資訊安全風險管理介紹

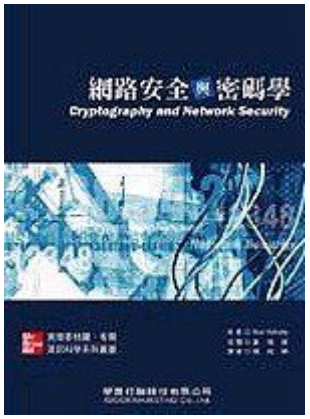
查士朝 Ph.D.

台灣科技大學資管系助理教授

1. 資訊安全風險管理的基本觀念
2. 常見的資安事件
3. 常見的風險識別方式
4. 風險的評估方式
5. 風險評鑑方法設計上常見的問題
6. 資訊安全風險管理比較框架
7. 學習地圖

1 資訊安全風險的基本觀念

- P 6-34 表 6.4 SSL vs. SET



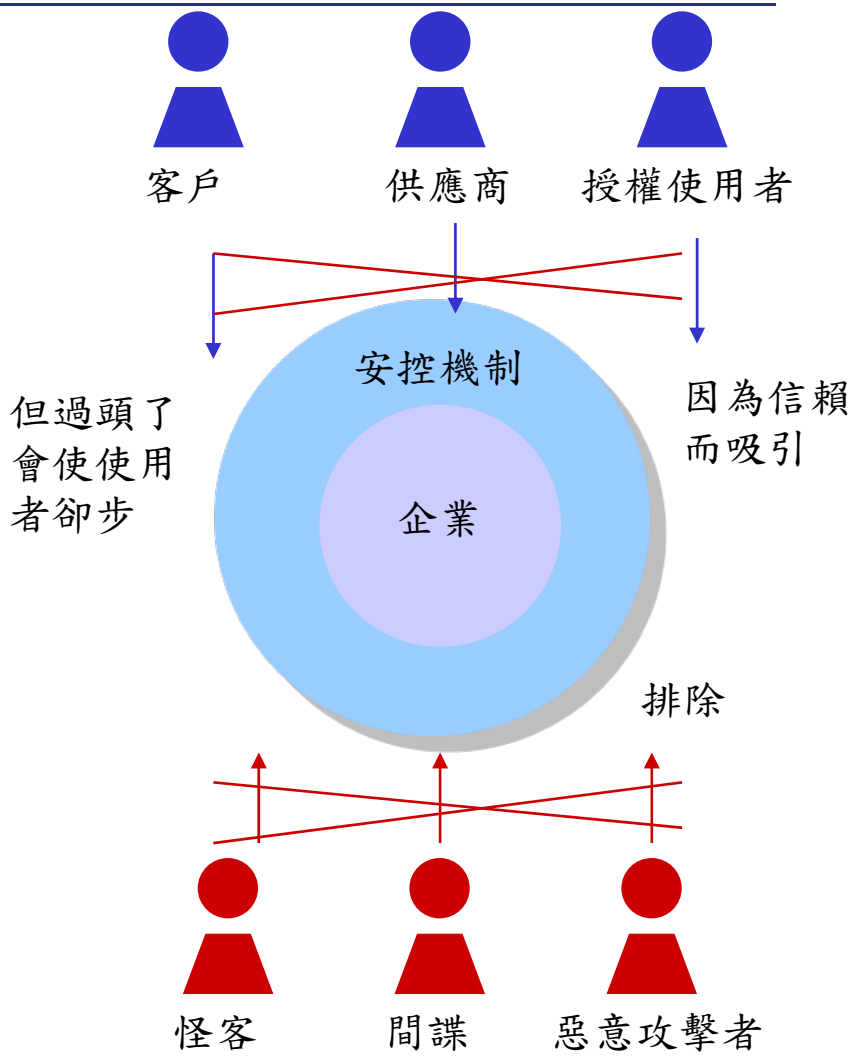
	SSL	SET
……		
實用性	高	目前尚低，預期將成長

安全與便利的拔河


花蓮縣稅捐稽徵處資訊服務網 2005 - Windows Internet Explorer
http://www.hltb.gov.tw/cht/rso_newsflash/detail.aspx?&pointid=401
花蓮縣稅捐稽徵處資訊服務網 2005
契 稅 地價稅 印花稅 房屋稅 娛樂稅 使用牌照稅 土地增值稅
花蓮縣地方稅務局 資訊網站
Local Tax Bureau,Hualien County
搜尋花蓮縣地方稅務局網站
輸入關鍵字
Go
線上申辦 預約服務 書 表 身心障礙服務
機關簡介 最新消息 招標徵才 查詢事項 繳稅專區 服務中心 交流園地 公開資訊 網路芳鄰 員工園地 會員專區 網站地圖 回到首頁
最新消息
HotNews
稅務新聞 what's news
電子錢包繳稅作業將於96年5月底停用，請納稅義務人儘速換發晶片金融卡繳納稅款
花蓮縣稅捐稽徵處表示：台灣網路認證股份有限公司將於95年5月底停止電子錢包憑證簽發，因已簽發之憑證有效期限為1年，所以，該公司將於96年5月全面停止SET憑證認證及維運服務，屆時納稅義務人不能再使用電子錢包憑證進行繳納稅款。
該處同時表示：財金資訊股份有限公司為因應上述情事，已將原先由網際網路電子錢包SET憑證繳稅作業，改由晶片金融卡網路繳稅作業取代，請納稅義務人儘速換發晶片金融卡，以利繳納稅款。
[返回上頁]
稅務新聞
活動訊息
榮譽榜
有獎徵答
地方稅宣導手冊
機關通訊 局長信箱 民意信箱 廉政信箱 隱私權及著作權申明 資訊安全政策
完成
網際網路 | 受保護模式: 啟動
100%

由風險為出發點的思維

- 為何要以風險為出發點：
  - 資安的吸引與排除效果，如果太過可能反而會造成反效果
  - 經濟效益考量
    - 資安不太會對整個生產過程產生加值，但通常需要投入許多額外的資源。
    - 如果不管控，等到發生事情又可能會造成巨大損失
- 透過從風險的角度來思考，可決定到底該要採用什麼樣的資安措施，並把錢花在刀口上。

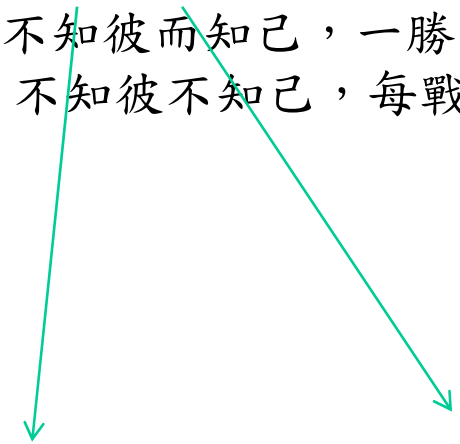


風險管理在做些什麼？

- 風險管理程序是要透過一套有系統的方法，來達到以下的目的：
  - 管控或降低資訊安全意外事件所可能造成的損失：風險管理要能夠辨識出可能發生的意外事件或風險，並採取適當回應，以使得可能的損失被控管在一個可接受的範圍內。
  - 提升資訊安全措施的成本效益：風險管理的方法要能夠協助企業或組織，在需要控管某項風險時，能夠找到最有成本效益的措施來進行控管。
  - 滿足法規或是利害關係人 (如客戶與消費者團體) 的相關要求。

風險管理的起源：孫子兵法謀攻篇

故曰：知己知彼，百戰不貽；
不知彼而知己，一勝一負；
不知彼不知己，每戰必貽。

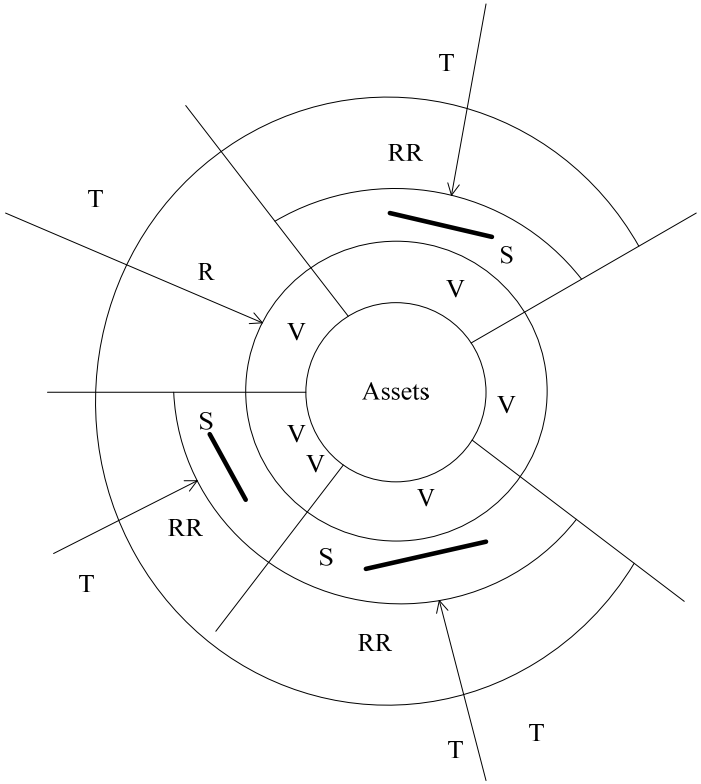


了解本身的弱點

了解可能遭遇的威脅

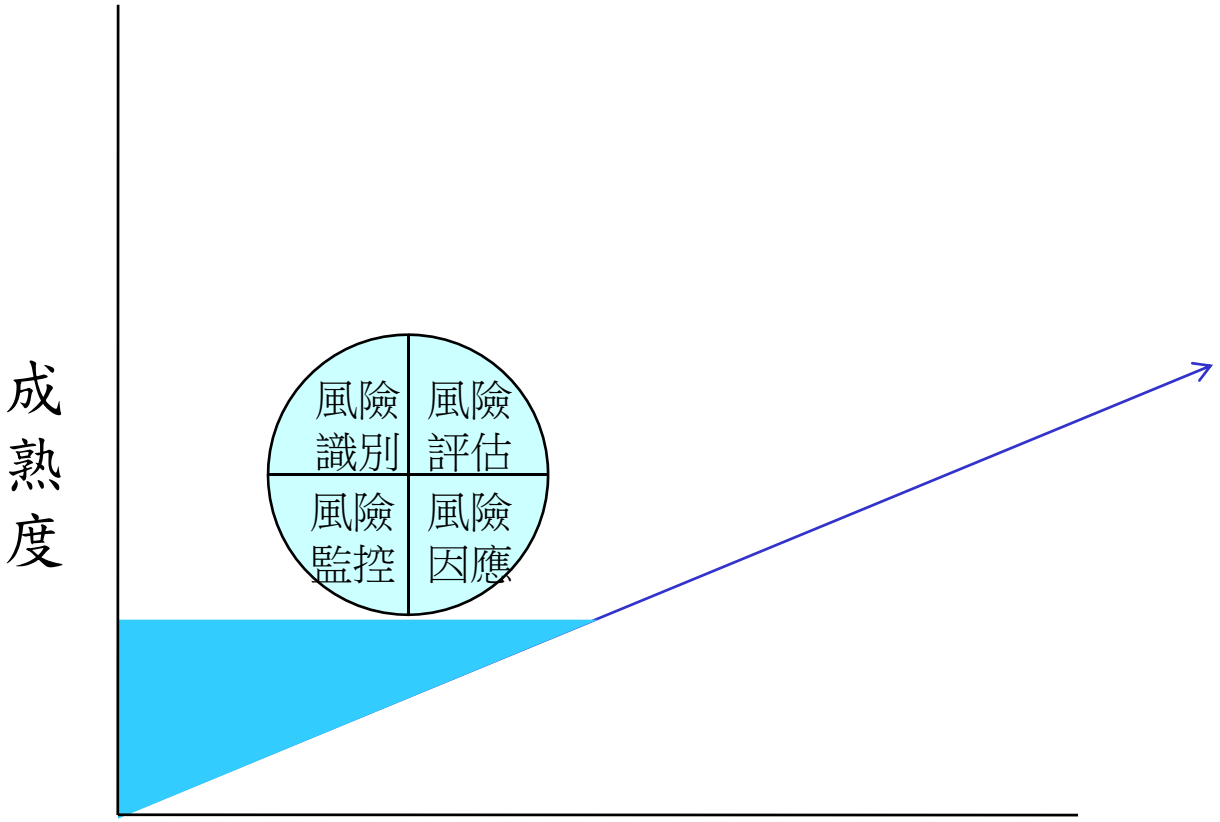
風險管理在資安上的概念

- 風險管理了解到威脅 (T) 利用到弱點 (V) 所可能造成意外事件的損失 (R)。而採取適當的控制措施 (S)，使得殘存風險 (RR)，是可被企業接受的。

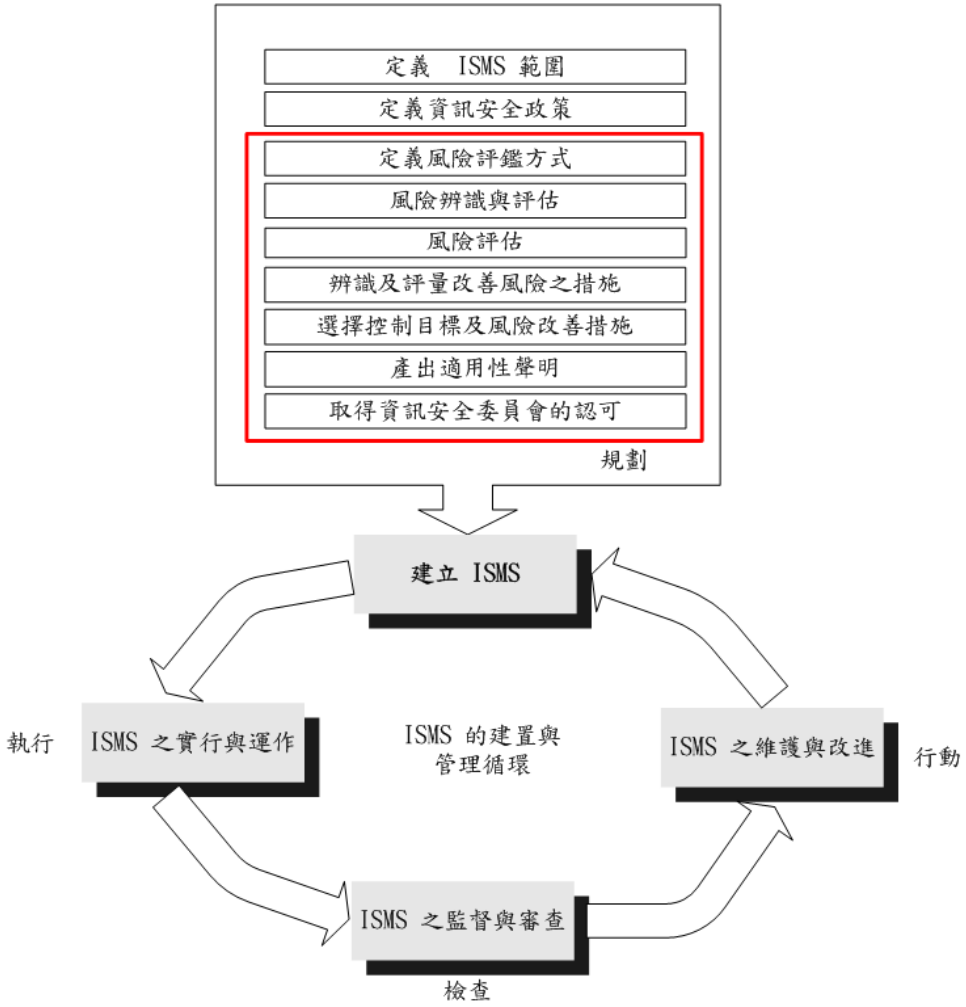


Source: ISO 13335-1

風險管理的主要程序



風險管理與 ISO 27001



Source: ISO 27001

2 常見的資安事件

常見的資安意外事件來源

類別	威脅
災難事件 Catastrophic incident	火災 Fire 水災Flood 地震Earthquake 暴風 Severe storm 恐怖攻擊 Terrorist attack 暴動 Civil unrest/riots 山崩 Landslide 雪崩 Avalanche 產業面影響 Industrial accident
機械故障 Mechanical failure	缺乏電源 Power outage 機械固障 Mechanical failure 應體失效 Hardware failure 網路中斷 Network outage 環境控制失效 Environmental controls failure 建築物意外Construction accident

類別	威脅
非故意 Non-malicious person	未被通知的員工 Uninformed employee 未被通知的使用者 Uninformed user 疏乎的員工 Negligent employee
人為惡意攻擊 Malicious person	駭客 Hacker, cracker 電腦犯罪 Computer criminal 產業間諜 Industrial espionage 社交工程 Social engineering 不滿的現任或離職員工 Disgruntled current or former employee 恐怖份子 Terrorist

Source: NIST 800-30

CSI 調查中的資訊安全威脅

事件	金額	比率
財務舞弊 (Financial Fraud)	$21,124,750	12%
病毒 (Virus)	$8,391,800	52%
資訊系統被外部滲透 (System penetration by outsider)	$6,875,000	13%
資料被竊取 (除了行動設備失竊外) (Theft of confidential data)	$5,685,000	17%
筆電或行動裝置遭竊 (Laptop or mobile hardware theft)	$3,881,150	50%
內部員工對網路的濫用 (Insider abuse of net access)	$2,889,700	59%
服務阻斷攻擊 (Denial of Service)	$2,888,600	25%
網路釣魚 (Phishing)	$2,752,000	26%
殭屍病毒 (Bot)	$2,869,600	21%

Source: CSI Security Survey 2007

CVE Top 10 2001~2006

- XSS
- Buffer overrun
- SQL Injection
- Php-include: PHP remote file inclusion
- Dot: Directory traversal
- Infoleak: Information leak by a product
- DoS-malform: DoS caused by malformed input
- Link: Memory leak (doesn't free memory when it should)
- Format String: Format string vulnerability; user can inject format specifies during string processing.
- Crypt: Cryptographic error (poor design or implementation), including plaintext storage/transmission of sensitive information.

Source: http://cwe.mitre.org/documents/vuln-trends/vuln-trends.pdf

OWASP (Open Web Application Security Project) Top 10 2007

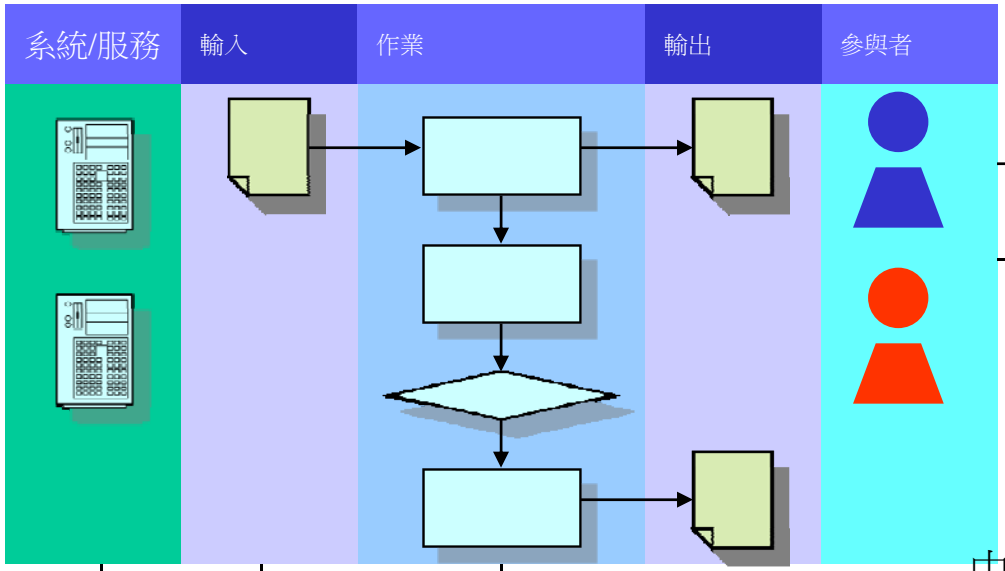
- No 1. Cross-Site Scripting (XSS)
- No 2. Injection Flaws
- No 3. Malicious File Execution
- No 4. Insecure Direct Object Reference
- No 5. Cross Site Request Forgery (CSRF)
- No 6. Information Leakage and Improper Error Handling
- No 7. Broken Authentication and Session Management
- No 8. Insecure Cryptographic Storage
- No 9. Insecure Communications
- No10. Failure to Restrict URL Access

3 常見的風險識別方式

風險識別方式

- Misuse Case
- FTA 法
- 資產導向

資產導向方法：流程訪談與資訊資產的辨識



人員權責

識別相關
負責人與
使用者

由流程進
行效正

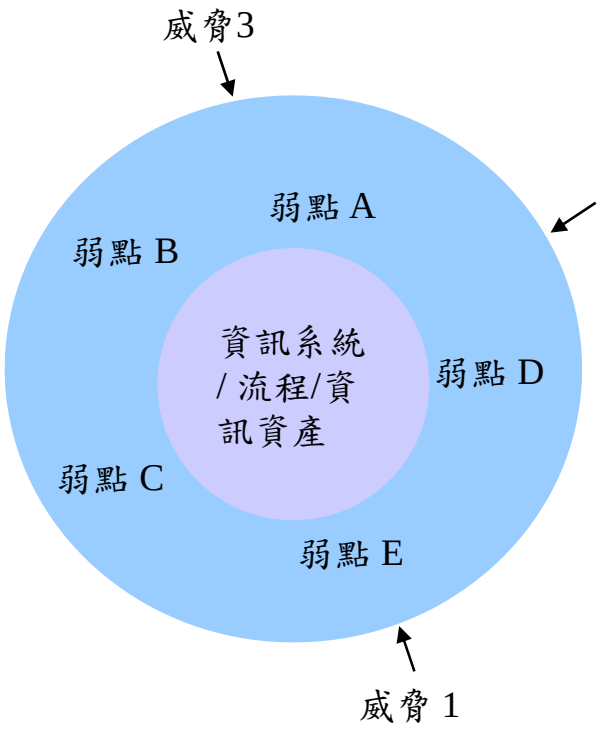
辨識資
料/文
件資產

編號	種類	說明	價值	負責人	使用者

就資產本身
評估重要性
或價值

辨識系統/服務，
以及其所需元件

資產導向方法：風險的評估



資產			價值		
可能風險	威脅	弱點	機率	影響	風險值

由資產去找出可能的資安事件

評估發生的機率

參考資產價值，評估發生資安事件後的影響

計算風險值

4 風險的評估方式

標竿法與非正式法

- 基準法：不進行詳細的風險分析，而以市面上的 Best Practice 或其它標準為基準。而以和 Best Practice 的差異為風險。
  - Baseline vs. Best Practice
- 非正式法：群體共同討論，決定可能遭遇的資安事件，發生的機率，以及可能造成的衝擊等，並共同決定風險

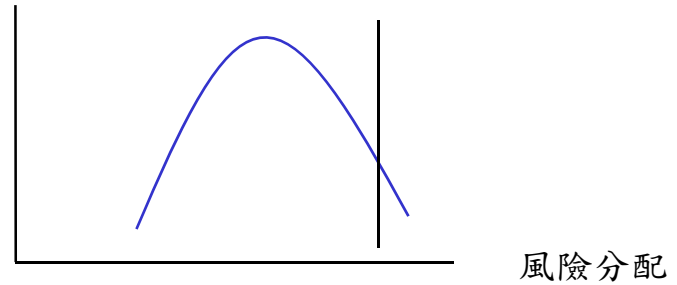
評鍵項目	目前狀況	說明
資安政策		
資安組織		
實體安全		未實行桌面及螢幕淨空

正式法的資安風險評量 (定量法)

– 定量風險評估方法：採用數量化的分析方式，去計算可能的損失。

Concept	Derivation Formula
曝險因子 Exposure Factor (EF)	威脅發生造成資產受損的比率
單一損失期望值 Single Loss Expectancy (SLE)	資產價值 x 曝險因子 (EF).
平均年發生率 Annualized Rate of Occurrence (ARO)	每年發生的頻率
年期望損失 Annualized Loss Expectancy (ALE)	單一損失期望值 (SLE) x平均年發生率 (ARO)

資安事件	預期風險
天然災害	
人為疏失	



正式法的資安風險評量 (定性法)

- 主要是針對可能發生的資安事件，進行細部的分析。又可以分為定性法和定量法：
  - 定性風險評估方法：利用質化的類別，來對風險進行評估。

威脅		大			中			小		
弱點		大	中	小	大	中	小	大	中	小
重要性	高	高	高	高	高	高	中	高	中	低
	中	高	高	中	高	中	中	中	中	低
	低	高	中	低	中	中	中	中	中	低

資訊資產	價值	風險
A	高	高
B	中	
C	低	

資安事件	威脅發生率	弱點易被利用率	資產重要性	風險
火災	高	中	高	高

比較

	定性法	定量法
優點	●計算較簡單	●算出來之結果比較容易做跨領域比較
缺點	●計算出來的結果可能沒有數學上的意義	●計算較複雜

混合法

- 混合法：同時採用上述方法，例如：
  - 首先用非正式法決定哪些部份特別重要
  - 重要的部份採用正式的方法進行風險評估
  - 而其它的部份採用基準法

5 風險評鑑方法設計上常見的問題

- 採用資產導向時，如何去處理大量的資產與其相關的風險？
- 一個資安事件發生，萬一有可能會影響到多個資產？
- 期望風險與極端值
- 採用 FTA 等方法時，如何計算風險？

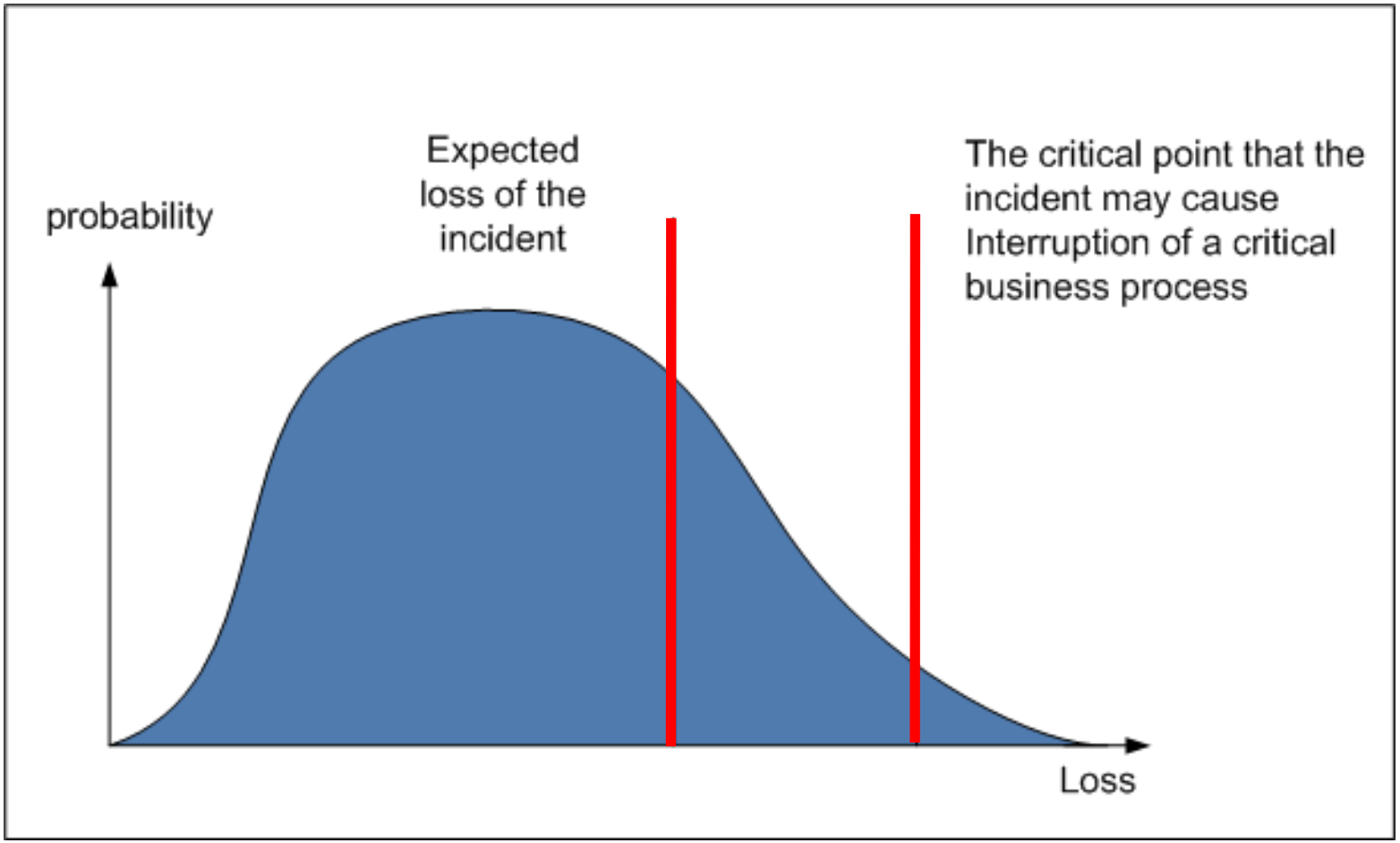
一種可能的作法

- 將資產分類，依類別產生風險清單
  - 可節省每個資產都要去判斷到底有哪些風險的問題
- 將會有相似風險的資產放在一起評
- 只看資產價值減損 (AV*EF)，而避免一個一個風險去判斷
  - 思考：資產價值可以如何判斷？

思考：資訊安全可以保險嗎？

- 是否有可能將資安事件保險，讓保險公司來負擔損失
  - 國內目前針對個人資料保護法修正案，有保險公司在思考推出這樣的產品
- 保險通常是一種風險分攤的概念，有沒有可能有一種資安事件會造成很多公司同時出現問題？
- 同樣的，在一家公司內，如果是看期望風險，萬一有某事件發生會同時影響到很多資產？

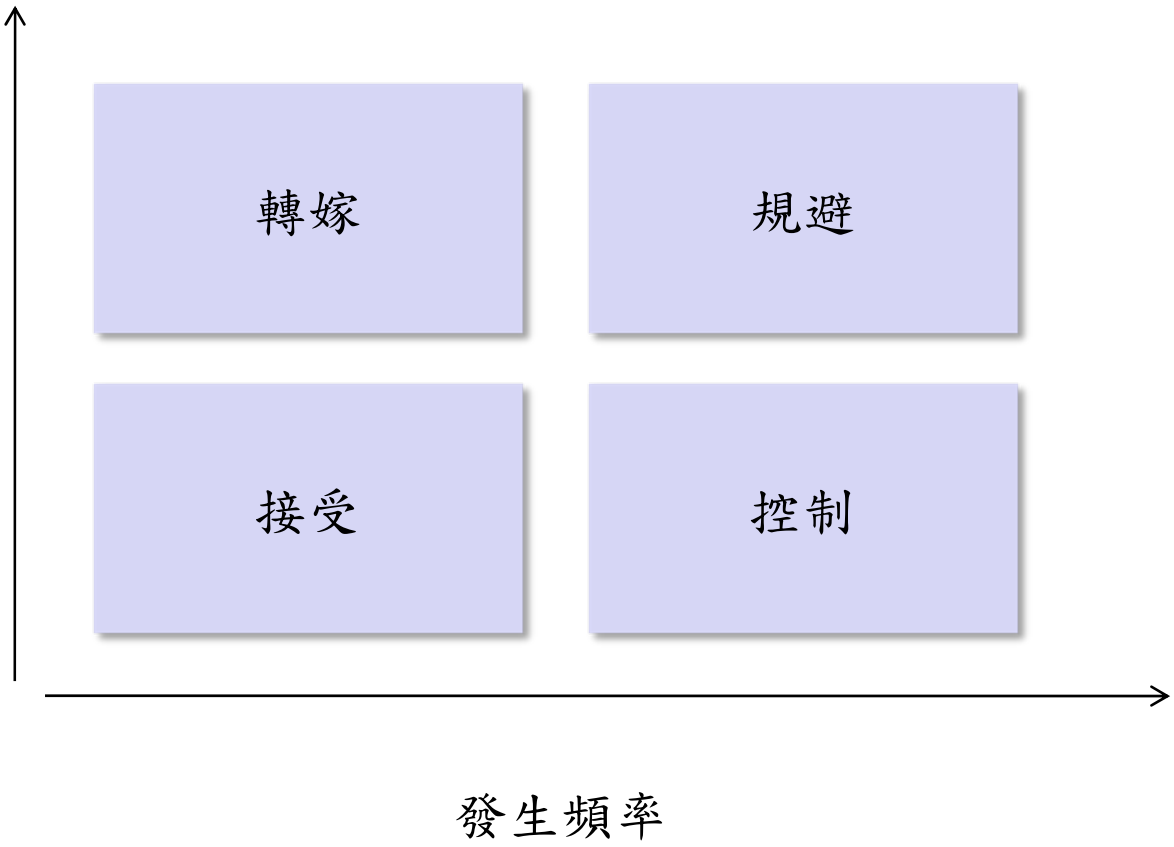
思考：如何考慮極端值的狀況



5 風險對應

風險的管理

- 當評估出來風險以後，一般可以採用以下四種方式加以管理：
  - 接受
  - 轉嫁
  - 繞道
  - 控制



6 資訊安全風險管理比較框架

為何要有一個比較框架

- 在 1990 年代初期，就已經有數十種風險管理方法論
- 這些比較標準或框架來說，主要可以分成兩類：
  - 針對各方法或程序本身的特色或功能
  - 提供組織依照本身的條件來做出選擇

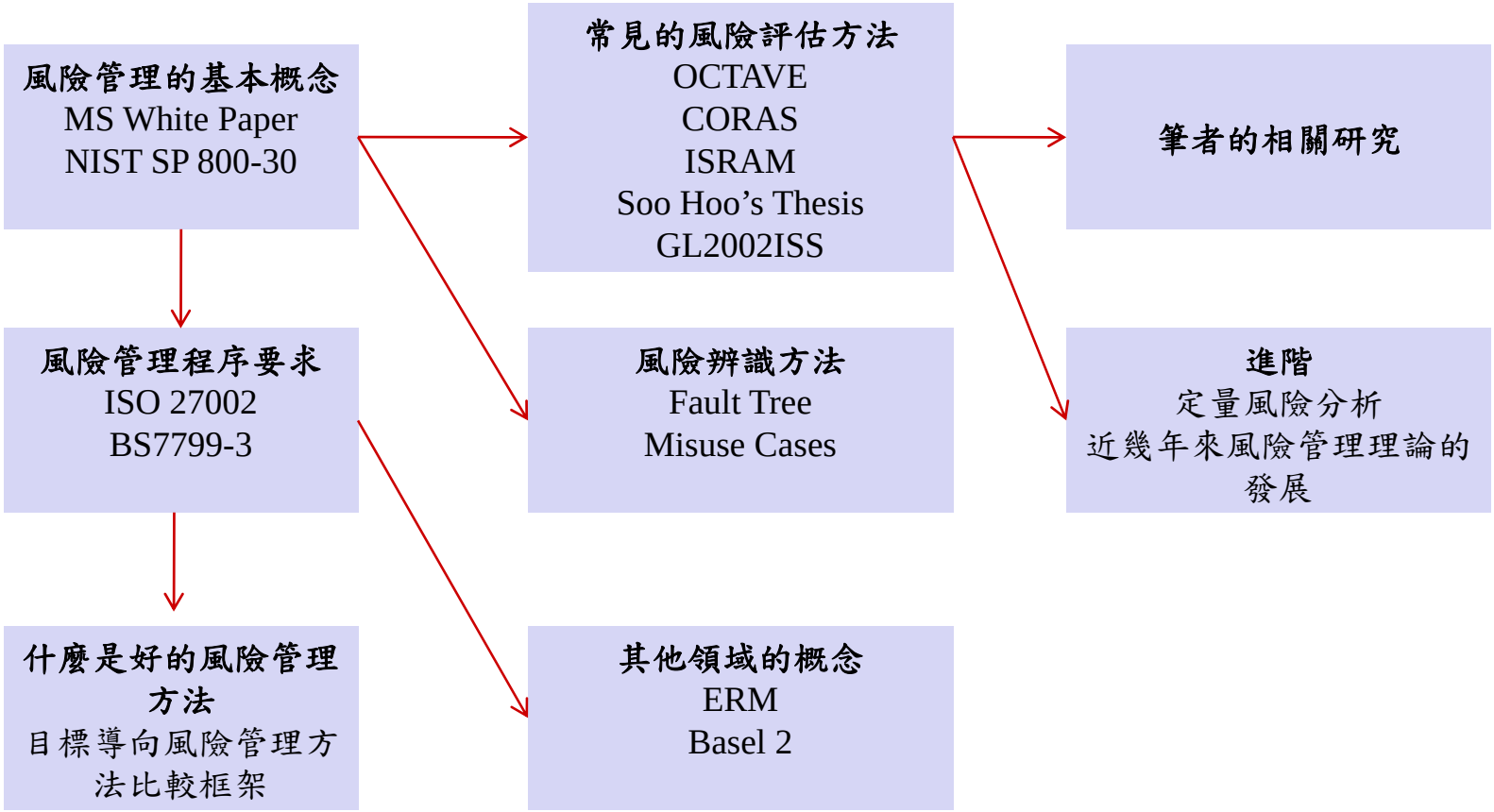
功能比較指標

- 一致性 (Consistency)：不同的人進行風險評估的結果不致於有一個顯著的差異。
- 易用性 (Useability)：因為要得到風險評估的結果，所必需要花費的成本 (如學習、作業，與準備輸出入資料等) 是值得的。而這也可表現在可被理解與容易使用的程度。
- 可調整性 (Adaptability)：方法或是工具可以被應用在許多不同的系統環境中。
- 可行性 (Feasibility)：可以採用最具經濟效益的方法來取得所需的資料或執行。
- 完整性 (Completeness)：是否有考慮到足夠周詳的元素或方面
- 有效性 (Validity)：程序的結果能夠反應真實的情況
- 可信賴性 (Creditability)：結果是可信並且是有價值的。

Garrabrants, W. M., Ellis, A. W., Hoffman, L. J., & Kamel, M. (1990). CERTS: A Comparative Evaluation Method for Risk Management Methodologies and Tools. In *Proceedings of the 6th Annual Computer Security Applications Conference* (pp.251-257). IEEE Computer Society Press.

7 學習地圖

- 學習地圖


風險管理的基本概念
MS White Paper
NIST SP 800-30
常見的風險評估方法
OCTAVE
CORAS
ISRAM
Soo Hoo's Thesis
GL2002ISS
筆者的相關研究
風險管理程序要求
ISO 27002
BS7799-3
風險辨識方法
Fault Tree
Misuse Cases
進階
定量風險分析
近幾年來風險管理理論的發展
什麼是好的風險管理方法
目標導向風險管理方法比較框架
其他領域的概念
ERM
Basel 2