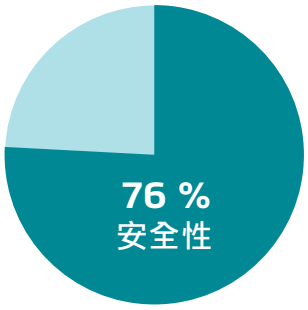
ISO/IEC 27018

公有雲個人資料(PII)處理者之個資保護作業規範

ISO/ IEC 27018 是第一個為在公有雲上保護個人資料（PII：Personal Identifiable Inforam-tion）所提供的專業國際標準。BSI台灣已開始提供 ISO/ IEC 27018的驗證服務。

調查顯示 雲端使用者非常關切安全性問題

近年來使用雲端服務的客戶急劇增加，但是對於安全的信任度卻比以往更低。根據2014 年英國電信對全球的 IT 相關決策者進行調查，對雲端安全性提出疑慮的就佔了 76%。



使用雲端服務最關注的部分

* BT（British Telecom）Global study (2014)

使用 ISO/IEC 27018 提高雲端服務使用者的信賴感

ISO/IEC 27018 是第一個用來保護公有雲個人資料安全性的國際標準。ISO/IEC 27018 可以消除使用者對雲端服務的不信任感。對於雲端的服務提供商而言，它提供了值得信賴的作業規範，也解決了用戶端關切的重要議題。

BSI 與其他企業組織合作，發展出可提供公有雲運算、個人資料處理服務、所有雲端的服務模式和具規模企業都適用的 ISO/ IEC 27018 驗證方案。

ISO/IEC 27018 的優點

實施 ISO/IEC 27018 的優點，列舉如下：

- ✔ 協助雲端服務顧客及雲端服務供應商之間協議的契約化
- ✔ 雲端服務供應商有義務確實遵守法規及合約的規範
- ✔ 使雲端服務供應商在相關事務上更加透明，雲端服務顧客可選擇有良好治理的雲端個人資料處理服務
- ✔ 審查可能發生的風險，以此機制確保雲端服務供應商遵循其義務

ISO/ IEC 27018 國際標準的架構

ISO / IEC 27018 由兩部分組成，大致如下：

1. **ISO/IEC 27002：2013**
   為補強 ISO/IEC 27002 對公有雲個人資料的資訊安全管理，納入個人資料保護的指導原則。

條號	內　　容	ISO/ IEC 27018 增加的指引
5	**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
6	**資訊安全支組織**	提供雲端服務顧客聯絡窗口
7	**人力資源安全**	讓員工知悉公有雲個人資料處理者可能帶來的影響
8	**資產管理**	沒有額外要求
9	**存取控制**	提供每個顧客帳號管理的權限、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、提供顧客安全的登入程序
10	**密碼學**	為了個人資料保護，提供加密的資訊給客戶
11	**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
12	**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、提供顧客日誌的時機及方式、和於文件化的期間內刪除日誌資訊。
13	**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
14	**系統獲取、開發及維護**	沒有額外要求
15	**供應者關係**	沒有額外要求
16	**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)
17	**營運持續管理之資訊安全層面**	沒有額外要求
18	**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

ISO/IEC 29100 針對個人資料保護於資通訊方面提供了一個治理框架，制定的個人資料保護原則可適用於公有雲環境。

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 管理的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 創建實體資料的限制
		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 管理
		A.10.11 合約量測
		A.10.12 委外個人資料處理
		A.10.13 預先使用的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

依據 ISO/IEC 27018 稽核公有雲的個人資料處理者，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個人資料得到適當的保護。

依據上述稽核判斷資訊安全管理系統是被有效實施時，將授予 ISO/IEC 27018 驗證。

公共雲個人資料處理者想要取得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，風險管理的控制措施可從 ISO/ IEC 27018 選擇及導入，以保護公有雲服務的個人資料處理環境
- ✔ 如果您沒有選擇 ISO/ IEC 27018 的管理措施，紀錄沒有選擇的正當理由
- ✔ 視個人資料處理者的角色（IaaS、PaaS或SaaS）選擇和導入控制措施
- ✔ 作為公有雲個人資料處理者因應其他要求而實施 ISO/IEC 27018 以外的控制措施

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>
training.taiwan@bsigroup.com