資通安全

Topical Requirement

特定議題要求 使用者指南

內容

特定議題要求總覽 **1**

適用性、風險與專業判斷 1

考量事項 4

附錄 A 實際應用範例 **8**

附錄 B. 與架構的對應 **9**

附錄 C. 可選的文件化工具 **13**

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

特定議題要求總覽

「特定議題要求」（Topical Requirements）是「國際專業實務架構」（International Professional Practices Framework®）不可或缺的組成部分，與「全球內部稽核準則」（Global Internal Audit Standards™）及「全球指引」（Global Guidance）同等重要。國際內部稽核協會（The Institute of Internal Auditors，IIA）規定，「特定議題要求」必須與「全球內部稽核準則」一併使用，「全球內部稽核準則」為必要實務提供權威基礎。本指南中隨處可見準則的引用，以提供更詳盡的資訊來源。

「特定議題要求」將內部稽核人員應如何因應普遍存在的風險領域予以正式化，以提升稽核業內的品質與一致性。「特定議題要求」建立了一條基準線，並為執行與「特定議題要求」主題相關的確信服務提供相關的評估標準（準則 13.4 評估判斷標準）。對於確信服務而言，遵循「特定議題要求」屬於強制性；對於諮詢服務而言，則建議於評估期間採用。「特定議題要求」並非僅在涵蓋執行確信專案時應考量的所有面向，而是在提供一套最低要求，使能針對特定主題進行一致且可靠的評估。

「特定議題要求」與國際內部稽核協會的「三道模型」（Three Lines Model）及「全球內部稽核準則」環環相扣。治理、風險管理與控制流程是「特定議題要求」的主要組成部分，與準則 9.1 了解治理、風險管理與控制程序相互呼應。參照「三道模型」而言，治理連結至董事會或治理機構，風險管理連結至第二道，而控制或控制程序則連結至第一道。雖然管理階層在第一道與第二道皆有代表，但在第三道中則將內部稽核職能描述為獨立且客觀的確信服務提供者，向董事會或治理機構負責（原則 8 由董事會監督）。

適用性、風險與專業判斷

當內部稽核部門對存在「特定議題要求」的主題執行確信專案時，或在其他確信專案中發現有「特定議題要求」的相關範圍情況下，則必須依「特定議題要求」執行。

如同準則所述，評估風險是內部稽核主管規劃的重要部分。為了確定將哪些確信專案納入內部稽核計畫，至少每年需要評估組織的策略、目標與風險（準則 9.4 內部稽核計畫）。在規劃個別確信專案時，內部稽核人員必須評估與專案相關的風險（準則 13.2 專案風險評估）。

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

當在以風險為導向的內部稽核規劃流程中，辨識出「特定議題要求」的主題，並將其納入稽核計畫時，便必須採用「特定議題要求」中所列出的要求，在適用的專案中評估該主題。 此外，當內部稽核人員執行專案（無論是否已納入計畫）且出現「特定議題要求」的要項時，即必須將「特定議題要求」的適用性評估納入專案範圍。 最後，若委託執行原先未編列於計畫中，但涵蓋「特定議題要求」主題的專案時，則必須評估「特定議題要求」的適用性。

專業判斷在「特定議題要求」的應用上扮演著關鍵角色。風險評估驅動內部稽核主管決定將哪些專案納入內部稽核計畫（準則 9.4 內部稽核計畫）。此外，內部稽核人員運用專業判斷，以決定各專案中將涵蓋哪些範圍（準則 13.3 專案目標和範圍、13.4 評估判斷標準、及 13.6 工作程式）。 附錄 A「實務應用範例」說明了內部稽核人員如何判斷「特定議題要求」是否適用。

針對「特定議題要求」中的每一項要求，皆必須保存已評估其適用性的佐證資料，內容包含排除任何要求的理由。 遵循「特定議題要求」的符合性，必須按照準則 14.6 專案文件中描述的稽核人員專業判斷，提供文件進行佐證。

雖然《資通安全特定議題要求》提供了可考量的控制流程基準，但將資安風險評估為極高的組織，或許將需要再進一步評估其他面向。

若內部稽核主管判斷，內部稽核部門不具備針對「特定議題要求」主題執行稽核專案的必要知識，則可將專案工作委外（準則 3.1 專業能力、7.2 內部稽核主管專業資格、10.2 人力資源管理）。 即使如此，委外亦不能免除內部稽核部門遵循「特定議題要求」的責任。 內部稽核主管仍須負起確保符合性的最終責任。 此外，若內部稽核主管判斷內部稽核資源不足，則內部稽核主管必須將資源不足的影響，及如何解決資源短缺之作法告知董事會（準則 8.2 資源）。

效能、文件化和報告

在應用「特定議題要求」時，內部稽核人員也必須遵循準則，並依循領域五：執行內部稽核服務之規範執行工作。 領域五中的準則描述了專案規劃（原則 13 有效規劃專案）、專案執行（原則 14 執行專案工作），以及溝通專案成果（原則 15 溝通專案結果並監督行動方案）。

「特定議題要求」的涵蓋範圍，可以根據稽核人員的專業判斷，記錄於內部稽核計畫或專案工作底稿中。 一個或多個內部稽核專案可能滿足這些要求。 此外，並非所有要求都適用。 對於「特定議題要求」評估適用性的佐證資料必須予以保存，內容應包括任何排除的理由說明。

附錄 C 的「選用工具」可用作參考，並記錄內部稽核人員所執行之工作。

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

品質確信

準則規定，內部稽核主管必須制定、執行與維持一套品質確信與改進計畫，以涵蓋內部稽核部門的所有面向（準則 8.3 品質）。計畫成果必須傳達給董事會與高階管理階層。溝通內容必須包含內部稽核部門對準則的遵循程度，以及績效目標的達成情況。

「特定議題要求」的符合性，將在品質評估中進行衡量。為了準備品質審查，內部稽核人員可以使用附錄 C 中所提供的工具。

資通安全

資通安全是一個範疇廣泛的主題，與任何組織的大部分技術層面息息相關。 除了資訊科技外，資通安全通常也是業務流程的一環，因此內部稽核人員在規劃、界定範圍及執行確信專案時，必須評估資通安全相關的風險。

美國商務部的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。」 《資通安全特定議題要求》著重於組織為防範未經授權的使用者與惡意資安威脅，所建構的外部邊界。 資通安全是範疇更廣的資訊安全之子集合，國家標準暨技術研究院 （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。」

《資通安全特定議題要求》的要求包括：

- 治理 – 明確定義支持組織目標、政策與程序的資通安全目標與策略的基準。
- 風險管理 – 辨識、分析、管理與監控資安威脅的流程，包括及時升級資安風險的機制。
- 控制 – 管理階層建立且定期評估的控制流程，以減輕資安風險。

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

考量事項

內部稽核人員或可參考下列事項，來協助評估《資通安全特定議題要求》中的各項要求。 這些考量事項與要求相互參照，僅為說明性質，並非強制性。 內部稽核人員在決定評估內容時，應依賴本身的專業判斷。

治理考量事項

為了評估治理流程在資通安全目標上的應用情況，內部稽核人員可以審查下列項目：

A. 正式制定並文件化的資通安全策略計畫與目標，包括董事會定期（通常為每季）審閱資訊安全主管（例如：資訊安全長，CISO）所提報的資安最新狀況。 證據資料可能包括以下報告：
   - 監控策略目標的達成情況。
   - 支持資安目標與目的之預算需求。
   - 風險與內部控制的關注重點，包括改善進度。
   - 關鍵績效指標 （KPI）的衡量。
   - 聘僱、培訓和發展資安人員所需的人力資源。

B. 用於管理資通安全流程的政策、程序與其他相關文件，包括：
   - 至少每年審查和更新政策。新興資安風險可能有需要更頻繁地進行審查與更新。
   - 確定政策和程序是否足以支持資安營運的機制。
   - 廣泛採用框架（NIST、COBIT 等）以強化資安流程與內部控制。

C. 支持實現資安目標達成的角色和職責，包括確保資安職能向組織中具有充分能見度以獲得組織支持的層級報告架構。
   - 定期評估擔任資安人員之知識、技能和能力的機制。

D. 與相關利害關係人（例如：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、策略供應商等單位）進行互動的證據，包含溝通現有與新興資安風險及已知潛在弱點的情形。 溝通佐證資料可能包括會議記錄、報告或電子郵件等。

風險管理考量事項

為了評估風險管理流程在資安目標上的應用情況，內部稽核人員可以審查下列項目：

A. 組織如何評估與管理資安風險，包括如何處理威脅與弱點：

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

- 初步辨識與報告。
- 分析評估對組織目標達成的風險。
- 減輕風險，包括將風險降低至可接受水準的行動方案。
- 監控，包括持續報告直至威脅完全解除的計畫。

B. 組織如何定期從各職能部門（例如：資訊科技、企業風險管理、人力資源、法務、法遵、營運、會計與財務）取得有關資安風險管理的意見。 可透過跨職能資安團隊或資訊科技指導委員會來取得相關資訊。

C. 組織如何將資安風險管理的當責性與責任指派給個人或團隊。
   - 負責人員應定期（每季、每月或依需求）在整個組織內部溝通資安風險的最新狀況，溝通內容可以包括風險減輕策略所需的資源。

D. 資安風險的升級機制，包括如何評估、劃分及排定威脅或風險等級的優先順序。 審查可包括下列的項目：
   - 組織已定義的風險等級（例如：高、中、低），並針對每個風險等級提供詳細說明，和各風險類別的升級程序。
   - 目前已辨識出的資安風險清單及各風險事件的減輕狀態。
   - 適用的法律、法規與法遵要求。
   - 財務與非財務（例如：聲譽）風險影響。

E. 向管理階層與員工溝通資安風險的流程，包括：
   - 定期（至少每年一次）員工資安訓練，例如：未預警的模擬網路釣魚活動，以測試與追蹤組織的資安意識。
   - 現有資安問題補救的最新進度及預期完成日期。
   - 監控不符法遵的情形，包括向董事會與高階管理階層更新最新狀況。
   - 當組織的風險胃納與風險容忍度變更時，重新評估威脅。

F. 組織對於事件回應和復原所實施的流程，包括：
   - 隨著組織營運變化而定期審查與更新的文件化計畫。 該計畫應包括：
     - 事件如何偵測與報告。
     - 如何控制事件以防止進一步損害。
     - 組織將如何復原與回應以恢復營運。
     - 如何分析事件並學習如何預防未來再發生類似事件。

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

- 定期（至少每年一次）測試（紙上演練）並向高階管理階層與相關利害關係人報告結果。 測試結果可能將產生後續的行動方案。

控制流程考量事項

為評估控制流程在資安目標上的應用情況，內部稽核人員可以審查下列項目：

A. 管理階層為建構有效的資安內部控制環境所採取的方法，包括：
   - 根據組織風險評估流程，評估與實施必要的內部控制，以減輕高風險並保護敏感、關鍵、個人或機密資料。
   - 確定維護關鍵資安控制所需的資源。
   - 將供應商控制納入控制環境，包括在建立業務關係前及關係存續期間，審查供應商的服務組織控制（SOC）報告。
   - 定期測試資安控制的運作，確認能否有效減輕風險，並支持實現資安目標的達成。
   - 補救內部控制缺陷，或解決內部稽核部門與其他確信服務提供者（例如：滲透測試）評估結果的流程。

B. 組織為招募與培訓資安專業人員所建立的人才管理機制，包括組織如何尋求機會，以提升資安專業人員的職能，以提升組織對新興議題的認知。
   - 例如參加培訓、加入知識分享團體，以及持續進修專業教育（包括取得資安相關證照）。

C. 管理階層以日常營運為重點，持續識別、劃分優先順序、監控和報告新興資安威脅與弱點的流程。 審查可能包括建立評估與人工智慧等新興技術相關威脅和弱點的流程。

D. 管理階層為管理和保護資訊科技資產在整個生命週期（包括硬體、軟體與供應商服務的選擇、使用、維護與汰除）中所建立的流程與控制。 硬體包括伺服器、網路設備（例如：路由器或防火牆）、桌上型電腦、筆記型電腦、手機、平板電腦及週邊設備。 軟體包括作業系統（例如：Windows）、企業資源規劃軟體、應用程式、防毒軟體等。 硬體與軟體考量事項包括：
   - 組織採用加密、防毒軟體、行動裝置管理、密碼複雜度要求、虛擬私人網路（VPN）、零信任網路（ZTN）驗證，及定期更新韌體的情形。
   - 資產管理流程，確保公司配發的硬體在發放時已具備適當的安全組態，並在資產報廢時妥善處置。

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

- 資料庫相關控制，包括限制使用者與管理員存取權限、確保使用加密、資料庫備份和測試，及部署強大的網路安全控制。
- 在系統開發生命週期（SDLC）中，如何考量資安威脅或弱點。
- 開發、安全與營運（DevSecOps）團隊所採用的方法，確保軟體開發過程納入資安考量，以主動辨識弱點。

E. 用於強化資通安全的流程，包括：
- 為極小化資安風險所進行的安全設定組態。
- 行動裝置管理（包括電子郵件和應用程式的使用）配置為減輕資安風險，並在使用者裝置受到威脅時進行遠端管理。
- 使用加密來保護「靜態資料」（例如：儲存於硬碟上的資訊）或「傳輸中」資料（例如：加密電子郵件）。
- 利用最新的安全版本修補伺服器或軟體（例如：作業系統）。
- 使用者存取管理，例如使用多因子認證（MFA）及具備定期過期複雜密碼的唯一使用者 ID。
- 部署監控控制，以判斷可用性與資源利用率是否充足，進行審查與分析危及效能的潛在資安問題。
- 將資安整合至系統開發生命週期（SDLC）中，以使在軟體轉移至正式環境前，辨識與解決資安弱點。

F. 保護組織邊界的網路相關控制，包括組織如何運用：
- 網路區隔。
- 防火牆。
- 使用者存取控制。
- 內外部連線的限制。
- 對於物聯網的網路控制。
- 入侵偵測或防禦系統用於網路攻擊中的預防、偵測和復原。

G. 適用於端點通訊安全的控制措施，適用服務包括電子郵件、網路瀏覽器、視訊會議、訊息傳遞（Zoom、MS Teams 及其他）、社群媒體、雲端與檔案分享協定等。 控制措施可能包括限制特定檔案副檔名（例如：.exe 檔案）的使用，以及針對檔案分享採用多因子身份驗證。

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

附錄 A 實際應用範例

下列範例描述《資通安全特定議題要求》適用的情境：

範例 1：內部稽核計畫中將資通安全確定為內部稽核專案的一部份。

當內部稽核部門完成以風險為導向的規劃流程，並在內部稽核計畫中包含一項或多項與資通安全相關的專案時，在執行此類專案時，便強制適用《特定議題要求》。可以透過在內部稽核計畫中的一項或多項專案中納入相關要求，以達成符合性。

資通安全是一個廣泛的主題，並非《特定議題要求》中的每一項要求皆適用於每個專案。 當內部稽核人員運用專業判斷，並確定《資通安全特定議題要求》中的一項或多項要求不適用時，應將其排除於專案範圍之外時，內部稽核人員必須記錄並保存排除這些要求的理由。 例如，排除部分要求的理由可能是內部稽核部門以輪流方式執行各項資安專案，或是已確定該風險在專案中的重要性偏低。

範例 2：在非以資通安全為重點的稽核專案中，識別出資安風險。

內部稽核人員在評估與資通安全沒有直接相關的流程時，可能會識別出資安風險。 例如，內部稽核人員在執行非以資安為重點的專案中評估應付帳款流程，於規劃專案範圍時，並未將資安風險納入考量。 然而，在執行初步查核後，內部稽核人員確定應將此類風險納入範圍；例如，他們辨識出透過網路請購單提交的相關資安風險（準則 13.2 專案風險評估）。

一旦辨識出相關風險，內部稽核人員必須審查《資通安全特定議題要求》，並判定哪些要求適用。 在此範例中，他們或許可以排除資安治理流程或資安風險管理流程，但他們必須在專案工作底稿中記錄排除《資通安全特定議題要求》其他要求的理由，並保存該文件。

範例 3：請求執行原先未納入內部稽核計畫的資安專案。

董事會、管理階層或監管機構等利害關係人可能會要求內部稽核人員在原稽核計畫之外執行資安評估。 例如，當組織成為資安攻擊目標時，董事會可能會要求執行內部稽核專案以評估資安控制。 此時即適用《特定議題要求》，必須評估這些要求，並記錄任何排除的情況。

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

附錄 B. 框架對應

組織可能有目前已在運行的資安工作，使用來自 COBIT 或 NIST 等風險管理和治理框架。 內部稽核人員可能已根據這些框架制定了稽核計畫與測試程序。 內部稽核人員應將其預計執行的資安控制測試與《特定議題要求》進行對應，以確保充的涵蓋範圍。下表將《資安特定議題要求》對應到三種常用的框架：NIST 資安框架 2.0、COBIT 2019 及 NIST 800-53。由於這些框架皆可免費取得，故建立其對應關係。

治理要求	框架參考		
	NIST CSF 2.0	NIST 800-53	COBIT 2019
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。	GV.RM-01； GV.RM-02； GV.RM-03； GV.RM-04； GV.OC-02； GV.RR-03； GV.RR-04； GV.PO-01； GV.PO-02； GV.OV-01； GV.OV-03	PM-1、PM-4； AT-2； AT-3； PM-9； PM-28	EDM01; EDM03; EDM04; APO06; APO01; APO10; APO12
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。	GV.PO-01； GV.PO-02； GV.OV-01； GV.OV-02； GV.OV-03； GV.SC-01； GV.SC-03； GV.RR-03	AC-1、PM-9； AC-1； AT-1； CA-1； CM-1； IA-1； IR-1； MP-1； PE-1	EDM01; EDM02; EDM03; APO01; APO11
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。	GV.RR-02； GV.RR-04； GV.SC-02； GV.OC-02	PM-13； AT-2； AT-3	EDM02; APO01; APO07

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

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。	GV.OC-02； GV.RM-01； GV.RM-05； GV.RM-07； GV.OV-03； GV.SC-03	AC-1； CM-1	EDM05; EDM01.01; EDM03; MEA01.02; APO01; APO08; APO11; APO13; MEA02
風險管理要求	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
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。	GV.RM-01； GV.RM-03； GV.OC-01	AT-1； PM-9； PM-28	EDM03; APO01; APO10; APO12
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。	GV.RM-01； GV.RM-05； GV.RR-01； GV.RR-02； GV.OC-03； GV.SC-07	PM-29；AT-1；PM-9；PM-28	EDM03; APO01; APO10; APO12
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。	GV.RR-01； GV.RR-02； GV.RR-03； GV.0V-01； GV.OV-02； GV.OV-03	PM-9； PM-29	EDM03; APO01; APO10; APO12
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。	GV.RM； ID.RA； RS.MA-04	CA-7； RA-3； RA-7	EDM03; APO01, APO10; APO12

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

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。	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
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。	RS； RC	IR-4； IR-5； IR-6； IR-7； IR-8； IR-10； SA-15	DSS02; DSS03; DSS04; DSS05.07
控制過程要求	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
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。	ID.IM-01; ID.IM-02; ID.IM-03; PR; DE; RS; RC; ID.RA06; GV.RM-05; GV.SC; ID.IM-02; RS.MA-01; DE.CM-06	AC-3；AC-4；AC-10；AC-13；AC-17；PM-30； RA-3； SA-9； SR-2	MEA02; MEA04; EDM03; APO09; APO10; DSS01
B. 對於資安營運建立人才管理機制並定期審查，內容應包括培訓機會，以發展和維持技術職能。	PR.AT-01； PR.AT-02； GV.RR-03	AT-2； AT-3； IR-2； PM-14	APOO7; DSS04
C. 建立持續監控與**報告**新興資安威脅與**弱點的機制**，並**識別**、**劃分優先順序**及**落實**改善資安營運的機會。	ID.RA-02； ID.RA-03、ID.RA-04	CA-7； PM-31； RA-5	DSS03.05
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。	ID.AM; PR.PS-03; PR.IR; DE.CM-09; ID.AM-08; ID.RA-09; PR.PS-06	AU-9； CM-7； SC-49； SC-51； CM-2； SA-3； SA-10； SA-15； SA-17； SA-20； AU-6； IR-7	DSS05.03; BAI03; BAI09; BAI03; BAI11; DSS05.01; DSS02; DSS03; DSS06.06

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

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（DevSecOps）。	PR.PS-01； PR.PS-06； PR.DS-01； PR.DS-02； PR.PS-05； DE.CM-03	CM-6； SI-2； AC-3； CA-7； SA-4； AC-16 ； AC-18	BAI10; DSS05; DSS06.03; DSS01.03; MEA01
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）。	PR.IR; DE.CM-01	AC-6； AC-17； AC-18； AC-20； SC-7； SC-10； CA-8	DSS05.02
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。	PR.DS-01; PR.DS-02; PR.DS-10; PR.IR	AC-2； AC-16； AU- 10 ； CA-3； SI-8； SI-20； SC-8	BAI10

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

附錄 C.選用工具

內部稽核人員應運用專業判斷，根據風險評估結果，判斷各項要求的適用性，並適當對於某些要求的排除妥善記錄。《特定議題要求》的文件化作業，可記錄於內部稽核計畫或專案工作底稿中，這端視稽核人員的專業判斷而定。 可由單一或多個內部稽核專案涵蓋這些要求。 此外，並非所有要求都適用。 下列提供可列印的表格式記錄《資安特定議題要求》遵循情況的一種方式，但並非是強制使用。

資通安全－治理

要求	執行範圍或排除理由	文件佐證
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。		

資通安全－風險管理

要求	執行範圍或排除理由	文件佐證
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。		

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

要求	執行範圍或排除理由	文件佐證
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。		

資通安全– 控制流程

要求	執行範圍或排除理由	文件佐證
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. 對於資安營運建立人才管理機制並定期審查，內容應包括培訓機會，以發展和維持技術職能。		
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。		

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

	要求	執行範圍或排除理由	文件佐證
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（DevSecOps）。		
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。		

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

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®）認書。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.

免責申明

本文件由 IIA（國際內部稽核協會）發布，僅供參考與教育用途。本資料並非針對特定個案提供最終解答，而僅作為指引使用。IIA 建議針對特定情境尋求獨立專家意見。IIA 對於任何人僅依賴本資料而採取行動所產生的後果概不負責。

版權

© 2025 國際內部稽核協會版權所有，如需複製許可，請聯繫copyright@theiia.org.

2025年2月

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101