

資訊安全管理系統

政治大學

電子計算機中心

劉勝雄

Certificate

This is to certify that

Sheng-Shyong Liu

has successfully completed a

BS 7799 Lead Auditor Course

following five days training

organized by

BSIP Training Services

and has passed the examination



Certified by: General Manager
Date: 09 July 2004
Certificate No: BSIP/TRAIN/7799/LA070904

BSI Pacific Limited 2301, 23/F, Caroline Centre, 28 Yun-Feng Road, Causeway Bay, Hong Kong
Tel (852) 2742 5628 Fax (852) 2742 8727 www.bsi-global.com

A member of the BSI Group

Disclaimer: Clients using BSI for certification will receive no preferential treatment and client data will be treated as confidential and divulged to another member of the BSI Group without written permission.

MCK301/ISSUE 3/TS/0305/SHDDP

BSI
Management
Systems



資訊安全管理系統綱要

- ◆ 何謂資訊安全
- ◆ BS7799資訊安全管理規範介紹
- ◆ 資訊安全系統導入、管控與稽核

何謂資訊安全？

- ◆ 資訊對組織而言就是一種資產，和其它重要的營運資產一樣有價值，因此需要持續給予妥善保護。資訊安全可保護資訊不受各種威脅，確保持續營運、將營運損失降到最低、得到最豐厚的投資報酬率及商機。



資訊存在的方式

- ◆ 列印或書面表示
- ◆ 電子方式儲存
- ◆ 郵寄或是電子郵件傳送
- ◆ 影片播放或以口頭說明
- ◆ 無論資訊的形式為何，何種方式與他人共享或儲存，都應以適當的方式加以保護





為維護資訊安全BS ISO 17799:2000 定義

- ◆ a) 機密性 (confidentiality) : 確保只有經授權 (authorized) 的人才能存取資訊。
- ◆ b) 完整性 (integrity) : 保護資訊與處理方法的正確性與完整性。
- ◆ c) 可用性 (availability) : 確保經授權的使用者在需要時可以取得資訊及相關資產。



如何執行資訊安全？

- ◆ 要達到資訊安全就必須實施適當的控制措施，譬如資訊安全政策、實務規範（practice）、程序、組織架構及軟體功能，為了達成營運既定的安全目標，就必須建立這些控制措施。



組織的資訊安全成功因素

- ◆ a) 能反映營運目標的安全政策、目標及活動。
- ◆ b) 與組織文化一致之實施安全保護的方法。
- ◆ c) 來自管理階層的實際支持和承諾。
- ◆ d) 對安全要求、風險評鑑以及風險管理的深入理解。



- ◆ e) 向全體管理人員和雇員有效推廣安全的理念。
- ◆ f) 向所有雇員和承包商宣傳資訊安全政策的指導原則和標準。
- ◆ g) 提供適切的訓練和教育。
- ◆ h) 一個全面與平衡的量測系統，用於評估資訊安全管理的績效及回饋建議，以便進一步改進。




什麼是 BS7799?

- ◆ BS 7799-2:2002是資訊安全管理系統要求的標準。它可以幫助公司鑑別，管理和減少資訊通常所面臨的各種威脅。
- ◆ BS ISO 17799:2000資訊安全管理作業要點



BS ISO 17799

- ◆ 資訊安全管理作業要點
- ◆ 用意是作為參考文件
- ◆ 提供廣泛性的安全控制措施
- ◆ 現行資訊安全之最佳作業方法
- ◆ 包含10個控制措施章節
- ◆ 無法作為評鑑與驗證




BS 7799-2:2002


- ◆ 資訊安全管理系統要求
- ◆ 資訊安全管理系統(ISMS)之建立實施與書面化之具體要求
- ◆ 依個別組織的需求，規定要實施之安全控制措施的要求



BS7799的作業要點

- ◆ 安全政策 --- 為資訊安全提供管理指導和支援。
- ◆ 組織安全 --- 在公司內管理資訊安全。
- ◆ 資產分類與管理 --- 對公司的資訊資產採取適當的保護措施。
- ◆ 人員安全 --- 減少人為錯誤、偷竊、詐欺或濫用資訊及處理設施的風險。
- ◆ 實體和環境安全 --- 防止對營運場所及資訊未經授權的存取、損壞及干擾。

- 
- ◆ 通訊與作業管理---確保資訊處理設施正確和安全運行。
 - ◆ 存取控制---管理對資訊的存取行為。
 - ◆ 系統開發和維護---確保資訊系統已建置安全機制。
 - ◆ 營運持續管理---防治營運活動的中斷，保護中要營運過程不受重大故障或災害的影響。
 - ◆ 符合性---避免違反所有刑、民法、行政命令、管理規定或合約義務及所有安全要求。



資訊安全管理系統之 建立一般要求

- ◆ Policy and Objectives (政策 與 目標)
- ◆ Develop, Implement, Maintain and Continually Improve (開發，實施，
維護及持續改善)。
- ◆ PDCA (計畫，執行，檢查，行動)

PDCA

計畫

建立ISMS

執行

實施與
操作

- ◆開發、實施
- ◆維護及持續改善

維持及
改進

行動

利害相
關團體
管理式
資訊安全

利害相
關團體
資訊安全
要求及期望

監控與審查ISMS

檢查





(BS 7799-2:2002) 資訊安全管理系統之建立及管理(ISMS)

- ◆ 資訊安全管理系統之建立
- ◆ 資訊安全管理系統之實施及運作
- ◆ 資訊安全管理系統之監控與審查
- ◆ 資訊安全管理系統之維護與改善



資訊安全管理系統之建立

- ◆ 組織應：
- ◆ 依據業務、組織、所在位置、資產及技術等特性，定義資訊安全管理系統之範圍及定義資訊安全管理系統之政策。
- ◆ 定義風險評鑑之系統化方法
- ◆ 鑑別各項風險
- ◆ 評鑑各項風險
- ◆ 鑑別並評估風險處理之選項作法
- ◆ 選擇控制目標及控制措施以處理風險
- ◆ 擬定一份適用性聲明書



安全管理系統之範圍及政策

- ◆ 1) 包含設定目標之框架，並建立有關資訊安全之整體方向意識與行動原則。
- ◆ 2) 考慮企業及法律或法規要求，以及合約性的安全責任。
- ◆ 3) 建立策略性、組織性及風險管理之內容，使其資訊安全管理系統得以建立及維持。
- ◆ 4) 藉以評估風險之標準應加以建立，風險評鑑之架構應加以定義。
- ◆ 5) 被管理階層核准。



定義風險評鑑之系統化方法

- ◆ 鑑別一風險評鑑方法，並適合其資訊安全管理系統、已鑑別之企業資訊安全、以及法律與法規要求。設定資訊安全管理系統之政策與目標，以降低風險至可接受程度。決定風險可接受之標準以及鑑別風險至可接受的程度。



鑑別各項風險

- ◆ 1) 鑑別資訊安全管理系統控制範圍內之資產以及該等資產之擁有者。
- ◆ 2) 鑑別這些資產所受威脅。
- ◆ 3) 鑑別這些威脅可能利用之脆弱性 (vulnerabilities)。
- ◆ 4) 鑑別這些資產若喪失機密性、完整性與可用性之各項衝擊。



評鑑各項風險

- ◆ 1) 安全措施失效時可能對企業之傷害應加以評鑑，並將喪失機密性、完整性與可用性可能導致之後果列入考慮。
- ◆ 2) 根據與這些資產有關之主要威脅、弱點與衝擊，評鑑這種失效實際發生的可能性及現行所實施的控制措施。
- ◆ 3) 預測各風險之層級。
- ◆ 4) 決定風險是否可接受或需利用項所建立之標準來處理。



鑑別並評估風險處理之選項作法

- ◆ 1) 採用適當的控制措施。
- ◆ 2) 若風險完全地滿足組織政策及可接受風險(參閱第4.2.1(c)節)之標準，則可在掌握狀況下客觀地接受該等風險。
- ◆ 3) 迴避風險。
- ◆ 4) 將相關之企業風險轉移至其他機構，如保險公司、供應商。



選擇控制目標及控制措施以處理風險

- ◆ 適當的管制目標與控制措施應於本標準之附錄A 中加以選擇，選擇時應依據風險評鑑與風險處理過程之結論為基礎加以判定。



擬定一份適用性聲明書

- ◆ 由4.2.1(g)節所選擇之管制目標與控制措施其選擇之理由應於適用性聲明書中加以文件化。附錄A 中任何排除之管制目標與控制措施亦應加以紀錄。




資訊安全管理系統之實施及運作


- ◆ (a) 有系統的陳述一項風險處理計畫以鑑別適當管理措施、權責及優先順序，以便管理資訊安全風險。
- ◆ (b) 實施風險處理計畫，以達到所鑑別的安全目標，計畫內容包括投資的考慮以及角色與責任的分派。
- ◆ (c) 實施所選之控制措施以符合管制目標。
- ◆ (d) 實施訓練與認知計畫。
- ◆ (e) 作業管理。
- ◆ (f) 管理資源。
- ◆ (g) 實施能加速偵知安全事件並予以回應處理之作業程序及其他控制措施。



資訊安全管理系統之監控與審查

- ◆ (a) 執行監控程序及其他控制措施，以便：
 - ◆ (1) 立即偵知系統處理結果之錯誤。
 - ◆ (2) 立即鑑別安全系統失效及遭他人破壞成功之事件。
 - ◆ (3) 促使管理階層決定是否委託他人或藉由資訊技術之實施均已如預期般實行。
 - ◆ (4) 決定採取哪些措施解決安全漏洞，以反應業務優先順序。

- 
- ◆ (b) 定期審查資訊安全管理系統之有效性(包含符合安全政策、目標及控制措施之審查)，並考慮來自安全稽核、事件、股東及利害關係團體之建議及回饋之結果。
 - ◆ (c) 審查殘餘風險 (residual risk) 與可接受風險 (acceptable risk) 等級，並考慮下數之變化：
 - ◆ (1) 組織。
 - ◆ (2) 技術。
 - ◆ (3) 企業目標及過程。
 - ◆ (4) 已鑑別之威脅。
 - ◆ (5) 外部事件，例如法令或法規環境之變化以及社會環境之變化。

- 
- ◆ (d) 已規劃之期間執行資訊安全管理系統內部稽核。
 - ◆ (e) 定期執行資訊安全管理系統管理階層審查(至少每年一次)，以確保範圍保持適當，及資訊安全管理系統過程之各項改進均已鑑別。
 - ◆ (f) 紀錄對資訊安全管理系統有效性或績效有衝擊之活動與事件。




資訊安全管理系統之維護與改善

- ◆ (a) 實施資訊安全管理系統所鑑定之改進活動。
- ◆ (b) 依據第7.2 及7.3 節採取適當矯正及預防措施。採用從其他組織及本身之安全經驗吸取教訓。
- ◆ (c) 與所有利害相關團體就結果及各項措施進行溝通並取得同意。
- ◆ (d) 確保各項改進措施達到預期目標。

文件要求(一般要求)

- ◆ (a)安全政策與安全目標之書面聲明。
- ◆ (b)資訊安全管理系統之範圍及支援資訊安全管理系統之各程序及控制措施。
- ◆ (c)風險評鑑報告。
- ◆ (d)風險處理計畫。
- ◆ (e)組織為確保有效規劃、操作與控制資訊安全過程所需之書面程序。

- 
- ◆ (f) 本標準要求之各紀錄。
 - ◆ (g) 適用性聲明書。
 - ◆ 所有文件應依據資訊安全管理系統之政策要求隨時可供取用。
 - ◆ 備考1：本標準所言之「書面程序」係指已建立、文件化、實施及維持的程序。
 - ◆ 備考2：每個組織可能有不同之資訊安全管理系統文件化，因為：
 - 組織規模及其活動型式。
 - 安全要求及系統管理之範圍與複雜程度。
 - ◆ 備考3：文件及紀錄可為任何形式或型態之媒介物。



文件要求(文件管制)

- ◆ (a)在文件發行前核准其適切性。
- ◆ (b)必要時， 審查與更新並重新核准文件。
- ◆ (c)確保文件之變更與最新改訂狀況已予以鑑別。
- ◆ (d)確保在使用場所備妥適用文件之最新版本。
- ◆ (e)確保文件保持易於閱讀並容易識別。



文件要求(文件管制)

- ◆ (f) 確保外來原始文件已加以鑑別。
- ◆ (g) 確保文件分發已管制。
- ◆ (h) 防止失效文件被誤用。
- ◆ (i) 過期文件為任何目的需保留時，應予以適當鑑別。




文件要求(紀錄管制)

- ◆ 為提供資訊安全管理系統符合要求及有效運作之證據，所建立並維持之紀錄，應予以管制。資訊安全管理系統應將各國法律要求列入考量。
- ◆ 紀錄應清晰易讀，容易識別及檢索。為了紀錄之鑑別、儲存、保護、檢索、保存期限及報廢，應建立文件化程序，以界定所需之管制。
- ◆ 所需之紀錄及其範圍應由管理過程加以決定。

管理階層責任

- ◆ 管理階層承諾：
- ◆ 管理階層應藉由下列各項，對資訊安全管理系統之建立、實施、操作、監控、審查、維持與改進之承諾提供證據：
 - ◆ (a) 建立一份資訊安全政策。
 - ◆ (b) 確保建立各項資訊安全目標及計畫。
 - ◆ (c) 為資訊安全建立角色與權責。




管理階層責任

- ◆ (d) 向全組織傳達符合資訊安全目標、遵守資訊安全政策、在法律下要求之權責，以及持續改進之需求。
- ◆ (e) 決定可接受風險之等級。
- ◆ (f) 提供充分資源以開發、實施、操作及維持資訊安全管理系統。
- ◆ (g) 執行資訊安全管理系統之管理階層審查。



管理階層責任(資源提供)

- ◆ (a) 建立、執行、操作及維護資訊安全管理系統。
- ◆ (b) 確保各資訊安全程序可支援企業需求。
- ◆ (c) 鑑別並提出法律與法規的要求以及合約上之安全義務。
- ◆ (d) 正確應用所有實施的控制措施，以維持適當之安全。
- ◆ (e) 當必要時，進行審查並針對審查結果作適當因應。
- ◆ (f) 當需要時，改進資訊安全管理系統之有效性。



管理階層責任 (訓練、認知及能力)

- ◆ (a) 決定執行影響資訊安全管理系統工作之人員其所需之能力。
- ◆ (b) 提供能力訓練，必要時僱用具備能力之人員，以滿足該需求。
- ◆ (c) 評估所提供訓練及所採措施之有效性。
- ◆ (d) 維持教育、訓練、技巧、經驗及資格之紀錄。

管理階層審查

- ◆ 概述
- ◆ 管理階層應在規劃之期間內，審查組織的資訊安全管理系統，以確保其持續的適用性、適切性及有效性。審查應包括改進時機之評估，以及資訊安全管理系統變更之需求，含資訊安全政策與安全目標。審查結果應予清楚的文件化，紀錄應予維持。



管理階層審查

- ◆ 審查輸入
- ◆ (a) 資訊安全管理系統稽核與審查之結果。
- ◆ (b) 來自利害相關團體之回饋。
- ◆ (c) 可用以改進組織資訊安全管理系統績效及有效性之技術、產品或程序。
- ◆ (d) 預防與矯正措施之狀況。
- ◆ (e) 先前風險評鑑未適切提出之脆弱性或威脅。
- ◆ (f) 先前管理階層審查之跟催措施。
- ◆ (g) 可能影響資訊安全管理系統之任何變更。
- ◆ (h) 改進之建議。

管理階層審查

- ◆ 審查輸出
- ◆ (a) 資訊安全管理系統有效性之改進。
- ◆ (b) 為因應可能影響資訊安全管理系統之內部或外部事件，必要時，影響資訊安全之流程應予修訂，包括：
 - ◆ (1) 營運需求。
 - ◆ (2) 安全需求。
 - ◆ (3) 影響既有營運需求之營運過程。
 - ◆ (4) 法令或法規要求。
 - ◆ (5) 風險等級及/或風險可接受程度。
- ◆ (c) 資源需求。



管理階層審查

- ◆ 稽核
- ◆ 組織應在規劃之期間內執行內部稽核，以決定資訊安全管理系統之管制目標、控制措施、各過程及程序是否：
 - ◆ (a)符合本標準及相關法令或法規之各項要求。
 - ◆ (b)符合所鑑別之資訊安全要求。
 - ◆ (c)有效地實施與維持。
 - ◆ (d)如預期的執行。



資訊安全管理系統之改進

- ◆ 持續改進
- ◆ 組織應經由資訊安全政策、安全目標、稽核結果、事件監控之分析、矯正與預防措施以及管理階層審查之使用，以持續改進資訊安全管理系統之有效性。

資訊安全管理系統之改進

- ◆ 矯正措施
- ◆ (a) 鑑別資訊安全管理系統實施及/或操作之不符合事項。
- ◆ (b) 判定不符合事項之原因。
- ◆ (c) 評估措施之需求，以確保不符合事項不再發生。
- ◆ (d) 決定與實施所需之矯正措施。
- ◆ (e) 採取措施結果之紀錄。
- ◆ (f) 審查所採取之矯正措施。




資訊安全管理系統之改進

- ◆ 預防措施
- ◆ (a) 鑑別潛在的不符合與其原因。
- ◆ (b) 決定並實施所需之預防措施。
- ◆ (c) 紀錄所採取措施之結果。
- ◆ (d) 審查所採用之預防措施。
- ◆ (e) 鑑別已變化之風險並確保焦點放在顯著變化之風險上，預防措施之優先順序應依據風險評鑑之結果加以決定。



名詞與定義

- ◆ 風險分析(Risk analysis): 以有系統的方式使用資訊，進而辨識風險的來源，並加以估計。
- ◆ 風險評鑑(Risk assessment): 風險分析與風險評估的整體程序。
- ◆ 風險評估(Risk evaluation): 把所估計的風險與已知的風險標準作比較的整個程序，以便決定風險的重要性。

- 
- ◆ 可接受之風險(Risk acceptance): 決定接受某個風險。
 - ◆ 風險管理(Risk management): 引導與控管組織有關風險的協調活動。
 - ◆ 風險處理(Risk treatment): 在選擇與實施修正風險的措施時，所用的處理過程。
 - ◆ 適用性聲明(Statement of Applicability) : 根據風險評鑑與風險處理程序的結果與結論，描述與組織資訊安全管理系統有關且適用之控制目標及控制措施的文件。

BS7799-2:2002


- ◆ Detailed Controls Annex A
- ◆ 附錄A控制措施介紹





3.1 資訊安全政策

- ◆ 提供管理階層對資訊安全的指示及支持。
- ◆ 資訊安全政策文件：
 - ◆ (a) 資訊安全、其整體目標及範圍的定義
 - ◆ (b) 管理階層的意圖，以及對資訊安全目標及原則支持的一份聲明；
 - ◆ (c) 簡要說明安全政策、原則、標準以及符合性要求（對組織的特別重要性），例如：

- 
- ◆ (1) 符合法令和合約的要求；
 - ◆ (2) 安全教育要求；
 - ◆ (3) 防止並檢測電腦病毒和其他惡意軟體；
 - ◆ (4) 營運持續管理；
 - ◆ (5) 違反安全政策的後果；
 - ◆ (d) 確定資訊安全管理的一般責任和特定責任，包括通報安全事件；
 - ◆ (e) 支援政策的文件索引，例如針對特定資訊系統的詳盡安全政策和程序，或使用者應該遵守的安全規則。
 - ◆ 審查與評估：



4.1 資訊安全基礎架構

- ◆ 管理階層資訊安全會報
- ◆ 資訊安全協調工作
- ◆ 資訊安全責任的配置
- ◆ 資訊處理設施的授權作業
- ◆ 資訊安全專家的建議
- ◆ 組織間的合作
- ◆ 獨立的資訊安全審查

4.2 第三方存取之安全

- ◆ 為維護組織內的資訊處理設施和資訊資產被第三方存取時的安全。
- ◆ 鑑別第三方存取風險

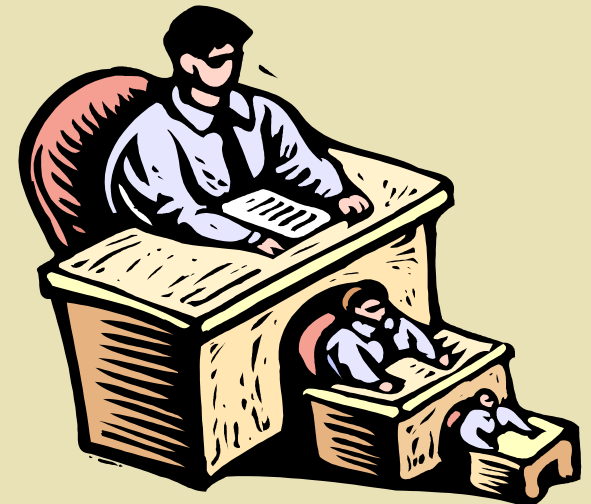
第三方存取組織的資訊處理設施應加以管制。如果讓第三方存取為營運要求，應執行風險評鑑，以決定所涉及的安全問題和控制要求。在合約中應與第三方就控制措施達成協議，並加以界定。

- ◆ 第三方合約中之安全要求

在安排第三方對組織資訊處理設施的存取時，應該以正式的契約為基礎，內容應包含或提及所有的安全要求，以確保能符合組的安全政策及標準。該合約應確保組織和第三方之間沒有任何歧義。組織應該要擬定自己能接受的供應商賠償條款。

4.3 委外作業

- ◆ 資訊處理的責任委託其他組織負責時，能維護資訊的安全。在雙方的合約中，委外協定應處理資訊系統、網路或桌上電腦環境的風險、安全控制措施以及程序。





5.1 資產可歸責性 (accountability)

- ◆ 資產清冊 Inventory of assets
- ◆ 對組織的資產維持適切的保護。
- ◆ 所有主要的資訊資產應有人負責， 並指定資產的所有人。
- ◆ 資產的可歸責性有助於確保適當的保護， 應確定所有主要資產的所有人， 並分配維護該資產適切控制措施的責任， 實施控制措施的責任可以授權， 但該資產的責任仍應由原來指定的所有人負責。

5.2 資訊分級

- ◆ 資訊分級指引
- ◆ 資訊標示與處理
- ◆ 確保證資訊資產受到適當等級的保護。
- ◆ 資訊應加以要分級，以指明所需要的保護措施，及保護措施的優先順序和程度。
- ◆ 資訊的敏感程度和重要程度各不相同，有些資訊需要加強保護等級或特殊處理，應該使用資訊分級系統界定合適的保護等級，並解釋所需的特殊處理方式。



6.1 人員安全

- ◆ 工作說明及資源分配的安全

降低因人為錯誤、竊盜、詐欺或誤用設施所造成的風險。安全責任應該在招募人才階段之合約中就要提出並在雇用期間進行監督。

- ◆ 將安全列入工作職掌中
- ◆ 人員篩選及政策
- ◆ 保密協議
- ◆ 雇用條件與限制



6.2 使用者訓練

- ◆ 應訓練使用者各項安全程序和正確使用資訊處理設施，以降低可能的安全風險。
- ◆ 資訊安全教育與訓練
- ◆ 組織所有員工以及相關的第三方使用者，皆應就組織的政策和程序以及其最新修訂內容接受適當訓練，此包括安全要求、法律責任和營運控制措施，以及資訊處理設施的正確使用之訓練，例如在賦予存取資訊或服務前，登入程序、套裝軟體的使用等等。

6.3 安全及失效事件的反應處理

- ◆ 通報安全事件
- ◆ 通報安全弱點
- ◆ 通報軟體失效
- ◆ 從事件中學習
- ◆ 懲罰處理



7.1 安全區域

- ◆ 避免營運場所及資訊遭未經授權之存取、損害及干擾。
- ◆ 實體安全邊界
- ◆ 實體進入控制措施
- ◆ 辦公處所及設施之保護
- ◆ 在安全區域內工作
- ◆ 隔離的收發與裝卸區



7.2 設備安全

- ◆ 設備安置及保護
- ◆ 電源供應
- ◆ 纜線的安全
- ◆ 設備維護
- ◆ 場外設備之安全
- ◆ 設備之安全報廢或再使用的安全防護



7.3 一般控制措施

- ◆ 避免資訊與資訊處理設施受危害或遭竊
- ◆ 桌面淨空與螢幕淨空政策
- ◆ 財產攜出





8.1 作業程序與責任

- ◆ 作業程序文件化
- ◆ 操作變更之控制
- ◆ 事件管理程序
- ◆ 職責區隔
- ◆ 分隔開發與作業設施
- ◆ 外部設施的管理



8.2 系統規劃與驗收

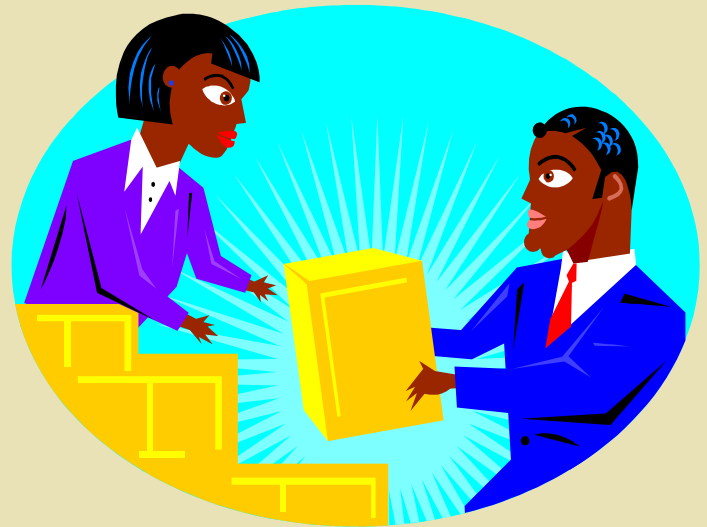
- ◆ 容量規劃
- ◆ 系統驗收
- ◆ 降低系統失效的風險。必須預先規劃和準備，以確保有足夠的容量和資源。應預測未來的容量要求，以降低系統超載的風險。
- ◆ 驗收及使用新系統之前，作業要求應加以建立文件化及測試。

8.3 惡意軟體的防範

- ◆ 對抗惡意軟體的控制措施
- ◆ 需要採取預防措施以便避免並偵測惡意軟體的入侵。軟體與資訊處理設施易受惡意軟體侵入，例如電腦病毒、網路蠕蟲、特洛伊木馬（另參閱10.5.4節）和邏輯炸彈。應讓使用者瞭解未授權軟體或惡意軟體的危險；管理員應在適當場合導入特殊的控制措施來偵測或預防這些軟體的侵入。特別是，採取預防措施，以偵測及預防個人電腦上的電腦病毒是重要的。

8.4 日常事務處理

- ◆ 資料備份
- ◆ 操作員日誌
- ◆ 錯誤事件登錄



8.5 網路管理

- ◆ 網路控制措施
- ◆ 確保網路內資訊之安全，並保護支援之基礎設施。可能超越組織邊界的網路，其安全管理需注意。可能需要額外的控制措施以保護透過公共網路傳送的敏感資料。



8.6 媒體的處理與安全

- ◆ 可攜式電腦媒體 管理
- ◆ 媒體之報廢
- ◆ 資訊處理程序
- ◆ 系統文件之安全
- ◆ 應建立適當的作業程序以保護文件、電腦媒體（磁帶、磁片和錄音帶）、輸入與輸出資料和系統文件，避免損壞、竊盜及未授權存取。



8.7 資訊及軟體的交換

- ◆ 資訊與軟體交換協議
- ◆ 媒體運送之安全
- ◆ 電子商務安全
- ◆ 電子郵件安全
- ◆ 電子化辦公系統之安全
- ◆ 公共系統
- ◆ 其它資訊交換形式

9.1 存取控制的營運要求

- ◆ 存取控制政策
- ◆ 應根據營運和安全要求基礎，加以控制資訊存取與營運處理，應考慮資訊傳遞和授權的政策。



9.2 使用者存取管理

- ◆ 使用者註冊
- ◆ 特權管理
- ◆ 使用者通行碼管理
- ◆ 使用者存取權限審查



9.3 使用者責任

- ◆ 通行碼之使用
- ◆ 無人看管之資訊設備
- ◆ 授權使用者的合作對有效的安全是重要的。應讓使用者瞭解自己對維護有效存取控制措施的責任，特別是有關通行碼的使用以及使用者設備的安全。





9.4 網路存取控制措施

- ◆ 使用網路服務的政策
- ◆ 強制存取路徑
- ◆ 外部連線之使用者身份鑑別
- ◆ 節點鑑別
- ◆ 遠端診斷埠保護
- ◆ 網路區隔
- ◆ 網路連線控管
- ◆ 網路路由控管
- ◆ 網路服務之安全



9.5 作業系統存取控制措施

- ◆ 自動終端機識別功能
- ◆ 終端機登入流程
- ◆ 使用者識別和身份鑑別
- ◆ 通行碼管理系統
- ◆ 系統公用程式之使用
- ◆ 保護使用者的反脅迫警報器
- ◆ 終端機自動關機時間
- ◆ 連線時間的限制



9.6 應用系統之存取控制

- ◆ 資訊存取限制
- ◆ 敏感性系統的隔離
- ◆ 防止資訊系統中的資訊遭未經授權存取，應在應用系統中使用安全設施限制存取行為。




9.7 監控系統之存取與使用

- ◆ 事件記錄
- ◆ 監控系統之使用
- ◆ 時鐘同步
- ◆ 偵測未經授權的活動。系統應予監視以偵策違反存取控制政策的情形，並記錄可監視的事件，以便出現安全事件時提供證據之用。



9.8 行動式電腦作業與遠距工作

- ◆ 行動式電腦作業
- ◆ 遠距工作
- ◆ 必要的保護措施應與特定工作方式產生的風險一致，使用行動式電腦作業時應考慮在無保護的環境中工作之風險，以及採取的適切保護措施。在遠距工作的情形下，組織應對遠距工作場所採取保護措施，並確保已經為該工作方式備妥適當的安排。



系統開發及維護-10.1系統之安全要求

- ◆ 安全要求分析及規格
- ◆ 包括基礎建設、營運應用程式和使用者開發的應用程式，支援應用或服務的營運作業之設計和實施，是安全的關鍵。開發資訊系統前就應確認安全的要求，並獲同意。

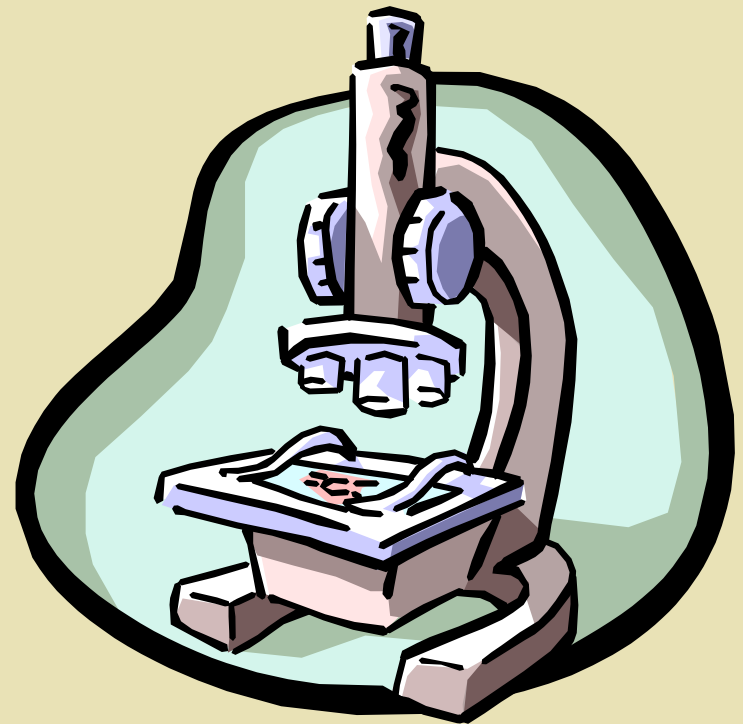


10.2 應用系統之安全

- ◆ 輸入資料之確認
- ◆ 內部處理之控制
- ◆ 訊息鑑別
- ◆ 輸出資料之確認
- ◆ 預防應用系統中的使用者資料遺失、遭修改或誤用。

10.3 密碼控制措施

- ◆ 使用密碼學控制措施之政策
- ◆ 加密
- ◆ 數位簽章
- ◆ 不可否認服務
- ◆ 金鑰管理



10.4 系統檔案之安全

- ◆ 作業系統軟體之控制
- ◆ 系統測試資料之保護
- ◆ 原始程式庫之存取控制
- ◆ 確保資訊技術專案及支援活動以安全的方式執行，存取系統檔案的行為應予控制。維護系統完整性應是應用系統或軟體所屬之使用者部門或開發小組的責任。



10.5 開發及支援作業的安全

- ◆ 變更管制程序
- ◆ 作業系統變更的技術審查
- ◆ 套裝軟體變更之限制
- ◆ 隱密通道與特洛伊木馬程式
- ◆ 軟體開發委外
- ◆ 負責應用系統的管理員還應負責專案或支援環境的安全，他們應確保所有的系統變更提案都經過審查，以檢查是否會破壞系統或操作環境的安全性。



11.1 營運持續管理之考量面

- ◆ 營運持續管理過程
- ◆ 營運持續及衝擊分析
- ◆ 持續計畫之撰寫及實施
- ◆ 營運持續管規劃框架
- ◆ 營運持續計畫之測試、維護及重新評鑑
- ◆ 防治營運活動的中斷，保護重要營運過程不受重大故障或災難的影響。



12.1 遵守法規要求

- ◆ 適用法令之鑑別
- ◆ 智慧財產權
- ◆ 組織記錄之保護
- ◆ 個人資訊的資料保護及隱私
- ◆ 預防資訊處理設施之不當使用
- ◆ 密碼學控制措施的規定
- ◆ 蒐證

12.2 安全政策及技術的符合性之審查

- ◆ 安全政策之符合性
- ◆ 技術符合性的檢查
- ◆ 確保系統符合組織的安全政策及標準。



12.3 系統稽核的考量

- ◆ 系統稽核控制措施
- ◆ 系統稽核工具之保護
- ◆ 使系統稽核過程得到最大成效，並將稽核過程產生或受到之干擾降到最低。在系統稽核時，應採取控制措施保護作業系統和稽核工具。





分析BS7799控制措施

- ◆ 100%安全？
- ◆ 唯一真正安全的系統就是關掉電源，拔掉插頭，鎖進一個鈦合金的保險箱，再將其埋在混凝土的雕堡內，和用神經瓦斯和高薪的武裝警衛來看管，儘管如此
 - ，我仍無法以生命保證它的安全！

吉尼, 斯怕佛



風險評鑑和風險處理

- ◆ 資產與資產價值
- ◆ 安全威脅和脆弱性
- ◆ 風險評鑑
- ◆ 風險處理
- ◆ 安全控制措施和對策
- ◆ 適用性聲明

資產

- ◆ 資產是甚麼？
- ◆ 資產就是組織直接賦予價值並需要組織的保護
- ◆ 必須是相關於資訊安全管理系統的範圍





資產

- ◆ 關於資訊系統資產的範例：
- ◆ 資訊資產-資料檔案，使用手冊等
- ◆ 書面文件-合約，指南等
- ◆ 軟體資產-應用程式與系統軟體等
- ◆ 實體資產-電腦，磁碟片等
- ◆ 人員-員工
- ◆ 公司形象與聲勢
- ◆ 服務-通訊，技術等



資產價值〈和潛在衝擊〉

- ◆ 組織已經鑑別其資產的價值嗎？
- ◆ 決定每個資產的價值是決定一個有效率安全策略的第一步
- ◆ 是甚麼樣的系統0-5或是低到非常高
- ◆ 這是風險評鑑過程中極為重要的部份

資產價值

- ◆ 然而，對於BS 7799，“資產”並不一定包括組織內一般視為有價值的所有事物
- ◆ 組織必須自行決定哪些資產的缺乏或降級可能實際影響產品/服務的交付





威脅

- ◆ 宣告意圖造成損害，痛苦，或不幸
- ◆ 可能造成一個有害的事件且這事件可能對系統，組織，和資產造成傷害
- ◆ 蓄意的或意外的，人為的或天災
- ◆ 資產容易受到許多威脅，這些威脅來自於利用脆弱性



威脅

- ◆ 天災-洪水、暴風雨、地震、閃電
- ◆ 人為-人員短缺、錯誤維護、使用者錯誤
- ◆ 科技-網路故障、流量超過負荷、硬體故障
- ◆ 蓄意的威脅
- ◆ 意外的威脅
- ◆ 威脅頻率



脆弱性

- ◆ 脆弱性是組織資訊安全的弱點/漏洞
- ◆ 脆弱性本身並不會造成傷害，而是可能允許威脅影響資產的一種或多種情況
- ◆ 脆弱性如果沒有妥善管理，將促使威脅形成

脆弱性

- ◆ 關鍵人員的缺席
- ◆ 不穩定的動力
- ◆ 未保護的電纜線
- ◆ 安全意識的缺乏
- ◆ 密碼權限的錯誤分配
- ◆ 安全訓練的不足
- ◆ 未安裝防火牆
- ◆ 未鎖的門





風險

風險

=

價值 x 威脅 x 脆弱性

由風險測量來劃分威脅的等級

威脅描述 A	衝擊 (資產) B	威脅發 生可能 性 C	風險測 量 D =BxC	威脅等 級 E
威脅A	5	2	10	2
威脅B	2	4	8	3
威脅C	3	5	15	1
威脅D	1	3	3	5
威脅E	4	1	4	4
威脅F	2	4	8	3

可容忍和不可容忍的風險之區分

損失價值	0	1	2	3	4
頻率價值					
0	T	T	T	T	N
1	T	T	T	N	N
2	T	T	N	N	N
3	T	N	N	N	N
4	N	N	N	N	N

風險處理-計畫

- ◆ 風險處理計畫是定義行動以降低無法接受的風險，和實施所需的控制措施以保護資訊的一種合作文件



風險處理-方向

- ◆ 接受剩餘的風險
- ◆ 避免風險
- ◆ 轉移風險
- ◆ 降低風險到可接受程度





可接受風險的等級

- ◆ 要達到完全的安全是不可能的
- ◆ 總是有剩餘的風險
- ◆ 甚麼樣程度的剩餘風險能為組織所接受

風險處理

- ◆ 地點
- ◆ 已存在的安全
- ◆ 攻擊者的數量
- ◆ 可用的設施
- ◆ 累積的機會
- ◆ 宣傳層次
- ◆ 營運持續計畫





風險處理

- ◆ 定義一個可接受的殘餘風險等級
- ◆ 持續的審查威脅和脆弱性
- ◆ 對已存在之安全控制措施的審查
- ◆ 應用其他的安全控制...BS7799
- ◆ 政策和程序介紹



控制措施的選擇

- ◆ 風險
- ◆ 要求的保證程度
- ◆ 成本
- ◆ 實施的容易性
- ◆ 服務
- ◆ 法律和法規的要求
- ◆ 客戶和其他的合約要求

成本

- ◆ 預算限制
- ◆ 應用控制措施的成本是否會超過資產的價值？
- ◆ 也許必須選擇“最佳價值”範圍內的控制措施



實施的容易性

- ◆ 環境是否支援控制措施？
- ◆ 控制措施需要多久才有辦法開始實施？
- ◆ 控制措施是否立即可用的？



服務

- ◆ 可獲得的技術是否能夠管理控制措施？
- ◆ 是否能夠立即的升級？
- ◆ 設備是否有當地工程師/協力廠商的支援？

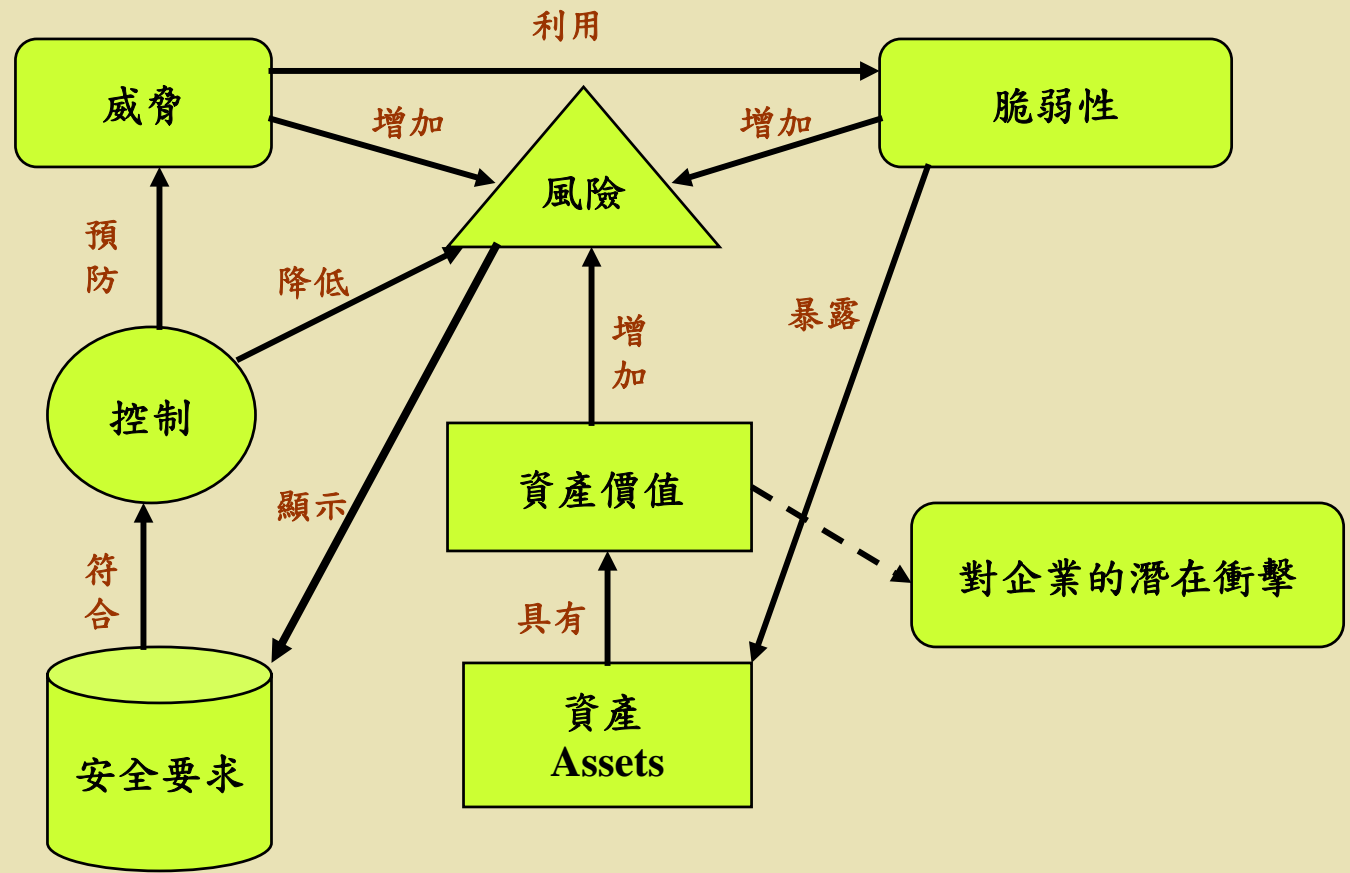




最佳作業的控制措施

- ◆ 資訊安全政策文件
- ◆ 資訊安全責任的分配
- ◆ 資訊安全教育和訓練
- ◆ 報告安全意外事件
- ◆ 營運持續管理

資產與風險





Statement of Applicability

適用性聲明

- ◆ 適合其企業營運需求的目標與控制措施評論
- ◆ 證明哪些控制措施是相關
- ◆ 記錄哪些不相關的控制措施
- ◆ 風險評鑑將決定哪一些控制措施應該被實施
- ◆ 是完整文件審查的一部份
- ◆ 將幫助決定最後評鑑階段的稽核計畫

稽核階段

- ◆ 稽核階段1—文件審查
- ◆ 稽核階段2—實施稽核





稽核階段1—文件審查

- ◆ 審查ISMS管理架構
- ◆ 評鑑ISMS的範圍
- ◆ 風險評鑑和管理
- ◆ 適用性聲明
- ◆ 安全政策和支援的關鍵程序
- ◆ 發現結果的正式報告
- ◆ 對組織解釋階段2



稽核階段2—實施稽核

- ◆ 目的
- ◆ 證明組織遵守本身的政策，目的和程序
- ◆ 證明ISMS遵照所有ISMS標準或規範文件的要求，而且達成組織的政策目的
- ◆ 測試ISMS的有效性



稽核階段2—實施稽核

- ◆ 主要活動
- ◆ 訪問ISMS的所有權人和使用者
- ◆ 審查高，中和/或低風險區域
- ◆ 安全目的和對象
- ◆ 安全和管理審查
- ◆ 系統中核心文件的連結
- ◆ 報告發現事項及做出最後是否發證之建議

Q&A

實例介紹

