圖片來源：Shutterstock

農業保險基金通過 ISO 27001 資訊安全驗證分享

文／盧定宏 任職於財團法人農業保險基金

壹、前言

隨著業務流程數位化轉型，資訊安全與個資保護已成全球關注焦點。近年來，網路攻擊與資料外洩事件頻傳，資訊安全係組織營運必要條件，亦為國家與社會安定的基石。在此背景下，提升全民與企業的資訊安全意識，對組織永續發展至關重要。基於前述需要，國際標準組織（ISO）訂定ISO 27001（資訊安全管理國際標準），旨在建立、實施、維護和持續

改進資訊安全管理系統（ISMS），此標準提供全面性框架，協助組織保護其資訊資產機密性、完整性和可用性，並可應對不斷變化的資訊安全風險。

財團法人農業保險基金（下稱本基金）屬C級非特定公務機關，基於資訊安全對於保護個資及確保業務持續運作重要性。為展現對資訊安全承諾，及因應升級為B級非特定公務機關，本基金超前部署，以符合資通安全責任等級分級辦法B級要求為目標，積極導入並驗證ISO 27001資訊安全管理系統。

貳、導入ISO 27001之動機與目標

本基金因業務運作需涉及大量個資，一旦發生資訊安全事件，不僅可能損害被保險人權益，更將嚴重影響政府形象與農險制度公信力。此外，隨著業務發展，本基金如升級為B級非特定公務機關時，屆時將面臨更嚴峻的資訊安全要求。基於上述考量，且本基金高度重視資訊安全議題，決定導入ISO 27001資訊安全管理系統，具體目標如下：

一、強化資訊安全意識

提升全體同仁對資訊安全風險的認知與警覺性，並培養積極主動的資訊安全防護意識及良好資訊安全習慣。

二、建立標準化資訊安全流程

依據ISO 27001標準建立一套系統化的資訊安全管理流程，涵蓋風險評鑑、政策制定、安全控制措施實施與監控等環節。

三、保護個資安全

透過有效安全控制措施，確保個資機密性、完整性與可用性。

四、提升本基金營運韌性

建立完善的災害復原與業務持續運作計畫，並定期進行演練與測試，確保其有效性，能在突發狀況下業務能迅速恢復。

五、為未來升級奠定基礎

提前符合B級非特定公務機關資訊安全要求，為本基金長遠發展做好準備。

六、取得國際認證

通過第三方認證機構驗證，展現本基金對資訊安全的承諾，提升社會公信力。

參、ISO 27001導入與驗證歷程

本基金自民國111年將ISO 27001併同ISO 27701（隱私資訊管理）導入，並

確立以ISO 27001為驗證目標後，積極展開相關工作，導入與驗證歷程可分為下列幾個階段：

一、專案啟動與規劃

由本基金資通安全暨個資保護管理代表（即副總經理）為召集人，並由各單位主管及資訊安全專責人員組成資通安全暨個資保護推動小組，負責統籌規劃與執行資通安全及個資保護相關事項。推動小組下設4個小組（如圖1），分別為策略規劃、技術防護、資通安全績效管理及個資保護工作小組。為確保導入工作順利，本基金亦藉由外部專業顧問團隊協助，提供專業指導與諮詢。

二、現況分析與風險評鑑

在專業顧問團隊協助下，本基金針對現有資訊安全管理狀況進行詳細分析，包括資訊資產盤點、法規遵循性檢視、以及既有安全控制措施的有效性評估。於首次辦理資訊資產盤點因缺乏經驗，歷經多次跨部門溝通會議與合作後終能順利完成資產盤點作業。接續，依據ISO 27001標準並同時參考ISO 27005（資訊安全風險管理）標準，進行資訊安全風險評鑑。本階段因各部門對風險認知與接受度不同，亦歷經多次討論後並達成共識制定風險處理計畫，本計畫可識別與評估本基金所面臨的資安威脅與弱點。

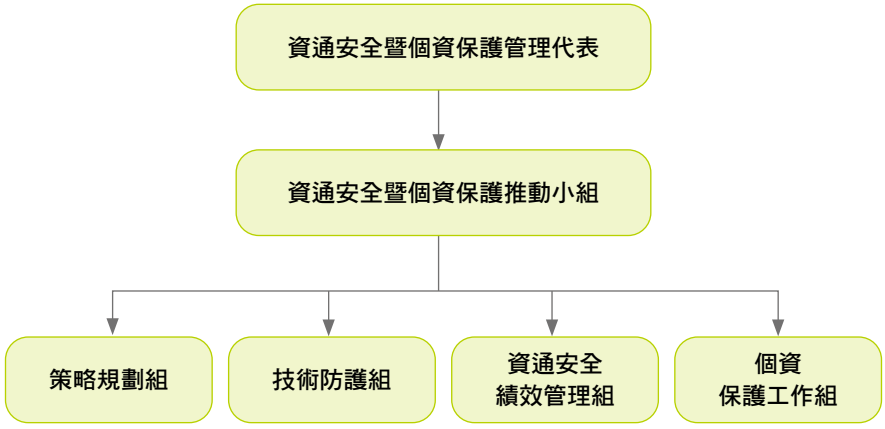

圖 1、資通安全暨個資保護推動小組架構

資料來源：財團法人農業保險基金

三、ISMS建置

依據風險評鑑結果，本基金著手制定符合ISO 27001標準的ISMS，內容包含資訊安全政策、程序、指導文件等，涵蓋各項控制措施，例如存取控制、密碼管理、網路安全、實體安全、人員安全、事件管理及業務持續運作管理等。文件制定初期經與各部門多次溝通並藉由顧問指導協助，將國際標準與內部業務特性結合，以確保文件符合實際作業流程及具備可操作性。

四、系統實施與內部稽核

系統實施與內部稽核階段，本基金於制定ISMS後，即於內部全面推動與實施，包含辦理資訊安全教育訓練、落實安全政策與程序，並制定事件通報與處理機制。為檢視系統有效性，本基金依據ISO 27001標準執行內部稽核，由專業顧問團隊稽核員對各單位資訊安全管理實施情況進行審查，並提出缺失及改善建議，然實務上資訊安全教育訓練成效往往需長時間才能呈現。在內部稽核階段，初期面臨同仁對稽核工作專業能力與經驗不足等問題，為避免稽核結果不如預期，透過資通安全暨個資保護推動小組持續與單位同仁及稽核員溝通說明，順利完成內部稽核；更重要的是，有效地追蹤與落實內部稽核所提出之稽核意見，亦是確保系統持續有效運作的關鍵環節，對於相關稽核意見，各承辦單位皆盡速完成矯正以符合ISO 27001要求。

五、管理審查

內部稽核完成後，本基金資通安全暨個資保護推動小組會召開管理審查會議，由高階管理階層負責審視資訊安全及個資管理系統整體運作情況，審查內容包含內部稽核結果、風險評鑑結果、事件處理情況以及改善建議的執行狀況。透過管理審查，旨在確保ISMS能夠持續改進，有效應對不斷變化的資訊安全風險。管理審查的成效取決於高階管理階層的參與程度與重視程度，本基金每年召開1次管理審查會議，於導入期間為確保管理審查能夠產生具體的改進措施並有效執行，額外召開多次管理審查會議。

六、第三方驗證

自導入ISMS後，經過一段時間系統運行與持續改善後，本基金於113年3月20日至21日正式邀請第三方驗證機構之英國標準協會臺灣分公司（下稱BSI）進行ISO 27001驗證稽核。BSI的稽核團隊透

本基金通過ISO 27001認證證書。圖片來源：財團法人農業保險基金

ISO 27001授證典禮。圖片來源：財團法人農業保險基金

過預先審查、文件審查、現場訪談、以及實地審查等方式，對本基金ISMS進行了全面且嚴謹的評估。為避免審查期間發生驗證準備不足狀況，本基金召開多次驗證說明及訓練會議；審查過程中，對於稽核員提出的不符合事項，亦經資通安全暨個資保護推動小組及外部專業顧問持續與稽核員溝通協商並提供證據，最終達成共識，並完成初次驗證審查。

七、順利取得ISO 27001認證

經歷兩天審查，BSI稽核團隊對本基金在資訊安全管理方面的努力與成果給予高度肯定，並於稽核結束後正式宣布本基金順利通過ISO 27001驗證，並於113年5月頒發認證證書。即使順利取得認證，並不代表資訊安全工作可以鬆懈。此認證僅表示本基金資訊安全管理已達國際標準，惟後續仍需持續維護、改善與定期追蹤稽核，確保系統有效性、保護個資，並提升營運韌性、強化資訊安全、符合相關法規要求、有效管理潛在的資訊風險，以確保業務的穩定運行與持續發展。

肆、驗證歷程之經驗與啟示

本基金順利導入並驗證ISO 27001資訊安全管理系統，不僅提升了自身資訊安全防護能力，同時也為其他機關團體提供了寶貴經驗與啟示：

一、高階管理階層承諾與支持至關重要

資訊安全並非單一部門責任，需要高階管理階層高度重視與全力支持，才能確保專案順利推動。

二、完善規劃與準備是成功的基石

導入ISO 27001之前，充分的現況分析、風險評鑑以及詳細專案規劃至關重要，能夠為後續系統建置與實施奠定堅實基礎。

三、全員參與與提升資訊安全意識是關鍵

資訊安全需要全體同仁共同努力，透過持續的教育訓練與溝通，提升同仁資訊安全意識，才能真正落實各項安全控制措施。

四、持續改進維持系統有效性的關鍵

ISO 27001是一個持續改善的過程，應定期進行內部稽核與管理審查，不斷優化ISMS，以應對不斷變化的資訊安全威脅。

五、尋求專業協助能事半功倍

導入ISO 27001需要專業知識與經驗，適時尋求外部專業顧問協助，能夠有效地提升導入效率與品質。

六、資源配置需求

本基金資訊安全初期導入時，發現人力及系統資源缺乏，因資源及預算有限狀況下無法及時補足，導致推動過程中進度延遲，最終以現有人力分配及年度預算編列逐步改善。

七、文件化數量

導入初期時，為了符合標準及本基金所制訂的相關文件要求，將所有業務流程文件化會產生大量表單，在實際執行中會帶來困難。因此，藉由外部專業顧問的建議，我們整合部分文件化表單，並調整使其更符合本基金的需求，以簡化流程並提升執行效率。

伍、結語與展望

本基金取得ISO 27001認證後，不僅是對組織在資訊安全方面努力的肯定，更是邁向永續發展的重要里程碑。未來，本基金將持續重視資訊安全，精進ISMS，確保個資的機密性、完整性與可用性，符合個資保護法規，提升營運韌性，並為未來升級預做準備。本基金深信，惟有透過持續的努力與投入，秉持ISO27001標準「規劃（Plan）－執行（Do）－查核（Check）－行動（Act）」持續精進本制度，強化資訊安全之防護與意識，增進資通安全與個人資料保護管理能力，才可確保系統在長期運作中保持高效、可靠並且符合使用需求，協助本基金持續營運。