國際內部稽核協會三道模型

THE IIA'S THREE LINES MODEL

三道防線模型的更新版

An update of the Three Lines of Defense

洪良明　翻譯／張信一　複核

The Institute of Internal Auditors | Global

內容目錄

簡介

機構是人類承擔工作，以因應當今日益隱晦未定、複雜、相互聯繫且詭異變化多端的現實世界。其間經常存在著多重複雜的利害關係人，彼此的利益各自糾結，甚至有時互相競爭。利害關係人將機構監督委任治理層，轉而讓他們將資源和權限委派給管理層，俾採取適當措施，包括管理風險。

當為了支持強大的治理和風險管理時，由於這些原因以及更多的理由，機構需要有效的結構和過程來達成目標。當治理層收到管理層報告有關機構營運活動、成果和預測時，治理層與管理層雙方對前述所有事項都需要依賴內部稽核，提供獨立、客觀的確認和建議，俾提升、激勵創新與精進改良。透過治理層、管理層和內部稽核的行動與行為達成治理，畢竟治理層最終要對公司治理負責的。

三道模型有助於機構對於目標完成及促成機構治理和風險管理，確認其本身何種結構和流程，是最好的。本模型適用於所有的機構，透過以下方式可以優化：

- 採用「原則基礎」的方法並調整模型，以適合機構目標和環境情況。
- 專注於風險管理，對目標達成與創造價值，及「防衛」事項和維護價值之貢獻。
- 清楚了解模型中呈現的角色和職責，以及彼此之間的關係。
- 採取的措施要確保活動和目標，是與利害關係人優先利益是一致。

關鍵字

機構—由一群為達成共同目標一起努力工作之人們透過一連串活動與資源所組成之集合體。

利害關係人—由機構提供服務，或影響其利益的那些團體與個人。

治理層—為機構成功向利害關係人負責之那些自然人。

管理層—對機構所指派，對客戶提供產品和（或）服務之那些個人、團隊和支援小組。

內部稽核—那些獨立於管理部門之個人，對治理和風險管理（含內部控制）之充分性與有效性，可以提供確認與見解。

三道模型—即是先前眾所周知的三道防線之模型。

內部控制—即在為達成目標完成提供合理確認之過程。

三道模型的原則

原則一：治理

機構治理應採取合適的結構和程序，以能夠達成：

- **當責性**由治理層對利害關係人負責，透過以誠信、領導和透明方式對機構進行監督。
- **行動**（含管理風險），透過風險基礎決策方式並運用機構資源，以達成機構目標之管理。
- **確認和建議**由獨立的內部稽核功能，透過嚴謹的詢問和具有洞察力的溝通所產生，以提供透明度和信心，及提升和促進持續改進。

關鍵字

風險基礎決策—經過深思熟慮的過程，包含分析、規劃、行動、監督和複核，並考量在目標下不確定性的潛在影響。

確認—獨立的確認和信心。

原則二：治理層之角色

治理層確保：

- 適當的結構與流程以進行有效之治理。
- 確保機構目標與活動，與利害關係人優先利益是一致的。

治理層：

- 委派責任與提供資源給管理層，以達成機構目標，確保符合法律、法規、和道德要求。
- 建置和監督一個獨立、客觀、稱職的內部稽核功能，以提供促進目標達成之透明度和信心。

原則三：管理層和第一道及第二道之角色

管理層為達成機構目標的職責，組成第一道與第二道之角色[1]。*第一道角色*大多直接與提供商品和服務，或服務給機構客戶有關，包含支援功能之角色[2]。*第二道角色*提供管理風險之協助。

第一道和第二道角色可能混合交融或獨立分開。有時候第二道角色可能指派專家提供額外的專業知識、支援、監控和挑戰第一道角色。第二道角色可以專注於風險管理的特定目標，諸如法律法規的遵循，以及可接受的道德行為；內部控制；資訊和技術安全；可持續性和品質確認。或者，第二道角色可能會承擔更廣泛的風險管理責任，例如企業風險管理 ERM。然而，管理風險責任，依然是第一道角色的一部分，而且屬於其管理範疇內。

原則四：第三道之角色

內部稽核對治理和風險管理的充分性與有效性，提供獨立和客觀的確認和建議[3]。它通過系統化、有紀律的流程、專業知識，和洞察力的有效應用來達成這個目標。它向管理層和治理層報告其所發現，以提升和促進持續改進。同時它可能會考量其他內部和外部提供者的確認。

原則五：第三道獨立性

內部稽核獨立於管理職責，對於其客觀性、權威性和信譽至關重要。它是透過以下方式建立的：對治理層的課責；基於完成其工作所需要，可以不受限訪談對象訪談機構任何人員、及接觸資源和數據；以及在規劃或提供稽核服務時不受偏見或阻擾。

註[1].為了閱讀熟悉起見，保留原先模型所用「第一道」、「第二道」、「第三道」的用語。「道」字眼，並非在表示組成元素，而是在角色上的使用有所區別。從邏輯上來講，治理層的角色也構成「一道」防線，但本模型並未採用，以避免混淆。編號第一道、第二道、第三道，不應該被視為暗示操作的順序，而是所有角色應該同步運作。

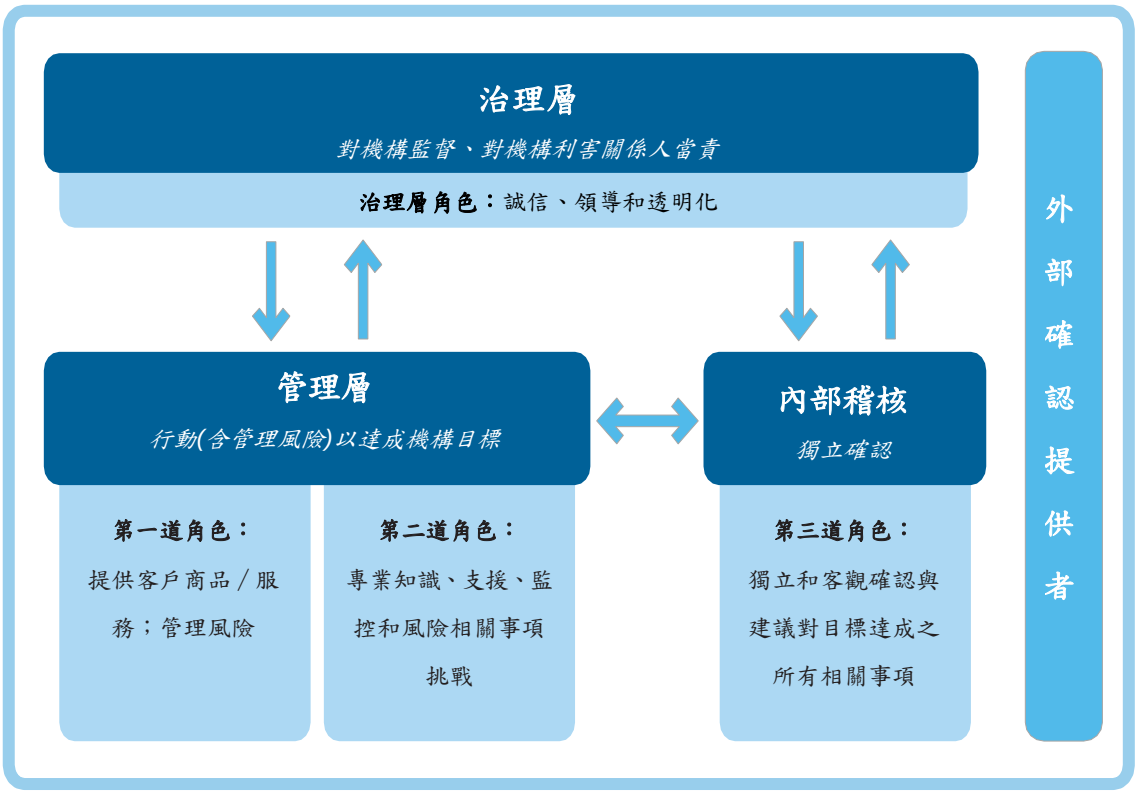
註[2].有些人將支援功能的角色，例如人力資源、行政和創建服務視為第二道角色。為清楚起見「三道模型」將*第一道角色*即包含「前台」活動及「後台後勤」支援活動。*第二道角色*包含那一些專注於風險相關事物的互補額外活動。

註[3].在某些機構中，還辨認出其他第三道角色，例如監督、檢查、調查、評估，和輔導補救，這些角色可能是內部稽核功能的一部分，或者獨立運作的。

原則六：創造與維護價值

當所有角色相互配合，並符合利害關係人的優先利益時，它們共同發揮各自應有的作用，有助於創造和維護價值。活動的協調是透過溝通、合作和協同達成的。這樣可以確保風險基礎決策所需要資訊的可靠性、連貫性和透明化。

國際內部稽核協會三道模型



三道模型主要角色

機構在職責**分配方面是有所差異**。然而，以高階層級角色來看「三道模型」之原則，是可以擴大的。

治理層

- 接受利害關係人對監督機構的課責。
- 與利害關係人進行透明地溝通，來監控他們的利益和機構目標的達成。
- 培育一種促進道德行為與當責的文化。
- 建立治理的結構和流程，包括必要的專案委員會。
- 委派責任和提供資源賦予管理層以達成機構目標。
- 決定機構對風險的胃納和對風險管理（包括內部控制）進行監督。
- 維持對法律、法規和道德要求遵循等監督。
- 建立和監督獨立、客觀和適當的內部稽核功能。

管理層

第一道角色

- 領導並指導行動（包括風險管理）和資源應用以達成機構的目標。
- 維持與治理層持續對話溝通並報告機構目標與風險之相關規劃，含預期與實際結果及其風險。
- 建立並維護適當的結構和流程，以管理營運和風險（包括內部控制）。
- 確保遵循法律、法規和道德要求。

第二道角色

- 提供與風險管理相關額外的專業知識、支援、監控和挑戰，包括：
    - 針對風險管理實務（包括內部控制），在程序、系統和實體級別上的開發、實施和持續改進。
    - 風險管理目標的達成，例如：遵循法律、法規和可接受的道德行為；內部控制；資訊和技術安全；可持續性和品質確認。
- 提供有關風險管理（包括內部控制）的充分性和有效性之分析和報告。

內部稽核

- 維持對治理層的主要課責，並獨立於管理層的職責。
- 就治理和風險管理（包括內部控制）的充分性和有效性向管理層和治理層傳達獨立和客觀的確認和建議，以支援機構目標之達成並提升和促進持續改進。
- 向治理層報告獨立性和客觀性的阻礙，並實施必要之保障措施。

外部確認提供者

- 提供以下方面的額外確認：
    - 滿足法律和法規的要求，可維護利害關係人的利益。
    - 滿足管理層和治理層對額外內部確認來源之要求。

核心角色間之關係

治理層與管理層間(第一道與第二道之角色)

治理層通常透過設定遠景、使命、價值觀和機構對風險的胃納，來確定機構**方向**。然後，將達成機構目標的責任與必要的資源下放給管理層。治理層從管理層收到有關規劃，含實際和預期結果之報告，也收到有關風險和風險管理的報告。

關鍵字

執行長（CEO）—**機構中負責營運的最高階人員。**

機構在治理層和管理層角色之間的重疊和分離程度方面各不相同。治理層可以在策略和營運事務上或多或少地「介入」。治理層或管理層可以帶頭制定策略計劃，也可以共同來承擔。在某些權限範圍，執行長（CEO）可能是治理層的成員，甚至可能是其主席。在任何情況下，管理層和治理層之間都需要進行強有力的溝通。執行長通常是這種溝通的焦點，但是其他高階管理階層人員可能會與治理層頻繁互動。機構可能希望，並且其主管機關可能會要求第二道職位的負責人（例如風控長（CRO）和法遵長（CCO））直接向治理層報告。這與三道模型的原理完全一致。

管理層(第一道與第二道之角色)與內部稽核間

內部稽核獨立於管理人員，可確保其在規劃和執行工作中不受任何阻礙和偏見，可以不受限制地自由訪談所需的人員，接觸資源和必要的訊息。它對治理層負責。但是，獨立並不意味著孤立。內部稽核和管理層之間必須定期進行互動，以確保內部稽核的工作是相關的，並與機構的策略和營運需求保持一致。透過內部稽核的所有活動，內部稽核會建立對機構的知識和了解，這作為有助於顯露其可為信賴的顧問和策略合作夥伴，及提供確認和建議。在內部稽核和管理層的第一道和第二道角色之間需要進行協同和交流，以確保沒有不必要的重複，重疊或空白。

內部稽核與治理層間

內部稽核對治理層負責，有時被形容為治理層的「耳目」。

治理層負責對內部稽核的監督，要求：確保建立獨立的內部稽核功能，包括聘用和解僱內部稽核主管（CAE）；作為 CAE 的主要報告渠道[4]；批准和分配稽核計畫；接收並考慮 CAE 的報告；並允許 CAE 自由地不受限制地訪問治理層，包括在沒有管理層參與的情況下，舉行秘密會議。

關鍵字

內部稽核主管（CAE）—**機構中負責內部稽核服務的最高階人員，通常稱為稽核長或類似頭銜。**

所有角色間

治理層、管理層和內部稽核有各自的職責，但是所有活動都必須與機構的目標保持一致。成功一致性的基礎是定期有效的協調、協同和溝通。

註 [4].出於管理目的，CAE 還可以向適當的高階管理階層人員報告。

結構、角色與責任

三道模型在機構目標和環境調適一致時，**是最有效的**。機構結構和角色分配是管理層和治理層所決定。治理層可以建立委員會，以對其特定職責（例如稽核、風險、財務、計畫和薪酬）提供額外的監督。在管理部門內部，隨著機構規模和複雜性的增長，可能會出現功能性和層級性安排，並趨向於專業化。

功能、團隊甚至個人都可能承擔第一道和第二道角色。但是，可以透過建立主要課責制度暨向治理層報告管道，來設計第二道角色的指導和監督，以確保與第一道角色，甚至與最高管理階層，維持一定程度的獨立性。「三道模型」允許在管理層和治理層之間建立所需的報告管道。在某些機構中，最著名的是受監管的金融機構，有一項法定要求，即此類安排必須確保足夠的獨立性。即使在這些情況下，具有第一道角色的管理人員仍然負責管理風險。

第二道角色可能包括監控、建議、指導、測試、分析和報告與風險管理相關的事項。只要這些功能是為具有第一道角色的人員提供支援和挑戰，並且是管理層決策和行動所不可或缺的，則第二道角色是管理層職責的一部分，永遠不完全獨立於管理層，而無論報告的管道和課責如何。

第三道角色的特徵是獨立於管理層。「三道模型」原則描述了內部稽核獨立性的重要性和本質，將內部稽核與其他管理職能區分開來，並賦予其確認和建議的獨特價值。內部稽核的獨立性可以透過不做出決策或採取管理職責（包括風險管理）中的一部分，並拒絕為內部稽核當前或最近承擔的活動提供確認。例如，在某些機構中，要求內部稽核主管對利用類似職能的活動承擔額外的決策責任，例如法規遵循或企業風險管理方面。在這種情況下，內部稽核並非獨立於這些活動或其結果，因此，當治理層尋求有關這些領域的獨立客觀的確認和建議時，有必要由合格的第三方來進行內部稽核。

監督與確認

治理層依靠管理層，包括擔任第一道和第二道角色的人員，與內部稽核及其他部門的報告，對達成機構目標進行監督，並向利害關係人負責。管理層可以利用直接的經驗和專業知識，對計畫、實際和預測的結果、風險及風險管理提供有價值的確認（也稱為簽證）。具有第二道角色的人員在風險相關事宜上提供了額外的確認。由於內部稽核獨立於管理層，因此所提供的確認具有最高的客觀性和信心，勝過第一道、第二道角色人員向治理層提供的確認，而與報告管道無關。也可以從外部提供者那裡獲得進一步的確認。

協調與一致

有效的治理要求適當地分配職責，並透過合作、協同和溝通來使活動緊密結合。治理層透過內部稽核尋求確認，以確認治理結構和流程已經過適當設計和營運符合所預期。