應用 ISO/IEC 27018，穩扎雲端服務個人資料管理

撰稿：BSI 英國標準協會雲端安全暨 PCI DSS 產品經理
吳晟熙 Peter Wu
Peter.Wu@bsigroup.com

調查顯示 企業非常關切雲端服務的安全性議題

近年來，各類雲端服務的應用日益廣泛，但是企業對於雲端服務的安全信任程度卻未見顯著的提升。例如，2014 年英國電信對全球的IT相關決策者進行調查，當時對雲端安全性提出疑慮的就佔了 76%。2016 年 iThome CIO 大調查的結果顯示，企業採用公有雲或混合雲的比例來到歷年新高(33.1%)，但依據雲端安全聯盟(CSA)公布的雲端安全調查報告 “The Treacherous 12” 顯示，資料外洩仍是企業於使用雲端服務上最關切的議題。對企業來說，租用雲端服務意味者將失去部分(或絕大部分)的資訊科技治理能力，在此限制下確保個人資料的處理符合法令法規規範及其安全性會是極度重要的議題。

ISO/IEC 27018

第一個針對雲端服務提供商如何於公有雲保護個人資料的國際標準

唯有充分瞭解雲端服務提供商對於其雲端服務採用的資料保護措施，企業才有可能提高對雲端服務的信心。因此，ISO 組織公佈了 ISO/IEC 27018，此標準制定的主要目的為將雲端服務的資料保護措施透明化，增強企業對於雲端服務的信任程度。通過 ISO/IEC 27018 驗證的雲端服務提供商可以宣告，在此國際標準的架構基礎上，個人資料處理的適法性、準確性、透明化及安全性等各面向均受到保護，包括公有雲運算、個人資料處理、各類雲端的服務模式、和使用雲端服務的企業都將受益於 ISO/ IEC 27018。

ISO/IEC 27018 規範責任及義務，明確解決企業所關切的個人資料保護議題

實施 ISO/IEC 27018 帶給雲端服務提供商與企業有諸多便利性與優勢，包括：

- 協助企業及雲端服務提供商進入契約化的協議
- 使雲端服務提供商在相關事務上更加透明，企業可選擇有良好治理的雲端個人資料處理服務
- 幫助雲端服務提供商擔任個人資料處理者時遵守適用的義務、合約及法規的規範

租用雲端服務或評估租用雲端服務的企業可參考 ISO/IEC 27018 的作業規範，應用於建立企業使用雲端服務的資訊安全政策、建立遴選雲端服務提供商的評估項目、確立雲端服務提供商與企業間雙方的資料保護責任、雙方書面化協議和契約的訂定、合約終止後的資料處理程序及其他相關作業上，以因應企業高度倚賴雲端化服務的時代。

ISO/IEC 27018 國際標準的架構

ISO/IEC 27018 要求雲端服務提供商於受委託處理個人資料的範圍內，保護個人資料於生命週期的各項歷程。同時，雲端服務提供商有義務對委託者充分說明蒐集、處理及利用個人資料等議題，因此標準架構由兩部分組成，分別說明如下：

1. ISO/IEC 27002：2013

在 ISO/IEC 27002 資訊安全管理作業規範的基礎上，納入公有雲環境適用的個人資料保護原則。

內 容	ISO/ IEC 27018 增加的指引
資訊安全政策	承諾遵循個人資料保護的法令法規及合約要求
資訊安全支組織	提供雲端服務客戶聯絡窗口
人力資源安全	讓員工知悉擔任公有雲個人資料處理者可能帶來的影響
資產管理	沒有額外要求
存取控制	提供每個客戶帳號管理的權限、使用者註冊和註銷的程序應注重使用者的存取控制被破壞的情形、提供客戶安全的登入程序
密碼學	為了個人資料保護，提供加密的資訊給客戶
實體及環境安全	內含儲存媒體的設備於汰除或重複使用時，應視為其可能包含個人資料
運作安全	當使用個人資料於測試目的為不可避免時，應實施風險評鑑和採取控制措施將風險降到最低、保護資料避免遺失、紀錄個人資料的變更、提供客戶稽核日誌的時機及方式、於文件化的期間內刪除日誌資訊
通訊安全	記錄內含個人資料之實體媒體的進出及確保傳送的安全性
系統獲取、開發及維護	沒有額外要求
供應者關係	沒有額外要求
資訊安全事故管理	資訊安全的審查(涉及到個人資料是否有資料洩漏的發生)
營運持續管理之資訊安全層面	沒有額外要求
遵循性	公有雲個人資料處理者應提供獨立的證據，證明其符合政策及程序

2. 基於 ISO/IEC 29100:2011 隱私權框架的 11 項原則追加控制措施

在 ISO/IEC 29100 隱私治理的框架上，納入公有雲環境適用的個人資料保護原則。

附錄 A	內 容	ISO/ IEC 27018 增加的指引
1	同意及選擇	A.1.1 有關個人資料當事人權利的合作義務
2	目的適法性及規定	A.2.1 公有雲 PII 處理者的目的
		A.2.2 公有雲 PII 處理者的商業使用
3	蒐集限制	N/A
4	資料極小化	A.4.1 暫時性檔案的安全刪除
5	利用、持有及揭露限制	A.5.1 個人資料揭露的告知
		A.5.2 個人資料揭露的紀錄
6	準確性及品質	N/A
7	公開、透明及告知	A.7.1 委外個人資料處理的揭露
8	個人參與及存取	N/A
9	可歸責性	A.9.1 通知涉及個人資料的洩漏
		A.9.2 管理之安全政策及指引的保存期間
		A.9.3 個人資料返還、傳輸及汰除
10	資訊安全	A.10.1 機密性或保密協議
		A.10.2 建立實體資料的限制
		A.10.3 控制及記錄資料還原
		A.10.4 保護離開儲存媒體上的資料
		A.10.5 未加密可攜式媒體及裝置的使用
		A.10.6 個人資料透過公眾網路傳輸的加密
		A.10.7 實體資料的安全汰除
		A.10.8 獨特的使用者ID
		A.10.9 經授權使用者的記錄
		A.10.10 使用者ID的管理
		A.10.11 合約量測
		A.10.12 委外個人資料處理
		A.10.13 預先使用之資料儲存空間上資料的存取
11	隱私遵循	A.11.1 個人資料的區域位置
		A.11.2 個人資料的預期目的地

ISO/ IEC 27018 國際標準驗證的考量與準備

雲端服務提供商所管理的資訊不應僅被視為單純的資料，而應考慮「含有個人資料」的情況下能否合理的運用。雲端服務提供商可藉由 ISO/IEC 27018 稽核證明其符合 ISO/IEC 27001 以及 ISO/IEC 27018 對公有雲個人資料處理者的額外控制措施要求，合理的運用驗證來確保雲端上的個人資料得到適當的保護。

雲端服務提供商若想要取得 ISO/IEC 27018 驗證，需要建置資訊安全管理系統以符合下列要求：

- ✓ 已將 ISO/IEC 27001 管理系統標準建立在營運風險的基礎上，可從 ISO/ IEC 27018 選擇及導入風險管理的控制措施，以保護公有雲的個人資料處理環境
- ✓ 如果沒有選擇 ISO/ IEC 27018 的任何控制措施，紀錄沒有選擇的適當理由
- ✓ 視雲端服務模式（IaaS、PaaS或SaaS）選擇和導入適用的控制措施
- ✓ 擔任公有雲個人資料處理者時，因應其他要求而實施ISO/IEC 27018 以外的控制措施

結語

在沒有可信賴的驗證機制下，風險是無法評估的。由於企業藉由作業委外來抑制成本的作法相當普遍，個人資料存放在何處以及雲端服務提供商是否遵照契約化協議的規範等議題都不夠透明，無法有效建立企業對於雲端服務的信賴，例如：個人資料的處理是否存有轉包和分包的情形？個人資料是否有對外揭露？因此，實施 ISO/IEC 27018 以完備個人資料的保護就顯得格外重要。國際知名的雲端服務提供商例如 Microsoft Azure、Amazon AWS、Dropbox 等已先後取得 ISO/IEC 27018 驗證，公有雲上的個人資料保護機制與規範已有明確的共識及目標。企業及雲端服務提供商應藉由實施 ISO/IEC 27018，來確立雙方的資料保護責任、書面化協議和契約的訂定、合約終止後的資料處理程序及其他相關作業，讓企業受益於雲端化服務帶來的各項便利時，能同時兼顧個人資料保護的各式議題。

BSI 英國標準協會
+886 2 26560333
infotaiwan@bsigroup.com
www.bsigroup.tw

BSI 訓練學苑
雲端服務之資訊安全
暨個資保護相關課程<點此參考>
training.taiwan@bsigroup.com