論著與分析

新常態下之內稽視野—新三線角色模型與區塊鏈內部控制

周靜幸

摘要

內部稽核人員面臨新常態來臨，除仍應持續強化風險導向稽核方法之運用外，更應及時擴展內部稽核視野，掌握並導入風險管理與內部控制之實務變革與國際新知，協助組織管理階層及治理單位有效達成組織目標，發揮稽核之監督、洞察或前瞻價值。

壹、前言

COVID-19 大流行迫使組織專注於危機管理、業務持續性、及如何最有效利用最新科技來適應快速變遷業務與社會之情況。事實上，在不到六個月的時間內，這個流行病使世界開始期待、反應及接受變革—通常是根本性的變革—成為新的常態。2020-2021 年新任國際內部稽核協會（IIA）理事長 Jenitha John 女士指出：二十多年來，許多組織都採用 IIA 在 2013 年發布之有效風險管理與內部控制三道防線模型，以簡單三道個別防線描述風險管理及控制責任，然隨著新舊風險的多變與起效速度愈來愈快，及組織日益複雜化，IIA 已於 2020 年 7 月發布「新三線角色模型（Three Lines Model）（以下簡稱新三線模型）」，協助機構必須決定其自身適當的、實用結構，並在不斷演變的風險局勢下考量其目標及情況。另在數位化浪潮下，區塊鏈變革並非個別存在，而是整合某些其他新興技術，才能提高其成功。這些新興技術—諸如人工智慧（Artificial intelligence, AI）、物聯網

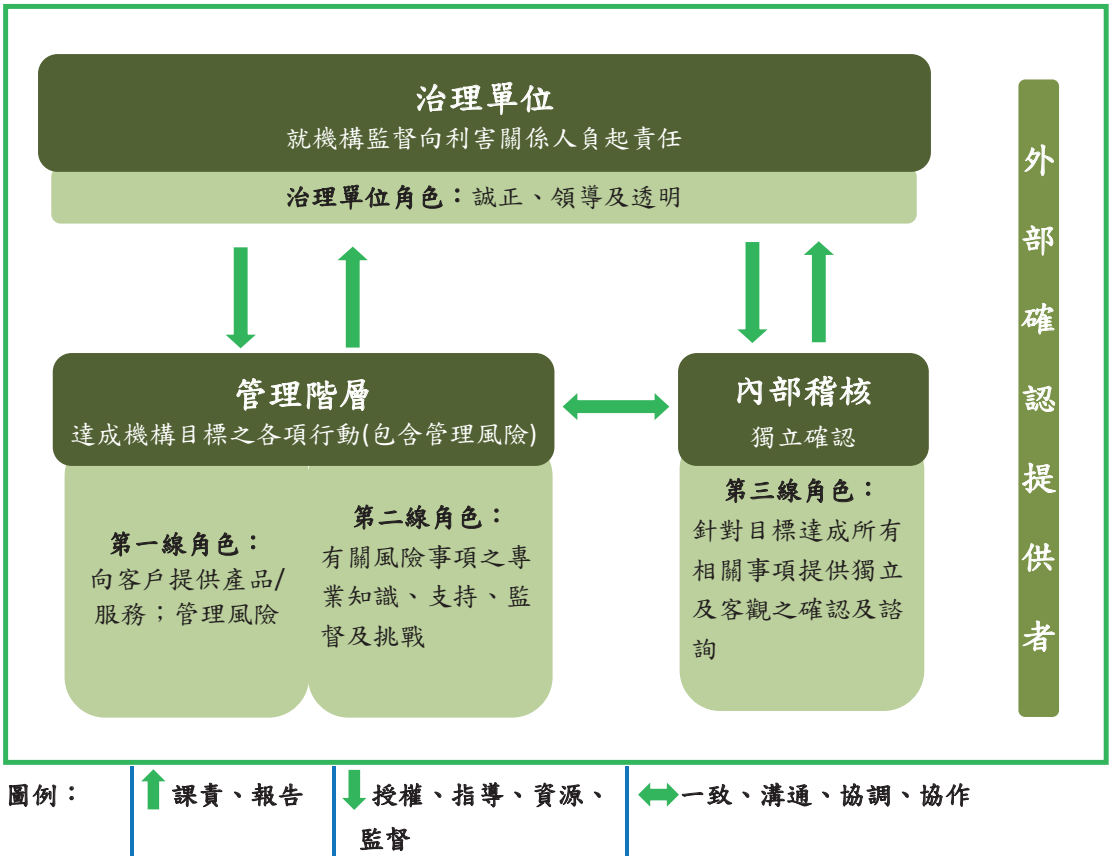
本文作者為審計部審計業務研究委員會稽察兼組長。本文為作者個人意見，不代表本公司立場。

（Internet of Things, IoT）、巨量資料 / 開放資料（Big Data/Open Data）—強調補充或消除人工作業，並透過更及時地報導攸關資訊且使財務報導更加簡便正確。準此，本文擬分享上述高度攸關內部稽核工作之風險與內部控制國際新知，提供稽核先進或高階管理者與治理單位作為規劃或辦理內部稽核相關工作參用並預為因應，以有效發揮稽核之洞察或前瞻價值。

貳、新三線模型

新三線模型旨在強調組織核心與共同組成要素之間的重要關係，及權衡模型概念的優勢、應用及有用性，以確保其在當今營運氛圍中繼續保有攸關性。IIA

圖 1　新三線模型關係圖



資料來源：作者參考 IIA Three Lines Model 自行繪製。

總裁 Richard F. Chambers 先生指出「風險管理不僅僅是防範。機構需要有效的結構及流程，以促進目標之達成及支持堅實的治理及風險管理。更新後三線模型解決我們現代世界的複雜性。」茲將新三線模型關係圖及六大原則彙如圖 1 及表 1。

表 1　新三線模型六大原則

原則	內涵
原則 1 治理	機構之治理需要適當的結構及流程，其有助於： ■ 治理單位為機構監督向利害關係人負起責任，透過誠正、領導及透明。 ■ 管理階層透過風險導向決策及資源應用以達成機構目標所採取各項行動 (包括管理風險)。 ■ 獨立內部稽核職能提供之確認及諮詢服務，目的在透過嚴謹詢問及洞察溝通以提供闡明及信心，及促進與推動持續改善。
原則 2 治理單位	治理單位確保： ■ 已為有效治理建立適當的結構及流程。 ■ 機構目標及作業與利害關係人優先利益相一致。 治理單位： ■ 授予權利及提供資源給管理階層以達成機構目標，同時確保符合法律、法規及倫理期望。 ■ 建立及監督獨立、客觀及稱職的內部稽核職能，為目標達成之進度提供闡述及信心。
原則 3 管理階層與第 1 及第 2 線角色	達成機構目標之管理階層責任包括第一線及第二線角色。第一線角色係最直接與向機構客戶提供產品及 / 或服務相一致者，包括輔助職能之角色。第二線角色係為管理風險而提供輔助。

原則	內涵
	第一及第二線角色可能混合或各自分離。有些第二線角色可能指派一些專家，負責對第一線角色提供互補性專業知識、支持、監督及挑戰。第二線角色可以專注於風險管理之具體目標，例如：遵循法律、法規及可接受的倫理行為；內部控制；資訊與科技安全；永續性；及品質保證。或者，第二線角色可能擴大更廣泛的風險管理責任，諸如企業風險管理(ERM)。但是，管理風險的責任仍然是第一線角色的一部分，且是屬於管理階層之範圍。
原則 4 第 3 線角色	內部稽核就治理及風險管理之適當性及有效性提供獨立及客觀之確認及建議。它透過系統化及有紀律的流程、專業知識及洞察之專業應用，以達成這項服務。它向管理階層及治理單位報告其查核發現，以促進及推動持續改善。如此，它可能考量來自其他內部及外部提供者之確認服務。
原則 5 第 3 線獨立性	內部稽核獨立於管理階層之責任，對其客觀性、權威性及可信度是至關重要的。它透過下列方式建立其獨立性：向治理單位負起責任；不受限制地接近必要的人員、資源及資料以完成其稽核工作；及避免在稽核服務規劃及提供過程產生偏見或干擾。
原則 6 創造及保護價值	一致地共同合作所有防線角色有助於創造及保護價值，當它們是與其他道防線及利害關係人優先利益相一致時。透過溝通、合作及協調可以達成作業之一致性。這樣一來，就可以確保風險導向決策必要資訊之可靠性、一致性及透明度。

資料來源：作者摘譯自 IIA Three Lines Model 。

參、區塊鏈與內部控制

近年，區塊鏈技術已成為各國政府與企業積極探索應用之領域，根據 2017 年 IBM 與 Economist Intelligence Unit 針對 16 個國家 200 個政府機構所做的調查，在 2018 年底之前，有 90% 的政府機構計劃在民眾服務、金融交易管理、資產管理、合約管理與法規遵各方面投資區塊鏈運用，以降低跨部會合作成本、提升效率與透明度。我國行政院國家發展委員會於 2019 年 7 月推動成立之臺灣區塊鏈大聯盟，目的在協助區塊鏈產業突破法規、人才培育或商業模式上的限制。目前已由政府委辦之區塊鏈技術導入公共治理研究計有 12 項區塊鏈應用計畫，涉及公共服務、金融保險、能源、醫療、農業等 5 大領域，涵蓋多個部會、公私營組織或公會。

美國 COSO 於 2020 年 7 月發布「區塊鏈與內部控制（Blockchain and Internal Control）」報告，指出隨著區塊鏈已逐漸變成主流，應適時關注這項技術如何與個體內部控制產生交集或影響，諸如控制環境相關之內部控制、調節、函證、零售商與供應商核准、第三方服務提供者及分散的外部系統等面向。簡言之，區塊鏈世界之控制類型，包括預防性及偵測性空制兩者，如表 2。

表 2　區塊鏈世界之控制類型

控制類型	區塊鏈含意
預防性控制	體認區塊鏈上交易紀錄之不可變特性，第一次就正確記錄交易是有好處的。
偵測性控制	區塊鏈世界中交易的能見度為偵測控制提供新的途徑，即當必要的資訊可在鏈上取得或從鏈上紀錄中可發現鏈外資訊時。另外，因可提供大量資料，整合區塊鏈與其他新興技術之分析能力—諸如人工智慧、物聯網及資料分析—可能被用於偵測異常值之一種方法。惟區塊鏈世界中之主要挑戰，在於當發現問題時該如何處理。儘管仍存有一般性更正之可能，但考量區塊鏈之自動寫入功能，更正需要及時反映各種調整，而不是直接更正一筆既有交易。請注意，這取決於所使用的特定區塊鏈之個別功能。

資料來源：作者摘譯自 2020 年 7 月 COSO「Blockchain and Internal Control」報告。

有關區塊鏈技術導入業務環境對五大要素所產生的影響，摘述如下：

一、控制環境：區塊鏈可能是有益於促進有效控制環境（例如，透過最少的人工干預進行交易記錄）之一種工具。然而，本要素多個原則主要涉及人工行為，諸如促進誠信及倫理道德之管理，即使整合其他技術，區塊鏈也無法加以評估。更大的挑戰是個體與其他個體或參與區塊鏈相關人員之多方關係，及如何管理這些成果之控制環境。

二、風險評估：區塊鏈產生各種新風險，同時有助於減輕既有風險，透過促進課責機制、保持紀錄完整性及提供不可辯駁的紀錄（即任何個人或組織不能否認或質疑他們在授權 / 傳遞訊息或紀錄方面所扮演的角色）。

三、控制作業：區塊鏈可作為協助促進控制作業之一種工具。區塊鏈與智能合約是有效推展全球業務之有力方法（例如，透過極小化人為錯誤及舞弊機會）。但是，區塊鏈之協作方面可能會帶來額外的複雜性，特別是在技術分散的情況下，沒有任何一方對財務報導內部控制之各個系統負起責任。

四、資訊與溝通：區塊鏈的固有屬性可提高交易的能見度及資料可用性，並為管理階層創造各種新途徑，以更快、更有效地向關鍵利害關係人溝通財務資訊。特別當管理階層在考量應用區塊鏈之一個面向，就是資訊的可用性，以支持財務帳簿與紀錄、及區塊鏈上交易資訊之可稽核。

五、監督作業：區塊鏈為促進更頻繁、更多主題、更詳細監督之承諾可能會大大改變實務作法。智能合約及標準化業務規則之使用、結合物聯網設備情況下，可能會改變監督之執行方式。

茲就該報告所提區塊鏈關鍵面向之控制，以及區塊鏈與內部控制等兩大核心思維，彙整如表 3 及表 4，前者按區塊鏈面向而提出控制作業設計或執行應考量重點；後者按內部控制整合架構之五大要素及 17 項原則，歸納使用區塊鏈相對增加之價值、新威脅或風險及降低新威脅與風險之各種控制。

表 3　區塊鏈關鍵面向之控制

區塊鏈面向	控制作業考量
1. 各節點	區塊鏈網路上之每台電腦都被稱為 " 節點 "。對組織來說，建立管理各節點活動之控制是必須且很重要的，這些節點儲存資料庫副本、執行交易驗證、準備要加入鏈中之資料或執行其他服務。控制可能與下列目標相關： • 確保足夠的節點，以極小化某些人協同攻擊系統之機會。 • 確保所有節點之適當分配運算能力，使共識協定無法被竄改。 • 測試網路中不同節點區塊鏈資料之可用性。 • 驗證網路中不同節點所蒐集資料之一致性。 • 在同意將資料加入鏈中之前，測試節點是否正在執行攸關驗證。 • 追蹤及提供正確驗證之激勵措施，及懲處不正確驗證。 (注意：鑑於網路上運行節點之數量龐大，組織可能無法對公有鏈執行上述各項控制。)
2. 共識協定	應定期評估特定區塊鏈之共識協定，以確定： • 適當節點是否有權參與共識協定。 • 協定是否適當地設計及有效地運作。 • 遵循協定之獎勵措施及未遵循協定之懲處是否已適當設計，以減少舞弊行為。 共識之主要類別是否包括工作量證明、持有量 (權益) 證明或多數表決。
3. 私鑰	組織應採取措施以管理他們的私鑰存取。這些控制將取決於這些私鑰之儲存方式 (例如，熱錢包或冷錢包)。在某些情況下，組織可能會委請第三方保管私鑰以協助管理或直接管理資產。保管人可能需要跨多方拆分以對私鑰進行存取，因此需要多方核准交易 (多重簽章)。同樣重要的是，確保組織已考量適當的職責分工，以確保核准區塊鏈交易者沒有權力在組織的帳簿及紀錄中記錄交易。

區塊鏈面向	控制作業考量
4. 智能合約	為降低與智能合約相關的風險，組織可能： • 實施各項控制以驗證智能合約設計及執行有效性是否適當、以受控制方式追蹤變更及更新、及確保有適當的文件及歷史紀錄以建立課責性。 • 對智能合約的輸入執行控制，包括來自區塊鏈預言機 (oracles) 的輸入。智能合約控制應提供及時的預警及例外報告，以確保一切正常，及各種違反及偏差會及時向適當各方報告。

資料來源：作者摘譯自 2020 年 7 月 COSO「Blockchain and Internal Control」報告。

表 4　區塊鏈與內部控制

5 大要素 17 項原則	使用區塊鏈所增加之價值	使用區塊鏈之新威脅或風險	降低區塊鏈使用之新威脅與風險
控制環境			
1. 展現誠信與道德價值之承諾 2. 行使監督責任 3. 建立結構、權限與責任 4. 展現適任人才之承諾 5. 強化課責性	• 區塊鏈流程通常具有加密可驗證之不可變性及不可逆轉性，因此，良好設計及執行之區塊鏈，管理階層應能依賴及提供行為之證據。 • 共用帳簿系統之較大能見度有助於強化透明度，從而促進完備控制環境及提升出具即時財務報告之	• 在區塊鏈上進行交易各方人士之偽匿姓名，加上開放性及潛在缺乏防護機制，構成一種威脅，即非許可制區塊鏈可能被不道德的應用。 • 每個區塊鏈之建立都具有獨特的治理結構，需要積極監督其運行狀況及營運有效性。對於某些區塊鏈，	• 在適當情況下，可訂定管理區塊鏈交易各方行為之行為規範，及解決未遵循問題之指引。另外嘗試實施私有鏈或建立聯盟鏈之組織，可能訂定此類行為準則及機制，以利 (1) 驗證每個成員對道德及誠正之承諾；(2) 透過行為規範實施課責

5 大要素 17 項原則	使用區塊鏈所增加之價值	使用區塊鏈之新威脅或風險	降低區塊鏈使用之新威脅與風險
	能力。 • 區塊鏈與人工智慧及資料分析等其他新興技術之分析能力，可能讓組織更及時辨識違反組織行為規範之情事。這對大型及 / 或分權組織實施有效監督方面，區塊鏈是特別有助的。 • 在某些情況下，區塊鏈可能促使從流程中刪除管理階層人工干預，使流程在很大程度上不受管理階層決策、誠正及道德之影響。	分權及缺乏一個中央中介機構、系統或監督機構，難以對交易各方之行為課以責任，導致實際上 " 不負責 " 的情況。如果且當事情真的出錯時，某些區塊鏈是無法求助於任何人且因此沒有課責一一個嚴重的治理相關缺點。 • 雖然一般認為，區塊鏈的使用具有前瞻性思維與積極性，但組織的員工、客戶、顧問及監督者可能會消極地看待有關倡議、採用及接受區塊鏈或與某些團體互動之行為。此外，根據區塊鏈之性質及參與者，組織可能面臨聲譽風險，因為參與可	機制及報告 / 解決 / 補救任何偏差。組織應清楚地瞭解治理過程、及積極監督與評估其是否有效。組織另可考量讓獨立的外部人士進行監督，及盡可能確認遵循既定行為規範之程度。在這種情況下，很重要的是，組織必須建立明確的報告體系，以確保外部人士直接向治理單位報告。 • 此外，應考量外包服務提供者行為規範、責任及職權之各項期望。儘管與外包服務提供者有關之許多活動是發生在區塊鏈之外，但如果與這些關係相關之不可靠資料進入

5 大要素 17 項原則	使用區塊鏈所增加之價值	使用區塊鏈之新威脅或風險	降低區塊鏈使用之新威脅與風險
		能被視為共享團體道德之最低共同標準（即，聯盟聲譽）。對於控制誰進入系統及對系統進行共識變更，將不再受管理階層的控制。 • 區塊鏈之新鮮感及複雜性意味著很難找到稱職人員，且對能力的承諾也難獲得保證或評估。區塊鏈可促進自動化之潛力意味著可以自動完成更多的工作，且人們責任與相關能力之實質也會發生變化或巨大的變化。同樣地，管理階層及治理單位可能很難獲得攸關的瞭解及專業知識，以協助其有效監督區塊鏈之執行與使用。	區塊鏈，結果會是極具挑戰性的。 • 擬訂盡職調查政策及其各種指引及標準，以確定組織將與其進行交易之各方；組織將核准其存取區塊鏈之各方；及組織可能選擇用於進行交易之公有鏈。這些政策可能包括瞭解您的客戶程序、反洗錢程序、要求系統與組織控制報告、以及其他盡職調查程序，目的在瞭解交易對手之身分及誠正。此類程序另可能包括瞭解在管理區塊鏈內各方行為已訂定政策。保持對治理過程之瞭解及繼續監督其有效性，是特別重要的。 • 評估有關蒐集或

5 大要素 17 項原則	使用區塊鏈所增加之價值	使用區塊鏈之新威脅或風險	降低區塊鏈使用之新威脅與風險
			建立區塊鏈技術之專業知識需求，以確保有效執行及執行後技術之適當使用與更新。此外，因應技術繼續迅速地發展，應繼續重新評估及監督這種能力。 • 確保組織能夠評估及評核新技術與流程，這可能需要透過內部資源、外包資源或組合兩者。
風險評估			
6. 具體指明適合目標 7. 辨識及分析風險 8. 評估舞弊風險 9. 辨識及分析重大改變	• 整合區塊鏈與其他新興技術可為管理階層、董事會及外部各方人士提供即時報導—從而創造一個更加敏捷的業務環境—該報導旨在辨識及評估個體各項目標之達成程度(例如，營運、外部財務報導、遵循或其他內	• 傳統風險評估係以個體為中心，但在使用區塊鏈技術下，組織需要更廣泛地考量各種風險。例如，個體可能考量區塊鏈網路中其他各方對風險的敏感性，及風險敏感性會對它們各自的業務所產生的影響。此外，在設計區塊	• 為區塊鏈之使用建立目標，如此，區塊鏈之實施即能支持可靠且可驗證的帳簿及記錄，進而完成適當會計及有效的財務報告。 • 建立更完備風險評估流程，其能考量區塊鏈對組織所有面向之影響。在進行此類評估

5 大要素 17 項原則	使用區塊鏈所增加之價值	使用區塊鏈之新威脅或風險	降低區塊鏈使用之新威脅與風險
	部目標)。	鏈之監督控制時，區塊鏈各方間之不同風險胃納 / 風險容忍度會產生衝突。對特定區塊鏈而言，如果沒有任一方負起責任，可能會存在誰負責管理風險及如何達成適當的課責機制等問題。 • 區塊鏈之實施可能會使組織遭遇新舞弊詭計或執行傳統舞弊詭計新途徑之高度脆弱性。 • 支持區塊鏈環境之可用資料量會變得更難管理；試圖管理過多的資料可能導致資料超載，進而加劇資料治理之問題。 • 智能合約既是一項潛在風險，同時也是風險減輕工具集之重要一部分。一旦建立妥適	時，組織與相關的 IT 及區塊鏈專家共同合作，以協助辨識潛在威脅、風險領域及舞弊詭計 (基於對組織控制環境、區塊鏈及常見舞弊詭計之瞭解)，可能會是有幫助的。 • 建立程序以瞭解區塊鏈業務及監管環境之變化。組織法律顧問及內部稽核部門儘早參與技術之實施，可能有助於隨時瞭解監管環境的變化。 • 因區塊鏈已整合至組織業務資訊流程中，且此類整合具有財務報告含意，管理階層應與相關人士 (如內部稽核人員、外部審計人員) 合作以確定攸關財務報導、內部控制、適

5 大要素 17 項原則	使用區塊鏈所增加之價值	使用區塊鏈之新威脅或風險	降低區塊鏈使用之新威脅與風險
		後，它們將自我執行且很難停止的。因此，如果未正確地開發或操作不當，這些影響可能會導致錯誤或擴大潛在重大損失之規模。 • 區塊鏈之使用會發生各種問題，即有關蒐集足夠適切證據以支持組織財務記錄中之已記錄交易 (因電子環境中交易稽核軌跡已喪失)。 • 數位資產導入一種新的資產類別，對這些數位資產而言，極少或缺乏以前的經驗，且在管理風險及辨識異常行為方面，幾乎缺乏有意義的相似之處。考量持有數位資產之企業針對資產本身已提高下列各項考量，包括：市場	當會計處理及稽核含意之新風險 (例如，潛在可稽核性挑戰)。 • 讓適當的 IT 及區塊鏈專家瞭解組織之既有系統，以評估實施區塊鏈前，其如何被整合於組織既有 IT 基礎架構中並成為其運行之一部分。 • 建立完備治理及變革控制流程，以部署新的或修正現有智能合約或區塊鏈之變更，此類流程另應考量事件回應管理、及辨識與回應智能合約與區塊鏈營運小故障之方法。

5 大要素 17 項原則	使用區塊鏈所增加之價值	使用區塊鏈之新威脅或風險	降低區塊鏈使用之新威脅與風險
		波動、或某些數位資產缺乏市場、有關保護私鑰之網路安全風險、此類資產的會計與財務報告、以及不斷變化的監管要求。 • 整合區塊鏈與既有傳統系統之挑戰可能會出現，區塊鏈是一個工具，更是更大型核心基礎架構的一部分，且必須與傳統基礎架構無縫協作。區塊鏈與個體其他系統之不佳整合可能會導致低於預期之結果，諸如負面的客戶體驗及監管未遵循問題。 • 有關區塊鏈、智能合約及數位資產之監管環境，正不斷地發展及可能因司法管轄區而異，導致監管要求 (包括稅收、資料	

5 大要素 17 項原則	使用區塊鏈所增加之價值	使用區塊鏈之新威脅或風險	降低區塊鏈使用之新威脅與風險
		隱私與保護、報導或其他監管要求) 之不確定性。 • 區塊鏈之業務環境正在持續發展中，以及每天正在發現之技術、最佳實務及新實例之改善。監督快節奏及快速發展環境之能力，可能已證明是困難且極具挑戰性的。 • 目前存在的零星解決方案可能很快就會被取代。將時間、人才、資金及媒體大量投資於技術與方法上，已經導致解決方案市場之高度零散，以及功能重疊、互通性低。鑑於區塊鏈發展方法之持續雜亂無章、不協調，預測 2021 年前，在 2019 年實施區塊鏈者，90% 將需	

5 大要素 17 項原則	使用區塊鏈所增加之價值	使用區塊鏈之新威脅或風險	降低區塊鏈使用之新威脅與風險
		要更換。 此外，因為技術具有高度自動化特性，在區塊鏈環境中之一般 IT 及其他風險可能會漸趨劇烈，諸如下列各領域： • 儘管諸如系統與資料存取許可權、及程式完整性等問題在其他技術解決方案中是很常見的，但對技術存取許可權之關注事項更加被重視，因為不當存取問題之影響可能成為區塊鏈上各組織之共有問題。 • 當區塊鏈對許多交易各方而言是可見時，能見度可能會帶來網路安全挑戰及網路攻擊。 • 對於大多數公有鏈而言，使用者可能無法了解已實	

5 大要素 17 項原則	使用區塊鏈所增加之價值	使用區塊鏈之新威脅或風險	降低區塊鏈使用之新威脅與風險
		施一般 IT 控制及這些控制之有效性。此外，如果沒有負責管理及執行議定書修改的中央機構，就會對該技術開發 / 維護過程之已建立控制作業產生一種挑戰。 • 鑑於區塊鏈上記錄交易之快速度，連同交易之不可變性及不可逆性，如果區塊鏈內部控制缺失未及時被辨識及改正，組織可能面臨提高重大損失或錯誤之風險。另外，刪除集中監督及中介機構可能會使組織在發生錯誤或損失時沒有追索權，從而造成治理的挑戰。以區塊鏈導向交易為主之組織，不可依賴諸如銀行之中央	

5 大要素 17 項原則	使用區塊鏈所增加之價值	使用區塊鏈之新威脅或風險	降低區塊鏈使用之新威脅與風險
		中介機構，在發生舞弊時拿回其資金。因此，組織將需要考量是否需要增強其內部控制基礎架構。 • 隨著組織開始整合區塊鏈，會存在一個過渡時期。此時，傳統系統、ERP 或第三方雲端系統將執行前端處理與資料蒐集，然後與區塊鏈進行介接以進行額外處理或記錄。儘管在區塊鏈中，資料基本上是安全的且防篡改的，但在區塊鏈之外的資料仍然容易受到一般常見的 IT 風險之影響。在這些新環境中，資料從上游系統到區塊鏈的介面傳輸，將是一個敏感的控制點。	

5 大要素 17 項原則	使用區塊鏈所增加之價值	使用區塊鏈之新威脅或風險	降低區塊鏈使用之新威脅與風險
控制作業			
10. 選擇及建立控制作業 11. 選擇及建立科技之一般控制 12. 透過各項政策與程序建置	• 良好設計及執行之區塊鏈可能提升組織強化其內部控制之能力 (例如，透過促進課責性、保持紀錄完整性及不可逆性)，適當地執行區塊鏈可能會減少直接存取紀錄、修改或刪除歷史資料之事項。例如，對某些區塊鏈而言，一旦一個區塊被充分掩埋 (即較新的驗證區塊存在於它上面)，歷史資料之變更風險是最小的，除非管理各方同意執行變更或對鏈進行分叉 (假定沒有破壞區塊鏈的安全性)。 • 區塊鏈之高度自動化性質，連同在共用帳簿上驗證及記錄不可變交	• 區塊鏈適當功能係高度依賴基礎技術之可靠性及互補業務流程與一般 IT 控制之執行。不佳的區塊鏈執行或缺乏適當的支持控制會導致攸關區塊鏈新的或更普遍的問題，包括有關智能合約、私鑰管理、共識協定、鏈回滾 (chain rollbacks) 及分叉 (forks) 等問題。 • 智能合約功能強大但會增加複雜性。與任何其他程式所設計應用程式一樣，智能合約可能包含程式設計錯誤或後門，或受到其他挑戰。設計及執行不良的智能合約且業務邏輯不足，可能導致大規模自動	儘管區塊鏈之執行可能提高或損害個體控制作業有效性，但可以採取一些具體步驟來減輕這些風險，並充分利用區塊鏈的潛力。例如，修正後政策及程序應解決與區塊鏈使用相關之新風險、內部控制及會計問題，及建立執行政策及程序之責任及課責性。此外，組織應考量確定及執行區塊鏈關鍵面向之攸關控制，包括表 3 所述的各項控制。

5 大要素 17 項原則	使用區塊鏈所增加之價值	使用區塊鏈之新威脅或風險	降低區塊鏈使用之新威脅與風險
	易之技術能力，為組織提供打擊交易及報告舞弊之機會，因為財務報告流程中人工干預之降低。隨著區塊鏈之使用，傳統的舞弊或人工錯誤機會將減少，從而減少損失之風險。此外，由於多方參與共識協定而更有可能辨識錯誤，因此在過帳之前，各方會驗證交易之準確性。 • 區塊鏈刪除某些 IT 一般控制之需求，因為它極小化資料損失之風險，因此，諸如資料備份、節點之間的批次處理、災難恢復等傳統控制，可能不再需要了，除非平臺被放棄或被廢止。因為區塊鏈帳簿在網路上多個節點之共用，因	化執行及記錄無效交易，而無效交易可能會是無追索權—這是一個非常不良的結果。 • 區塊鏈無法為存取組織私鑰提供管理保護，因此不能為其數位資產提供直接控制。缺乏對私鑰之適當控制及啟動區塊鏈導向交易之能力，可能導致組織資產之潛在損失或挪用。企業私鑰管理軟體才剛剛開始出現，私鑰管理指引也是剛剛開始出現。 • 依據協議性規則，區塊鏈共識協定 (或機制) 訂定為驗證交易之規則、先決條件及要求。設計及執行不佳之共識協定損害依據協議性規則適當驗證交易之	

5 大要素 17 項原則	使用區塊鏈所增加之價值	使用區塊鏈之新威脅或風險	降低區塊鏈使用之新威脅與風險
	此對備份的依賴就不那麼重要了，因為最新版本帳簿可能會從網路上其他未受影響的節點獲得復原。 • 使用區塊鏈另可能降低交易處理及紀錄未及時等風險，因為根據特定的區塊鏈，它可能為組織提供近乎即時基礎之處理及記錄交易的能力。此功能可以大大減少錯誤。 • 智能合約可能增強控制作業及預防舞弊機會 (由於合約條款之自動化執行)。但請注意，由於智能合約是一種工具，智能合約所使用的工具或輸入 (包括來自區塊鏈預言機的輸入) 可能會被竄改以犯下舞弊。	技術能力。在這種情況下，在共用帳簿上記錄之資訊可能是無效的且不可靠的。即使執行有效的共識協定，區塊鏈上所記錄之交易仍有可能是無效的，原因很多，包括如果網路成員之間的運算能力分布使一組成員的一個或多個成員能夠篡改共識協定，即 "51% 的攻擊 (51% 的攻擊者將擁有足夠的礦池算力從而能夠故意排除或篡改交易順序。)"。 • 共識協定推動系統之更新及變更。鏈回滾是 " 改正 " 區塊鏈中重要錯誤之主要方法，但可用於規避鏈的不可變性，透過從較早時點重新啟	

5 大要素 17 項原則	使用區塊鏈所增加之價值	使用區塊鏈之新威脅或風險	降低區塊鏈使用之新威脅與風險
		動。因此，鏈回滾可能為管理階層提供變更區塊鏈上已紀錄交易之能力。 • 如果組織從事記錄鏈外交易，區塊鏈上所記錄交易之完整性可能會受到質疑。區塊鏈上不會擷取鏈外交易，及需要額外的考量及控制，才能與鏈內交易及相關財務報導進行調節。	
資訊與溝通			
13. 使用攸關資訊 14. 內部溝通 15. 外部溝通	• 區塊鏈可提高交易的能見度，並為管理階層向關鍵利害關係人溝通財務資訊提供新途徑 (例如，透過臨時的、即時財務報導)。 • 作為一個全面性、共享資料庫，區塊鏈可作為提供與財務報導及決策	• 因為區塊鏈全部功能、區塊鏈是什麼、及區塊鏈能做什麼，存有高度不確定性，因而產生一種虛假的舒適感，就是區塊鏈上的資訊都是正確的、資訊是可用的、人們已經知悉，以及已經獲得回反饋。	• 教育關鍵利害關係人 (包括治理單位) 瞭解企業如何使用區塊鏈及使用該技術之相關效益及風險。很重要的是，利害關係人必須明白，儘管區塊鏈設計係為改善交易執行及記錄流程，目的是提供即時已

5 大要素 17 項原則	使用區塊鏈所增加之價值	使用區塊鏈之新威脅或風險	降低區塊鏈使用之新威脅與風險
	制定攸關各種交易資料之基礎。 • 如果執行得當，區塊鏈可促進資料之可用性，該等資料是可存取的、準確的、一致的、最新的、保存的及及時的。 • 在一般及全面性數位帳簿中輸入或整合資料時，資料不太可能會遺失，從而提高能見度及提供補充性證據。	事實上，維護區塊鏈上之資訊完整性只能依賴輸入的正確性；就像其他一樣，「垃圾進垃圾出」占多數。另外，存儲在區塊鏈上資料之可靠性取決於基礎技術之有效性，缺失技術所支持區塊鏈可能提供不可靠且無法補救潛在缺失之資料。 • 儘管區塊鏈能夠及時記錄大量交易資料，但這些資料需要被處理成有用的且可操作的資訊。 • 由於與財務報告有關，組織可能面臨的挑戰，包括在蒐集足夠且適當證據以支持其對區塊鏈上已處理數位資產或數位資產交易之五大聲明。另外，組織	驗證交易，但仍存在可能使資料不可靠之相關風險。 • 確定董事會及審計委員會擁有必要資訊，供其履行相關監督責任之需求。 • 建立各種方法以為區塊鏈網路各方報告任何關注事項，可能包括舉報人熱線，如果尚未建立的話。 • 擬訂溝通方法，確保與區塊鏈使用相關之操作及其他變更 / 更新溝通給適當的人員，以利他們能瞭解及履行其內部控制相關責任。 • 根據區塊鏈之使用而確定所需的新資訊要求，以利產生攸關的、高品質資訊，進而支持內部控制之有效運作。

5 大要素 17 項原則	使用區塊鏈所增加之價值	使用區塊鏈之新威脅或風險	降低區塊鏈使用之新威脅與風險
		可能面臨的挑戰為審計人員是否能夠蒐集證據，這些證據是評估帳簿及記錄是否獲得到充分支持所需的。	• 擬訂資料分析程序，以利從區塊鏈中辨識及蒐集攸關的、高品質資料，然後這些資料可以被處理成資訊，用於支持管理階層之業務流程及報導目標。 • 在發展或辨識用於組織流程之區塊鏈時，與內部及外部稽核人員進行討論。很重要的是，管理階層必須瞭解與使用區塊鏈相關的典型可稽核性問題，及為減輕此類問題所執行之回應流程，如此一來，可獲得之持交易之適當資訊。
監督作業			
16. 執行持續性及（或）個別評估 17. 評估及溝通缺失	• 因區塊鏈可透過最小化人工干預而促進更整合性、流通式環境，評估本身可以使用智	• 處理經常更新之大量資料可能會加劇有關資訊超載之風險及敏感性，並造成充分監	• 鑑於區塊鏈上已處理資料的數量是很巨大的，且處理這些交易的頻率是很高的，因此

5 大要素 17 項原則	使用區塊鏈所增加之價值	使用區塊鏈之新威脅或風險	降低區塊鏈使用之新威脅與風險
	能合約、AI 及標準化規則引擎，構建一個區塊鏈增能流程。另外，區塊鏈還可與其他技術一起使用，以協助辨識為進行有效監督之資訊。例如，IoT 設備可以在人工干預不可行的情況下採取行動，以便根據環境的變化即時記錄交易。區塊鏈可維持詳細的資料，該等資料可以不同的方式被彙總，以利完成不同範圍及頻率之評估。 • 因為資訊係以即時基礎被蒐集或整合至區塊鏈上，監督作業可以擷取更接近缺失發生時之問題，從而極小化暴險及加速補救。 • 如果有效執行，區	督方面之其他挑戰。 • 與控制環境要素之挑戰類似，找到有能力的人來設計及執行區塊鏈之有效監督控制，可能是極具挑戰性的。 • 區塊鏈之使用案例，在數量上及複雜性上正快速成長，區塊鏈相關法令規定亦如此。跟上持續變化是困難的，及確保技術與所需任何其他程序或操作流程是適當且及時更新的，包括監督。 • 分權及缺乏某些區塊鏈中央中介機構可能導致沒有既定的人或單位負責執行監督控制、並構成治理挑戰。	使用電腦化持續監督技術以執行持續性評估，而不是傳統的人工技術。 • 使用持續性評估以辨識技術之變化及更新，並驗證內部控制要素是否存在並有效運作。 • 辨識及蒐集具備組織基礎控制環境、區塊鏈技術及監督技術最佳實務之必要知識人才，以利：1. 協助設計及執行適當的監督控制及；2. 評估此類監督作業之成果與效率。 • 評估區塊鏈之獨特方面，諸如共識協定、智能合約及私鑰，以及與使用中區塊鏈之運行狀況、治理及整體可靠性相關之各種因素。

5 大要素 17 項原則	使用區塊鏈所增加之價值	使用區塊鏈之新威脅或風險	降低區塊鏈使用之新威脅與風險
	塊鏈之使用可更及時辨識錯誤及績效複核，從而更全面地進行區塊鏈。高階分析、AI 及其他工具可用於分析詳細資訊，使管理階層能專注於高風險領域。內部稽核人所執行個別評估也可以聚焦於自身所使用最攸關之資訊。		• 在聯盟鏈或私有鏈中，辨識負責執行監督控制之個人及建立協議性政策與程序者，以溝通缺失及在發現缺失時採取改正行動。 • 在某些情況下，保留客觀第三方來評估聯盟鏈。例如，如果需要從各個個體提供專有資訊，以確定各要素是否有效運作、評估缺失、及溝通缺失，則受信任的中介者可以存取此類資訊。 • 監督與外包服務提供者之服務層級協議與控制報告。如前所述，如果與這些關係有關之不可靠資料進入區塊鏈，結果可能會受到嚴重損害，甚至是災難性的。

資料來源：作者摘譯自 2020 年 7 月 COSO 「Blockchain and Internal Control」報告。

肆、結語

新三線模型適用於所有組織，組織可透過下列方式優化這個新方法：一、採用原則導向方法及調修模型以適應組織目標及情況；二、聚焦於達成目標及創造價值之風險管理投入，以及＂三線＂及保護價值之事項；三、執行相關措施以確保各項活動及目標係符合利害關係人之優先利益；四、清楚地瞭解模型中的角色及責任，以及它們彼此之間的關係。另區塊鏈實施及整合雖會產生新的風險及對新控制之需求，組織可利用區塊鏈之獨特功能為組織創造更堅實的控制，同時，區塊鏈增強型工具（blockchain-enhanced tools）亦具有提升營運效率及效果、改善財務及其他報導之可靠性及回應能力，以及改善遵循法令規定之潛力。希冀我國相關主管機關能及時關注及洞悉數位時代下新興風險與其控制之國際脈動，從政策面、法令面、實務面、影響面等，以擁抱風險並掌握機會之新思維，盤點檢討後策進改善並前瞻擘劃適合我國私部門各產業、非營利組織及公部門之有效風險管與內部控制，協助各場域內部稽核人員在新常態下採取敏捷稽核方法與視野，特別是優化風險導向稽核規劃頻率、深度及廣度，以回應利害關係人期望及積極展現內部稽核之附加價值。