經濟部iPAS
「資訊安全工程師能力鑑定」

資訊安全管理概論

Bryan Chen

CISSP, CEH, ISO 2700I LA, Security+, CIW Security Analyst
ITIL Expert SO 2000 LA, ISO 20000 Consultant

講師簡介

- **學歷**
  - 賓州大學 (U. of Pennsylvania) 資訊科學研究所 碩士
- **經歷**
  - **(現) 104 資訊科技 副總 暨 資安長**
  - 中華電信研究院 資安所 研究員
  - 英國標準協會(bsi) 主導稽核員/講師
  - Asiainfra Ltd. 資安服務處協理
  - 鈺松國際 監控中心(SOC)資安工程師
  - 啟碁科技 研發工程師
  - 大同世界科技 軟體工師
- 講師資格
  - (ISC)2 CISSP CBK Review Seminar 講師
  - Quintica ITIL 講師/ TAOS ITIL 講師
  - 資策會/恆逸 ITIL特約講師
  - BSI 英國標準協會 ISO27001/ISO20000 講師
- **資訊安全認證**
  - CISSP – 資訊安全系統專家
  - EC-Council CEH – EC-Council 白帽駭客
  - CompTIA Security+ - CompTIA資訊安全
  - CIW Security Ayalyst – CIW 資訊安全分析專家
- **資訊服務管理 (ITSM)認證**
  - ITIL Expert ITIL - ITIL專家認證
  - ITIL V2 Service Manager – ITIL V2最高認證
  - ITIL V3 SO – ITIL服務維運
  - ITIL V3 RC&V – ITIL服務發行控制與確認
  - ITIL V3 OS&A – ITIL服務提供與支援
  - ITIL V3 SO&A – ITIL服務提供與協定
  - ITIL V2/V3 Foundation – ITIL V2/V3 基礎
  - ISO 20000 Consultant – ISO 20000 顧問
- **稽核**
  - IRCA ISMS LA - 國際註冊資訊安全主導稽核員
  - ISO 20000 LA - ISO 20000 主導稽核員
  - ISO 27001 LA - ISO 27001 主導稽核員
  - ISO 20000 Auditor – ISO 20000 稽核員 (itSMF)

小遊戲

IPX BSF ZPV

-1

報考對象與通過標準

- 對象
  - 不限科系
  - 對資訊安全有興趣
- 考題
  - 單選題

- 通過標準
  - 一次報考兩科
    - 總分達140分
    - 但單科成績不得低於50分
  - 分次報考
    - 三年度內完成兩科目
    - 成績皆達70分

初級資訊安全工程師-考科一

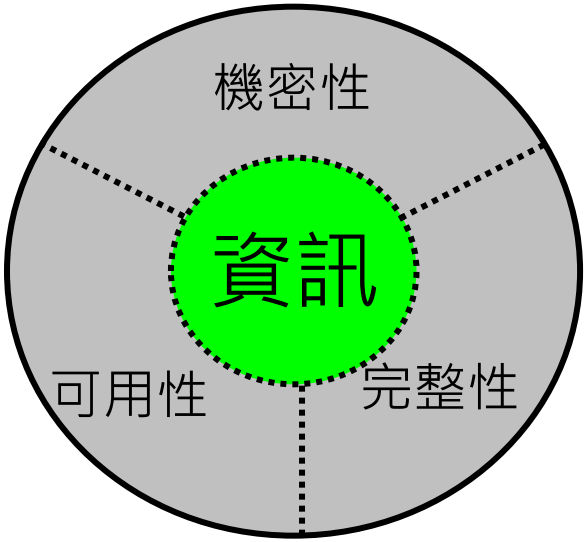
科目	評鑑主題	評鑑內容
科目一： 資訊安全管理概論	資訊安全管理概念	機密性、完整性與可用性定義
		資訊安全管理系統
	資產與風險管理	資產分類分級與盤點
		風險評鑑與風險處理
	存取控制、加解密與金鑰管理	**存取控制與身份認證**
		加解密與金鑰生命週期
	事故管理與營運持續	事件與事故管理
		備援與營運持續
	法規遵循與資訊倫理	隱私保護與智慧財產權
		資訊倫理、法規遵循**(含GDPR)**與稽核

證照價值

- 常見資安證照
  - iPAS
  - CISSP
  - CEH
  - CHFI
  - ISO 27001
  - CISA
  - CISM

資訊安全的三個目標

機密性 (Confidentiality)	資訊之秘密性與隱私性，應防止機密資訊外洩
完整性 (Integrity)	資訊或系統之正確性，應防制人為刻意竄改與自然雜訊干擾；防制假冒或未授權方式存取系統資源進行資料之處理或更改
可用性 (Availability)	資訊與資訊處理的可獲得性，應避免資訊因系統故障或人為惡意的阻斷服務



資訊安全之目標及保護資訊之C.I.A

對於組織來說還要做到法規的遵循 (compliance)

評鑑主題—
資訊安全管理概念

1.機密性、完整性與可用性定義

2.資訊安全管理系統

重要字辭與定義

重要字辭與定義

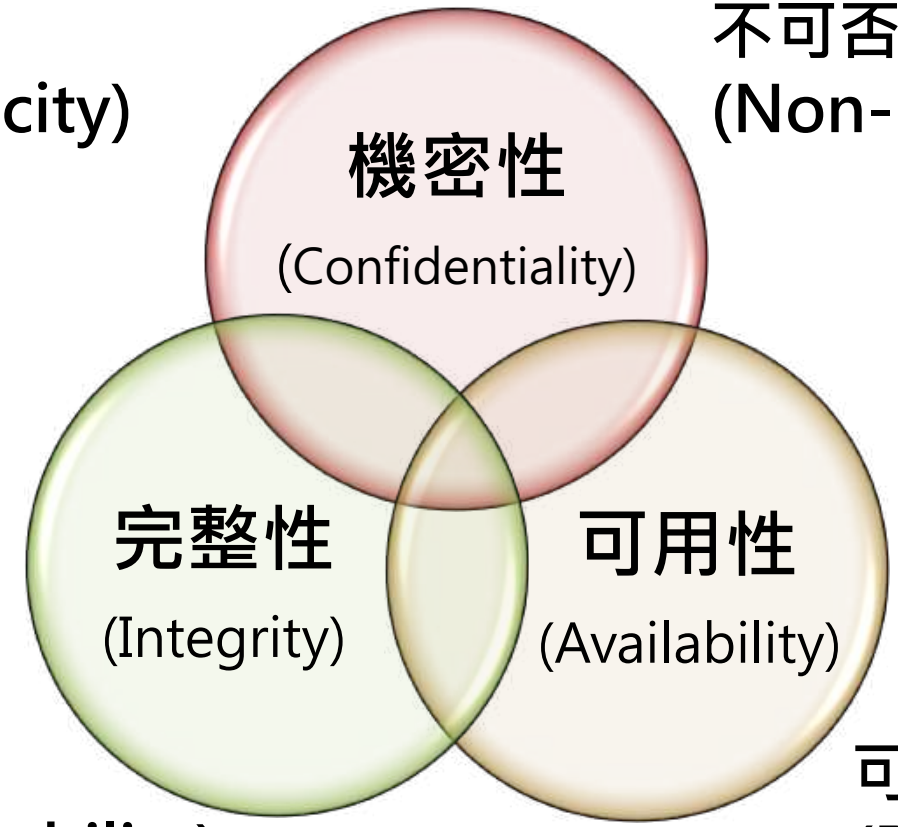
重要資安概念

- 邊界與分類 (Boundary and classification)
- 職務區隔 (Segregation of duties, SOD)
- 縱深防禦 (Layered defense, defense in depth)
- 單一脆弱點 (Single point of failure, SPOF)
- 阿奇里斯腱 (Achilles heel)
- 木桶理論 (Bucker principle)
- 僅知原則 (Need to know)

安全 (Security)

鑑別性
(Authenticity)

不可否認性
(Non-repudiation)

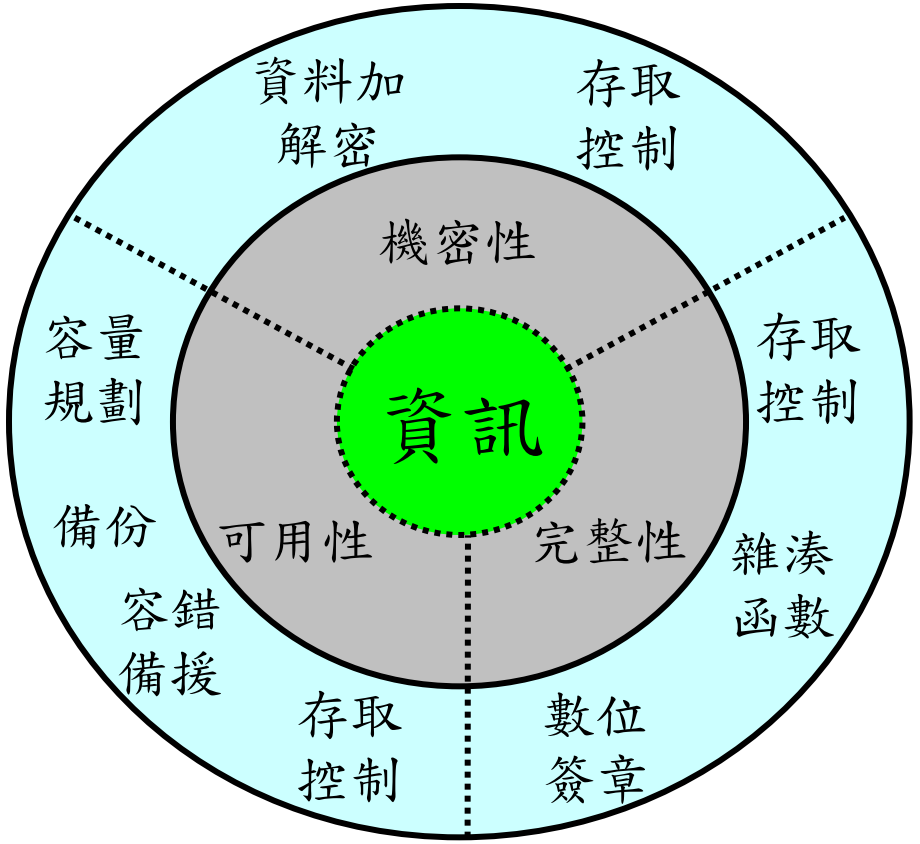


可歸責性
(Accountability)

可靠度
(Reliability)

保護資訊C.I.A.不同的技術與方法

- 機密性保護
  - 加解密技術
  - **存取控制**
- 完整性保護
  - 雜湊函數
  - 數位簽章
  - 存取控制
- 可用性保護
  - 容量規劃
  - 備份
  - 容錯、備援及負載平衡
  - 存取控制
- **法規的遵循**



不同的安全性需求使用
不同的方法與技術

ISO 27000系列的資安標準

- ISO 27000 開頭的都是資安相關的國際標準
- 國內有相對應的翻譯　CNS 2700X
  - 目的在於制定一個可用來建立、實作、運作、監視、審查、維持及改進「資訊安全管理系統」(Information Security Management System, ISMS)的模型。
- 雲端安全相關的ISO 27017與ISO 27018
  - **ISO/IEC 27018**《公有雲個人資料(PII)處理者之個資保護作業規範》
  - **ISO/IEC 27017**《雲端運算服務的資訊安全控制措施實務守則 》

資訊安全管理系統

界定範圍：最重要的第一步

ISO 27001 架構


政策/目標
風險分析
風險評鑑
決定管控
有效性量測/
管理審查/內部稽核
持續改善
溝通
溝通
溝通
溝通
統御
資源
文件
Plan
Do
Check
Act

範例考題

學生侵入學校的伺服器，偷偷竄改自己的期末考成績。這是破壞了資訊的哪一項特性？

- (A)保密性（Confidentiality）
- (B)完整性（Integrity）
- (C)可用性（Availability）
- (D)責任性（Accountability）

組織對外服務之官方網站遭受駭客透過DDoS攻擊，請問此為下列哪項遭受破壞？

- (A) 機密性
- (B) 完整性
- (C) 可用性
- (D)可讀性

請問下列何項說明內容是關於「可用性」的敘述？

- (A)使用者以專用帳號及密碼登入ERP系統
- (B)電信商機房故障，暫時無法使用網路
- (C)親自遞送機密文件給總經理核閱
- (D)出勤系統異常，導致薪資計算錯誤

下列何種作為，展現了最高管理階層對資訊安全管理系統（Information Security Management System, ISMS）之領導和承諾？

- (A) 確保資訊安全政策和目標需至少維持三年不變
- (B) 確保資訊安全的要求已整合至組織的各項作業流程
- (C) 確保在未來一年內降低組織的營運成本
- (D) 確保適當規劃和制訂完成組織的年度營運計畫

評鑑主題二
資產與風險管理

1. 資產分類分級與盤點
2. 風險評鑑與風險處理

重要字辭與定義

重要字辭與定義

資訊資產包含哪些項目

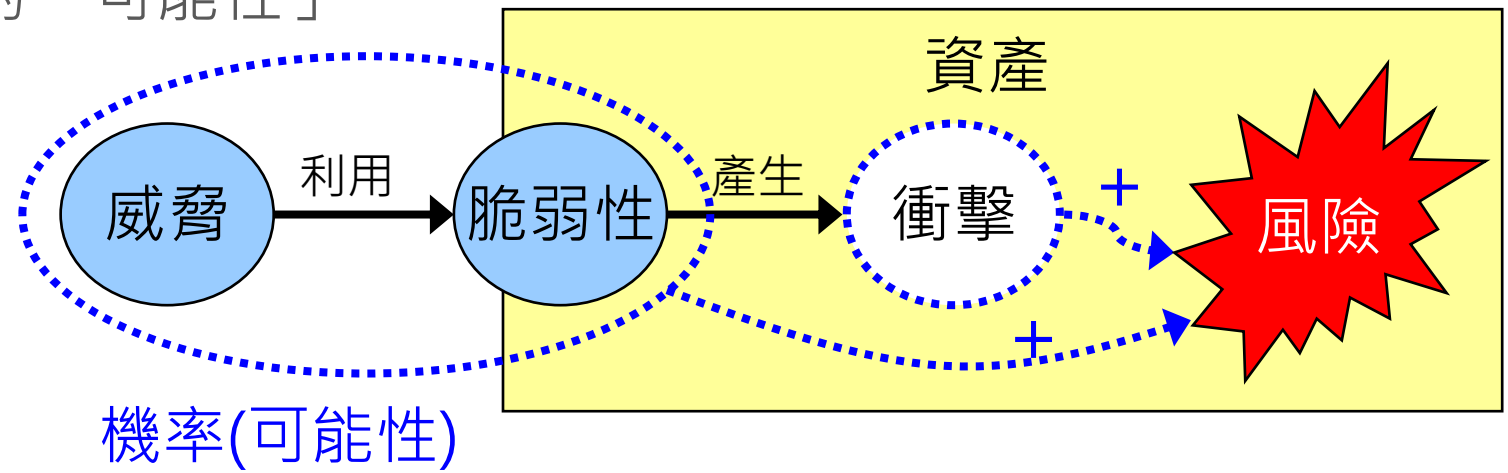
- 實體資產
  - 所有電腦設備、通信與網路設備及相關週邊設備等
- 軟體資產
  - 自行或委外開發之軟體、套裝軟體、公用程式等
- 電子化資訊資產
  - 電子儲存之文件、系統資料、組態設定檔、稽核紀錄檔等
- 書面文件
  - 書面管理文件與紀錄、系統相關文件等
- 服務
  - 通訊、網路、照明、電力等
- 人員
  - 正式職員、約聘人員、廠商駐點人員及工讀生等

資訊資產蒐集與管理

- 應維持資產清冊的正確性
- 設計資訊資產清冊的更新流程

風險的定義

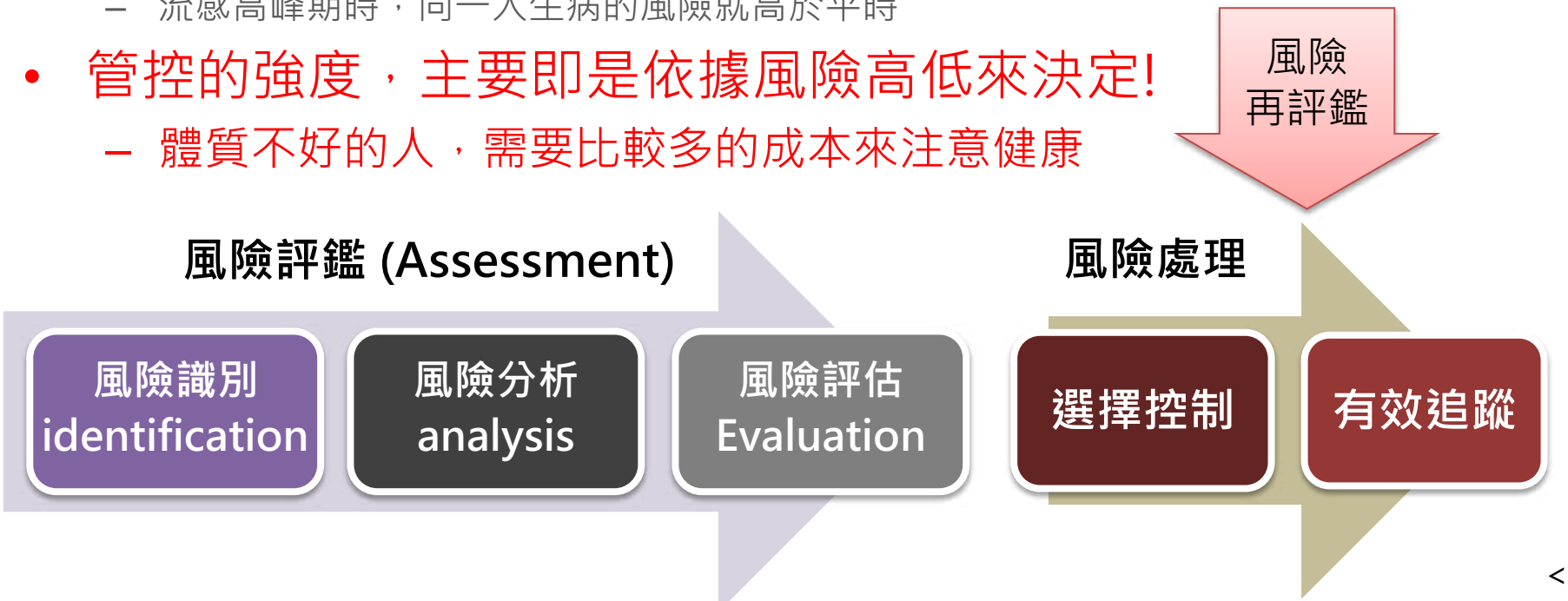
- 所謂「風險」是指「威脅」利用「資產」相對應「脆弱性」直接或間接造成組織一個或一群「資訊資產」受到「衝擊(Impact)」的「可能性」



- 風險管理的目標
  - 在最低的防護成本投入下獲得最優化的安全性(最優化非最強固，而是最合適)

風險管理

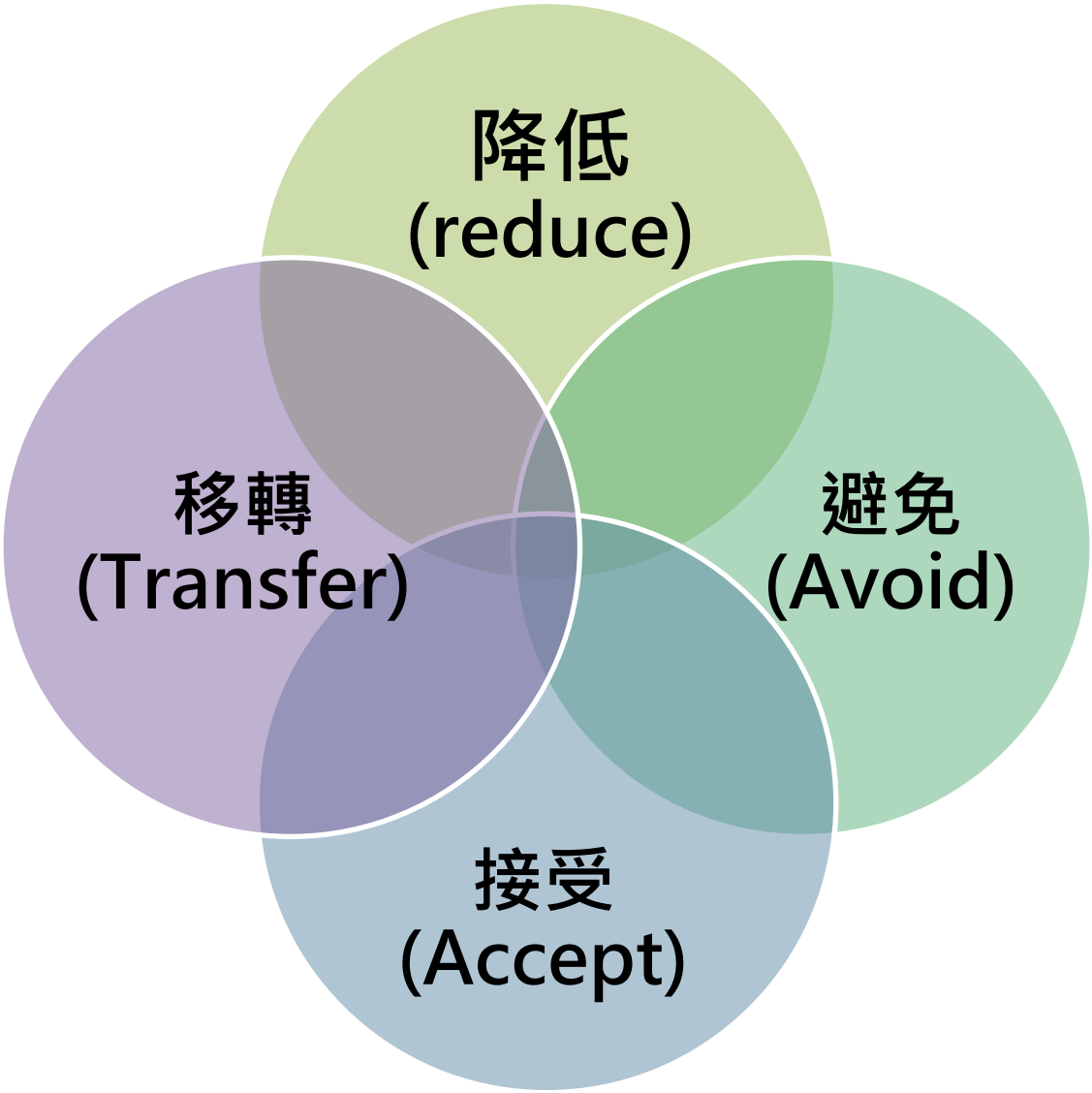
- 何謂風險 (常用的精簡定義)
  - 威脅 (Threat)利用資產 (Asset)的脆弱性 (Vulnerability
    造成衝擊 (Impact)的可能性 (Likelihood)
- 例：
  - 病毒 (威脅)利用人 (資產)的身體抵抗力弱 (脆弱性) 造成生病的衝擊的可能性
  - 同樣的環境，抵抗力低的人，生病的風險高於抵抗高的人
  - 流感高峰期時，同一人生病的風險就高於平時
- 管控的強度，主要即是依據風險高低來決定!
  - 體質不好的人，需要比較多的成本來注意健康



風險接受準則

- 用途
  - 用來判斷風險是否可以接受或必須要進行處理的原則，例如：
    - 可接受風險的評估原則
- 通常依據組織政策、目標及業務關係來定義可接受或不可接受的狀況與條件
- 可參考接受的原因
  - 風險處理成本高過損失
  - 有能力處理相關安全事故
  - 尚無有效處理風險的技術

風險處理活動



不可漠視

ignore

重要名詞定義

- 資產弱點
  - 資訊資產本身存在之特性，可被威脅利用而使得資訊資產遭受破壞。
- 風險識別與分析
  - 可利用弱點，因而對資訊資產造成破壞的外在因素。各類弱點會因為不同威脅的發生而產生風險，故需考量威脅發生之重大性。
- 可接受風險
  - 由資訊安全組織依所面臨之風險及所願意投入之資源，而決定風險可接受水準，以作為控管機制設計執行者
- 殘餘風險管理（接受風險、移轉風險、降低風險、規避風險）
  - 當控管規範或機制增加或強化後，應重新評估風險權值，並重複執行辨認及降低風險步驟，直到降至風險可接受水準為止。

Data Owner
（資料擁有者）

vs.

Data Custodian
（資料保管者）

範例考題

關於資訊資產分級的目的，下列敘述何者正確？

- (A)確保員工及承包商之相關安全責任
- (B) 限制對資訊及資訊處理設施的存取
- (C) 確保資產依其對組織之重要性，受到適切等級的保護
- (D)確保運作中系統的完整性

在進行資產管理時，下列哪一項應優先建立？

- (A)稽核計畫
- (B) 溝通管理
- (C) 風險登記表
- (D)資產清冊

關於資產分級盤點施作方式，下列敘述何者不正確？

- (A) 保管人離職轉移，需要進行相關資產歸戶變更
- (B) 異地備援端相關系統，需另標示位置資訊，以為識別
- (C) 電腦規格需依據製造商規格項列於資訊紀錄中
- (D) 資訊設備送修，無法列入盤點，可以不用處置追蹤

下列何者非資產擁有者所負責執行之工作？

- (A)確保資產已盤點並造冊
- (B) 確保資產已經適切分級，並實施適當之保護
- (C) 確保資產以最低之成本進行採購
- (D)確保資產的銷毀已採取適當之處置程序

下列何者為建立組織資訊安全管理系統（Information Security Management System, ISMS）活動中優先於另三項需要進行的任務？

- (A)識別弱點
- (B) 識別現有及已規劃之控制措施
- (C) 識別資訊資產
- (D)識別威脅

如果資訊安全事件的攻擊者的獲益小於成本時，或是預估的損失在組織可以容忍的範圍內，此時可以採取哪一種風險處置策略？

- (A)風險接受
- (B) 風險降低
- (C) 風險移轉
- (D)風險避免

關於資訊安全管理系統中的風險處理，下列敘述何者不正確？

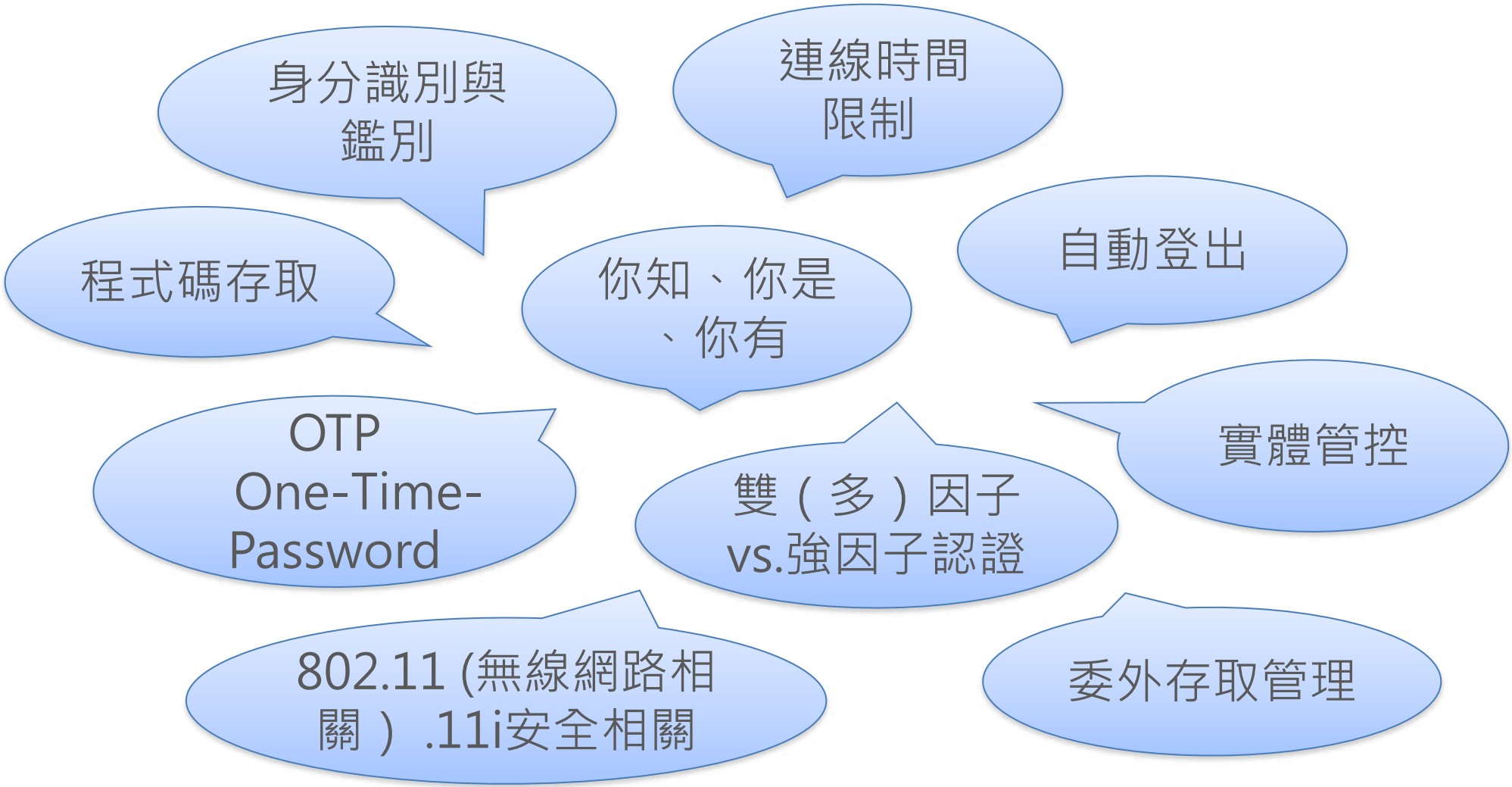
- (A)依照風險等級，實施控制措施，降低風險
- (B) 可選擇風險轉移；比方購買地震或防火保險
- (C)所有風險都可以選擇直接接受
- (D)移除風險來源

評鑑主題三
存取控制、加解密與金鑰管理

1. 存取控制
2. 加解密與金鑰管理

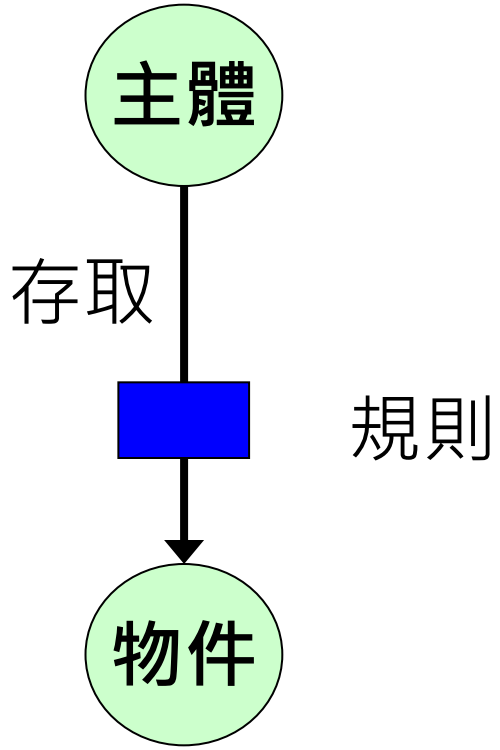
重要字辭與定義

重要字辭與定義


身分識別與鑑別
連線時間限制
程式碼存取
你知、你是、你有
自動登出
OTP One-Time-Password
雙（多）因子vs.強因子認證
實體管控
802.11 (無線網路相關） .11i安全相關
委外存取管理

存取控制的定義

- 主體(Subject)
  - 主動發起存取行為的個體
  - 通常為資料流的起點
  - 例如：使用者與處理程式
- 物件(Object)
  - 被動存取的個體
  - 通常為資料的接收端與保存端
  - 例如：檔案、資料庫及處理程式
- 存取(Access)
  - 主體對物件進行某些動作
  - 例如：讀取、修改、刪除、建立或執行
- 存取規則(Access Rule)
  - 可強制控管主體與物件之間存取路徑的控制機制
- 信賴路徑(Trusted Path)
  - 確保主體可以存取到其所預期存取到之物件的路徑



存取控制的類型

- 實體類控制(Physical Controls)
  - 門、窗及圍牆
  - 鎖
  - 警衛
- 技術類控制(Technical Controls)
  - 通行碼鑑別
  - 加解密技術
  - 生物特徵識別技術
  - 防火牆系統、入侵偵測及防禦系統
- 管理類控制(Administrative Controls)
  - 政策與程序
  - 安全認知訓練
  - 風險管理

存取控制的功能

- 防禦性 (Preventive)
  - 讓不當的損害事件不會發生(消除威脅或弱點)
- 偵測性 (Detective)
  - 當發生不當的損害事件時可被識別，以利即時處理(入侵偵測與煙霧偵測)
- 矯正性 (Corrective)
  - 發生不當的損害事件時可立即防制(滅火設備)
- 嚇阻性 (Deterrent)
  - 降低威脅發生的意圖，但無法阻擋(CCTV)
- 復原性 (Recovery)
  - 發生不當損害後可回復原來的正常運作
- 補償性 (Compensation)
  - 對其他控制措施提供選項的控制措施

存取控制的管理

- 帳號管理(身分識別與鑑別)
  - 身分識別(Identification)：主體告知身分識別資訊，例如：帳戶、使用者代號及使用者名稱
  - 身分鑑別(Authentication)：驗證身分識別資訊的技術，例如：通行碼、生物特徵及動態通行碼
- 授權(Authorization)
  - 決定主體是否能夠存取物件的判斷準則
- 可歸責性(Accountability)
  - 稽核紀錄(Auditing)
  - 存取行為不可否認的機制

授權原則

- 業務需知原則/ 僅知 (Need to know)
  - 只提供執行業務上所需知道的資訊
- 最低權限原則 (Least privilege)
  - 權限開放時採用最低權限原則
- 職務區隔 (SOD)
  - 「重要」的工作任務可切割由多人負責，避免需共謀進行的惡意行為(例如：掌管存取安全的人員不應擔任安全稽核的工作)
- 特殊權限管理
  - 對於系統管理者帳號及相關安全組態設定權限，應採特別的控管方式，並詳細記錄特權人員的存取行為

實體環境的存取控制

- 存取控制的角色
  - 主體：人員
  - 物件：機房、線路室、保險櫃及電腦等
  - 存取規則：只有在職員工能從1F大門進出
  - 強制信賴路徑：2M圍牆加電網、獨棟建物且與其他建物棟距20M以上(強制性足夠嗎？)
- 存取控制的管理
  - 鑑別：門口警衛檢查人員通行證
  - 授權：通行證有效且為在職員工者放行，無效或非在職員工則不放行
  - 可歸責性：登記人員進出的時間、目的、攜入或攜出的物品

作業系統的存取控制

- 存取控制的角色
  - 主體：人員與執行中的程式(Process)
  - 物件：檔案、資料庫、其他執行中的程式及記憶體等
  - 存取規則：通行碼檔案只能被管理者存取
  - 強制信賴路徑：所有磁碟機的檔案存取由OS控制，一般程式不能直接存取磁碟機，使用者所執行的程式繼承該使用者的身分與權限(強制性足夠嗎？)
- 存取控制的管理
  - 鑑別：簽入作業(帳號通行碼比對正確)
  - 授權：是否為管理者群組？是否符合檔案存取權限？
  - 可歸責性：檔案開啟、修改及刪除都被記錄下來，包含時間與存取者等

應用系統的存取控制

- 存取控制的角色
  - 主體：人員
  - 物件：檔案與資料庫等
  - 存取規則：只有主管才能簽核其部屬的假單
  - 強制信賴路徑：所有簽核動作集中於個別程式處理，且配合電子簽章技術(強制性足夠嗎？)
- 存取控制的管理
  - 鑑別：應用程式簽入作業(帳號通行碼比對正確)
  - 授權：是否為主管？請假人是否為其部屬？
  - 可歸責性：所有簽核動作都應記錄，包含時間、申請人、簽核人及簽核結果等

網路服務的存取控制

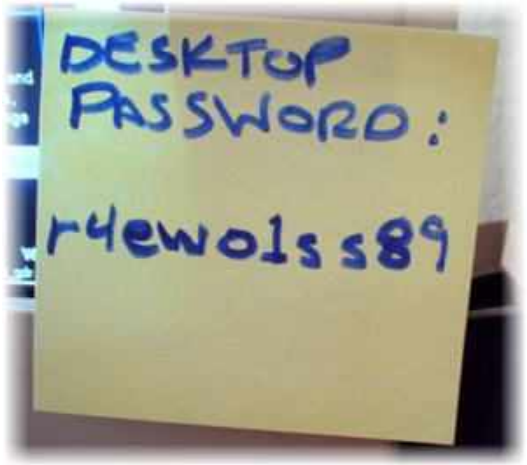
- 存取控制的角色
  - 主體：人員、執行中的程式(Process)及傳送端設備等
  - 物件：網路服務(例如：電子郵件與網站存取)
  - 存取規則：內部電子郵件必須透過內部郵件伺服器對外傳送
  - 強制信賴路徑：防火牆只開放內部郵件伺服器IP可以對外傳送電子郵件(強制性足夠嗎？)
- 存取控制的管理
  - 鑑別：來源IP
  - 授權：是否為內部郵件伺服器？是否為對外寄送信件連線？
  - 可歸責性：防火牆記錄所有進出的網路連線請求

身份認證因素

- 所知之事，你知 (Something you know)
  - 例：通行碼
- 所持之物，你有 (Something you have)
  - 例：晶片卡
- 所具之形，你是 (Something you are)
  - 例：指紋

通行碼身分鑑別技術(1/2)

- 目前使用「最廣泛」也「最簡便」的身分鑑別技術
- 也是最不安全的身分鑑別技術
  - 使用者選用了「懶人通行碼」
  - 共用通行碼
  - 將通行碼貼在螢幕上
  - 從不更改通行碼
  - 輸入通行碼時被別人看到按下的通行碼
- 針對通行碼的攻擊
  - 字典猜測法
  - 暴力式通行碼猜測
  - 通行碼監聽



通行碼身分鑑別技術(2/2)

- 避免通行碼被破解的防護措施
  - 系統強制要求長度至少8碼
    - 包含文字、數字及符號、包含大小寫
    - 在字典中查不到、**以中文字注音符號按鍵來設定**
  - 系統強制要求使用者定期更換通行碼
  - 由系統判斷通行碼不重覆使用
  - 可限制通行碼容許簽入失敗的次數
  - 簽入成功或失敗都應被記錄
  - 使用通行碼檢測工具尋找脆弱通行碼
  - 通行碼不以明碼方式儲存
  - 通行碼不以明碼方式在網路上傳送
  - 加強保護集中存放通行碼的伺服器

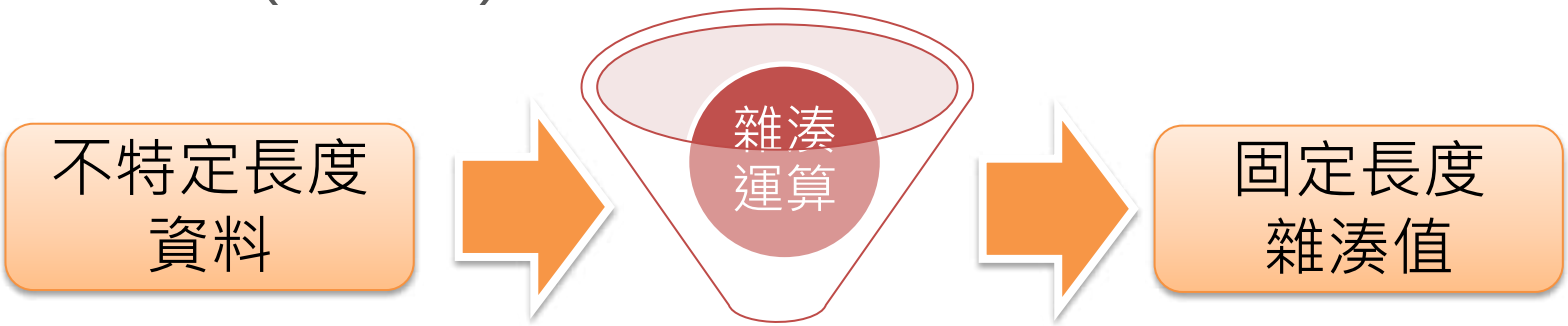
OTP（One-Time Password）

- 一次性通行碼(One-Time Password)或稱動態通行碼的特質
  - 由隨身攜帶的代碼(Token)或軟體自動產生簽入用通行碼
  - 簽入時每次產生的通行碼只能使用一次
  - 可防止通行碼被竊聽而偽冒簽入的問題
  - 可防止通行碼猜測攻擊

雜湊 (Hashing)

- 輸出結果
  - 稱為訊息摘要（message digest）或摘要（digest）
- 特性
  - 無法反推出原來的訊息
  - 雜湊值必須隨明文而改變
- 檢查完整性（正確）

- 常見演算法
  - MD5、SHA-1已不安全
  - SHA-2 (SHA-224/256...)
  - SHA-3 (SHA3-225/256/384...)



鹽(Salt)

- 將雜湊內容的任意固定位置插入特定的字串
- 例：
  - 一個太短的密碼x7faqgjw
  - 經過SHA 算出
    58ecbf2b3136ceda7fddfd986ba8bd8d59b2d73779691e839f3f176ce2c04b84
  - 但因為原密碼太短，容易被破解
  - 加上綠字的鹽　x7faqgjwabcdefghijklmnopqrstuvwxy
  - 算出新的值（同長度６４，但不易被破解）
    7b5001a5a8bcdcfa1b64d41f6339cfa7a5c0eca04cca6ff6a6c1d6aad17794cc

鹽(Salt)程式範例

```php
<?php
function hash($a) {
    $salt="WIKIPEDIA";
    $b=$a.$salt;
    $b=sha($b);
    return $b;
}
?>
```

加鹽「WIKIPEDIA」

把原字串加上鹽

算出雜湊值

回傳雜湊值

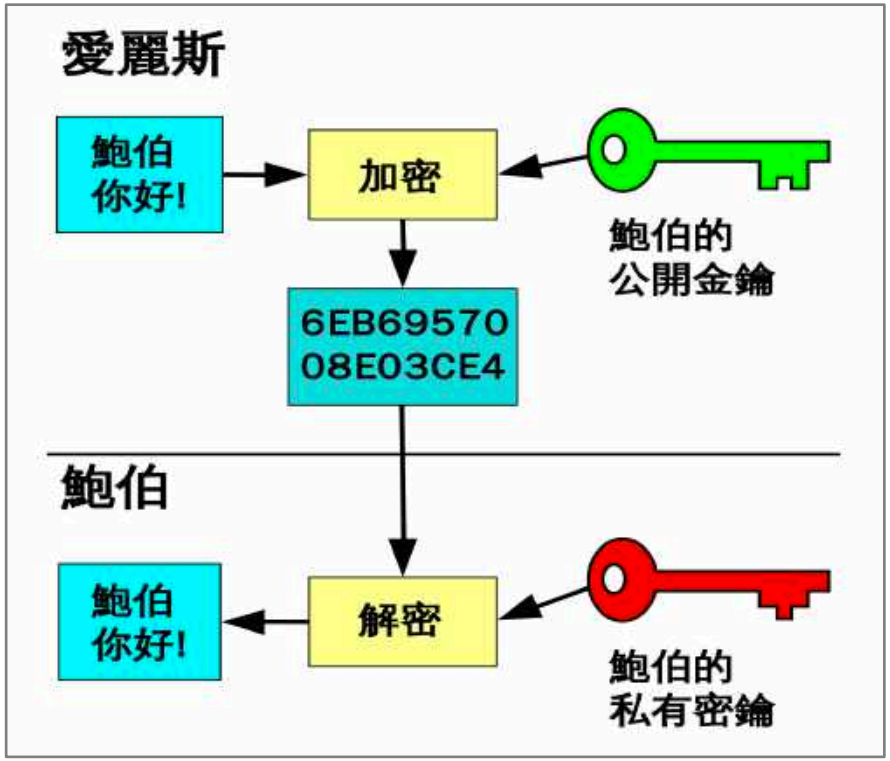
對稱密鑰 (Symmetric-key)

- 私鑰加密
- 雙方用同樣的Key加解密文
- 換key議題

- DES已不安全
  - 3DES
  - AES192/256

公開金鑰密碼學

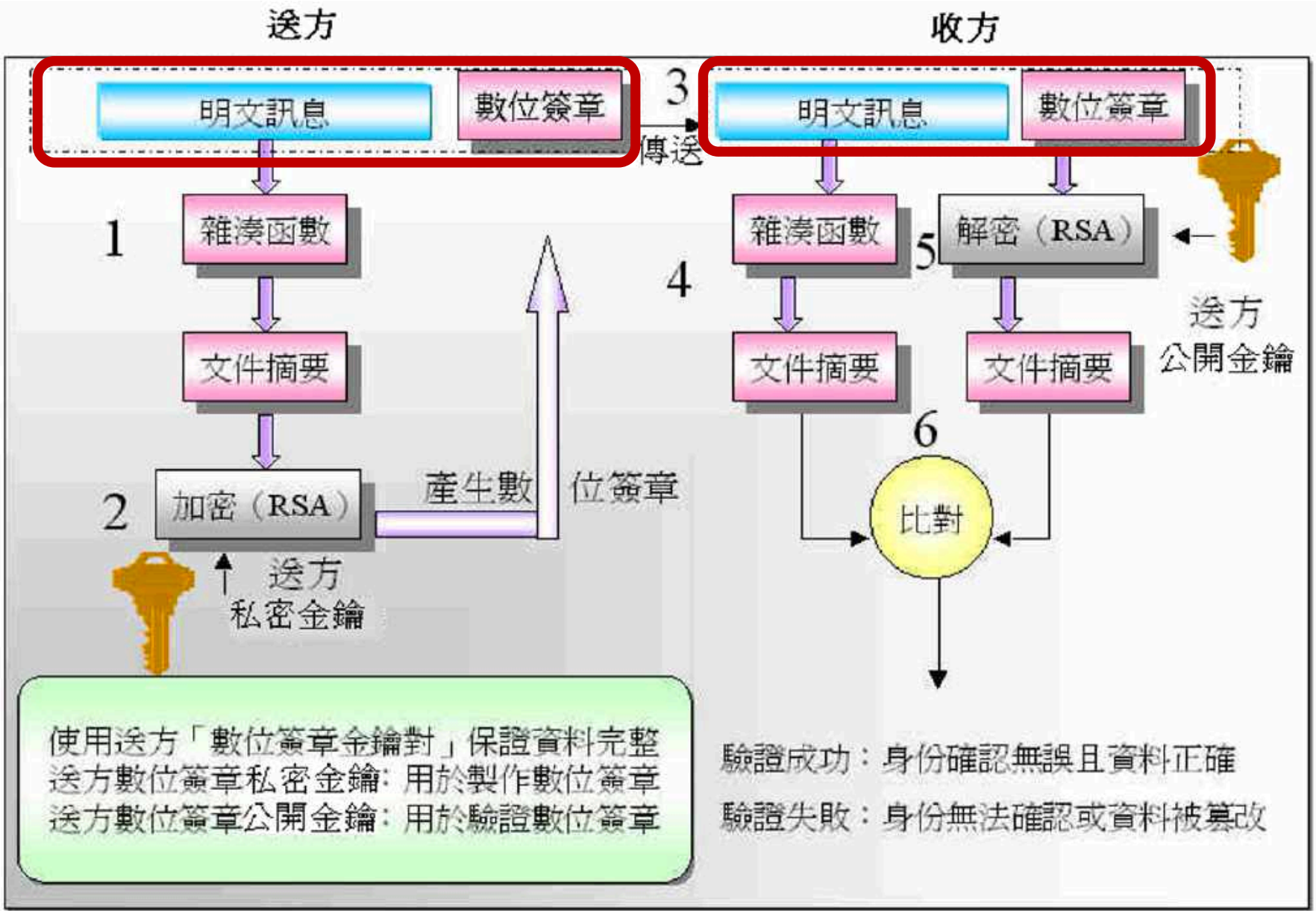
- Public-key cryptography
- 也稱**非對稱式密碼學**
- 公開密鑰：加密，
- 私有密鑰：解密



數位簽章

流程見次頁

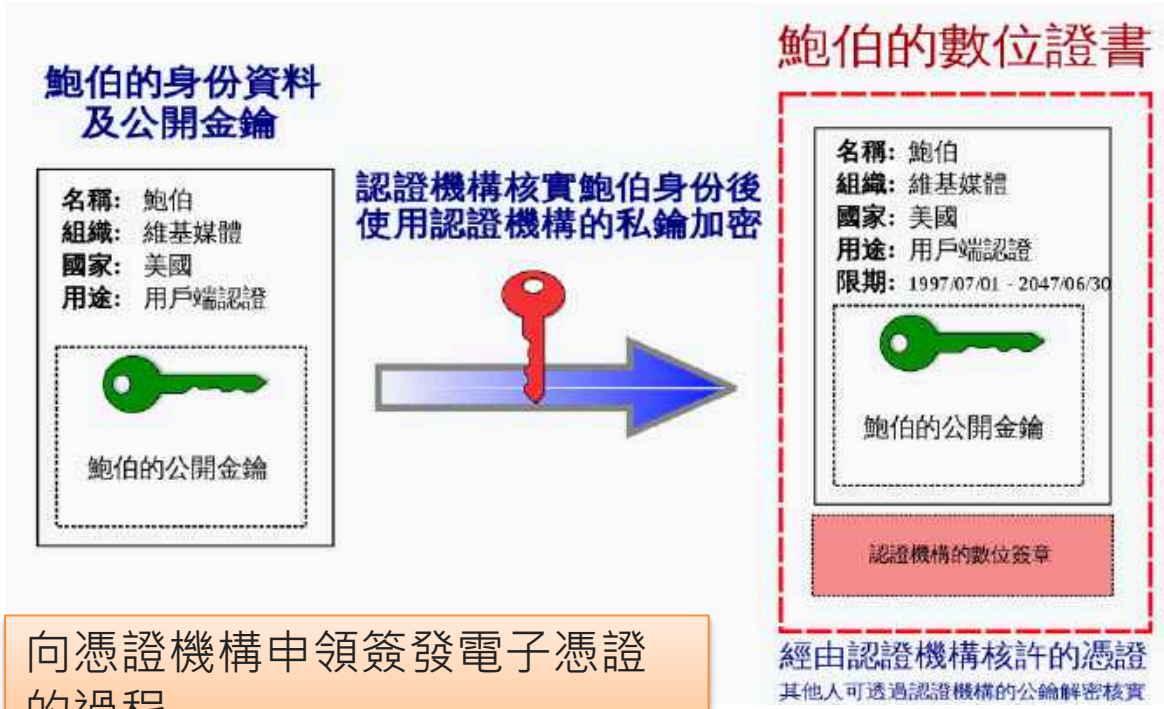
- **Digital Signature**
- **公鑰數位簽章 (例：RSA)**
- 私鑰加密：生成簽名
- 公鑰解密：驗證簽名
- 訊息「完整性」(先算Hash)
- 傳送者「不可否認性」


送方
收方
明文訊息
數位簽章
3
傳送
明文訊息
數位簽章
1
雜湊函數
雜湊函數
4
5
解密（RSA）
送方
公開金鑰
文件摘要
文件摘要
文件摘要
6
比對
2
加密（RSA）
產生數位簽章
送方
私密金鑰
使用送方「數位簽章金鑰對」保證資料完整
送方數位簽章私密金鑰：用於製作數位簽章
送方數位簽章公開金鑰：用於驗證數位簽章
驗證成功：身份確認無誤且資料正確
驗證失敗：身份無法確認或資料被篡改

數位憑證（digital certificate）

- 又稱**公開金鑰認證**（Public key certificate）
- 用來證明**公開金鑰擁有者**的**身分**
- 認證機構用自己的私鑰對需要認證的人（或組織機構）的公鑰施加數位簽章並生成憑證

- 包含了
  - 公鑰資訊
  - 擁有者身分資訊（主體）
  - **數位憑證認證機構**（發行者）對此檔案的**數位簽章**
- 一般遵從X.509格式規範



向憑證機構申領簽發電子憑證的過程

數位憑證認證機構

- Certificate Authority，縮寫為CA
  - 又稱：電子商務認證中心、電子商務認證授權機構
- 電子商務交易中受信任的第三方，承擔公鑰體系中**公鑰的合法性檢驗**的責任
- 為每個使用公開金鑰的用戶發放一個**數位憑證**
- 數位身份認證原理
  - 註冊公鑰後，身分認證機構就向註冊者發一數位憑證 (在註冊者的數位身分證上加簽)

範例考題

關於存取控制措施，下列敘述何者不正確？

- (A)應建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序
- (B)組織應在符合資訊存取限制條件下，讓授權的使用者可指派分享的存取權限
- (C)對於每一種允許的遠端存取類型，都應先取得授權，建立使用限制、組態/連線需求及實作指引，並予以文件化
- (D)資訊系統無需對行動裝置之連線要求授權

存取控制大概可分為三類，系統、實體與網路存取控制。以下哪種行為是屬於實體存取控制？

- (A)讀取公司郵件
- (B)列印生產報表
- (C)進入機房巡檢
- (D)上網瀏覽新聞

新進員工好奇嘗試操作公司資訊系統，發現很多功能都無法使用。上述較可能的原因為？

- (A)系統有缺陷造成
- (B)最小權限原則
- (C)硬碟發生壞軌
- (D)系統感染電腦病毒

下列何種權限管理行為較不適當？

- (A)公司負責人擁有ERP所有系統的唯讀權限，並另外擁有最高管理者的帳號密碼
- (B) 採購主管擁有ERP採購系統除單據（紀錄）刪除外的所有權限，並擁有物料庫存數量的查詢權限
- (C) 資訊人員擁有ERP系統設定權限，並同時擁有ERP系統採購單據的新增、編輯、刪除權限
- (D)會計主管擁有ERP系統每月結轉權限

Faker是公司的資訊人員，主要職責為避免非法存取控制的資安事件發生。請問以下「不是」他應有的作為？

- (A)將多台電腦共用同一組存取密碼
- (B) 記錄所有登入的事件
- (C) 呼籲同仁在離開電腦時需上鎖
- (D)呼籲同仁切勿將自己的帳戶提供他人使用

下列何者不屬於實體控制（Physical Controls）層面？

- (A)門禁系統
- (B) 安全政策
- (C) 纜線保護
- (D)大樓保全或警衛

關於OTP（One-Time Password）的特性，下列敘述何者不正確？

- (A)不可預測
- (B) 使用一次
- (C)不可重複
- (D)能防止釣魚網站

身份認證主要是來證明使用者的身份，相關的機制設計主要包含三要素，請問下列何者不包含在其中？

- (A)Something you know
- (B) Something you have
- (C)Something you are
- (D)Something you need

使用通關密碼或是PIN碼來登入資訊系統，這是屬於下列何種身份認證方式？

- (A)所知之事
- (B) 所持之物
- (C)所具之形 - 靜態特徵
- (D)所具之形 - 動態特徵

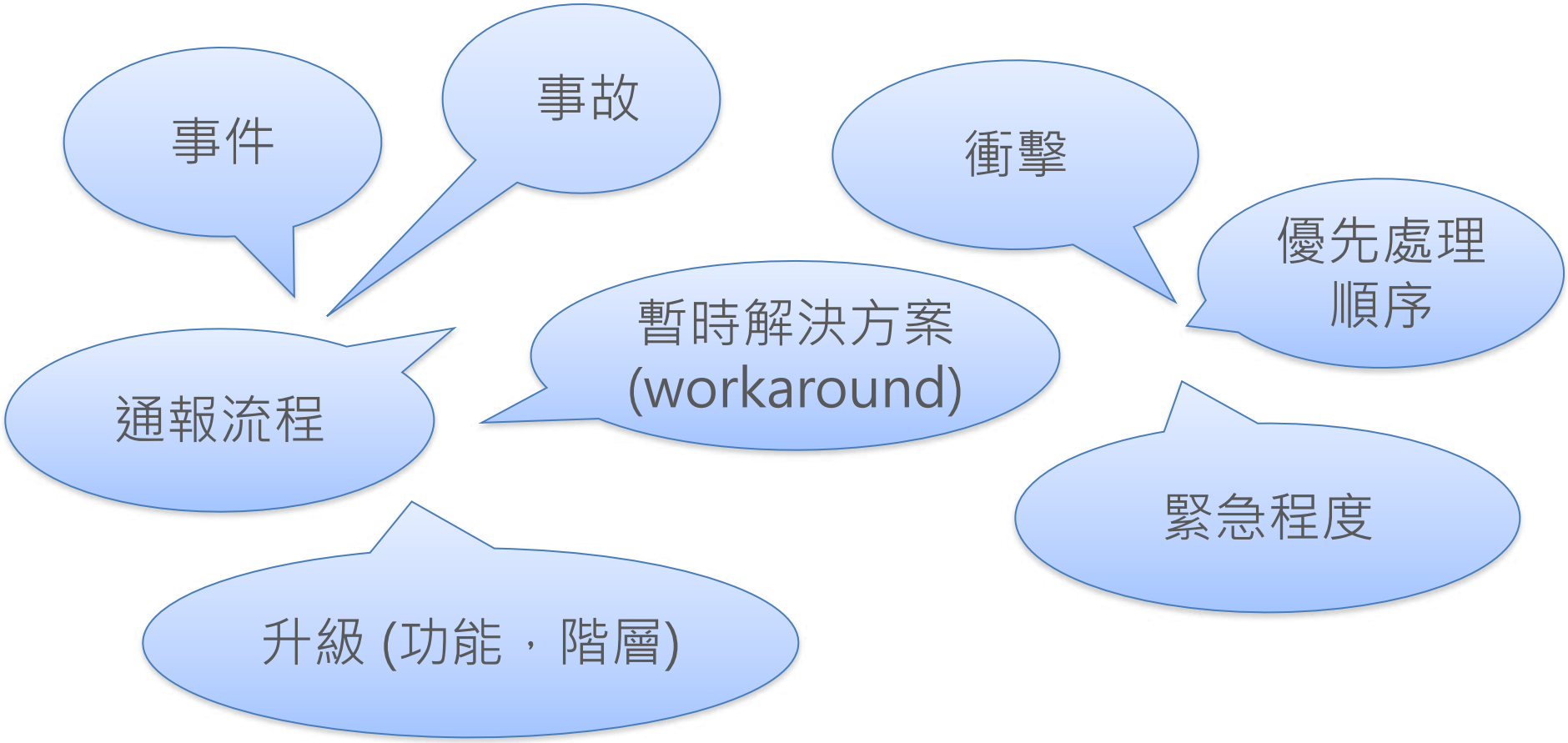
某家國防工業公司，員工被要求需使用智慧卡（Smart Card）和個人識別碼（Personal Identification Number, PIN）登入公司資訊系統，請問這家公司使用的是哪一種驗證方法？

- (A)時間基礎的一次密碼（Time-based One-Time Password, TOTP）
- (B) 多因子認證法（Multifactor）
- (C) 相互認證法（Mutual Authentication）
- (D)聯邦認證法（Federal Authentication）

評鑑主題四
事故管理與營運持續

1. 事件與事故管理
2. 備援與營運持續

重要字辭與定義



資安事故處理的目的

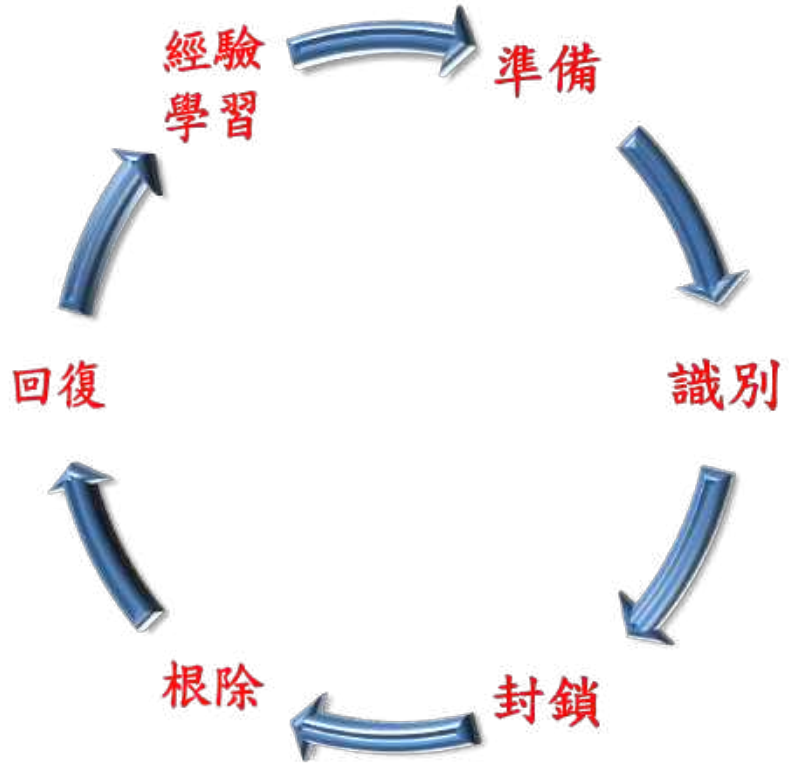
- 確認資安事故是否發生
- 降低對業務與網路服務的中斷時間
- 提供精準與及時的資訊
- 保障由政策與法律要求的權利
- 實作控制措施以維護監管鏈
- 讓法務組織可對惡意者提起訴訟

有效的資安事故處理計畫

- 定期重新審查計畫文件
  - 更新人員、科技及業務處理流程
- 訓練
  - 組織分工與權責、資訊安全技能、危機處理、數位鑑識與調查技能及溝通能力
- 財務支持
  - 預算、額外的設備、專業人員、員工薪資及訓練費用
- 演練
  - 定期驗證與修正作業流程

資安事故處理

- 識別
- 封鎖
- 根除
- 回復
- 經驗學習



資安事故處理程序 – 準備(1/2)

- 資安事故成功處理的關鍵是事前的「準備」
  - 組織資安事故處理小組
  - 建立資安事故處理策略
  - 設計資安事故處理程序
  - 建立溝通管道與方式
  - 蒐集所需資源
  - 練習、練習、再練習

資安事故處理程序 – 準備(2/2)

- 資安事故處理小組
  - 技術部門(IT、資訊安全及系統管理者)
  - 管理人員
  - 法務部門
  - 數位鑑識專家
  - 公共關係部門
  - 人力資源部門
  - 實體安全與維護部門
  - 通訊部門

資安事故處理程序 – 識別(1/2)

- **記錄 (第一步)**
- 識別意圖(故意或無意)
- 確認範圍
  - 識別哪些系統、人員及資訊資產被包含在處理的資安事故中
- 保留證據
  - 保護資安事故的事實
- 可疑的事故
  - 新增帳號、新建檔案及檔案的修改
  - 入侵偵測系統觸發的事件與防火牆存取紀錄
  - 效能變差、服務無回應及系統不穩定
- 監聽正在進行的攻擊行為
  - 透過網路封包的蒐集

資安事故處理程序 – 識別(2/2)

- 數位證據的取得
  - 採用被接受的磁碟映像複製工具(所有磁區的複製，配合雜湊函數以檢驗被複製出來的資料沒有被竄改)
  - 配合錄影機記錄螢幕顯示的內容與採證過程
- 識別出來的相關證物從發現到提出至法院必須有完整明確的監管紀錄
  - 每一項證據必須由可證明身分的人員所保管
  - 當保管人交接時必須被記錄
  - 在儲存體中的證物必須被保護，以免被污染或變更

資安事故處理程序 – 封鎖

- 當資安事故已被識別且相關證物監管鏈已被建立後，接下來就開始「封鎖」入侵來源，以避免災害擴大
- 識別可信任來源
  - 不只是來源網路地址或設備，也包含使用者
- 避免驚動入侵者以避免證據被銷毀
- 開始進行證據分析與數位鑑識
- 減緩攻擊的封鎖行動
  - 變更通行碼與權限
  - 變更主機名稱與IP位址
  - 將可疑的流量導到不存在的位址
  - 阻擋攻擊來源IP或網段
  - 在類似系統上更新修補程式
  - 關閉服務

資安事故處理程序 – 根除

- 一旦資安事故已被控制，接下來要從系統或網路中完全移除惡意程式
- 決定採用移除或回存方式
  - 是否可以完全移除乾淨
  - 備份資料中可能就存有惡意程式
- 強化防禦機制
  - 建立額外的偵測與防禦方法
  - 提升稽核紀錄的詳細程度
  - 在其他系統中尋找已發現的惡意程式
  - 更嚴謹控管存取來源

資安事故處理程序 – 復原

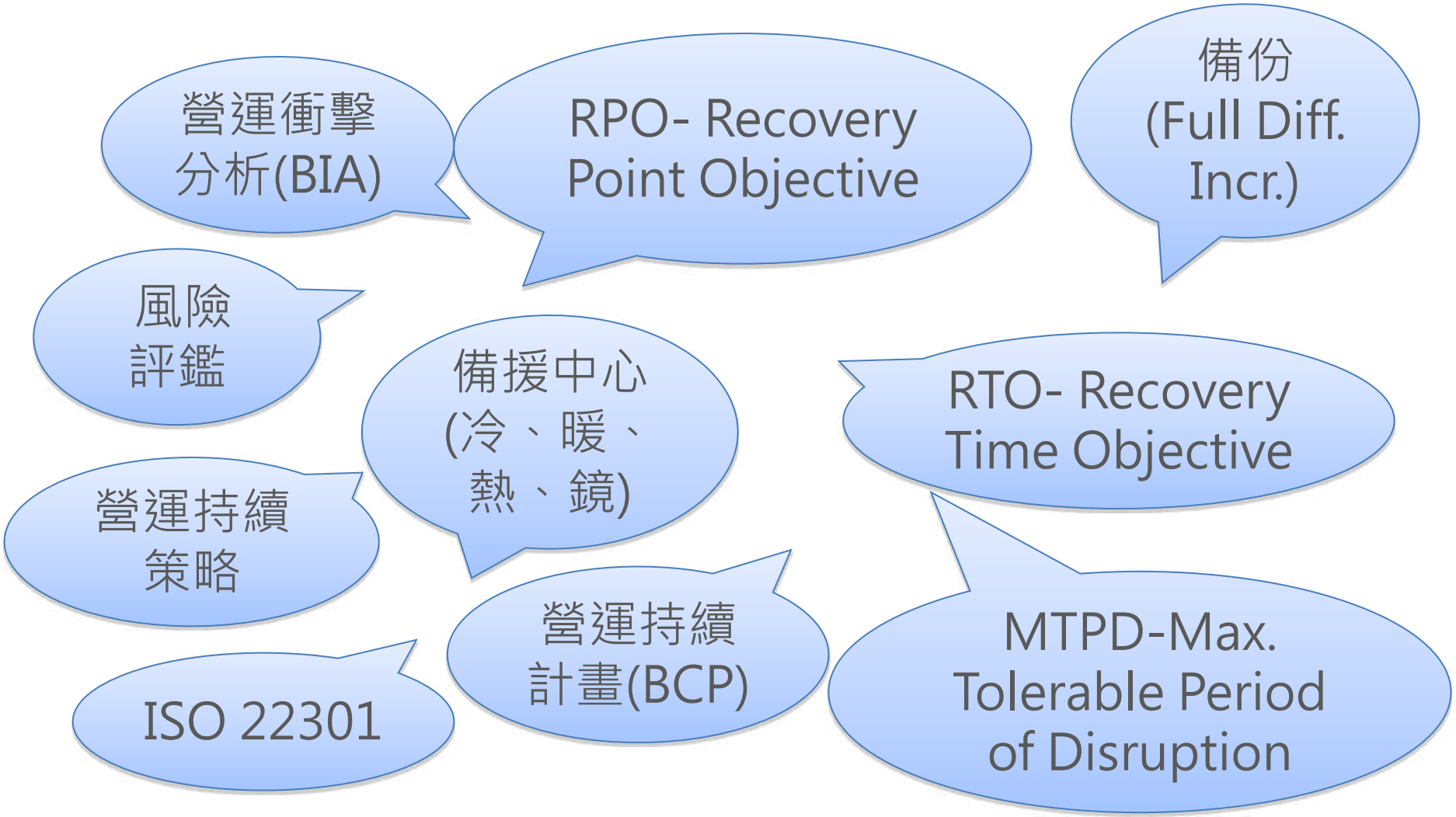
- 一旦威脅被根除，接下來應開始將業務與服務回復至正常運作狀態
- 加強監控以偵測攻擊是否再發生
  - 客製化入侵偵測規則
  - 在網路、主機及應用程式中，實作額外更詳細的稽核紀錄

資安事故處理程序 – 經驗學習

- 召開經驗學習會議
  - 在相關處理人員記憶猶新的情況下
  - 讓組織在資安事故中學習防護經驗
  - 建議修改相關政策或程序，以利未來安全防護機制實作時可避免重蹈覆轍

備援與營運持續

重要字辭與定義


營運衝擊分析(BIA)
RPO- Recovery Point Objective
備份 (Full Diff. Incr.)
風險評鑑
備援中心(冷、暖、熱、鏡)
RTO- Recovery Time Objective
營運持續策略
營運持續計畫(BCP)
MTPD-Max. Tolerable Period of Disruption
ISO 22301

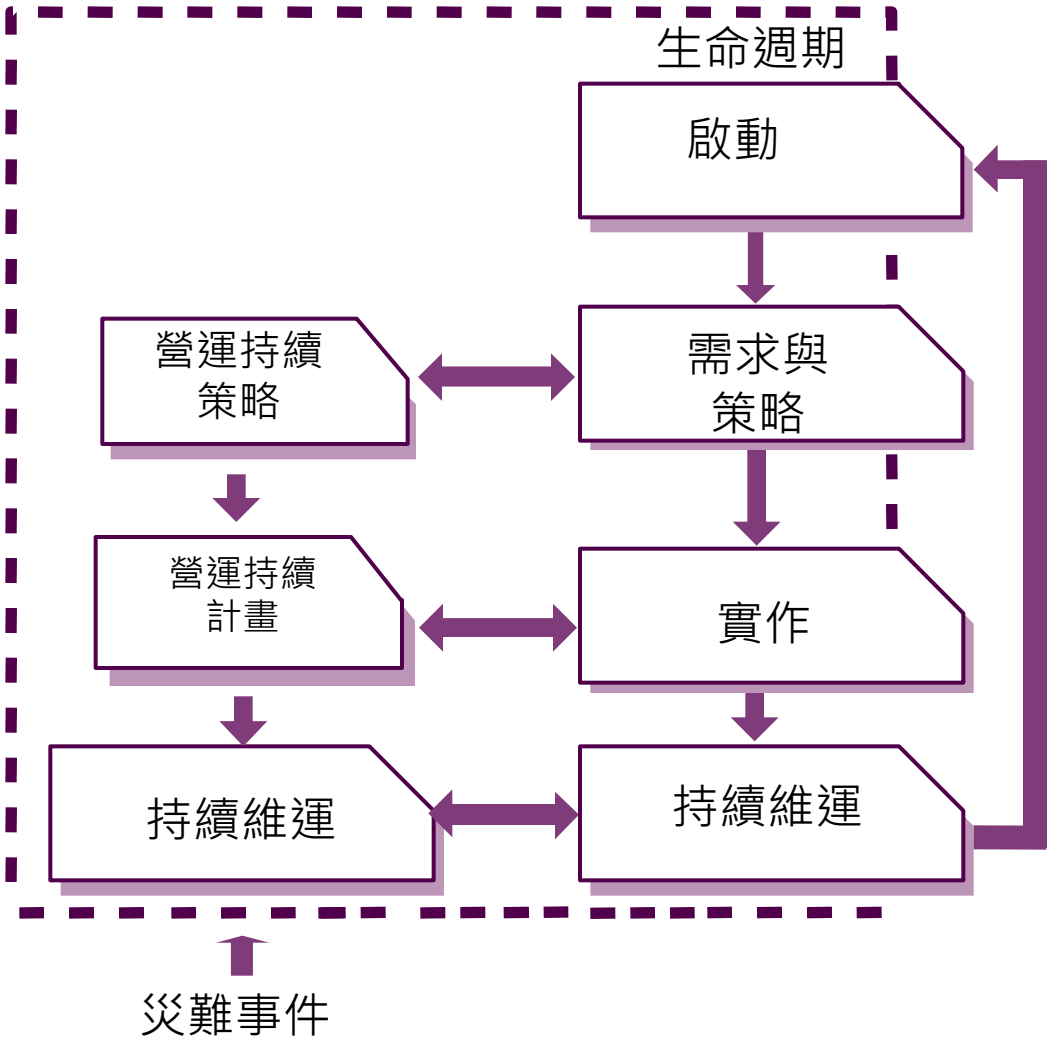
業務持續運作計畫的必要性

- 天災、人禍、意外
- 風險無所不在，未雨綢繆，有備無患

業務持續運作計畫之目的

- 防止業務活動中斷，確保重要關鍵業務流程不受重大故障與災難的影響
- 結合預防與復原措施，將風險造成的影響降低到可以接受的等級
- 分析災難、安全缺失及服務損失的後果。制定與實施應變計畫，確保在要求的時間內恢復業務流程
- 選用控制措施降低風險，限制破壞性事件造成的後果，確保重要作業能及時復原

營運持續管理生命週期



- 決定策略
- 範圍
- 啟動專案

- 營運衝擊分析
- 風險評鑑
- IT服務持續策略

- 發展 IT 服務持續性計畫
- 發展回復計畫與程序
- 風險降低實作
- 測試

- 教育訓練、認知訓練
- 審查、稽核
- 測試
- 變更管理

業務持續運作的需求

- 法律與規範的要求
- 定義範圍
  - BCP需要處理的災害類型：天災與人禍
  - 全部、特定區域及特定業務
- 參與角色
  - 計畫主要負責人
  - 各部門主管與高階管理人
  - IT部門、安全部門及通訊部門
  - 法務部門
  - 當災害發生時需要執行BCP計畫的部門都應參與BCP的發展

營運衝擊分析

- 營運衝擊分析(Business Impact Analysis)，簡稱BIA
- 用來瞭解當災害發生後的嚴重程度，
- BIA的步驟
  - 識別組織的關鍵業務功能
  - 計算關鍵業務
    - 最大可承受中斷時間 (Max. Tolerable Period of Disruption, MTPD)
    - 目標回覆時間(Recovery Time Objective, RTO)
    - 各營運活動可容忍資料遺失之期間(Recovery Point Objective, RPO)
    - 最低服務水準 (Min service level)

風險評鑑

- 識別
  - 所有會造成中斷大於「MTPD」的事件
- 例：
  - 台電大斷電
  - 水災
  - 地震
  - 機房大火

復原策略(1/4)

- 目的
  - 指導復原作業的規劃方式與規模(成本)
- 參考
  - 關鍵業務最大容許中斷時間
- 必須包含下列復原策略
  - 業務流程復原策略
  - 設施場所復原策略
  - 供應與技術復原策略
  - 使用者環境復原策略
  - 資料復原策略
- 業務流程復原策略
  - 其他業務處理流程(自動 vs 人工)
  - 業務處理流程重建

復原策略(2/4)

- 設施場所復原策略
  - Hot(數小時)、Warm(1天或更長)或Cold(數天) Site合約
  - 同業互惠合作、自建備援場所及自建分散式多重處理機制
  - 備援場所應有足夠合理的距離(避免同一災害同時受損)
- 場所備援方案比較

場所相關準備項目	Hot Site	Warm Site	Cold Site
空間已備妥	是	是	是
電力、網路及空調已備妥	是	是	是
軟硬體已就緒	是	部份	無
資料復原	需要	需要	需要
人員	無	無	無
所需復原時間	數小時或更短	1天或更長	數天

復原策略(3/4)

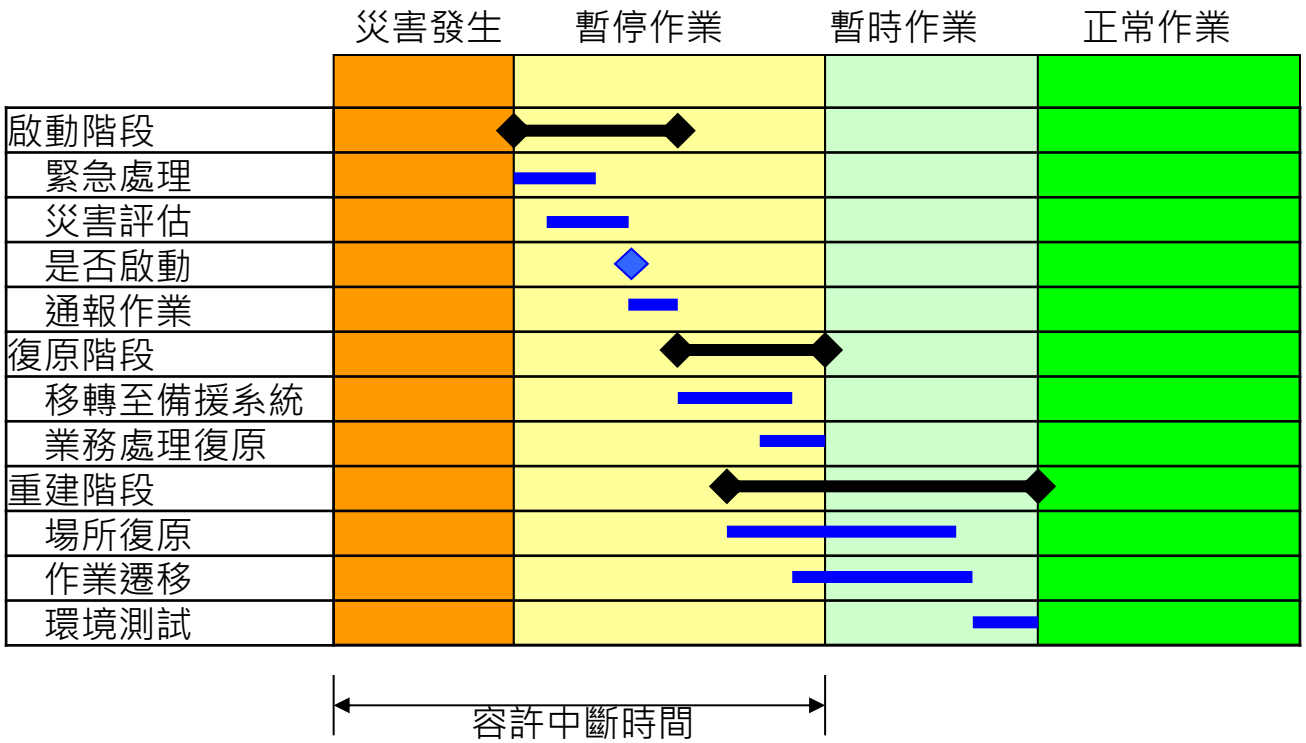
- 供應與技術復原
  - 網路與電腦設備
  - 語音與資料通訊
  - 人力資源
  - 人員與設備的運送
  - 作業環境(空調等)
  - 資料與人員安全
  - 耗材
  - 文件
- 使用者環境復原
  - 發展災害情況下的通報網
  - 識別關鍵使用者以利關鍵業務的運作
  - 必要時發展人員運送至備援場所的程序

復原策略(4/4)

- 資料復原
  - 備份
  - 異地備份
  - 異地備援
- 其他注意事項
  - 備援與復原機制的選擇應考量成本效益
  - 備份與備援機制的安全要求應與線上相同
  - 備份與備援機制應定期測試與演練

發展業務持續運作計畫(1/4)

- BCP時程



- 前言
  - 目標
  - 適用範圍
  - 角色與權責
  - 定義
- 啟動階段
  - 通報作業程序
  - 損害評估
  - 計畫啟動
  - 緊急處理程序
- 復原階段
  - 移轉到備援系統
  - 業務處理復原
  - 復原程序
- 重建階段
  - 場所復原
  - 環境測試
  - 作業遷移
- 附錄
  - 通報網路
  - 系統需求

發展業務持續運作計畫(2/4)

- 前言
  - 目標
  - 適用範圍
  - 角色與權責
    - 損害評估小組
    - 法務小組
    - 媒體公關小組
    - 搬遷小組
    - 復原小組
    - 安全小組
    - 網路與通訊小組
  - 應明確定義與外部關係人溝通的窗口
    - 媒體
    - 客戶
    - 緊急救難服務
    - 供應商

發展業務持續運作計畫(3/4)

- 啟動階段
  - 緊急處理程序
    - 人員疏散程序
    - 急救步驟(CPR)
    - 依不同災害定義相關處理程序(火災、地震及輻射等)
  - 執行損害評估決定是否啟動BCP
  - 復原人員的通報程序
- 復原階段
  - 主要目的是讓關鍵業務回復至暫時可運作的狀態(Min. service level)
  - 復原程序應包含系統回復至可運作狀態的每一步動作，而且必須在可容許中斷的時間 (MTPD)內完成 (但組織有時會自訂更短的RTO)

發展業務持續運作計畫(4/4)

- 重建階段
  - 主要目的是讓關鍵業務從暫時運作狀態，在原地點或其他地點回復到一般正常作業
  - 在重組後的新環境應執行相關系統與作業測試
  - 由較不重要的業務功能先移轉至新環境

測試與演練(1/3)

- 目的
  - 檢驗BCP的可行性並補強未考量之缺陷
  - 確保在可容許中斷時間內可完成復原作業
  - 讓相關人員熟悉相關災害復原的作業
- 測試方式
  - 檢核表測試(部門個別檢視BCP工作)
    - 無法得知不同部門間的合作與溝通結果
  - 整合測試(各部門一起檢視BCP過程)
    - 無法模擬不同的災害類型或損壞情況來應變
  - 狀況模擬測試(紙上模擬災害情境與復原過程)
    - 缺乏實際執行復原與重建的經驗

測試與演練(2/3)

- 測試方式
  - 並行測試(實際將部份系統及業務移轉到備援場所，但原場所仍持續運作，可實際測試是否能在最大容許中斷時間內復原) ，**可能導致部份業務無法運作**
  - 完全中斷測試(中斷原場所系統及服務，實際摸擬BCP的復原階段與重建階段)
    - ➢關鍵業務必須中斷一段時間
    - ➢部份業務可能無法及時復原運作
    - ➢重建階段演練時，資料若需回存到原系統，可能導致資料錯亂
- 測試與演練的時機
  - 定期(每年)
  - BCP有重大變更時可額外進行

測試與演練(3/3)

- 人員訓練的需求
  - BCP的目的
  - BCP的角色與權責
  - 復原小組間的協調與溝通
  - 處理回報程序
  - 安全要求
  - 各小組在不同階段中的工作
  - 特定人員在不同階段中的責任
- 在測試與演練中學習
  - 測試結果與經驗應被記錄
  - 彙整測試結果並於測試後進行檢討，以改善現有BCP的缺失

維護業務持續運作計畫

- 目的
  - 確保BCP可符合組織現況需求
- BCP會因下列因素變成不符現況需求
  - 科技的快速變動或軟體升級
  - 組織組織變更(分工方式、合併或裁減)
  - 人員異動
- 如何確保BCP可符合現況
  - 指派專責人員或部門負責持續更新
  - 將計畫的審查加入組織定期稽核項目
  - 在變更控制程序中審查是否需要更新BCP

如何判斷BCP是正確且有效的？

- 在可容許中斷時間內可以復原
- 在暫時備援環境中的作業是適當可行的
- 備份資料可被成功回存
- 緊急處理人員、服務人員及合約要求人員在可接受的時間內可以到達
- 小組成員瞭解現有BCP內容
- 小組成員可執行BCP的職責
- BCP與現況需求符合

範例考題

關於資安事件發生前的預先準備計畫，下列敘述何者不正確？

- (A)應訂定災害預防計畫
- (B) 應規劃建置資通安全整體防護環境
- (C)利用防火牆等設備隔離受害主機
- (D)應定期實施安全稽核

依據「行政院國家資通安全會報通報及應變作業流程」，各級政府機關於通報並著手處理資安事件後，若判定為1級或2級事件，應於幾小時內完成復原或損害管制？

- (A)24小時
- (B)48小時
- (C)72小時
- (D)96小時

請問發生資安事故的第一步驟為何？

- (A)蒐集證據
- (B) 記錄
- (C)將系統回復
- (D)檢討原因

當組織遇到資訊安全事件時，必須採取正確、有效的處理程序。處理事件的第一步驟是？

- (A)問題隔離
- (B)問題分析
- (C)問題分類
- (D)問題調查

您是資安經理，正在分析異地備援的模式，公司將以最低成本考量，您將建議下列何者方案？

- (A)冷備援站（Cold Site）
- (B) 暖備援站（Warm Site）
- (C) 熱備援站（Hot Site）
- (D)冗餘備援站（Redundancy Site）

下列何者與營運持續計畫之規劃的關聯度較低？

- (A)風險評鑑的結果
- (B)可接受RTO（回復時間目標）、RPO（回復點目標）的標準
- (C)營運衝擊分析的結果
- (D)資訊資產的盤點結果

下列何者是營運持續管理的國際標準？

- (A)ISO 9000
- (B) ISO 14000
- (C)ISO 20000
- (D)ISO 22301

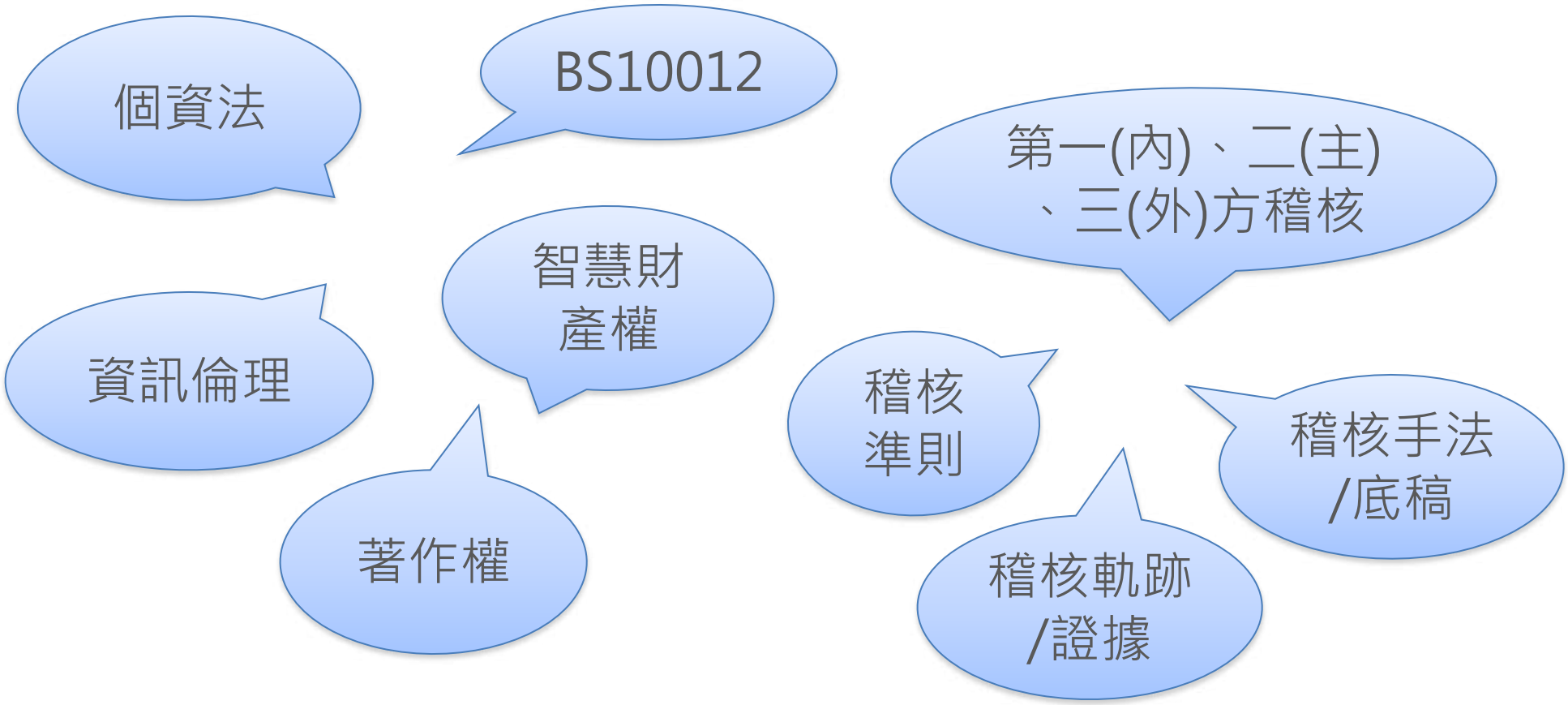
在訂定企業營運持續計畫時，下列何者是首要進行的事？

- (A)訂定災難復原計畫（Disaster Recovery Plan, DRP）
- (B) 執行營運衝擊分析（Business Impact Analysis, BIA）
- (C) 獲得高階管理階層的支持
- (D)鑑別關鍵性業務

評鑑主題五
法規遵循與資訊倫理

1. 隱私保護與智慧財產權
2. 資訊倫理、法規遵循與稽核

重要字辭與定義



個人資料定義

- 個人資料(以下簡稱個資)，指任何關於可識別個人或足資識別該個人之資料。依據我國個資法之定義，指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料
- 在規範地區的部份，只要是具有中華民國國籍的自然人，個人資料不論在境內或境外，皆受此法保護

特種個人資料定義

- 特種個人資料(以下簡稱特種個資)，依據我國個資法定義，包括個人資料中有關病歷、醫療、基因、性生活、健康檢查及犯罪前科等內容，特種個資除符合我國個資法中所列之特定情形外，不得蒐集、處理或利用
- **可蒐集、處理、利用敏感性資料的情況(參考個資法第六條)**
  - –法律明文規定
  - –執行法定職務所必要，且有適當安全維護措施
  - –自行公開或已合法公開
  - –基於醫療、衛生或犯罪預防的目的，為統計或學術研究而有必要，且經一定程序所為蒐集、處理或利用

個人資訊管理系統(PIMS)

- BS 10012 PIMS由英國標準協會基於OECD、APEC及資料保護法對於個人資訊管理制定而來
- BS 10012與其他國際標準一致，定義了個人資訊管理系統(Personal Information Management System PIMS)的要求
- 採用過程方法來建立、施行、運作、監控、審查、維護及改善組織的個人資訊管理系統(PIMS)
- BS 10012除針對資通訊(ICT)技術的標準要求，亦從法律面、管理面與流程面對於個人資訊的管理，在符合國內 個人資料保護法及組織所應遵循產業之最佳實務要求下，進行**保障組織所持有之個人資訊**

ISO/IEC 29100 資訊安全技術-隱私框架標準

- 科技化社會運用個資情形普遍，隱私保護重要性愈來愈高
- 我國已全面實施的個人資料保護法來其他國家也積極透過法制及管理來平衡個人資料之運用及隱私保護
- 個人資料及隱私的保護不是單純的法律要求，需要與科技發展整合，以真正落實個資與隱私的保護
- ISO/IEC 29100:2011適用於從事指定的採購、架構、設計、開發、測試、維護、管理和運營的自然人和組織，都需要**PII(Personally identifiable information)**處理隱私控制的訊息、通訊技術系統或服務

個資清查

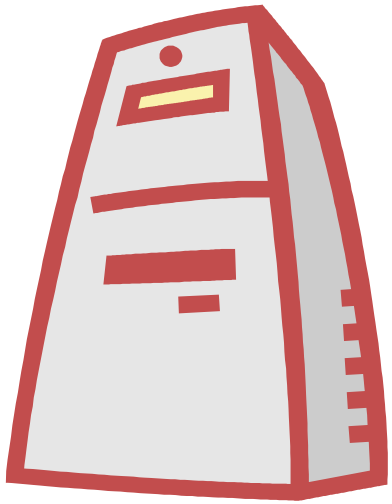
- 清查組織內的個資
  - 透過管理面的盤查方式：擁有者填報與造冊
  - 透過搜尋檢索技術：全文檢索功能的工具
- 去個資化/去識別化
  - 不影響作業的前提下，儘量把個資資料去個資化。
  - 也就是刪除或分割資料，讓資料不再具有個資的特性，達到保護的目的。

電子資料蒐集之安全威脅

- 未落實資料分級
  - 電子檔案未依分級受妥善防護，導致資料外洩、遭竄改或毀損
  - 發生資安事故後，不易追蹤來源與釐清責任，並進行補強矯正措施
- 引用不當資料
  - 所蒐集而得之資料不當，導致電子檔案內容發生謬誤
  - 蒐集之資料未獲授權，侵害他人版權
  - 不當使用個人隱私資料，違反個資法

檔案存取授權

- 讀取權限：可開啟檔案，讀取內容
- 列印權限：可將檔案印出為紙本或轉為其他電子檔案格式(如PDF)
- 複製貼上權限：利用複製與貼上，可將檔案內容複製至另一個未受管控的檔案中



電子資料處理之安全威脅

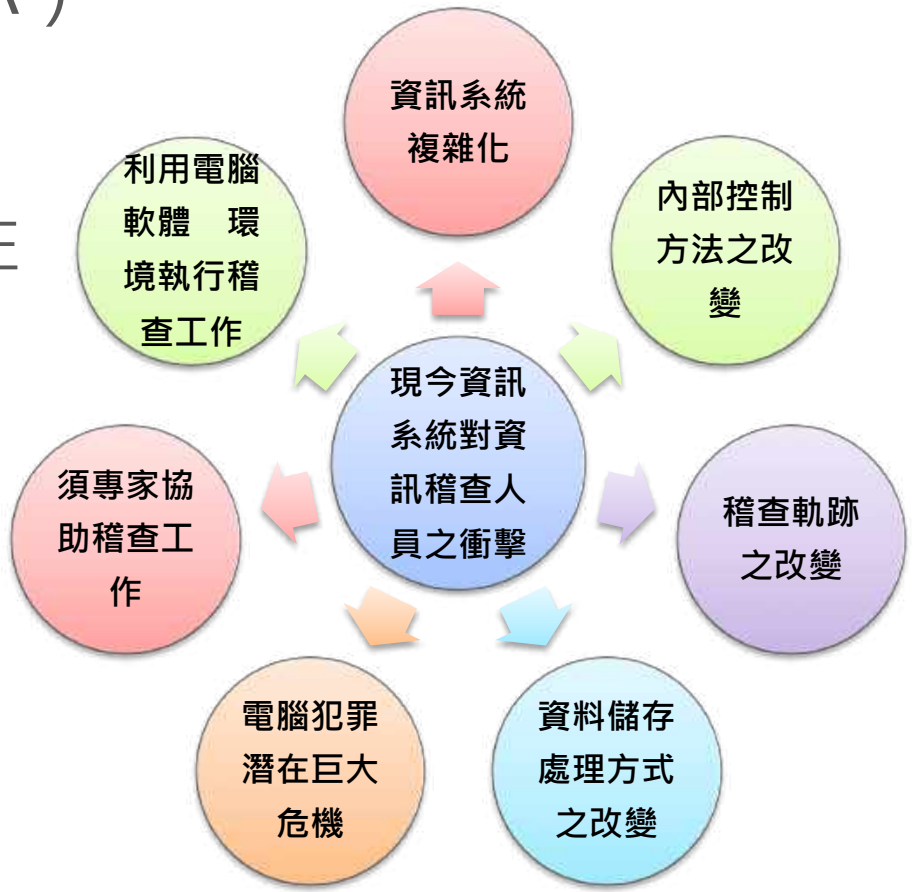
- 資料外洩
  - 檔案遭列印為紙本流出
  - 駭客透過軟體的暫存檔案進行資料竊取
- 資料毀損
  - 編輯作業操作疏失，導致資料遺失
- 資料內容錯誤
  - 人為操作的疏忽導致內容不正確
  - 檔案未進行版本管控，缺乏追蹤修訂紀錄，發生錯誤後，不易修補

電子資料處理之防護

- 於電腦中安裝暫存檔清除工具，可減少資訊殘存問題之發生
- **確認雲端儲存的資料在合約終止後是否完全清除**
- 文件管理系統具有良好的版本管理功能
- 存取權限管理
  - 透過相關工具軟體
  - 遵循「**最小揭露原則**」，僅供存取職務所需之最少資料
- 稽核工具
  - 記錄使用者的存取行為
  - 嚇阻非授權存取與具有權限人員進行不合理之非法存取
- 防範內賊

稽核查核目的

- 優良管理系統不在於達到100%零缺失，而是具備不斷持續改善的能力（PDCA）
- 驗證是否符合規定的要求
- 評估管理系統之實施有效性
- 為管理審查提供相關資訊
- 加強整體安全意識
- 降低管理系統失效的風險
- 提供管理系統改善之機會



稽核基本概念

稽核

係指一個有能力且獨立的人員，以系統化程序方式來執行，主要目的為取得及評估有關經濟個體或事件之證據，以支持表示意見及提出符合準則報告之確認性聲明。

稽核步驟

經過適當規劃、全面性風險評鑑、研擬稽查工作底稿、收集證據、依證據評估控制強弱及準備稽查報告（以客觀地態度表示意見予管理當局）、適當的資源與時程來執行後續追蹤。

稽核類型

1. 第一方稽查（內部稽查）
   組織對自己之業務流程進行稽查
2. 第二方稽查（外部稽查）
   為主管組織對下屬或同儕，如：組織對其委外廠商之業務流程進行稽查
3. 第三方稽查（驗證稽查）
   由獨立驗證組織（如BSi）對組織業務流程進行稽查工作

稽核員基本原則

道德行為

資安稽查工作各方面，都應盡職業上應有之注意，及遵循職業道德規範及專業稽查準則。

專業

稽查人員應具有資訊安全與之認知、執行稽查工作之技巧及知識，藉由充分且持續之專業教育訓練，以維持其專業技術能力。

謹慎客觀

稽查人員對於稽查所見應保持客觀、謹慎求證之態度。

獨立性

稽查人員對於涉及稽查之任何事項，在態度及言行表現及實質（需兼顧組織及職能）上皆應獨立於被稽查部門（或人員）。

證據

藉由蒐集並評估證據的過程，以決定是否達成目標。

稽核之職責

GDPR

- 2018/5/25
- General Data Protection Regulation
- 保護以及加強**歐盟**成員國人民的資料隱私，以及重塑整個地區內的組織處理資料隱私的方法
- 雖然在歐盟，但**網路無遠弗屆**的特性，讓資料本身根本沒有地域性可言

GDPR (續)

- 「**被遺忘權**（right to be forgotten）」
  - 是一種在歐盟已經付諸實踐的人權概念
  - 可以要求控制資料的一方，刪除所有個人資料的任何連結（link）、副本（copies）或複製品（replication）
- 「**資料可攜權**（Right to data portability）
  - 意思是用戶可以將A服務的資料，轉移到B服務上，這也就是為什麼Instagram最近推出資料打包備份功能、蘋果推出管理個資工具

GDPR (續)

- **保護個資範圍**
  - **個人身分、生物特徵：**
    - 例如電話號碼、地址、車牌、病歷資料、指紋、臉部辨識、視網膜掃描、相片、影片、電郵內容、問卷表單等，甚至社會認同、文化認同、地理位置等，只要是一個人所能產生出的任何資料，幾乎都被重新定義為個人資料並受到保護
  - **線上定位資料**
    - 例如 Cookie、IP 位置、行動裝置 ID、社群網站活動紀錄等

其他重要法律

- **智慧財產權**
  - Intellectual Property Rights，簡稱「IPR」
  - 人類智慧創造出來的無形的財產
    - 主要涉及版權、專利、商標等領域
    - 音樂和文學等形式的藝術作品，以及一些發現、發明、詞語、詞組、符號、設計
    - 分為工業產權與版權兩類，工業產權包括發明（專利）、商標、工業品外觀設計和地理標誌，版權則包括文學和藝術作品

其他重要法律

- 專利法
  - 「專利」是專利權的簡稱，為專有之利益及權利，國家授與發明人在一定時間內享有排他性之製造、利用、販賣該項發明的權力
  - 三個特點
    - **專有性或排他性**：權利人享有佔有、使用、收益和支配的權利。其他人未經權利人許可，不得利用此權。
    - **地域性**：權利人享有的權利，只有在核准該權利所屬的領土有效。美國的專利在台灣領土上無效
    - **時間性**: 除商標可依法延展外，專利權都有一定的期限。法律規定的期限屆滿以後，專利權即告終止

其他重要法律

- **商標法**
  - 商標專用權的簡稱
    - 是指商標使用人依法對所使用的商標享有的專用權利
    - 商標註冊人依法支配其註冊商標並禁止他人侵害的權利，包括商標註冊人對其註冊商標的排他使用權、收益權、處分權、續展權和禁止他人侵害的權利
    - 財產所有權，商標權可以分解為
      - 占有權 ：我國需申請在先，並獲准註冊。(但部分國家只要證明先使用即占有)
      - 使用權：排他性，未經所有人許可，不得在相同或類似商品使用
      - 收益權：可透過合約，許可他人使用，而取得代價(收費)
      - 處分權 ：轉讓、贈予、放棄

其他重要法律

- **著作權**
  - 在我國，“著作權”與“版權”為同一法律概念
  - 是指文學、藝術、科學作品的作者依法對他的作品享有的一系列的專有權
  - 著作權是一種特殊的民事權利
    - 也包括法律賦予表演者、音像製作者 廣播電臺、電視臺或出版者對其表演活動、音像製品、廣播電視節目或版式設計的與著作權有關的權利
  - 著作權是在作者的作品創作完成之後，即**依法自動產生，而不需要經過任何主管機關的審查批准**

資訊倫理

- 討論人們對資訊的態度以及行為，應用於電腦的使用、資訊科技、資訊系統、資訊網路的倫理規範
  - 資訊倫理不同於一般的法律，資訊倫理是屬於一種自律、自我的約束態度
- PAPA 理論
  - 1986 美國梅森提出，包含了隱私權(Privacy)、正確性(Accuracy)、財產權(Property)及使用權(Accessibility)，成為了資訊倫理重要的主軸

範例考題

先進的網路技術，開啟了個人電腦使用挖掘大量資料的可能性，因此能比過去難以想像的大規模及精準地侵犯個人隱私。下列何者不算個人隱私？

- (A)醫療、健康狀況
- (B)性生活
- (C)財務情況、社會活動
- (D)證件上照片

下列何種不是智慧財產相關的法令規範？

- (A)專利法
- (B) 著作權法
- (C) 商標法
- (D)公司法

下列何者不是個人資料的當事人可行使的權利？

- (A)查詢當事人的個人資料
- (B) 查詢親友的個人資料
- (C) 請求製給複製本
- (D)請求補充或更正

請問下列敘述何者不屬於稽核員的主要工作？

- (A)依據稽核規劃與時程執行稽核活動
- (B)在稽核的過程中，紀錄相關發現與待確認事項
- (C)針對前一次稽核活動中的發現事項，規劃並執行相關的矯正預防作為
- (D)在稽核結束會議前，與受稽者再次釐清並確認相關稽核發現事項

組織內部的人員擔任稽核人員，進行內部稽核，又稱為？

- (A)第一方稽核
- (B)第二方稽核
- (C)第三方稽核
- (D)驗證稽核

請問下列何者不可作為稽核證據？

- (A)受稽人員口述
- (B) 檢視紙本紀錄之結果
- (C) 利用稽核工作檢測之結果
- (D)稽核人員之主觀判斷

問題與討論

敬請指教