Feature

基於 COBIT 5®的 IT 政策架構
IT Policy Framework Based on COBIT 5®

作者:**Jorge Carrillo, Ph.D., CISA,CISM, CISSP,** is an IT security and IT audit professional with experience in developing IT policy and risk management processes. Carrillo is a lecturer at Prague College (Czech Rebublic).

譯者: 邵之美, CISA, ISO27001 LA 中華民國電腦稽核協會 教育訓練委員會副主委

隱私權與 IT 政策有許多相同之處：兩者都很重要；組織很重視有沒有這兩項；但不是每一個人都完全瞭解這兩項如果被誤解所牽連的問題與後果。隱私權與 IT 政策是不斷演進的觀念—今天能被接受的政策（或者是被考慮為一個隱私權的顧慮），在明天可能不是一個滿意的實務了。相同的，COBIT 也在 1996 年從一個稽核架構演進到 2012 年成為一個企業 IT 的治理與管理（GEIT）架構。在其他方面之中，它呈現出政策是影響正確治理與管理 IT 的根本要素。

本文將介紹一個使用 COBIT5 原則來設計政策架構的現代作法，它提供一個健全且系統化的作法，以確保這政策能被用來做為建置企業策略的工具。政策架構是一個提供組合及定義策略的邏輯性結構，它同時也建立能支持實施與執行政策的其他文件。

本文的目的在提供一個結構化的方法論，用來協助組織發展並建置一個有效果的政策架構。

IT 政策的演進

IT政策能幫助組織正確的達成組織所期望的行為、降低風險以及增進組織目標的達成，IT政策之演進可以借由比較以下兩份文件來描述：Generally Accepted Principles and Practices for Securing Information Technology Systems[1] 與 Information Security Handbook: A Guide for Managers.[2]

前者在 1996 年出版，敘述一個政策應該在其他方面之中，對特定的相關制度定義及詳述其規則。而後者在 2006 年出版，以資訊安全為觀點，定義政策是一個指令、規則與實務的集合，它規定組織如何管理、保護、以及散布資訊。

在 1996 年，IT 應用系統與基礎架構的組態及標準是優先事項。而 10 年之後，組織了解到要取得 IT 的優勢，必須有正確的資訊資源管理與治理。

更進一步來說，若無法設計與建置健全的企業流程，很明顯的將很快的置以科技為基礎的控制於無效。舉例來說，Verizon 2011 Payment Card Industry Compliance報告[3]指出，尚未符合 Payment Card Industry Data Security Standard（PCI DSS）第12項需求（維護安全政策）的組織，對其他的PCI需求也無法推動其實務及成功的建置。

IT 政策的挑戰

在變動的環境中創設IT政策不是一個簡單直接但卻經常是一個必需的工作，組織可能不全然喜歡新科技的優點、限制以及風險因素。舉例來說，選擇雲端運算的解決方案，在一個充滿不確定性的環境之下，須要

對所牽涉的風險加以管理，以及對命令授以權力才能產生商業價值。

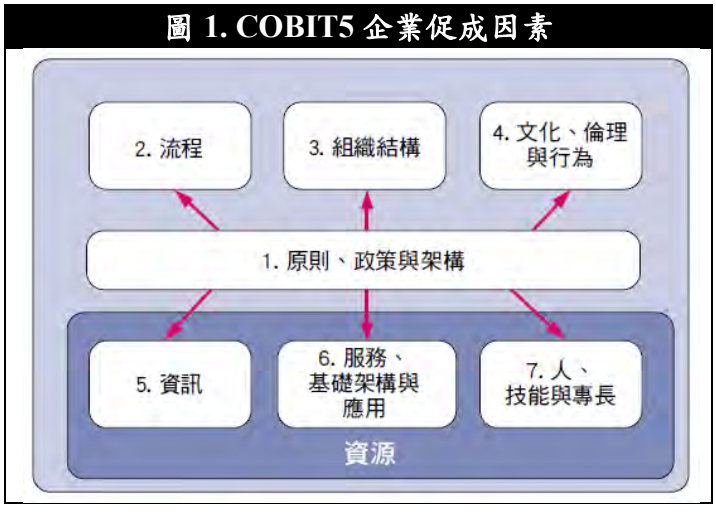
IT 政策不只是 IT 的活動，把 IT 原則從頭到底結合企業流程，可以確保更佳的跨企業涵蓋面與合作（即：明確訂定責任與權力）、減少跨不同團隊的重疊控制，以及針對企業需求提供一致性的作法。

最後如同在 Information Security Management Handbook 中所述，任何企業的核心是它的『人』－它們的個別屬性包含正直、道德價值、以及能力。[4] 因此，政策應該要對每一個人溝通，並被了解、支持及接受。否則他們便是沒有意義的。

政策是促成因素

COBIT5 提出 7 個促成因素（如圖 1），它們是建置 GEIT[5] 的支持工具。促成因素『1. 原則、政策與架構』的四個構面（利害關係人、目標、生命周期、以及最佳實務）將在以下的章節討論，同時並對設計與建置一個政策架構的系統化方法提供建議。

圖 1. COBIT5 企業促成因素



COBIT 5®確保政策架構符合利害關係人的需要、涵蓋各層面的流程（不是只有 IT 功能）、並且建立額外的文件以確保達成治理與管理的目標與活動。

利害關係人構面

某些利害關係人是定義與設定政策原則，而其他的則是遵守、信奉或是建置這些原則。

這些定義與設定政策原則的第一組利害關係人，考量組織一般的治理原則，並分析與辨別內部、外部因素（如：法規）、企業的方向、以及組織的文化。組織的董事會與高階管理階層屬於這一組，另外，他們對於指出方向、溝通與建置治理目標、以及定義政策架構的核心元件負有可歸之責任。一個政策架構的核心元件有：

- 對有權核准政策以及其相關職責人員的任命權
- 對沒有遵循既定政策之後果的決定權
- 定義處理政策例外情形的流程
- 定義衡量與監控政策遵循情形的方法定義政策的範圍以及必須遵守政策的利害關係人。

透過遵守政策的原則，可以降低其他利害關係人的恐懼、不穩定感以及懷疑。

目標構面

目標是根據先前已定義的政策原則所做的聲明，它描述所期望的成果。目標聲明的例子如：

- 做為員工認識新環境的工具
- 紀錄正確的委任關係並定義權力與職責的限度
- 做為遵循法規的文件根源
- 保護智慧財產及營運持續
- 改進專案與營運的透明度與動能

就政策的關係，目標與政策原則應該是相互關連的，如此才能針對利害關係人的需求提供保證。

生命週期構面

政策的生命週期組合了政策原則與前面定義

的目標，並且包含以下的階段：

- 規劃－本階段以涵蓋前面已定義的利害關係人與目標兩個構面，來建立一個政策架構的基礎。通常組織內已經有一些政策存在，所以驗明治理原則與現有政策之間的差異，使妥當的政策有助於重新設計與改進規行的政策架構。在此階段中，將會定義能支持與闡明政策原則的一個文件邏輯結構，文件的最佳數量則視組織的文化與管理風格而定，這個活動的目的是要改進政策原則的透明度並支持它們的建置。
- 設計－本階段有兩個活動：

  1. 設定優先順序－驗明具體政策、針對政策原則使用以風險為基礎的方式、設定檢討或創立的時限與優先順序。
  2. 定義政策架構－書寫政策不是只有撰寫活動，它須要充分的協調包含：

     - 政策起草－驗明研究和書寫政策人員的職責。其中一個成功關鍵因素是；要解決建置政策原則可行性的所有的潛在問題。
     - 政策評論－驗明負責提供獨立評論的人員，本活動的目的在提高政策的可信度與品質。
     - 核准、溝通及散播－建立程序為從先前利害關係人構面中所定義的授權人員獲得對政策的最終核准，並且決定政策的溝通與訓練策略。
     - 風格－定義書寫的品質標準，包含文件格式、字型種類、語言風格、辭彙解釋、以及文件結構。本項活動的目的是確保政策的書寫、呈現，及結構在一個清楚、具體、完整、一致、以及容易遵守的方式之下。

- 建置－本活動相當於施行及執行政策，定義能協助組織從不符合狀態，簡明的轉換成符合狀態的活動。
- 營運－一個有效的政策應該是組織 DNA 的一部分。建立可歸責的文化，以及在日常運作中使用政策，能確保組織的目標被達成。在這階段，組織應該說到做到政策的原則。
- 評估/監督－這階段有目的的去確認政策需求是被正確的建置，以及組織是有效的運作的。支持企業目標之政策原則的成功之程度要被評鑑，並且政策架構的整體效率要向有關的利害關係人溝通。
- 更新/處置－為保持政策與企業方向一致，政策要被覆審以更新或處置。

這項活動有兩個目的：確保組織擁有的是有效的政策，以及調整前面所定義的階段以維持或改進政策架構的成熟度。好的實務會要求定期覆審政策，通常是每 12 個月。

最佳實務構面

將治理與管理活動區隔開，指出如何建置及管理政策是須要夠明確的指引。一個好的實務是能產生支持政策效果與效率的，更多的文件[6.7.8]，舉例：

- 標準－一個必要的行動、明確的規則、控制或組態設定，其設計是為支持及符合一個政策。一個標準應包括硬體、軟體或行為的已被接受的規格，而讓政策更有意義與效果。標準是經常應該指向它們所關連的政策。
- 程序－是透過特定、指定行動來執行政策的一組書面步驟，他與政策的關係是『如何做』。程序傾向比政策更詳細，對於如何絲毫不差的完成一個想要的任務、達成期望的商業或功能成果、以及執行政策，它們在一系列的步驟中辨明其方法與狀態。
- 準則－為陳述指引的概要，這是支持政策、標準與程序的附加(非強制性的)文件－對於像『在特殊情況下如何處理』這種問題的一般性指示。這些不是應該要符合的需求，但卻是強烈建議要的。
- 基線－是一個被業界廣為接收，對一個特有

的建置提供最有效的方式。

結論

所有組織都有指導如何做決策與如何達成企業目的政策，一個有效果的政策架構可以提升組織的可歸責性透明度，並且是幫助組織達成其目的的基礎。

創建政策不是只把一些文字打在頁面上，它牽涉一個系統化的做法，以正確的形成治理與管理原則。COBIT 5® 的原則有助於提供一個整體的做法，以包含一個政策架構的最低需求，且能避免推翻重來，並確保一個政策的完整生命週期能被充分了解。

ENDNOTES

1. *Swanson, Marianne; Barbara Guttman; SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996, http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf*
2. *Bowen, Pauline; Jan Hash; SP 800-100, Information Security Handbook: A Guide for Managers, October 2006, htt6p://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf*
3. *The Verizon PCI and RISK Intelligence Teams, Verizon 2011 Payment Card Industry Compliance Report, 2011, www.verizonbusiness.com/resources/reports/rp_2011-payment-card-industry-compliance-report_en_xg.pdf*
4. *Tipton, Harold F.; Micki Krause; Information Security Management Handbook, 6th Edition, 2007*
5. *ISACA, COBIT 5®, USA, 2012, www.isaca.org/cobit5*
6. *Bacik, Sandy; Building an Effective Information Security Policy Architecture, CRC Press, USA, 2008*
7. *Op cit, Tipton*
8. *Writing, Stephen B.; Exceptional Policies and Procedures, Process Improvement Publishing, USA, 2009*