財團法人國家實驗研究院
國家地震工程研究中心

資訊安全管理制度輔導顧問案

一般人員資訊安全認知及法令宣導

NII財團法人中華民國國家資訊基本建設產業發展協進會

課程大綱

- 資訊安全之概念說明
- 行政院推動資訊安全現況
- ISMS/ISO27001簡介
- 使用者作業安全管理
- 危機處理與應變措施實例討論
- 資訊安全內部稽核
- 資訊安全法令

課程大綱

- 資訊安全之概念說明

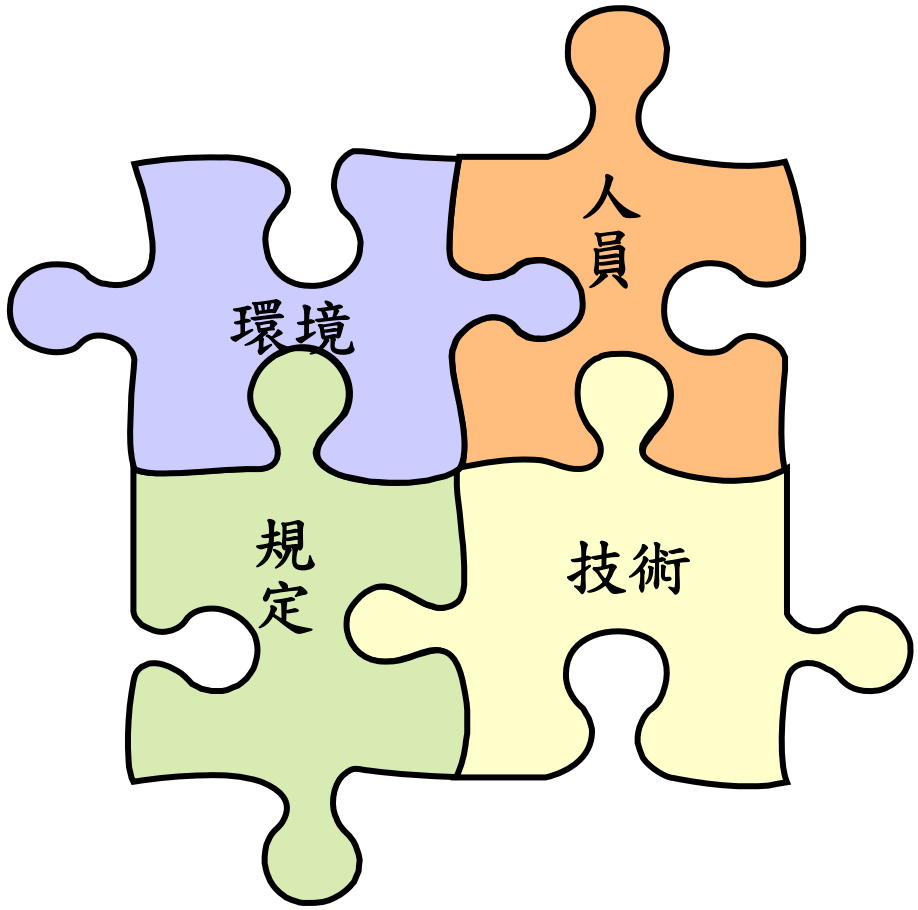
重要詞彙說明

- 什麼是資訊？
- 資訊安全管理制度 (Information Security Management System,ISMS)

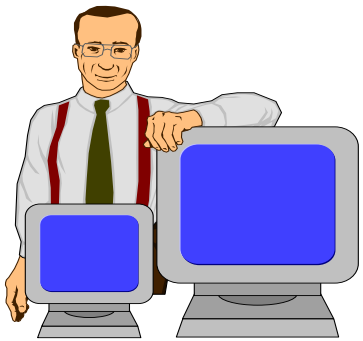
"The Information security management system is that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, maintain and improve information security"

資訊安全範圍

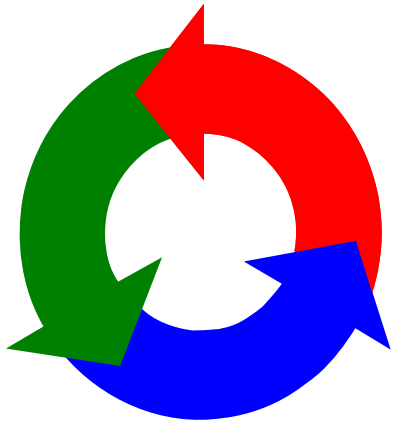
- 資訊使用之『環境』
- 資訊使用之『技術』
- 資訊使用之『規定』
- 資訊使用『人員』

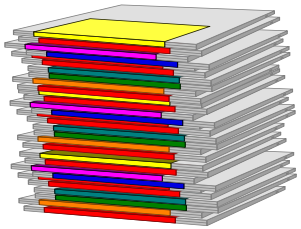


資訊安全管理重點

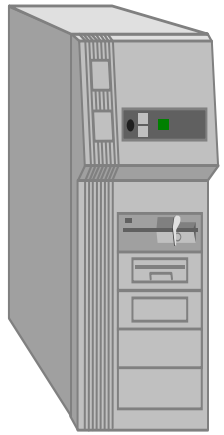


People





Process



Technology

資訊安全三大原則

- 機密性(Confidentiality)：
  確保只有經授權的人才可以取得資訊，避免資訊洩露

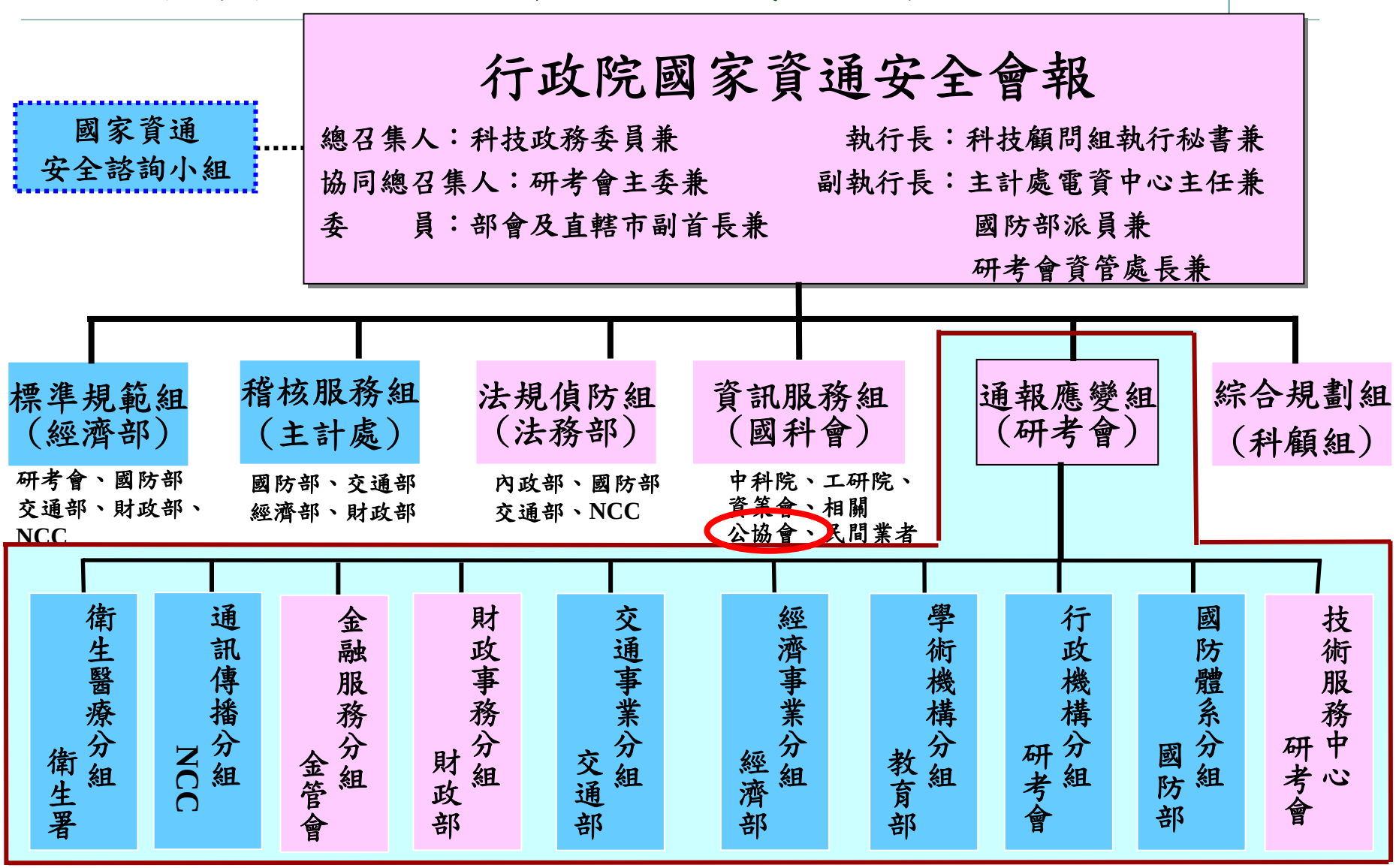
- 完整性(Integrity)：
  確保資訊不受未經授權的竄改與資訊處理方法的正確性

- 可用性(Availability)：
  確保經授權的使用者，在需要時可以取得資訊，並使用相關資產

課程大綱

- 行政院推動資訊安全現況

國家資通安全會報組織架構



資通安全推動計劃

94年~97年
「建立我國通資訊基礎建設安全機制計畫」

NICST
國家資通安全會報

願　　景

確保我國擁有安全、可信賴的資訊通訊環境

94~97資通安全推動計劃 — 政策

1. 健全通報機制，加強應變能力
2. 強化資訊分享，建立互通管道
3. 提昇技術研發，增強防護能量
4. 確保資通安全，提升e化能量
5. 研訂資安法令，查緝網路犯罪
6. 保障人民隱私，加強宣導活動
7. 普及資安教育，加強人才培育
8. 加強區域聯防，建立國際合作

94~97資通安全推動計劃 — 目標

1.健全資通安全應變機制，以服務代替管制，達成二十四小時內通報機制效能

2.建置政府及重要基礎建設之資訊分享及分析中心，提升國家競爭力

3.建立二十四小時監控國家重要基礎建設資安系統，以降低資安威脅及減少被攻擊

4.建置安全無虞資通環境，確保民眾隱私權益，促進政府e化效能

5.推動資訊安全管理制度之認證達一百家以上，提升資安防護能量

6.配合國際資安法令及標準之發展趨勢，訂定我國資安相關法令及標準之制定率達70%以上

7.增強網路犯罪查緝能力，建立國家級資安鑑識實驗室

8.增強全民資安認知能力，培育專業資安人才，每年培育資安專業人才達400人以上

9.健全資通安全防護體系，有效遏止駭客入侵

10.積極參與全球資安活動，建立國際資安聯防機制

94~97資通安全推動計劃 — 範圍及策略

NICST 行政院國家資通安全會報
National Information & Communication Security Taskforce

策　略

1. 由政府機關落實，逐年向民間產業及企業推動
2. 由重點機關（構）推動，逐年全面性、全民性推動擴展
3. 政府機關及民間機構的密切合作，建立完備的資安整體防護體系

政府機關(構)資訊安全責任等級分級作業施行計畫－各類資安系統等級應執行之工作事項

作業名稱 / 內容 / 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(重要核心單位)	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(核心單位)	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(重要單位)	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
D 級(一般單位)	強度等級 1	防火牆防　毒	推動 ISMS 觀念宣導	自我檢視	每年至少(1,4,8,2 小時)	資安專業訓練

課程大綱

- ISMS/ISO27001簡介

ISO27001過去與現在

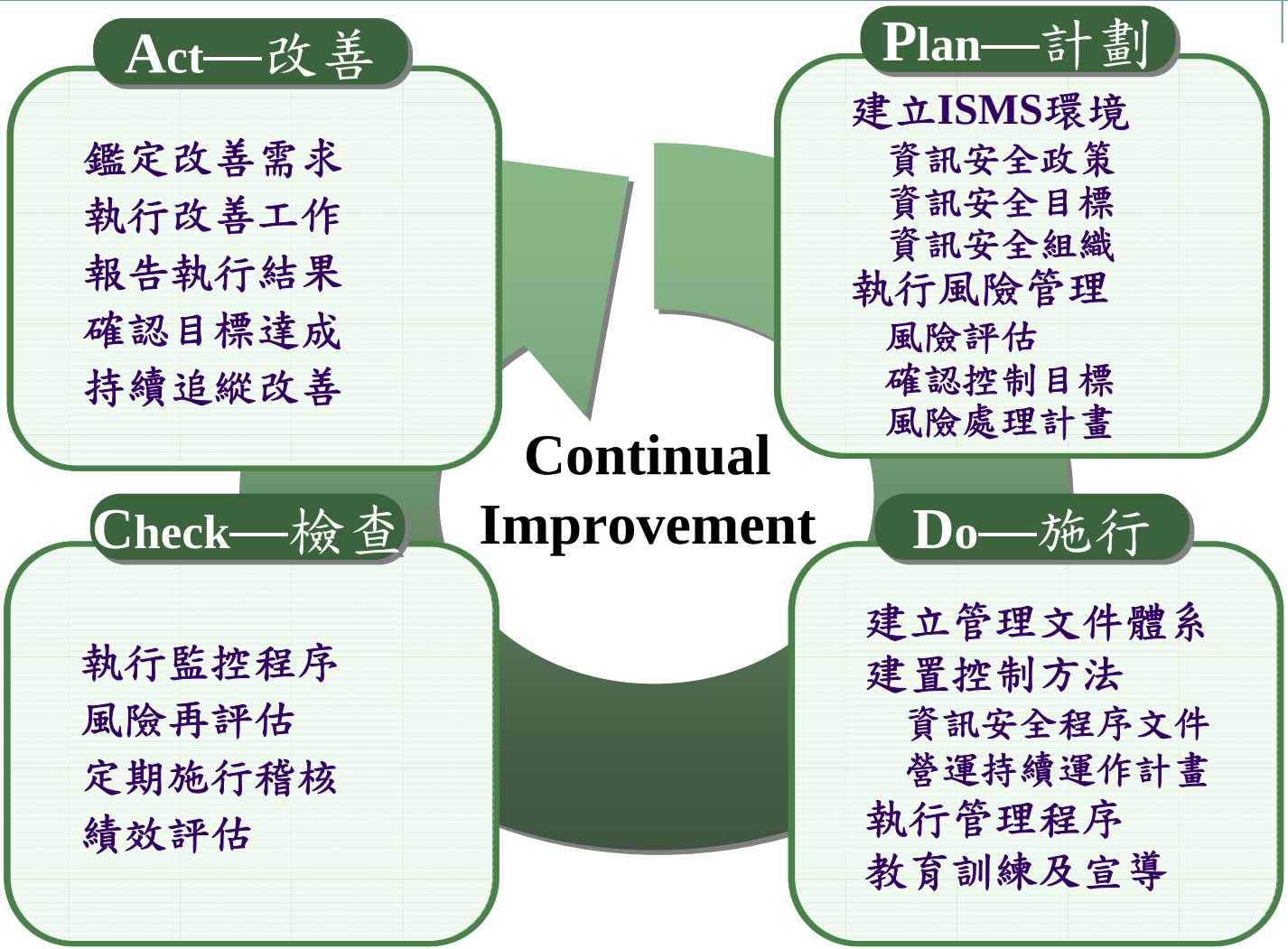
- **BS7799標準更新之歷史：**
  - 1995:英國公佈BS7799 Part I
  - 1998:英國公佈BS7799 Part II
  - 1999:英國公佈新版BS7799 Part I、Part II
  - 2000:ISO通過成為ISO/IEC 17799 Part I
  - 2002:BS7799:2-2002 -資訊安全管理系統驗證規範
  - 2005: ISO/IEC 17799:2005
  - **2005: ISO27001 ISMS認證標準**
  - **2007:ISO/IEC 17799作業規範，正名為ISO27002**

ISO27001驗證現況

2007/11/22　資料來源：
http://www.iso27001certificates.com/

Japan	2317*	Switzerland	12	Lithuania	2
UK	363	Turkey	12	Oman	2
India	347	Saudi Arabia	10	Peru	2
Taiwan	149	UAE	9	Portugal	2
Germany	87	Slovenia	8	Qatar	2
China	74	Sweden	8	Slovak Republic	2
Hungary	58	Iceland	7	Sri Lanka	2
USA	54	Kuwait	6	Vietnam	2
Australia	53	Pakistan	6	Armenia	1
Korea	51	Russian Federation	6	Bulgaria	1
Italy	45	France	5	Chile	1
Netherlands	32	Greece	5	Egypt	1
Hong Kong	30	Thailand	5	Gibraltar	1
Czech Republic	28	Bahrain	4	Lebanon	1
Singapore	28	Canada	4	Luxemburg	1
Malaysia	21	Indonesia	4	Macedonia	1
Brazil	20	Argentina	3	Moldova	1
Austria	17	Colombia	3	Morocco	1
Ireland	17	Isle of Man	3	New Zealand	1
Poland	16	Macau	3	Ukraine	1
Finland	14	Romania	3	Uruguay	1
Norway	14	South Africa	3	Yugoslavia	1
Mexico	12	Belgium	2		
Philippines	12	Croatia	2	**Relative Total**	**4047**
Spain	12	Denmark	2	**Absolute Total**	**4036***

ISMS Lifecycle-PDCA模型之應用

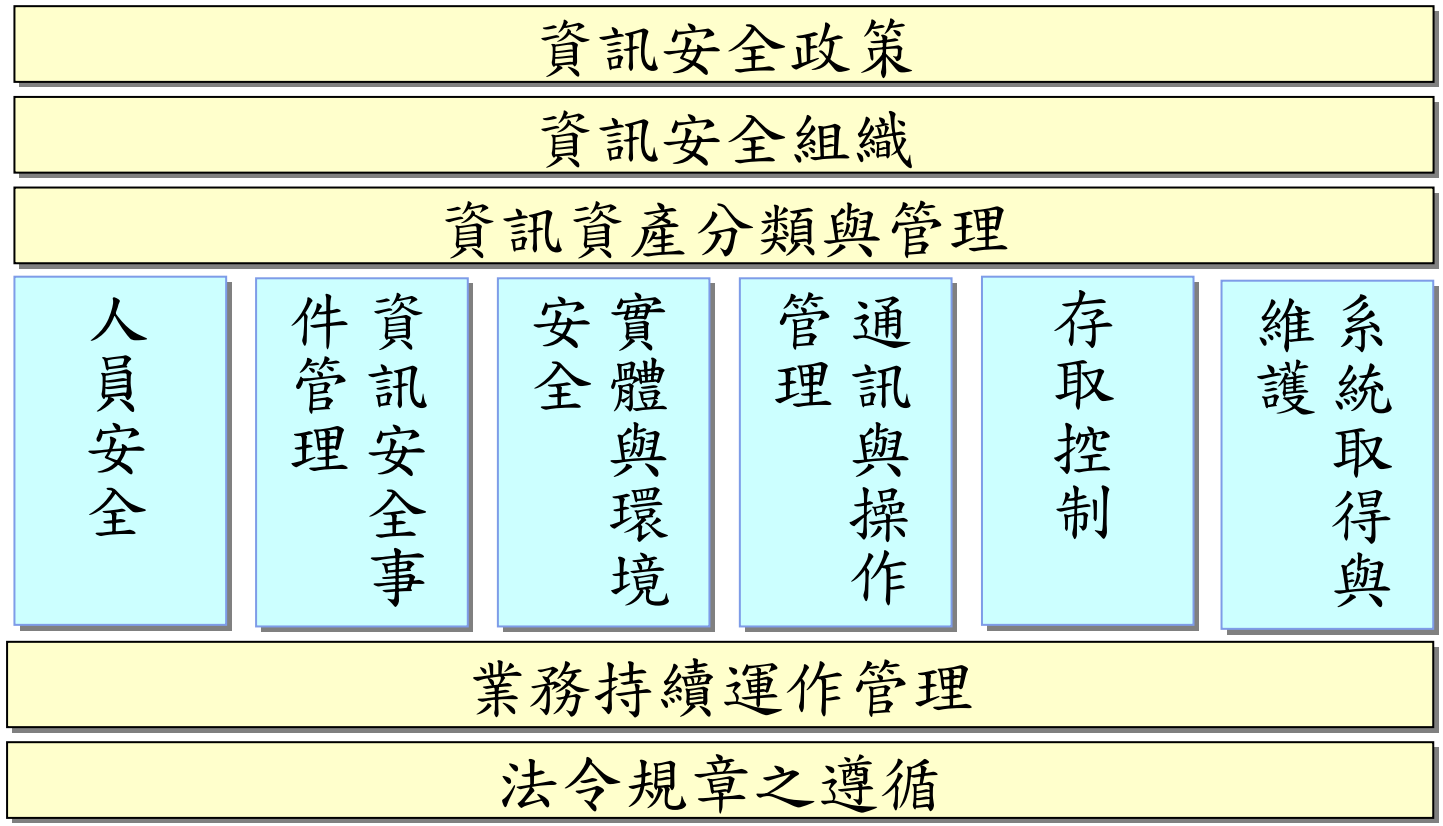


ISO27001本文

- 資訊安全管理系統
  - 一般要求
  - 建立與管理ISMS
  - 文件化要求
- 管理階層責任
- ISMS內部稽核
- ISMS之管理階層審查
- ISMS之改進

ISO27001涵蓋之內容

11 個領域、 39 個控制目標、 133 個控制要點



課程大綱

- 使用者作業安全管理

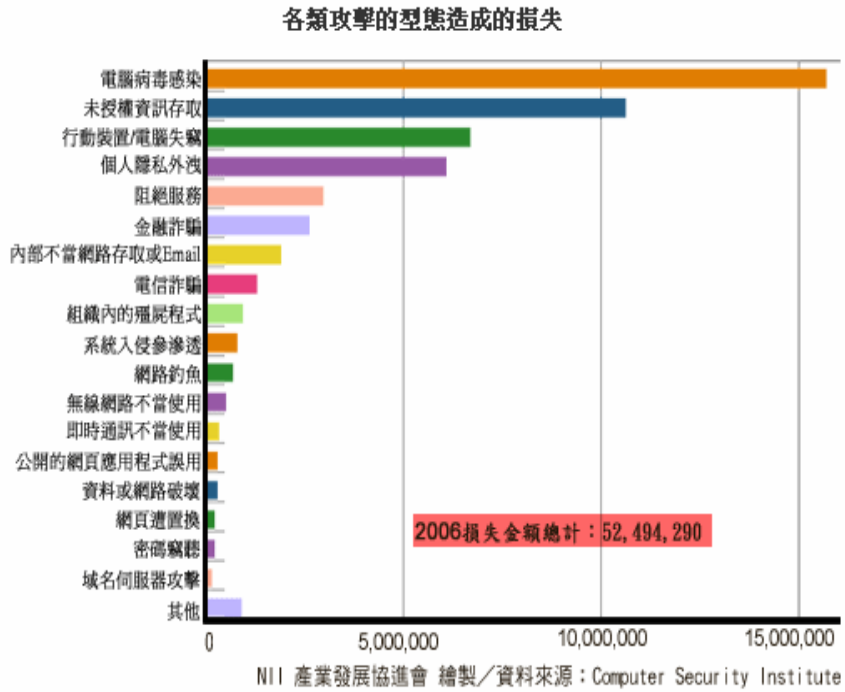
資訊安全損失

- 美國企業2006年資安損失約達5千萬美元

CSI/FBI 2006 Computer Crime and Security Survey：美國企業2006年資安損失約達5千萬美元

資料來源：Computer Security Institute
公布日期： 2006年

根據CSI/FBI 2006 Computer Crime and Security Survey，針對美國企業、政府、金融、醫療、學校等單位資訊安全從業人員調查「各類攻擊的型態造成的損失」，前三名分別是電腦病毒感染、未授權資訊存取、行動裝置/電腦失竊。



使用者責任

- 使用者的態度，對於有效防止非法的使用者存取，以保障安全的工作非常重要
- 目標：防止未經授權的使用者存取資訊與資訊處理設施，以及使其遭受破壞或竊盜
  - 通行碼的使用
  - 無人看管的使用者設備
  - 桌面淨空與螢幕淨空政策

通行碼的使用—密碼管理

- 定期更新密碼
- 定期檢查密碼
- 設定優質密碼
  - 避免使用重複數字/單位簡稱/詞語/生日
  - 數字字母符號穿插且不過於複雜
  - 避免重複使用密碼
- 不告訴他人密碼或寫下密碼
- 懷疑密碼外洩立即更新

無人看管的使用者設備

- 使用者應確保無人看守的設備獲得適當保護。

  安裝在公共區域的設備（如公用主機、印表機或伺服器），應有具體的保護：

  - 在活動完成時應終止對話，結束畫面
  - 使用密碼保護的螢幕保護程式
  - 活動結束時登出系統或主機，再關閉電腦
  - PC或設備不用時，應使用相關安全控制措施，以防止他人非法使用；抑或考慮汰除

桌面淨空與螢幕淨空政策

- 桌面淨空
  - 重要/機密文件不置於桌上
  - 重要/機密文件下班或離開辦公室前應鎖入安全空間
- 螢幕淨空
  - 設定螢幕保護程式
  - 設定保護密碼
  - 離開座位或暫時不使用時鎖定螢幕

網際網路管理要求

- 與網路服務的連線如果不安全，就會影響整個組織
- 在敏感或重要業務應用或與處於高風險區域（如無法管理與控制的公共或外部區域）使用網路連接時，安全控制措施非常重要
- 制定網路服務的使用政策要包含：
  - 允許存取的網路和網路服務
  - 確定存取網路和哪種網路服務的授權程序
  - 保護網路連接和服務存取的管理控制措施和程序
  - 與存取控制政策取得一致性

公共區域無線上網安全性

- 選擇有加密功能的無線基地台
- 使用認證機制對使用人員做好身份管理
- 牽涉到高度機密之相關資訊，避免使用無線傳輸

(資料來源：i-security-輕鬆學資安/資安小撇步 http://www.i-security.tw)

公共電腦使用安全

- 登入網路服務動作的保護
  - 使用公共電腦時，尤其要注意避免勾選任何的記住帳號或密碼的功能
- 使用公共電腦後，關閉網頁瀏覽器，清除個人相關資料
  - 清除網頁瀏覽記錄/網站上所留下的個人資料/電腦中的**cookie**/隱私權記錄/密碼記錄
- 盡量避免利用公共電腦上網處理重要或私密事務
- 特別注意坐在或站在你旁邊的人
- 更換密碼的頻率要更高

網路內容安全風險

- 惡性程式/廣告
  - 假冒輸入畫面
  - Pop-Up廣告
  - ADware(廣告軟體)
- 首頁綁架(Brower Hijacking)
- 間諜軟體(Spy Ware)
- 瀏覽器控制項(Browser Helper Object)

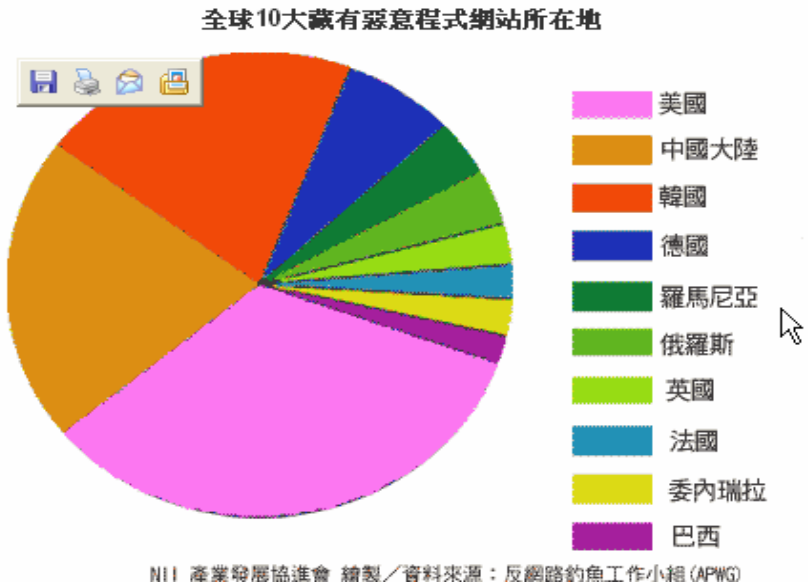
惡意程式網站

- 每十個網站就有一個是惡意網站

APWG: 全球藏有惡意程式網站的前三名國家
2006年11月：美國、中國大陸、韓國，委內瑞拉首次入榜
資料來源：反網路釣魚工作小組(APWG)
公布日期： 2007年1月

反網路釣魚工作小組（Anti-Phishing Working Group） 2006年11月全球網路釣魚調查報告：

全球藏有惡意程式的網站前十名分別在美國(24.2%),中國大陸(15.42%),韓國(14.88%),德國(5.27%),羅馬尼亞(2.84%),俄羅斯 (2.64%), 英國(2.04%), 法國 (1.83%),委內瑞拉(1.81%), 巴西(1.43%)。



網路釣魚攻擊

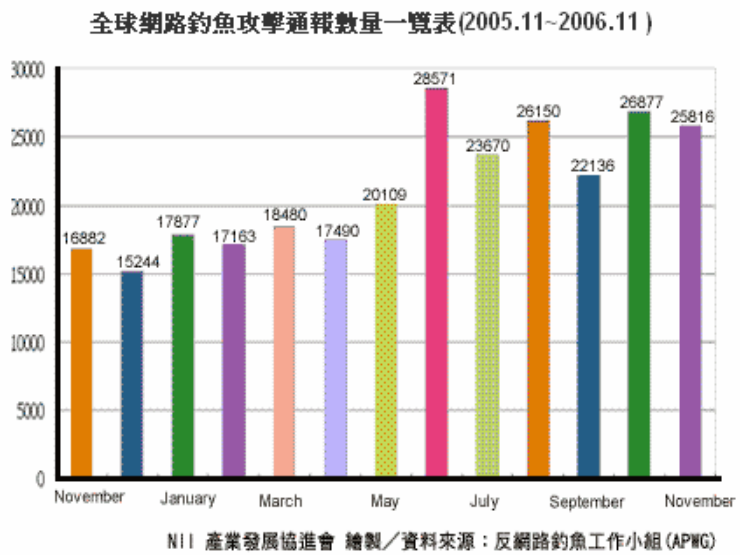
- 全球120個企業品牌被駭客用來透過電子郵件進行網路釣魚詐騙活動
- 英國2006年約350萬人遭網路詐騙

2006年11月全球網路釣魚攻擊通報數量超過25,816個

資料來源：反網路釣魚工作小組(APWG)
公布日期： 2007年1月

反網路釣魚工作小組（Anti-Phishing Working Group） 2006年11月全球網路釣魚調查報告：

- 全球釣魚網站數量達到37,439個
- 全球網路釣魚攻擊通報數量約25,816件
- 全球總計有120個企業品牌被駭客用來透過電子郵件進行網路釣魚詐騙活動



網路犯罪事件

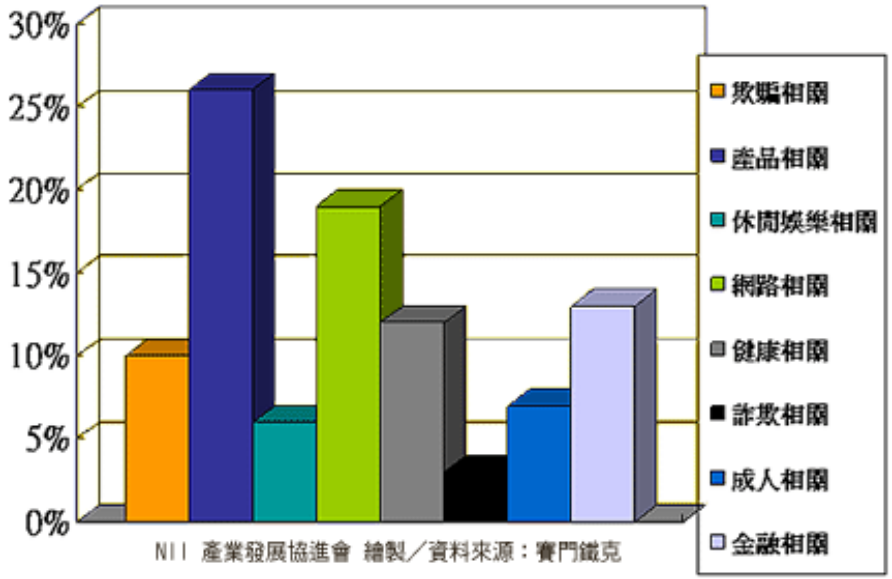
- 據警政署統計，2007年上半年電腦網路犯罪案件數高達一萬三六０八件
- 其中，攸關資料外洩的「網路詐欺」、「妨礙電腦使用」兩項案類，就分佔33%、27%
- 警政署預估，全台有三分之一電腦遭惡意程式入侵或被遠端駭客操縱而不自知

網路使用安全

- 確保網頁瀏覽器使用安全
  - 設定網頁瀏覽器安全性/隱私權
  - 設定信任的網站
- 遠離網路釣魚犯罪陷阱與騙局
  - 不回應不明公司/技術部門要求提供個人隱私或安全資訊
  - 不點選來路不明郵件的網頁連結
  - 不利用企業網路轉寄垃圾郵件

電子郵件風險

- 垃圾郵件量占整體電子郵件流量70%，其中圖像式垃圾郵件數量在全部垃圾郵件中約佔7%
- 常見手法有：
  - 「你在找工作嗎？」徵人垃圾郵件
  - 重複利用相同的連結以及常見品牌來製造垃圾郵件訊息
  - 假冒雅虎Geocities網址的手法持續增加且變化多端



資料來源：賽門鐵克垃圾郵件研究報告
公布日期：2007年10月15日

電子郵件的安全

- 安裝防毒軟體過濾郵件
- 不隨意開啟郵件附檔
- 防堵垃圾郵件
  - 絕對不回覆垃圾電子郵件訊息
  - 不購買垃圾電子郵件的廣告商品
  - 不轉寄串接式的電子郵件，(例如聲稱不轉寄給10 個人就會倒楣的電子郵件。)
  - 要寄送同一訊息給許多收件者時，可採用「密件副本」方式來進行
  - 刪除寄件者為空白的電子郵件
  - 使用垃圾電子郵件過濾軟體
- 垃圾郵件過濾簡易設定
  - 在**Web** 郵件上設定過濾垃圾郵件寄件者
  - 利用常見關鍵字過濾郵件

即時通訊軟體風險

- 存在的風險
  - 病毒威脅
  - 垃圾訊息
  - 檔案交換
  - 洩密
  - 工作效率的影響
- 常犯之錯誤
  - 盲目的檔案分享
  - 將個人帳號資訊以儲存密碼方式設定儲存
  - 任意將個人之連絡者清單給他人

即時通訊軟體使用安全

- 使用者
  - 登入密碼最好不要用「儲存密碼」記錄於系統內
  - 不任意傳遞與分享公司重要資訊或檔案
  - 不任意接收來路不明之分享檔案
  - 使用者必須秉持以公事使用之目的使用企業即時訊息
  - 隨時更新使用端程式

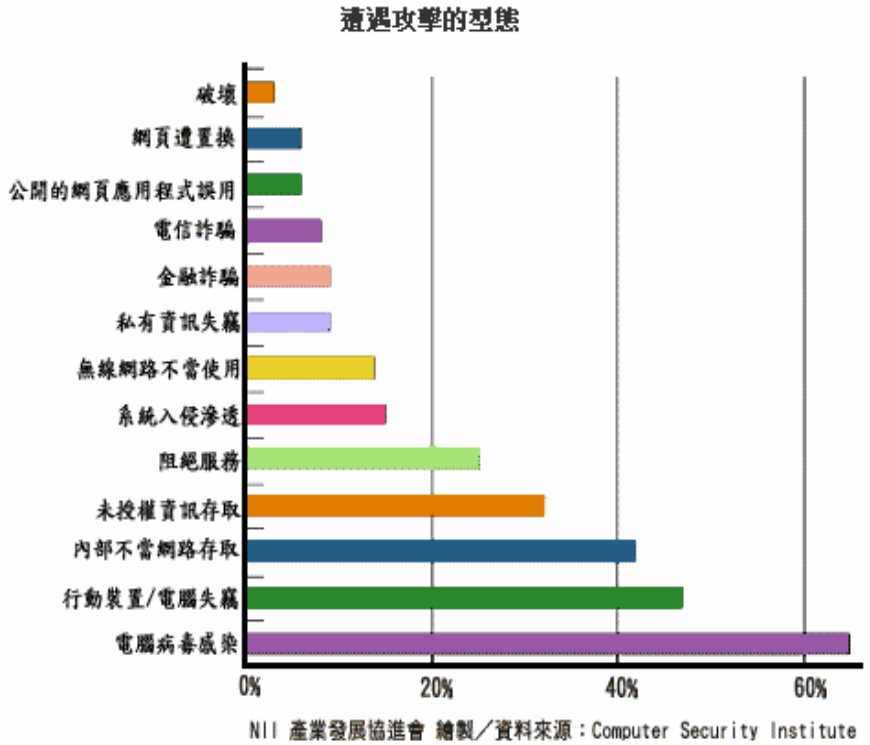
電腦作業威脅—電腦病毒

- 電腦病毒是最常見的攻擊形態

CSI/FBI 2006 Computer Crime and Security Survey：電腦病毒感染是最常見的攻擊形態

資料來源：Computer Security Institute
公布日期： 2006年

根據CSI/FBI 2006 Computer Crime and Security Survey，針對美國企業、政府、金融、醫療、學校等單位資訊安全從業人員調查「遭過攻擊的型態」，前三名分別是電腦病毒感染(65%)、行動裝置/電腦失竊(47%)、內部不當網路存取(42%)。



NII 產業發展協進會 繪製／資料來源：Computer Security Institute

電腦作業威脅—電腦病毒

- 電腦中毒徵兆
  - 電腦系統運行速度異常緩慢
  - 上網速度越來越遲緩
  - 異常的系統訊息通知
  - 螢幕顯示異常，例如畫面突然一片空白
  - 來自防毒軟體的警告訊息
  - 電腦無故自動關機或不斷重新開機
  - 瀏覽器自動出現產品廣告或色情網頁
  - 網路流量異常，例如沒有使用網路服務或收發電子郵件，但網路的連線燈號卻一直閃爍

電腦作業威脅—電腦病毒

- 電腦病毒簡易處理步驟
  - 將中毒電腦離線網路作業
  - 設法使防毒軟體運作
  - 以防毒軟體執行病毒的掃瞄與清除
  - 若防毒軟體無法正常執行，則執行以下替代方案：
    - 手動掃毒
    - 使用未受病毒感染健康的電腦之防毒軟體來進行問題硬碟掃毒作業
    - 透過免費線上掃毒資源，在不危害狀況下連線網路進行

    http://housecall.trendmicro.com/　http://www.symantec.com.tw/
  - 受感染的檔案並執行隔離或刪除動作
  - 未知病毒的處理方式
    - 電腦病毒事件的通報，尋求資源協助
    - 聯絡病毒軟體廠商協助

電腦作業威脅—電腦病毒

- 電腦病毒的防範
  - 確認防毒軟體隨時運作
  - 勿隨意安裝未經許可的電腦軟體
  - 確保軟體在最新更新狀態
  - 使用有問題立即反應

電腦作業威脅—廣告/間諜軟體

- 廣告或間諜軟體的症狀
  - 沒有上網卻還是一直看見廣告視窗
  - 網路速度時快時慢
  - 首頁被更改成奇怪的網站
  - 視窗下方的工具列出現許多原本沒有的工具
  - 瀏覽器多出沒有安裝過的工具列、搜尋工具，而且無法移除
  - 電腦處理速度變慢或當機頻率增加

電腦作業威脅—廣告/間諜軟體

- 間諜或廣告軟體的防範
  - 使用防火牆阻擋
  - 關閉網路瀏覽器的ActiveX 功能
  - 安裝封鎖彈跳視窗功能的工具， 例如Google Toolbar
  - 下載免費軟體前仔細閱讀所有相關資訊
  - 學習資料備份基本技巧
  - 使用至少兩個反間諜軟體程式
- 刑事警察局木馬及鍵盤側錄惡意程式清除軟體「GK 1.0」 http://www.cib.gov.tw/news/news02_2.aspx?no=343

電腦作業威脅—駭客入侵

- 駭客入侵的徵兆
  - 檔案及資料庫內容遭到竊取或篡改
  - 不知名的IP來源與電腦連線
  - 系統中異常的服務程式
  - 異常通訊埠開啟
  - 稽核紀錄及檔案中的異常事件
  - 系統帳號的異常增加
  - 系統異常的訊息或行為

電腦作業威脅—駭客入侵

- 駭客入侵的簡易處理
  - 系統備份
  - 可能入侵途徑系統隔離
  - 蒐集入侵紀錄、檔案等軌跡
  - 追查駭客IP來源
  - 分析資料找出入侵方式
  - 報告相關單位
  - 適時尋求協助

電腦作業威脅—駭客入侵

- 駭客入侵的防範
  - 即時更新修正檔
  - 檢視權限設定
  - 日常備份作業
  - 紀錄及檢視稽核軌跡
  - 設定自動時間校正作業

可攜式設備之安全管理要求(一)

- 使用可攜式設備（如筆記型電腦、掌上型電腦和行動電話）時，應確保業務資訊不受損壞
- 訂定可攜式設備連接網路的規則和公共場所中使用的指導說明，並提供適當保護連接網路的設施
- 使用可攜式設備進行遠端存取時，必須先成功地進行身份識別和驗證並採用適當的存取控制機制
- 在公共場所使用可攜式設備時應採用一定的保護措施，並防範被窺視，以避免儲存和處理的資訊遭到非法存取或洩密

可攜式設備之安全管理要求(二)

- 制定並即時更新用於防範惡意性軟體的程式
- 準備對資訊備份的必要設施，並適當地保護備份的資訊，避免被盜或遺失
- 應防止可攜式電腦化設備被盜，尤其是比如丟在汽車等其他交通工具、旅館、會議中心以及聚會場所內
- 內含重要、敏感和/或關鍵業務資訊的設備不應無人看管。如果可能，應上鎖。應使用專用鎖來保障設備的安全
- 進行可攜式設備的資安訓練，提高他們對可攜式設備可能帶來額外風險的防範意識，以及因應措施的認識

資料備份

- 不論是紙本或電子檔的重要資料，皆應：
  - 定期備份
  - 存放在不同地方(異地備份)
- 資料備份原則
  - 資料價值較高時應優先備份
  - 選擇適合之儲存媒介進行資料備份工作
  - 按所欲備份的資料型態，選擇方法進行備份 Ex.完全備份/ 選擇性備份/漸進式(增量)備份
  - 備份的資料需定期做資料回復測試， 以確認備份資料的可用性

資訊儲存媒體的管理

- 儲存媒體的管理
  - 制定儲存媒體（如磁帶、磁片、盒式磁帶以及列印報告）的管理辦法
  - 應明確記錄所有的管理步驟和授權級別
- 儲存媒體的報廢
  - 具敏感資訊的媒體應該進行安全保險的保存和處置
  - 安全收集和報廢所有媒體
  - 謹選具有經驗及技術的合格合約商
  - 儘可能記錄敏感資料的報廢，並保留稽核追蹤
- 儲存媒體的運送安全
  - 使用可靠的傳輸工具或投遞人
  - 包裝應該可以保護不受運輸過程中事故造成損壞
  - 依需要採取特殊的控制措施保護敏感資料免遭非法公開或修改

課程大綱

- 危機處理與應變措施實例討論

2001 – 9 –11 ?

認識風險及災害

- 何謂風險 **(Risk)**
- 何謂災害（**Disasters**）
- 災害的種類
  - 人為：火災、人為破壞、偷竊等等
  - 天然：火災、風災、地震、水災等等
- 為何需要災害復原計畫？
- 一套災害復原計畫夠不夠？

（儘可能辨識所有可能的災害）

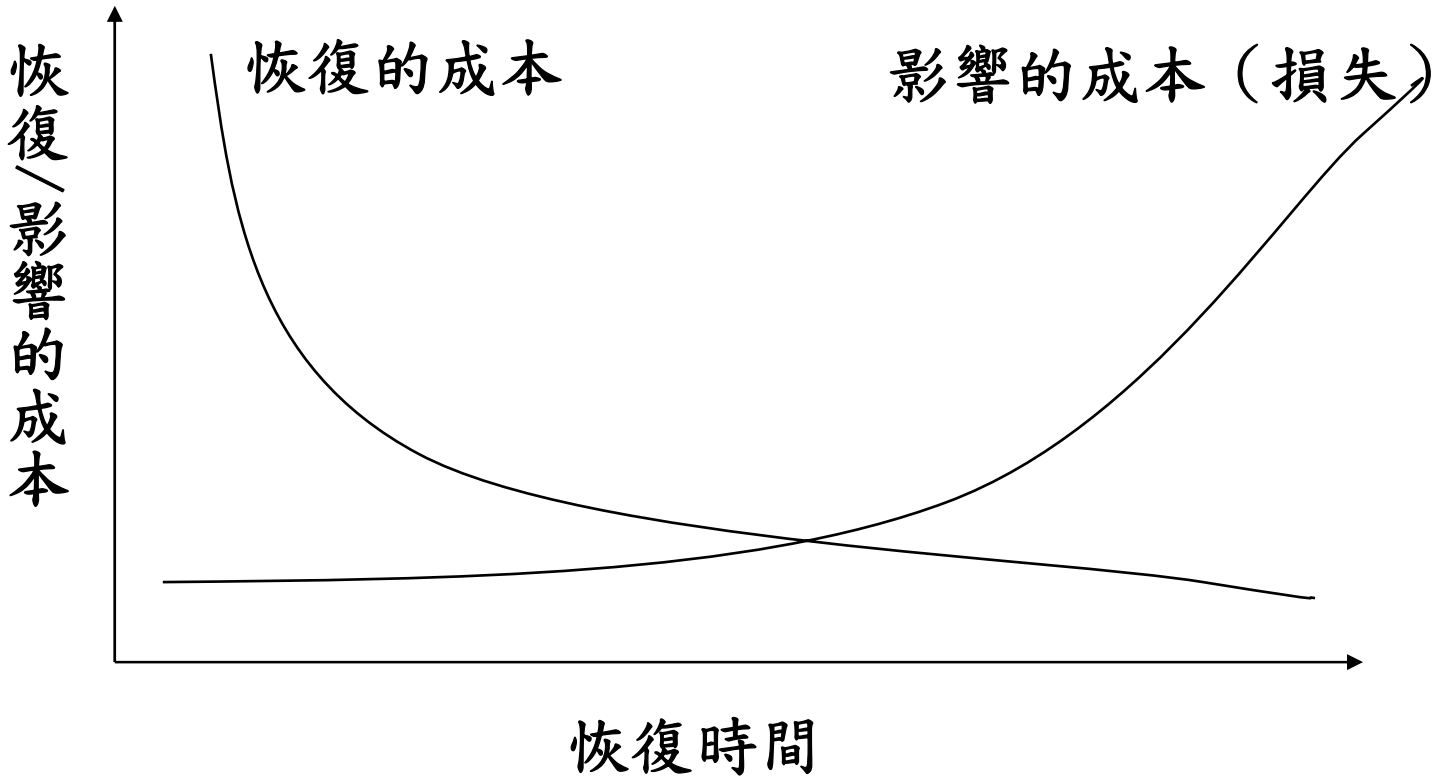
危機處理的第一步

- **BIA- Business Impact Analysis(營運衝擊分析)**
- **BIA的目的？**
  - 鑑別企業關鍵營運活動無法持續時的營運衝擊，以及復原至最低營運水準，所要求的可接受時間長短。
- **執行BIA的重點為何？**
  - 組織有哪些關鍵性業務（Critical Business）
  - 關鍵性業務所需的關鍵性資源

危機處理的第二步

- 將關鍵系統（資源）排序（依風險大小）
  - **Critical**：取代性低、故障容忍度較低、損失大
  - **Vital**：可暫時由人工取代、故障容忍度比Critical的系統高一點、損失是在可接受範圍
  - **Sensitive**：系統可長時間由人工取代，損失是在可接受範圍
  - **Non-critical**：系統既使故障也不會影響組織的運作

危機處理的第三步



災害復原計畫大綱

- 主要決策人員（Key Decision-Making Personnel）
- 所需設備之備援（Backup of Required Supplies）
- 組織及人員任務的分派（Organization and Assignment of Responsibilities）
- 通訊網路（Telecommunication）
- 保險（Insurance）

主要決策人員

- 回報體系的建立
- 回報窗口，災難發生的第一時間點應該向誰回報？
- 通報的方式（如電話、地址）
- 供應商或服務廠商的緊急聯絡表
- 保險代理人的緊急聯絡表

課程大綱

- 資訊安全內部稽核

資訊安全稽核的中心思想

資訊安全內部稽核目的

- 覆核控管程序是否落實
- 評估管理成效
- 協助發現缺失
- 提供改善方案

控制風險

稽核應有之內涵

- 有系統的過程
- 符合組織之目標
- 查核證據
- 客觀性
- 與公認標準相符合
- 傳達查核結果

課程大綱

- 資訊安全法令

資通安全相關法令

- 國家機密保護法
- 電子簽章法
- 刑法(防駭條款)
- 電腦處理個人資料保護法
- 檔案法
- 著作權法
- 行政院及所屬各機關資訊安全管理要點
- 智慧財產權 **Intellectual Property Rights (IPR)**

案例(一)

- **案例描述** (資料來源:2007/10/10 天下雜誌)
- 多家知名電信公司、ISP廠商、學術網站等，**遭駭客入侵破解通行碼**，客戶個資遭盜竊合計近千萬筆，經查犯案者為苗栗某國立大學學生，該學生計畫以數百萬元代價販賣給犯罪組織。警政署呼籲電信、網路服務公司由於存放眾多客戶資料尤應加強資安防範，若本案未能即時查獲，其所造成之損害難以估計。

- 適用法條
  - 觸犯刑法第358條「**無故入侵電腦罪**」。
  - 觸犯刑法第359條「**無故取得、刪除或變更他人電磁紀錄罪**」。

案例(二)

- **案例描述** (資料來源:2007/11/16 中國時報)
- 電腦駭客蘇柏榕，涉嫌夥同林姓高二生，以**學術網站**為掩護，入侵各國中網站，竊取學籍資料，以每筆五元代價販售給補習班。他們將**跳板主機**隱藏在**台灣學術網路**內，利用木馬程式、網站漏洞，侵入網站取得資料，**存放在國外網站主機**，用以規避追查，於九月廿一日遭刑事局及桃園縣警局聯手查獲。

- 適用法條
  - 觸犯刑法第358條「**無故入侵電腦罪**」。
  - 觸犯刑法第359條「**無故取得、刪除或變更他人電磁紀錄罪**」。
  - 違反「**電腦處理個人資料保護法**」。

案例(三)

- **案例描述** (資料來源:2007/11/17 中國時報)
- 衛生署疾病管制局(ＣＤＣ)爆發電腦網路管控不當，致使1279名被限制搭機的結核病患者個人資料在網路曝光！民眾在知名網站「Google」(中文版)就可搜尋得到病人資料，從姓名、居住地，乃至身分證號碼、罹病狀況統統一目了然。ＣＤＣ十六日晚聲明認錯道歉，必要時將國家賠償。
- 全國25縣市、1279名經ＣＤＣ列管為「痰陽」之開放性結核病患（**不得搭乘航程八小時以上班機**），包含暫時不得搭機之多重抗藥性（ＭＤＲ）及超級抗藥性（ＸＤＲ）患者的姓名全名、設籍縣市及地區、照護院所代號、最近就醫日，甚至連英文字母在內十碼身分證字號...，竟然全都可以透過Google搜尋 。
- 適用法條
  - 依「**傳染病防治法**」受害當事人得提請國家賠償。
  - 違反「**電腦處理個人資料保護法**」

案例(四)

- **案例描述** (資料來源:2007/11/21 中國時報)
- 曾任職**銀行外包代辦現金卡公司**的男子翁文欽，離職後做起出售客戶個人資料的生意，詐欺及盜刷集團都向他買過資料。
- 警方調查，銀行外包代辦現金卡的常豐公司，前年十一月設立，去年四月停業，翁文欽藉此機會**留存客戶個資**，還上網利誘在賣場、加油站打工的工讀生側錄民眾信用卡卡號及背面檢核碼。翁文欽並將持有的民眾個資，以電子郵件**轉賣寄往詐欺或盜刷集團**。

- 適用法條
  - 觸犯刑法「**電腦詐欺罪**」、「**偽造文書罪**」以及「**電腦處理個人資料保護法**」等刑責。

刑法(第36章)

- 隨著資訊科技快速發展，網際網路應用日益普及與多元，除了帶給我們許多生活上的便利，但也衍生一些資通安全問題，特別是網路犯罪行為已有增多趨勢
- 網路犯罪行為大約可歸類下列三種
  - **以網路作為犯罪工具–網路詐欺、網路恐嚇等**
  - **以網路作為攻擊標的–竄改檔案、阻斷式服務攻擊、駭客入侵、電腦病毒等**
  - **以網路作為犯罪場所–如色情、誹謗、賭博等**
- 為避免電腦犯罪與維護網路秩序，特於刑法中設立相關法令條文以為管理-**刑法第36章「妨害電腦使用罪」**

刑法(第36章)

- **第358條 無故入侵電腦罪**
  - 無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金
  - 本條主要目的為遏止駭客入侵行為。
- **第359條 無故取得、刪除或變更他人電磁紀錄罪**
  - 無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金
  - 本條主要目的為確保電腦內部電磁紀錄安全
- **第360條 無故干擾電腦系統罪**
  - 無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金
  - 本條主要目的為維護電腦及網路運作正常

刑法(第36章)

- 第361條 對公務機關犯罪之加重
  - 對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一
  - 本條主要目的為確保國家安全
- 第362條 製作供犯罪程式罪
  - 製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金
  - 本條主要目的為防止犯罪工具之利用與擴散
- 第363條 告訴乃論
  - 第三百五十八條至第三百六十條之罪，須告訴乃論
  - 本條主要目的為集中司法資源對抗重大犯罪

電腦處理個人資料保護法(一)

- 立法目的
  - 對公務與非公務機關蒐集、處理、與利用個人資料的情形，加以明文規範
  - 避免個人人格權（隱私權）遭受侵害，促進個人資料之合理利用，特此制定電腦處理個人資料保護法
- 保護客體
  - 本法保護客體限於經電腦處理的個人資料
  - 受本法保護之個人資料以現仍生存之自然人為限，已死亡之自然人與法人，不受本法之規範
  - 個人資料包含:自然人之姓名、出生年月日、身分證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情況、社交活動、及其他足以識別該個人之資料

電腦處理個人資料保護法(二)

- 適用主體
  - 本法規範的對象有公務機關及非公務機關
  - 公務機關係指依法行使公權力之中央或地方機關
  - 非公務機關係指以下所列之事業、團體或個人
    - 徵信業、以蒐集或電腦處理個人資料為主要業務之團體或個人
    - 醫院、學校、電信業、金融業、證券業、保險業、大眾傳播業
    - 其他經法務部會同中央目的事業主管機關指定之事業、團體或個人
  - 受公務機關或非公務機關委託處理資料之團體或個人，於本法適用範圍內，其處理資料之人，視同委託機關之人

電腦處理個人資料保護法(三)

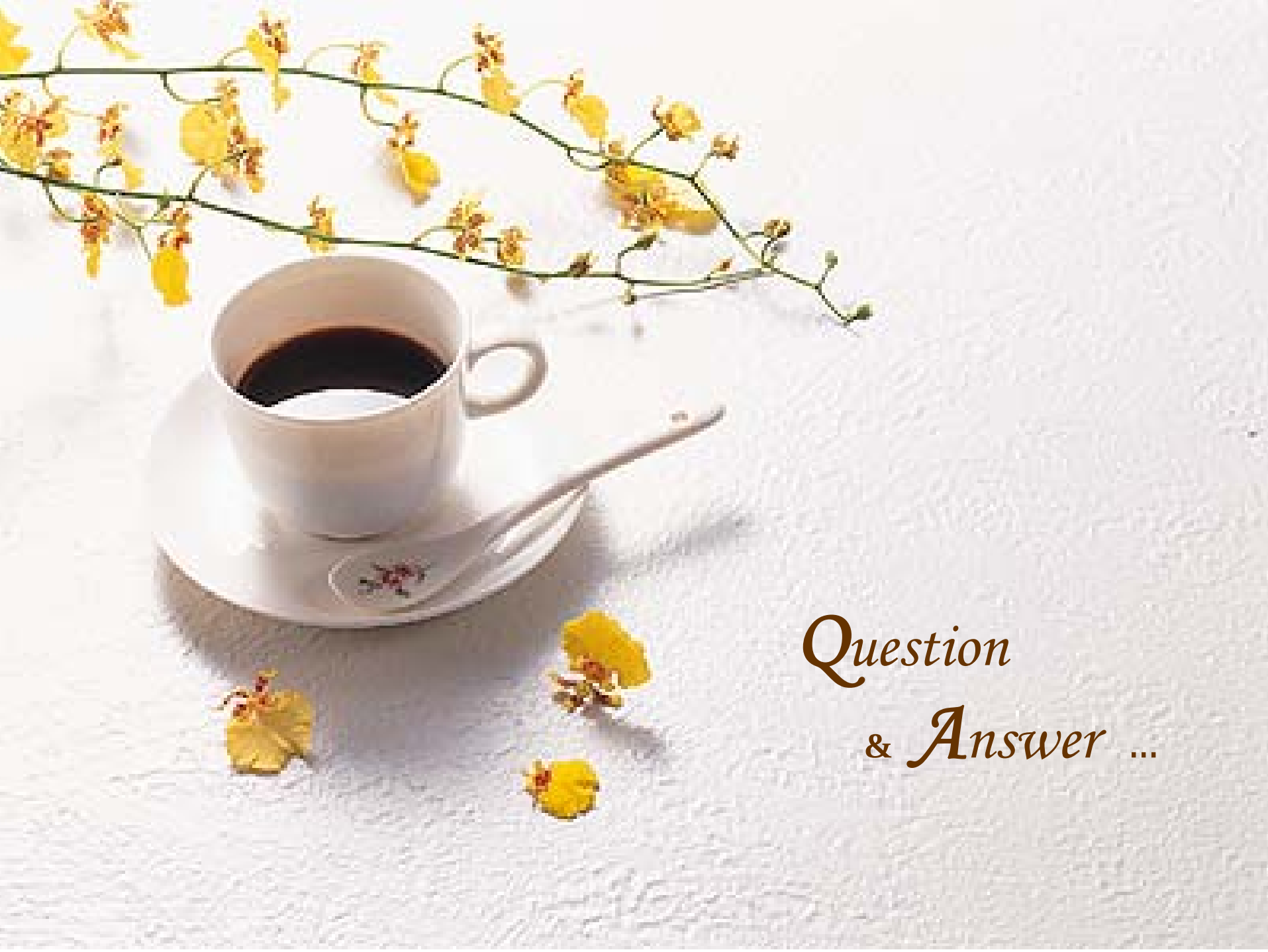
- 機關對個人資料之蒐集或利用的原則
  - 應尊重當事人之權益，依誠實及信用方法為之
  - 不得逾越特定目的之必要範圍，以確保當事人權益，避免人格權受到侵害
- 揭露個人資料，當事人是主要關鍵人物，當事人本身需審慎決定何者為提供給公務與非公務機關的必要個人資料

電腦處理個人資料保護法修訂草案

- 修法背景
  - 法務部為因應急速變遷之社會環境，特別彙整國內學界與實務界的相關修法建議，並參考其他國家之個人資料保護相關法令來針對本法進行修訂
- 修訂草案共有55條，預計將本法名稱修訂為「個人資料保護法」
- 草案修正方向
  - 擴大保護客體
  - 普遍適用主體
  - 增修行為規範
  - 強化行政監督
  - 妥適調整罰則
  - 促進民眾參與

電腦處理個人資料保護法修訂草案

- **修法重點說明**
  - **將買賣個人資料行為從告訴乃論罪修改為公訴罪，並提高刑責，最高為五年有期徒刑**
    - 寄廣告信、垃圾郵件將觸法，未經個人同意，網路公司或個體戶大舉販賣蒐集的大筆電子郵件信箱供寄發垃圾郵件等行為，均將觸犯本法，檢警接獲檢舉後必須主動追查
    - 若是**公務員涉案，依法得加重其刑二分之一**，最重可處七年半徒刑，與刑責已接近涉及貪瀆案
- **重罰意圖營利而違法的行為**，修訂草案大幅加重「意圖營利而違法蒐集、利用或盜賣個人資料者」的刑責，由原本二年以下徒刑，提高為**五年以下徒刑**，且併科由原先四萬元大幅提高為**五百萬元罰金**


Question
& Answer ...