以 ISMS 整合管理國際標準與合規性

談 ISO 27001、資料保護、隱私和 PCI DSS

網際網路與電子商務蓬勃發展，網路安全管理已不再只侷限單一領域，企業組織還需一併考量其他關聯風險，其中特別是因為隱私資料與信用卡交易資料的管理不當而引發爭議、盜領或詐騙案件，在這幾年間也頻頻登上國際新聞頭條。社會大眾不僅驚覺自己曾留下的資料和數位足跡可能遭到濫用或盜用，也更具有資訊安全意識，這讓**企業組織如何有效分配資源管理網路安全風險**，以及如何**善盡自己遵法的責任與義務**，成為關鍵的管理議題。

本文將剖析如何應用資訊安全管理系統（ISMS）來推動一套整體性的作法管理如 ISO/IEC 27001、PCI DSS 支付卡產業資料安全標準和隱私等安全標準與法令遵循的義務。

透過一套系統持續管理合規、主管機關監管及法律上的資訊安全義務，可以鑑別出重疊的要求、提升流程效率，並為企業組織提供更好的能見度和保證。為了實現這項整合管理方式，我們**建議採用大家最熟悉的 ISO/IEC 27001 – 資訊安全管理系統（ISMS）作為模型**。

ISO/IEC 27001 資訊安全管理系統

ISO/IEC 27001 是國際公認的管理系統，可管理資訊安全治理風險並提供一個最佳實踐框架，描述實施一套合規且有效的 ISMS 所需的關鍵要求。這些要求與企業組織正在進行的治理及良好的系統管理有關，並預期確保：

- 不斷意識和理解組織的運作環境以及內部和外部利害關係者的需求
- 高階管理者的領導與支援必須到位，以推動政策和分配職務及責任
- 進行規劃以確保 ISMS 與組織的目標保持一致
- 提供支持和資源以有效地運行系統
- 進行風險管理，以確保組織的風險偏好（Risk appetite）和控制措施能切合外部和內部的風險因素
- 對系統進行監測和持續改進

ISO/IEC 27001 標準附錄 A 包含 114 項控制措施，其中的風險處理（Risk Treatment）應該要能夠解決所識別出的資訊安全風險。

利用 ISO/IEC 27001 管理更廣泛的法規、法律和產業特定要求

除了建議的控制措施外，ISO/IEC 27001 還要求組織徹底瞭解法律和法規義務，並將其納入管理系統。在本文所設定的案例中，必須同時考慮資料保護和 PCI DSS，將透過較高層次的視野來分析，看到這兩項規範內重疊的要求。

隱私（Privacy）

歐盟一般資料保護規範（GDPR）於 2018 年 5 月正式生效。這一項法規建立在歐盟 1995 年頒布之個人資料保護指令（Data Protection Directive）的基礎上，儘管它與現有的歐洲資料保護原則沒有太大區別，但確實帶來嶄新的概念，可**視您組織持有的個人資料機敏性及比例原則，來判斷能否透過 ISMS 的合規計劃整合到組織的安全性和合規性管理中**。

GDPR 特別適用於以下領域：

- 增強風險管理流程，將隱私視為首要考慮因素
- 盤點（Inventory）與當責（Accountability）
- 與客戶和員工的溝通方式

- 個人隱私權和支援程序
- 近用權（access requests）的更改
- 同意（consent）和法律依據
- 處理兒童資料
- 外洩事件通報
- 隱私衝擊分析（PIAs）和「隱私保護設計（Privacy by design）」
- 資料保護長（DPOs）
- 跨境資料傳輸

人們普遍認為歐盟 GDPR 是一份複雜的法律文件，著重於法治基礎。因此，**將歐盟 GDPR 的大部分內容轉化為可付諸實行的行動**，是一項非常重要的任務。

要實踐 GDPR ，組織通常採用的作法是**與國際隱私管理標準保持一致**，以確保這套作法站得住腳。諸如 ISO 29100 和 BS 10012 這類個資管理標準，可**提供強大且有足夠防禦力的隱私管理系統**。同樣，利用 ISO/IEC 27001 管理系統整理歸納上述隱私標準所建議的控制措施，亦可實現統一一致的效率，且能夠透過單一且綜觀途徑檢視兩者的合規性。

但必須注意的是，在有明確的法令規定下，例如 GDPR，**組織應充分考慮法令中的額外要求，才可能讓通過驗證成為法令遵守的有力證明**。考量法令對資料外洩通報時間的規定，組織也必須對敏感的個人可識別資訊（PII）、資料保護長（DPO）的職務和責任、罰款等項目進行特殊分類。

支付卡產業資料安全標準（PCI DSS v3.2.1）

支付卡產業資料安全標準（Payment Card Industry Data Security Standard ），通常簡稱為 PCI DSS，提供一組強制性且詳細的控制措施以保護持卡人資料，適用於特約商店、信用卡資料處理者、收單行、發卡機構和服務提供者。

PCI DSS 的控制措施與 ISO/IEC 27001 附錄 A 的規範相似，但更為具體，並且**是強制性的標準，根據不同的交易量分級以詳細規定組織必須實施的要求**，而非只是基於風險思維來選擇適用的要求。若您的組織恰好有提供或執行信用卡相關服務，可**將 ISO/IEC 27001 作為資安管理的原則，而將 PCI DSS 視為實際上要達成的管理程度**。

由於 ISO/IEC 27001 附錄 A 的要求與 PCI DSS 有部分相同，故透過 ISO/IEC 27001 來管理 PCI DSS 將相對地容易。

範圍（Scope）是關鍵

在標準驗證方面，範圍是一項關鍵因素。在多數情況下，組織的管理系統驗證會考量維護治理流程的成本和人力，以及安全系統的軟體和許可成本，相對應到一項特定服務、部門或系統組合。

我們建議，在整個組織中定義並採用最低可接受的安全基礎。如果存在極為重要的資產/系統/服務，則應提高安全管控的程度，以保障其價值。採用這種基於風險的方法可確保以適當的成本開支，保護下列類型的產品或服務：

- 用於創造營收
- 受主管機關監管
- 處理 PII 或信用卡資料
- 涉及智慧財產權
- 透過網際網路進行

因此，在考慮管理系統的範圍時，組織應明智地分配資源以創造最大價值。ISO/IEC 27001 藉由「資產管理」控制領域（Domain）來推動此過程，其中的資訊與系統資產盤點及資產分類扮演關鍵地角色。

藉由瞭解您所擁有的資訊、資訊的流向地和所流經的系統，可以快速辨識和分類在組織內具有關鍵作用的系統。

資產盤點清冊可作為管理的優先順序參考依據，資產分類策略則決定組織該採用哪些方式保護這些資訊系統。例如，您可以規定所有資訊系統都必須採用最低的安全基準，但是，如果該系統係儲存信用卡或敏感性的個人識別資訊（SPII），您的分類策略則可能會規定存放在此系統上的資訊必須予以加密。此控制項涉及許多合規要求，例如：

ISO/IEC 27001

- A 8.1.1 資產清單
- A 8.2.1 資訊分類

PCI DSS v3.2.1

- 執行摘要第 3 條、第 4.3 條
- 第 2.4 條，維護一份 PCI DSS 範圍內的系統元件清單

歐盟一般資料保護規範（GDPR）

- 第 30 條

在前述情境中，資產分類方式和清冊可滿足 ISO/IEC 27001、PCI DSS 及 GDPR 這 3 項領域的資產盤點要求，並帶給組織以下效益：

- 單一來源的系統和資訊資產清冊
- 一致性的管理方法：
    - 資訊分類
    - 資訊處理
    - 資訊保存
    - 資訊銷毀
    - 資訊安全
    - 資訊標籤
    - 近用請求

因此，組織將能夠透過一組治理文件進行審查和維護，並在整個組織中推動驗證，證明已經適當管理其法令遵循的義務。

分類和清冊管理不是這 3 項規範唯一重疊的要求，組織還必須考量：

- 治理、角色和責任
- 風險評估
- 使用者意識
- 存取控制
- 日誌記錄和監督
- 事件回應和外洩通知

- 變更控制〔隱私設計（Privacy by Design）和隱私衝擊分析（PIA）〕
- 委外廠商管理

當然，這 3 項規範之間還有許多重疊之處，必須在控制基礎上加以管理。

結語

資訊安全和合規的最佳推動力係來自董事會和高階管理者，在這些層級上能夠綜觀全局，以更宏觀的角度來進行管理，明確且適當地下放職務與相關責任。

讓高階管理團隊參與風險與合規性管理政策的溝通，有助於擬定明智的決策，進一步確保管理系統能在未來更廣闊的商業領域中給予更好的支援。

整合式的 ISMS 可給予您提升效率和發現重工的機會，提供組織治理、風險管理和合規程度的證明與可視性。如果您的組織同時管理多項標準規範的需求 1. 資安（如：ISO 27001、NIST 美國網路安全框架、資通安全管理法） 2. 個資管理（如：BS 10012、ISO 29100、GDPR） 3. 雲端安全（如：ISO 27017、ISO 27018、CSA STAR），或是組織規模較小，不妨試試透過一套 ISMS 管理系統來收納管理各式合規要求。●

BSI 資訊安全與網路安全系列課程

資訊安全	個資管理	雲端安全	服務管理	營運持續	產業資安
ISO 27001 資訊安全管理系統 基礎課程 建置課程 風險評鑑課程 內部稽核員課程 主導稽核員課程	BS 10012 個人資訊管理系統 基礎課程 建置課程 內部稽核員課程 主導稽核員課程 主導稽核員/稽核員轉版課程	雲端服務資訊安全管理系統 Cloud 主導稽核員課程	ISO 20000 服務管理系統 基礎課程 建置課程 內部稽核員課程 主導稽核員課程	ISO 22301 營運持續管理系統 基礎課程 主導稽核員課程	PCI DSS 支付卡產業資料安全標準 以 PCI DSS 強化電子支付服務的資訊安全管理及法規遵循課程 內部稽核員課程 主導稽核員課程
NIST 網路安全框架 **建置課程**	ISO 29100 隱私框架基礎課程 主導稽核員課程	ISO 27017 & ISO 27018 建置課程		BSI 營運衝擊分析課程	ISO 27799 健康醫療資安基礎課程
	GDPR 歐盟一般資料保護規範 基礎課程				

課程詳情請洽BSI 訓練學苑：02-26560333 | training.taiwan@bsigroup.com

● 洽詢 BSI | 稽核驗證、產品測試、BSI 訓練學苑、VerifEye 認證平台、BSOL 標準資料庫