IBM 雲端安全措施實施要點

依據 IBM 研究團隊及客戶經驗，在 IBM 的雲端安全指引中，將雲端安全措施分為以下 8 大類，共計 25 項要點，茲說明如下：

（一）建置安全計畫

1. 安全計畫應具備：

1.1 衡量組織文化對於安全的需求，包括所屬產業是否有特殊法規要求，例如美國醫療產業需符合 HIPAA。若貿易機密是企業競爭優勢，安全計畫中就應特別作好規劃；

1.2 雲端環境中的安全機制，應考慮重要性，以作為佈署的優先順序。

1.3 制定組織在雲端的安全政策：定義雲端的潛在威脅並加以控制；參考產業規定或最佳實例制定可監控及衡量的矩陣；要發展出究責結構；統整事件回應建議步驟，如關鍵行動、人員職責，以及若事件持續特定時間範圍內，回應處理應增加的程序等。

1.4 與雲端建置的團隊合作，確保其了解並能支援相關行動計畫。

1.5 對全組織進行教育訓練，使所有管理者了解安全政策，並容易取得政策文件。

1.6 建置能掌控安全狀態及異常事件的系統。

1.7 建立稽核計畫。

1.8 建置執行架構，確保事件發生時的溝通管道及可究責性。

1.9 建立訊息通知計畫，當異常事件發生時能儘可能即時與負責人員溝通。企業制定一致的政策及存取控制機制，以確保所有雲端服務元件都能維持資料保密性及遵循法規，也可善用平台工具。例如醫療研究應用系統須從各醫院的診間系統及計價系統擷取資料時，必須先從來源系統移除病患姓名及其他個人資料。因此，在雲端環境中，藉由中央控管的政策管理服務，可透過事先政策制定後強制執行。

（二）建置安全的雲端基礎架構

安全的基礎架構能讓雲端保有彈性，也可確保雲上的資料得到適當保護。企業應確保廠商能滿足與法規、產業、客戶有關的各種需求。

2. 維護防火牆的組態設定

2.1 防火牆的組態設定應包含以下條件：a. 防火牆上的變更管理程序應有正式簽核及接受組態調整；b. 防火牆應設置在與外部網路的每一界接處，以及雲端每個安全區域間；c. 網路架構、資訊流及防火牆的設置，要考慮到虛擬環境及軟體防火牆；d. 企業營運持續所需的服務及通訊埠應整理成文件並妥善維護，而防火牆的通訊埠應預設為關閉；e. 對於防火牆通訊協定的例外狀態或對異常的定

義應做驗證或風險評估；f. 對於群組、角色的清楚描述以及對邏輯網路管理的定義；g. 對防火牆、路由器的組態及規則設定每季進行評估；h. 為防火牆及路由器組態設定標準。

2.2 防火牆應拒絕來自未被信任的來源或應用程式存取，並且應記錄這些事件。

2.3 防火牆應限制被有直接外部連線的系統存取，以及存有機密資料或組態設定資料的系統。

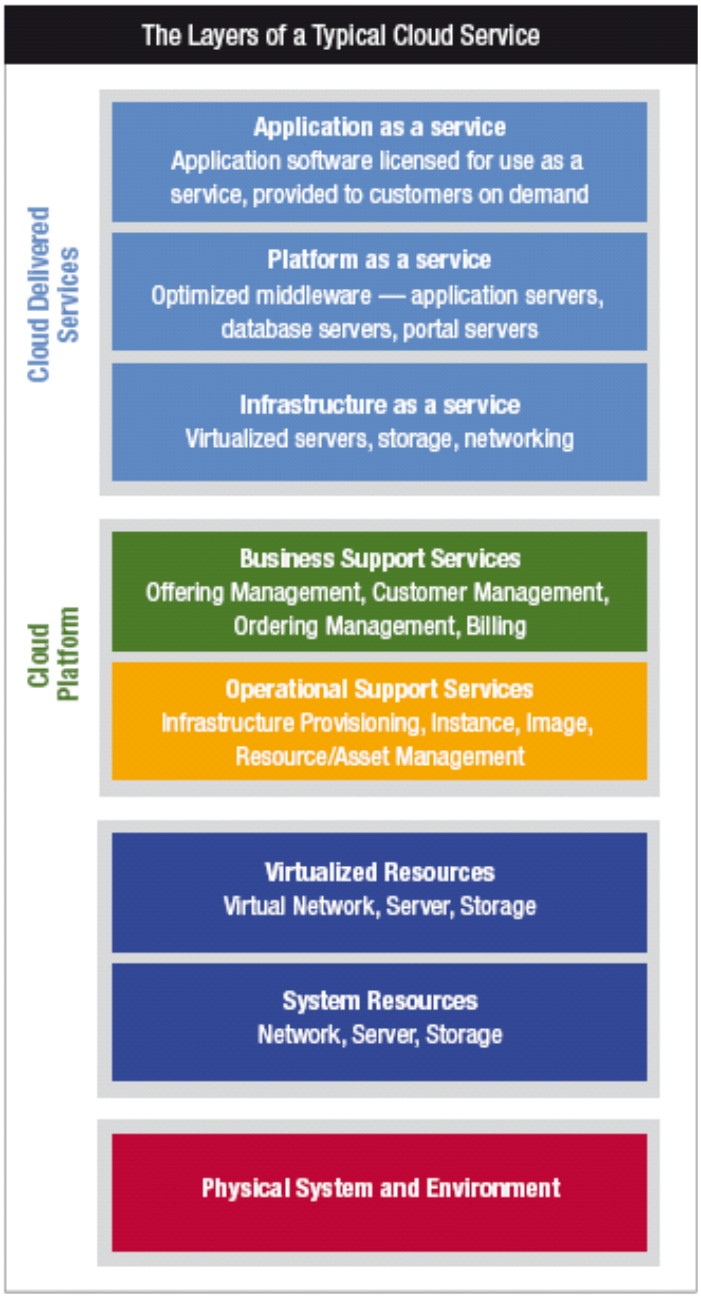
2.4 應在存有機密及組態資料的系統與雲端供應商的外部界接處之間安裝邊界防火牆。

2.5 在外部設備如筆記型電腦或移動裝置中安裝個人防火牆軟體，該介面及雲端環境須由雲端供應商支援。

2.6 進行 IP 遮罩，以避免內部系統架構輕易被外部探查。

2.7 防火牆應隔離機密資料，並確保所有機密資料都存放在防火牆之後。

3. 不要使用供應商預設的密碼或安全參數。
4. 保護管理者的存取控制及安全連線。
5. 確保修補程式的管理。
6. 實體環境的安全。
7. 適當保護遠端與企業基礎架構之間的連線溝通。雲端運算的基礎架構，每一層都有其安全需求，必須一致符合政策規定。從實體層、系統資源層、虛擬資源層、雲端管理平台（營運支援服務；企業支援服務）、各種雲端服務（Saas、Paas、Iaas），如圖二。



圖二：雲端環境基礎架構圖

（三）機密資料的保護

8. 保護個人資料，包含：參酌產業特殊需求，從個資的蒐集取得、處理、傳輸、儲存到銷毀須制定一套規則；制定個資外洩通知策略；制定個資盤點及分類計畫；維持個資數量的最小化。
9. 安全銷毀非必要的個人資料：包括個資在系統顯示時應適當遮罩；確認個資不會被記錄在日誌檔或其他系統檔案中；確認所有個資調閱動作被記錄下來。
10. 保護機密性的企業關鍵資料，如同上述保護個資的方式，在資料搬上雲端前應進

行資料衝擊評估，衡量企業風險忍受度。

11. 保護智慧財產：進行風險評估，確認公雲供應商的 SLA 協議能涵蓋智財的保護；資料搬上雲端前，企業應使用加密等技術，使惡意使用者難以用逆向工程破解系統。
12. 保護加密金鑰以避免誤用或洩漏：制定並執行金鑰儲存管理計畫，應包含：安全的金鑰配置及管理方法；定期回收金鑰，至少每年一次；銷毀過期、失效的金鑰；當發現金鑰疑似被複製外洩時，應有立即中止或替換機制，與通知程序；避免金鑰在非授權下被替換；建立金鑰的雙重共有控制機制；金鑰的儲存位置應盡量減少；所有的金鑰存取都要留下記錄。

    每個企業對加密需求都不同，某些企業要求使用特殊加密演算法，並對於存取金鑰的權限有嚴格限制，也有些企業只對特定資料加密，並把金鑰交給信任的雲端供應商管理。
13. 保護資料傳遞溝通時的安全：利用 SSL/TLS 和 IPSEC 安全通訊協定。
14. 導入防制資料外洩（DLP）機制。
15. 確保應用程式所處理的資訊都被安全保護。

（四）強固的存取及身分管理

16. 最低權限的架構：應確保使用者的存取權限是適當的，並且存取機制受到安全保護。包括定期檢查使用者存取權限列表，確認擁有權限者才能存取系統；當要存取管理者功能時，使用個人憑證搭配遠端 VPN；傳送及儲存密碼時需要加密；確保所有系統都有適合的認證及密碼管理功能。
17. 聯邦式的身分管理：當要界接各種雲端環境時，聯邦式的身分管理十分重要。許多企業部署雲端會從建置私雲或混合雲開始，與原有 IT 後端系統的整合成為重要課題，部署成功與否，端視企業現有的安全管理架構是否能延伸到雲端。在公雲環境中，企業需要一套通用且以標準為基礎的身分認證機制──聯邦式的身分認證通訊協定，例如 OpenID 或 SAML（Security Assertion Markup Language），才能提供使用者無間斷地存取各種雲端服務。

（五）建立應用程式與環境的自動佈建（provisioning）

集中控管的雲端環境中，自動佈建防護（automated provisioning）的功能至為關鍵。

18. 制訂應用程式自動佈建的計畫：確認虛擬映像檔的自動佈建符合權限控管及授權，且具安全機制；所有變更或取消佈建的動作都需留下記錄；定期檢視記錄，以確保最低存取權限原則；制定銷毀舊映像檔的機制；虛擬資源應依照政策組合搭配，並透過自動化安全組態管理以確保設定一致；在安全的虛擬化環境中，安全機制也以 SOA 方式來提供，包括身份認證、稽核、金鑰管理、政策及其他服務。

（六）建立 IT 治理及稽核管理計畫

為了法規及稽核需要，須制定計畫說明時、地、蒐集日誌的方式與稽核資訊。

19. 隱私管理計畫：個人資料及企業機密資料的蒐集、處理、利用、刪除都需建立政策文件；為執行上述政策，建立一套監控稽核程序；進行教育訓練；訂定資料外洩事件通知程序。稽核人員及管理階層必須明白雲端環境中的個資安全威脅。
20. 稽核管理計畫：與法務人員討論，雲端系統必須符合哪些法規，例如 ISO 27001、PCI DSS、個資法等；建立相關規範文件並定期檢視。
21. 確保資料的處理、儲存遵照法規及跨境保護要求辦理，並整理成文件。不同服務需要不同程度的安全，其中最重要的需求之一，是第三方的安全稽核與驗證，政府單位尤其需要正式的驗證或證書。

（七）建立弱點及入侵管理計畫

22. 定期更新防毒、入侵偵測／防禦系統。

（八）測試與驗證

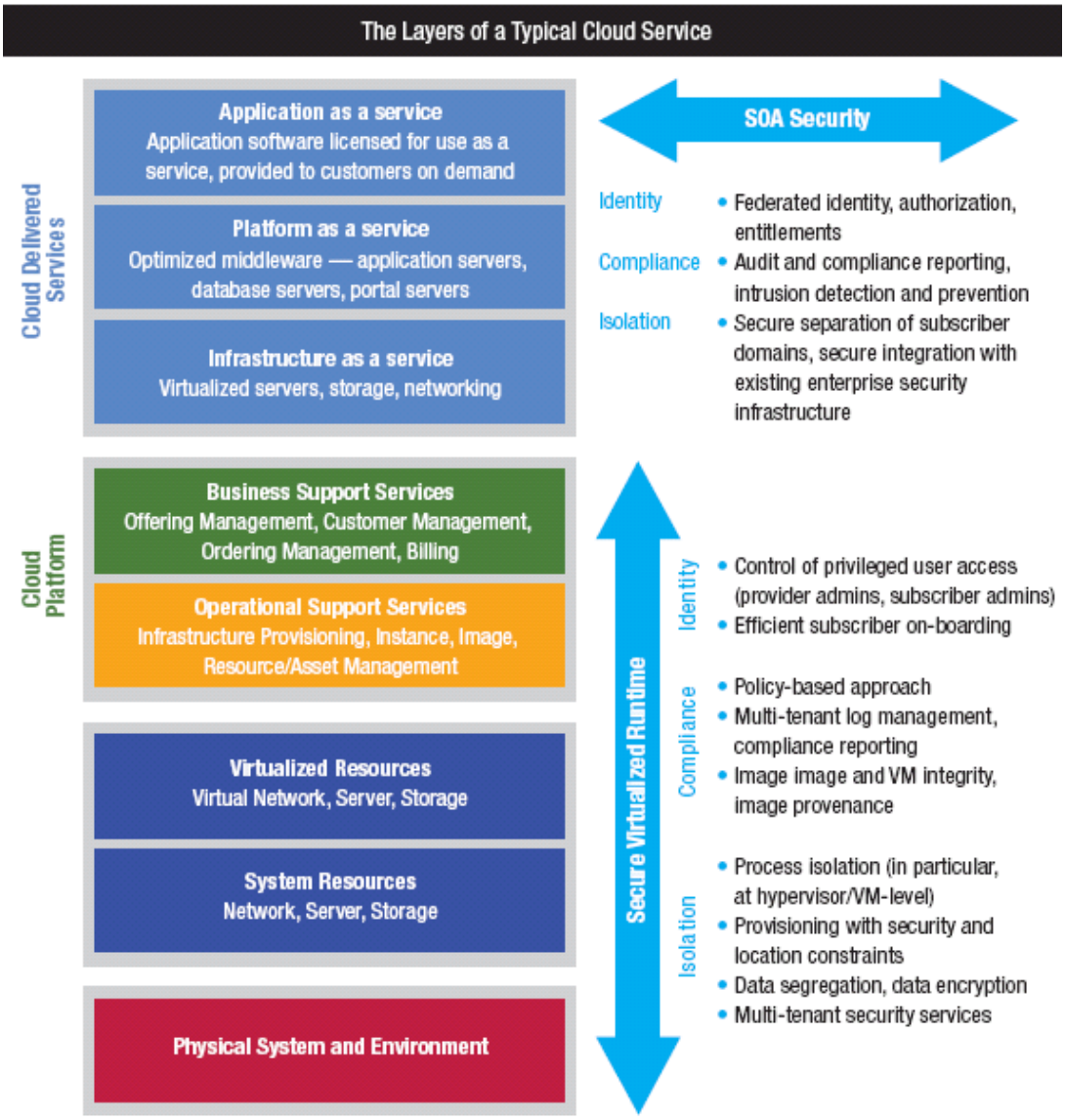
為了建置完善的雲端 IT 環境，必須部署不同的測試驗證機制。

23. 導入變革管理的程序：雲端系統必須遵照組態變更管理程序，包括變更請求須留下記錄、衝擊評估說明、上線前測試結果並簽核、回復到前一階段的程序。
24. 導入資料加密及存取計畫：測試資料庫及其他儲存媒介透過適當加密技術受到保護。
25. 發展安全的應用程式開發及測試計畫，包含：所有修補程式在上線部署前需要經過驗證；區隔測試及開發環境；劃分不同人員負責測試、開發及管理的工作；在測試環境中不要使用正式系統中所含機密資料或個資；測試環境轉為正式上線環境前，移除所有測試資料或管理資訊；上線前確認所有測試帳號已移除；上線前進行原始碼檢測。所有網頁應用程式應遵照 IBM 或 OWASP 等安全程式碼準則，並定期進行源碼檢測。

總結來說，雲端安全由 SOA 安全層與安全的虛擬化環境所組成，如圖三。比起企業 SOA 環境，雲端運算進一步整合不同供應商的服務，因此更須高度動態、敏捷。當企業選擇採取混合雲的策略時，應用程式或服務將不會被綁在一個固定的基礎架構，而能隨著企業需求變化而快速調整。

若要快速將資料從企業後台系統搬移到私雲或混合雲上，需支援更多其他通訊協定的雲端平台。許多雲端環境只專注特定的通訊協定，例如身分認證機制就選擇 OpenID 或偏好某種架構方式，如 REST（representational state transfer）。但企業用的雲端運算環境應能提供彈性及選擇，IBM 可支援以 REST 為基礎的介面及通訊協定，也支援 SOA 安全所

需要的各種安全服務。



圖三：雲端安全由 SOA 安全層與安全虛擬環境所組成