Cloud Computing

雲端上之資料是否安全?

Are Your Data Secure in the Cloud?

作者: John Nye, CISA, CISM, CRISC, CISSP

is the director of technology risk solutions at ProcessUnity (www.processunity.com), a cloud-based provider of governance, risk and compliance (GRC) solutions. He is responsible for the governance of ProcessUnity's Software as a Service (SaaS) solutions and advises clients in the art of third-party vendor risk management. Nye has worked with firms such as @stake, Symantec and Moody's as an assessor of third-party risk and has served as an information security executive for a midsized technology service provider, protecting information and managing corporate risk from both sides of the due-diligence table.

譯者: **劉其昌**, 中華民國電腦稽核協會編譯出版委員會委員、立法院教育及文化委員會主任秘書

本人第一次參與接近網路資訊處理以網頁為基礎、多層次列、多重性租借、分時分享軟體基礎架構設施服務解決方案是在 1998 年之時。它係一個 x.509 經權威認證之數位化模式，在這以前吾人並不稱呼它為一個雲端解決方案，但是今天或許我們會稱呼它是，自從過往之數年以來，本人也曾經涉獵參與過另外二個其它之雲端解決方案:其一為有關顧客通訊活動行為之管理(自動電話撥號系統)，為顧客服務中心提供解決方案，而目前我地角色為集中就責方之風險管理，提供一項管理其風險與依從方面之解決方案，救我服務的顧客而言，上述提供的這些解決方案中皆有下面之共同之一般特性:

- 易於接近特殊專門之技術
- 具合理效率化同時易於升級和維護
- 容易可計量之方式衡量
- 享有與第三方公正團體分享非公開資訊之機會
- 享有信任具關鍵成功企業營運過程經驗之機會

顯然地對上述表列之內容會有正反不同之看法，針對上述之解決方案為前提之差異化比較分析指出，資訊外包服務之傳統性優點為---易於接近獲取專業技術以及營運操作可無縫接軌-----通常可以在企業認為某種合理之費用範圍內順利完成，從企業戰術之觀點而言，企業通常會選擇最佳之解決方案，對企業會比較有利而不會介意究竟來自於內部完成，抑或為外包之方式，但就戰略上之觀點而言，資訊外包服務可使企業組織更集中營運之焦點在其核心之競爭能力部分，然而一旦有更合適的第三方部門團體介入服務管理包括治理監管等，此時不論企業部門是如何在監督管控其資訊外包服務，資訊外包服務將不必然具有企業營運成本節約之效果。

然而針對資訊外包服務方程式加諸過多可計量之雲端式之解決方案，將使企業之經濟行為活動產生巨大之變化，此時透過廣泛雲端服務提供之解決方案數量雖達具經濟化之規模，而使企業之成本處於下降之狀況，通常這一個狀況點不易達成，但是甚至可能遭到忽視而不予理睬。

就某些組織之機構而言，採取雲端服務解決方案決策行為兼具明顯性與急迫性兩者，至於其他的組織雲端服務解決方案代表的是一種無法容忍之風險，的確時至今日不斷成長中之企業所需面對之資訊確保品質、資訊保證安全、滿足所需資訊之各種服務之便利可及性者出現在雲端上，就正如它彷彿是在其他資訊外包服務解決方案中，啊在雲端上保存因此所有各種風險因子變成更為恐怖，其理由原因為何?

這個答案是十分簡單地:因為不明瞭而恐懼，從下述二個方面可以了解其真實性，首先就是透明度會遭致挑戰，因為雲端一詞本身似乎在說明表達，你並不需要去了解在雲端內部

是什麼東西，的確雲端之圖像非常宛如大眾所熟悉網路互聯網之圖形形狀符號，告訴我們的是雲端內部是一個大又具複雜性且與討論無關聯之內容，就企業傳統上之概念以一個明確定義規範連結各網路之周邊範圍---一個外在和無法信賴之團體----其對連結複雜性之困惑度以及所表達之無關聯性是完全合理地。但是當雲端服務提供者為企業提供功能性服務時，其真實性係無可更為比擬者，就專業性之風險管理者而言，它們一部分之職責就是在評核資訊委外風險對第三部門之影響，以及評估或審計稽核其控制機能。檢視觀察雲端服務之內部作業是我們地職責工作，但是不幸地，這項工作通常並不是經常可能，也的確是，當雲端服務之提供者變得越來越大，同時更具有成本之節約效益時，愈獲取對雲端服務進行外部之審計稽核所面臨之挑戰也會越巨大。

其次，雲端服務提供者通常是用一種大家不熟悉之方法在處理執行大家熟悉之控制性機能，讓吾人用一個簡單之實例來比較說明，企業軟體服務解決方案與軟體就是服務(SaaS)之雲端服務解決方案之差異，當企業意欲運用獲取其資料時，通常最普通之管制措施之一，是接近獲取其防火牆內部包括之資料加以應用，同時防止不當獲取者經由網路得以接近使用上述資料，也就是說企業藉助以網路為基礎來源之網路通訊協定進行某種安全之網址過濾作用。不幸地是，這項網路技術對許多地雲端服務提供者並無法有效運作，例如當企業顧客透過網路接取獲得服務解決方案時，此時有為數眾多之企業顧客皆在分享此單一服務平台，同時全域化之皆取自是被允許的。當然企業之防火牆應當在它應有之適當位置，但是防火牆應該是允許而非防止，藉由網路方式接取主要之應用解決方案，不幸的網路之管制機制目標在於控管規範資料之接取，而非解決方案之應用面，因此若非使用以網路為基礎之解決方案(亦即一個防火牆設置)，以無差別地規範管理資料接取之應用，吾人可藉執行以網路為基礎來源之網路通訊協定網址過濾作用，直接管理接取資料應用時之規範機制，在此一方式下，可依據每一位之企業顧客為基礎，來強化應採取之必要對策內容，亦即，來自關聯性企業顧客之使用者們皆被要求有限度的接取其顧客們之資料。

這剛好是一個雲端服務提供者在執行相關控管機制時是如何不同於傳統企業軟體服務解決方案、或甚至屬於一個非雲端服務提供者情況之實例， 對大多數扮演資訊風險管理者角色的我們而言，職責應當包括評估我們的雲端服務提供者是否真正完成達到其必要之管控目標內容，我們也應當完成準備用以了解位我們提供資訊雲端服務之提供商其運作是否妥適，同時評核雲端服務提供商其管控流程之設計構思與執行之有效性。同時我們也應該去考量了解這種管控流程設計之改變，是如何影響改變了其他管控流程在原先傳統上之優先性。

讓我們另外檢視一下稍早的一個實例，即在企業軟體應用服務方案之情況下，企業網路之防火牆至少具有二個管理控制機能，第一個，它必須要確認使用者以網路為基礎來源之網路通訊協定之網址，藉以確定保證該使用者現在仍在該企業之工作位置上，第二它防止當使用解決方案時不會有來自以網路為基礎為攻擊對象之駭客攻擊。在以雲端為服務提供解決方案者之情況時，以網路為基礎來源之網路通訊協定之網址認證，已轉移至資訊之應用階層面，但是應用階層面在網路上是曝露未遮掩地，因此網路駭客會修正其攻擊之面向，此一曝露構成一個新的威脅。顯然地，就雲端資訊應用層面而非單一企業資訊應用服務來說，運用資訊之安全控管機制之維護應該具有最高之優先性，不僅是因為雲端資訊應用層面會暴露在網路之上要盡責維護安全，而且針對企業防火牆先前所提供之若干安全機制也應盡其職責。

如何瞭解雲端服務提供者之運作模式是一項關鍵因素，若是沒有這類資訊吾人將無

法瞭解它們所面臨之風險何在，同時倘若你不知道它們經營管制之風險，你將無法決定它們規畫管制設計是否正確或是否有效地在運作，而諸如同儕之專業性風險等口頭禪將會在實務界及學術界兩方面被不經意發現，不過在第三方部門的資訊風險管理領域中，以一項標準大小用以評估所使用之全部系統管理，企圖嘗試壓制以標準化為基礎之正式評核審計管制機制，使其評核作用只能夠持續一天或二天，這項危險之假設使其餘部分獲得承認其正當性，為了避免上述之錯誤發生，尤其在有時間限制之情況下，對任何雲端服務提供者在一開始要評核其安全議題時必須要詢問下述之問題。

・雲端服務提供者解決方案係採用何種形式(亦即採取網路架構就是一種服務、網路平台就是一種服務、軟體設計就是一種服務)，以及原本所規畫控制設計時就會帶來何種固有之影響衝擊?

・雲端服務提供者是否運用實質性或其他新的技術解決方案，同時假若如此，雲端服務提供者是如何針對這些新技術解決方案所形成之新局面，規劃設定企業組織之管控目標方向，例如網路間互聯之開放體系(OSI)模型[1]將被如何施行?

・雲端服務提供者是否已經完成履行備妥預備性之工具方案? 倘若真是如此，

這些工具方案是否足以增強管理面之治理機能?抑或會不經意地破壞雲端服務提供者之安全架構?抑或是兩者皆有?

・雲端服務提供者是一個相對屬於新穎的觀念，就一個雲端服務提供者之業務營運而言，究竟有多新?它的涵義有意旨到表示，雲端服務之經營財務和營運業務處於一種不穩定之狀態嗎?

・雲端服務提供者通常不願意就企業客戶之個別使用者們提供管理面之服務，取而代之的是，支持採取某種代理接取管理的型式，雲端服務提供者在資訊使用接取和身分認證管理方面究竟可以提供什麼可利用之選項? 而這些可利用之選項又如何有助於檢視資訊接取之控管機制，和監視使用過之軌跡內容? 同時上述這些特徵資料是否可以滿足企業組織資訊治理和營運作業之需求?

・是否雲端服務提供者之解決方案皆係處於獨立之狀況，抑或其解決方案涉及多元化之提供者(亦即例如一個網路軟體即服務託管在一個平台即服務之解決方案中)?

・是否在單一企業之軟體服務解決方案其管理風險有趨於集中呈現之可能? 當多元化之軟體服務應用皆朝向同一個軟體基礎架構即服務之運用平台移動時，這將如何對企業組織造成何種衝擊影響分析?顯示出有多少企業組織將相同之資訊服務功能外包給同一個雲端服務提供者，同時如果有非常多，那麼就整個市場來說，他可能容易對企業組織之營運造成那些附帶之衝擊影響?

上述這些問題尚不足以涵蓋所有全部之問題，但是它卻提供應將焦點集中於在一開始就應透視評估雲端服務提供者之未來願景，瞭解雲端服務提供者之營運如何讓你超越因為不明瞭所產生之恐懼，升華到在一個十分舒適理性之環境下，以資訊管理風險為基礎去做企業之決策。

我通常對於工作上同事、企業客戶、和門外漢等，最常提出地眾多問題之一-----是雲端服務是否安全? 再回答此一問題時，我指出有一些之雲端服務提供者的確較其它之雲端服務提供者更為安全，但是在典型上當我問出這個問題時，是對某些享有十分知名度之網站產生好奇心了，包括以消費者為導向之網路解決服務提供者(諸如類菲斯Netflix)，或眾多全球最大的之一，以企業服務為導向提供公共雲端服務解決方案者(亦擊谷哥之應用服務或亞馬遜 EC2)，我們可以在某範圍內同意，即使在最佳資訊治理條件下之資訊服務解決方案本身亦面具資訊安全事件之經驗，同時當我們說及安全一詞，其實我們之真正含意係指在有效設計管理，伴

隨良好之治理，同時營運控管係建立在以合理有意義方式分析企業風險為基礎之情況下，我們的回應通常是，大多數之大型規模雲端服務提供者可能使比較具有安全性地，但是若沒有更進一步較佳之接取方式時，吾人是無法去證實它地。

雖然我尚未幸運到能夠獲得針對我曾經已經使用過地，所有規模較大型之雲端服務提供者，進行直接審計稽核之權利，但我還是十分愉快地在使用其提供之雲端服務。例如任何地資訊安全計畫中其最關鍵的一個部份就是所謂的一項安全，即針對可重複建置的主機設備具有無縫接軌應用維修使用之能力，從直覺上我們可以瞭解知悉，任何營運服務數以百萬計之雲端主機代管業者，一定已完成建置主機之服務模式，同時在可控制範圍內隨著調整情況變化而改變其管理方式，我的證據顯示出雲端服務提供者之服務非常成功---某些事情已它們之營運規模而言，若非經過仔細小心地事前規劃、極佳之一致性、輔以卓越之情境變化管理下，它們是不會去進行從事地，當然事證這些皆屬於情況證據，但是對於大多數之雲端服務提供者，我仍然有一個意見看法，那就是由於它們在一些或某個小議題裡，具有獨到專業之特殊服務解決方案能力，而通常他們在這些服務解決方案安全性之作業上，有較佳之工作能力同時是優於它們服務的企業客戶。例如當我曾經負責過一項以雲端為基礎之自動電話機撥號系統，有關妻運作安全性及相關之依從成本問題，有相當多的特殊性控管計畫之執行係針對電話之詐欺問題，但是僅有少數的大約 400 位服務客戶是真正瞭解控管之問題所在。在這種方式下，雲端服務提供商在某方面之特殊專業性可以為我們減緩，在客戶服務之解決方案前提下所無法完全消除之風險因子。

從透視專業性風險之角度而言，使用公共化雲端服務提供商之服務最大的缺點之一，為它是一個固定不變的預約模型，這就相似於企業對消費者間之服務契約也是一樣，企業客戶預約加入使用公共化雲端服務提供解決方案時，基本上必須接受同意解決方案服務提供者所提供之契約內容。而這類契約內容通常不會賦予某種相當具有意義之審計查核權力，或是含括其他另外之之特定項目與條件，而這些內容是符合企業所要或滿足監管機關所需要者。

這個意思並不表示你應該完全放棄對安全之保證，載以企業資訊服務為導向之公共化雲端服務提供商之情況，就潛在之企業顧客而言，通常可利用相當之機會得以檢視，資訊服務提供商其確保服務安全之文件(亦即包括 ISO27001 之證書，SOC 之審計性報告)，這類安全證書可用來回答許多有關確保安全性之問題，同時也應當能夠讓你做出一個兼具合理地、理性化、以風險為基礎之企業營運決策，以及決定是否參與加入資訊之服務，不過不幸的是，尤其如果企業正在作調控時，上述這些機能尚未充分到足以配合滿足你的實地查核義務工作。

若以規模較小的資訊服務提供商而言，上述這些動態之變化方向將會完全倒置，此時你相對比較可以就你比較想要的契約內容與對方進行溝通談判，同時也可以直接地審計稽核或評核資訊服務提供商，而你也最好要進行這些檢視，因為當你從百萬倍最大規模的資訊服務提供商移開後，從本質上而言，你將無法在等同原先良好治理情況下，營運所具有之活動力，而雲端服務提供商之規模愈小，你越不易假定其安全性，此時實地之查核也就變得更為重要，有一些可能非常值得相互信賴。然而其他另外的參與其企業可能是非常帶有風險性地，除非你十分貼近距離觀察，否則你是部會知道的。

以企業階層為分級之資訊服務提供解決方案，通常甚少僅提供一個單一應用服務，再以企業服務為基礎架構之前提下，他將包括企業與另外一個跨界之交岔整合性之應用、認證性基礎架構、軌跡基礎架構、和相類似的基礎架構，而雲端服務之基礎架構並

沒有什麼大不同，若參與一個以雲端為基礎之軟體即是服務提供者契約服務，僅獲取其中最重要服務項目之一，或者只在監管其使用是否合理正當，那將會是一個十分不尋常的事。他係需要與其他企業之應用面做一個整合集成地和完成技術面之基礎架構，通常來說，資訊服務解決方案應預約較多之資訊服務提供商共同參與彼此間一片片相互整合連結聚焦在一起，同時當你為滿足原始首先之企業客戶需求，而與各雲端服務提供商緊密結合在一起時，你會發現你已與其他另外許多之雲端服務提供商整合在一起，也組合完成一個完整之解決方案。倘若能正確地架構雲端服務提供之基礎架構，那將可以整合集成同時延伸你企業所創造之營運基礎架構，Salesforce.com 的服務應用交換機制，就是在這個生態體系下最好第一個實例，不過其中有一個缺點，那就是在最起初開始時的實地查核成本會十分昂貴，因為你必須完成有關涉及多元化第三部門資訊提供者滿足對原先企業營運需求服務配合度風險性之評核作業。

就 Salesforce.com 的服務應用交換機制做一個迅速觀察，將會喚起吾人想起雲端服務本身就是一個極佳供做行動化和社會面應用之場所，或是在企業之外，需要進行任何共同協同合作應用，和各種團體間進行訊息互換之場所，倘若沒有雲端服務提供者，你必須與他人間籌建一個企業間之網路連結，用以彼此交換資訊用，也將使貴企業留下一個如同若干雲端服務提供者一樣都應面對，而必須想法解決之網路基礎架構安全性之問題，亦即本文稍早所敘述之網路通訊協定網址之來源地經過過濾機制後所面對之挑戰，以專業化之資訊安全和風險管理角度觀之，支援企業協同合作的能力較易達到，這也是比較傾向主張以雲端為基礎提供軟體服務解決方案，它也是最有俱強制性之眾多各種理由之一，同時在某種程度上，複雜性本身就是資訊安全之敵人，而雲端服務提供者之解決方案具有減少企業協同合作間之複雜性效果(或者至少可將複雜性之程度外溢至更具有較多資源和專業技能之寬廣空間中)。

因此就我所參與之相關經驗而言，企業之協同合作作業係構成以雲端為基礎企業服務解決方案中一個關鍵之因數，那是不值得驚奇地，X.509 所具證據服務之權威性，也係藉由公正第三方團體提供之託管服務，用以達成註冊模型核心部分之職責分離工作，同時依據證書上之要求提供各方面之服務，同時也較容易地分配處置廢止之資訊。企業客戶間之交流互動已逐漸被推向行動化和社會性之平台上，而資訊服務之提供者面對之風險管理需要處理，企業客戶與它們第三方團體間之協同合作與資訊交換時之評核與審計稽核，在這一方面之作業活動中，雲端服務提供者扮演不錯之角色。

正如雲端服務提供者善用其專業性能力，和經濟規模能力，用以為企業提供完美之服務解決方案，它們也可以利用彼此間之服務差異為槓桿因子，來確保和維護管理它們解決方案，企業建置之基礎架構用於營造計算之環境，一般使用之情況為支援多元性、和全然性不同之用途上，每一種的服務應用在其使用、營運、確保、和監理上皆會面對單一之挑戰，在解決方案之前提下，如此將一則導致巨額花費和你將之用戶化所造成之複雜性，或者導致你將其一般化之後必須接受增加風險。相反地，雲端服務解決方案之安全架構則比較具有其特殊性。在單一服務解決方案後之實際例證來說，在安全確保事件上，雲端服務之安全架構所驅動之安全機制和風險之控管能力計畫接近於實足完美，優於其他任何環境情況下之結果。這可能就是造成雲端服務提供解決方案對職業性風險管理者具有吸引力，而成為選項之理由。不過不幸地是，並不是所有每一位雲端服務提供皆願意進行此類之投資，通常就一位職業性之服務風險管理者而言，我們地質則非常明確，那就是將不知之事情加以解說讓人明白瞭解，並加以透明化。因此在以風險為基礎的企業決策下，取代因為恐懼不知

的無理性，同時扶植企業得以在良好的機會下，正確地茁壯本身之營運發展。

ENDNOTES

[1] Open Systems Interconnection (OSI) model is developed and maintained by the International Organization for Standardization (ISO); see ISO/IEC 7498-1.

Quality Statement:

This Work is translated into Chinese Traditional from the English language version of Volume 1, 2015 of 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 2015,Volume 1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。

Copyright

© 2015 of Information Systems Audit and Control Association ("ISACA"). All rights reserved. No part of this article may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system, or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise), without the prior written authorization of ISACA.

版權聲明：

© 2015 of Information Systems Audit and Control Association ("ISACA"). 版權所有，非經ISACA書面授權，不得以任何形式使用、影印、重製、修改、散布、展示、儲存於檢索系統、或以任何方式(電子、機械、影印、或錄影等方式)發送。

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。

Cloud Computing

ISACA Journal收錄的文章及刊物僅代表作者與廣告商的意見，其意見可能與ISACA以及資訊科技治理機構與相關委員會之政策和官方聲明相左，也可能與作者的雇主或本刊編輯有所不同。ISACA Journal 則無法保證內容的原創性。

若為非商業用途之課堂教學，則允許教師免費複印單篇文章。若為其他用途之複製，重印或再版，則必須獲得 ISACA 的書面許可。如有需要，欲複印 ISACA Journal 者需向 Copyright Clearance Center(版權批准中心，地址：27 Congress St., Salem, MA 01970) 付費，每篇文章收取 2.50 元美金固定費用，每頁收取 0.25 美金。欲複印文章者則需支付 CCC 上述費用，並說明 ISACA Journal 之 ISSN 編碼(1526-7407)、文章之出版日期、卷號、起訖頁碼。除了個人使用或內部參考之外，其他未經 ISACA 或版權所有者許可之複製行為則嚴明禁止。