第三方特定議題要求

Public Consultation Draft

《國際專業實務架構》(Professional Practices Framework®) 包含《全球內部稽核準則》(Global Internal Audit Standards™)、特定議題要求和全球指引。特定議題要求具有強制性，必須與《準則》一併使用，而《準則》為這些要求提供了權威來源基礎。

特定議題要求透過建立稽核特定風險領域的最低基準，為內部稽核人員提供明確的期待。組織的風險概況可能要求內部稽核人員考量此特定議題的其他面向。符合特定議題要求將提高內部稽核服務執行的一致性，並改善內部稽核服務和結果的品質和可靠性。最終，特定議題要求可提升內部稽核專業。

內部稽核人員必須依照《全球內部稽核準則》應用特定議題要求。提供確信服務時，應強制依循特定議題要求，而提供諮詢服務時，則建議依循特定議題要求。特定議題要求適用於下列任一情形之主題：

A. 內部稽核計畫中專案的主題。
B. 在專案進行中發現此主題。
C. 原內部稽核計畫以外所要求的專案主題。

評估每項特定議題要求中的要求是否適用，相關證據必須記錄與留存。並非所有個別要求都適用於每個專案；若排除某些要求，必須記錄並留存原因。符合特定議題要求為強制性，並將在品質評估時進行評估。

第三方

第三方是與組織有業務關係的外部個人、群體或實體。第三方關係可透過合約、協議或其他方式正式化，以為組織提供產品或服務。「第三方」一詞的使用可能因產業或其他情境而異。本指引使用「第三方」一詞代表廠商或供應方、承包商或分包商、委外服務提供者、其他代理人和顧問，並包含第三方與其分包商（通常稱為「下游」分包商）之間的協議。

本特定議題要求並未規範與主要組織存在間接關係、利益或參與其中的對象，如員工、財務合作夥伴、主管機關、代理人或受託人等。

雖然主要組織可藉由第三方協助達成一個或多個業務目標，但主要組織仍須對達成這些目標所伴隨的風險負最終責任。若第三方與組織的合約或協議允許其分包給第四方或更「下游」的一方，提供這些分包關係的治理和監督的確信服務時，本特定議題要求同樣適用。在這些情況下，內部稽核人員必須按照風險評估的結果應用所有要求，如有排除須加以記錄。

與第三方合作往往帶來風險，必須透過適當的治理、風險管理與控制程序加以辨識、評估並管理。若第三方無法履行契約、涉及不道德行為或遭逢營運中斷，主要組織恐因此蒙受損失。第三方風險的類別與範例如下：

- 營運風險，如服務中斷或未達成業務目標。
- 網路安全風險，如機敏資料外洩。
- 財務風險，如供應商無力償債。
- 遵循適用於本地、國家和國際監管要求。
- 法律風險，如利益衝突、糾紛和違約訴訟。
- 聲譽風險，如對環境或主要組織的客戶、消費者或利害關係人造成的損害。

第三方生命周期包含選商、簽約、導入、監督及終止合作等階段。內部稽核人員在評估治理、風險管理和控制程序的要求時，應考量上述各階段。

衡量與評估第三方之治理、風險管理與控制程序

本特定議題要求提供一致、全面的方法，用於評估第三方治理、風險管理和控制程序的設計和實行。這些要求即為組織進行上述評估的最低基準。

治理：衡量與評估第三方治理

要求:

內部稽核人員必須評估組織第三方治理（含董事會監督機制）的以下面向：

A. 建立一套用以決定是否與第三方簽約的正式方法，並確實執行、定期檢視。該第三方係以提供產品或服務協助組織達成業務目標。此方法包含合適的標準，用於定義和評估可用資源以達成目標。
B. 建立政策、程序和流程，以在第三方生命週期中定義、評估和管理與第三方的關係和風險。這些政策、程序和流程與適用的監管要求一致，並定期檢視和更新以強化控制環境。

C. 明確界定組織內的第三方管理角色和責任，詳述誰負責選擇、指導、管理、與第三方溝通和監督，以及應告知哪些人員第三方之最新狀況，並有機制確保被指派管理第三方角色和責任的人員具備必要的知識、技能與能力。
D. 與相關利害關係人定義溝通協議，包含報告優先第三方的績效、風險和法令遵循狀態。相關利害關係人可能包含董事會、高階管理層、營運部門、風險管理、人力資源、資訊安全、法務、法令遵循、採購和其他單位。

風險管理：衡量和評估第三方風險管理

要求:

內部稽核人員必須評估組織第三方風險管理的以下面向：

A. 第三方的風險管理流程是標準化且全面的，包含明確的角色和責任，並充分應對關鍵風險（如財務、營運、策略、網路安全、法令遵循、聲譽、道德、永續、地緣政治和法律風險）。監督流程遵循情況，並對任何偏離採取矯正措施。

B. 識別並評估第三方在整個生命周期所涉及的風險。風險評估用於分類和排序第三方，也用於決定風險回應措施的優先排序。定期檢視和更新相關評估。
C. 風險回應措施充分且準確，且與優先排序相應。風險回應措施經實施、檢視、核准、監督與衡量，並視需求調整。

D. 現有相應流程可管理並於必要時呈報第三方出現的問題，確保結果的責任歸屬明確，並提高滿足合約或其他協議條款的可能性。若第三方對於已呈報的問題無法提出適切回應，現有相應流程可進行補救，補救措施最嚴重可終止合約。

控制：衡量與評估第三方控制程序

要求:

內部稽核人員必須評估優先第三方的以下控制，包含管理階層持續評估和監督組織第三方的流程：

A. 有記錄且經核准的業務需求分析或其他相關文件，描述並證明與第三方建立關係的必要性與性質。
B. 已有嚴謹的盡職調查流程，用於尋源和選擇第三方。該流程包含如審閱網路安全協定、進行財務背景調查和驗證銀行帳戶資訊等重要面向。
C. 依據組織的第三方風險管理政策、程序和流程進行簽約與核准，並於過程中與相應部門合作。
D. 最終合約或協議由所有相關利害關係人（情況適用時可納入法務和法遵部門）審閱並核准，並由雙方授權人員簽署，且安全保存。所有合約均指派給合約經理或管理者負責。
E. 已維護一份準確、完整和及時更新的第三方列表，如於集中式合約管理系統中。

F. 已建立第三方導入的書面流程，並確實遵循以使第三方能夠履行合約或協議條款。

G. 已建置持續監控流程，以評估優先第三方是否在整個生命週期中按照合約或協議條款履行，並履行合約義務。流程包含驗證所提供資訊的可靠性，並定期以及在協議變更時重新評估績效。

H. 已建立相關協定，若第三方未能達到預期、導致風險提高或帶來意外風險時，啟動矯正措施。協定包含根據嚴重程度呈報事件、執行事件後審閱和分析事件根本原因。

I. 監督合約更新日期，並在必要時採取更新措施。

J. 對於優先第三方，實行並遵循正式的終止合作計畫。流程包含如何：

- 終止與第三方的關係。
- 必要時更換第三方。
- 移轉資料保管權，並要求第三方歸還或銷毀其儲存的組織機敏資料。
- 移除第三方對組織系統、工具和設施的存取權限

