資通安全

Topical Requirement

特定議題要求

The Institute of
Internal Auditors

資通安全特定議題要求

「國際專業實務架構」（International Professional Practices Framework®, IPPF）包含「全球內部稽核準則」（Global Internal Audit Standards™）、「特定議題要求」（Topical Requirements）及「全球指引」（Global Guidance）。「特定議題要求」屬於強制性規範，須與「全球內部稽核準則」搭配使用，以提供內部稽核實務所需的權威性基礎。

「特定議題要求」透過為特定風險議題設定最低基準，為內部稽核人員提供明確的期望。組織的風險狀況可能需要內部稽核人員進一步考量該議題的其他面向。

遵循「特定議題要求」將能使內部稽核服務的執行更趨一致，並增進內部稽核服務與成果的品質和信賴度。 最終，「特定議題要求」將能提升內部稽核專業的地位。

內部稽核人員在應用「特定議題要求」時，必須符合「全球內部稽核準則」的規範。 對於確信服務（assurance services）而言，遵循「特定議題要求」屬於強制性；對於諮詢服務（advisory services）而言，則建議採用。

當議題符合以下條件之一時，即適用「特定議題要求」：

A. 該議題為內部稽核計畫中的查核專案。
B. 在執行查核專案時發現該議題。
C. 該議題為內部稽核計畫外之查核專案需求。

內部稽核人員須記錄並保存每項「特定議題要求」適用性的評估證據。並非所有個別要求都適用於每個稽核專案；若有不適用的情形，則必須記錄並保留合理性說明。遵循「特定議題要求」是強制性規範，在品質評估時將進行審查。

若想了解更多資訊，請參閱《資通安全特定議題要求使用者指南》。

資通安全

美國國家標準暨技術研究院（NIST）將資通安全簡要地定義為：「在網路空間中，抵禦資安攻擊的能力。」資通安全是範疇更廣的資訊安全之子集合，而NIST 對於資訊安全的定義為：

「為了確保機密性 、完整性及可用性，對資訊及資訊系統進行保護，使其免於未經授權的存取、使用、洩漏、中斷、竄改或損毀。」

資通安全藉由強化整體控制環境，並保護組織的資訊資產免於未經授權的存取、中斷、竄改或損毀，進而降低風險。 資安攻擊可能會導致直接和間接的影響，且其影響通常相當重大，因為電腦、網路、程式、資料和敏感資訊是大多數組織至關重要的組成要素。

評估與評量資通安全治理、風險管理與控制流程

本「特定議題要求」提供了一致且全面的方法來評估資通安全治理、風險管理與控制流程的設計和實施狀況。 這些要求代表了組織在評量資通安全時的最低標準。

治理：評估與評量資通安全治理

要求：

內部稽核人員在評估組織的資通安全治理時，必須考量以下事項：

A. 制定正式的資通安全策略與目標並定期更新。定期溝通並由董事會審查資安目標達成情況，包括支持資安策略所需的資源與預算考量。

B. 制定與資通安全相關的政策與程序，並定期更新及強化控制環境。

C. 建立支持實現資安目標達成的角色和職責，並建立機制定期評估擔任這些職務人員的知識、技能與能力。

D. 相關利害關係人應參與討論現有弱點與新興資安威脅，並採取因應行動。利害關係人包括高階管理階層、營運部門、風險管理部門、人力資源部門、法務部門、法遵部門、供應商及其他相關單位。

風險管理：評估與評量資通安全風險管理

要求：

內部稽核人員在評估組織的資通安全風險管理時，必須考量以下事項：

A. 組織的風險評估與風險管理流程涵蓋了資安威脅的辨識、分析、減緩和監控，以及這些威脅對策略目標達成所造成的影響。

B. 資安風險管理應在全組織範圍內實施，可能涵蓋資訊科技、企業風險管理、人力資源、法務、法遵、營運、供應鏈、會計、財務等部門。

C. 資安風險管理的當責性與責任歸屬。 已指派專責人員或團隊，定期監督與報告資安風險的管理狀況，內容包括減輕風險所需的資源，以及識別新興的資安威脅。

D. 依據組織既定的風險管理準則或適用的法律與監管要求建立相關流程，對於任何不可接受水準的資安風險（不論是新興或先前已辨識）進行迅速升級處理。 並應將資安風險的財務與非財務影響納入考量。

E. 建立向管理階層與員工宣導資安風險意識的流程，並確保管理階層定期審查缺失、落差、缺陷或控制失效之處，並及時進行報告與改善。

F. 組織已實施資安事件應變與復原流程，內容應涵蓋偵測、控制、復原及事後分析，並應定期測試事件應變與復原程序。

控制：評估與評量資通安全控制流程

要求：

內部稽核人員在評估組織的資通安全控制流程時，必須考量以下事項：

A. 建立相關流程，以確保內部控制與供應商控制皆已就緒，進而保護組織系統與資料的機密性、完整性與可用性。 應定期執行評估，以判斷相關控制的運作是否能促進組織資通安全目標的達成並及時解決問題。

B. 人才管理機制，內容應包括培訓，以發展和維持與資通安全營運相關的技術職能。 並應定期審查此機制。

C. 建立持續監控及回報機制以辨識新興資通安全威脅及弱點，並辨識及優先改善資通安全營運的機會。

D. 將資通安全納入所有資訊科技資產的生命週期管理（選擇、使用、維護與汰除），包括硬體、軟體與供應商服務。

E. 建立強化資通安全的流程，包括組態設定、終端使用者裝置管理、加密、修補程式管理、使用者存取管理，以及監控可用性與效能。 並應將資安考量納入軟體開發 （Dev SecOps）。

F. 建立與網路相關的控制措施，如網路存取控制與網路區隔、防火牆使用與部署、限制與外部網路的連線、虛擬私人網路（VPN）、零信任網路存取（ZTNA）、物聯網（IoT）網路控制，及入侵偵測與防禦系統（IDS/IPS）。

G. 對於端點通訊安全建立控制，包括電子郵件、網路瀏覽器、視訊會議、訊息傳遞、社群媒體、雲端與檔案分享等服務協定。

關於國際內部稽核協會

國際內部稽核協會（The IIA）是國際性專業協會，為全球超過255,000名會員提供服務，並在全球頒發超過200,000位國際內部稽核師（CIA®）證書。國際內部稽核協會成立於1941年，是全球公認在內部稽核領域專業標準、認證、訓練、研究和技術指導面向的領導者。

如需了解更多訊息，請連結網址：www.theiia.org.

版權

2025年2月

The Institute of Internal Auditors

全球總部
1035 Greenwood Blvd., Suite 401 Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101