

創新科技環境下的資訊管理重點

雲端資訊安全、個資隱私保護、營運持續服務

(Information Security, Personal Information Protection, Business Continuity)

蒲樹盛(Peter Pu)

peter.pu@bsigroup.com

BSI 英國標準協會 副總經理(Vice President)

IRCA 國際註冊主導稽核/主任講師

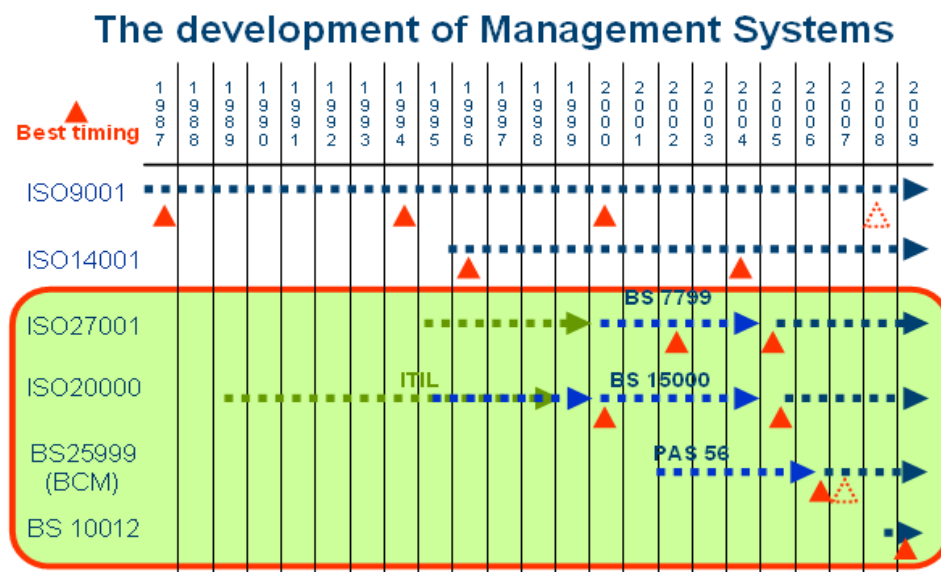
科技創新一日千里

科技日新月異，內容漸趨豐富的電子書、功能愈加強大的智慧型觸控手機、容量持續增加的隨身儲存裝置，發展到遠端集中控管的資訊雲端運算，不斷展示出創新科技對人類生活及組織運作模式的劇烈改變。這些資訊科技的跳躍成長，也形成組織對資訊改造與資訊管理的一大挑戰。

本文特別摘要提出三大創新科技環境下的資訊管理重點：雲端資訊安全、個資隱私保護、營運持續服務，提供管理階層或承辦人員作為因應科技發展及國際趨勢下的資訊管理重點參考，應可順應潮流，提供組織享受科技及安全兼具的營運環境。

下圖為品質及資訊相關管理系統標準的發展及發佈圖示：

- 資訊安全 Information Security Management System (ISMS) – ISO 27001
- 個資隱私 Personal Information Management System (PIMS) – BS 10012
- 營運持續 Business Continuity Management(BCM) – BS 25999



雲端資訊安全

近年來，雲端(Cloud Computing)概念及應用的話題不斷，從 Apple iPhone 到 Facebook 都充滿了令人興奮的話題性。IDC(國際數據資訊中心) 提出未來 5 年雲端服務平均年成長+26%；Apple iPhone 超過 10 萬個下載軟體提供 USD 10 幾億商機；如果將機房設備維護、網路管理與軟體升級通通交給雲端處理，根據麥肯錫的研究報告，一家規模兩百人的公司，光是軟體的部分，至少可以比現在省下三〇%的成本。市場調查機構將雲端運算列為 IT 產業未來十大趨勢首位。

運用雲端技術，營運成本及效率或許可能更有競爭力，但安全防護的挑戰也隨之而來，尤其是資訊安全、個人隱私，及遠端集中管理的高可用率保證程度(確保營運服務不中斷)。大家可以輕易的上傳、下載並交換各種類型資訊及影像，也造成組織必須正視此類應用的資訊安全風險。

ISO 27001 是國際資訊安全管理系統標準，透過推動並實施其相關指引及控制措施，將可以幫助組織鑑別、管理和減少資訊所面臨的各種資訊安全風險。ISO 27001 包括建置組織管理系統所需要的 PDCA 管理架構及廣泛的安全控制措施要求，其中的 11 個控制措施章節（共 133 項控制措施）：

- 安全政策 --- 表達對資訊安全管理系統的支持和承諾。
- 資訊安全組織 --- 建立一個管理架構，用於公司內部資訊安全的管理和控制，以及執行現有的資訊安全規定。
- 資產管理 --- 確保對組織各項資產的安全進行有效保護。
- 人力資源安全 --- 明訂所有人員在安全方面的職責和角色。
- 實體和環境安全 --- 對組織營運場所及人員提出簡單明確的安全要求。
- 通訊與作業管理 --- 盡可能完善公司內外的溝通聯繫，以利於資訊安全管理系統的順利運行。
- 存取控制 --- 管理對資訊的存取行為。
- 資訊系統取得、開發和維護 --- 確保公司 IT 專案和相關的支援活動已實施安全控制，必要時進行資料管制和加密。
- 資訊安全事故管理 --- 確保在某種程度上傳達與資訊系統有關的資訊安全事件與弱點，始能採取即時的矯正行動。確保實施一致與有效的方法管理資訊安全事故。
- 營運持續管理 --- 發展和維護企業營運持續計劃，保護關鍵的業務活動免受重大災難或中斷的影響。
- 符合性（遵循性） --- 符合資訊安全法令或規定的相關要求。

個資隱私保護

民眾引領期盼已久的「個人資料保護法」終於在 2010 年 4 月 27 日在立法院三讀通過，除了代表台灣在個人資料的保護及個人隱私的尊重方面有了具體規範外，更象徵台灣在人權保障方面進入新的里程碑。

有鑑於個人資訊保護的重要性愈來愈高，全球各國政府均立法規範確保個人資料受到適當保護與運用。日本在 2003 年通過日本版的《個人情報保護法》，明訂只要擁有 5 千筆以上個資的政府單位或企業，都必須做好防範資料外洩的措施。為了讓政府和企業有遵循的參考，日本積極規畫資訊安全管理系統 ISMS 認證基準，並成功導入 JISQ 15001 隱私標誌制度。並在 2005 年獲得日本內閣認可，發行日本隱私權證照，配合日本個人資料保護法全面實施，協助政府推動隱私權。

BSI 英國標準協會於 2009 年正式發佈 BS 10012:2009 個人資訊管理系統 Personal Information Management System (PIMS)；本標準具體說明對個人資訊管理系統的各项要求。個人資訊管理系統參照 OECD 的隱私權綱領(Privacy Framework)提供了一套 PDCA 管理架構，讓組織能維持和改善對資料保護法律及優良實務的遵循。本國際標準的目的便是希望協助組織建立個人資訊管理系統 (PIMS)，作為整體資訊治理基礎的一部分。

個人資訊在蒐集、使用、儲存、傳遞及歸檔或銷毀的過程中，牽涉的使用者既廣且深，無論管理面或技術面的知識，均具備相當程度的專業及技巧，各組織應妥善規劃透過適當的教育訓練達成效果，除可強化組織知識管理外，更可透過個人證照的取得，提高個人價值。

在「個人資料保護法」正式通過的此刻，組織應積極著手規劃並實施針對個人資訊保護的相關防護工作，參考國際手法，詳實檢視現行工作流程中個人資訊的處理細節，結合預防和控制措施及程序，確認已有足夠的防護管理能力。

營運持續服務

企業經營強調品質及客戶滿意，在創新科技的發展下，e 化已是許多企業提昇競爭力的明確作法。高度資訊應用發展過程中，除持續創新的服務內容品質及資訊安全外，如何確保營運服務不中斷，提供優質穩定可靠的系統服務，已是提昇品質及客戶滿意的基本要求。

營運持續管理系統(BCMS, Business Continuity Management System)便是在持續的高度需求下產生，且受到國際高度重視，各組織均積極導入與實施。BS

25999 為英國標準協會 (BSI, British Standards Institution) 所推動的營運持續管理系統標準。BS25999 分為 BS 25999-1 & BS25999- 2 兩部分，其中 BS 25999-1 已於 2006 年 11 月發佈，BS 25999-2 亦於 2007 年 11 月正式發佈。

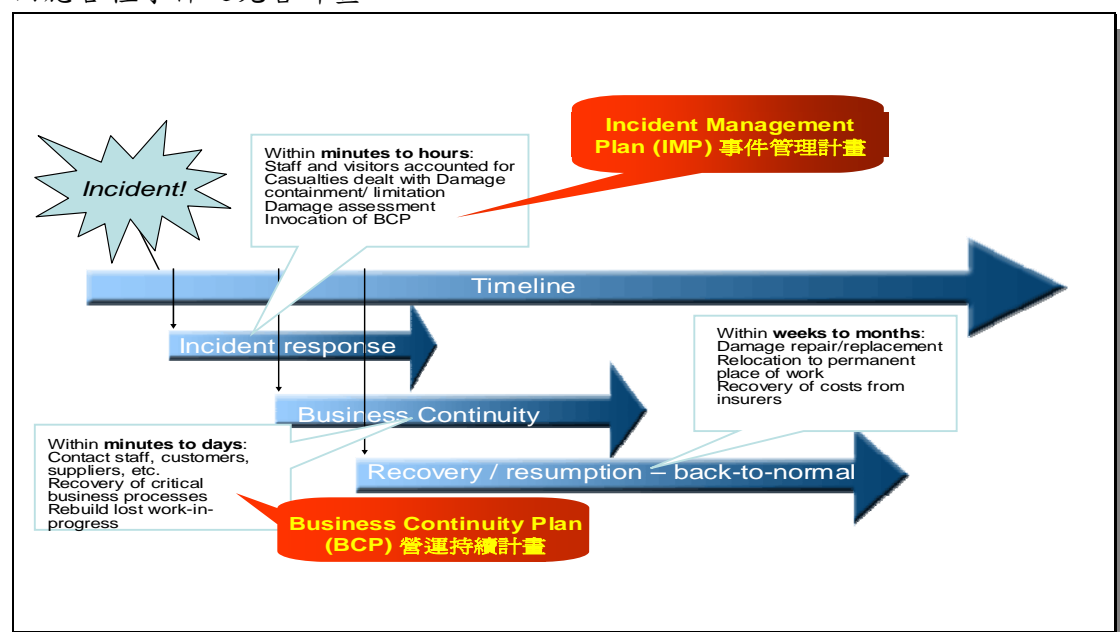
美國國土安全部 (DHS, Department of Homeland Security) 已宣佈計畫採行 BSI 英國標準協會領導世界的營運持續管理標準 BS 25999，做為自願性民間備戰鑑定與驗證方案 (PS-Prep, Voluntary Private Sector Preparedness Accreditation and Certification Program) 使用的標準之一。

PS-Prep 是因應 911 恐怖攻擊事件而發展的計畫，目的是要提升全國恢復運作的能力，改善民營部門的準備程度，為民營部門的準備建立一套共同的標準，包括災難管理、緊急事件管理及營運持續計畫。國土安全部的任務是發展綜合的全國策略，並協調實行，以確保美國的安全，免於恐怖份子的威脅或攻擊。

每一年都有數千家公司行號面臨業務營運中斷的風險，這些風險可能小至斷電等日常中斷的影響，或不利的天氣狀況，大至大規模的恐怖攻擊。企業的營運中斷可能造成「連鎖效應」，嚴重時甚至可能危害全國和國際的基礎建設。美國此時對良好營運持續指引的需求，從未如此強烈。

BS 25999 提出建立和維持有效營運持續管理系統的要求，讓組織能有效預期營運中斷，並做好準備。這可能表示組織必須能在無事先通知下，快速召集臨時人員或搬移工作場所：每個組織面臨的風險不同，但 BS 25999 能協助組織判斷它們需要什麼安排。在目前全球風險大增的趨勢下，似乎沒有組織能保證不會發生意外事件，更遑論都能安然度過事件的考驗。

事件發生後，通常會歷經幾個階段 (請參考附圖- Incident Timeline)；事件發生初期的重點在於損害防阻，有賴預警及通報系統，立即啟動應變程序，避免事件演變成嚴重事故，甚至導致組織危機。組織應於事件演變的各個階段發展建立因應各種事件之完善計畫。



圖、Incident Timeline (BS 25999-1)

透過參照前述標準，組織將可建立良好的預防管理制度，滿足利害關係人之要求及信心。