雲端風險—評估風險的十項準則和架構
Cloud Risk—10 Principles and a Framework for Assessment

作者：David Vohradsky, CGEIT,CRISC,

is a principal consultant with Tata Consultancy Services and has more than 25 years of experience in the areas of applications development, program management, information management and risk management. He has worked in senior management and consulting across multiple industries, adapting, implementing and utilising industry frameworks and ensuring compliance with regulatory requirements. Vohradsky specialises in governance, risk and compliance within TCS's Global Consulting Practice, is a member of the ISACA CGEIT Test Enhancement Subcommittee, and an external thesis examiner for the Doctor of Business Administration at Charles Sturt University (Australia).

譯者: 周濟群,台北商業技術學院會計資訊系 副教授,電腦稽核協會編譯出版委員會委員

雲端運算(特別是「軟體即服務」(SaaS)之範疇)在企業內部發展之效益已是相當著名而顯而易見的，其中包含了快速配置、客製化變得更容易、降低建構及測試上的投入及專案風險的減少。而同樣著名的還有「基礎建設即服務」(IaaS)所帶來的效益，包含成本的減少、支出從資本層面移轉至營運層面以及增進企業靈活度。然而，由於各產業缺乏一個對於風險辨認及評估的完整架構，造成現今仍難以對於雲端運算之風險有一共識。除此之外，企業更因為缺乏瞭解和明確的指引而對於雲端運算的導入顯得窒礙難行。矛盾的是，對於小型及中型企業來說，導入雲端運算卻是一個有效降低風險的方式。舉例來說，導入雲端運算能夠有效降低伺服器錯誤配置之可能或是無效率補丁管理導致系統遭受攻擊的可能性，以及可降低由於無法有效利用可攜式移動裝置所造成的資料遺失。

近期內備受矚目的企業發生斷電、保全漏洞等事件層出不窮，更進一步的影響企業對於將目前現有的內部控制制度以及即將針對外部重大事件而設立的雲端相關控制產生質疑。舉例來說，在2011年四、五月由Sony、VMware和Microsoft的雲端服務所爆發出一連串的損失，造成雲端風險開始引起高度重視。

文獻回顧

過去數年來已有許多文獻探討雲端運算相關的議題，如雲端運算的風險暴露、雲端運算之導入以及建置雲端運算應注意的內部控制要點。其中大部分文章已對於基本安全作考量，惟對於評估整體IT風險仍尚缺乏一完整之架構。

據傳，國際標準化組織(特別是ISO/IEC JTC 1/SC27)正開始著手針對雲端運算相關服務之風險管理訂定一正式標準，而雲端遷移本身實際上也尚未成熟，正如同現有的產品及服務正逐漸成熟，而新的產品及服務也如同雨後春筍般冒出。如近期新推出的數據即服務(DaaS)以及提供現今尚未出現的中介、監督、轉型和移植、治理、供應及整合相關的雲端服務。

2009年歐洲網路及資訊安全公司(European Network and Information Security Agency，ENISA)發表了一篇文章：雲端計算—資訊安全的利益、風險及建議，文章整理出19名提供者所所辨識出的35種風險，並基於ENISA所考量之可能性及影響辨識出8種首要的風險。2010年3月，雲端安全聯盟(Cloud Security Alliance，CSA)出版「雲端運算之重大威脅V1.0」，

該冊內容包含開放式網路應用安全計畫(Open Web Application Security Project，OWASP) 根據其他文獻所整理出的「準預覽名單」，再從其中所整理出的十大雲端安全風險中再取出七大雲端威脅。2011年5月，美國國家標準技術研究所公告了一份草案：「雲端運算概要及建議」(特別出版800-146)，該份草案提供了對雲端風險的分析，但同樣的並未對整體雲端風險提出一個完整的架構。**表一**提供CSA、OWASP和ENISA所辨識風險類型之比較，表示出其風險內容和排序之差異。

表一、風險排名比較表

風險	CSA 排名	OWASP 排名	ENISA 排名
惡意或濫用雲端運算—由於某些雲端運算具有匿名性，易誘使使用者將其作為犯罪用途	1	-	-
不安全的使用介面和應用程式介面—由於雲端服務具有開放性，且其介面通常可匿名存取、授權及內容傳輸	2	-	-
惡意的內部人員—雲端提供者開放部分透明度給予其供應鏈成員、人力資源部門成員及安全管理和事件管理成員	3	-	8
分享技術風險(多租戶技術、資訊隔離)—一位租戶故意或是不經意地接取另一租戶的安全和表現資料	4	7	3
資料所有權(治理)和責任—資料的所有權、加密、傳輸、營運失敗、資料丟棄/資料刪除及資料可用性都是雲端環境中的一大挑戰。	5	1(所有權) 5(資料遺失)	1(所有權) 7(資料刪除)
挾持帳戶或服務(包含介面管理)—利用社交工程、網路釣魚、詐欺或漏洞攻擊、攻擊方可能危害保密性、正當性、和可行性。	6	9	5
未知的風險輪廓—雲端提供者開放部分透明度給法令遵循、安全程序、配置管理、登錄及監督，僅提供消費者一個模糊的輪廓。	7	8	-
使用者身分濫用—使用過多的雲端服務會造成身分維護上的困難。	-	2	-
規定的遵循—不同國家、地區之法令規範可能大不相同，特別是隱私相關之規定。	-	3	4
企業永續性和彈性—可能不適當的授權給雲端服務提供者，訂價的壓力可能導致忽略此點的商品化。	-	4	-
服務與資料的整合及保護—使用者和資料中心間或是雲端間資料的傳輸可能使資料的持有和保護發生問題。	5(CSA 將此項與前項並列第五)	5	6

非正式環境之暴露—用以設計、發展和測試的環境往往較少受到控制。	-	6	-
鎖定—缺乏用以確保資料、應用程式及服務，或是業務流程的可移植性之工具、流程、標準或介面。	-	10	2

在2011年7月，ISACA發布了「雲端運算的IT控制目標：雲端科技中的控制與確信」，提供一個為COBIT、Val IT和Risk IT所採用雲端控制的全面性指南。ISACA所發表的該篇文章同時也批判了當時許多的標準、認證或是架構，包含COBIT、ENISA、CSA、NIST、ISO27001、美國註冊會計師協會(AICPA)、SOC(Service Organisation Control) 1 Report、美國註冊會計師協會確信服務(SysTrust)、CSA的雲端安全矩陣、聯邦風險與授權管理計畫(FedRAMP)、健康資訊信託聯盟(HITRUST)、BITS共享式評估計畫和Jericho Form自我評估計畫(SAS)。如此一來，該文章不僅強調現今對於一個具有一致性和廣泛性的風險評估架構的需求，同時也再次強調現今仍無法發展出一個完整的風險評估架構。

評估的架構

ISO/IEC 9126（資訊科技—軟體產品之評估—品質特性與使用指引）與深層安全性評估同時採用時，能為新供應商與新科技（包含雲端服務）之適用性評估提供更多架構與協調。此國際準則的目標為提供一個由六項品質特性組成之架構，以評估軟體品質。而此準則似乎亦能適用於軟體即服務（SaaS, Software as a Service）、平台即服務（PaaS, Platform as a Service），和基礎架構即服務（IaaS, Infrastructure as a Service）之雲端評估。

前述文段中各類型風險可直接映對至 ISO/IEC 9126 架構（表 2），此外，準則可被用以導出現今尚未被產業共同解釋的風險集合。表 2 所示之範例源自一份數年前 Force.com 作者所作之評估，可能未能反映 Salesforce.com 目前提供之服務。

表 2 風險映對至 ISO 9126

ISO 9126 特性	子特性	雲端風險	Force.com 範例評估
功能性	適用性（按企業需求）	發展/解決方案並未能滿足企業需求（新）	資料模型、畫面排版及商業邏輯僅能滿足基礎企業需求，高度客製化的必要性
	準確	N/A	N/A
	內部操作性（與內部系統）	發展/解決方案並未能滿足 IT 部門之架構，如：介面、資料整合等（新）	所有透過 Web API 的整合需要 ETL 工具，且無法得知績效透過 Apex Data Loader 輸入/輸出有使用上的限制 Sales Force 的物件查詢語言（Object Query Language, SOQL) 並沒有加總功能（如：加總、計數、平均等）與聯合功能
	遵循（符合規範政策）	OWASP(3)—規範遵循	

	安全性	詳見表 3	Web API 使用統制帳戶；安全性須藉由外部應用程式執行
穩定性	成熟度（提供之服務）	缺乏系統/服務的品質，如：既存的使用與支援（新）	
	容錯程度（服務層級協議[SLAs]與預期停機時間）	OWASP(4)—企業運作持續性與復原	
	回復性（企業運作持續性[BC]/災害回復[DR]）	無法於企業時間需求內回復服務的運作，如：企業的備份、持續運作、災害回復方案為何？（新）	
可使用性	可理解性（技術人員及使用者）	系統/服務並未如預期的操作，如：缺乏對系統架構、復原、處理能力的認知（新）	人員需要學習 Visualforce 架構、網路服務 API 及 APEX 程式語言
	可學習性（需要技術人員及使用者訓練）	人員並未具備足夠的技能以執行其工作與職責（新）	需要專家層級之人員在制式與制式外的產品達到相同觀感及體驗
	操作性（需要技術人員及使用者的付出）	人力不足以支援解決方案，包含雲提供者及雲訂閱者（新）	將要求配有新 ETL 及報導工具與客製化需求的支援
效率	時間表現（回應及處理時間）	OWASP(6)—服務與資料整合 ENISA R26—網路管理	Web API 整合依賴使用者電腦的記憶體（最低需求 1GB）和瀏覽器
	資源表現（多工影響）	ENISA R8—資源消耗	指令運行限制（200 筆封包/每 24 小時 5,000 次 API 呼叫）提供保戶但需要複雜的程式語言以執行部分企業報導的功能
可維護性	可分析性（技術透明度）	CSA(7)—未知風險輪廓	

	可變換性（置換及配置管理程序）	變動的對企業造成的負面影響，如：職能分工、集中式/分散式的變動、針對變動管理的遵循、配置管理工具（新）	提供資源碼控制和控制環境的區別，但僅每月且透過單一方式測試環境更新有高達 15 個程式設計者案例，但僅有一個應用層，且不能自程式更新
	穩定性（壞損中斷的可能性）	CSA(4)—共享技術議題 ENISA R25—網路中斷	
	可測試性（包含可行的測試環境）	IT 變動對企業造成的負面影響，如：測試程序、測試環境、測試資料禁止（新）	詳見可變換性欄位
行動性	可適應性（因應企業的多變樣）	OWASP(2)—合法使用者身分（可能需要數個帳號）	
	可安裝性（移轉所付出的代價）	執行計畫之風險，如：範圍、時間、成本及品質（新）	
	遵循性（符合規範）	缺乏品質（新）	
	可替換性（可否移轉至替代方案）	ENISA R1—鎖定	輸入/輸出的容量限制，且容易受執行限制

與安全相關的風險可被類似的結構性方法評估，透過相互評估 ISO 2700x、COBIT 及 NIST 800-53 中於雲端運算所揭露的控制。例如：表三展示了與安全相關風險的交叉索引（前面文獻探討段已辨識之風險）至 COBIT 4.1 DS5 確保系統安全。

表 3 安全相關風險與 COBIT DS5

COBIT 控制目標	控制	雲端風險	Force.com 範例評估
DS5.1 IT 部門安全管理	管理(ISO 27002–6)	ENISA R2—治理失敗	將會維持適當的保護措施；債務額度限制為美金 $500,000 或債務於未來 12 個月內清償
DS5.2 IT 安全計畫	遵循(ISO 27002–15)	ENISA R3—遵循風險 ENISA R22—管轄權變化之風險	主機設於新加坡，並設有備份機制回送北美；將被認定為由金融產業規範者提供的重大外包

DS5.3 身分管理 DS5.4 使用者帳戶管理/ISO 27002—11	唯一身分碼（ID）	OWASP 2—合法使用者身分	個人及權責基礎的權限設制於系統、套件軟體、物件、檔案及欄位層級
	一般帳號	CSA 3/ENISA R10 & R28—惡意內部使用者	未知
	帳號保安	CSA 6—帳號或服務的入侵	登入受 IP 位置和時間的限制，服務是被監控以防止安全侵犯的嘗試，登入資訊會被保留六個月以利下載及查閱
DS5.5 安全測試、管制及監視	安全性日誌檔(ISO 27002–10)	OWASP 8—事件分析及鑑識支援	審計軌跡可被定義；可能造成效能影響
DS5.6 安全事件定義	事件管理(ISO 27002–13)	ENISA R18—惡意偵查或掃描 ENISA R30 & R31—遺失或損毀日誌檔	
DS5.7 安全科技防護	技術控制	OWASP 7/ENISA R9—多租戶及實體安全 ENISA R24—帳戶風險	每個資料庫存有靜態資料表能存放數千筆混合的客戶資料，控制及存取則由後設資料管理
	安全弱點管理	OWASP 9—基礎設備安全 ENISA R20—雲端強化 ENISA R15—分散式阻斷攻擊	未知
	公用程式存取	OWASP 10—非生產環境暴露 ENISA R11 & R19—服務引擎/介面妥協方案	未知
DS5.8 密碼鍵管理	加密	ENISA R17—密碼鍵遺失	所有資料在傳輸過程中皆加密，資料欄位可以採用 AES-128 方式加密，但可能影響效能
DS5.9 惡意軟體防護、偵測及修正 DS5.10 網路安全/ISO 27002–5	病毒與惡意軟件	CSA 1—雲端運算的濫用與惡意使用	未知
	預防及偵測性方法		侵擾偵測系統(IDSs)於所有部門運行
	網路安全	ENISA R27—修正網路	防火牆僅對 http、https 及

		流量	ICMP 流量限制 ，網路由第三方單位驗證
DS5.11 敏感資料交換	信任的交換	CSA 2/ENISA R12 & R13—非安全介面及APIs ENISA R23—資料保護	所有資料在傳輸過程中皆加密
	資料遺失	CSA 5—資料遺失或洩漏 OWASP 5—使用者隱私及資料次級使用	
	資料管理(ISO 27002–7)	OWASP 1—問責性與資料擁有權 ENISA R14 & R32—非安全或不完整資料之移除	資料皆備份至硬碟或磁帶，亦備份至全球資料中心

雲端計算風險的十大原則

這十個雲端計算風險的原則可以對先前的討論內容提出一個評估風險架構，也可以對移動式的雲端計算提供一個完整的路徑地圖。這個路徑地圖是基於下列四個指導原則：

1.視野－企業的視野是什麼及誰擁有主動權?

2.能見度－需要做什麼及風險是什麼?

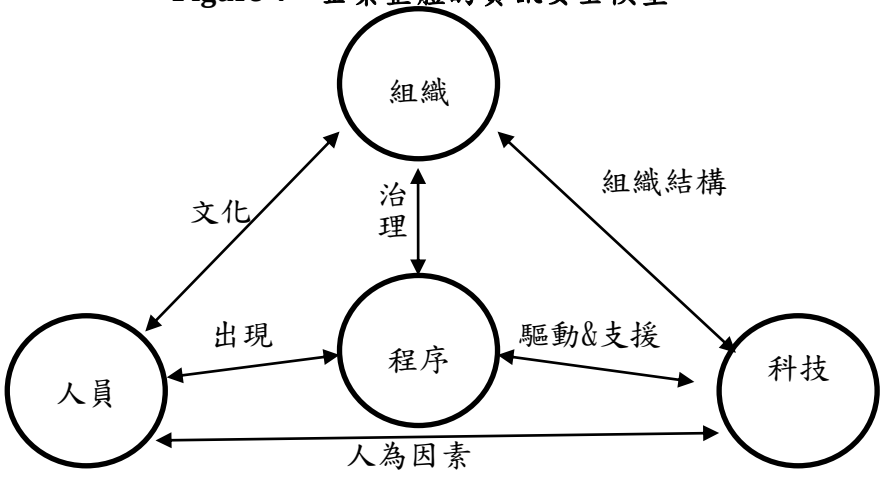
3.責任－誰該負責任及對誰負責?

4.持續性－該如何被監視及衡量?

國際電腦稽核協會(以下簡稱：ISACA)將整體的風險和安全性的架構做成企業的資訊安全模型(figure 4)。

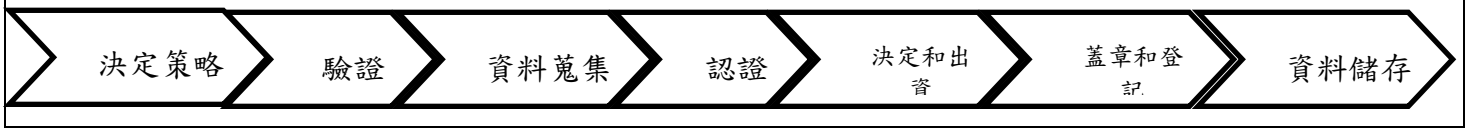
基於企業的資訊安全模型(以下簡稱：BMIS)，即雲端計算風險的十大原則，可以提供轉換至雲端運算環境的架構，如本案例研究所述。

Figure 4－企業整體的資訊安全模型



資料來源：ISACA，企業資訊安全模型，美國，2010，www.isaca.org/bmis

Figure 5－端到端(End-to-End)的房屋貸款企業流程



本案例研究如何將企業的風險管理功能(如：房屋貸款擔保保險的計算)移到雲端。企業風險管理功能是決定策略過程的一部分，如 Figure 5 所表示的端到端房屋貸款企業流程。在這個過程中，一個申請案件可能被接受和承認，需執行不同計算，且決定是否要貸出款項。

企業將風險管理的功能放在雲端的好處是可以允許分支機構、電話客服中心、經紀人、其他管道的人使用同樣的規定，並避免在多種位置重複計算同一件事。

使用雲端可以減少紙張的處理、主機系統的存取及減少其他相關的安全風險。如果企業將資料放在公開的雲端讓客戶能取用其資料，亦是一種潛在的商業動因。

整個架構的第一步驟是在企業或商業單位層級中制定並溝通出雲端的願景。有關於這個願景的首要兩項準則是：

1. **高階管理階層必須監督雲端**

企業整體必須認識以雲端為基礎的科技和資料的價值。他們必須持續的警惕和持續性的監督資訊資產的風險，包括確保相關法規、準則、政策、架構的遵循。這是與 BMIS 中的"治理"方面相關。在案例研究中，個人客戶銀行部門主管從內部和(/或)外部企業和科技專家的簡報中，了解科技和 企業目標的符合程度。接著則設置"高層意見"（Tone from the top），強制訂出政策或架構，以確保這些科技的組合必須符合產業標準和規則的限制。

2. **管理階層必須理解雲端的風險**

相關的企業個體中，管理階層們必須理解他們使用雲端服務的相關風險，而且必須在正在營運的企業基礎下建立、直接監督和評估出相似的管理風險。這是與 BMIS 中的"組織"方面相關。在本案例研究中，在剛開始時，企業決定將他們全部的風險(企業和資訊科技)，分配給個人客戶銀行營運風險部門的負責人，這個營運風險部門的負責人和資訊科技風險部門的負責人一起工作，共同規劃如何保護企業及科技風險。

一旦這些願景被清楚的表達且已經建立出風險管理組織架構後，在路徑地圖的下一步是要確保能見度，像是還需要做什麼事情和這樣做會產生什麼風險。下列有三個是與確保能見度的準則相關：

3. **所有必要員工必須擁有雲端的知識**

所有雲端的使用者應該具備雲端和雲端風險的知識，了解他們的責任和對使用雲端的行為負責。這是與 BMIS 中的"人為因素"方面相關。在本案例研究中，企業房屋貸款流程中的決定者與資訊部門的負責人一起工作以確保相關的企業和技術員工有足夠的技能從事雲端的使用或需要從外部專家獲得協助。

4. **管理階層必須知道誰在使用雲端**

必須建立適當的安全性控制在所有雲端的使用上，包含人力資源的業務(例如:徵才、轉調、解雇)，這是與 BMIS 中"人員"的維度相關。在這個案例研究中，企業房屋貸款流程中的決定者必須確保在企業、資訊科技和雲端服務的提供者有建置必要的背景檢查、職能分工、給予最少的特權和使用者複審的控制。這些都必須要和資訊科技的負責人及可能雇用外部組織的專家一起執行。

5. **雲端資料的放置必須經管理階層的授權**

所有以雲端為基礎的科技和資料必須區分為機密 (confidentiality)、道德 (integrity)、可取得

(availability)(合起來簡稱：CIA)三類，且在資產使用生命周期中，運用商業詞彙、最佳實務和技術控制，來評估其風險 。這是與 BMIS 中"科技"維度相關，且 ISO 9126 中評估的基礎架構也被使用在這張路徑地圖裡。在本案例研究中，房屋貸款擔保保險的計算過程使用了敏感性的資料，例如客戶的個人資料、出生日期、課稅所得。基於 Figure 6 的評估，企業資料的 CIA 評分則為平均獲得高度的評分。

一個越完整的 CIA 分析，更可以考慮到複雜的企業規定、資料保留的規定、及隱私或管理的規定。

一旦完成評估後，資產可以繪製出潛在的雲端部署模型。因為案例研究中高度的關心，所以管理階層考慮將這個過程遷移到私有雲中。在這種型態的部署下，這些計算可以被眾多的利害關係人以各種不同的裝置所使用，但這些資料還是在一個可接受的安全性層級裡面。私有雲和公共雲的比較，主要考量在有限制的登入或靈敏度。在這個案例中，個人客戶銀行的高階管理階層決定部署一個私有雲直到客戶取用資料變成一個強制性的需求。

下一個步驟，則應將與雲端導入相關的風險、現在所使用系統的風險和購買新的內部營運系統的選擇，三者共同比較評估。評估這些架構的風險，可用在每一個決策中，藉此取得如不當廠商或內部支援、導入複雜度、及導入可信度等風險的資料。在案例研究中，評估已存在的貸款擔保保險申請中，發現存有過度信賴單一廠商及有限災難回復之情形。

圖 6、機密性、完整性及可用性評估

機密性	公開	內部使用	機密	高度管制
完整性	低(備份)	適當(常規)	高(信賴)	最大(高度信賴)
可用性	容忍>14d	容忍 1-14d	容忍<24 小時	容忍<4 小時

圖 7、企業內部系統流程的風險分析

影響 / 可能性	不顯著(<AU $100,000)	微小(AU $100,000–$500,000)	顯著 (AU $500,000–$1 million)	嚴重 (AU $1 million–$10 million)	災難 (> AU $10 million)
非常有可能					
很有可能		積壓處理（時間的行為）/更改失敗		業務中斷(可靠性)	
一半一半		資料洩漏導致流失客戶(資料流失)	安全漏洞—用戶/技術（安全）		
不太可能		操作失誤（可用性）	功能遺失（適宜度）	難以吸引投資的商業損失	天災造成業務中斷（可靠性）
機率極小			監管機構罰款（合規）		

目前的風險評估花費有每年 2000 萬美元的風險價值模型（VaR），以及需花費約 1 百萬美元到 200 萬美元穩定和保護現有的系統。對於當前的企業內部系統的原樣風險概況（使用與相關聯的風險從 ISO9216 框架缺陷特性）示於圖 7。

將企業流程轉至私有雲後的風險概況（使用 ISO 組合 9126 和 COBIT 評估框架）如圖 8 所示，類似的風險評估（以及相關的商業價值進行評估），應實行其他選擇 - 內部操作和託管系統。

圖 8、私有雲流程的風險分析

影響 / 可能性	不顯著 (<AU $100,000)	微小 (AU $100,000–$500,000)	顯著 (AU $500,000–$1 million)	嚴重 (AU $1 million–$10 million)	災難 (> AU $10 million)
非常有可能					
很有可能		最終客戶的流失導致企業損失			
一半一半		更改失敗(可變性)	操作失誤（可用性）		
不太可能		積壓處理（時間的行為）	功能遺失（適宜度）/安全漏洞(用戶)	業務中斷(可靠性)	
機率極小		資料洩漏導致流失客戶(資料流失)	監管機構罰款（合規）/安全漏洞（技術）		天災造成業務中斷（可靠性）

將企業功能轉至私有雲可將 VaR 每年降至 200 萬美金，主要來自於去除了 系統更新、移除性能較差的技術，以及具有系統和數據流通的多個副本的用戶和數據安全風險。在更具體的層面上，組織可能有一個整體的記分卡覆蓋相結合 ISO9126 和 COBIT 框架;適用的預防，檢測和控制影響的詳細評估，控制;並為每個風險呈現固有的（控制前）和剩餘（控制後）的影響和可能性進行風險評估。

雲端計算路線圖的第三步驟是責任歸屬；在案例分析中，企業主和營運風險管理者發展出一套權責矩陣，如圖 9 所示。

圖 9、角色與責任				
	企業主	企業代表（營運風險管理者）	風險和安全諮詢和 IT 風險管理者	提供者
目標設定	決定企業風險偏好	站在企業主的角度接受風險或往上呈報	站在企業的角度評估風險	提供ＩＴ服務，包括ＩＴ保全
事件辨認	核准事件管理流程	監控或程爆企業內部事件	評估威脅和事件管理	事件和威脅的辨認及管理
風險評估	核准風險及控制評估文件	彙編和監控風險及控制文件	分類和評估資產的風險和控制	分類和評估風險和控制
風險因應	監督顯著的補救措施	監督補救措施	評估及報告補救措施	評估補救措施
控制活動	批准內部控制	企業營運控制	定義和評估控制	設計、整合以及操作控制
遵循	提供控制評估和測試的法律監督。	監督和測試控制流程	進行獨立的審查及測試	保持控制有效性的證據
報告		對於遵循、威脅及控制狀況的報告	對於遵循、威脅及控制狀況的報告	對於遵循、威脅及控制狀況的報告

這套權責透過三個原則延伸至流程、組織體系以及企業文化：

6. 在雲裡，必須要遵循成熟的ＩＴ流程

所有基於雲的系統開發和技術基礎設施的進程必須與政策方向一致，滿足既定的業務需求，妥善紀錄，並傳達給所有股東，和提供適當的資源。這關係到 BMIS 的流程層面。在案例研究中，個人客戶銀行營運風險管理者確保相關政策的到位和溝通，以及政策條款的評估框架的映射也包括在內。然後針對 IT 開發和支持過程進行差距分析中，並包含在風險和控制配置文件。

7. 在雲裡管理階層必須支付或建立管理與安全

資訊風險和安全性，以及它的監控和管理，必須是在所有的雲投資決策中的考慮因素。這關係到 BMIS 的體系結構層面。在案例研究中，IT 部門風險經理主動參與各個決策，包括供應商評估與管理，技術審查，安全評估和設計，以及最終的投資決策。

8. 管理階層必須確保雲端運算符合規定

雲端運算的所有提供者和使用者必須符合規定，法律，契約和政策的義務;秉承誠信和客戶的承諾的價值;並確保所有的使用是適當的，且經授權。這關係到 BMIS 的文化層面。在案例研究中，零售銀行營運風險管理者與內部稽核人員，確保各項政策，規定和員工行為規範適當到位;培訓有執行、有定期內部審查遵循度。營運風險管理者與 IT 風險管理者和供應商管理者，確保流程到位，符合雲服務提供商的標準。

在雲端運算路線圖的最後階段是持續性，並且有兩個相關的原則：

9. 在雲裡，管理者必須管控風險

所有基於雲的系統開發和取得必須要透明且及時回報資訊風險，並且要在妥善紀錄、監測溝通及升級流程的支援下進行。這關係 BMIS 的實

現和支持方面。在案例研究中，零售銀行營運風險經理和 IT 部門的風險經理共同制定一個持續的雲端運算風險和安全監測，回報和往上呈報流程。理想情況下，這個流程包括雲服務供應商提供的定期訊息和上報。

10. 在雲裡，必須遵循最佳的實踐

雲端運算基礎的系統開發和技術基礎設施相關的流程必須考慮現代技術和控制，以應對透過內外部監測所發現的新興資訊風險。這關係到BMIS的新興層面。在案例研究，IT風險管理者和IT部門，透過正規教育，實務接觸和相關協會，如ISACA等，持續接受雲技術和相關風險的教育。

結論

本篇文章回顧了現有關於雲端科技之指南，並指出 ISO 9126 在評估現有雲端服務上是一個十分具有價值的標準，提供更有架構且更具攸關性的評估依據，並且在 BMIS 和由四大指南準則：視界、可見度、課責性、永續性為基礎，建立雲端風險的十項準則。

但本項架構也並非萬靈丹，各種不同的雲端服務類型(SaaS、PaaS 或 IaaS)和配置模型(公有型、社群型、私有型或混合型)之間之差異甚巨，並非能依單一架構所套用；甚至公有雲/私有風險的資料，例雲端運算雲是否為自有、外包或是虛擬雲都會產生巨大的差異。因此，使用雲端運算的企業需要更加注意在不同雲端模型中所應考量的不同風險類型，並且無論使用的是何種類型之雲端模型，都應考量風險及安全之承擔程度，或者是與雲端服務提供者間相互承擔的契約責任。

以此項建議的架構為基礎，使用者可依據不同的雲端模型而發展為適合各種環境之評估架構，並且可以依照 ISO 27001、COBIT、NIST 或是在不同產業下的各項需求和規範而發展為良身訂做的風險評估架構。而另一個發展的領域則是在於能夠將品質特性(特別是功能性、可靠性、效率性)與各種雲端服務的一致性、可行性、分隔性之間的取捨加以擴大。

ENDNOTES

1. Wei, Yi; M. B. Blake, 'Service-Oriented Computing and Cloud Computing: Challenges and Opportunities', *IEEE Internet Computing*, November/December 2010
2. Hofmann, P.; D. Woods, 'Cloud Computing: The Limits of Public Clouds for Business Applications', *IEEE Internet Computing*, November/December 2010
3. *Infoworld*, 'The 10 Worst Cloud Outages (and What We Can Learn From Them)', 27 June 2011, *www.infoworld.com*
4. ENISA, 'Cloud Computing: Benefits, Risks and
5. Recommendations for Information Security', 2009, *www.enisa.europa.eu*
6. Cloud Security Alliance, 'Top Threats to Cloud Computing V1.0', March 2010, *www.cloudsecurityalliance.org/topthreats*
7. OWASP, 'OWASP Cloud—10 Project', *www.owasp.org/index.php/Category:OWASP_Cloud_ _10_Project*
8. ISACA, *IT Control Objectives for Cloud Computing:Controls and Assurance in the Cloud*, USA, 2011, *www.isaca.org/cloud*
9. The ten principles of cloud computing risk arose from a client engagement. The chief executive officer (CEO), overwhelmed with security issues, asked the chief information security officer (CISO) and his consultant (the author) to provide a list of the six principles that he should ask everyone in the organisation to follow regarding cloud computing. The author took this on as a challenge, but could not keep the list to six.
10. ISACA, *Business Model for Information Security*, USA, 2010, *www.isaca.org/bmis*

EDITOR'S NOTE

Guidance for BMIS is now incorporated in COBIT 5, *www.isaca.org/cobit*

Quality Statement:
This Work is translated into Chinese Traditional from the English language version of Volume 5, 2012 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 2012,Volume 5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
© 2012 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：
© 2012 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。

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。