教育部100年度C、D級機關學校資訊安全稽核服務聯合輔導

NII產業發展協進會　吳昭儀 經理

A課程大綱

一、資訊安全管理制度導入說明

二、資訊資產鑑別、評價與管理

1. 資訊資產概述
2. 資訊資產鑑別與評價
3. 資產管理作業

三、風險評鑑與管理

1. 風險概述
2. 風險評鑑與管理
3. 範例說明

一、資訊安全管理制度導入說明

資訊安全三大目標

- 機密性
- 完整性
- 可用性

資訊安全三大目標

- 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。
  - 資料不得被未經授權之個人、實體或程序所取得或揭露的特性。避免未經授權的人以不法手段竊取資料內容。
  - 例如：在網路上看機密文件時要避免資料被他人以不法方式竊取。

資訊安全三大目標

- 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。能判斷資訊內容是否保持原貌、未被竄改。
  - 例如：確保資料在傳輸的過程中能夠受到完整的保護，且確保不會被阻擋並篡改資料。

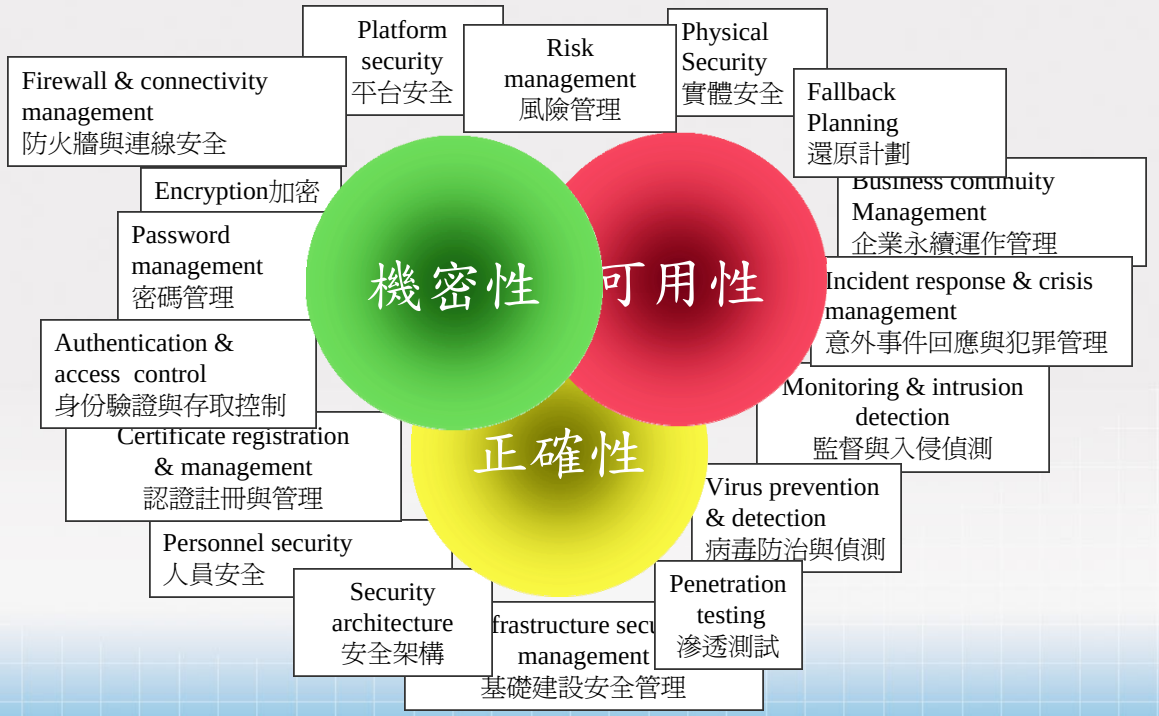
資訊安全三大目標

■ 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。
- 例如：確保資料能夠隨時儲存及使用。

ISMS目的在於保護資訊資產的機密性、可用性與完整性。

資訊安全管理內容



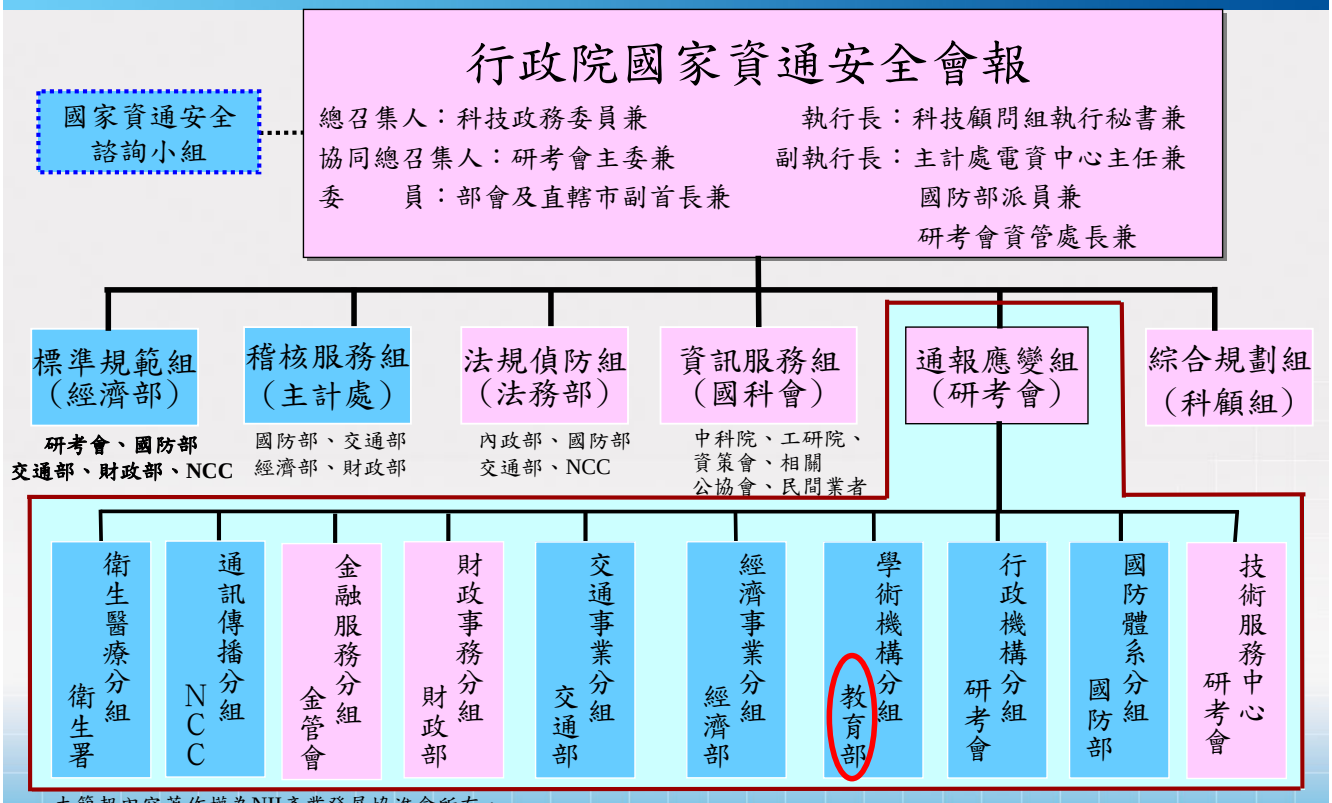
資訊安全管理制度

■ 資訊安全管理制度

(Information Security Management System, ISMS)

- 整體管理系統的一部分，以營運風險方案為基礎，用以建立、實施、操作、監督、審查、維持及改進資訊安全。

國家資通安全會報組織架構



98~101國家資通訊安全發展方案－願景、政策

願景：

安全信賴的智慧台灣、安心優質的數位生活

政策：

1. 強化整體回應能力
2. 提供可信賴的資訊服務
3. 優質化企業競爭力
4. 建構資安文化發展環境

98~101國家資通訊安全發展方案－重要措施

1.提升通報應變及復原能力
2.落實電子化政府資安管理
3.推動關鍵基礎建設網路安全
4.強化企業資訊安全
5.發展資安服務業
6.完備法治建設
7.推動認知宣導
8.鼓勵創新合作
9.規劃衡量指標

98~101國家資通訊安全發展方案－行動方案

1.提升通報時效
2.建立資安事件管理與回應程序
3.持續發展緊急應變及復原能力
4.訓練資安事件回應能力

5.發展與維護政府機關資安作業規範與參考指引
6.推動資安治理
7.推動資訊與資訊系統分類分級
8.強化電子化政府資通安全，落實公務資料保護

9.推動政府機關(構)採購符合安全驗證之資通訊設備

10.充實資安人力
11.提升資安防護技術與服務品質
12.強化資安素養與能力培訓
13.加強資安稽核與推動資訊安全管理系統驗證

14.發展關鍵資訊基礎建設保護策略
15.強化電子商務信賴安全
16.依法規授權促進事業機構運用第三方評鑑
17.促使業者發揮自律精神，善盡資安社會責任
18.發展資通安全產品及管理系統認驗證標準及體系
19.強化國家資安研究能量
20.建構資安人才培育體系
21.檢討修訂國家資通安全相關法規
22.持續發展數位鑑識能量
23.推動教育體系資通安全計畫
24.提供全方位資安資訊服務
25.整合資安資源之訊息，分眾加強宣導
26.規劃依資安策略需要而運作的新型組織
27.鼓勵讓資源發揮最佳效益的創新作法
28.促進有效的團隊合作
29.促進國際合作
30.調查與發佈資安關鍵指標

政府機關(構)資訊安全責任等級分級作業施行計畫－各機關資安等級應執行之工作事項

作業名稱 / 等級	防護縱深	ISMS推動作業	稽核方式	資安教育訓練(一般主管、資訊人員、資安人員、一般使用者)	專業證照	檢測機關網站安全弱點
A級	NSOC直接防護/SOC自建或委外、IDS、防火牆、防毒、郵件過濾裝置	98年底前通過第三者驗証	每年至少2次內稽	1.每年至少(3、6、18、3小時) 2.資訊人員、資安人員需通過資安職能鑑定	維持至少2張資安專業證照	每年2次
B級	SOC(選項)、IDS、防火牆、防毒、郵件過濾裝置	100年底前通過第三者驗証	每年至少1次內稽	1.每年至少(3、6、16、3小時) 2.資訊人員、資安人員需通過資安職能鑑定	維持至少1張資安專業證照	每年1次
C級	防火牆、防毒、郵件過濾裝置	自行成立推動小組規劃作業	自我檢視	每年至少(2、6、12、3小時)	資安專業訓練	每年1次
D級	防火牆、防毒、郵件過濾裝置	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	每年1次

行政院資訊安全責任等級分級作業

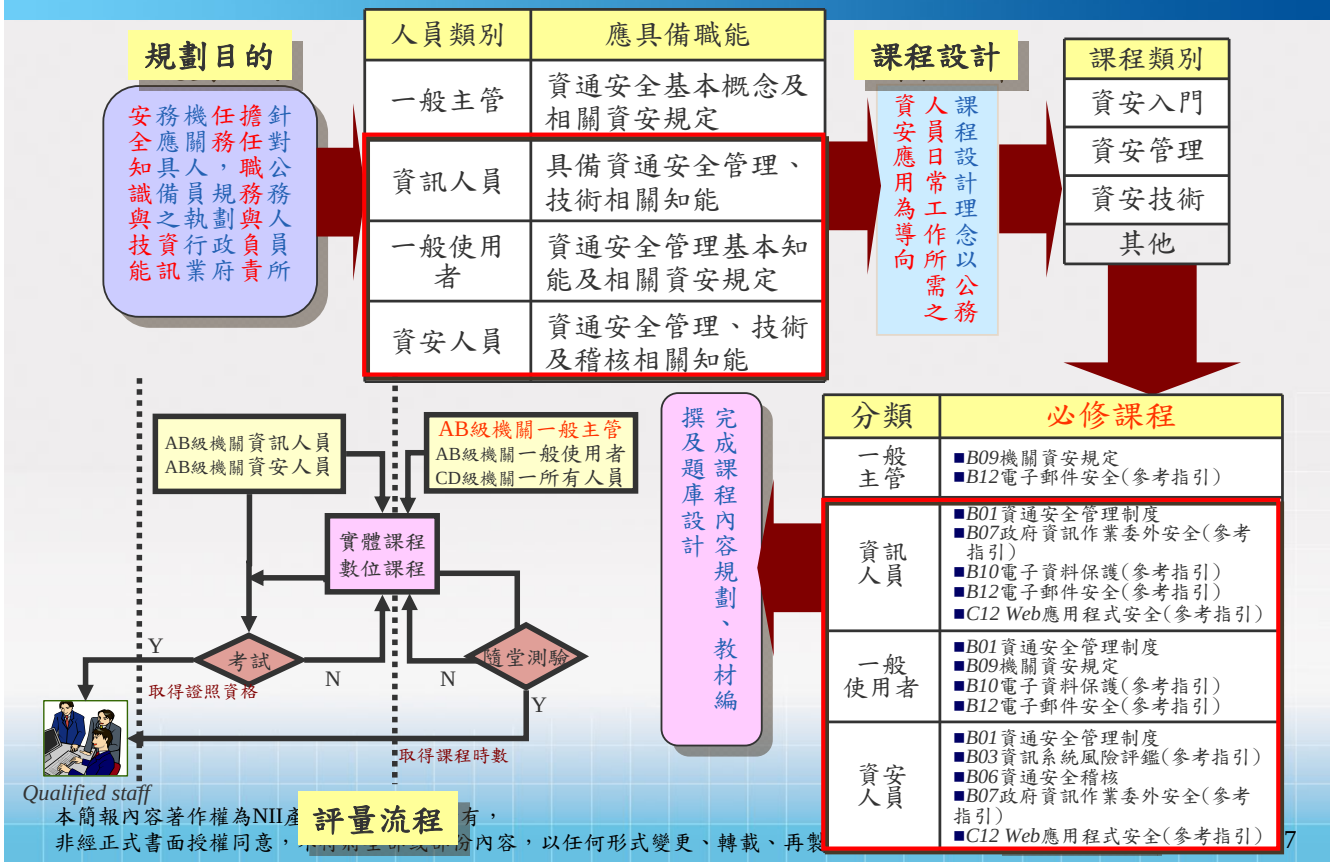
- 教育部所屬機關及各級公私立學校資訊安全責任分級
  - A級：教育部、台大醫院、成大醫院
  - B級：大學、區域網路中心、縣(市)教育網路中心
  - C級：學院、專科學校、部屬館所
  - D級：高中職、國中小學

作業名稱 / 等級	防護縱深	ISMS推動作業	稽核方式	資安教育訓練(主管、資訊人員、資安人員、一般使用者)	專業證照	檢測機關網站安全弱點
A級	NSOC直接防護/SOC自建或委外、IDS、防火牆、防毒、郵件過濾裝置	98年前通過第三者驗証	每年至少2次內稽	每年至少(3、6、18、3小時)資訊人員、資安人員需通過資安職能鑑定	維持至少2張資安專業證照	每年2次
B級	SOC(選項)、IDS、防火牆、防毒、郵件過濾裝置	100年前通過第三者驗証	每年至少1次內稽	每年至少(3、6、16、3小時)資訊人員、資安人員需通過資安職能鑑定	維持至少1張資安專業證照	每年1次

政府機關(構)資訊安全責任等級分級作業施行計畫－各機關資安等級應執行之工作事項註釋說明(一、二)

- 驗證範圍應涵蓋機關（構）之核心業務資訊系統，並逐步擴大至全單位。
- 資安教育訓練
  - 一般主管：擔任主管職務相關人員，如機關(副)首長、部門主管(含資訊主管)等。
  - 資訊人員：負責資訊作業相關人員，如系統分析設計人員、系統設計人員、系統管理人員及系統操作人員等。
  - 資安人員：負責資通安全業務相關人員，如資安管理人員、資安稽核人員等。
  - 一般使用者：一般業務、行政、會計、總務人員等單位內資訊系統的使用者。

公務人員資安職能規劃示意圖



學術單位的資訊安全需求

- 為什麼學校單位需要資訊安全
  - 學生學籍資料
  - 成績資訊
  - 強化資訊網路防護能力
  - 建立機制、程序與PDCA流程管理
- 學校單位所擁有的資訊特色
  - 非機密性
  - 敏感性且涉及隱私及個人資料保護法相關規定

教育體系資通安全管理規範計畫

- 政府為了滿足各行政單位之需求，民國88年制定了「行政院及所屬各機關資訊安全管理規範」。
- 由於學術單位與政府機關的屬性不同，雖然行政院已有頒布可依循之規範，但無法適用於教育體系，因此有必要研擬一套專屬的資通安全管理規範。

教育體系資通安全管理要求

- 教育部於 96 年 6 月 11 日發函各機關學校公布推動「教育體系資通安全管理規範」及「國中小學資通安全管理系統實施原則」為教育體系 ISMS 建置參考。
- 可於校園資訊安全服務網http://cissnet.edu.tw/下載

教育體系資通安全管理規範發展背景

- 為協助教育體系各級單位，以有限的成本與時間，達到資訊安全之目標，95年度由成功大學賴溪松教授、NII 團隊共同草擬，並邀請產官學研界專家共同檢視與修正。
  - 參考 CNS_ISO 27001、CNS_ISO 27002與我國政府規範等法令標準，訂定出適用於教育體系之資訊安全管理規範。
  - 使各級學校與教育網路中心能以最低成本與時間，建構嚴謹且合適之資訊安全管理系統。
  - 配合教育部規劃之「教育機構資訊安全管理系統(ISMS)驗證機制」，建構國內專屬之第三方驗證標準。

教育體系資通安全管理規範設計原則

- 施行單位規模
- 施行單位之業務內容
- 施行單位可運用之資源
- 施行單位之執行能力
- 施行單位於資訊安全控管上的需求
- 成本效益原則

規範設計之參考準則

- 將CNS_ISO 27001中不適用各連線單位之項目予以調整；並將語義不清或不適用之文字進行修改。
- 參酌CNS_ISO 27002控制措施之最佳實務說明進行實作建議。
- 參酌行政院及所屬各機關資訊安全管理規範為稽核項目範本，並刪除其中不適用之項目。

適用範圍

- 本規範適用於教育部電算中心、部屬館所、縣市網中心、大專院校以及高中職資訊管理單位等資訊業務相關單位（或其他管理單位認為應加入ISMS規範範圍之部門）。
- 依單位層級區分二群
  - 第一群：教育部電算中心、部屬館所、縣市網中心、公私立大專院校（計網中心及校務行政）等。
  - 第二群：公私立高中職學校為主要。
- 依業務分為「學術網路系統」與「行政資訊系統」。

與 ISO 27001 標準之比較

規範名稱	章節數	控制目標	較適用於學術網路系統	較適用於行政資訊系統
ISO 27001:2005(E)	11	39		
教育體系資安管理規範	11	36	33（除A.10.5, A.12.1, A.12.2之外）	35（除A.10.6之外）

規範名稱	控制項		稽核項	
ISO 27001:2005(E)	133		至少424項（行政院版本）	
教育體系資安管理規範	(1)100	(2)69	(1)約323	(2)約215

(1) 較適用於第一群項目（A、B、C級）
(2) 較適用於第二群項目（D級）

規範內容 – 整體架構

- 資訊安全管理制度建置步驟
  - ISMS之建立、ISMS之實施與操作、ISMS之監控及審查、ISMS之維持及改進
- 資訊安全管理系統 (ISMS)建置需求
  - 文件要求、管理階層責任、管理階層審查
- 控制項（共11個領域）
  - 資訊安全政策訂定與評估 (A.5)
  - 資訊安全組織 (A.6)
  - 資訊資產分類與管制 (A.7)
  - 人員安全管理與教育訓練 (A.8)
  - 實體與環境安全 (A.9)
  - 通訊與作業安全管理 (A.10)
  - 存取控制安全 (A.11)
  - 系統開發與維護之安全 (A.12)
  - 資訊安全事件之反應及處理 (A.13)
  - 業務永續運作管理 (A.14)
  - 相關法規與施行單位政策之符合性 (A.15)

資訊安全管理制度建置步驟

- ISMS之建立
  - 依據該單位之類型、規模、資源、業務性質等特性，定義ISMS 範圍；考慮相關法律、法規，以及合約之要求，於適度評估風險及應對措施後，訂出經由管理階層核准之ISMS政策，並擬定一份適用性聲明書文件。

- ISMS之實施與操作
  - 施行單位應確實實施控制措施，以符合控管的目標，並執行訓練與認知計畫，確保偵測安全事件的能力，以及迅速回應和應對處理的時效。

資訊安全管理制度建置步驟（續）

- ISMS之監控及審查
  - 施行單位應針對ISMS進行監控程序與其他控制措施，即時鑑別資安事件的發生、處理順序與解決方法；定期審查ISMS有效性（建議一學年至少一次），並將相關有顯著影響之活動與事件記錄下來。

- ISMS之維持及改進
  - 施行單位應定期實行改進活動，採取適當的矯正與預防措施，並得到管理階層之同意，並確保各項措施達到預期目標。

資訊安全管理系統建置需求

- 文件要求
  - 關於ISMS文件化（電子檔案或紙本），必須包含安全政策、安全目標、ISMS範圍、適用性聲明、資安事件紀錄，以及其他有助於提升ISMS成效之文件；上述之文件需接受保護與管制，並定期的審查及更新，確保文件之最新版本；任何過期文件需保留或銷毀，應予以適當的鑑別。

- 管理階層責任
  - 管理階層最為重要的是給予承諾及實際的支持，並適度的提供資源以助ISMS程序進行，必要時審查 ISMS 的控制措施與有效性；另外，確保於ISMS範圍內之員工具備足夠之能力及認知，並定期進行教育訓練。

資訊安全管理系統建置需求（續）

- 管理階層審查
  - 管理階層應在規劃期間內，審查該單位的ISMS與適用範圍，確保其持續的適用性、適切性及有效性；其中應審查包含變更需求與改進時機，並將其結果確實文件化。

- ISMS之改進
  - ISMS的改進是持續的，必須藉由各資安事件與審查結果，做出適度的反應與改進，持續系統之有效性；另外，對應的矯正措施以及防範未然的預防措施，亦須予以制定並文件化。

規範－附錄A控制目標與控制措施說明(1/3)

A.7

控制目標 ⟶ 資訊資產分類與管制

控制目標說明

施行單位內有多少資訊資產？其資訊安全等級與分類為何？為確保施行單位資產獲得適切的保護，明確的資產分類與保護層級，將有助於資產保管的執行效率，降低受危害的可能，勢必進行徹底財產清點與分類；由於財產記錄在各學校單位已有職掌單位，為避免工作重疊的浪費，可僅進行補充加強的部份，擴充既有的資訊資產清單，使其符合資安政策，降低可能的威脅及危險。

本章節主要的內容可參照下表：				ISO27001:2005(E)
A.7 資訊資產分類與管制				A.7
控制目標	A.7.1	資訊資產分類與責任分屬		A.7.1 A.7.2
	A.7.1.1	資訊資產目錄建立	應製作所有資訊資產之清冊，並定期維護、更新。	A.7.1.1 A.7.1.2

ISO/IEC 27001:2005版本編號

規範－附錄A控制目標與控制措施說明(2/3)

控制項 ⟶ (一) 資訊資產分類與責任分屬(A.7.1)

控制細項 ⟶ 1. 資訊資產目錄建立(A.7.1.1)

控制細項說明 ⟶ 應製作所有資訊資產之清冊，並定期維護、更新。

資訊資產之清冊應達到：

參考項 ⟶ (1) 建立一份資訊資產目錄，訂定該資產之項目、擁有者及安全等級分類等，並定期維護與更新其內容。

(2) 資訊資產參考項目如下：

參考細項 ⟶ a. 一般資產：資料庫及資料檔案、系統文件、使用者手冊、訓練教材、作業性及支援程序、業務永續運作計畫、預備作業計畫等。

規範－附錄A控制目標與控制措施說明(3/3)

指定本控制項適用之群組，
若未註明則兩個系統皆適用

(六) 網路安全管理 (A.10.6)—較適用於學術網路系統

1. 網路安全規劃與管理(A.10.6.1)

應實施網路控制措施，維護網路安全。

指定本控制項適用之群組

c. 利用公眾網路或無線網路傳送敏感性資料，應採取特別的安全保護措施，保護資料的完整性及機密性，並保護連線作業系統之可用性。(較適用於第一群)

d. 網路安全管理應考量：(較適用於第一群)

- 盡可能將電腦作業及網路作業責任分開。
- 建立管理遠端設備的責任及程序。
- 實施適當的記錄與監控。
- 密切協調電腦及網路管理作業，以便發揮網路系統最大的服務功能，確保其在跨單位的基礎架構上運作。

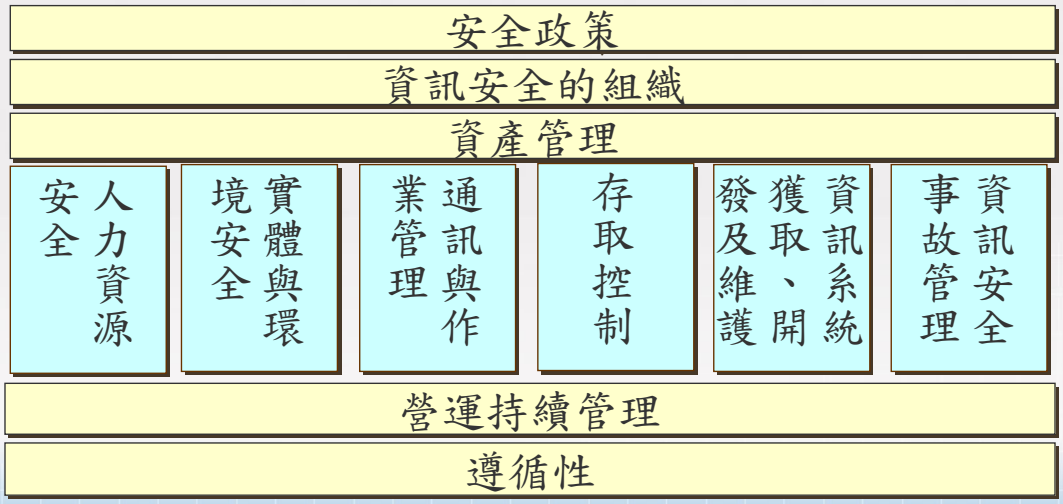
ISO 27001過去與現在

1995年發生了
什麼大事？

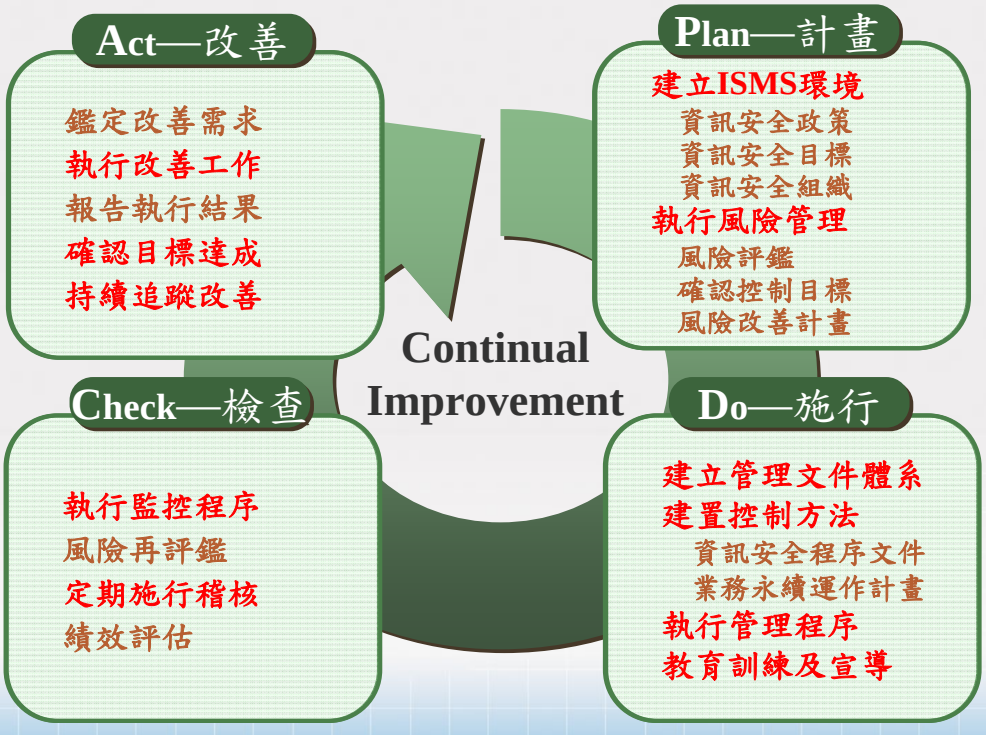
- **BS 7799標準更新之歷史：**
  - 1995: 英國公佈BS 7799 Part I
  - 1998: 英國公佈BS 7799 Part II
  - 1999: 英國公佈新版BS 7799 Part I、Part II
  - 2000: ISO通過成為ISO/IEC 17799 Part I
  - 2002: BS 7799:2-2002 -資訊安全管理系統驗證規範
  - 2005: ISO/IEC 17799:2005
  - **2005: ISO 27001 ISMS驗證標準**
  - **2007: ISO/IEC 17799作業規範，正名為ISO 27002**

ISO 27001涵蓋之內容

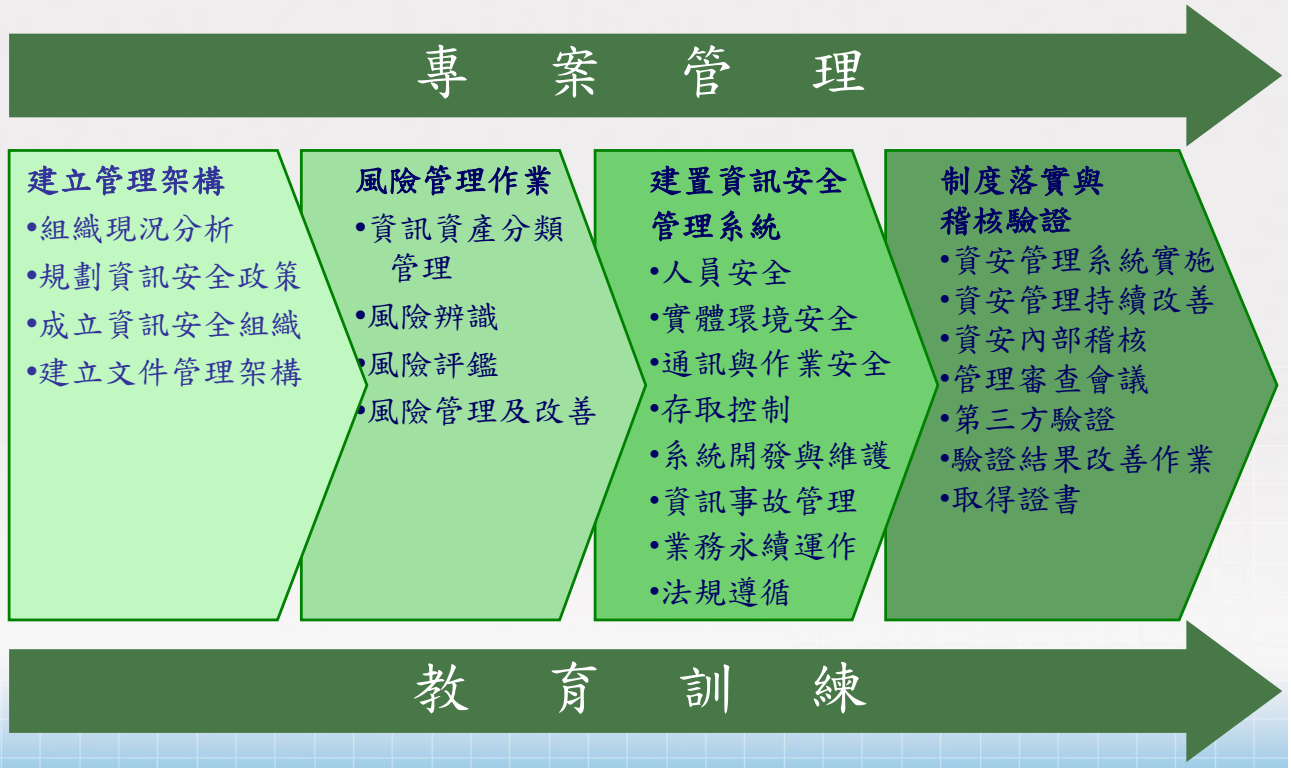
- 本文4~8章
- 11 個領域、 39 個控制目標、 133 個控制措施



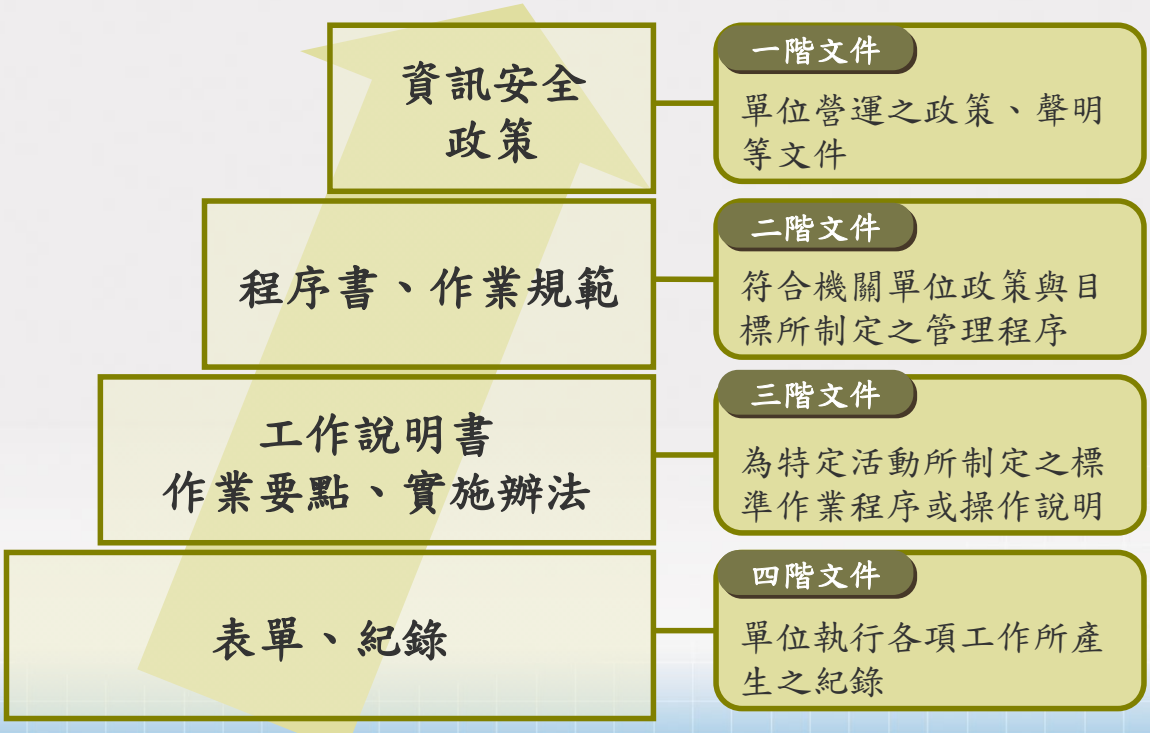
ISMS Lifecycle-PDCA模型之應用



ISMS導入流程



文件形式



稽核範圍

- ISMS之稽核範圍
  - 機房（或是電腦教室、設備室）及一套關鍵性校務行政系統（如學籍，選課或成績系統）
- 個資保護之稽核範圍
  - 業務相關單位：
    - 註冊組
    - 人事室
    - 健康中心

二、資訊資產鑑別、評價與管理

資產管理之目的

適切保護資訊資產→ 確保達成資訊安全之要求

資產管理角色

- Owner 權責單位：

  由組織指定的資訊資產擁有單位。

  註：Owner指的是負有被認可管理責任個體，負責資產的生產、發展、維護、使用及安全；並非對該資產有任何實質的財產權。

- Keeper 保管單位：

  由組織指定的資訊資產保管單位。

- User 使用單位：

  由組織授權的資訊資產使用單位。

資產類別(1/2)

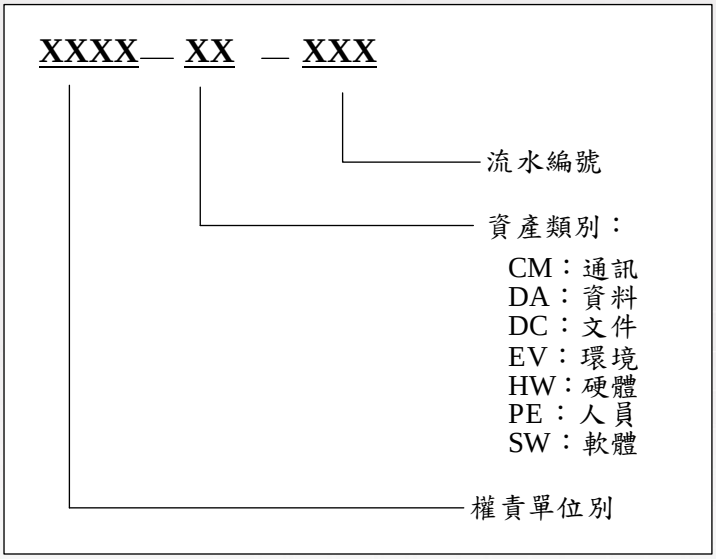
- 人員 (People)
  - 包含全體同仁，以及委外廠商。
- 文件 (Document)
  - 以紙本形式存在之文書資料、報表等相關資訊，包含公文、列印之報表、表單、計畫、合約等紙本文件。
- 軟體 (Software)
  - 作業系統、應用系統程式、套裝軟體等，包含原始程式碼、應用程式執行碼、資料庫等。

資產類別(2/2)

- 通訊 (Communication)
  - 網路設備、網路安全設備 、提供資訊傳輸、交換之線路或服務。
- 硬體 (Hardware)
  - 主機設備等相關硬體設施。
- 資料 (Data)
  - 儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊。
- 環境 (Environment)
  - 相關基礎設施及服務，包含辦公室實體、實體機房、電力、消防設施等。

資產編碼範例

- 除「文件」類之資訊資產外，資產編號之編碼方式，如右圖：
- 1~4碼為權責單位別
- 5~6碼為資產類別
- 7~9碼為資產流水編號



資訊資產編碼方式圖

資產群組化

- 群組的好處
  - 降低風險評鑑負擔，減少威脅、弱點的重複識別
- 群組做法
  - 先依據識別出之資訊資產進行分類，再從分類中群組化資產，以避免遺漏重要資產
  - 針對群組化之資訊資產進行風險評鑑
- 群組原則
  - 同性質之資產且數量大
  - 相同控管措施
  - 存在於相同的實體、邏輯環境
  - 資產價值相同
  - 遭遇弱點、威脅相同

群組化範例

Windows 作業系統

個人電腦

合約、系統文件

商用軟體

建立資訊資產清單

- 權責單位應清點及鑑別所管轄之資訊資產，建立「資訊資產清單」
- 權責單位應定期更新與維護所管轄之資訊資產清單
- 資訊資產清單由各權責單位提供，資安執行小組負責彙整，並陳報至資訊安全工作小組，以確保資訊資產編號及清單之完整性

資訊資產清單範例

文件編號：CAC-ISMS-D-009　　日期：99年11月18日

紀錄編號：IL1209902010001

資產編號	資產類別	資產名稱	資產說明	權責單位	保管單位	使用單位	機密性	完整性	可用性	資產價值
XXXX-CM-001	CM	Core Router & Switch	Cisco 6509 Router 1部	網路及資源組	網路及資源組	全校	2	3	4	4

資訊資產分級

- 以資產之C、I、A特性對組織之價值進行評估
- 設定評估等級標準採定性化、定量化法則，如：
  - 機密性 (C)：此資訊資產所包含資訊為組織或法律所規範的機密資訊 。
  - 完整性 (I)：資產具有完整性要求，且完整性被破壞會對組織造成傷害，甚至會造成業務終止。
  - 可用性 (A)：容許該資訊資產失效的時間長短。

資產價值鑑別(1/4)

- 權責單位應鑑別管轄內所有資訊資產之價值
- 資產價值鑑別方式除考量機密等級之外，尚需考量可用性及完整性，其評估標準如下：
  - 機密性評估標準（範例）

評估標準	數值
此資訊資產無特殊之機密性要求	1
此資訊資產僅供組織內部人員或被授權之單位及人員使用	2
此資訊資產僅供組織內部相關業務承辦人員及其主管，或被授權之單位及人員使用	3
此資訊資產所包含資訊為組織或法律所規範的機密資訊	4

資產價值鑑別(2/4)

- 完整性評估標準（範例）

評估標準	數值
該資訊資產本身完整性要求極低	1
該資訊資產本身具有完整性要求，當完整性遭受破壞時，不會對組織造成傷害	2
該資訊資產具有完整性要求，當完整性遭受破壞時會對組織造成傷害，但不至於太嚴重	3
該資訊資產具有完整性要求，當完整性遭受破壞時會對組織造成傷害，甚至造成業務終止	4

資產價值鑑別(3/4)

- 可用性評估標準（範例）

評估標準	數值
該資訊資產可容許失效3工作天以上	1
該資訊資產可容許失效8工作小時以上，3工作天以下	2
該資訊資產僅容許失效4工作小時以上，8工作小時以下	3
該資訊資產僅容許失效4工作小時以下	4

資產價值鑑別(4/4)

- 評估資訊資產之機密性、完整性及可用性後，取三者之**最大值**，為資訊資產之價值

資產價值 = MAX (C, I, A)

資訊資產清單

文件編號：CAC-ISMS-D-009　　日期：99年11月

紀錄編號：IL1209902010001

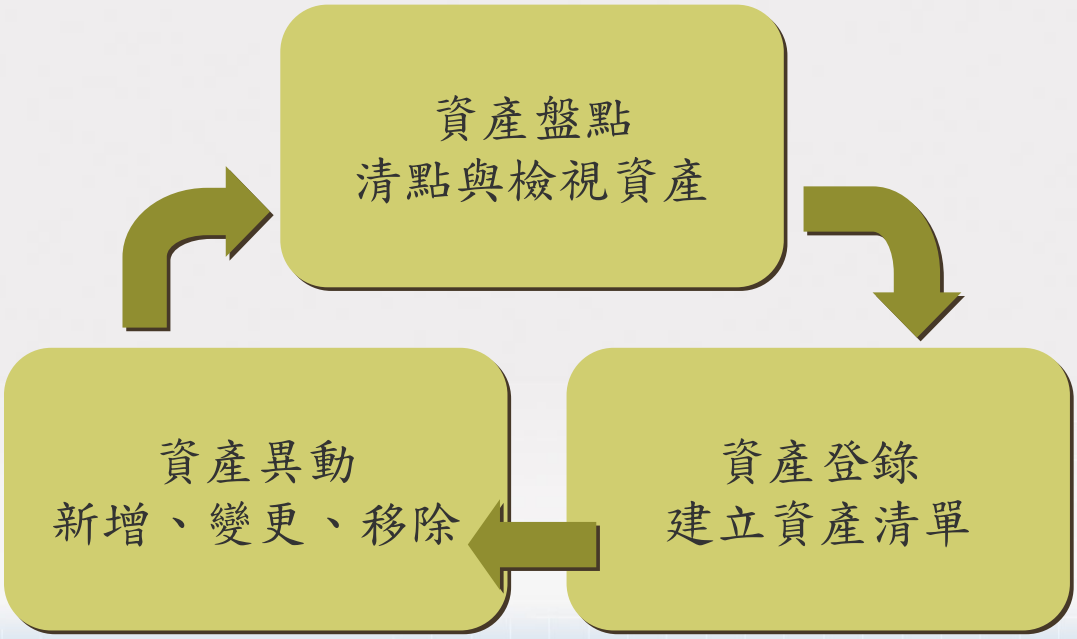
資產編號	資產類別	資產名稱	資產說明	權責單位	保管單位	使用單位	機密性	完整性	可用性
XXXX-CM-001	CM	Core Router & Switch	Cisco 6509 Router 1部	網路及資源組	網路及資源組	全校	2	3	4

資產價值
4

資產價值確認

- 資訊資產權責單位應依據資訊資產清單之機密性、完整性、可用性之評估標準，確認資產價值
- 資訊資產清單及價值評估結果，應陳報至資訊安全工作小組審議

資產管理



資產標示

- 機密等級分類的資訊資產及系統之輸出資料，應明確標示，避免其機密性遭破壞

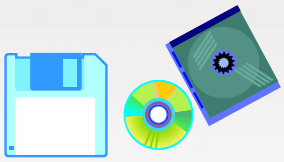
- 重要等級標示方式：
  - 不同顏色標籤區分，並註明資產編號與資產名稱
    - 資產價值2為綠色標籤
    - 資產價值3為黃色標籤
    - 資產價值4為紅色標籤

資產清單檢視

- 權責單位每年至少進行一次資產盤點與資產清單覆核，以更新及確保資產清單的正確性及完整性
- 當範圍內有以下的狀況發生之時，則實施不定期的覆核，以更新及確保資產清單的正確性及完整性
  - 有新增、變更或移除資訊資產；
  - 系統有重大異動；
  - 作業環境改變。

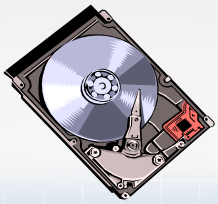
資產報廢

- 資訊資產之報廢（或銷毀）應依「資訊資產異動作業說明書」之相關規定，採取適當之方式進行銷毀

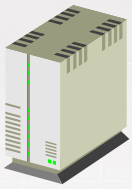


光碟、磁片

文件



磁碟、硬碟

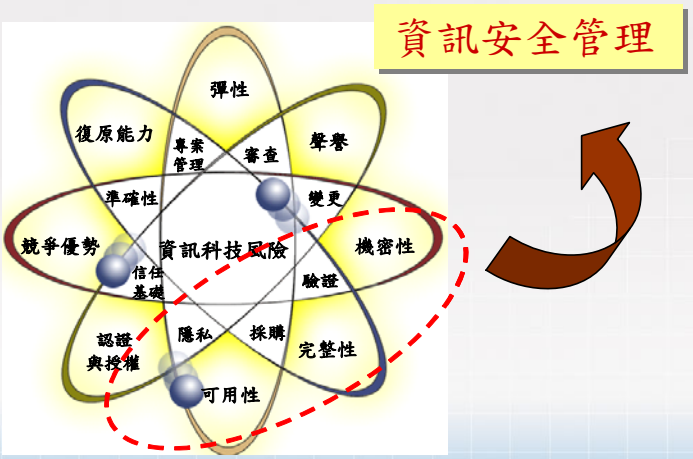


電腦設備

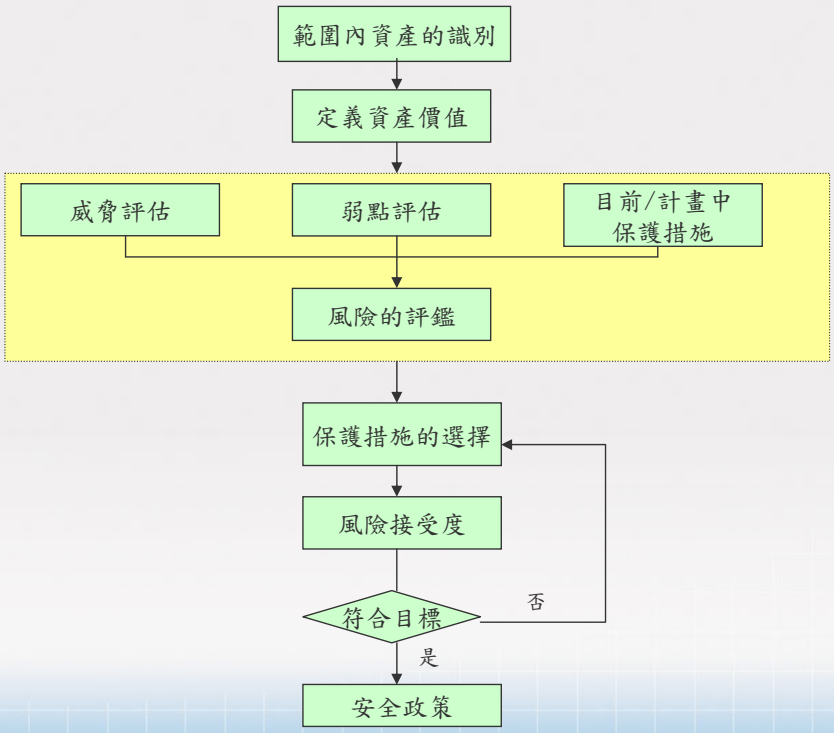
三、風險評鑑與管理

風險概述

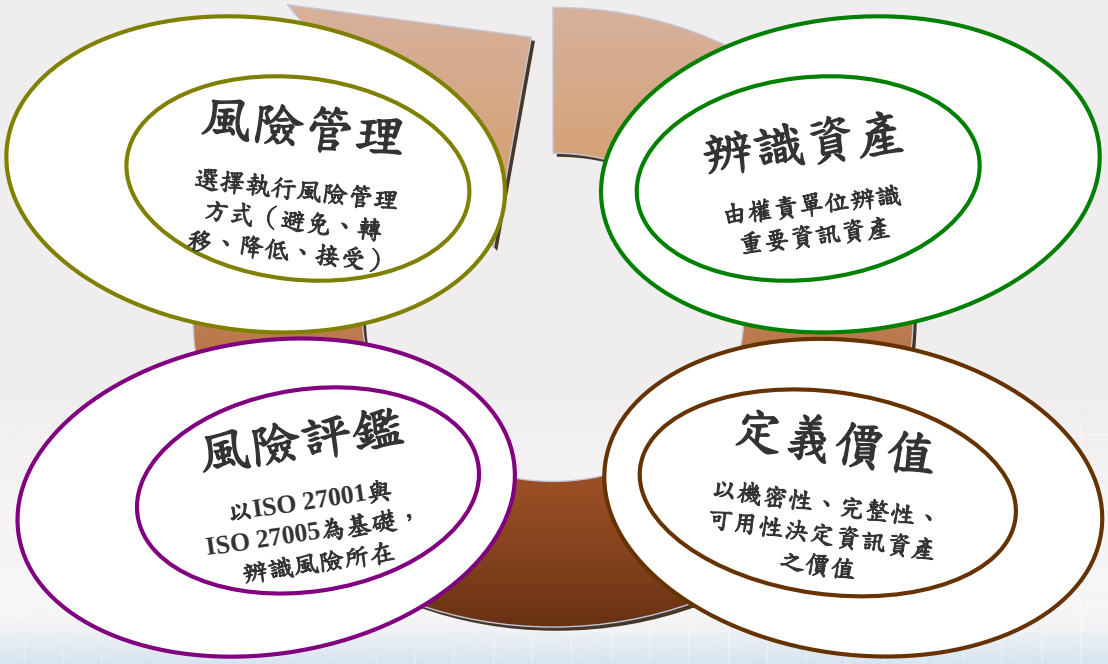
- 風險是具有破壞某種事物發生的可能性
- 風險管理是識別、評估風險，並將這種風險減小到一個可以接受的程度
  - 物理損壞
  - 人為錯誤
  - 設備故障
  - 內部和外部攻擊
  - 資訊誤用
  - 資料遺失
  - 應用程式出錯



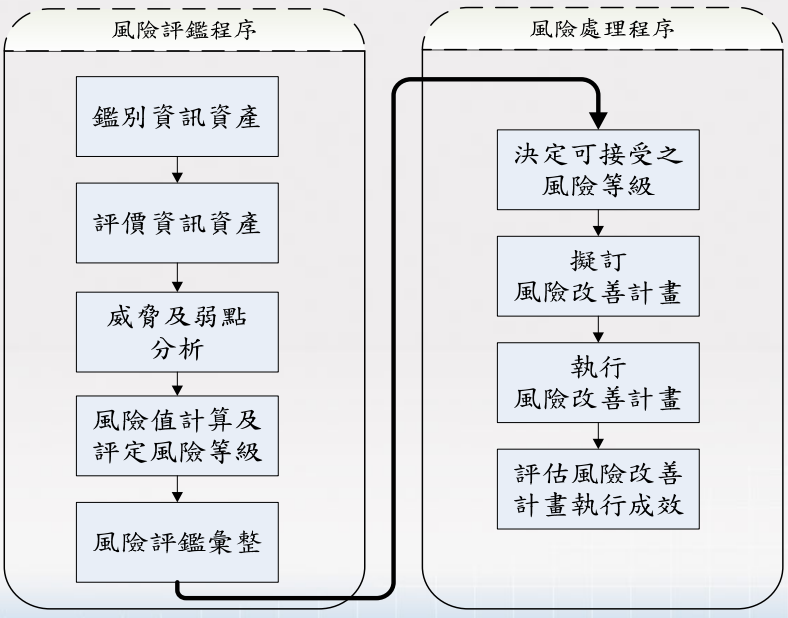
風險管理流程



風險管理循環



風險評鑑與風險處理

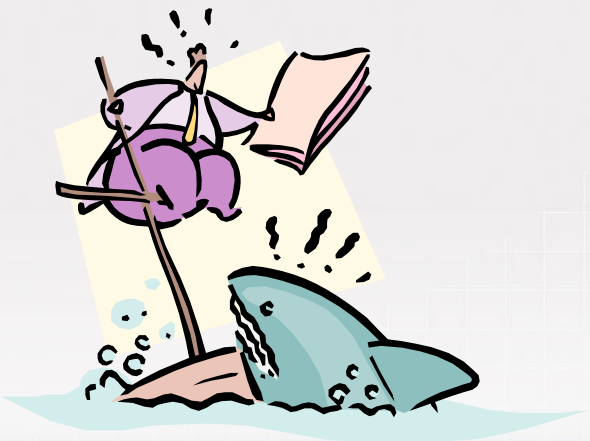


威脅

- 威脅為資產本身外來足以造成資產危害之狀況或事件
- 可分為意外的及蓄意的安全威脅
- 可能的安全威脅
  - **天然災害：颱風、地震、水災及停電等**
    - 地震可能威脅到資訊資產的可用性及完整性
  - **人為因素：非法存取資料、偷竊及竄改資料等**
    - 偷竊可能威脅到資訊資產的可用性及機密性

弱點

- 弱點存在於資產本身，若被威脅利用，可能會造成危害
- 可能的安全弱點
  - 作業上的安全弱點
  - 人員上的安全弱點
  - 科技上的安全弱點



風險公式

- 威脅利用弱點而對資產所造成傷害
- 風險 = f【資產價值，威脅等級（發生之可能性），弱點等級（受到威脅利用之容易度）】
- 威脅發生之可能性
- 受到威脅利用之容易度

威脅等級之評估

- 依以下標準評估各事件之威脅等級（發生之可能性）

威脅的等級對應表

評估標準	評估值
威脅發生之可能性為低	1
威脅發生之可能性為中	2
威脅發生之可能性為高	3

弱點等級之評估

- 依以下標準評估各事件之弱點等級（受到威脅利用之容易度）

弱點的等級對應表

評估標準	評估值
該弱點不容易被威脅利用	1
該弱點容易被威脅利用	2
該弱點非常容易被威脅利用	3

計算風險值

- 資產價值 = MAX (C, I, A)
  - 機密性、完整性、可用性，取最大值
- 風險之定義與評估
  - **風險值 =（資訊資產價值 x 威脅等級 x 弱點等級）**
- 風險值：1~36

風險權值對照表

	威脅等級（發生之可能性）	低(1)			中(2)			高(3)		
	弱點等級（受到威脅利用之容易度）	低(1)	中(2)	高(3)	低(1)	中(2)	高(3)	低(1)	中(2)	高(3)
資產價值	1	1	2	3	2	4	6	3	6	9
	2	2	4	6	4	8	12	6	12	18
	3	3	6	9	6	12	18	9	18	27
	4	4	8	12	8	16	24	12	24	36

風險管理原則與方法

管理原則

- 決定組織可接受之風險值
- 高於可接受風險值者，優先控管或處理

管理方法

- 避免(Avoid)
- 接受(Accept)
- 轉移(Transfer)
- 降低(Reduce)

ISMS實務與考量

實務

- 建立及執行風險改善計畫
- 建立適用性聲明書
- 執行風險再評鑑

考量

- 辨識資產和它們面臨的威脅
- 量化潛在威脅的影響
- 計算風險
- 在風險影響和處理對策費用之間取得預算上的平衡

風險評估範例(一)

威脅及弱點評估表						機密等級：□一般 ■限閱 □敏感 □機密						
文件編號：CAC-ISMS-D-010						版　　次：1.0						
紀錄編號：						填表日期：99年XX月XX日						
資產編號	資產類別	資產名稱	資產價值	威脅	弱點	威脅等級(發生之可能性)			弱點等級(受到威脅利用之容易度)			風險值
						低(1)	中(2)	高(3)	低(1)	中(2)	高(3)	
CAC-SW-001	SW	重要系統（軟體/應用程式）	4	軟體失效	不夠充的維護措施							0
				軟體失效	缺乏有效的變更控制措施							0
				軟體失效	缺乏監督與稽核機制							0
				軟體失效	未適當的執行軟體測試							0
				操作失誤	複雜的操作介面							0
				操作失誤	操作文件不足							0
				操作失誤	專業訓練不足							0
				操作失誤	不正確的參數設定							0
				誤用	存取權限授與不當或未定期審查							0
				誤用	缺乏監督與稽核機制							0
				誤用	文件或檔案未適當儲存							0
				冒用	通行碼管理不足							0
				冒用	離開工作站未進行「登出」作業							0
				冒用	識別與認證機制不足							0
				軟體竄改	未控管軟體下載或使用							0
				軟體竄改	缺乏備份							0
				不合法令的資料處理流程	不需要的服務被啟用							0
				惡意軟體攻擊	軟體漏洞							0

風險評估範例(二)

項次	資產編號	資產類別	資產名稱	資產說明	權責單位	資產價值	風險事件		風險值	風險再評鑑			
							威脅	弱點		資產價值	威脅等級	弱點等級	風險值
1	XXXX-CM-001	CM	Core Router & Switch	Foundry BigIron RX-16路由交換器 1部	網路管理組	4	線路損毀	連線電纜缺乏保護	24				
4	XXXX-CM-007	CM	網路安全設備	Firewall（Fortigate-800）1部、IDP(IBM ISS Proventia GX5108) 1部	網路管理組	4	硬體失效	缺乏硬體耗損控管	36				
7	XXXX-CM-007	CM	網路安全設備	Firewall（Fortigate-800）1部、IDP(IBM ISS Proventia GX5108) 1部	網路管理組	4	網路元件的失效	維護服務回應時間過長	36				
8	XXXX-DA-001	DA	重要系統資料	E-Mail、校務行政系統、人事系統、MeWork、LDAP、財產保管系統、宿網資料、個人網頁，論壇	電算中心	4	未經授權的使用者使用軟體	存取權限授與不當	16				
9	XXXX-DA-001	DA	重要系統資料	E-Mail、校務行政系統、人事系統、MeWork、LDAP、財產保管系統、宿網資料、個人網頁，論壇	電算中心	4	未經授權的使用者使用軟體	缺少密碼管理	16				
12	XXXX-DC-004	DC	機密文件	保密切結、人員資料表	電算中心	4	失竊	未保護儲存文件	24				
13	XXXX-DC-004	DC	機密文件	保密切結、人員資料表	電算中心	4	失竊	資料銷毀時的不注意	24				
14	XXXX-DC-004	DC	機密文件	保密切結、人員資料表	電算中心	4	洩密	未保護儲存文件	16				

Q & A