論述 》專論 · 評述

政府資訊科技治理與稽核

2020 年新冠肺炎（COVID-19）疫情嚴重衝擊各國，我國政府及相關業者齊心協力，超前部署此項疫情之防治（包含資訊科技之應用），成效卓著，深獲國際肯定。為推動電子化政府，政府機構應建立適當的 IT 治理及管理系統，以提供便捷、優質的公共服務，確保業務持續。本文簡介 COBIT® 2019 架構及 IT 治理稽核觀念，可作為政府推動 IT 治理的參考。

陳錦烽（實踐大學管理學院國際企業英語學位學程副教授兼主任）

壹、前言

2020 年初出現的新冠肺炎（COVID-19）演變成爲全球疫情，嚴重衝擊各國經濟及生活，無論是政府、企業或人民都受到嚴重的影響。我國政府及相關業者齊心協力，針對新冠肺炎的防治進行超前部署及因應，獲得極大的成效，使得疫情不至於在臺灣蔓延，深獲國際肯定。

在此次防疫過程中，除了政府官員及民間業者奮力不懈，勇於任事之外，資訊科技（information technology, IT）的應用也扮演著極爲重要的角色。例如，中央流行疫情指揮中心陸續實施下列措施：(1) 利用健保卡勾稽移民署入境資料，供醫護人員查詢疫區旅遊史；(2) 針對居家隔離或檢疫者實施電子監控，並與警察機關連線，以落實防疫；以及 (3) 實施口罩實名制，民眾可透過健保卡、自然人憑證登入平台，或健保快易通 APP 認證，進行口罩預購；以及 (4) 利用大數據資料進行疫情調查及監控[1]。由此可見，資訊科技的有效應用對於政府施政效能極爲重要。本文在於簡述電子化政府及 IT 治理架構，並說明如何進行 IT 治理稽核。

貳、電子化政府與 IT 治理

隨著 IT 的迅速發展，政府必須善用 IT 推展政務，以提供便捷、優質的公共服務，進而推動「電子化政府」。所謂電子化政府，係指「政府應用資訊通訊科技提升內外部關係」[2]或「使用資訊通訊技術提昇政府與民眾、企業或其他政府機

關之間的關係」[3]。換言之，電子化政府涉及各項資訊通訊基礎設施（包含硬體、軟體、網路）、政策與程序的建立、導入及運作。政府電子化落實的程度，直接影響施政效能及國家競爭力，因此，政府必須重視電子化過程的治理，亦可稱爲政府的 IT 治理。

IT 治理爲政府治理的重要環節，其目的在於擬定及實施各項流程、架構及相關機制，以支持及促進政府的施政。政府 IT 治理的預期成效包含 (1) 實現效益：透過 IT 投資，提供即時、優質的公共服務，實現相關效益，增進機構價值；(2) 風險最適化：適當的管理有關 IT 取得、使用及運作的風險，使其與運用 IT 所產生之效益具有合理的關係；以及 (3) 資源最適化：確保 IT 相關資源（包含IT基礎架構、硬體、軟體、人員、資料、資訊等）之充足、適當及有效，以具備執行機構各項計畫之能力[4]。政府機構應採用適當的 IT 治理架構，以期達成 IT 治理的預期效益。

參、IT 治理架構與稽核

如前所述，IT 治理需要一套適當的架構，引導機構建立 IT 治理及管理系統，落實相關的流程及作業，以達成治理目標。此外，治理及管理系統需要透過適當的稽核，以確認其是否有效運作。茲簡介 COBIT 2019 架構及相關稽核觀念如下。

一、COBIT 2019 架構

國際電腦稽核協會（Information Systems Audit and Control Association, ISACA）所發布的「資訊及相關技術的控制目標」（Control Objectives for Information and Related Technology, COBIT）2019 年架構（以下簡稱 COBIT 2019），可做爲機構 IT 治理的架構及標準[5]。COBIT 是一套用於企業 IT 治理與管理的指引，其涵蓋治理系統的原則、基本觀念、治理與管理目標、績效管理以及治理系統設計與實施，提供機構管理階層、稽核人員及使用者 IT 治理架構、流程及最佳實務，以提升機構 IT 治理，增進機構價值。

COBIT 2019 明確區分治理（governance）與管理（management）[6]。「治理」在於確保 (1) 機構評估利益相關者（stakeholders）之需求、情況及選項，以訂定平衡、有共識（balanced, agreed-on）的目標；(2) 透過優先排序及決策，提供指引；(3) 根據有共識的指引及目標，監督績效及遵循。「管理」則在於依照治理單位的指示，規劃、建構、執行及監控各項作業，以達成機構目標。治理系統的組成要素包含流程、組織結構、政策與程序、資訊流、文化及行爲，以及基礎架構。COBIT 亦界定 IT 治理系統的設計因子（design factors），將治理議題連結至相關的治理及管理目標，以便機構進行設計及管理。COBIT 2019 設定的對象爲機構內部及外部的利益相關者，前者包含董事會、高階管理者、業務經理、IT 經理、確認服務提供者、風險管理人員等；後者包含主

論述 》專論 · 評述

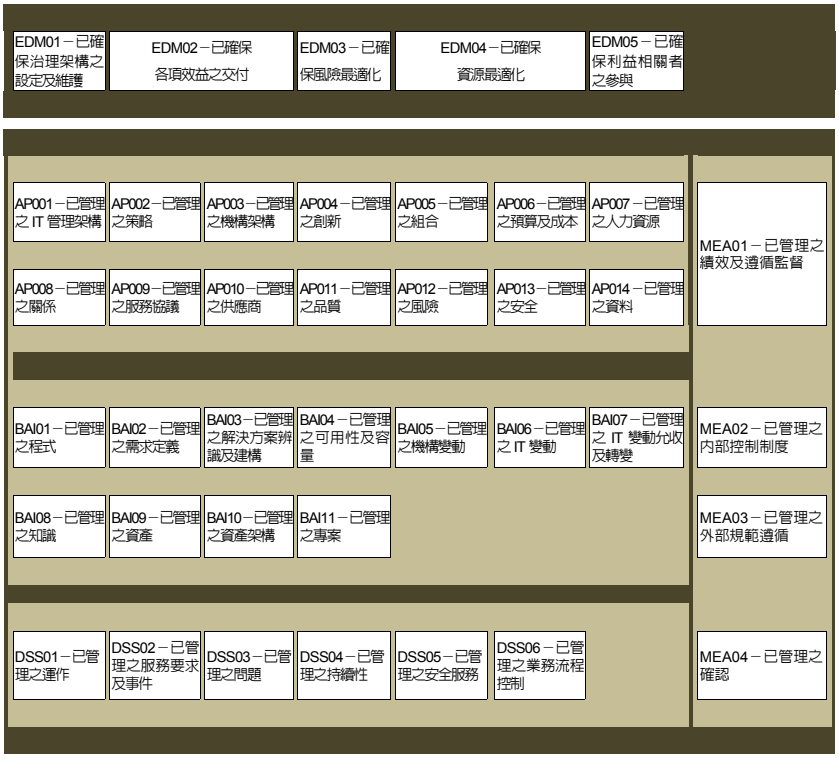
管機關、業務夥伴、IT 供應商等。

針對 IT 治理架構及系統之建立，COBIT 2019 制定相關的原則。IT 治理架構的原則爲 (1) 以觀念模型爲依據、(2) 開放及彈性以及 (3) 符合相關的主要標準、架構及法規；IT 治理系統的原則包含 (1) 提供利益相關者價值、(2) 採用整體的法（holistic approach）、(3) 動態的治理系統、(4) 明確區分治理與管理、(5) 切合機構需求以及 (6) 全面性的治理系統[7]。除了 COBIT 2019 架構之外，ISACA 亦發布 COBIT 2019 設計指引及 COBIT 2019 實施指引，可供機構客製化設計符合其需求的 IT 治理系統。

機構建立 IT 治理系統時，應先確立 IT 治理及管理目標。根據 COBIT 2019，每一項治理或管理目標一定連結至某項流程及有助於達成該項目標的一系列相關組成要素。治理目標連結至某項治理流程，管理目標則連結至某項管理流程。這些目標區分爲五個群組，其中治理目標稱爲評估、指示及監督（EDM）範疇（domain），管理目標則包含四個範疇：接軌、規劃及組織（APO）；建構、取得及導入（BAI）；交付、服務及支援（DSS）；以及監控、評估及評核（MEA）[8]。上述範疇及相關目標構成 COBIT 的核心模型，如附圖所示。

IT 治理系統的建構、運作與維護，須具備適當的組成要素，並考量相關的設計要素。IT 治理系統組成要素通常包含 (1) 流程、(2) 組織結構、(3) 各項原則、政策及架構、(4) 資訊、(5) 文化、倫理及行爲、(6) 人員、技術及能力，以及 (7) 服務、基礎架構及應用程式[9]。上述組成要素交互作用，共同促進治理系統的良好運作。至於 IT 治理系統應考量的設計因素則包含機構策略、目標、風險圖像、IT 相關議題、威脅樣貌、遵循要求、IT 角色、IT 資源模型、IT 導入方

附圖　COBIT 核心模型



資料來源：ISACA（2018）COBIT® 2019 Framework: Introduction and Methodology, p.21。

法、科技採用策略以及機構規模。機構在設計 IT 治理系統時，應將利益相關者之需求轉變成機構目標，並發展連結目標（alignment objectives），確保 IT 方面的努力與業務目標接軌，以 IT 達成治理及管理目標。

在績效管理方面，COBIT 2019 提出多項原則。例如，績效管理應 (1) 易於瞭解及使用；(2) 與 COBIT 觀念模型一致，且涵蓋所有流程及組成要素；(3) 提供可靠、可重複及攸關的結果；(4) 具有彈性，以支持不同機構的需求；以及 (5) 支持不同類型的評估（例如自行評估、正式評估或稽核）。COBIT 2019 採用能力成熟度模式整合（Capability Maturity Model - Integrated, CMMI）[10]，以評估機構 IT 治理及管理系統各項流程與其他組成要素的能力水準以及成熟度。治理及管理目標之相關流程運作的能力水準係以上述 CMMI 機制衡量，其水準值爲 0 至 5。組織結構能力水準則通常根據事先設定的標準予以衡量，符合部分標準者，列爲低能力水準；符合全部標準者，列入高能力水準。此外，資訊項目通常爲相關流程的產出，其衡量係參照 COBIT 的資訊參考模型（information reference model）。該模型界定三項主要的資訊品質標準：眞實（intrinsic）、符合情境（contextual）及安全 / 隱私 / 可及性（security/privacy/accessibility）以及 15 項子標準（sub-standards），如附表所示。資訊項目可根據其符合該表列示之品質標準的程度，予以評估。

整體而言，COBIT 2019 提供一套可供機構用於發展、運作與評估 IT 治理及管理系統的架構及相關指引。ISACA 特別指出，這套架構與相關的標

附表　資訊參考模型：資訊品質標準

主要標準（main standards）	子標準（sub-standards）
眞實（intrinsic）	正確性（accuracy）
	客觀性（objectivity）
	可信度（believability）
	信譽（reputation）
符合情境（contextual）	攸關性（relevance）
	完整性（completeness）
	及時更新（currency）
	適量（appropriate volume）
	精簡表達（concise representation）
	一致表達（consistent representation）
	可解釋性（interpretability）
	可瞭解性（understandability）
	易於操作（ease of manipulation）
安全 / 隱私 / 可及性（security/privacy/accessibility）	可用性（availability）
	限制存取（restricted access）

資料來源：ISACA(2018) COBIT® 2019 Framework: Introduction and Methodology, p.42。

準、架構及 / 或法規接軌。因此，機構可利用 COBIT 2019 建構及維護其 IT 治理及管理系統，同時遵循相關的標準及法規。

二、IT 治理之稽核

機構應定期評估 IT 治理及管理系統運作之效能，以確保其足以達成 IT 治理及管理目標，爲機構增加價值。根據「國際專業實務架構（International Professional Practice Framework, IPPF）」，" 內部稽核爲獨立、客觀之確認性服務及諮詢服務，用以增加價值及改善機構營運。內部稽核協助機構透過有系統及有紀律之方法，評估及改善風險管理、控制及治理過程之效果，以達成機構目標。"[11]，確認性服務 " 爲獨立評估機構之治理、風險管理及控制過程，而對證據加以客觀檢查，可能包括財務、績效、遵循、系統安全及審愼性檢查等專案。" 因此，IT 治理及管理系統之評估應由內部稽核單位執行，以確認該系統效能及目標達成之程度。

內部稽核人員查核 IT 治理及管理系統時，應確認其是否正常運作，且能達成 IT 治理及管理目標。例如，管理目標 "DSS04 －已管理之持續性 " 要求機構在面對重大的中斷（disruption）時，快速因應、持續業務運作，以及將各項資源及資訊之可用性維持在可接受的水準。面對新冠肺炎疫情，各國政府及企業之運作受到嚴重衝擊，不無中斷之虞。爲避免疫情散播，各國政府實施邊境管制、封城、居家隔離、居家檢疫等措施，導致機構人員無法正常上班、差旅及執行業務，其原有的災害復原及業務持續計畫通常不足以因應此種全面性的中斷。在此種環境下，機構面臨的挑戰可能包含 (1) 缺乏支持遠端工作之員工所需的技術及設備、(2) 虛擬私人網路存取時間的延遲、(3) 視訊會議軟體授權使用人數不足、(4) 員工家中無線網路的頻寬偏低、(5) 安全及隱私規範必須修訂、(6) 供應鏈緊繃、(7) 通訊延遲，以及 (8) 生產力下降。機構必須適當的因應這些挑戰，以確保業務目標之達成[12]。

爲確保業務持續運作，提升組織韌性，機構應聚焦於員工、顧客與夥伴、組織內財務及營運以及社群關係四個構面，採取積極的行動，以因應新冠肺炎疫情危機[13]。許多機構採取異地分區上班、居家上班、遠距上班、工作調整等方式因應，因而衍生新增的 IT 需求及風險，例如遠端存取的資訊安全、IT 基礎架構（包含電腦硬體、軟體、資料庫、網路及通訊設備等）的調整、雲端平台的使用等。內部稽核單位應評估這些改變對於 IT 治理及管理系統帶來的影響，並確認其風險已獲得適當的評估及管理。

內部稽核人員辨識新冠肺炎主要風險及評估機構之相關回應時，應考量不同的面向，例如通訊（telecommunications）、人員及組織風險、流程風險、供應鏈及外包風險、系統及安全風險等。在通訊方面，內部稽核人員應了解 (1) 遠端工作是否影響員工士氣及生產力？(2) 選擇遠端工作的員工能否取得所需的設備？以及 (3) 視訊會議軟體授權使用人數是否足

夠？就系統及安全風險而言，內部稽核人員應了解 (1) 大多數員工遠端工作帶來哪些安全風險？ (2) 針對員工攜帶外出的設備有哪些控制？ (3) 遠端工作的員工能否使用重要的設備及技術，以完成其工作？ (4) 員工需要遠端存取哪些重要或敏感的資訊？以何種方式存取？以及 (5) 機構有哪些用於保護資訊的控制措施[14]？內部稽核人員應接著評估機構的業務持續計畫，確認能否有效因應相關的風險，並根據查核結果，提出改善建議，且追蹤業務持續計畫更新及執行情形，以確保此項 IT 管理目標之達成。

肆、結語

新冠肺炎疫情方興未艾，嚴重衝擊各國政府與企業的運作。我國政府超前部署及因應此項疫情，企業及民眾全力支持與配合，防疫成效良好，深獲國際肯定。然而各國防疫作為及效果不一，導致疫情難於短期內緩解，無論政府或企業都應有長期防疫之心理準備及作為。

隨著 IT 的迅速發展，政府應善用 IT 推展政務，以提供便捷、優質的公共服務。政府機構應建立適當的 IT 治理及管理系統，以確保業務持續，並達成電子化政府的目標。本文簡介之 COBIT 2019 架構與 IT 治理稽核，可作為政府推動 IT 治理的參考。至於 IT 治理的實施過程及方法，則可參考相關的細部指引。

註釋

1. 聯合報（2020），抗新冠肺炎 臺灣防疫決策贏在哪裡？
2. United Nations（2003）. World Public Sector Report 2003: E-government at the Crossroads.
3. World Bank（2015）. "e-Government." .
4. ISACA（2018）. COBIT(r) 2019 Framework: Introduction and Methodology. p.11-12.
5. 同上。
6. 同上 p.13&15。
7. 同上 p.17-18。
8. 同上 p.19-20。
9. 同上 p.21。
10. CMMI 可支援整合不同專業領域之特定能力成熟度模式及相關產品，以持續改善軟體工程、系統工程之專業領域及整合性產品與流程發展。
11. 中華民國內部稽核協會(2017)，國際專業實務架構，p.35。
12. AuditBoard (2020). COVID-19 Response Strategy: Evolving Internal Audit Practices for Success. p.4.
13. 游復興（2020），IBM 觀點：企業因應新冠肺炎之應對措施。
14. AuditBoard（2020）. COVID-19 Response Strategy: Evolving Internal Audit Practices for Success. p.5.

參考文獻

1. 中華民國內部稽核協會（2017），國際專業實務架構。
2. 游復興（2020），IBM 觀點：企業因應新冠肺炎之應對措施。
3. 聯合報（2020），抗新冠肺炎，臺灣防疫決策贏在哪裡？。
4. AuditBoard（2020）. COVID-19 Response Strategy: Evolving Internal Audit Practices for Success.
5. ISACA（2018）.COBIT® 2019 Framework: Introduction and Methodology.
6. United Nations（2003）. World Public Sector Report 2003: E-government at the Crossroads.
7. World Bank（2015）. "e-Government". https://www.worldbank.org/en/topic/digitaldevelopment/brief/e-government.❖