屏科大 National Pingtung University of Science and Technology

雲端運算服務風險治理模型

許文西
國立屏東科技大學企業管理系 副教授
信箱：hsuw@mail.npust.edu.tw
電話：(08)770-3202#7698

摘要

近年來，雲端運算服務(Cloud Computing Service)被公司或組織採用已快速的飆升。然而，雲端運算服務存在著許多的風險，主要的風險來自於雲端運算服務的安全風險，失去控制的風險和管理不當的風險。

本文針對雲端運算服務所面臨的風險，提出一個雲端運算服務風險治理模型。這個治理模型提供了有效的方針，讓使用者了解到企業應如何治理他們雲端運算服務和相關的風險。一個適當的雲端運算治理模式，將可以幫助組織去確認雲端治理環境的安全和遵守所有相關組織資訊科技政策，並且最終將提升企業的績效表現。

一、前言

雲端運算服務是一種根據需求提供服務的模式，企業通常將雲端服務委外或者自行提供雲端服務平台[4]。根據一項針對50個國家的2,014位資訊長(Chief Information Officers, CIOs)的調查，3%的資訊長回應，在2011年，他們公司大部分的資訊科技(Information Technology, IT)已經在雲端執行。43%的公司也計劃將他們公司的資訊科技於2015年在雲端執行[2]。雲端運算快速的成長，已成為一個重要的資訊平台，提供企業一個更節省成本的模式去處理他們每日電腦的需求和實現企業的目標。

雲端運算服務提供公司許多潛在利益。然而，在雲端環境有很多安全的風險可能影響公司策略。當雲端運算服務持續成長，需要更多的治理策略，一個良好的治理模型將變得更重要，有效的雲端運算服務治理模式有利於公司的運作。

根據全球資訊系統稽核與控制協會(Information System Audit and Control Association. ISACA)所發布的指導方針「雲端運算資訊技術控制目標：雲端控制和雲端確保(IT Control objectives for Cloud Computing: Controls and Assurance in the Cloud)」指出，為了從雲端運算服務獲得更多的利益，公司需要發展一個清楚的治理策略和管理計劃，用來設定雲端治理的方向和目標。[2][8]

本文主要建構一個端運算服務治理模式，提供企業組織了解如何治理他們的雲端運算服務應用和有關的風險。主要目的是提供對於雲端運算服務有更深一層的認識，包括雲端運算服務的風險及管控，並進而建構一個有效的治理機制與模式。

本文其餘部分分列如下：第二個部分概述雲端運算的特徵和它的利益及風險。第三部分建構一個雲端運算服務治理模型。最後一個部分是結論。

二、雲端運算的概述

美國國家標準和技術研究機構(National Institute of Standards and Technology, NIST)將雲端運算定義為：一個共用的可配置的運算資源（例如網路、伺服器、儲存、應用程式和服務等），可按不同的網路需求，快速發佈和配置雲端資源的分享空間的模式。雲端運算技術可以在各種的體系結構下，以不同的服務方式和部署模式執行[7]。雲端運算模型是由三個服務模型和四個部署模式所組成，詳述如下[2][3][7]。

A.雲端運算服務模式

雲端運算服務可分為三種傳遞模式：應用軟體雲端服務(Software as a Service, SaaS)，平台雲端服務(Platform as a Service, PaaS)，基礎設施雲端服務(Infrastructure as a Servie, IaaS)，如圖1，每個模式為客戶提供了不同的雲端服務。

圖1.雲端運算服務模式

1.應用軟體雲端服務(Software as a Service, SaaS)：

應用軟體雲端服務(SaaS)提供了客戶使用雲端服務提供者 (Cloud Service Provider, CSP)所建構的雲端基礎架構上運行的各種應用程式。服務提供者提供給使用者隨選且完整的應用程式，客戶可在自己的電腦設備上透過網路使用雲端上的程式，如Web瀏覽器（例如：網路的電子郵件），但無法對其進行調整，只能在操作介面外觀與工作流程的設定上做少許的改變。SaaS 服務提供者，較知名的有：FACEBOOK 、G-MAIL™ 、Yahoo® 、Google Docs 和 Microsoft線上服務等。

2. 平台雲端服務 (Platform as a Service, PaaS)

平台雲端服務(PaaS)提供客戶建置或部署應用程式到雲端基礎設施，藉由提供者來應用及創造可用的程式語言、程式庫、伺服器和支持的工具。PaaS 供應商為客戶提供了以服務為主的體系架構應用程式構造區塊，讓使用者可以在平台上自行編寫開發新的應用程式。PaaS 使用者具有對部署的應用程式和應用程式主控環境的配置控制權，但省去硬體設施維護成本。PaaS 提供雲端服務平台的例子有微軟的 Azure™ 服務平臺，谷歌的Google App Engine 等。

3. 基礎設施雲端服務(Infrastructure as a Service, IaaS)

基礎設施雲端服務(IaaS) 提供客戶企業內部所需的IT基礎架構去部署和運行任意的軟體，包括伺服器、作業系統和應用程式[7]處理系統、 儲存資源、 網路和其他基本的雲端運算資源。IaaS 提供線上處理或資料存儲能力。客戶不需管理底層的雲端基礎架構，但能掌握作業系統、儲存、網路以及所部署的應用程式，IaaS 較適合企業具有很大的資料儲存，一次性處理要求的企業 [2][3]。亞馬遜(Amazon) 的 Amazon Web Services™ 是IaaS服務提供的一個例子。

上面提到的雲端服務模型都有其不同程度的經營風險。企業需要建立自己的雲端運算服務治理模型，以確保雲端運算在一個安全的環境裡運行。

B. 雲端運算配置模式 (Cloud Computing Deployment Models)

上面提到的三種雲端運算服務模式是以下列四種配置方式提供雲端服務給客戶：私有雲(Private Cloud)，公有雲(public Cloud)，社區雲(Community Cloud)和混合雲(Hybrid Cloud)，如圖2。

圖2.雲端運算配置模式

雲端運算配置模式依照服務的對象及需求不同，以不同的配置方式來傳遞服務給消費者。公有雲是將雲端運算資源提供給一般民眾。私有雲是只為單一特定組織或企業運作，雲端基礎設施不對公眾開放，私有雲服務讓供應者及使用者更能掌控雲端基礎架構，提供更具安全性的雲端環境。社區雲是界於公有雲和私有雲之間，由一群特定群體共享雲端服務及設施。可有兩個或兩個以上具有雲端服務需求的組織組成一個社群、社群成員共同使用雲端資料及應用程式。混合雲則是比其他配置模式更複雜，因為此一模式涉及的組合模型中允許在同一時間使用兩個或兩個以上雲端運算配置模式(結合公有雲、私有雲或社區雲），在此混合雲模式中之企業或組織之資料數據和應用程式可以共享，但又各自保有其獨立性[1][3][7]。

三、雲端運算服務治理模式

隨著安隆公司破產，公司治理在全球和世界各地備受關注並且在世界各地成為董事會關注的重點[10]。而在現代的企業運作中，雲端運算無疑的可望發揮關鍵作用，幫助企業組織實現其企業目標，然而，企業雲端環境中也產生監管和經營風險，因為企業的資料於雲端運算服務中傳送給第三方用於存儲，處理或者支援，在雲端中，資料和資訊並非由客戶控制和監視，因此，對於保護知識產權，維護員工、客戶和第三方的資料隱私，成為雲端運算服務主要的挑戰。本研究針對雲端運算服務所面臨的風險及管理困境，將董事會的責任及企業員工教育學習融入治理模式中，提出四個階段來建立雲端運算的治理模式。

A.雲端運算治理中董事的責任及角色

最近在資訊科技治理(IT Governance)的研究中對於公司治理董事會的責任提起了高度的關注[10]，在2011年所舉行的國際性的研討會議中，資訊科技（IT）和雲端運算成為審計委員會成員的關注重點[5]。雖然雲端運算被認為是公司的一個重要課題，但Portio[11]的研究調查顯示，超過50%的IT決策者對於雲端運算了解的非常少。由於缺乏對雲端運算的了解而引發治理問題，可能使企業面臨失去競爭優勢的危險。

董事會的監控功能是組織中一個重要的治理機制[10]。董事會需要針對雲端運算服務為企業所帶來的風險進行審慎評估，並使雲端運算服務與公司的目標一致。企業在實施雲端運算時必須有充分的準備，並採取必要的控制措施。

通常情況下，董事的責任關於內部控制委託給審計委員會，該委員會是著重企業內部和外部審計的合適性及其審查與控制方面的問題。審計委員會組織應當要求公司管理當局必須關注雲端運算服務所產生的治理問題，並確保企業採取可能的因應措施，包括風險管理，災難恢復計劃，安全漏洞評估，業務連續性，突發事件回應，身份加密，存取管理和虛擬化等。以下提出雲端運算的治理模式所採取的必要的四個階段，以確保雲端運算系統中有良好的治理效能。

圖3：雲端運算治理模式

B.實施有效的雲端運算的治理模式程序

為了建立一個有效的雲端運算的治理模式，本研究提出了四個實施階段如圖3所示：

第一階段：設定雲端運算服務政策和標準

好的標準和做法，將有助於雲端治理，以建立企業雲端目標和風險的考量。因此，雲端運算治理模式第一階段，企業要建立自己的雲端運算標準和政策。這整個程序是一個持續的過程，並且是根據雲端運算的標準和政策的架構來執行。

隨著企業分配越來越多的IT預算資金在雲端運算，使得採用雲端服務的公司逐漸增加，ISACA指出[2]，重要的是，組織要能從雲端技術服務及治理中獲益。為了從雲端運算措施中獲得最大的利益，企業必須為雲端運算發展出明確的管理策略和管理計劃，設立確定的方向和目標。因此，資訊安全風險管理對雲端運算治理是一個重要的組成部分。風險管理可以幫助企業認識雲端運算的風險，使他們面臨其潛在風險時，知道如何執行相關防護措施的優先順序。

第二階段：評估雲端運算相關的風險

雲端運算要建立適當的治理機制，審計委員會應設立雲端運算政策，以評估呈現在他們公司的雲端運算環境中的風險和機會。這就面臨了一個問題，董事會的董事是否有專業知識以及能力評估公司所採用的措施或程序是適當或有效的? 為了探討組織是否符合他們的雲端運算政策和標準，並幫助董事們實現他們的IT職責，ISACA建議組織在採用雲端運算服務之前，要問以下的問題[2]：

- ●從雲端運算中組織期望要達到怎樣的層級可用性？
- ●組織的資料被存儲在哪裡？
- ●組織的資料安全是如何管理？
- ●如何執行監督和審計？
- ●如何在雲端中管理身分識別與存取？
- ●服務供應商的災難恢復能力是什麼？
- ●如何保護來自網際網路的威脅？
- ●企業期望從雲端服務供應商得到什麼類型的認證或保證？

安全問題是企業外包資訊科技的服務到雲端運算環境中的關鍵因素之一，董事會應遵守雲端運算服務治理模式，分析現有的安全和隱私選項，以確保公司在雲端環境中的安全。

第三階段：管理階層融入雲端運算治理模式

要建立適當的雲端運算治理，首席資訊長（CIO）扮演了一個重要的角色，CIO們需要履行其職責，確保公司雲端運算的運作符合公司所設立的所有準則及標準[6]。實施雲端運算服務後，企業需要定期評估企業雲端運算進行中所遇到的困難，預防威脅的政策和技術，並回反饋給負責IT治理的董事們或委員會，以研擬相關的改善措施。

第四階段：評估雲端運算服務績效

定期評估雲端運算服務的績效是很重要的，並且要定期檢視雲端運算治理模式中所依據制定的標準和政策是否和企業的目標一致。一個設計良好的雲端運算治理模式，要確保這些政策及標準和組織的策略是一致的。商業智慧（Business Intelligence ,BI） 以及平衡計分卡(Balanced Scorecards, BSC)也可以應用來設計績效指標，以評估雲端運算治理的監察效能，確保雲端運算服務滿足公司的目標或關鍵績效指標。

整個雲端運算治理模式中，組織持續的學習和教育，亦是導致有效的治理的因素之一。Tillery[9]強調，最大的IT安全威脅並不是因為雲端運算本身，而是在保護公司的資料中不足的IT安全政策和缺乏教育員工的角色。因此，教育員工關於雲端運算相關的風險和治理過程中是很重要的，而且應該開始從整個組織的底部到頂部作為一個不斷學習的過程。 管理者的責任在於延伸雲端治理模型擴展到整個組織，藉由教育員工到雲端運算實踐的政策和標準。

四、結論

雲端運算技術可以運用在各種各樣的架構，透過不同的傳遞服務模式和配置形式而提供。雲端運算的安全風險所不在，然而雲端運算亦提供企業一個新的契機。因此，企業需要制定一個雲端運算服務治理模式。

本研究提出一個經由四個階段建立雲端運算治理模式。隨著雲端運算應用的擴大，益增其對企業日常運營的重要性，企業應了解如何以最佳方式處理雲端運算服務模式所帶來的挑戰，如此才能使企業蒙受雲端運算服務所帶來的最大的益處，也免於安全風險的威脅。

董事會需要了解和監控他們的公司的雲端策略。在參與雲端運算服務治理模式中，不斷的學習和雲端運算治理教育是必要的，也是實施一個雲端運算的治理模式成功與否的關鍵因素之一。公司了解雲端運算的影響並能獲取必要措施，設置適當的安全政策，將能減少與雲端有關的安全風險。

參考文獻

[1]R. Farrell, 2010, “Securing the cloud-governance, risk and compliance issues reign supreme,” Information Security Journal: A Global Perspective, 19, pp. 310-319.

[2]ISACA (Information Systems Audit and Control Association), 2011, IT control objectives for cloud computing: controls and assurance in the cloud, ISACA.

[3]W. Jansen, and T. Grance, 2011, Guidelines on security and privacy in public cloud computing, National Institute of Standards and Technology (NIST), Department of Commerce, USA. NIST Special Publication 800-144 (http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494).

[4]J. Kobielus, 2009, “Storm clouds ahead: SOA governance clashes with cloud computing model,” Network World, 26(9), pp. 24-28.

[5]M. P. McCarthy and S. Hill, 2011, “Cloud adoption points to IT risk and data governance challenges,” NACD Directorship, April/May, p. 72.

[6]C. R. McClure and J.C. Bertot, 2000, “The Chief Information Officer (CIO): Assessing its impact,” Government Information Quarterly, 17(1), pp. 7-12.

[7]P. Mell and T. Grance, 2011, The NIST definition of cloud computing, Special Publication 800-145, National Institute of Standards and Technology, September, <URL: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf >.

[8]S. Steffee, 2011, “Cloud computing governance remains elusive,” Internal Auditor, 68(5), p.14.

[9]S. Tillery, 2010, “How safe is the cloud?” Baseline, September/October, p.15.

[10]G. Trites, 2004, “Director responsibility for IT governance,” International Journal of Accounting Information Systems, 5, pp. 89-99.

[11]P. Williams, 2009, “Governance in the cloud: head in the sand? Computer Weekly, 12/8.