種苗場導入資訊安全管理系統 (ISMS) 之分享

Sharing of introduction of information security management system for ISO 27001 in Taiwan Seed Improvement and Propagation Station

徐麗芬[1]、劉月娟[2]、張文昌[3]、郭宏遠[4]

一、前言

爲積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益，我國於 2018 年 5 月 11 日制定資通安全管理法，並於同年公布，於 2019 年 1 月 1 日施行。依資通安全管理法第七條第一項規定，主管機關應衡酌公務機關及特定非公務機關業務之重要性與機敏性、機關層級、保有或處理之資訊種類、數量、性質、資通系統之規模及性質等條件，訂定資通安全責任等級之分級。

爲明確規範資通安全責任等級之分級基準、…專責人員之設置及其他相關事項，以利各受規範對象得妥適辦理資通安全維護事務，強化資通安全管理能量，爰訂定「資通安全責任等級分級辦法」。

依據資通安全責任等級分級辦法規定，種苗改良繁殖場 (以下簡稱本場) 配合法規要求並盤點現有軟、硬體設備及設施，係爲列位 C 級機關 (定期檢討等級)，依規應持續維持導入資訊安全管理系統（Information security management system, ISMS）之標準及要求。爲符合此一要求，本場於 2020 年開始規劃導入 ISO 27001 資訊安全品質管理系統，範圍涵蓋本場各業務課室、研究單位及屏東種苗研究中心。本文以本場現行導入 ISMS 符合性做一介紹，希冀提供相關單位導入 ISMS 示範參考。

二、何謂 ISMS?

(一) 定義與概念

資訊可以多樣貌形式存在，無論形式爲何或是透過何種方式儲存，都應適當的接受保護，ISMS(資訊安全管理系統，Information security management system 英

[1] 種苗改良繁殖場技術服務室 助理研究員
[2] 種苗改良繁殖場技術服務室 技工
[3] 種苗改良繁殖場技術服務室 駐點資訊工程師
[4] 種苗改良繁殖場技術服務室 副研究員兼主任

註 ISO 27001:2013 條文

文縮寫)，便是一套有系統的分析和管理資訊安全風險的方法。我國經濟部標準檢驗局 2014 年 4 月 24 日公告 CNS 27001「資訊技術 - 安全技術 - 資訊安全管理系統－要求事項」國家標準，CNS 27001 係參考 2013 年最新版 ISO 27001 國際標準修訂，爲 ISMS 系列標準之重要指導綱要。現行 ISO 27001:2013 其主文計有十個章節，該標準是爲了提供建立、實施、維護與持續改進一個資訊安全管理系統 (ISMS) 的要求而籌設，另有附錄 35 項目標與 114 項控制措施需遵守，並配合 PDCA(規劃、行動、檢查、執行) 模式循環運作。

(二) 重要性

如同科技研發成果與軟硬體設施等財產，資訊也是一種對機關具有價值的重要資產，包含電腦系統、資訊紀錄、基礎設施服務、配置區域與設備以及人力資源。我們常認爲資訊安全是資訊人員的事，或者購買高級防護設備或軟體就 100% 資訊安全。然而，資訊安全管理從單位上到下都需要承諾與支援，對於風險事件識別與審查需要協調、溝通與持續改善，人員的資訊安全概念與適切教育訓練，都需一有系統的管理。

(三) 目標

資源與經費有限，風險的發生常無法避免，要達到 100% 資訊安全管理有時可能需耗費過多人力、物力等資源。對機關內部而言，進行有系統的資訊安全管理便是透過控制方法把資訊風險降低，使其 (風險) 至可接受的範圍，保障機關資訊資產免於不可承受的風險。另外部因應法律與規範要求方面，機關需考量保護範圍是從人員資料以至全機關的隱私，亦期待透過 ISMS 導入來符合要求。

三、種苗場 ISMS 運作模式

(一) 成立資訊安全組織

ISO 27001:2013 條款 1~3 爲範圍、參考標準及名詞與定義，由條款 4 進入資訊安全管理系統主要內容 (表一)，以下分就各條款與本場現行導入範圍，茲提供其他單位參考使用。爲確保本場資訊安全管理制度之有效運作，凡有影響品質之管理、執行及相關人員，其權責與相互關係，均明訂於組織權責管理程序 (條款 4 組織背景)[註]。組織架構圖如下：

表一、 ISO 27001:2013 標準條文

項次	章	節	小節
第一章	範圍（Scope）		
第二章	規範性引用文件（Normative references）		
第三章	術語和定義（Terms and definitions）		
第四章	組織的背景（Context of the organization）		
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	
第五章	領導（Leadership）		
5.1		管理者承諾	
5.2		政策	
5.3		組織角色、責任及權限	
第六章	規劃（Planning）		
6.1		因應風險及機會之行動	
6.1-1			一般要求
6.1-2			資訊安全風險評鑑
6.1-3			資訊安全風險處理
6.2		資訊安全目標及其達成之規劃	
第七章	支持（Support）		
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	
7.5-1			一般要求
7.5-2			制訂及更新
7.5-3			文件化資訊之控制
第八章	運行（Operation）		
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	
第九章	績效評估（Performance evaluation）		
9.1		監督、量測、分析及評估	
9.2		內部稽核	
9.3		管理審查	
第十章	改善（Improvement）		
10.1		不符合項目及矯正措施	
10.2		持續改善	

本場以提供建立、實施、維護與持續改進 ISMS 的要求爲目標，以技術服務室專責該系統之運作，成員計有資安長 1 人、技術服務室主任 1 人、資訊主辦 1 人、技工 1 人及駐點資訊工程師 1 人。並依照標準設有資通安全組 (轄下設置策略規畫小組、資安防護小組、績效管理小組) 與資訊推動組，其成員爲本場各業務課室主管兼辦及其課室內指派資訊幹事各 1 名。

(二) 制定資訊安全相關文件

文件的撰擬常常讓人摸不著頭緒，建議可參考使用行政院國家資通安全會報所提供之「資通安全維護計畫」範本，來加以制定成符合機關的資訊安全管理手冊。

該範本另包含核心業務及重要性、資安政策與目標、資安推動組織 (條款 4 組織背景、條款 5 領導) [註]、人力及資源分配 (條款 7 支持) 、資訊及資通系統之盤點、資安防護及控制措施、資安事件通報與應變及演練、委外服務之管理 (條款 6 規劃、條款 8 運行) 、資安教育訓練 (條款 7 支持) 、持續精進及績效管理 (條款 9 績效評估、條款 10 持續改進) 等，已有提供撰寫說明及相關表格範例，比對 ISO 27001:2013 條款內容多有符合，可減輕單位承辦撰寫文件壓力。ISO 27001：2013 條文與本場資訊安全管理系統各文件對照表規劃如表二。

爲補足範本文件與符合條款基本要求，本場另訂有：

1. 資訊推動小組設置要點，其任務包含本場資訊作業整體規劃之審議事項、年度資訊作業計畫及資訊預算之審議事項、推動農業種苗網際網路之應用等事項之督導、資安需求及資訊安全機密維護、稽核、使用管理事項之審議以及資訊管理規定之審議等 (條款 9 績效評估、條款 10 持續改進)。
2. 內部資訊安全稽核作業，其目的係爲建立一管理程序，以規劃、執行及檢討內部稽核、確認各項活動及其相關結果是否符合資訊安全管理之要求目標，藉以掌握本場資訊安全的可能缺失，適時執行矯正行動及追蹤確認，並確保其有效性及持續之改善 (條款 9 績效評估)。
3. 資通安全事件通報及應變管理程序，遵照資通安全管理法第 14 條及本機關資安全維護計畫之規定，建立本機關資通安全事件之通報及應變機制，以迅速有效獲知並處理事件，特制定本資通安全事件通報及應變管理程序 (條款 8 運行)，以期更加提升並符合條款內之要求。

(三) 制定資訊資產分類分級與風險評鑑

導入資訊安全或通過驗證，並不表示機關就不會再發生資安事件或風險，而是使其資安事件或風險發生時，機關能快速且有效的啓動應變與後續改善使其事件不再發生或降低至可接受範圍，而什麼是機關可接受範圍？機關可透過制定資訊資產分類分級與風險評鑑來判斷。實務上風險管理階段操作的介紹與需要說明的篇幅較多，本段僅就觀念簡單說明。

所謂風險，亦即是當威脅利用其相對應脆弱性，直接或間接造成機關資訊及資通系統 (一個或一群) 受到損害的可能性，例如筆記型電腦 (資產) 可能因爲較爲輕巧好攜帶 (脆弱點)，有心人士 (威脅) 可快速且不易被發現情形下取得 (攻擊手法)。

風險可大可小，資訊資產耐受性與管理的程度也有不同，因此我們需要知道機關內各資訊資產的分類與分級爲何？並可考慮現存控制措施是否適當或需要另行制定？評估風險並決定該風險是否爲可接受？以避免當某一風險發生恐造成無法負荷之重，便是風險評鑑之目的。

本場執行此一階段時，首要步驟先針對各資訊資產本場會先盤點列出清單 (此一步驟在撰寫資訊安全維護計畫時會需要，可以搭配使用) 並歸納屬性類別，以及區別各資訊資產面對內、外部因子下的安全特性 (機密性、完整性、可用性) 以利了解資產價值，接著並搭配風險發生之威脅與脆弱，依其嚴重性、可能性形成風險評估矩陣，最終識別各個資產價值並排序風險等級，依風險等級數值高低，給予適當控制措施。

(四) 監控與審核 ISMS

本場執行 ISMS 主要依據「資通安全維護計畫」，於年度內皆會定期辦理策略規劃、資安防護、績效管理等小組會議，以達成監控與有效性，各小組任務包含：

1. 策略規劃小組：(1) 資通安全政策及目標之研議；(2) 訂定資通安全相關規章與程序、制度文件，並確保相關規章與程序、制度合乎法令及契約之要求；(3) 依據資通安全目標擬定年度工作計畫；(4) 傳達資通安全政策與目標以及 (5) 其他資通安全事項之規劃。
2. 資安防護小組：(1) 資通安全技術之研究、建置及評估相關事項；(2) 資通安全相關規章與程序、制度之執行；(3) 資訊及資通系統之盤點及風險評估；(4) 資　及資通系統之安全防護事項之執行；(5) 資通安全事件之通報及應變機制之執行以及 (6) 其他資通安全事項之辦理與推動。
3. 績效管理小組：(1) 辦理資通安全內部稽核以及 (2) 每年定期召開資通安全管理審查會議，提報資通安全事項執行情形。

以上對於資安組織之運作均於年度內執行完成，而於年度內對於資通訊設備與人員均有實施相關教育訓練課程 (內、外訓等)，場內駐點維護廠商於招標時即有要求須符合 CNS 27001 或 ISO 27001 等資訊安全管理系統標準，以期符合 ISMS 條文規則。

四、結語

種苗場因業務屬性，場內各業務單位之實驗室在近 10 年間，均有陸續導入符合 ISO 9001 品質管理的標準以及 ISO 17025 實驗室品質管理系統。而依據筆者往年協助內部稽核發現，各實驗室在品質管理上均有重複相同性質作業在運行，有鑑於部分階層作業重複性 (例如文件管理、知識管理及內部稽核等)，本場積極規劃將實驗室整合並持續維持其符合性，以降低同仁重複執行相同作業的耗損與每年評估有效性的費用成本。

經濟部標準檢驗局於 2006 年開始全面導入 ISO 27001 資訊安全品質管理系統，範圍涵蓋總局、6 個分局及 15 個辦事處，表示相關符合國際或國內的管理系統，蓋無論組織大小均可透過規劃與範圍設定而有效地併行與實施。爰此，希冀透過本場現行導入 ISMS 符合性做簡單之介紹，提供相關單位導入 ISMS 示範參考。

表二、 ISO 27001：2013 條文與本場資訊安全管理系統各文件對照表

ISO 27001：2013 條文	對應文件名稱
4. 組織的背景	
4.1 瞭解組織及其全景	資通安全維護計畫
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	
5.1 管理者承諾	資通安全維護計畫 資訊推動小組設置要點
5.2 政策	
5.3 組織的角色、職責和權限	
6. 規劃	
6.1 因應風險和機會之行動	資通安全維護計畫
6.1.1 一般要求	
6.1.2 資訊安全風險評鑑	
6.1.3 資訊安全風險處理	
6.2 資訊安全目標及其達成之規劃	
7. 支持	
7.1 資源	資通安全維護計畫 資訊推動小組設置要點
7.2 能力	
7.3 認知	
7.4 溝通或傳達	
7.5 文件化資訊	
7.5.1 一般要求	
7.5.2 制訂及更新	
7.5.3 文件化資訊之控制	
8. 運行	
8.1 營作之規劃及控制	資通安全維護計畫 資通安全事件通報及應變管理程序 內部資訊安全稽核作業
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、分析和評估	資通安全維護計畫
9.2 內部稽核	內部資訊安全稽核作業
9.3 管理審查	資通安全維護計畫
10. 持續改進	
10.1 不符合項目和矯正措施	資通安全維護計畫
10.2 持續改進	