ISMS資訊資產管理暨資產價值鑑別課程

資深顧問師 陳威州 (Joe Chen)

ISO27001/BS10012主導稽核員

曾任區域教學醫院資訊部門主管

曾任上櫃公司資安部門理級主管

Mobile: 0972-387776

E-mail: cyword0920@gmail.com

課程大綱(Agenda)

- 資訊資產概述
- 資產登錄
- 資訊資產(書面&數位紀錄)
- 軟體資產(電腦系統)
- 硬體資產
- 人員資產
- 資產價值評估

課程安排

時間	規劃課程內容	備註
09:00~09:20	資訊資產概述	
09:20~09:40	資產登錄	
09:40~10:00	資訊資產(書面&數位紀錄)	
10:00~10:15	軟體資產(電腦系統)	
10:15~10:30	硬體資產	
10:30~10:40	人員資產	
10:40~10:50	中場休息	
10:50~11:40	資產價值評估	
11:40~12:00	課程評量	紙本評量

第一章 資訊資產概述

前言（1/2）

- 資訊是企業的命脈，許多企業甚至是國家重大民生設施，例如電力、航空、銀行等，都需依賴資訊系統才得以運行，假若資訊遭受破壞或中斷，這些企業將受重大傷害。例如前一陣子美國大停電、日本股市大當機，都是因為資訊系統造成國家重大損失。
- 資訊需要依靠硬體、軟體、人員、電力、網路與其它設施等資產才能運行。

前言（2/2）

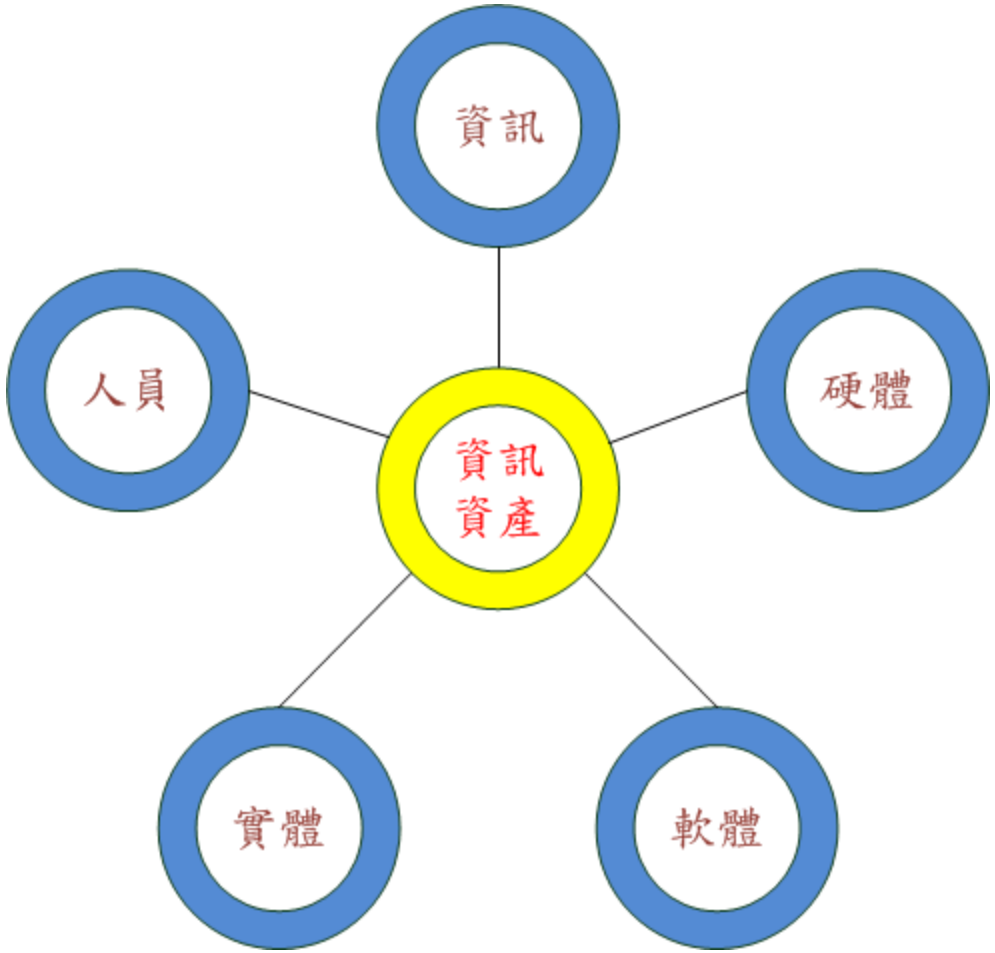
- 資訊資產管理的目的：

對組織的資訊資產實行並維持適切的保護

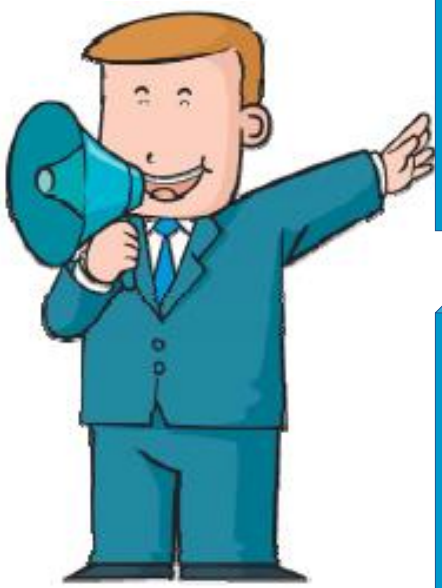
保護資訊資產 ➡ 保護資訊安全

資訊資產類別（1/3）

資訊資產的類別有哪些呢？



資訊資產類別（2/3）



資訊記錄

資料庫內容、資料檔、系統規劃與設計文件、使用與操作手冊、合約以及教育訓練教材等。

電腦系統

資訊中心與各使用單位之電腦作業系統、應用系統、開發工具、套裝軟體、公用程式等。

實體

指與資訊相關之實體空間，例如辦公室、機房...等，以及與相關設備，例如：電腦、通訊、網路，以及其它技術設備...等。

資訊資產類別（3/3）

人員

- 公司人員：系統開發、系統管理、設備保管人員、一般使用者、聘僱人員等。
- 外部人員：承包商與業務合作夥伴。

硬體

一般硬體、通訊設備、儲存媒體、個人電腦、可攜式電腦、伺服器、資安設備、網路設備、電腦保護設施、...。

第二章　資產登錄

資 產 登 錄

目的：確保資產被識別並納入管理

1. 清點

2. 登錄

3. 異動

清點步驟

教育訓練

針對清點工作負責人說明：

1. 清點工作意義與目的。
2. 資產分類類別與內容。
3. 清點工作的實施方式（編組）

開始清點工作

- 依業務內容，由資產所有人或保管人負責清點。
- 將清點結果填入—資產清冊

匯總資料

- 由ISMS推動小組成員逐條檢討，剔除重複或不適當項目。
- 彙總並適當維護此資產清冊。

資產清冊之製作與維護

資　產　清　冊

製作人員：王大年
更新日期：2018.02.10

編號	名稱	類別	數量	使用單位	保管單位	風險擁有者	風險擁有者	資產評估	資產價值
I010001	電子公文主機	硬體	1	各組室	資訊科	資訊科	資訊科	(C.I.A)	9

1. 基本資料

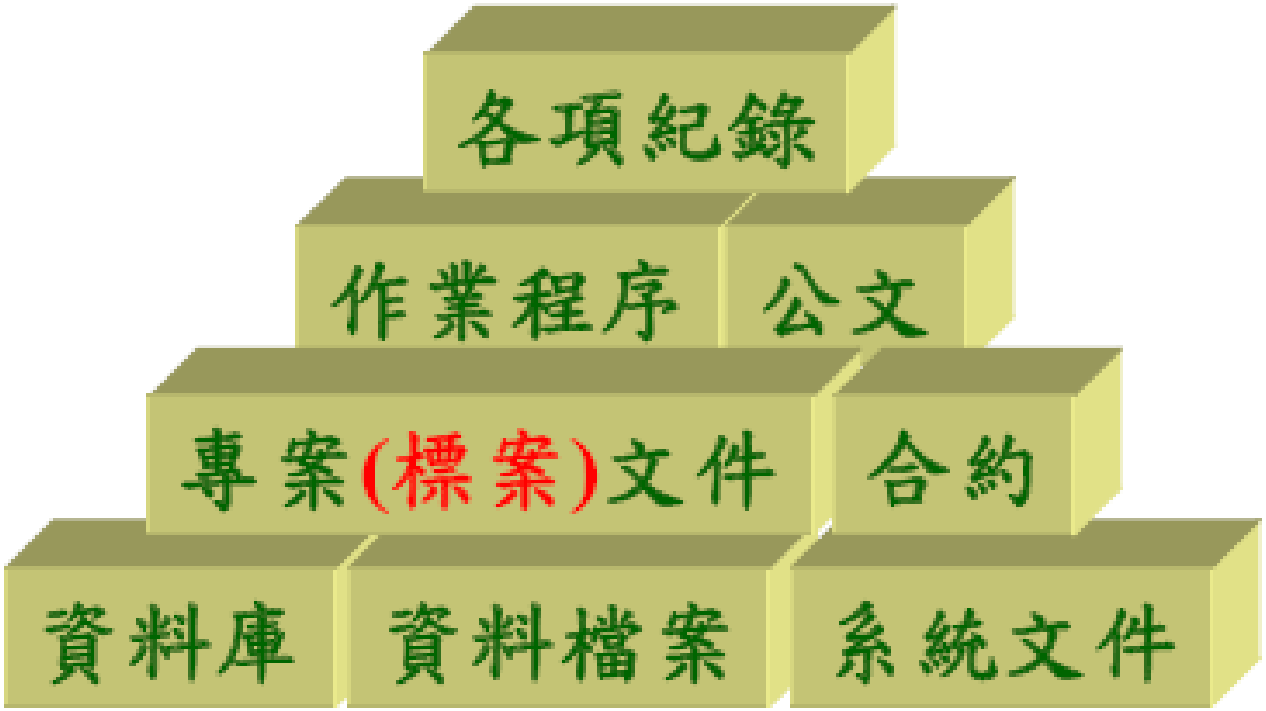
2. 使用單位

3. 權責人員

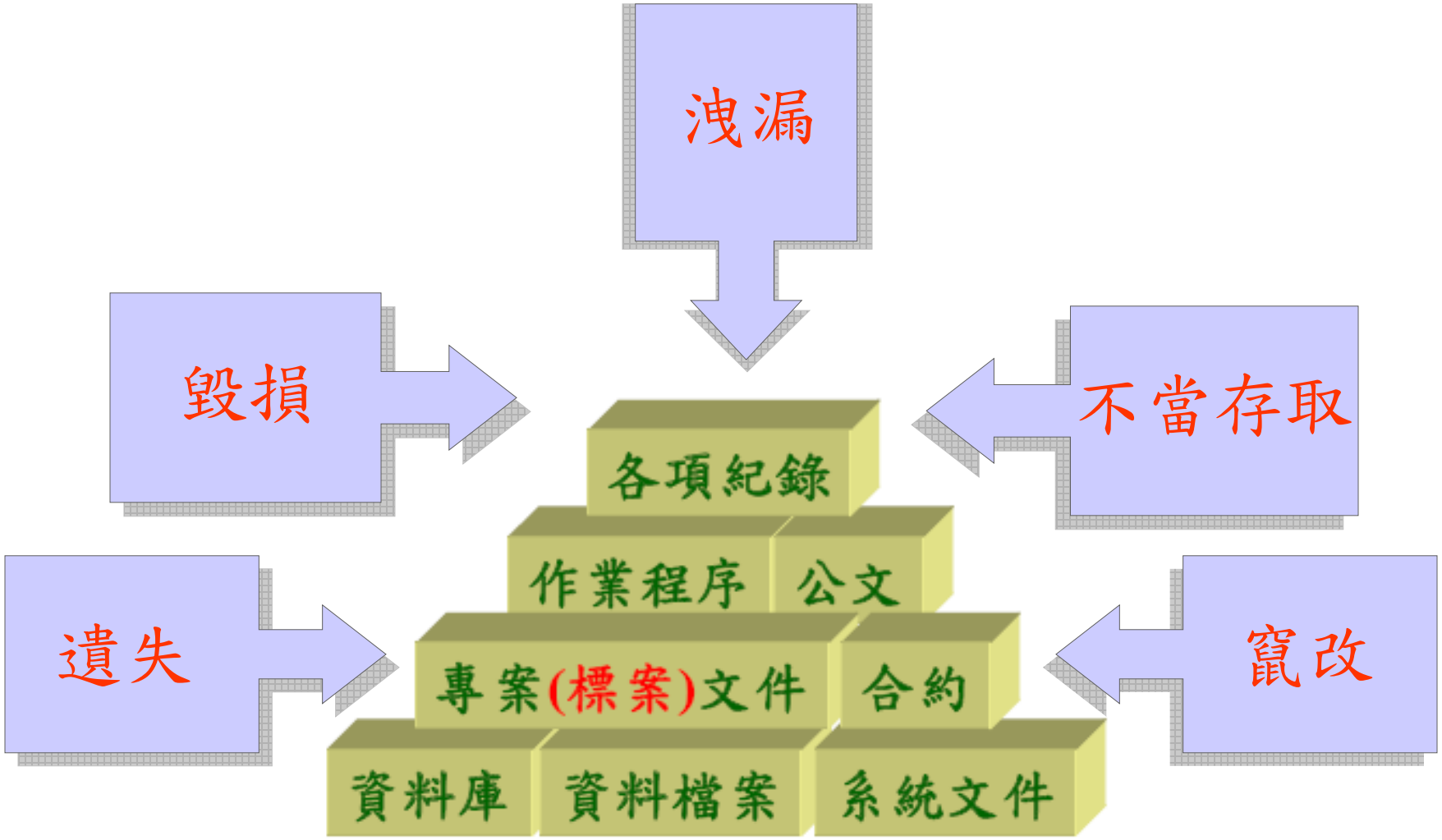
4. 價值重要度

第三章 資訊資產(書面&數位紀錄)

資訊記錄-資產範例



資訊記錄-常見資安威脅



資訊記錄–資安措施

1.分級

2.標示

3.加密

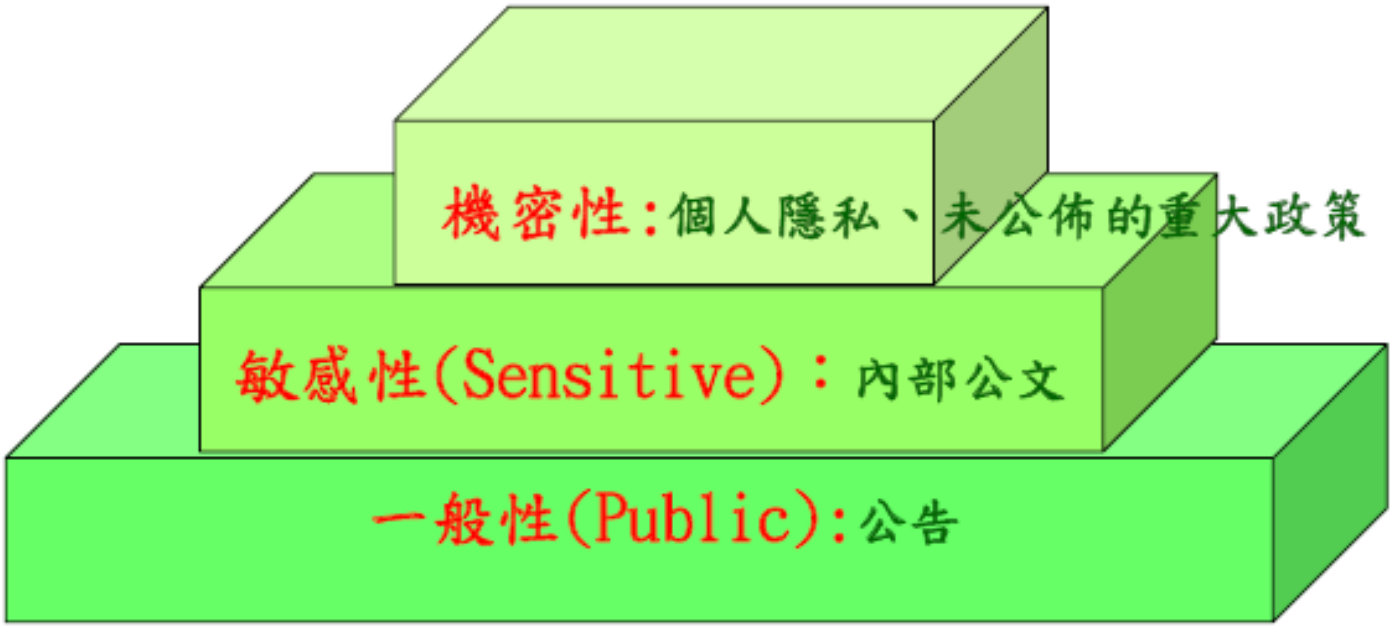
4.備份

5.實體隔離

6.其他

分級的範例與規範

我國資訊安全分級，依據行政院及所屬各機關資訊安全管理規範，可區分為：



資訊備份

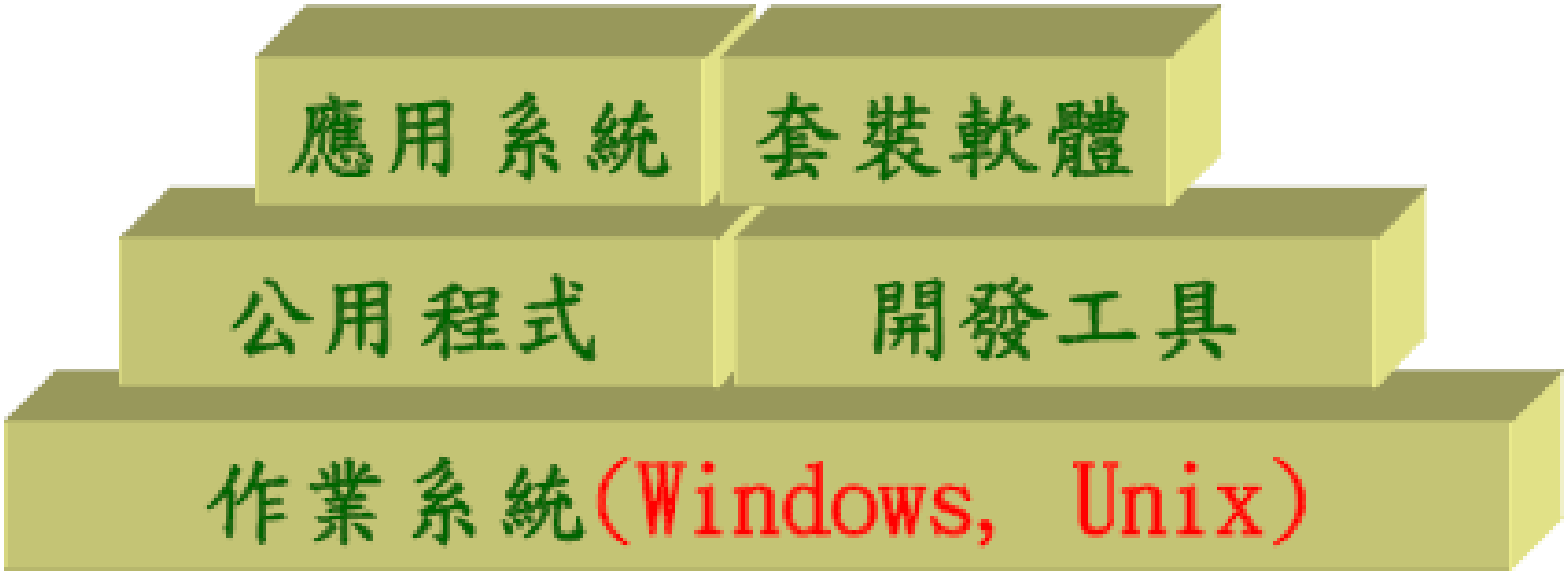
- 目標：
  - 確保當資訊遭毀損、竄改、遺失時，可以回覆原有資訊。
- 管理重點：
  - 備份頻率：日、周、月
  - 備份容量：增加備份、full backup
  - 備份測試：定期、不定期
  - 異地存放：30公里以外

其它資安措施

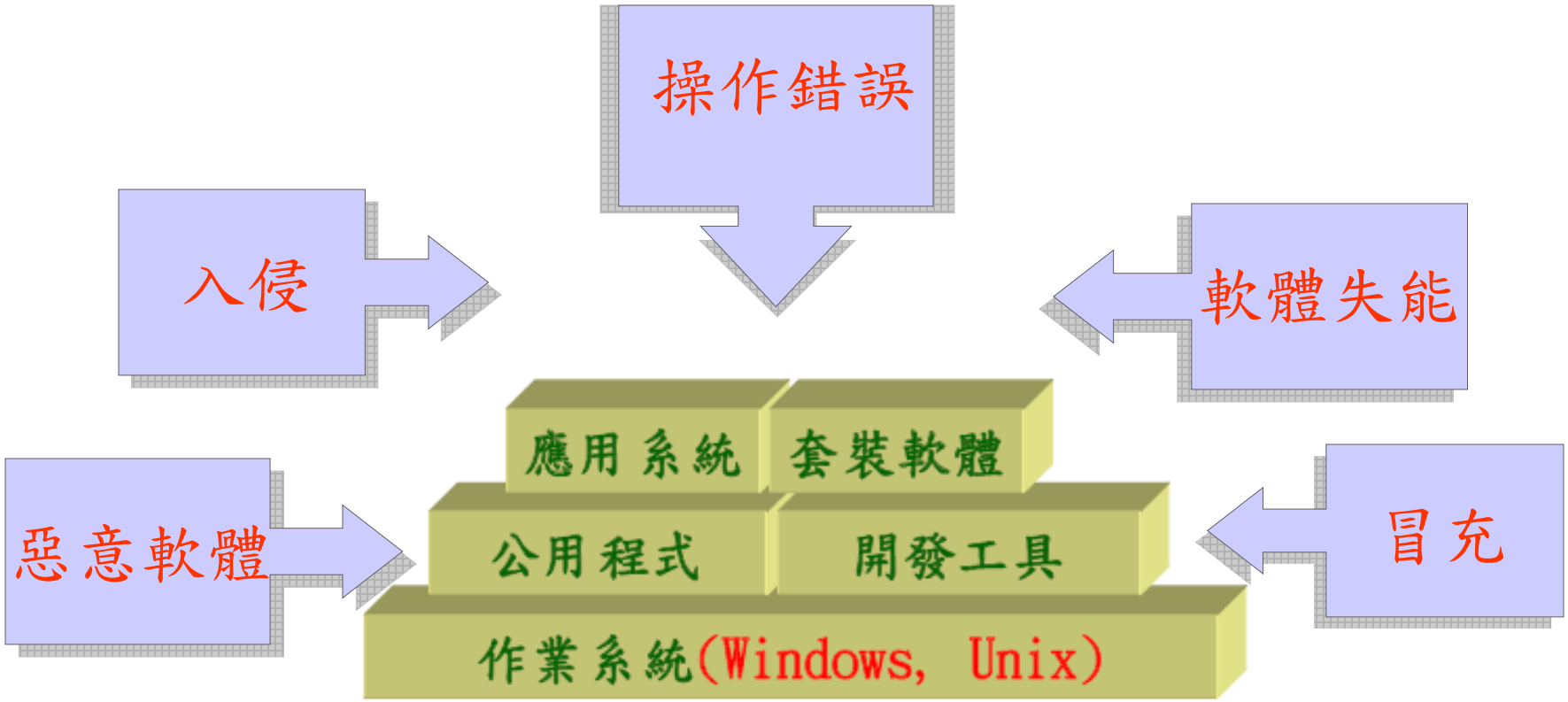
- 實體隔離
  - 抽屜、櫃子、保險箱、檔案室
  - (低----- <- 價值 -> ----高)
- 桌面淨空
- 螢幕保護程式
- 提高警覺

第四章 軟體資產(電腦系統)

電腦系統-資產範例



電腦系統（軟體）-常見資安威脅



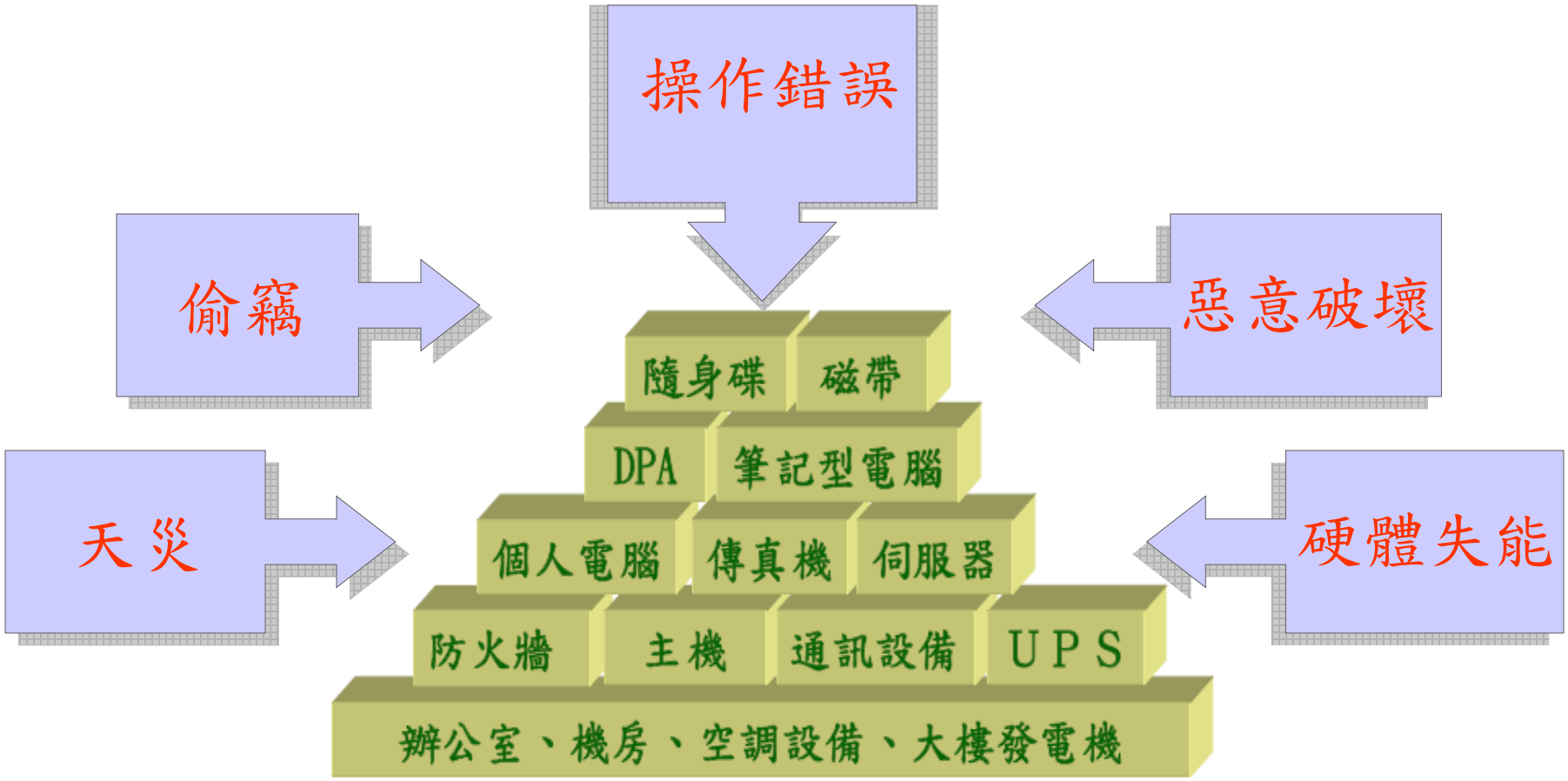
電腦系統資安措施

1. 使用合法軟體並更新系統漏洞
2. 正確使用通行碼(password)
3. 使用防毒軟體(or硬體)
4. 建立救援磁片與軟體備份
5. 安裝防火牆(firewall)或偵測系統

第五章 硬體資產

硬體-資產範例

硬體–常見資安威脅


操作錯誤
偷竊
惡意破壞
天災
硬體失能
隨身碟
磁帶
DPA
筆記型電腦
個人電腦
傳真機
伺服器
防火牆
主機
通訊設備
UPS
辦公室、機房、空調設備、大樓發電機

硬體-資安措施

1. 實體防護

2. 門禁管制

3. 工作區域作業規則

4. 保養維護

第六章 人員

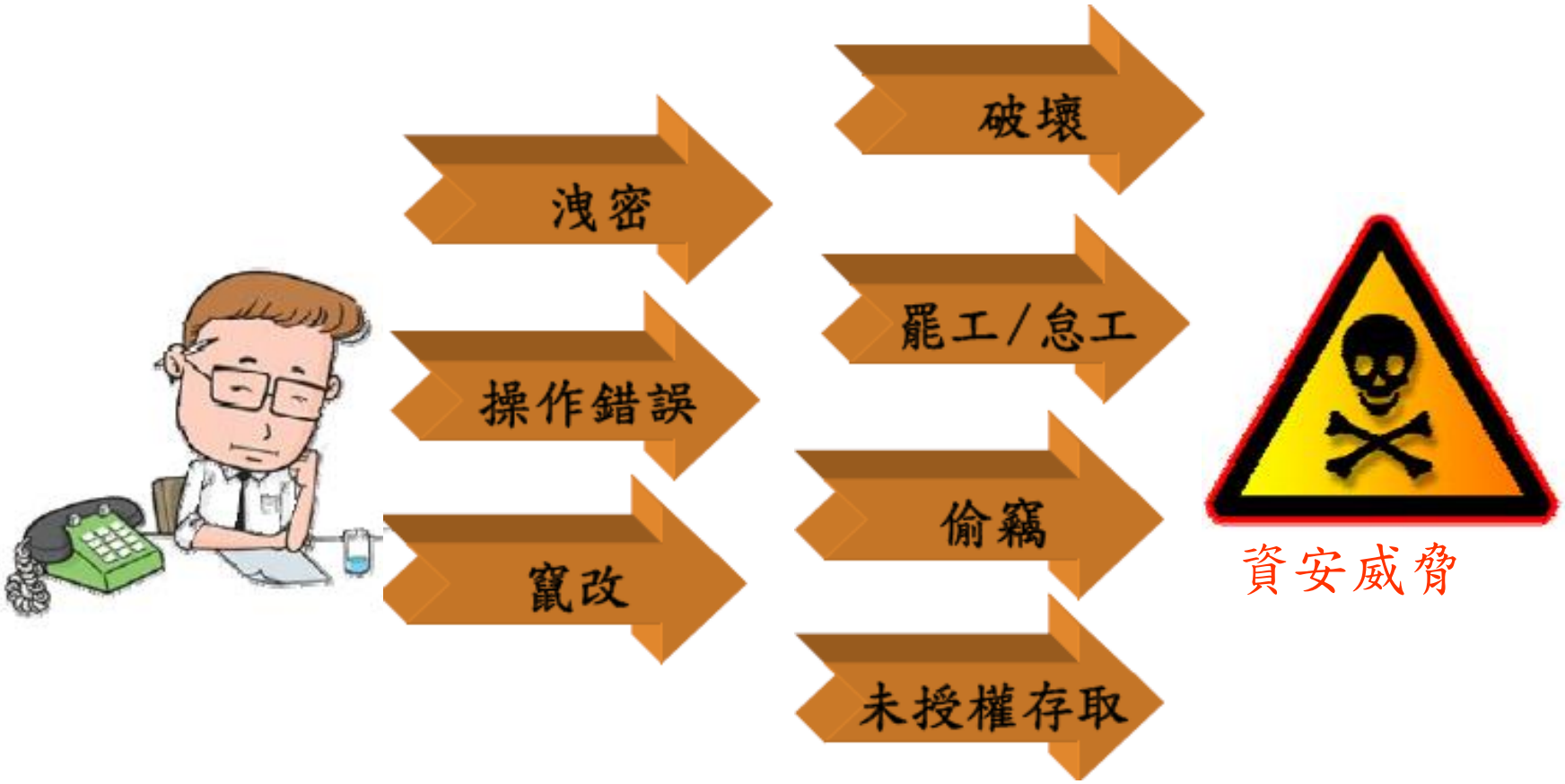
人 員

對資訊安全有重大影響的人：

- 擁有或處理機密資料
  - 機密專案承辦人，機要祕書
- 維運或管理大量資料
  - 資訊中心、檔案室管理人員

- 提供資訊服務
  - 網路管理員、重要資訊系統管理員

人員-可能產生的資安威脅



人員-資安措施

任用前

- 明訂各項工作之角色與職掌
- 人員篩選
- 簽訂保密合約
- 明訂各項工作之條件與限制

工作期間

- 主管監督與管理
- 教育訓練
- 懲處措施

離職或調職後

- 終止職權
- 歸還公司資產
- 移除各項存取權限

第七章 資產價值評估

資產價值（資產鑑價C、I、A）

機密性(Confidentiality，簡稱C)

確保只有經過授權的人才能存取資訊（使資訊不可用或不揭露給未經授權之個人、個體或過程的性質）。

完整性(Integrity，簡稱I)

保護資訊及其處理方法的準確性（accuracy）和完整性（completeness）的性質。

可用性(Availability，簡稱A)

確保經授權的使用者，在需要時可以隨時存取資訊並使用相關資訊資產。

資產評估-人員類(1/3)

機密性評估(C)

等　級	量化值	內 容 說 明
高	3	其工作執掌可存取限定資料（含機敏、內部使用及一般等三類）。
中	2	其工作執掌可存取內部使用類資料及一般類資料。
低	1	其工作執掌僅可存取一般類資料。

資產評估-人員類(2/3)

完整性評估(I)

等　級	量化值	內 容 說 明
高	3	▪ 未正確執行業務而造成資料不完整，會對業務造成很大的衝擊，甚至造成業務中斷失敗。 ▪ 可能影響全組織對外所提供的服務作業。
中	2	▪ 未正確執行業務而造成資料不完整，可能對業務運作不造成中斷，但降低運作效率及影響。 ▪ 可能影響單一部門運作。
低	1	▪ 未正確執行業務而造成資料不完整，可能對業務運作不會造成中斷或雖降低效率但不會造成影響。 ▪ 僅僅影響少數承辦人的作業。

資產評估-人員類(3/3)

可用性評估(A)

等　級	量化值	內 容 說 明
高	3	▪ 欲維持業務正常運作，在該等人員無法持續提供服務時，可容忍替換時間為4小時。 ▪ 業務高度仰賴該員，且一旦該員無法作業時，將影響本公司對外所提供的服務作業。
中	2	▪ 欲維持業務正常運作，在該等人員無法持續提供服務時，可容忍替換時間為12小時以內。 ▪ 業務仰賴該員，且一旦該員無法作業時，將影響本公司多數部門作業。
低	1	▪ 欲維持業務正常運作，在該等人員無法持續提供服務時，可容忍替換時間為24小時以上。 ▪ 業務仰賴該員，且一旦該員無法作業時只影響少數承辦人員作業，其工作可暫時委由他人替代。

資產評估-非人員類(1/3)

機密性評估(C)

等　級	量化值	內 容 說 明
高	3	▪ 敏感性資訊處理設施與系統資源，僅開放給必要知道的人使用。 ▪ 資料內容若洩漏會影響組織聲譽及利害關係人之權益。
中	2	▪ 非公開使用之非敏感性資訊處理設施與系統資源僅開放給內部人員使用。 ▪ 資料內容若洩漏會對組織造成有形或無形的損害，此損害為組織可承受之範圍。
低	1	▪ 不限制使用資訊處理設施與系統資源等。 ▪ 資料內容若流傳至組織以外，不會對組織造成任何有形或無形的傷害。

資產評估-非人員類(2/3)

完整性評估(I)

等　級	量化值	內 容 說 明
高	3	▪ 不當的損失、破壞資訊處理設施與系統資源，會對業務應用造成顯著的衝擊。 ▪ 資訊系統服務若不完整，將導致組織作業受影響。
中	2	▪ 不當的損失、破壞資訊處理設施與系統資源，會對業務應用造成輕微的衝擊。 ▪ 資訊系統服務若不完整，將造成單一部門作業受影響。
低	1	▪ 不當的破壞或竄改資訊、資訊處理設施與系統資源，所造成的業務衝擊可以忽略者。 ▪ 資訊系統服務若不完整，將造成少數或個別承辦人作業受影響。

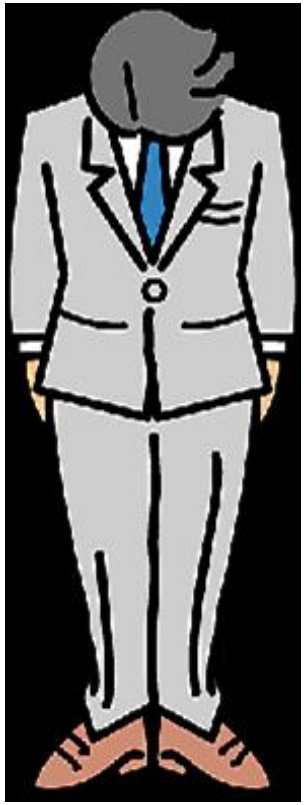
資產評估-非人員類(3/3)

可用性評估(A)

等　級	量化值	內 容 說 明
高	3	▪ 僅容許短暫時間（4小時內）無法使用，作業停頓期間極易產生客訴事件，使組織受到損害者 ▪ 作業完全仰賴資訊資產，且一旦服務中斷時將影響全組織對外所提供的服務作業。
中	2	▪ 容許較長時間（8小時內）無法使用，會造成部份人員之抱怨，使組織受到輕微損害者。 ▪ 作業仰賴資訊資產，且一旦服務中斷時將影響部門運作。
低	1	▪ 容許長時間（1天以上）無法使用，作業停頓期間可利用其他替代方案，不致造成組織之損失 ▪ 作業仰賴資訊資產，且一旦服務中斷時將影響少數承辦人作業。

Q&A 問題與討論

～如有任何問題，歡迎隨時來電詢問～



E-mail: cyword0920@gmail.com