工業技術研究院

資訊安全簡介與資訊安全政策

工業技術研究院
資訊技術服務中心
陳國增

工業技術研究院

講師介紹

- 任職機構：工業技術研究院
- 單位：資訊技術服務中心
- 職稱：工程師
- E-mail：NelsonChen@itri.org.tw

輔導案例

- 核心智識股份有限公司「 ISO9001品質系統」輔導建置
- 五鼎生物科技股份有限公司「軟體驗證與確認（SV&V）」輔導
- 新竹國際商業銀行資訊室「 ISO9001品質系統」 及「BS7799 資訊安全系統」既「軟體外包專案監控」輔導
- 中華電信數據分公司HiNet IDC 「 ISO9001品質系統」 及「BS7799 資訊安全系統」建置輔導
- 星動科技股份有限公司「BS7799 資訊安全系統」建置輔導

工業技術研究院

輔導案例（續）

- 財團法人中小企業信用保證基金「BS7799 資訊安全系統」建置輔導
- 「XX保全公司」資訊安全管理制度（ISMS）導入輔導案（通過ISO 27001）
- 經濟部中小企業處縮減產業數位落差計畫『建立資訊通信安全典範與標準作業流程』分項計畫

大綱

- 第一單元 資訊安全一般概論
- 第二單元 資訊安全管理制度ISMS
- 第三單元 資訊安全政策簡介
- 第四單元 如何架構資訊安全政策
- 第五單元 資訊安全風險評估與管理
- 第六單元 企業營運持續管理
- 第七單元 資訊安全稽核與認證
- 第八單元 政府資通安全現況與未來發展
- 總結
- 參考資料

第一單元

資訊安全一般概論

工業技術研究院

2004年國內資安事件

工業技術研究院

企業的智慧財產風險

駭人聽聞的國防資訊安全事件

- 英國一個男子鄧馬丁**到舊貨攤上買電腦，竟然買到了英國軍方的絕對機密資料**
- 三十一歲的鄧馬丁喜歡自己給電腦升級。最近他去舊貨市場買舊主機板。買回家一打開，鄧馬丁可樂壞了。電腦裡面竟然有最新遊戲軟體，英國陸海軍基地、港口爭奪戰
- 他跟同好一研究才發現資料是真的。裡面有英軍七十個陸海軍基地的詳細資料，要是落入敵人手裡，後果不堪設想。（94.04.25 奇摩新聞 ）

A.9.2.6 設備之安全報廢再使用

工業技術研究院

資訊安全的覺醒

慎防發生無法承受的狀況！

重視*資訊安全*的議題

何謂「資訊安全」

- 資訊對組織而言就是一種資產，和其他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。

摘錄自 CNS 17799

何謂「資訊安全」（續）

- 資訊安全係指保護機密或敏感資料，以防制未授權的揭露、修改與運用，並兼顧人員、程序、資料、硬體、軟體、實體環境等安全管理議題。
- 廣義而言，資訊安全包含技術面與管理面。
- 資訊安全是需要通過實施一整套適當的控制措施才能實現的。
- 資安4P＝＞Policy（管理制度和策略）、People（管理人員）、Process（管理流程）和Product（安全管理軟硬體）

資訊安全核心思維

Availability
可用性

Integrity
完整性

Confidentiality
機密性

資訊安全之目標

- 保護資訊的**機密性**、**完整性**與**可用性**（舊版定義的目標）
- 另外也涉及**鑑別性**（Authenticity）、**可歸責性**（Accountability）、**不可否認性**（Non-repudiation）及**可靠度**（Reliability）

摘錄自CNS 17799

完全避免資訊安全事件之前提

- 確定公司所在的位置不會發生天災
- 確定公司的營運項目沒有競爭對手
- 確定公司沒有任何價值連城的資訊
- 確定公司不與外國公司彼此較勁
- 確定公司完全不使用電腦
- 確定公司所使用的軟硬體均不會發生問題
- 確定公司的所有員工都沒有潛在的敵人
- 確定公司過去及現在仍為公司效命的員工全部都幸福快樂美滿、忠心耿耿

電子商務資訊安全序曲

No Security　No Trust
No Trust　No Transaction
No Transaction　No Money
No Money　No E-Commerce

⇩

No Security　No E-Commerce

⇩

My Business Rely on Your security

第二單元

資訊安全管理制度ISMS

什麼是「ISMS」？

- Information Security Management System
- 中文翻譯為「資訊安全管理制度」

資訊安全管理制度簡史

- 1995 ： 英國訂定「資訊安全管理實務準則」之國家標準BS7799 part 1，並提交ISO國際標準組織
- 1996/2/24 ： ISO審議6個月後，沒通過BS7799成為ISO標準
- 1998 ： 英國公佈BS7799 part 2，並成為資訊安全管理認證之依據
- 2000/12/1 ： 增修後之BS7799 part 1通過ISO審議成為ISO/IEC 17799國際標準
- 2002/9/5 ： 英國公佈發行BS7799-2:2002修訂版
- 2002/12/5 ： 我國經濟部標準檢驗局依據ISO/IEC 17799及BS7799-2:2002版公佈國家標準CNS17799及CNS17800
- 2005/6/15 ： ISO國際標準組織修定公佈ISO/IEC 17799(2005年版)
- 2005/10/14 ： 修定BS7799 part 2通過ISO審議成為ISO/IEC 27001國際標準
- 2007(預計) ： 將ISO/IEC 17799改為ISO/IEC 27002，使資訊安全標準成為ISO 27000系列

資訊安全國際標準

ISO/IEC 17799:2005 （原ISO/IEC 17799:2000）

Information technology - Security techniques - Code of practice for information security management

ISO/IEC 27001:2005（原 BS7799-2:2002）

Information technology - Security techniques - Information Security Management Systems - Requirements

CNS國家標準

ISO/IEC 17799:2005 ＝＞ CNS17799

Information technology - Security techniques - Code of practice for information security management

資訊技術 - 安全技術 - 資訊安全管理之作業要點

ISO/IEC 27001:2005 ＝＞ CNS17800

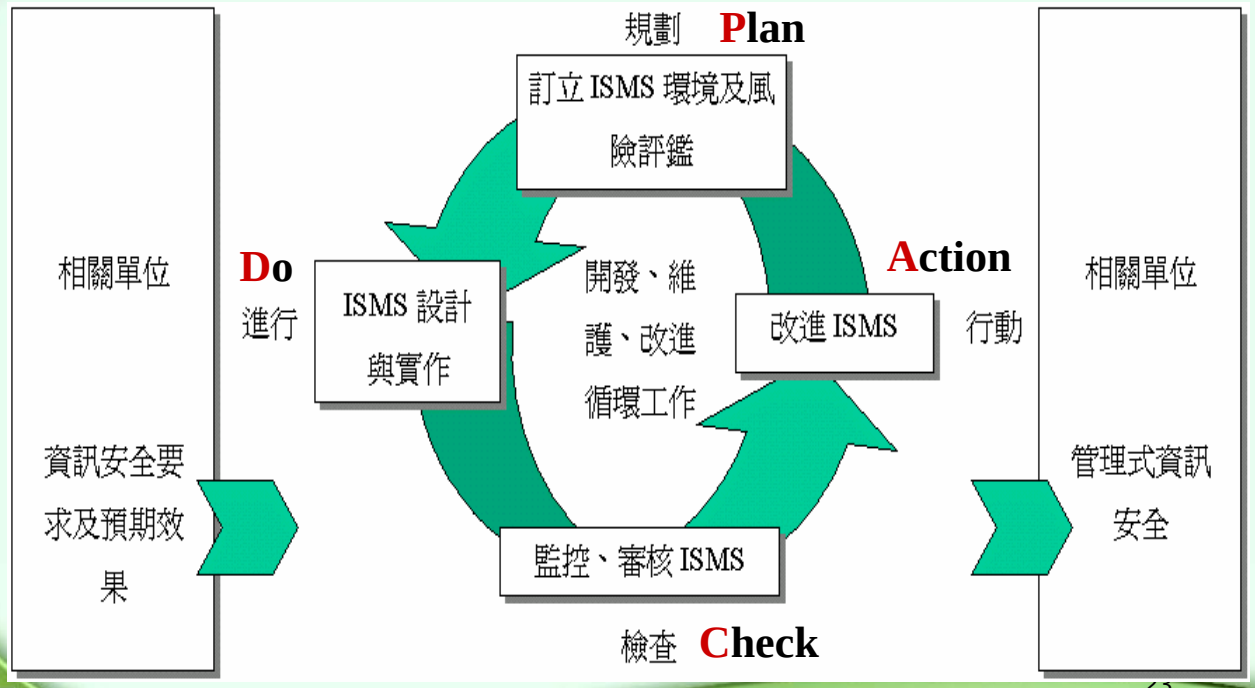
Information technology - Security techniques - Information Security Management Systems - Requirements

資訊技術 - 安全技術 - 資訊安全管理系統 - 要求

資訊安全管理之整體架構

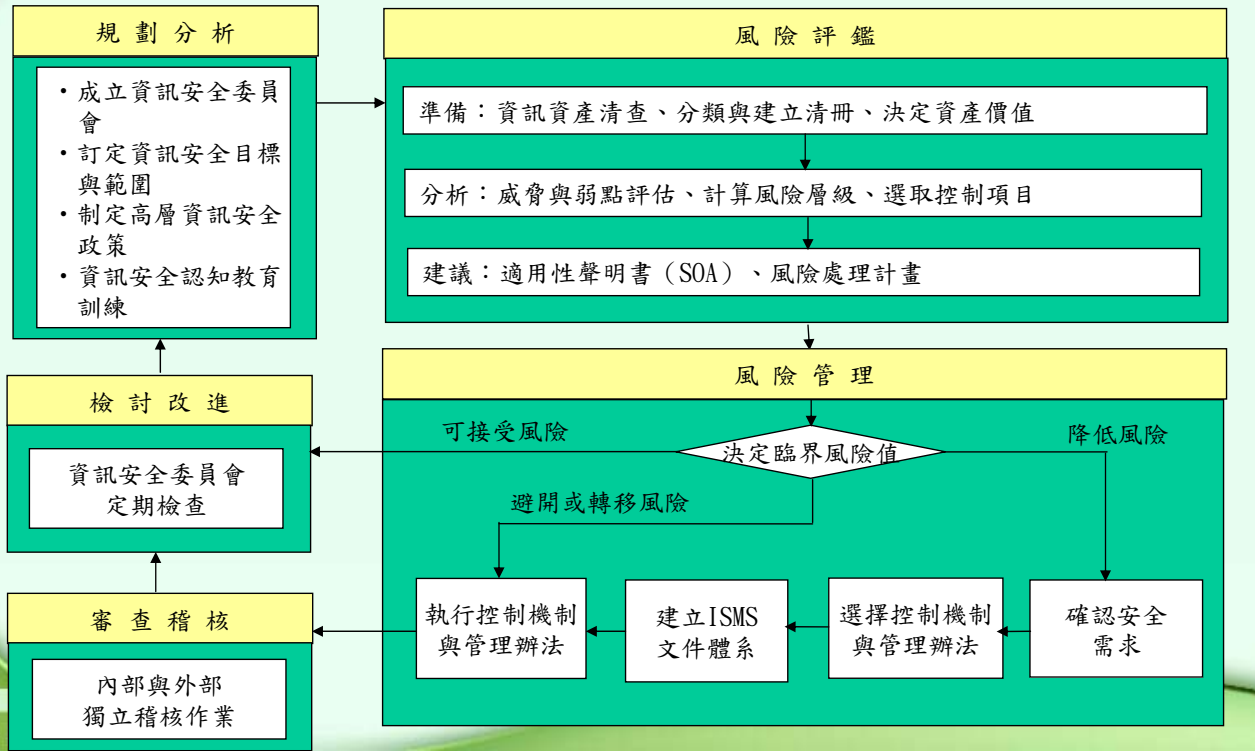
工業技術研究院

資訊安全管理之PDCA循環



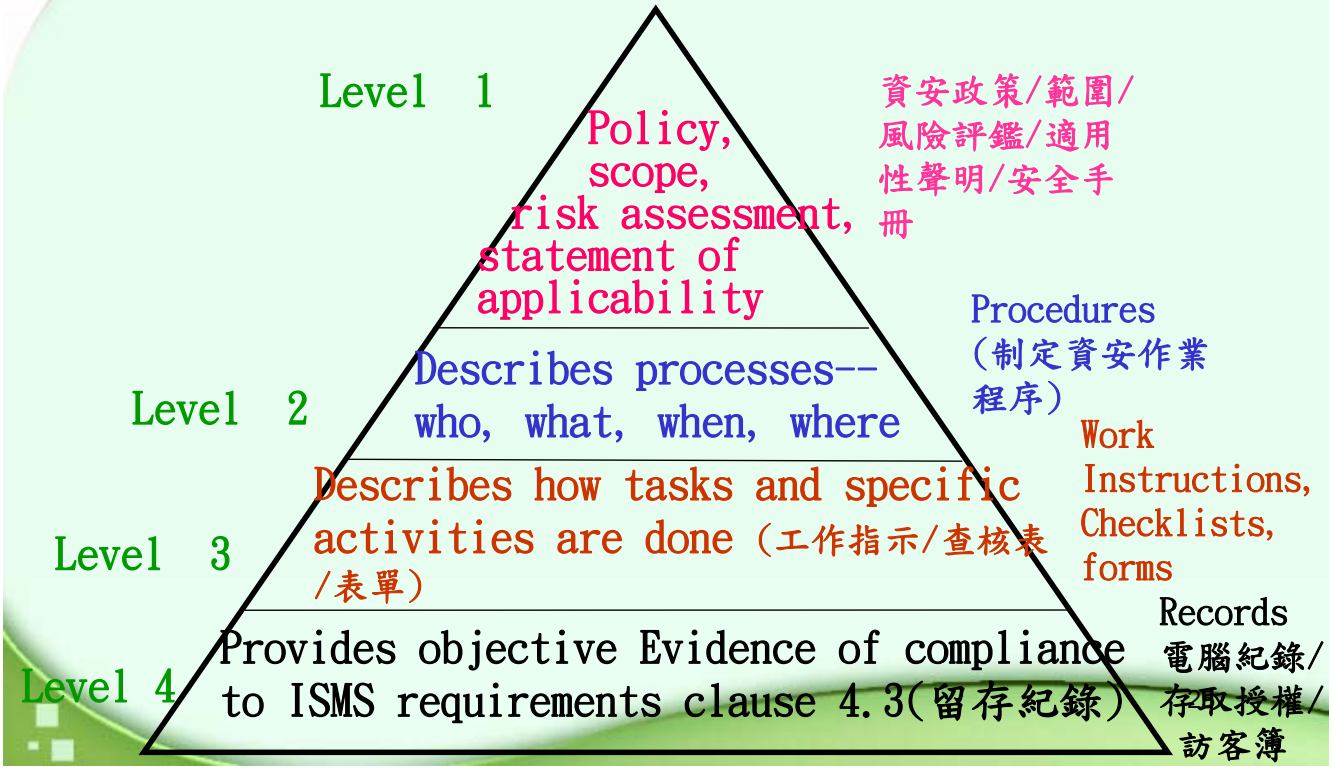
工業技術研究院

ISMS工作流程



工業技術研究院

資訊安全管理文件架構



工業技術研究院

資訊安全管理成功關鍵因素

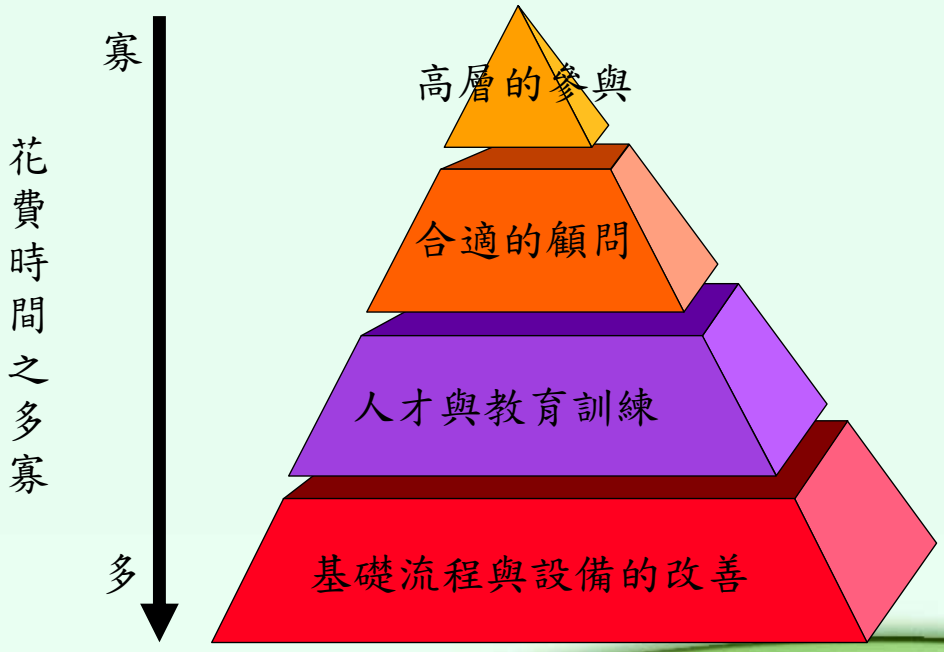
- 高階管理層明確的支持與承諾。
- 擬定與公司經營目標及企業策略相結合的資訊安全政策。
- 符合企業文化的資訊安全落實方式。
- 全體員工對資訊安全需求、資訊風險評估及風險管理皆有正確之認識

  ➔資訊安全是一個流程而非僅是技術產品
- 對管理階層及員工有效地推銷資訊安全概念。

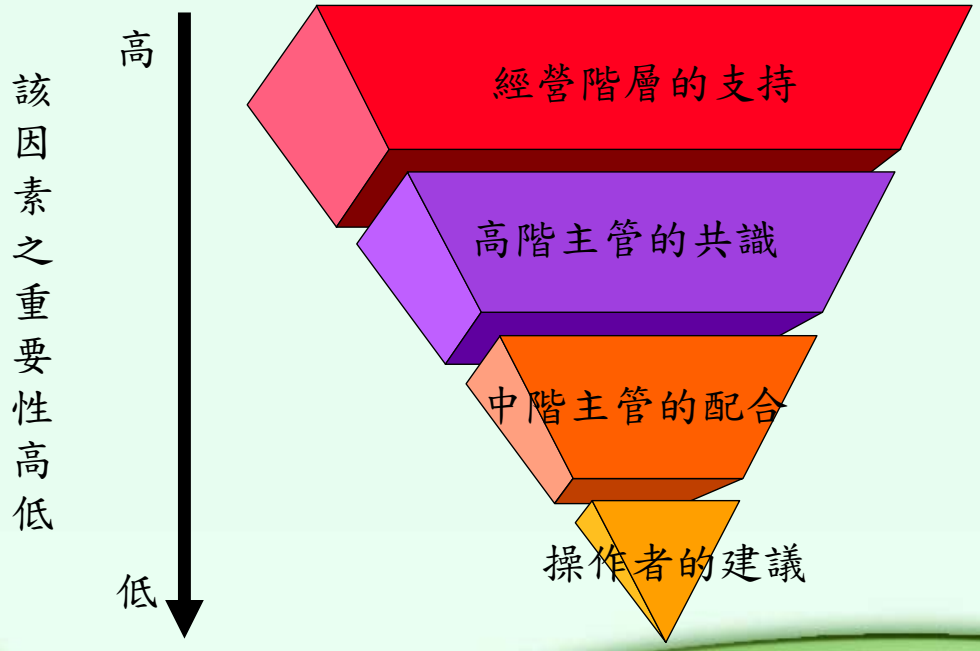
資訊安全管理成功關鍵因素（續）

- 對所有正式員工及簽約外包員工發行資訊安全政策及標準之指導方針
- 提供適當的教育訓練和宣導活動
- 一套全面且均衡的度量系統，用以衡量資訊安全管理的效能，並對如何改善的意見做適當的回饋

資訊安全管理成功關鍵因素（續）



資訊安全管理成功關鍵因素（續）



第三單元

資訊安全政策簡介

資訊安全政策

- 何謂「資訊安全政策」：

指導組織資訊安全的最高原則及指導方針

資訊安全政策（續）

- 組織整體資訊安全的提昇有賴於：
  - 完整的資訊安全**管理制度**
  - 資訊安全**防護技術**
- 資訊安全政策為建構上述二者的**基礎建設**，也是組織建立安全環境的**首要工作**

資訊安全政策（續）

- （民國91年）一份調查研究指出：
  - 80.4%的銀行有定期修正資訊安全政策。
  - 外商銀行表現優於本國銀行。
- 顯示銀行對於資訊安全政策的重視程度高。

資訊安全政策的意義

- 爲組織設定如何安全的使用資訊，以及安全的優先順序，以達成組織目標。
- 在符合組織的目標下，規範「資訊安全」的範圍。
- 以資訊安全為基礎的資訊管理與資源使用原則
- 支援資訊安全技術，以建立資訊安全成本效益的原則。

資訊安全政策的重要性

- 界定資訊安全防護目標，以獲得最高管理階層的支持，並建立與高層主管之溝通管道
  - 對應執行每一作業規章是符合哪一項安全政策規定
- 確定資訊安全防護之預算及資訊安全組織架構
  - 以在有限預算下建立最可靠的資訊安全體系
- 增進資訊安全的可信度與能見度
  - 清楚地呈現已建立之防護機制及可能面臨的資訊風險

資訊安全政策的重要性（續）

- 建立資訊安全人員之工作考評基準
- 改變同仁對資訊安全之體認，並取得其合作執行
- 作為選擇資訊安全產品的重要基準
- 建立稽核人員在從事內部稽查的重要參考依據
- 當有資訊安全事件發生時，做為訴訟所需的證據

資訊安全政策之目的與功能

- 對資訊資產安全的需求，提供指導方針與規範
- 具體表現高層管理者對資訊安全的支持與承諾
- 定義有關部門與人員對資訊安全管理的角色與責任
- 對資訊系統的存取，建立安全標準與控制的基準，促使組織建置一致的控制制度
- 指引資訊安全產品的選擇與技術的引進
- 將資訊安全控制的程序與做法正式化與文件化，以支援內部與外部的檢視，確保這些程序與做法能維護資訊安全的規劃與執行

資訊安全政策的制定

- 啟始階段
  - 初步評估並促使高階主管提昇資訊安全敏感度。
- 政策發展
  - 安全需求分析、草擬政策草案。
- 諮詢與核定
  - 諮詢專家或顧問意見、核定發布資訊安全政策。
- 安全意識與政策教育
  - 實施安全政策教育、建立安全意識。

資訊安全政策的制定（續）

- 政策宣導
  - 對內宣導，作為資訊安全基礎建設。
  - 對外宣導，建立資訊安全信賴。

資訊安全政策的實施範圍

- 資訊安全組織、任務、角色與責任（Roles and Responsibilities）
- 資訊資產分類與控制（Information Classification and Control）
- 資訊資產風險評估（Information Risk Assessment）
- 資訊安全教育訓練（Information Security Training）
- 存取控制（Access Control）

資訊安全政策的實施範圍（續）

- 實體及環境安全（Physical and Environment Security）
- 病毒防護與管理（Anti-virus and Control）
- 資訊安全事故之緊急處理程序
- 業務持續營運管理（Business Continuity Management）
- 違反資訊安全政策的懲處
- 法令規定的遵循

資訊安全政策的主要內容

- 資訊安全制定與稽核
- 資訊安全部門權責
  - 資訊安全組織
  - 資訊安全組織權責
- 資訊資產之安全管理
  - 安全等級分類
- 人員管理及教育訓練
  - 人員的安全管理
  - 人員的資訊安全教育訓練

資訊安全政策的主要內容（續）

- 實體及環境安全管理
  - 設備安置地點之保護
  - 周圍環境之安全
  - 人員進出管制
- 電腦系統安全管理
  - 系統規劃
  - 電腦媒體
  - 電腦軟體
  - 外部入侵
  - 資料備份

資訊安全政策的主要內容（續）

- 網路安全管理
  - 網路安全控管機制
  - 網路使用者安全規定
  - 電子郵件安全管理機制
  - 防火牆控管設定與測試
  - VPN加密及安全控管機制
  - 透過Internet傳送資料之保護
  - 主機及伺服器備援
  - 備份架構及定期備份
  - 網路安全稽核及紀錄

資訊安全政策的主要內容（續）

- 系統存取控制
  - 使用者之存取管理
  - 網路存取安全控制
  - 應用系統之存取控制
  - 系統之存取及應用之監控
- 系統發展維護安全管理
  - 系統安全需求規劃
  - 應用系統之安全
  - 系統變更及維護環境之安全

資訊安全政策的主要內容（續）

- 永續運作之規劃及管理
  - 業務永續運作之規劃
  - 業務永續運作計畫之測試
  - 資訊安全事件緊急處理機制

資訊安全政策範本

- 提供兩份資訊安全政策範本供參考：
  - 附件一：商業銀行資訊處資訊安全政策範本
  - 附件二：航運管理的資訊安全政策範本

資訊安全政策之評估與維護

- 遵循PDCA（Plan-Do-Check-Action）持續改善模式。
- 定期評估-確保實際作業與政策吻合。
- 定期稽核-確保政策與規定之貫徹執行。

資訊安全政策之評估週期

- 定期
  - 政策中所定義的評估週期。
- 非定期
  - 重大資安事故發生
  - 出現新的弱點或漏洞
  - 組織變動或組織文化變化
  - 資訊技術或基礎建設發生變化
  - 資訊或控制需求改變
    - 例如機密等級變更

第四單元

如何架構資訊安全政策

資訊安全政策的型態

- 安全政策聲明（General Security Policy）
  - 整體適用、共同遵循。
  - 較為抽象，屬於聲明性質。
  - ISO 27001稱之為「安全政策聲明」（Security Policy Statement）。
- 功能性安全政策（Functional Security Policy）
  - 導因於組織龐大、業務複雜、遵守不同地區法令。
  - 依據整體安全政策精神，提出更具體符合不同功能特性、更易落實的安全政策。

安全政策聲明 範本

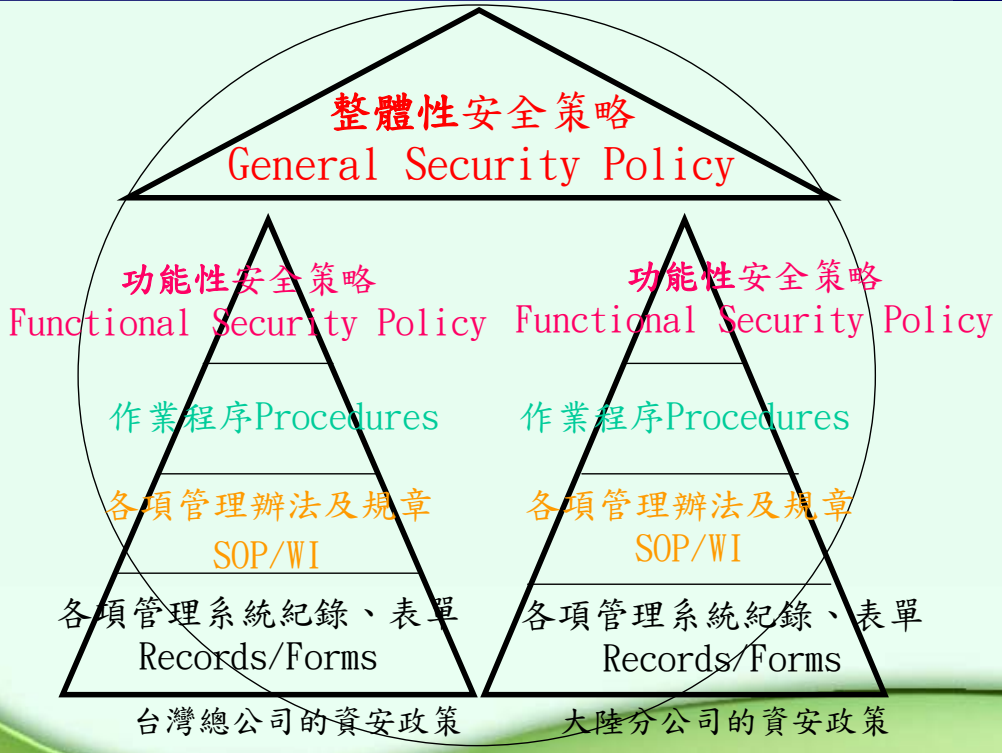
- 資訊安全是確保本公司永續經營的要素之一
- 管理階層必須清楚地界定本公司全體員工對於資訊安全的權責。
- 資訊安全是本公司全體員工的責任
- 資訊安全管理系統必須符合本公司業務需求，並兼顧投資成本效益
- 本公司應以一致的資訊安全環境兼顧資訊安全及資訊分享

資訊安全政策基本架構

推動策略-示範點

- 爲了快速導入，先擇定一個部門、作業流程、或者一個實體部門
- 作為後續擴大制度的基礎
- 好處：
  - 降低組織適應新管理制度的成本
  - 快速將風險管理的方法與觀念導入，並依組織文化修正
  - 示範點範圍小，衝擊日常作業機率降低

資訊安全政策整合架構



資訊安全政策之關鍵成功因素

- 導入資訊安全政策的關鍵成功因素為：
  - 授權（Approve）：資訊安全政策之訂定與宣告，取得關鍵單位之書面之正式核准。
  - 溝通（Communicate）：決策階層之書面公佈，公告於內部資訊傳遞系統，及員工之認知。
  - 評量（Measure）：定期由資訊部門或外部專家評估，確認執行之有效與遵行。
  - 維護（Maintain）：因需要變更政策內涵之管理與核准程序。

第五單元

資訊安全風險評估與管理

安全的議題從何而來？

弱點（Vulnerability）

- 弱點是組織資訊安全的脆弱的地方/漏洞。
- 弱點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。
- 弱點如果沒有妥善管理，將促成威脅形成。

威脅（Threat）

- 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弱點。

風險（Risk）

- 風險是指特定威脅利用弱點，造成資產損失或毀損的潛在可能。

風險評估（Risk Assessment）

- 風險評估主要是針對資訊處理設施的威脅、衝擊與弱點以及其所發生的可能性進行評估分析。

風險評估與風險管理的目的

- 找出資訊資產所隱藏的潛在威脅（Threat）和弱點（Vulnerability）
- 藉由判斷資產價值與威脅和弱點發生的機率或強度，決定該資訊資產所面臨的風險值。
- 決定企業『可容忍風險值』
- 對於高於可容忍風險值之資訊資產，採取適當的控制措施

第六單元

企業營運持續管理

美國911事件企業的省思

- 美國911恐怖攻擊事件恐怖份子攻擊世貿大樓，除了造成6000人死亡之外，在世貿大樓的1200家公司也發生企業經營危機，許多企業從此消失。

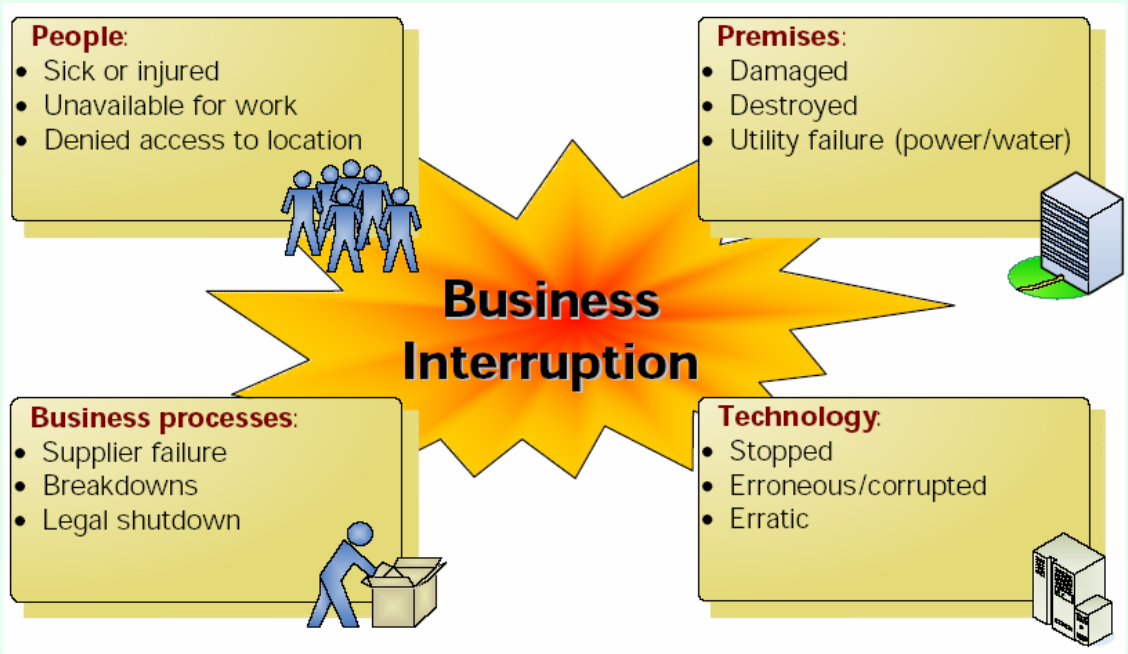
摩根史坦利集團的危機應變

- 當8:48分第一架飛機撞上大樓時，該公司9:03 分即啟動企業備援計畫疏散3500名員工，9:50分全部員工疏散完畢，9分鐘後大樓全部倒塌。
- 在關鍵時刻該公司的危機應變計畫，成功的保護了公司最重要的資產及員工的生命。
- 危機應變成功重要因素：
  - 發生時，員工被授權作決策，不須請示高層主管。使得3500名員工能在第一時間下樓。
  - 意外發生時，利用預先規劃的備援網路及電話線，成功的向員工及外界報導現況，維持通訊及指揮系統的暢通。
  - 事先規劃的設備清理計畫，該公司的電腦備援系統順利的在9:25分即開始運作，電腦中斷時間不超過1個小時。

造成企業營運中斷的重大事件

- 自然災害
- 硬體與通訊設施嚴重故障
- 爆發傳染性疾病
- 重大駭客入侵事件
- 內部或外部罷工
- 恐怖攻擊行動
- 供應鏈或行銷通路停擺
- 其他...

影響企業營運的風險因素



資料來源：KPMG Information Risk Management Business Continuity Management

實施營運持續管理的目的

- 減少因組織事件發生對企業營運造成之衝擊。
- 降低系統停止服務時間到可接受等級。
- 以減低財務損失、維持企業聲譽、保護企業人員、提高客戶滿意度，以及符合法律的需求。

何謂 BCP & DRP

- BCP – Business Continues Planning（企業營運持續計畫）
- DRP – Disaster Recover Planning（災害復原計畫）

BCP之目的

- 建立風險因應的體系。
- 預先評估營運可能遭受的衝擊，並決定因應的方針。
- 可以在風險真的發生時，從容不迫的處理。

DRP之目的

- 面對災害發生時的處理因應之道及步驟

第七單元

資訊安全稽核與認證

稽核定義與目的

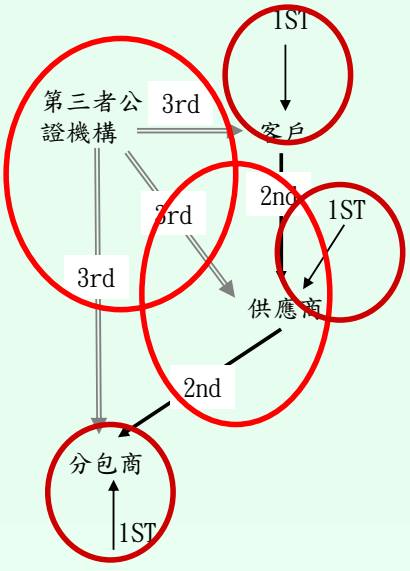
- ISO 19011（CNS 14809）定義稽核為：
  - 有系統的、獨立的及文件化過程用以取的稽核證據，並客觀的評估它，已決定稽核準則所被滿足的程度。
- 稽核之目的：
  - 查核實務（相關活動及相關結果）與理論（預定的事項或計劃）是否符合。
  - 稽核的目的在發展品質或資訊安全系統。

資訊安全稽核目標

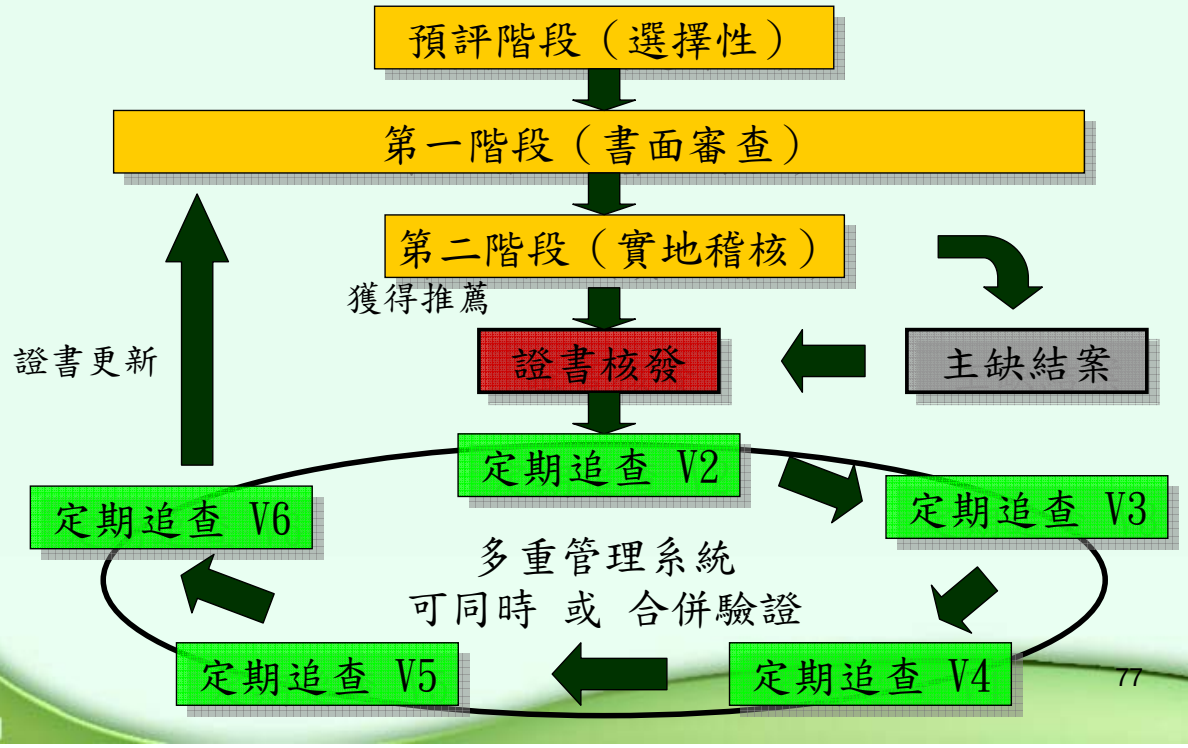
- 審查ISMS對ISO 27001的符合性
- 審查ISO 27001的實施程度
- 審查系統的有效性和適切性，以符合安全政策和目標
- 鑑別安全漏洞和弱點
- 提供改善ISMS的機會
- 符合合約的要求
- 驗證需要

稽核的類型

- 第三方稽核：外部稽核
  - 由具有公信力且獨立於被稽核組織及其供應商與客戶的團體所執行，通常會依據公認之資訊安全系統標準進行。
  - 驗證組織的ISMS是否符合特定標準
- 第二方稽核：外部稽核
  - 組織對其供應商或分包商所做的稽核
  - 目的在驗證供應商或分包商的績效是否適切
- 第一方稽核：內部稽核
  - 由組織對自身系統及程序所做的稽核
  - 目的在確保組織資訊安全系統的實行與改進



資訊安全認證稽核流程



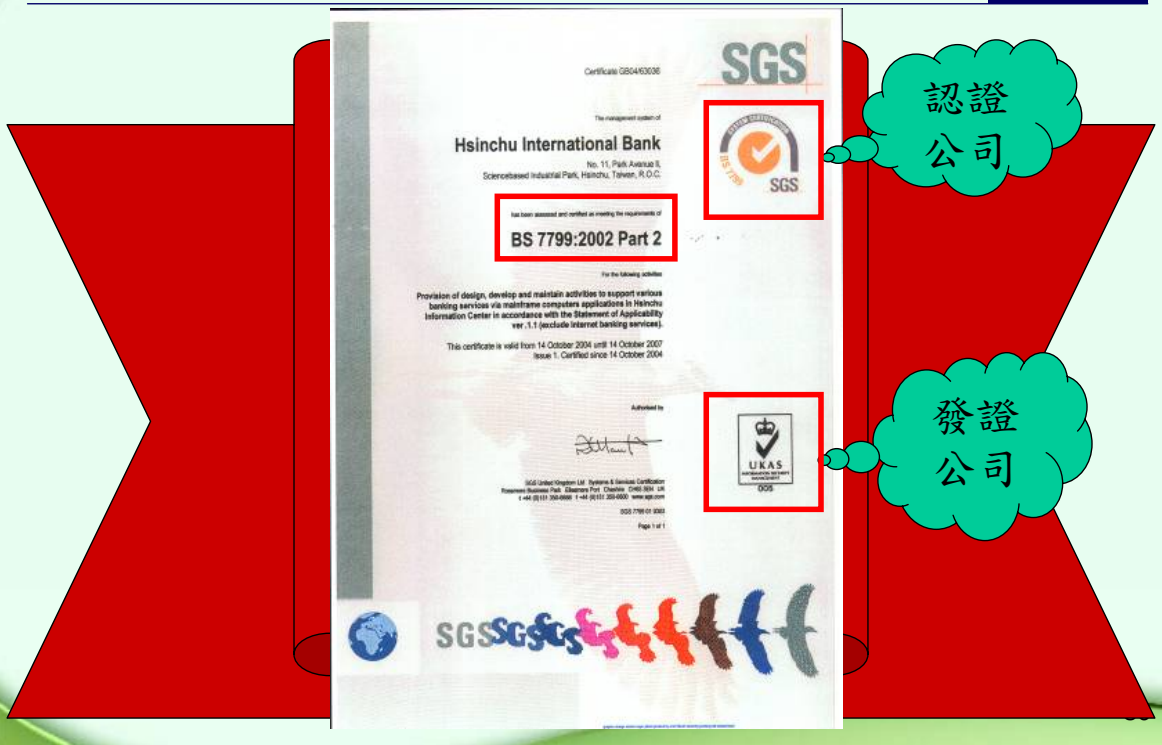
驗證稽核時的重點

- 確認資安管理系統的存在
- 與ISO 27001適用性聲明（SOA）的符合性
- 施行ISO 27001的落實程度
- 資安政策與資安目標是否有效的執行
- 風險評估、處理及殘餘風險是否適當
- 企業資安事件的自我偵測與改善能力
- 確認管理審查、內部稽核及矯正預防措施的有效性
- 營運持續管理（BCM）與相關計畫（BCPs）的可行性
- 資安管理系統的持續改善（PDCA）能力
- 是否符合合約要求及適用法規規範

推薦 VS. 證書

- 獲得認證公司**推薦**：
  - 主要缺失（Major）結案後。
  - 成功通過各階段的驗證。
- 當**發證單位**（Accreditation Body，如英國UKAS）核可後，將被授予ISO 27001的證書，並授權使用相關的標章（logo）。
- 當證書核發後，組織名稱、證書號碼及驗證範圍等資訊將予以公開。

推薦 VS. 證書（續）



定期追查

- 於證書有效期間內，需進行定期追查，以確認證書的有效性
- 定期追查的次數原則上依據受證單位與認證公司雙方合約明定的稽核天數及頻率
- 在證書三年有效期間結束前，需進行更新驗證（Renew）

全球證書分佈概況

2006.04.30 update

> 57% In Japan

> 72% In Asia

Japan	1516*	Sweden	8	Denmark	2
UK	238	Brazil	7	Slovak Republic	2
India	176	Malaysia	7	South Africa	2
Taiwan	81	Iceland	6	Armenia	1
Germany	56	Spain	6	Bahrain	1
Italy	42	Turkey	6	Chile	1
Korea	38	Greece	5	Egypt	1
USA	36	Kuwait	4	Lebanon	1
Hungary	29	Mexico	4	Lithuania	1
Netherlands	27	Philippines	4	Luxemburg	1
China	26	Saudi Arabia	4	Macedonia	1
Hong Kong	21	Argentina	3	Morocco	1
Australia	19	Canada	3	New Zealand	1
Poland	16	France	3	Peru	1
Finland	15	Isle of Man	3	Qatar	1
Norway	14	Macau	3	Romania	1
Switzerland	13	Russian Federation	3	Serbia and Montenegro	1
Czech Republic	12	UAE	3	Slovenia	1
Ireland	11	Belgium	2	Thailand	1
Singapore	11	Colombia	2	Relative Total	2529
Austria	9	Croatia	2	Absolute Total	2516*

取得認證的優點與好處

- 成為業界的標竿，提昇企業形象。
- 為全球認可的標準，證明企業對資訊安全的承諾。
- 全方位安全的量測指標，建立資訊安全的「防護網」。
- 建立資訊安全的控管機制。
- 讓資訊安全管理具成本效益，廣泛且更務實。

取得認證的優點與好處（續）

- 強化安全防護保證，展現一個高水準、適切的安全管理系統。
- 互信基礎與參考基準，讓顧客安心的明確證據。
- 增加管理能力及災害存活機率。
- 提昇投標資格，增加商機。

第八單元

政府資通安全現況與未來發展

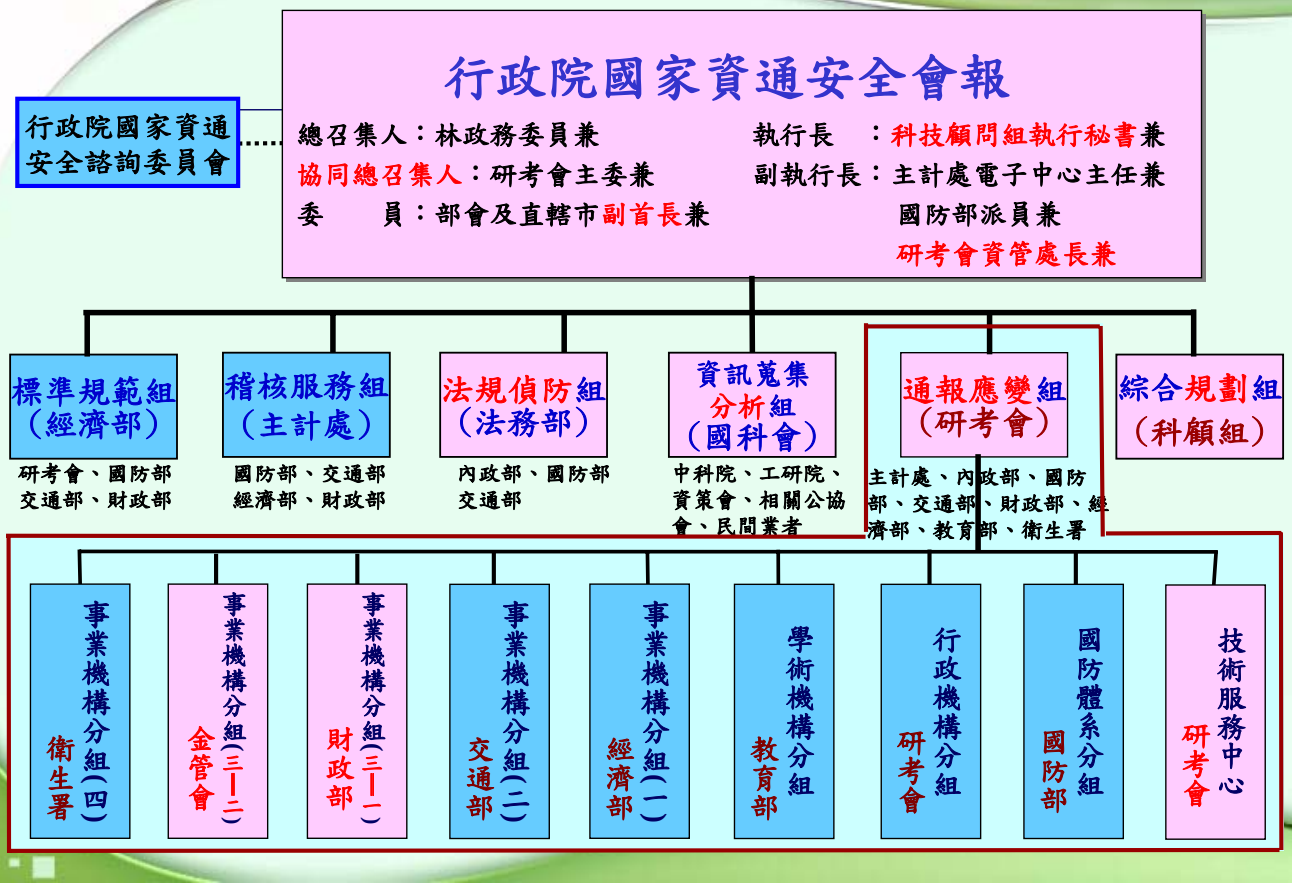
政府資通安全實施

- 89年8月30日 總統核定國家安全會議研提之「建立我國資通基礎建設安全機制建議書」
- 90年1月行政院第2718次院會核定第一期資通安全機制計畫，並成立「行政院國家資通安全會報」，積極推動我國資通安全基礎建設
- 93年3月17日行政院頒布實施第二期資通安全機制計畫（94年至97年）

政府大力推動資訊安全

- 第一期計畫目標：建立國家資通安全*基本*防護能力（90年1月至93年12月）。
- 第二期計畫目標：建立國家資通安全*整體*防護能力（94年1月至97年12月）。

國家資通安全會報組織架構



資訊安全等級工作項目

作業內容 / 名稱 / 等級	防禦機制強度	防護縱深	ISMS 推動作業	稽核方式	資安教育訓練(主官、主管、技術、一般)	專業證照
A 級	強度等級 4(註一)	NSOC 直接防護/自建 SOC、IDS、防火牆、防毒	96 年通過第三者認証(註二)	每年至少執行二次內稽	每年至少（4,6,18,4 小時）	96年資安專業鑑定二張(註三)
B 級	強度等級 3	SOC (Optional)、IDS、防火牆防毒	97 年通過第三者認証	每年至少執行一次內稽	每年至少(4,6,16,4 小時)	96 年資安專業鑑定一張
C 級	強度等級 2	IDS,防火牆防 毒	各單位自行成立推動小組規劃作業	自我檢視	每年至少(2,6,12,4 小時)	資安專業訓練

重點工作

- 落實執行CISO資訊安全長責任制度，強化政府機關之自我防護能力。
- 持續推動CNS17800/BS7799資安管理系統驗證。
- 推動e化政府機密資料加密等資安防護措施。
- 推行內部稽核制度，健全內部控制。
- 推廣全民資安認知。
- 研擬資安人才培育與訓練政策，鼓勵大專院校設立資安學程

資安責任制度

- 組織管理
  - 由各部會副首長擔任CISO資訊安全長，協助首長善盡維護資安的責任。
  - 各機關應肩負本身資安管理的責任，培育相關人才，並強化自我防護作為。
  - 考量採一定比例方式編列資通安全預算，以確保資通安全設施經費與維護費用的需求。
- 安全控管
  - 指派專人負責資安管控，資訊業務委外時應要求廠商提供資通安全相關服務。

總結

- 資訊是有價的，所以需要保護。
- 資訊安全首要的工作是資訊安全政策的擬定。
- 資訊安全要做好，風險評估不可少。
- 想要企業持續經營，做好營運持續管理及計畫
- 取得資訊安全的認證，不保證100%的安全，需要持續不斷的改善再改善！

參考資料

- ISO/IEC 17799:2005
- ISO/IEC 27001:2005
- CNS 17799。
- CNS 17800。
- ISO/IEC TR 13335 - Guideline for the management of IT Security
- ISO/TR 13569 - Banking and related financial services - Information security guidelines

參考資料（續）

- ISO 19791 - Security assessment of operational system
- ISO 18045 - Methodology for IT security evaluation
- PD 3001 - Preparing for BS 7799 certification
- PD 3002 - Guide to Risk assessment and risk management

參考資料（續）

- PD 3003 - “Are you ready for a BS 7799 audit？”
- PD 3004 - Guide to BS 7799 auditing
- PD 3005 - Guide to the selection of BS 7799 controls

問題與討論

電話：03-5916096
E-mail：NelsonChen@itri.org.tw