# 雲端風險管理

## 商業領導者的首要考量

# Managing Cloud Risk

## Top Considerations for Business Leaders

**作者: Phil Zongo,**

Is a cybersecurity consultant based in Sydney, Australia. He has more than 10 years of technology risk consulting and governance experience working with leading management consulting firms and large financial institutions. He recently led a successful risk assessment initiative for a complex, multimillion-dollar cloud transformation program.

**譯者: 徐立群,** 國立成功大學會計學系,教授、電腦稽核協會 編譯出版委員會委員

雲端運用以迅速的步伐持續成長，改變全球商業。美國訊息系統審計與控制協會(ISACA®) 創新洞見報告[1]中引用雲端計算作為引導商業策略的主要商業趨勢。且雲端運算也在十大最有可能提供重大商業價值新興科技中排名第三。而大數據分析與行動科技分別名列第一與第二，國際數據資訊(IDC)預測全球雲端使用量，在未來的五年將會有19.4%的成長，從2015年約700億美元增加到2019年的1410億美元，將近成長了一倍。這幾乎是企業IT整體支出增長的六倍[2]。

雖然雲端有著重大的利益，包括增強財務靈活性，以及提高敏捷性和獲得領先技術，但有些組織仍然不使用，主要是擔心失去對高價值資訊的控制。這些風險擔憂是合理的，如果不適當考慮和管理這些風險，可能會導致不利的業務影響，包括客戶體驗退化，敏感的數據外洩或品牌形象受損。

本文章提供了一些實際建議，以解決採用雲端的相關風險，包含三個關鍵領域：

1. 雲端計劃不符合商業策略。
2. 失去對高價值訊息的控制。
3. 過度依賴雲端服務提供者。

但這些並不是企業在採用雲端計算時會遭遇到的所有風險。一些組織提供幾個框架，特別是雲端安全聯盟（CSA），美國訊息系統審計與控制協會（ISACA®）和美國國家標準與技術研究所（NIST），為管理雲端風險提供了更全面的指導。

### 將雲端計算與商業策略整合

企業通過承擔風險提供股東價值，但風險未明確理解和有效管理而導致失敗。為了提供商業價值並最小化風險，這些雲端計畫應與商業計畫完全一致。董事會或相關風險管理委員會的積極參與和監督是雲端計劃成功的先決條件。

在2012年6月的"雲端計算企業風險管理"[3]中，贊助組織委員會強調(COSO)，雲端風險管理的責任為最重要。該文件指出"雲端計算應在組織的總體治理活動中被考慮，並被認為是一個需要組織董事會進行討論和調查的話題"。董事會應根據企業目標，風險偏好和能力來確定雲端服務適合企業。但事實並非總是如此。

澳洲審慎監理署(ARPA)在2015年7月發布的雲端資訊文件[4]中提出了一個議題，即受監管個體向董事會（BoD）報告的雲端主要集中在利益上，但對於相關風險卻不能提供足夠的可見度。有效的雲端風險管理需要董事會針對偏好和商業策略有著充足的風險措施。為此，應提供相關資訊，包括：

- 雲端價值主張，可追溯的商業策略連結以及如何衡量效益。
- 最重要的業務風險和處理策略，數據安全，隱私法律，數據位置，業務彈性，合法性。
- 建議的雲端部署模式：公共、私有或混合以及相關的風險影響。
- 計劃雲端服務傳遞模式：軟體即服務（SaaS），平台即服務（PaaS）或基礎設施即服務（IaaS）以及涉及到的相關的風險。
- 服務提供商選擇標準，包括財務可行性，運營穩定性和網絡安全能力。
- 合理中斷業務的情況和復原計劃。
- 服務層級協議（SLA），事件回應和運營管理。
- 第三方認證，滲透測試，漏洞評估和審核權限條款。

雲端計劃應從確定企業問題和策略目標開始，然後制定特定企業需求的解決方案。很明顯的，持續的傳達雲端價值和風險管理方法對於獲得企業對雲端計劃的信任並獲得最終成功是至關重要的。

## 保護高價值的資訊

在不限制企業創新和靈活性的情況下管理網絡風險有相當重要的企業必要性。儘管雲端提供商持續大力投入安全性能，但對資料安全性和法規遵從仍然是採用雲端會關注的主要障礙之一。2015年，經濟學人智庫與IBM合作，進行了全球雲端發展度研究。這個多方面研究的結果反映了784個利害關係人（包括董事會成員，執行長[CEOs]，財務長[CFOs]，資訊長[CIOs]和其他首席級管理者[C-level executives]）的觀點，顯示在未來三年採用雲端最有可能發生負面影響的是資料安全性，也代表了一些管理人尚未確信雲端安全。特別是這些擔憂因為公用雲要素的新風險進一步加劇：[5]

- 多租戶—多個雲端客戶共享計算能力，存儲空間和網絡。 雖然這種模式讓雲端提供商得以實現規模經濟和降低服務成本，但單一漏洞或錯誤配置可能會導致波及至多客戶的風險增加。
- 分擔責任—將商業應用程式遷移到雲端創建了雲端客戶和服務提供商之間共同承擔責任的模式。客戶讓與一些關鍵責任給服務提供商，例如實體存取和基礎架構管理。

歐洲網絡和訊息安全機構（ENISA）表示，雲端集結大量的資源和數據，為網絡犯罪提供了更多的具吸引力的目標。[6]此外，安全漏洞佔據了更大的媒體報導篇幅，他們放大了這類事件的影響。廣泛的媒體報導 2014 年蘋果發生了外洩了名人的照片的雲端漏洞，說明了這一點。

有三個關鍵的安全控制來保護雲端中具有的高價值的訊息：訊息分類，加密和特權存取管理。

## 識別高價值的資訊

資訊分類是建立有效的雲端安全控制環境的重要一步。資訊擁有者應根據企業風險進行評估和分類資訊資產。這免除了不必要的安全性支出，因為挹注更多的資源來保護‘皇冠珠寶’。

不同組織資訊的關鍵程度有所不同，具體取決於行業或企業目標。 例如，保險公司可能關注客戶健康訊息的隱私性，而高科技公司可能會擔心其產品開發計劃的安全性。

同時還應考慮對網絡犯罪分子具有高價值的訊息。在 2014 年 9 月路透社的一篇文章指出，現今在黑市中，醫療資訊比信用卡卡號的價值高出 10 倍，也被越來越多的網絡犯罪分子視為犯罪目標，[7]其他被網絡犯罪分子鎖定的高價值資訊包括商業計畫書，定價模型，合夥協議，企業管理人員電子郵件和個人財務記錄。

如圖 1 所示，分級的資訊使企業的領導者能夠明智的決定出其追求創新所願意承擔的風險是多少。例如，一個組織可能不希望在公共雲系統中託管高度機密的資訊，但是有興趣利用公共雲系統託管公共資訊。

## 隔離高價值資訊

資料分類後，企業可能會考慮使用私有雲來隔離高價值的應用。歸企業擁有和管理虛擬環境的私有雲提供了實現雲端的優勢的機會，同時也消除了多租戶和分擔責任的問題。以前，由於設置成本高昂，某些組織不願設置私有雲。Verizon 2016 的“市場狀態 - 企業雲報告”揭露，私有雲的成本正在下降，為組織提供更安全、更具成本效益的環境來承載高價值系統。[8]

## 加密敏感資料

根據 CSA 2012 年 9 月出版的雲端加密－SecaaS 實施指南，類別 8[9]，加密與加密後密鑰的保護是最有效的資料保護控制。在雲端託管高價值資訊時應先經過加密，以盡可能地減少未經授權的洩漏風險。強大的密鑰管理至關重要，因為密鑰的遺失可能導致資料的遺失。在雲端實施加密時，應考慮以下建議：

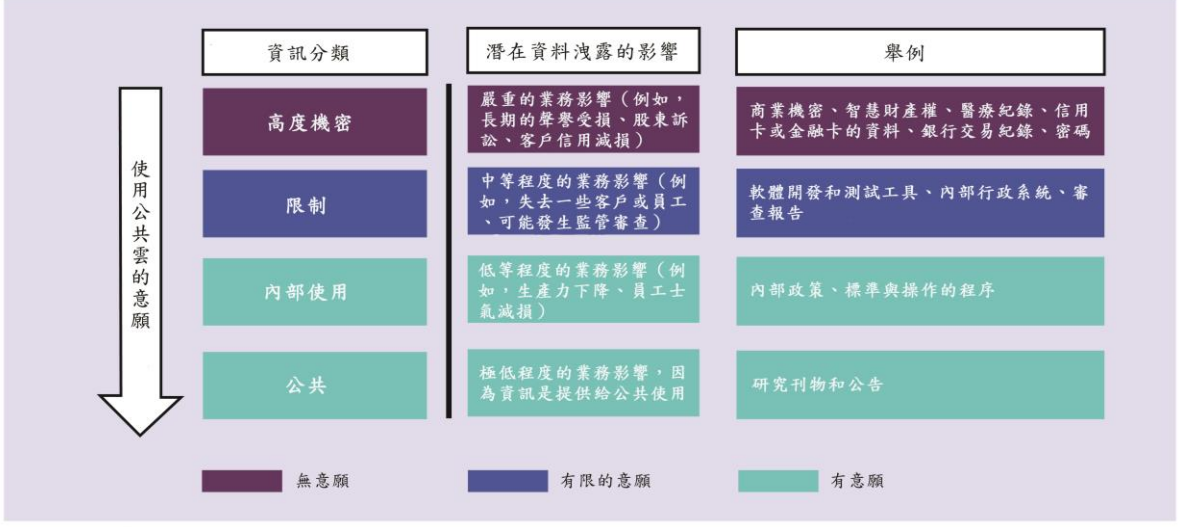
- 實施嚴格的控制來保護密鑰，包括密鑰生命週期的管理方針。 NIST 特刊 800-57[10] 第 1,2 和 3 部分提供了更詳細的密鑰管理指南。
- 確保雲端加密服務包括災難恢復和故障轉移功能，以減少密鑰丟失時的商業影響。
- 制定管理密鑰的職責。保留密鑰管理以減輕服務提供商的特權用戶對供應商的外部違約或惡意攻擊。
- 測試以確認資料庫加密不會對應用程式的性能產生不良的影響。
- 當資料從雲端存儲空間中被刪除，就要實行清除資料的控制。
- 補足資料加密的完整性保護，如數字簽名，以維護資料的真實性。

## 在高權限存取中部署強大的控制權

管理權限存取對於在雲端保護資料至關重要。特權帳戶一直都是網絡犯罪分子想要攻擊的媒介，因為它們可以無限制地存取高價值應用程式和資料。CSA 2016 年 2 月出版的“詭詐十二：2016 年雲端計算的最高等級威脅”[11] 中確認帳戶劫持是最高等級的雲端安全威脅之一，其中通常包含被盜用憑證。雲端計算的動態性質通過多種方式擴大了現有的特權用戶風險，其中包括：

- 某些雲端存取的角色風險極高，甚至有可能

圖 1－雲端採用的資訊分類 （舉例說明）




Source: Phil Zongo. Reprinted with permission.

使整個雲端環境被迫停工。

- 共享責任模型意味著，雲端服務管理員有權存取模型中組織的基礎架構、應用程式或資料庫。這會增加被攻擊的標的。
- 快速且無縫地提供新的虛擬伺服器會迅速向環境中引入新的授權帳戶。這些帳戶通常使用默認密碼的方式創建，這是可被網絡犯罪分子利用的簡單目標。
- 在雲端管理員可以點擊一個按鈕來配置新的虛擬伺服器的情況下。如果繞過相關授權，可能會破壞組織的雲端業務而導致意外的開銷。

以下人員，流程和技術控制可以幫助減少這種風險：

- 確認雲端服務提供商特權訪問控制的有效性，尤其是針對招聘和系統管理員的疏忽。
- 實施高難度密碼並自動執行安全策略配置。
- 對高影響力的活動實施雙因素認證和雙人治理。
- 記錄和監視對特權帳戶的訪問，包括執行高影響的命令。
- 為能夠完全訪問所有雲端資源的帳戶保留超級用戶帳戶憑據。
- 使用自動密碼管理解決方案定期更換帳戶的密碼。

一些雲端服務提供商有提供一些特定的具體指導關於如何在其環境中實作。例如，Amazon Web Services（AWS）Security Blog[12] 為 AWS 中的特權帳戶管理提供了詳細的指導。

## 最大限度地減少對雲端服務提供商的依賴

提高服務可用性仍然是雲端採用的主要推動力之一。精心設計的雲端解決方案可以顯著提升服務提供商持續改進的業務彈性透過群集，複製和高可用性產品提供平台彈性。

儘管有這些改進事項，仍然會發生、影響許多個雲端服務位置的中斷。如果沒有仔細計劃，這些事件可能導致主要的供應鏈和營運中斷。

好消息是，可靠的統計數據現在可供企業評估不同供應商的雲端服務可靠性。舉例來說，Cloud Harmony 是第三方雲端供應商監控公司，它提供了基於服務可用性的雲端服務的獨立比較。

以下建議將有助於企業減輕這些罕見但影響很大的事件：

- 檢查雲端服務提供商的業務連續性計劃和災難恢復計劃，以確定它們是否符合組織的恢復目標。
- 利用多個雲端服務提供商降低供應商鎖定的風險。
- 實施高可用性雲端架構以最減化服務中斷。
- 通過定期備份和還原過程補充彈性架構，並將備份數據存儲在雲端提供商之外。
- 更新和測試組織的危機管理計劃。
- 模擬從不同災難場景的恢復，包括恢復個別應用程式、虛擬環境和整個雲端服務供應商。

企業不定期終止外包安排 - 雲端的安排也不例外。如果業績不符合要求，安全漏洞或破產等因素可能會導致合約終止。為了保持業務連續性並促進平穩過渡，組織應制定退出策略或應急計劃，將關鍵記錄遷移到備用解決方案雲端上或非雲端上。

## 結論

在適當規劃、實施和管理的情況下，雲端可以成為流程改進的主要催化劑，也是業務轉型的驅動力。雲端服務提供商正在不懈地努力提高其安全性和彈性能力。實際上，組織的現場系統可能並不比雲端安全。安全性和可靠性風險可能不會超過轉變企業戰略使用雲端的機會。基於企業戰略的雲端計算，加上強大的風險管理流程，有

可能加快業務創新，轉變客戶體驗，提高競爭優勢。

**致謝**

作者要感謝 Gina Francis，Innocent Ndoda，Kathleen Lo，Andrew Strong 和 Joe Chidwala，有助於改進這篇文章的寶貴意見。

**END NOTES**

1 ISACA, Innovation Insights: *Top Digital Trends That Affect Strategy*, USA, 2015, *www.isaca.org/Knowledge-Center/Research/Pages/isaca-innovation-insights.aspx*

2 IDC, "Worldwide Public Cloud Services Spending Forecast to Double by 2019, According to IDC," USA, 21 January 2016, *www.idc.com/getdoc.jsp?containerId=prUS40960516*

3 Chan, W.; E. Leung; H. Pili; *Enterprise Risk Management for Cloud Computing*, Committee of Sponsoring Organizations of the Treadway Commission, June 2012, *www.coso.org/documents/Cloud%20Computing%20Thought%20Paper.pdf*

4 Australian Prudential Regulation Authority, *Outsourcing Involving Shared Computing Services (Including Cloud)*, 6 July 2015, *www.apra.gov.au/AboutAPRA/Documents/Information-Paper-Outsourcing-Involving- Shared-Computing-Services.pdf*

5 The Economist Intelligence Unit, *Mapping the Cloud Maturity Curve*, IBM, 2015 *http://public.dhe.ibm.com/common/ssi/ecm/ku/en/kul12355usen/KUL12355USEN.PDF*

6 ENISA, Cloud Computing—*Benefits, Risks and Recommendations for Information Security*, Greece, December 2012, *https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks- and-recommendations-for-information-security*

7 Humer, C.; J. Finkel; 'Your Medical Record Is Worth More to Hackers Than Your Credit Card', Reuters, 24 September 2014, *www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924*

8 Verizon, State of the Market: Enterprise Cloud 2016, 2016, *www.verizonenterprise.com/ enterprise-cloud-report/*

9 Cloud Security Alliance, SecaaS Implementation Guidance, Category 8: *Encryption*, September 2012, *https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_8_Encryption_Implementation_Guidance.pdf*

10 National Institute of Standards and Technology, *Special Publication 800-57*, USA, *http://csrc.nist.gov/publications/PubsSPs.html#SP 800*

11 Cloud Security Alliance, *The Treacherous Twelve—Cloud Computing Top Threats in 2016*, USA, 2016, *https://downloads.*cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf

12 Amazon Web Services, AWS Official Blog, *http://aws.amazon.com/blogs/aws/*

**Quality Statement:**

*This Work is translated into Chinese Traditional from the English language version of Volume 4, 2016of the ISACA Journal articles by the Taiwan Chapter of the Information Systems Audit and Control Association (ISACA) with the permission of the ISACA. The Taiwan Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.*

**品質聲明：**

*ISACA臺灣分會在ISACA總會的授權之下，摘錄ISACA Journal 2016,Volume 4中的文章進行翻譯。譯文的準確度及與原文的差異性則由臺灣分會獨立負責。*



**Disclaimer:**

*The ISACA Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the ISACA Journal.*

*Opinions expressed in the ISACA Journal represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute and their committees, and from opinions endorsed by authors' employers, or the editors of this Journal. ISACA Journal does not attest to the originality of authors' content.*

*Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, MA 01970, to photocopy articles owned by ISACA, for a flat fee of US $2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.*

**免責聲明：**

*ISACA Journal係由ISACA出版。ISACA 為一服務資訊科技專業人士的自願性組織，其會員則有權獲得每年出版的ISACA Journal。*