圖片來源：Shutterstock

從 ISO 驗證到應變能力提升——資訊安全治理持續精進實務分享

文／潘嘉玟 任職於財團法人農業保險基金

壹、前言

數位轉型使資訊系統成為營運核心，資訊安全亦由技術議題升級為治理議題。隨環境複雜化，資安風險持續擴大，對組織營運與資料保護帶來更高要求。

依據世界經濟論壇（WEF）《Global Cybersecurity Outlook 2026》指出，當前資安威脅呈現高度動態與跨領域特性，包

含AI濫用、供應鏈攻擊及地緣政治風險，導致資安事件頻率與影響持續擴大，並進一步衝擊組織營運與信任基礎。同時，攻擊手法亦由技術漏洞轉向結合AI與社交工程之複合型態，透過釣魚郵件與身分冒用等方式繞過防護，使資安風險由「系統弱點」延伸至「人與流程弱點」，顯示單一技術防護已難以有效因應。

在上述背景下，國際逐步強調「資安韌性」（Cyber Resilience）概念。相較於以防禦為主之資安策略，資安韌性更著重於事件發生時之即時應變、影響控制與營運復原能力。然而，實務上若僅透過制度文件或標準導入，雖可建立管理架構，卻未必能確保應變有效性，甚至可能因流程不明確或決策不一致而影響處置效率。

財團法人農業保險基金（下稱農險基金）因辦理農業保險業務，掌握大量投保與理賠相關機敏資料，並仰賴關鍵資訊系統運作，一旦發生資安事件，除影響系統可用性外，亦可能衝擊被保險人權益與制度公信力。因此，農險基金在既有資訊安全制度基礎上，進一步導入國際框架並落實，將其轉化為可實際執行之應變機制，推動資安治理由「制度導向」邁向「制度與實務整合」，強化整體資安韌性。

貳、資安治理背景

農險基金主要辦理農業保險相關業務，涵蓋投保、理賠及行政管理等作業，並透過資訊系統支援各項業務運作。隨著資訊應用範圍持續擴展與系統整合程度提升，資訊安全已成為支撐業務穩定運作之關鍵基礎，並逐步由技術管理議題提升為整體治理層面之重要構成。

依現行資通安全責任等級分級制度，農險基金屬C級非特定公務機關。惟經整體業務特性與資安風險評估，面對日益複雜之資安環境，應以更高標準自我要求，主動強化資訊安全防護與治理能力。爰此，採取「提升治理標準」之策略，以B級非特定公務機關之資安要求為發展方向，持續強化制度與管理機制，展現對資訊安全治理之高度重視與前瞻規劃。

在實務推動上，農險基金透過導入國際標準、建立制度化管理機制及強化內部控制流程，逐步提升整體資安治理成熟度，使資訊安全由被動合規轉為主動治理，並作為後續制度深化與資安韌性建構基礎。

參、國際標準導入與治理基礎建構

依現行資通安全相關規範，資通安全管理制度係以ISO 27001資訊安全管理系統（Information Security Management

System, ISMS）為核心依據。農險基金在此架構下，透過制度化方式建構完整之資訊安全管理機制，並結合風險評估、內部稽核及持續改善（PDCA）循環，逐步強化組織整體管理架構與治理效能，並提升制度運作之穩定性與可持續性。

在ISMS制度建置之基礎上，考量業務涉及大量個人資料之蒐集、處理與利用，為進一步完善資料治理架構，另導入ISO 27701隱私資訊管理系統（Privacy Information Management System, PIMS），將個人資料保護機制整合至既有資安治理體系之中。透過角色權責界定、資料生命周期管理、隱私風險評估及相關控制措施之建立，使資訊安全與隱私保護由原本相對獨立之管理面向，轉化為彼此相互支援且整合運作之治理模式，全面提升資料保護之完整性與一致性。

農險基金於制度推動過程中，秉持「風險導向治理」原則，避免僅停留於文件合規之形式要求，而著重於制度與實務之有效連結。透過導入外部資安顧問專業量能，協助進行制度設計優化、差異分析及稽核準備，確保各項控制措施不僅符合國際標準要求，亦能實際落實於日常營運流程中。同時，藉由建立明確之作業流程、紀錄機制及追蹤控管程序，使各項控制措施之執行情形可被記錄、追蹤並進行稽核。

此外，透過ISMS與PIMS之整合推動，逐步建立以「資訊安全為基礎、隱私保護為延伸」之整體治理架構，不僅提升組織對資安風險與隱私風險之辨識與應變能力，亦強化跨部門協作與責任分工，使資安治理由單一部門職責，轉型為全組織共同參與之管理機制，進而奠定長期穩定運作之治理基礎。

肆、資安治理驗證與持續精進機制之實務推動

農險基金為確保管理機制之嚴謹度並預先識別潛在缺口，於民國113年2月邀請英國標準協會（British Standards Institution, BSI）協助辦理「預先審查」作業。預審結果顯示制度架構完整且執行狀況良好，為後續正式驗證奠定了堅實基礎。

BSI為具國際公信力之驗證機構，長期參與跨國組織驗證與稽核作業，實務經驗豐富，其稽核過程著重於制度落實程度與實際運作情形，能有效檢視管理機制於實務面之執行情形。透過驗證作業取得相關證書，不僅確認制度符合國際標準要求，亦提升整體資安治理之可信度與外部信賴性。憑藉預審階段的良好基礎，農險基金隨即於113年3月進行ISO

bsi.

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2022

This is to certify that: Taiwan Agricultural Insurance Fund
1F, 2F, 4F, No. 70-1, Sec. 1, Jinshan S. Rd.
Zhongzheng Dist.
Taipei City
100022
Taiwan

Holds Certificate No: **IS 803481**

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2022 for the following scope:

The provision of development, operation and maintenance of Agricultural Insurance Fund Global Information web site, Agricultural Insurance Training Learning web site, Pig and Livestock Insurance System, Agricultural Industry Insurance Underwriting System, Reinsurance and Accounting Management System, management of networking, server room activities, and related supporting information processing activities.
This is in accordance with the Statement of Applicability, ISMS-004-A34, version 2.1 dated 20 March 2024.

For and on behalf of BSI:

Michael Lam - Managing Director Assurance, APAC

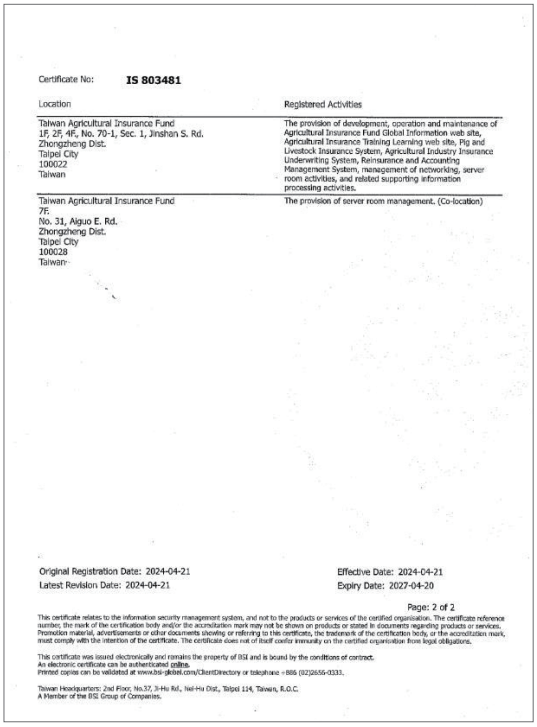
Original Registration Date: 2024-04-21
Latest Revision Date: 2024-04-21
Effective Date: 2024-04-21
Expiry Date: 2027-04-20

Page: 1 of 2

...making excellence a habit.

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsi-global.com/ClientDirectory or telephone +886 (02)2656-0333.

Taiwan Headquarters: 2nd Floor, No.37, Ji-Hu Rd., Nei-Hu Dist., Taipei 114, Taiwan, R.O.C.
A Member of the BSI Group of Companies.



Certificate No: **IS 803481**

Location	Registered Activities
Taiwan Agricultural Insurance Fund 1F, 2F, 4F, No. 70-1, Sec. 1, Jinshan S. Rd. Zhongzheng Dist. Taipei City 100022 Taiwan	The provision of development, operation and maintenance of Agricultural Insurance Fund Global Information web site, Agricultural Insurance Training Learning web site, Pig and Livestock Insurance System, Agricultural Industry Insurance Underwriting System, Reinsurance and Accounting Management System, management of networking, server room activities, and related supporting information processing activities.
Taiwan Agricultural Insurance Fund 7F, No. 31, Aiguo E. Rd. Zhongzheng Dist. Taipei City 100028 Taiwan	The provision of server room management. (Co-location)

Original Registration Date: 2024-04-21
Latest Revision Date: 2024-04-21
Effective Date: 2024-04-21
Expiry Date: 2027-04-20

Page: 2 of 2

This certificate relates to the information security management system, and not to the products or services of the certified organisation. The certificate reference number, the mark of the certification body and/or the accreditation mark may not be shown on products or stated in documents regarding products or services. Promotion material, advertisements or other documents showing or referring to this certificate, the trademark of the certification body, or the accreditation mark, must comply with the intention of the certificate. The certificate does not of itself confer immunity on the certified organisation from legal obligations.

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsi-global.com/ClientDirectory or telephone +886 (02)2656-0333.

Taiwan Headquarters: 2nd Floor, No.37, Ji-Hu Rd., Nei-Hu Dist., Taipei 114, Taiwan, R.O.C.
A Member of the BSI Group of Companies.

通過ISO27001:2022資訊安全管理系統驗證證書。圖片來源：財團法人農業保險基金

27001:2022驗證稽核，經由嚴格審查，順利取得國際證書，確認管理體系符合國際標準要求，亦顯著提升整體資安治理之外部信賴度。

取得驗證僅是治理精進的起點。為確保制度不隨時間鬆懈，並維持運作穩定性與有效性，115年度ISO覆審作業已於2月順利完竣，並於3月正式接獲BSI通知通過審查，顯示既有制度在文件建置、流程執行及紀錄留存等面向均已具備一定成熟度。

透過「預先審查、正式審查、年度覆審」的完整循環，農險基金持續縮減制度與實務間落差。此種藉由外部專家監督及內部持續優化機制，已落實資安治理的核心動能，並成為後續應變能力提升與資安韌性發展的關鍵支撐。

伍、制度落實之挑戰與資安韌性導向之治理轉型

農險基金雖已通過第三方驗證，並確認制度文件與實務運作具一定程度之結合，惟於實際資安事件發生時，仍可能因時間壓力、人員判斷差異及經驗落差等因素，影響應變處理之即時性與一致性，現行資安管理機制仍須持續精進制度落實至實際應變能力之落差，過度依賴個別人員

經驗，對組織長期發展並非理想，因此有必要進一步強化資安韌性，透過實際情境演練與應變機制驗證，提升整體應對能力，使資安管理由制度建構轉化為穩定且可複製之運作機制（如圖1）。

一、NIST框架為基礎之應變方法論與實務轉化機制

為將資安韌性概念具體落實於實務運作，農險基金參考「NIST SP 800-61」事件應變框架（如圖2），建立系統化應變流程，作為內部資安事件處理與演練基礎。該框架以事件生命周期為核心，涵蓋準備、偵測與分析、控制與清除、復原及事後改善等階段，強調資安事件應變應納入持續循環治理機制，而非單次處置行為。

在事件應變框架轉化上，並未直接套用框架內容，而係依實務需求進行調整，將抽象之控制原則轉換為具體決策節點與操作行為，並進一步整合為可執行之

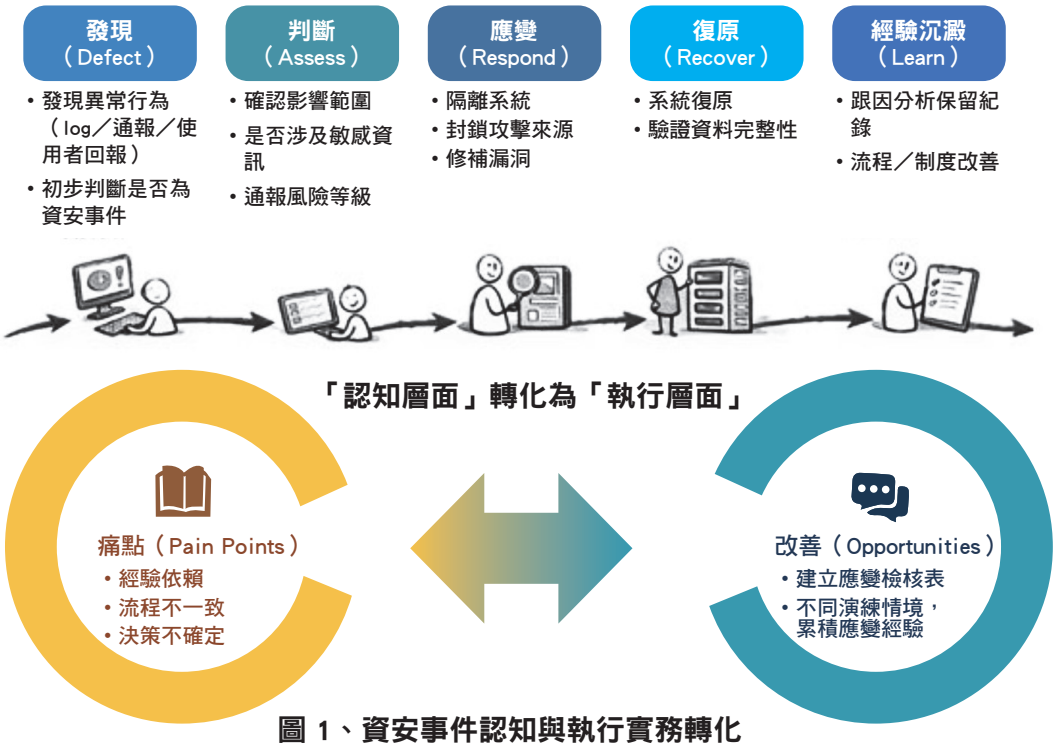


圖 1、資安事件認知與執行實務轉化

資料來源：本文整理

應變流程。此一轉換機制，使框架由指導原則轉化為可分工、可判斷且可追蹤之治理模型。

以實務為例，非特定公務機關須遵循《資通安全事件通報應變及演練辦法》及內部通報等相關規定，於資安事件發生時進行通報與應變處置。相關法規多著重於原則性要求，對實際操作流程細節規範相對有限，故於制度設計過程中，進一步將法規要求納入應變流程，具體化通報時點判斷、責任分工及處置步驟，使人員於事件發生時能依循既定邏輯進行判斷與執行。

在實務推動上，進一步將相關流程整合為資安事件應變檢核清單表（如表1），明確定義各階段應執行事項、責任分工及關鍵決策節點，使應變流程具備一致性與可操作性，並降低對個人經驗依賴。透過整合國際框架、法規要求與操作工具，使資安應變從「認知層面」轉化為「執行層面」，並由制度要求落實為可實際運作之

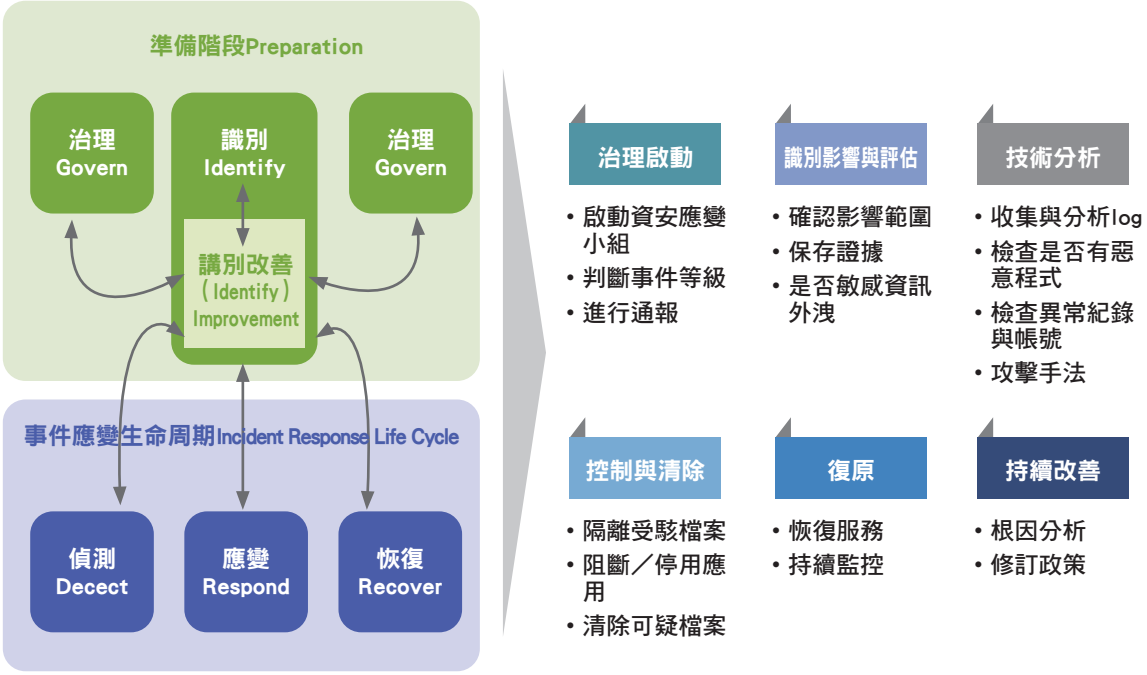


圖 2、NIST SP 800-61 事件應變周期模型架構之衍生應變流程

資料來源：整理自NIST SP 800-61

機制，使人員於資安事件發生時能依循既定流程快速判斷與處置，提升應變效率與一致性，進而強化整體資安韌性。

二、情境驗證與實務應用：以攻擊事件為例

為驗證前述資安治理機制實際運作情形，已透過模擬常見網頁攻擊情境進行演練，檢視從事件偵測、通報、應變處置至系統復原整體處理流程。演練過程中，依循既定應變機制與相關作業指引，分階段執行事件辨識、影響範圍評估、系統隔離、漏洞修補及後續監控等作業，使各階段處理具備明確依循，並強化跨單位間之協作與決策效率。

情境演練並非僅止於桌面演，而係透過模擬真實攻擊情境，由具備攻擊能力人員實際進行測試，使整體應變過程涵蓋事

表 1、資安事件應變檢核清單表設計示意（節錄）

處理階段 （資安事件發生時，可能會同時處理不同階段）	工作項目 （應實際發生期況，適用項目請打勾，不適用請刪除，避免於執行確認時混亂）	預計完成日	是否完成	各項負責人	廠商人員	備註
治理啟動 （Governance）	☐ 啟動資安事件應變程序					
	☐ 指派資安事件指揮官					
	☐ 建立事件編號					
	☐ 記錄發現來源（SOC／民眾通報／掃描工具）					
	☐ 判定事件等級					
	☐ 判定是否涉及資料外洩					
	☐ 判定是否涉及重要資訊系統					
	☐ 判定是否需外部法定通報					
	☐ 判定是否需通報主管機關					
	☐ 通知資安廠商（如需）					
	☐ 其他（請自行增加）					

資料來源：本文整理

圖片來源：Shutterstock

件偵測、調查分析、處置應變及系統復原等實際作業流程。透過此類方式，可具體檢視制度設計與實務運作之差異，例如在事件初期判斷、資訊傳遞及決策機制上，是否能迅速形成共識並採取適當行動，亦可檢驗既有控制措施於實際攻擊情境下有效性。相較於僅透過文件或稽核方式檢視，此類方式已由情境演練提升為接近實戰之應變能力驗證，能更真實呈現組織面對資安事件時之反應能力與處置成熟度。

在實務運作上，已將應變流程彙整為檢核清單表作為輔助工具，雖現行內容尚未涵蓋所有可能情境，惟可透過逐次演練與事件處理過程，記錄各階段應變做法與決策依據，使相關經驗得以累積與傳承。此一機制有助於降低對個別人員經驗之依賴，使後續人員能依循既有紀錄進行判斷與應對，逐步建立組織層級之應變能力。

三、持續精進與能力深化

未來將持續透過不同情境演練與實務案例累積，逐步擴充檢核清單表涵蓋範圍與內容，使其更貼近實際需求，並強化應變流程之完整性與適用性，進一步提升整體資安韌性。

陸、結語

綜上農險基金資安治理已由單一防護機制，逐步轉向整體應對能力。面對持續變化資安風險環境，需建立具備明確判斷依據與標準化流程運作機制，使不同人員於各類情境下能做出適當之應變處置，並維持整體運作穩定。

未來將持續強化應對能力與決策機制，並透過經驗累積與機制優化，使相關作業得以穩定運作並持續精進。

參考文獻

Alexander Nelson, Sanjay Rekhi, Murugiah Souppaya, Karen Scarfone(2025)。Incident Response Recommendations and Considerations for Cybersecurity Risk Management,https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

WEF(2026)。Global Cybersecurity Outlook 2026,https://www.weforum.org/publications/global-cybersecurity-outlook-2026/in-full/