in Chinese)】

國家發展委員會（2016）。第五階段電子化政府計畫—數位政府。檢自https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvNTU2Ni84MjA3L2M0ODQ2NWZkLTIwNTMtNDExMy1iMDhjLTMwNDIzZDkyZTE3NC5wZGY%3d&n=44CM56ys5LqU6ZqO5q616Zu75a2Q5YyW5pS%2f5bqc6KiI55WrKDEwNuW5tC0xMDnlubQpLeaVuOS9jeaUv%2bW6nOOAjS5wZGY%3d&icon=..pdf【National Development Council. (2016). *Di wu jie duan dian zi hua zheng fu ji hua—shu wei zheng fu*. Retrieved from https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvNTU2Ni84MjA3L2M0ODQ2NWZkLTIwNTMtNDExMy1iMDhjLTMwNDIzZDkyZTE3NC5wZGY%3d&n=44CM56ys5LqU6ZqO5q616Zu75a2Q5YyW5pS%2f5bqc6KiI55WrKDEwNuW5tC0xMDnlubQpLeaVuOS9jeaUv%2bW6nOOAjS5wZGY%3d&icon=..pdf (in Chinese)】

國家發展委員會檔案管理局（2019）。文檔系統資訊安全宣導。檢自https://www.archives.gov.tw/Download_File.ashx?id=17228【National Archives Administration, National Development Council. (2019). *Wen dang xi tong zi xun an quan xuan dao*. Retrieved from https://www.archives.gov.tw/Download_File.ashx?id=17228 (in Chinese)】

國家發展委員會檔案管理局（2020a）。108年度機關檔案管理調查結果（中央與地方各級機關）。檢自https://www.archives.gov.tw/Publish.aspx?cnid=1708&p=4082【National Archives Administration, National Development Council. (2020a). *108 nian du ji guan dang an guan li diao cha jie guo* (*zhong yang yu di fang ge ji ji guan*). Retrieved from https://

www.archives.gov.tw/Publish.aspx?cnid=1708&p=4082 (in Chinese)】

國家發展委員會檔案管理局（2020b）。檔案法令彙編。新北市：作者。【National Archives Administration, National Development Council. (2020b). *Dang an fa ling hui bian*. New Taipei: Author. (in Chinese)】

陳龍田、林巧敏（2021）。政府機關電子檔案風險評鑑指標之研究。檔案半年刊，*20*(1)，16-37。【Chen, L.-T., & Lin, C.-M. (2006). A study on risks and evaluation criteria of electronic records in government agencies in Taiwan. *Archives Semiannual*, *20*(1), 16-37. (in Chinese)】

資通安全管理法（2018年6月6日）。【Cyber Security Management Act. (2018, June 6). (in Chinese)】

歐芳伶（2008）。個人資訊安全認知量表設計之研究（未出版之碩士論文）。樹德科技大學資訊管理研究所，高雄市。【Ou, F.-L. (2008). *Development and validation of a perceptual instrument to measure personal information security awareness* (Unpublished master's thesis). Shu-Te University, Kaohsiung. (in Chinese)】

蕭瑞祥、羅雅萍、鄭哲斌（2012)。非營利組織資訊科技能力對資訊安全認知影響之研究。電腦稽核，*25*，57-71。doi: 10.30007/JICTA.201201.0005【Shaw, R.-S., Lo, Y.-P., & Cheng, C.-P. (2012). Fei ying li zu zhi zi xun ke ji neng li dui zi xun an quan ren zhi ying xiang. *Journal of Information Communication and Technology Auditing*, *25*, 57-71. doi:10.30007/JICTA.201201.0005 (in Chinese)】

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, *16*(3), 293-314. doi:10.1111/j.1365-2575.2006.00219.x

Drevin, L., Kruger, H. A., & Steyn, T. (2007). Value-focused assessment of ICT security awareness in an academic environment. *Computers & Security*, *26*(1), 36-43. doi:10.1016/j.cose.2006.10.006

Hansche, S. (2001). Designing a security awareness program: Part 1. *Information Systems Security*, *9*(6), 1-9. doi:10.1201/1086/43298.9.6.20010102/30985.4

International Organization for Standardization. (2018). *Information technology—Security techniques—Information security management systems—Overview and vocabulary* (ISO/IEC Standard No. 27000:2018). Retrieved from https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

International Organization for Standardization. (2019). *Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management—Requirements and guidelines* (ISO/IEC Standard No. 27701:2019). Retrieved from https://www.iso.org/standard/71670.html

International Organization for Standardization. (2020a). *Information technology—Information security incident management—Part 3: Guidelines for ICT incident response operations* (ISO/IEC Standard No. 27035-3:2020). Retrieved from https://www.iso.org/standard/74033.html

International Organization for Standardization. (2020b). *Information technology—Cybersecurity—Overview and concepts* (ISO/IEC Standard No. 27035-3:2020). Retrieved from https://www.iso.org/standard/72434.html

Kruger, H. A., & Kearney, W. D. (2008). Consensus ranking—An ICT security awareness case study. *Computers & Security*, *27*(7), 254-259. doi:10.1016/j.cose.2008.07.001

McKemmish, S., Cumming, K., Acland, G., Reed, B., & Ward, N. (2017). SPIRT Conceptual and relationship models (Version 3). *Monash University*. Retrieved from https://bridges.monash.edu/articles/report/SPIRT_Conceptual_and_Relationship_Models/5673646

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity: *Version 1.1*. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Raosoft. (2004). *S*ample size calculator. Retrieved from http://www.raosoft.com/samplesize.html

System Administration, Networking and Security. (n.d.-a). About SANS institute. Retrieved from https://www.sans.org/about/?msc=main-nav

System Administration, Networking and Security. (n.d.-b). Measuring your program maturity. Retrieved from https://www.sans.org/security-awareness-training/resources/maturity-model/

Wall, J. D., & Palvia, P. (2022). Understanding employees' information security identities: An interpretive narrative approach. *Information Technology & People*, *35*(1), 435-458. doi:10.1108/ITP-04-2020-0197

Wilson, M., de Zafra, D. E., Pitcher, S. I., Tressler, J. D., & Ippolito, J. B. (1998). *Information technology security training requirements: A role-and performance-based model* (National Institute of Standards Technology

Special Publication 800-16). Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf

Wilson, M., & Hash, J. (2003). *Building an information technology security awareness and training program* (National Institute of Standards Technology Special Publication 800-50). Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

附錄：「資通安全意識」調查問卷

第一部分：填答說明

1. 本問卷的填答對象為機關內文書檔案管理人員及資訊人員（包括有給職專任人員、約聘僱人員、業務委外廠商駐點人員）。
2. 本問卷填答分為兩部分，分別為「資安意識評估題項」及「個人基本資料」。有關資安意識評估題項，請根據您認為該資安議題的重要性以及該議題在您目前服務機關的達成程度，勾選您認為最符合的選項。填答時您僅需根據您個人之感受、同意程度及機關實際狀況，在對應選項右邊的方格（□）內打勾（V）即可。
3. 若您還有其他寶貴意見，請填入最下方的空欄內。
4. 本問卷填答時間約10 ~ 15分鐘左右，所填寫的資料將做為本研究之用，絕不個別對外公開、絕對保密，敬請安心作答。

第二部分：資安意識評估題項

填答說明：請在下列每一項目中，表達您認為該資安議題的重要性，以及該題描述您認為機關目前達到的程度。

認知重要性欄位：（您認為該題目重要性）5 表示「非常重要」、4 表示「重要」、3 表示「普通」、2 表示「不重要」、1 表示「非常不重要」。

機關達成程度欄位：（您認為該題目在貴機關達成程度）5 表示「完全符合」、4 表示「大部分符合」、3 表示「部分符合」、2 表示「大部分不符合」、1 表示「完全不符合」、0 表示「不清楚」。

資安意識	認知重要性					機關達成程度					
題項／欄位	非常重要	重要	普通	不重要	非常不重要	完全符合	大部分符合	部分符合	大部分不符合	完全不符合	不清楚
一、帳戶管理											
1. 自行管理電腦及各項系統（包含文檔系統）之個人帳戶資料及密碼，不提供他人使用或與他人共用。	□	□	□	□	□	□	□	□	□	□	□
2. 定期（約3 ~ 6個月）更換個人帳戶密碼並採用高強度密碼（8碼以上，且由英文數字及符號混合組成），發覺有洩漏之虞時，則立即更換。	□	□	□	□	□	□	□	□	□	□	□
3. 自然人憑證限本人使用，不提供他人使用或放在他人容易取得之處。	□	□	□	□	□	□	□	□	□	□	□
4. 不會採用生日、身分證字號或電話號碼等個人資料來設定重要密碼。	□	□	□	□	□	□	□	□	□	□	□
5. 系統帳號應有安全管理機制（例如密碼變更機制、帳號鎖定機制等），管理者不得未經使用者同意，自行閱覽、增加、刪除及修改使用者之私人資料。	□	□	□	□	□	□	□	□	□	□	□
6. 對於完成離職或異動之員工帳號，應停用或異動其帳戶權限。	□	□	□	□	□	□	□	□	□	□	□
其他寶貴意見，請於此說明：											
二、存取控制											
1. 文檔系統中根據人員業務需要建立使用者權限，非業務人員不會擁有該業務權限，例如文檔系統當中，發文人員有發文處理權限、檔案管理人員有檔案管理權限。	□	□	□	□	□	□	□	□	□	□	□
2. 使用者權限申請需具有相關異動管理紀錄，並定期對使用者權限進行清查。	□	□	□	□	□	□	□	□	□	□	□

資安意識	認知重要性					機關達成程度					
題項／欄位	非常重要	重要	普通	不重要	非常不重要	完全符合	大部分符合	部分符合	大部分不符合	完全不符合	不清楚
3. 使用者因業務調整、調職、停職或離職時，使用者帳戶依規定辦理異動，不可直接轉移至下一位業務承辦者。	□	□	□	□	□	□	□	□	□	□	□
4. 委外人員或廠商，不可未經授權遠端存取個人電腦或登入文檔系統。	□	□	□	□	□	□	□	□	□	□	□
5. 透過網路分享資料或建立共用資料夾時，會設定使用權限。	□	□	□	□	□	□	□	□	□	□	□
6. 當公文為非密等文書，可考量電子檔案長期保存風險，並於設備、人員能配合時，執行線上簽核及電子交換。	□	□	□	□	□	□	□	□	□	□	□
7. 保存年限超過10年之公文或機密公文，不採線上簽核方式處理。	□	□	□	□	□	□	□	□	□	□	□
8. 機關應採用開放性標準格式存取檔案，例如ODF、PDF等。	□	□	□	□	□	□	□	□	□	□	□
9. 資通安全需要明確指定專責人員進行規劃。	□	□	□	□	□	□	□	□	□	□	□
10.人員每日下班前，確定已登出作業系統並關機。	□	□	□	□	□	□	□	□	□	□	□
其他寶貴意見，請於此說明：											
三、系統防護											
1. 在電腦、行動設備及伺服器應安裝防毒軟體，定期掃描並更新病毒碼及修補系統漏洞。	□	□	□	□	□	□	□	□	□	□	□
2. 使用外接式硬碟或隨身碟時，應先執行病毒掃描。	□	□	□	□	□	□	□	□	□	□	□
3. 機關內各單位自行開發或管理之應用系統，需要建立版本控管機制，不得任意修改。	□	□	□	□	□	□	□	□	□	□	□

資安意識	認知重要性					機關達成程度					
題項／欄位	非常重要	重要	普通	不重要	非常不重要	完全符合	大部分符合	部分符合	大部分不符合	完全不符合	不清楚
4. 機關與外界網路連接的網點，應加裝防火牆，軟體程式之儲存由系統人員規劃並建立權限控管機制。	□	□	□	□	□	□	□	□	□	□	□
5. 機關的應用系統於開發或維護階段，不提供正式資料測試。	□	□	□	□	□	□	□	□	□	□	□
6. 機關應用系統進行開發、測試時，與正式作業環境應作區隔。	□	□	□	□	□	□	□	□	□	□	□
7. 廠商參與機關資訊系統開發、建置、資料轉置及資訊系統維護人員均應簽訂保密切結書。	□	□	□	□	□	□	□	□	□	□	□
8. 有關機關之資訊系統相關之硬體、軟體及資料，廠商不得任意攜離機關場所或任意增修調整。	□	□	□	□	□	□	□	□	□	□	□
9. 文檔系統應符合相關國內外技術標準/協定較有保障。	□	□	□	□	□	□	□	□	□	□	□
其他寶貴意見，請於此說明：											
四、行動安全											
1. 機關人員在手機、平板等行動裝置執行業務時，應避免裝置來路不明或不需要的行動應用程式（App）。	□	□	□	□	□	□	□	□	□	□	□
2. 從手機、平板等行動裝置連入機關內部網路，要執行身分辨識作業（如使用動態密碼辨識系統）及使用防火牆等方式進行安全控管。	□	□	□	□	□	□	□	□	□	□	□
其他寶貴意見，請於此說明：											
五、上網行為											
1.瀏覽網頁時發現可用資料，會先判斷來源，不會直接下載使用。	□	□	□	□	□	□	□	□	□	□	□

資安意識	認知重要性					機關達成程度					
題項／欄位	非常重要	重要	普通	不重要	非常不重要	完全符合	大部分符合	部分符合	大部分不符合	完全不符合	不清楚
2. 面對不清楚來源的網路超連結，不輕易去點選。	□	□	□	□	□	□	□	□	□	□	□
3. 對於不信任之網站出現要求同意相關授權之資訊，不輕易點選同意。	□	□	□	□	□	□	□	□	□	□	□
4. 具機密或有敏感性之資料，不會存放於對外開放之系統中。	□	□	□	□	□	□	□	□	□	□	□
5. 當要從遠端登入內部網路系統之資通服務，要執行身分辨識作業（如使用動態密碼辨識系統）及使用防火牆等方式進行安全控管。	□	□	□	□	□	□	□	□	□	□	□
6. 對於公務機關之連線，須透過機關網路，未經機關核准，不擅自建置連線設備，如有個別需求時，應提出申請，另建置防火牆，並於作業結束後關閉權限。	□	□	□	□	□	□	□	□	□	□	□
7. 不在機關電腦巡行安裝未具合法版權或非公務用之軟體。	□	□	□	□	□	□	□	□	□	□	□
其他寶貴意見，請於此說明：											
六、電子交換											
1. 收到來源不明之電子郵件或特殊標題之郵件，會先判斷郵件的安全性，不會輕易點開。	□	□	□	□	□	□	□	□	□	□	□
2. 具機密或敏感性之資料，不以電子郵件傳送，如有電子郵件傳送之必要時，應經單位主管核准並加密處理。	□	□	□	□	□	□	□	□	□	□	□
3. 使用者停職或離職後，應刪除其公務郵件帳號。	□	□	□	□	□	□	□	□	□	□	□
4. 機關收文人員收到電子來文於辨識解簽章後，應即儲存，如發現資料遭竄改，應立即通知原發文機關處理，並通報機關資訊單位。	□	□	□	□	□	□	□	□	□	□	□

資安意識	認知重要性					機關達成程度					
題項／欄位	非常重要	重要	普通	不重要	非常不重要	完全符合	大部分符合	部分符合	大部分不符合	完全不符合	不清楚
5. 電子交換須使用有效期之機關憑證，機關憑證應妥善保存，並於效期過期前更新，以免交換異常。	□	□	□	□	□	□	□	□	□	□	□
其他寶貴意見，請於此說明：											
七、實體安全											
1. 機關總收文人員收到來文時，應檢視包封、附件是否完整相符，如包封破損應予註明，附件不齊全，應即洽詢原發文機關補送。	□	□	□	□	□	□	□	□	□	□	□
2. 機關總收文人員收到文件拆封後，如為機密文件或書明親啟字樣之文件，應於登錄後，交由長官指定之專人或收件人收拆。	□	□	□	□	□	□	□	□	□	□	□
3. 總收文人員收到現金、支票、貴重或大宗物品，應先送出納人員或相關單位之承辦人簽收保管。	□	□	□	□	□	□	□	□	□	□	□
4.機關應指定專人（簡稱登記桌）負責單位收發業務，如有異動，應將業務有關事項詳實交代接任者。	□	□	□	□	□	□	□	□	□	□	□
5. 對於機關各類公文流程，會依文書處理手冊、機關檔案管理作業手冊相關規定辦理，並避免不相干的人接觸、拿到或看到機密或有敏感性之資料。	□	□	□	□	□	□	□	□	□	□	□
6. 使用電腦時，若離開座位，會確保鎖定使用環境，確保他人無法使用我的文檔系統或開啟我的檔案。	□	□	□	□	□	□	□	□	□	□	□
7. 有關載有機密或敏感性資料之筆記型電腦、行動裝置、隨身碟、光碟片等，存放時不放置於他人容易取得之處。	□	□	□	□	□	□	□	□	□	□	□

資安意識	認知重要性					機關達成程度					
題項／欄位	非常重要	重要	普通	不重要	非常不重要	完全符合	大部分符合	部分符合	大部分不符合	完全不符合	不清楚
8. 使用共用系統或設備（如共用筆記型電腦）時，於使用完畢，會避免留下個人資料。	□	□	□	□	□	□	□	□	□	□	□
9. 對於機關之廢棄公文、文稿、光碟等各類形式文件，如具機密或敏感性之內容時，會依規定澈底銷毀處理。	□	□	□	□	□	□	□	□	□	□	□
10. 機關之機敏資料未經允許不得攜出機關。	□	□	□	□	□	□	□	□	□	□	□
11. 機密文書歸檔時，承辦人員應使用機密檔案專用封套裝封，並於封面上註明單位名稱、收發來文字號、未涉及機敏資料之案由或案名、分類號等完整資料，封口簽章後，送檔案管理單位辦理歸檔。	□	□	□	□	□	□	□	□	□	□	□
12. 各類形式之檔案均應依保存年限妥善保管，機密檔案則應由機關首長指定專人或由檔案管理單位主管管理，並應與一般檔案分別存放。	□	□	□	□	□	□	□	□	□	□	□
13. 資訊機房應有出入管制及監錄系統。	□	□	□	□	□	□	□	□	□	□	□
14. 檔案庫房應有出入管制及監錄系統。	□	□	□	□	□	□	□	□	□	□	□
其他寶貴意見，請於此說明：											
八、備份機制											
1. 機關應訂定完整備援機制。	□	□	□	□	□	□	□	□	□	□	□
2. 資料建置後，應定期執行資料及系統軟體備份。	□	□	□	□	□	□	□	□	□	□	□
3. 備份資料至少製作2份為宜，除存放在主要的作業場所外，應另存放在離機關有一段距離的場所。	□	□	□	□	□	□	□	□	□	□	□

資安意識	認知重要性					機關達成程度					
題項／欄位	非常重要	重要	普通	不重要	非常不重要	完全符合	大部分符合	部分符合	大部分不符合	完全不符合	不清楚
4. 電子儲存媒體（如光碟片、硬碟等）需要定期確認其有效性，必要時執行備份及轉置。	□	□	□	□	□	□	□	□	□	□	□
5. 公文檔案管理系統要定期執行災害復原演練。	□	□	□	□	□	□	□	□	□	□	□
其他寶貴意見，請於此說明：											
九、遵守政策											
1. 機關應訂有資通安全計畫。	□	□	□	□	□	□	□	□	□	□	□
2. 機關應訂有資通安全風險管理。	□	□	□	□	□	□	□	□	□	□	□
3. 人員應清楚知道所屬機關的資安等級及資安政策。	□	□	□	□	□	□	□	□	□	□	□
4. 人員應配合機關資安政策，參與相關資安訓練。	□	□	□	□	□	□	□	□	□	□	□
5. 各機關每年辦理1次通報演練及2次電子郵件社交工程演練。	□	□	□	□	□	□	□	□	□	□	□
6. 當文書及檔案管理相關法規修訂施行後，資訊系統必須配合修正。	□	□	□	□	□	□	□	□	□	□	□
其他寶貴意見，請於此說明：											
十、事件通報											
1. 當電腦的資料外洩或遭入侵時，應立即主動通報。	□	□	□	□	□	□	□	□	□	□	□
2. 當發現電腦有中毒跡象時，應立即主動通報。	□	□	□	□	□	□	□	□	□	□	□
3. 機關在知悉資通安全事件後，應於1小時內依主管機關指定之方式及對象，進行資通安全事件之通報。	□	□	□	□	□	□	□	□	□	□	□
其他寶貴意見，請於此說明：											

第三部分：個人基本資料

1. 性別：□男　□女　□其他

2. 年齡：
□18～30歲　□31～40歲　□41～50歲　□51～60歲　□61歲以上

3. 服務年資：
□未滿2年　□滿2年未滿5年　□滿5年未滿10年　□滿10年未滿20年
□超過20年

4. 您的職等：□簡任　□薦任　□委任　□其他_____

5. 您的職務：
□文檔主管：機關內文書檔案業務單位之正副主管。
□資訊主管：機關內文書資訊業務單位之正副主管。
□文書人員：機關內辦理收發文、登記桌、公文時效管制等業務人員。
□檔案人員：機關內辦理檔案點收、立案編目、保管、檢調、清理、安全維護等業務。
□資訊人員：機關內文檔系統之管理者、機關資通安全專責人員及其他資訊人員。
□委外人員：其他文檔系統相關業務人員，包含廠商駐點人員、委外援服務人員。
□其他

6. 您的最高學歷：
□國小　□國中　□高中（職）　□專科　□大學　□碩士　□博士
□其他_____

7. 您是否接受過文檔或資訊相關教育訓練?
□是，請勾選接受的文檔或資訊教育訓練（可複選）：
□文書教育訓練　□檔案教育訓練
□資訊教育訓練（包含資安訓練）
□否

8. 您工作上接觸到電腦的頻率為：
□幾乎每天　□經查（平均每週3～5天）
□偶爾（平均每週1～2天）　□很少（平均每週小於1天）
□幾乎沒有

9. 您工作上接觸到文檔系統的頻率為：
□幾乎每天　□經查（平均每週3～5天）
□偶爾（平均每週1～2天）　□很少
□幾乎沒有

※問卷到此結束，再次感謝您的協助與支持！

Discussion on the Assessment Framework of Cybersecurity Awareness on Electronic Record Management System and Its Practical Application

Chiao-Min Lin
Professor
Graduate Institute of Library, Information and Archival Studies
National Chengchi University

Yin-Chih Liu
Associate Clerk
Taoyuan Police Department

Introduction

Information security threats for electronic records management systems (ERMS) in the information era are increasing daily. Therefore, it is essential to strengthen the information security awareness of individuals involved with ERMS to maintain government information security and defend the authenticity of the content of documents and archives. This study investigated the level of information security awareness of personnel using ERMS to determine whether there are differences between different personnel. The findings can help clarify the need for information security education for government agency personnel and provide a reference for revising the agencies' archive management policies or establishing information security training courses.

Method

Based on Taiwan's laws and regulations related to information security and relevant foreign standards, this study compiled the first draft of the "Information Security Awareness Assessment Questionnaire" by synthesizing

the essential concepts and consolidating the textual descriptions. Eight scholars and experts from the archive management and information management fields (four from each field) were invited to participate in the Delphi survey. The Taoyuan City Government was treated as the target for the analysis of the information security awareness. A total of 148 questionnaires were distributed, and 100 were returned, with a recovery rate of 67.56%.

Results

1. Survey Results From the Information Security Awareness Assessment Questionnaire

The questions of the information security awareness assessment questionnaire were categorized into 10 dimensions: "account management," "access control," "system protection," "mobile security," "internet behavior," "electronic exchange," "physical security," "backup mechanisms," "policy compliance" and "incident notification." Eight scholars and experts in archive or information management with theoretical and practical backgrounds were consulted. The questionnaire statistics indicate a high level of relevance and consensus during the first and second rounds of the survey. The questionnaire responses reached an average convergence rate of 89.6% in the second round. Thus, the survey process was considered complete after the second round.

2. Results of the Case Evaluation of the Information Security Awareness Assessment Questionnaire

This study analyzed the survey results from 100 questionnaires collected from the agencies of the Taoyuan City Government. The mean of each dimension of the questionnaire ranged from 4.68 ~ 4.82. The standard deviation values ranged from .40 ~ .59. The mean of the "incident notification" dimension was the highest (M = 4.82, SD = .40), and the mean of the "access control" dimension was the lowest (M = 4.68, SD = .59) (see Table 1).

Table 1 Statistical Analysis of the Information Security Awareness Survey Results for ERMS

Dimension	Perceived importance		Agency's level of achievement	
	Average	Standard deviation	Average	Standard deviation
Account management	4.77	.47	4.49	.69
Access control	4.68	.59	4.53	.69
System protection	4.75	.48	4.59	.66
Mobile security	4.78	.45	4.50	.67
Internet behavior	4.77	.45	4.53	.65
Electronic exchange	4.77	.50	4.61	.62
Physical security	4.76	.45	4.64	.60
Backup mechanism	4.70	.52	4.37	.82
Policy compliance	4.70	.49	4.61	.64
Incident notification	4.82	.40	4.70	.49
Overall	4.74	.49	4.57	.66

3. Correlation Analysis of Perceived Importance and Achievement Level

We used Pearson's product-difference correlation to analyze the correlation between the "perceived importance" and "agency's level of achievement" vectors. The results indicate significant positive correlations between the two vectors as a whole and each dimension of the two vectors. There was a low positive correlation ($r < 0.4$, $p < .001$) for "account management." However, the remaining dimensions all indicate a moderate positive correlation ($r \geq 0.4$, $p < .001$). Those with higher perceived importance had a higher level of achievement, and the two were positively correlated.

4. Differences in Information Security Awareness Between Record Management Staff and Information Staff

This study conducted an independent sample *t*-test to determine the difference in information security awareness between information staff and record management staff in the city government. Regarding "perceived

importance," only the "incident notification" dimension reached a significant level. This indicates that information staff attached more importance to "incident notification" than record management staff. The remaining and the overall dimensions did not reach a statistically significant level. regarding "agency's level of achievement," only the "policy compliance" dimension reached a significant difference. This indicates that the information staff agreed more than the record management staff that the agency complied with the information security requirements, reaching a statistically significant difference.

Conclusions

The following conclusions were obtained in this study.

1. This study's Delphi method survey questionnaire reached convergence in the second round. We found a high degree of relevance and consensus in both the first and second rounds. The findings indicate a high degree of consensus among scholars and experts from archival and information backgrounds regarding ERMS information security issues. Thus, 67 questions in 10 dimensions were finalized and proposed.
2. The overall information security awareness of the government agencies' record management and information staff was positive, and most opinions tended to be the same. Most respondents attached the highest importance to "incident notification" and had the most confidence in the agency's level of achievement for "incident notification." "Access control" was considered the least important, and both types of staffs had the least confidence in the agency's level of achievement concerning the "backup mechanism."
3. The "perceived importance" of information security awareness of the personnel in the government agencies was slightly higher than the "agency's level of achievement" on average. Moreover, there was a significant positive relationship between "perceived importance" and the "agency's level of achievement."
4. Comparing the differences between record management staff and information staff illustrates that information staff paid more attention to the "incident notification" dimension of "perceived importance" than record management staff. Regarding the "policy compliance" dimension of the

"agency's level of achievement," information staff were more confident than record management staff in the agency's level of achievement.