CSA STAR Certification 及 PCI DSS 更新版本摘要說明

撰稿: BSI 英國標準協會
撰文者: 吳晟熙 產品經理
Peter.wu@bsigroup.com

繼 ISO 27001 資訊安全管理系統於 2013 發布新版本後，國際上其他資訊安全相關的驗證標準也陸續更新版本，其中以雲端安全的 CSA STAR Certification 及規範支付卡交易安全的 PCI DSS 兩份標準最具有代表性。

一、CSA STAR Certification

CSA STAR 驗證於 2013 年由雲端安全聯盟(Cloud Security Alliance，CSA)與 BSI 共同推出後，全球通過驗證的雲端服務提供商已超過 20 家。CSA STAR 驗證的組成要素包括:

1. CSA STAR 驗證的範圍(scope)需先行/同時通過 ISO 27001 的驗證;
2. 以雲端控制矩陣(Cloud Control Matrix，簡稱 CCM)作為稽核的準則;
3. BSI 制訂的管理能力模型(Capacity Model)作為評估管理能力及授與獎牌等級的依據。

2014 年，CSA 及 BSI 更新了開放式驗證架構(OCF)Level 2 的其中兩個要素，分別為發佈雲端控制矩陣(CCM) 3.01 版及新版管理能力模型(Capacity Model)。

1. **雲端控制矩陣(CCM) 3.01 版**: CSA 於 2014 年發佈 CCM 3.01 版，對應 ISO 27001:2013 (CCM1.4 版對應 ISO 27001:2005)。CSA 也重新編排了控制措施章節，加入 Mobile Security、Supply Chain Management, Transparency and Accountability、及 Interoperability & Portability 三個全新的章節，章節數自原有的 11 個增加到 16，控制措施數也自 98 個增加到 133 個。此外，CSA 於官方網站上公佈，配合 ISO 27001 的轉版作業，CSA STAR 驗證自 2015 年 3 月起以 CCM 3.01 版作為驗證準則。

   (CCM 3.01 版: https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/)
   (參考網址: https://cloudsecurityalliance.org/star/certification/#_overview)

2. **新版管理能力模型(Capacity Model):** 在初始版管理能力模型的設計，各個控制措施以溝通、程序、人員技能、領導力、監督及量測等五個面向進行評估，再依據管理

能力的成熟等級分別授與 1~15 的給分。在新版的管理能力模型設計上，保留 1~15 分的成熟度等級給分，但整合原有的五個評分面向至單一評分表上，使組織不管在執行內部稽核或是第三方驗證機構執行外部稽核時，讓稽核員評分的結果更趨於一致。

(參考網址: https://cloudsecurityalliance.org/star/certification/#_resources)

二、PCI DSS 支付卡產業資料安全標準

PCI DSS 是五家國際支付卡品牌基於為支付卡產業保障持卡人資料安全所共同建置的全球統一規範。為保障其他持卡人的資料安全，繼而針對安全管理、政策、程序、網路配置與軟體設計等多方需求，所訂定之資料安全標準。所有從事持卡人資料之保管、處理、傳輸的機構，包含發卡機構、收單機構、商家，及任何服務供應商，均須關注其組織是否符合 PCI DSS。

2015 年 4 月 15 日 PCI DSS 更新版本至 3.1 版，不再視 SSL 及早期版本的 TLS 為安全的服務協定。3.1 版與 3.0 版的主要差異說明如下:

1. 2016 年 6 月 30 日後，SSL 及早期版本的 TLS 不能再被使用於保護信用卡交易資料;
2. 2016 年 6 月 30 日前，現行應用 SSL 及早期版本的 TLS 的部分必須實施風險減緩計畫，可參詳 PCI SSC Information Supplement: Migrating from SSL and Early TLS (https://www.pcisecuritystandards.org/security_standards/documents.php)
3. 即日起，新的建置不可使用 SSL 及早期版本的 TLS;
4. Point-of-sale (POS)/Point-of-interaction (POI) terminals 如經過確認不受 SSL 及早期版本 TLS 相關弱點影響，可於 2016 年 6 月 30 日後繼續使用該些服務協定。

三、結語

提供雲端服務或是處理信用卡交易資訊的組織，應儘快評估及實施 CCM 3.01 版及 PCI DSS 3.1 版的差異要求，降低資料遺失/外流的可能性，進而提升組織的形象和信譽。