風險評鑑教育訓練

講師：劉志銘 資深顧問

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

1. 風險概論
2. 風險管理過程
3. 風險識別作業
4. 風險評鑑方法
5. 風險控管方式
6. 風險管理

課程大綱

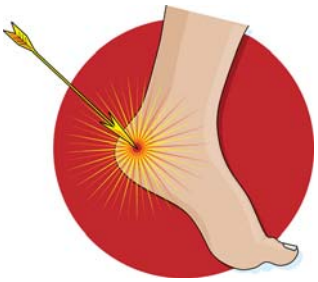
1. 風險概論
2. 風險管理過程
3. 風險識別作業
4. 風險評鑑方法
5. 風險控管方式
6. 風險管理

Enter your subtitle here

(圖片來源)
http://www.atrium-media.com

- 2004年5月，電影「特洛依：木馬屠城」
- 電影主角阿基里斯在希臘神話中是刀槍不入的勇猛戰士，堪稱無敵！

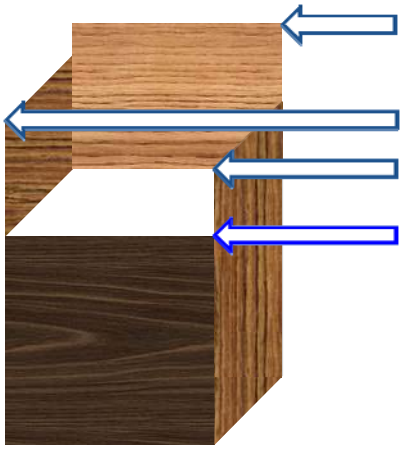
- 阿基里斯刀槍不入的全身，源於嬰兒時由母親倒抓其右腳踝浸泡冥河，所以只有沒浸泡到的右腳踝是其唯一弱點
- 所以縱使阿基里斯神勇無敵，在敵人一箭射中其右腳踝後，無敵神話仍舊破碎！



(圖片來源)
http://blogs.vembu.com

在資訊安全裡，我們說：
Security is a chain.
It's only as secure as the weakest link.

資訊安全的「木桶理論」



- 四塊長短不一的木板組成木桶，所能承盛的水量高度取決於最短的那塊木板
- 一個團體的整體素質水準不取決於最好的一位，而是取決於最差的那一名

- 組織建構了護城河 → 內部網路保護
  建起了高昂的城牆 → 各項安全防護
  建造了堅固的城門 → 防火牆
- 而您的輕忽，可能開啟防護漏洞...

(圖片來源)
http://www.japaneselifestyle.com.au

何謂：風險

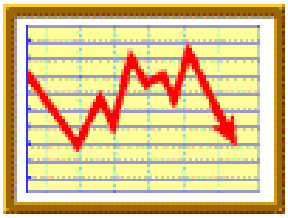
- 風險是具有破壞某種事物發生的可能性
- 風險管理是識別、評估風險，並將這種風險減小到一個可以接受的程度
  - 物理損壞
  - 人為錯誤
  - 設備故障
  - 內部和外部攻擊
  - 資訊誤用
  - 資料遺失
  - 應用程式出錯

為何需要風險管理

- 風險無所不在，藉由建立風險管理體系，在風險發生的第一時間搶得先機-降低損失或提早避免或預防
- 大部份組織面臨的最大風險??
  - 不清楚如何管理風險
  - 完全不知道有風險的存在
  - 清楚有風險，確不瞭解如何去管理與執行

風險管理的目的

- 讓組織選擇所能容忍的風險水準，並排除無法承擔的風險
  - 不在於100%避免風險
  - 並非追求最小的風險

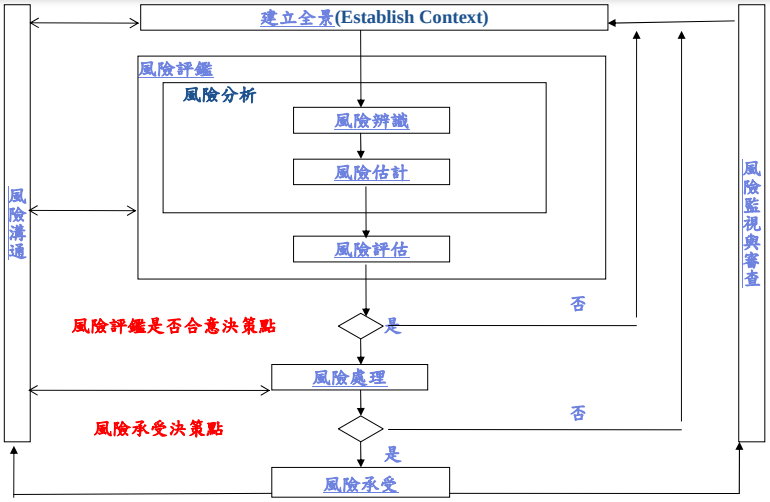


風險控制圖

課程大綱

1. 資訊風險概論
2. 風險管理過程
3. 風險識別作業
4. 風險評鑑方法
5. 風險控管方式
6. 風險管理

風險管理過程



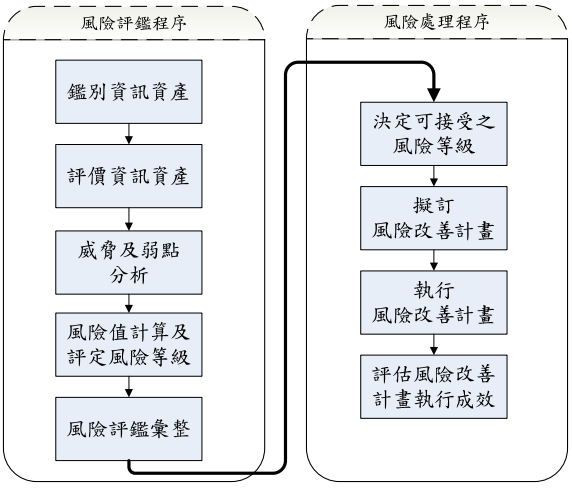
Source：ISO 27005

風險管理循環

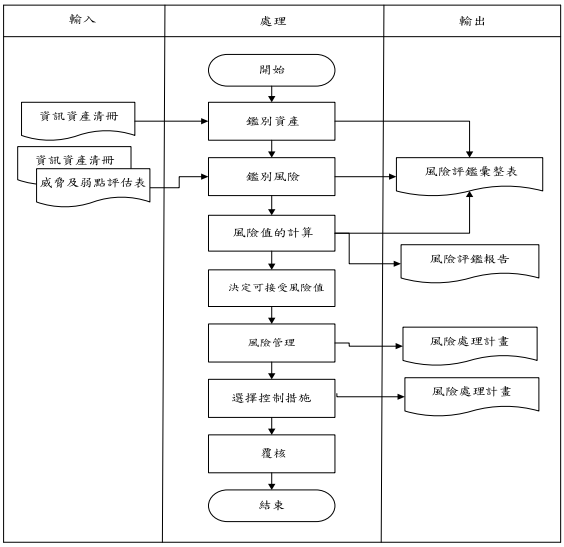
課程大綱

1. 風險概論
2. 風險管理過程
3. 風險識別作業
4. 風險評鑑方法
5. 風險控管方式
6. 風險管理

風險評鑑與處理程序



風險評鑑



安全威脅

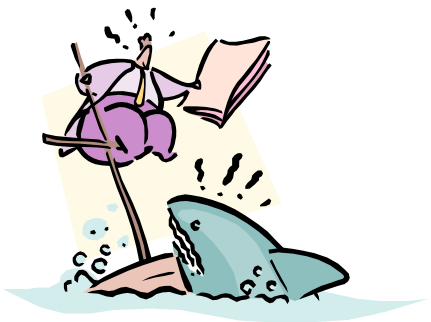
- 威脅為資產本身外來足以造成資產危害之狀況或事件
- 可分為意外的及蓄意的安全威脅
- 可能的安全威脅
  - **天然災害：颱風、地震、水災及停電等**
    - 地震可能威脅到資訊資產的可用性及完整性
  - **人為因素：非法存取資料、偷竊及竄改資料等**
    - 偷竊可能威脅到資訊資產的可用性及機密性

威脅評估

- What
  - 評估資產本身**脆弱點的嚴重程度**，亦即容易**被威脅所利用的程度**
- Why
  - 利用所評量之威脅發生機率計算資產風險值，作為後續評估每項資產之可接受風險值

安全弱點

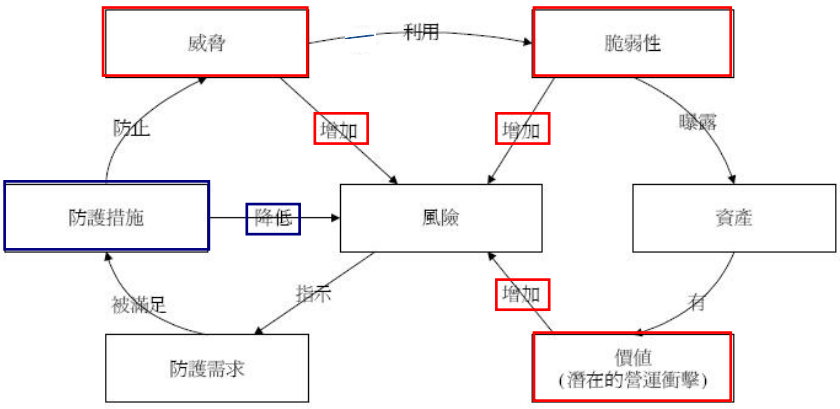
- 弱點存在於資產本身，若被威脅利用，可能會造成危害
- 可能的安全弱點
  - 作業上的安全弱點
  - 人員上的安全弱點
  - 科技上的安全弱點



弱點評估

- What
  - 評估資產本身**脆弱點的嚴重程度**，亦即容易**被威脅所利用的程度**
- Why
  - 依據判斷出之弱點及其脆弱度，評估每項資產之威脅。

風險管理示意圖



Source：ISO 13335

課程大綱

1. 風險概論
2. 風險管理過程
3. 風險識別作業
4. 風險評鑑方法
5. 風險控管方式
6. 風險管理

威脅、弱點、風險之間的關係

- 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

資產價值之評估

- 依**七大類**資產之**機密性**、**完整性**與**可用性**評估標準評估資產等級
- 設定評估標準等級採定性化、定量化法則
- 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

例：**人員類**資訊資產-可用性評估標準

評估標準	等級
■作業仰賴該員，若該員無法作業時，將影響**少數承辦人**作業。	1
■作業仰賴該員，若該員無法作業時，將影響**部門**作業。	2
■作業高度仰賴該員，若該員無法作業時，將影響組織內**跨部門**作業。	3
■作業完全仰賴該員，若該員無法作業時，將影響**全組織或對外**提供服務作業。	4

威脅等級之評估

- 依以下之標準評估各事件之威脅等級（發生之可能性及造成的衝擊）

評估標準	等級	評估值
每年發生一次之可能性	低	1
每季發生一次之可能性	中	2
每月發生一次之可能性	高	3

弱點等級之評估

- 依以下之標準評估各事件之弱點等級（受到威脅利用之容易度）

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

風險值的計算

- 資產價值=MAX (C, I, A)
  - 機密性、完整性、可用性，取最大值

資訊資產清冊

文件編號：ISMS-S-D-010　　日期：99年XX

紀錄編號：097-001

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
ISMS-HW-00	HW	IBM主機	IBM主機	資料組	資料組	資料組	1	1	4	4

- 風險之定義與評估
  - **資產價值×威脅等級×弱點等級**
- 風險值：1~36

風險評鑑原則

- 評鑑人員
  - 資訊資產權責單位(Owner)
- 風險評鑑主要執行步驟
  - 資訊資產價值(C、I、A)
  - 資訊資產弱點評估
  - 資訊資產威脅評估
  - 風險值計算
  - 風險值檢查

風險評鑑作法

- Input：資訊資產清冊
- 作法：
  - 資訊資產可群組→修正資產清冊(資產說明欄位)
    - 威脅與弱點評估表→檢視威脅與弱點值
  - 資訊資產不可群組→新增於資產清冊
    - 新增展開威脅與弱點評估表→威脅與弱點評估→系統自動進行風險值計算

弱點等級之評估

- 依以下之標準評估各事件之弱點等級（受到威脅利用之容易度）

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

風險值的計算

- 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

事件風險權值對照表

	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

資訊資產風險值檢查、確認

- 組織重要資產是否有被凸顯
- 流程重要資產是否有被凸顯
- 機密性極高是否有被凸顯
- 完整性極高是否有被凸顯
- 可用性極高是否有被凸顯
- 風險值極高
- 風險值極低

是否合理、可以解釋？

風險評鑑弱點與威脅的資訊來源

- 資訊資產的威脅及弱點可由下列項目得知：
  - ISMS管理紀錄(如異常狀況處理紀錄表、資訊安全事件報告單、弱掃結果報告、電腦機房出入登記表、硬軟體設備故障維護記錄表、電腦機房操作人員值班日誌、設備維護紀錄、源碼檢測結果、系統測試報告、營運持續計畫演練結果或其他相關表單報告等)
  - 內外稽及有效性量測及安全查核的結果
  - 觀察工作流程
  - 與資訊資產權責單位(Owner)或保管單位(Keeper)訪談
  - 外部資安事件的經驗

實務－確認風險評估結果

- 經完成鑑別資產及其相關風險後，產出「風險評估彙整表」 。
- 運用該表彙整之相關綜合風險值，產出風險評鑑報告。
- 該報告供組織作風險管理之依據。

課程大綱

1. 風險概論
2. 風險管理過程
3. 風險識別作業
4. 風險評鑑方法
5. 風險控管方式
6. 風險管理

風險控管原則

- 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

風險控管方法

- 選擇風險控管方式
  - 避免
  - 轉移
  - 降低
  - 接受
- 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

風險管理

- 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

委外風險管理考量?

- 委外廠商的管理。
  - 委外廠商素質?技術能力?
  - 委外廠商工作環境?
  - 委外廠商負責之業務是否為營運核心?
- 委外風險應變管理。
  - 當委外廠商退場後，您可不可以一肩扛起?
  - 委外廠商倒了，開發的應用程式怎麼辦?
- 制度落實為降低風險的不二法門。
  - 單位已制訂哪些委外廠商管要求?
  - 是否將已外廠商納入風險評估考量?

委外事件討論

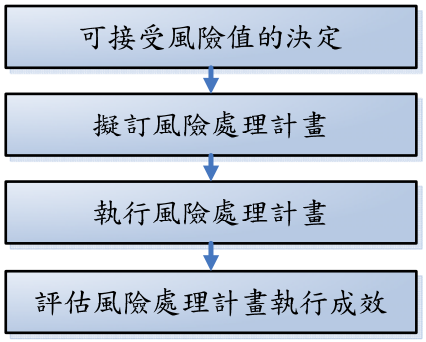
- 移民署36小時當機談委外管理?您怎麼思考?
  - 委外廠商素質?技術能力?
  - 委外廠商工作環境?
  - 委外廠商負責之業務是否為營運核心?
  - 當委外廠商退場後，您可不可以一肩扛起?
  - 委外廠商倒了，開發的應用程式怎麼辦?

課程大綱

1. 風險概論
2. 風險管理過程
3. 風險識別作業
4. 風險評鑑方法
5. 風險控管方式
6. 風險管理

風險管理–風險處理程序

風險處理(Risk Treatment) - 選擇與實施各項控制措施，以降低風險影響程度



各單位可接受風險等級

風險控管原則

- 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

實務－風險接受度

- ISO27005
  - 風險接受度應該用組織可接受或不可接受來分類。
  - 不可接受的風險乃經再三考量可能不被容許存在的。
  - 管理者要決定是否因為不願花費額外且昂貴的保護措施來降低不可接受的風險，進而選擇接受這些風險。

實務－可接受風險值

- 依據：CNS/ISO27001本文4.2.1(c)(2)，發展風險接受準則，並識別風險可接受等級。
- 實務作法：
  - 資訊資產之可接受風險值，需經**管理審查會議決議**，並記載於會議紀錄中。
- 管理審查會議須定期召開會議，並檢視／討論可接受風險值。
- 可接受風險值得考量組織環境及作業之安全需求作適當調整。

風險管理作業

- 確認、控制及降低安全風險至可接受程度所採取的程序
- 管理作業
  - 訂定風險接受等級
  - 檢討資產威脅及弱點
  - 檢討目前使用之控制措施
  - 加強其他控制措施
  - 訂定相關安全政策及作業程序

選擇控制措施

- 考慮因素
  - 安全風險所造成之影響
  - 需要的風險接受等級
  - 所需費用是否合理
  - 是否容易執行
  - 需花費多少時間
  - 與現有環境及技術之整合是否可行
  - 符合法令規定
  - 相關契約規定

控制風險策略說明

- 規避風險
  - 修改資訊作業方式或採用技術以避開風險。
  - 經由政策或標準以禁止從事高風險交易或活動。
- 轉移風險
  - 轉移相關之營運風險至他者，例如：承保商、供應商。
- 接受風險
  - 符合組織的政策與風險接受準則，則知悉且客觀地接受風險。
- 降低風險
  - 參考標準選擇適當之控制措施以降低風險。
  - 藉由加強各項作業之內控以降低風險發生之機會。

控制措施說明

- 預防性控制
  - 藉由「事前」的控制，形成一道屏障來防止特別交易的不當進行或阻止錯誤的發生。例如：承保前之風險評估、對銷貨客戶之徵信、使用經核准之供應商名單
- 偵查性控制
  - 利用某些程序來偵測已發生之錯誤或不當交易。例如：編製銀行調節表、存貨盤點、與銷貨客戶之定期對帳
- 矯正性控制
  - 用來矯正偵查性控制所發現之問題或矯正交易之控制。例如：透過電腦對採購單之檢核可以偵測到未經核准之供應商號碼，進而追蹤其原因及時修正交易資料或防止向不適當供應商之採購
- 補償性控制
  - 用來補償其他控制之不足，使得某些控制弱點不成為問題。例如：未有足夠之人力執行職能分工時，可透過由客戶或管理階層親自監督來彌補此一控制弱點。

控制措施的選擇考量

- 時效性
  - 控制執行時間及有效期限為何
- 人力
  - 每年需要多少工時來監控和維護
  - 負責執行、監控及維護控制的人員需要接受多少訓練
  - 必須容易執行，了解對使用者造成多少程度不便
- 成本
  - 是否有預算執行這項控制措施
  - 控制的費用相對於資產價值而言合理嗎(成本)
  - 控制成本<資產價值<威脅損失
- 法規或合約要求

風險處理

- 依據資訊資產風險評鑑的結果，對於超出組織風險值可接受程度之風險，進行處理
- 目的：降低風險發生機率及風險發生時產生之損害
- 工具：風險處理計畫

使用表單:風險處理計畫表

風險改善計畫表

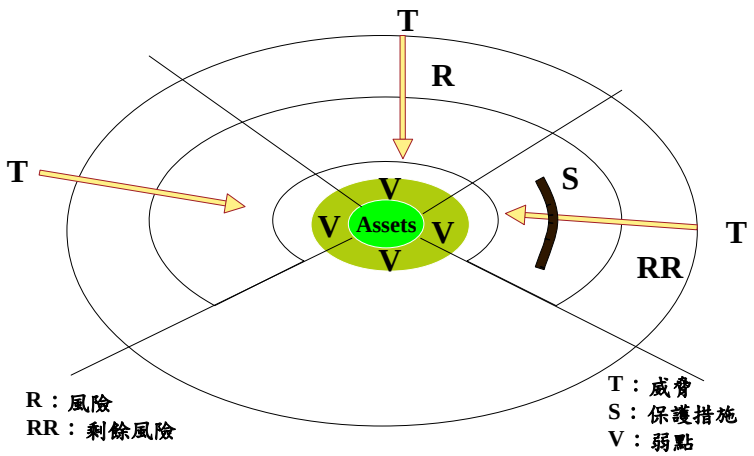
機密等級：□一般 ■限閱 □敏感 □機密

文件編號：ISMS-CC-ISMS-D-012
紀錄編號：99-001

版　　次：1.0
填表日期：XX年XX月XX日

教育體系資通安全管理規範或ISO 27001控制目標	現況說明	風險改善建議措施	教育體系資通安全管理規範或ISO 27001條文	建議權責單位	預計改善時間與處理方式	與高風險資產之風險評估彙整表對照
備份-資訊備份	XXX非同步教學平台缺乏資料(資料,程式與文件)備份	1.依據本中心通信與作業管理程序辦理，並落實備份管控措施 2.新架構採用NAS作每日備份	A10.5.1	電算中心	2010/1/31前完成	1
備份-資訊備份	XXX非同步教學平台儲存媒體維護不足/安裝瑕疵	1.依據本中心通信與作業管理程序辦理，並落實備份及設備維護管控措施 2.新架構採用NAS作每日備份	A10.5.1	電算中心	2010/1/31前完成	2
備份-資訊備份	XX系統資料缺乏資料(資料,程式與文件)備份	1.依據本中心通信與作業管理程序辦理，並落實備份管控措施 2.每日定期備份	A10.5.1	電算中心	2010/1/31前完成	10
備份-資訊備份	XX系統資料儲存媒體維護不足/安裝瑕疵	1.依據本中心通信與作業管理程序辦理，並落實備份及設備維護管控措施 2.每日定期備份	A10.5.1	電算中心	2010/1/31前完成	11

殘餘風險的概念



風險處理後

- 建立評量指標
  - 審視控制措施之有效性
  - 以評量指標作為績效參考依據
- 評估處理計畫之適切性
  - 人員指派是否適切？
  - 所需資源、時間是否合理？
  - 督導人員是否確實監督？
- 追蹤成本控制
  - 費用預估是否正確？未來須如何調整？
  - 相對於資產價值，控制的總成本是否於預算內？
  - 營業收入是否因風險改善後提升 (遠期效益) ？