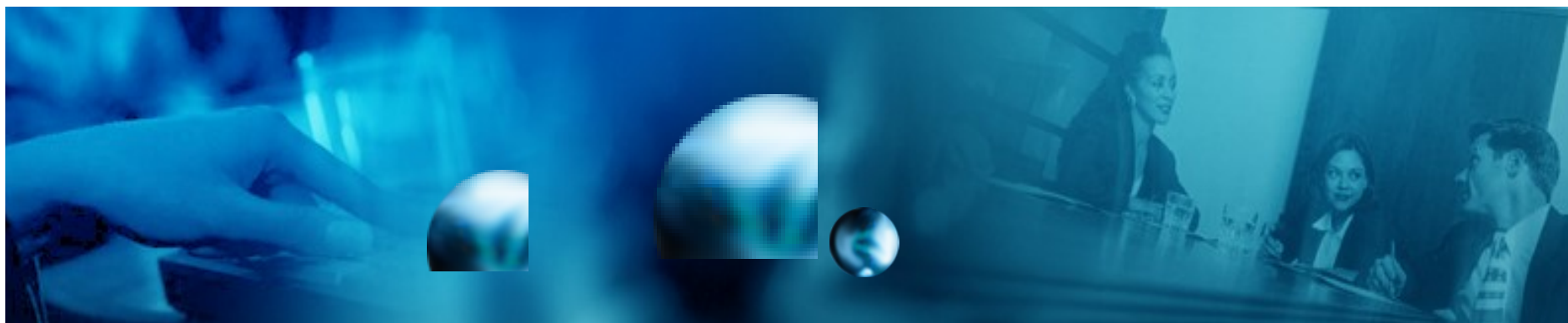


資訊資產管理概論與實務





課程大綱(Agenda)

- 概述
- 資產登錄
- 資安措施規劃與執行
- 資訊資產(書面&數位紀錄)
- 軟體資產(電腦系統)
- 硬體資產
- 人員-可能產生的資安威脅
- 資安措施-制度化
- 稽核與改進
- 結論





第一章 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。

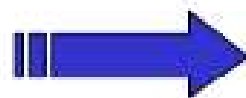




前言 (2/2)

- 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



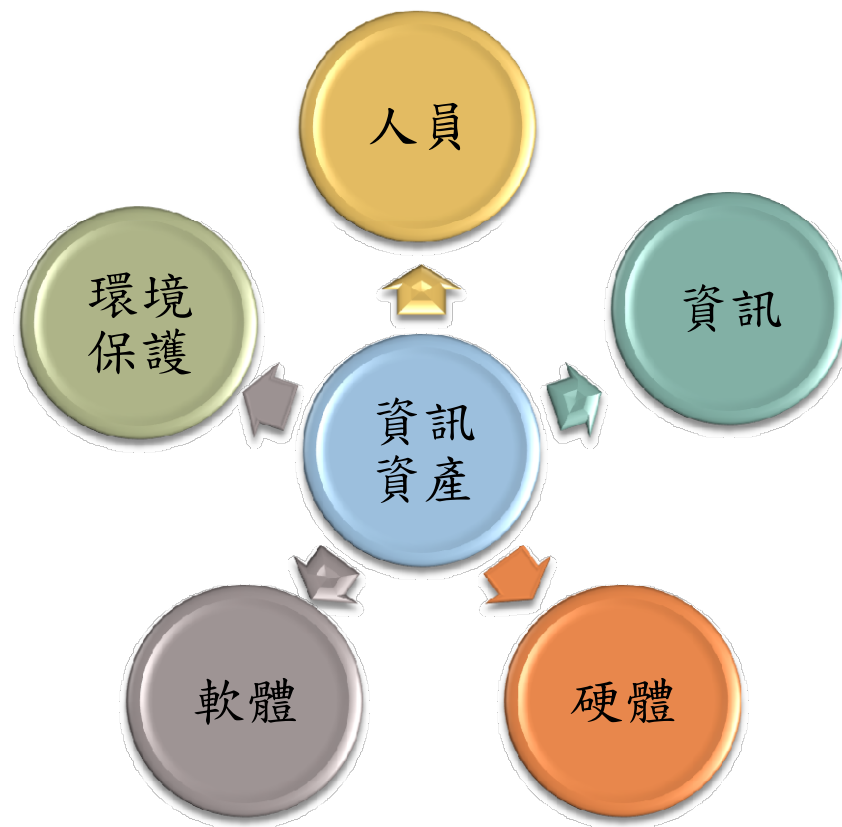
保護資訊安全





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。

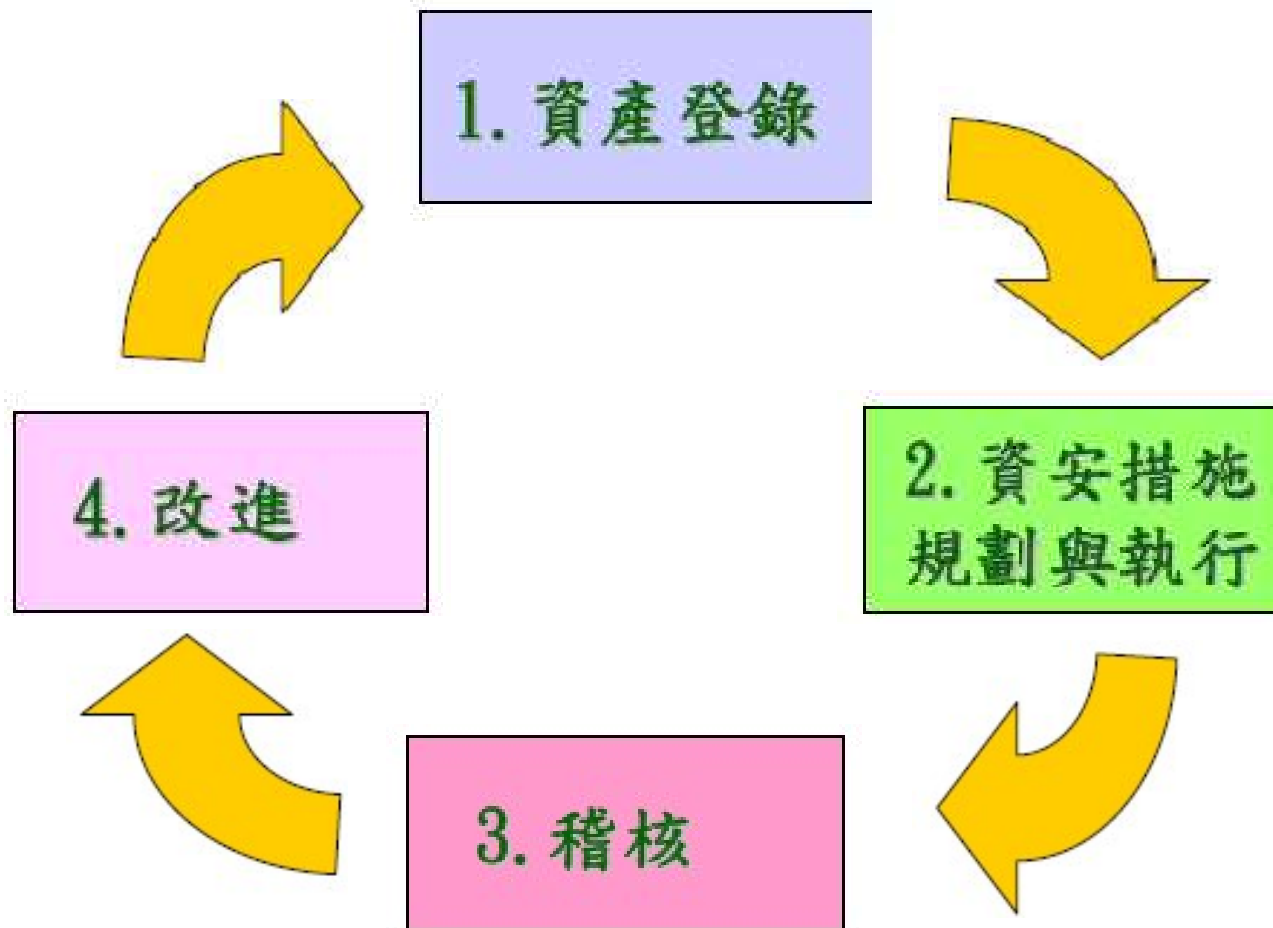
硬體

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、...





資訊資產的管理議題





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—資產清單

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單。





資產清冊之製作與維護

資訊資產清冊(參考範本)

單位名稱：○○○

NO.	登錄時間	資產類別		資產名稱	資產說明	數量	存放位置	風險擁有者(部門)
		大類	小類					



資產清冊-資產類別 (1/4)

資訊資產清冊(參考範例)

單位名稱：○○○

更新日期：109/06/01

NO.	登錄時間	資產類別		資產類別的優點				
		大類	小類					
1	109/02/11	人員類	聘雇人員	•幫助資產盤點，減少遺漏。 •容易歸類，並選擇適當的資安管理措施				
2	109/02/11	資訊類	資訊紀錄					
3	109/02/11	硬體類	網路設備					
4	109/02/11	軟體類	套裝軟體		3	3	3	9
5	109/02/11	環境保護類	建築保護設施		1	2	2	5



資產清冊-基本資料 (2/4)

資訊資產清冊(參考範例)

單位名稱：○○○

更新日期：108/06/01

NO.	...	資產名稱	資產說明	數量				
1		資訊組專員	資訊人員	2				
2		○○暨代檢系統資訊記錄	○○系統 192.168.92 .180資料庫	1				
3		Brocade FWS624	○○VPN Switch	1				
4		SYBASE Adaptive Sever...	○○資料庫系統	2	3	3	3	9
5		消防滅火系統	12磅指標式氣體式CO2	1	1	2	2	5

資產名稱

- 協助資產識別，容易辨認。

資產說明

- 認知資產內容及特性、型式更明確

- 容易掌握數量



資產清冊-風險擁有者 (3/4)

資訊資產清冊(參考範例)

單位名稱：○○○

- 可指定個人或單位
- 兩者可以相同或不同
- 使單位負責日常資安管理，如
 - 螢幕清空
 - 防竊
- 保管單位負責周期性資安管理，如
 - 定期維護保養
 - 資產清點

...	管理者/部門 (風險擁有者)	使用者 (部門)
	人事組 徐○○	資訊組
	資訊組 彭○○	醫檢科
	資訊組 彭○○	全院
	資訊組 張○○	全院
	裝備組 李○○	資訊組

資產清冊-資產價值 (4/4)

資訊資產清冊(參考範例)

單位名稱：○○○

更新日期：108/06/01

				資產評估			資產價值
				機密性	完整性	可用性	
•依資產評估可考量下列因素 <u>-機密性 資訊資產-機密等級區分</u> -完整性 -可用性 •依據資產價值讓使用者容易判斷 對該資產的保護程度				3	2	2	7
				2	2	3	7
				1	2	2	5
				3	3	3	9
5	108/02/11	環境保護類	建築保護設施	1	2	2	5



資產清冊-其它

- 電腦系統：（Windows 10,MS-office）
 - 原版光碟
 - 安裝序號
- 實體：（個人PC）
 - 配備
 - 硬體：螢幕、硬碟、記憶體等
 - 軟體：該PC中所安裝的軟體
 - 配備





資產盤點

資產清冊



螢幕

 印表機

 軟體光碟



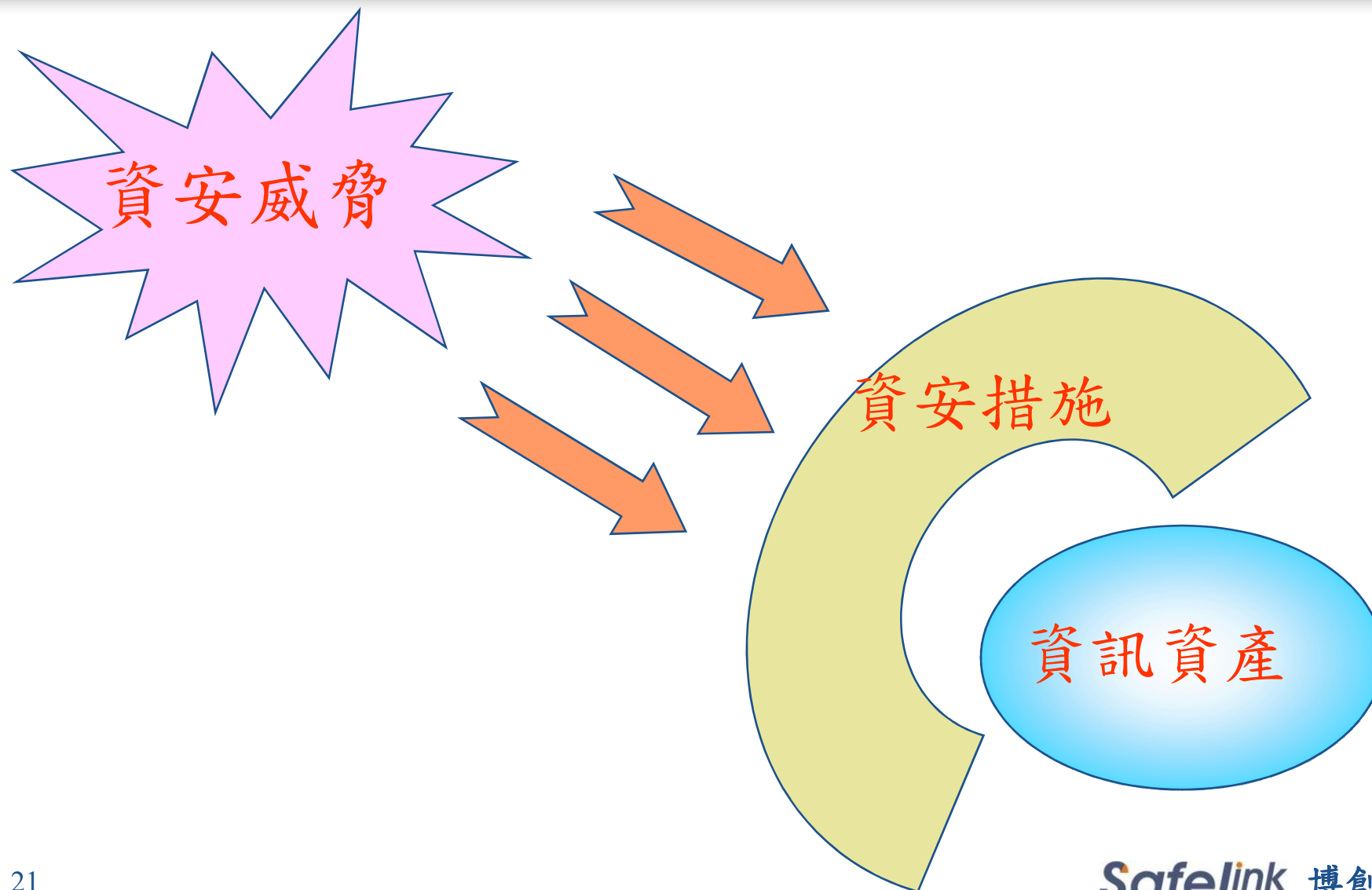
 文件



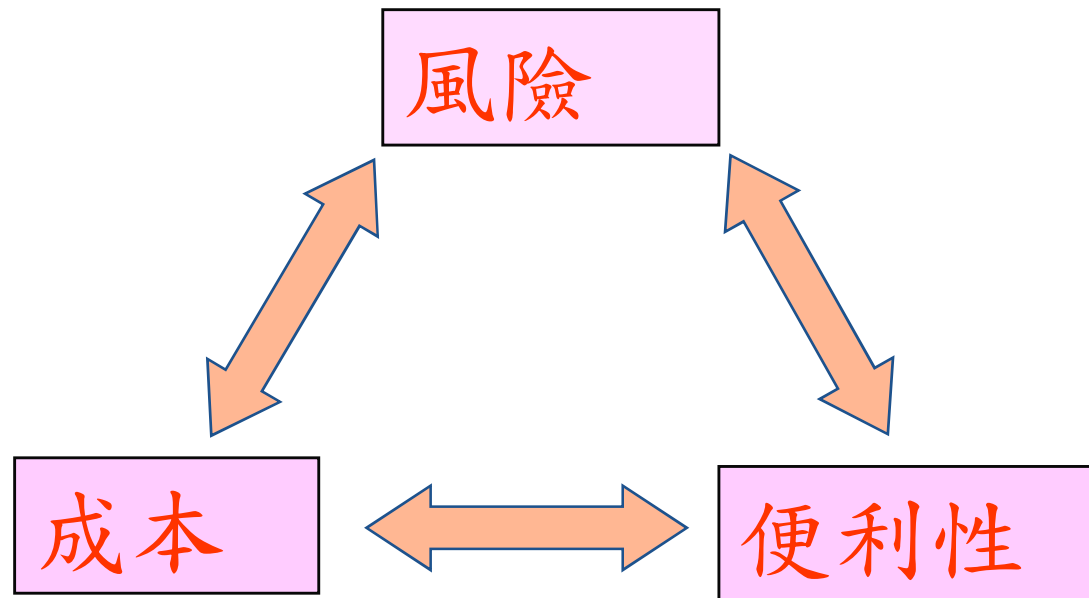


第三章 資安措施規劃與執行

資安措施規劃與執行 (1/2)



資安措施規劃與執行 (2/2)



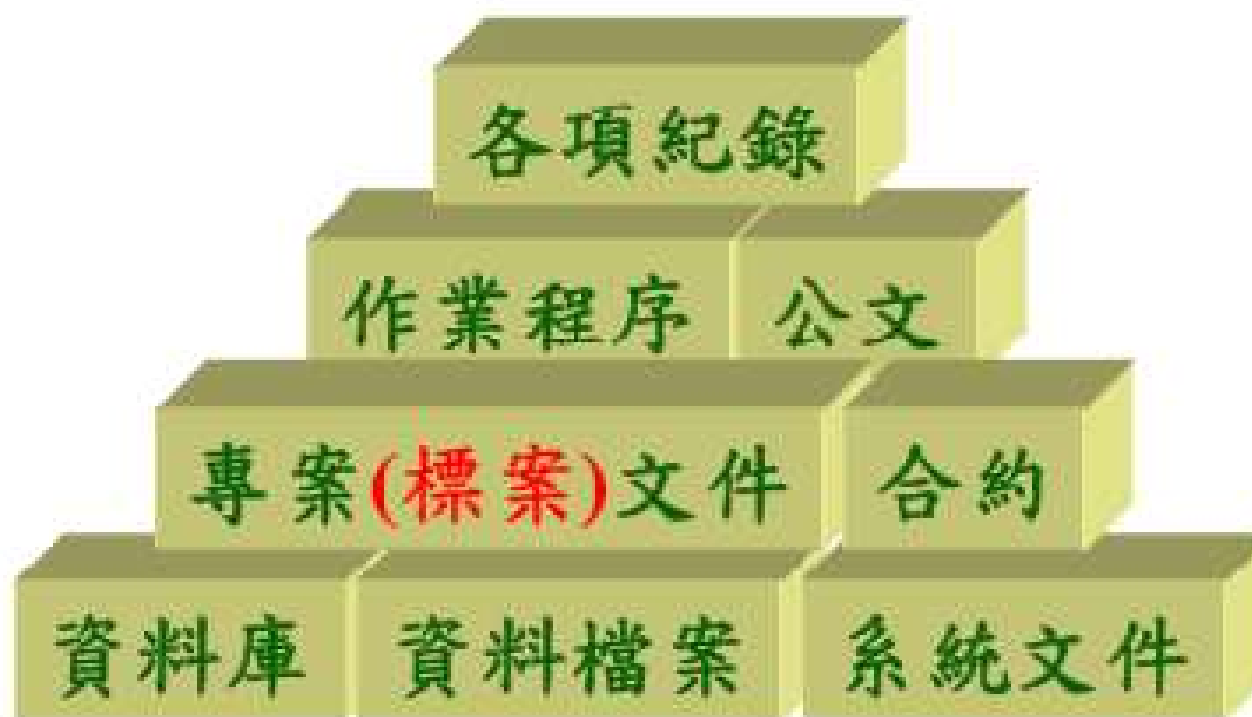
安全總是要在三者之間取捨！



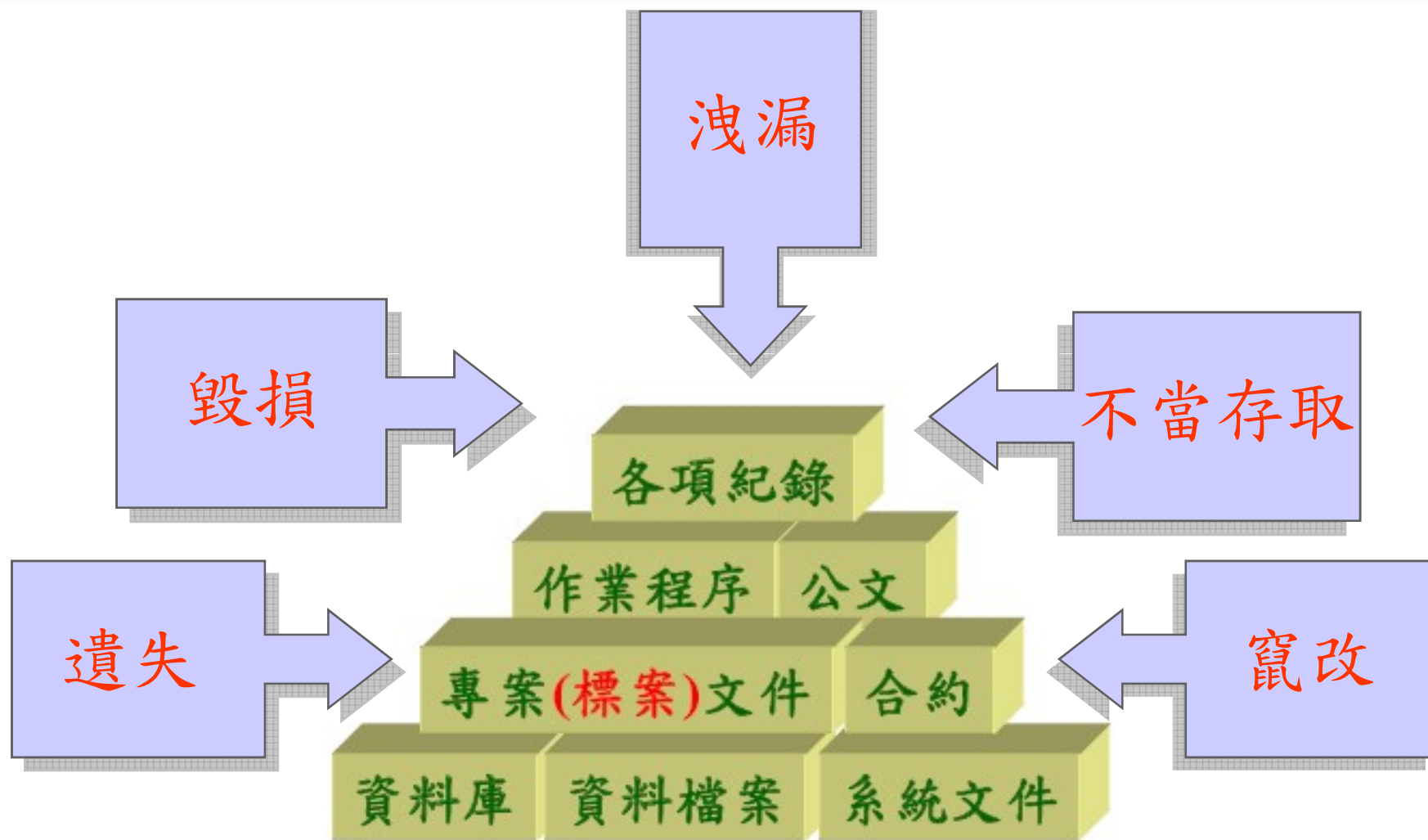
第四章 資訊資產(書面&數位紀錄)



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



1.分級意義

- 並非所有資訊資產都有相同價值。
- 保護資訊資產需要投資相當大的時間、金錢、人力、物力…。
- 分級可以確保資訊資產受到**適當的保護**。





分級好處

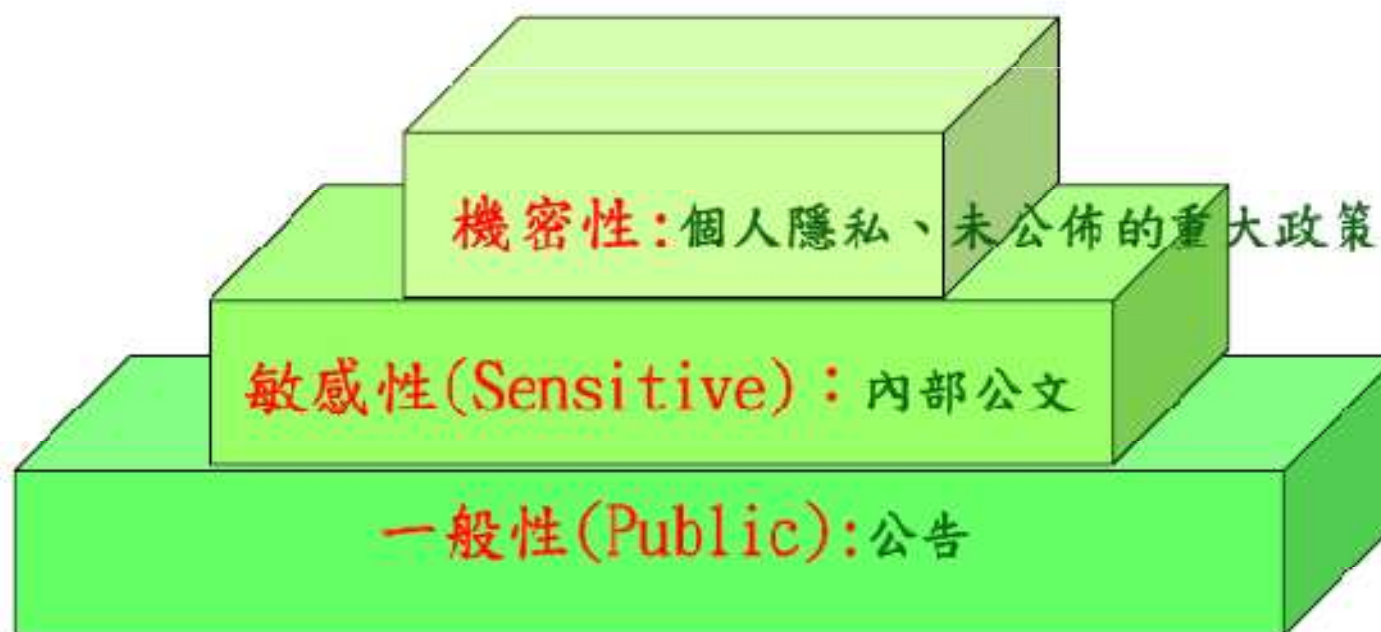
- 展現單位對資訊資產保護的決心。
- 有利於**確定**哪些資產對企業有**絕對的價值與重要性**。
- 有助於**分辨**資產等級的不同，以給予不同、**適當的處理（相稱性）**。



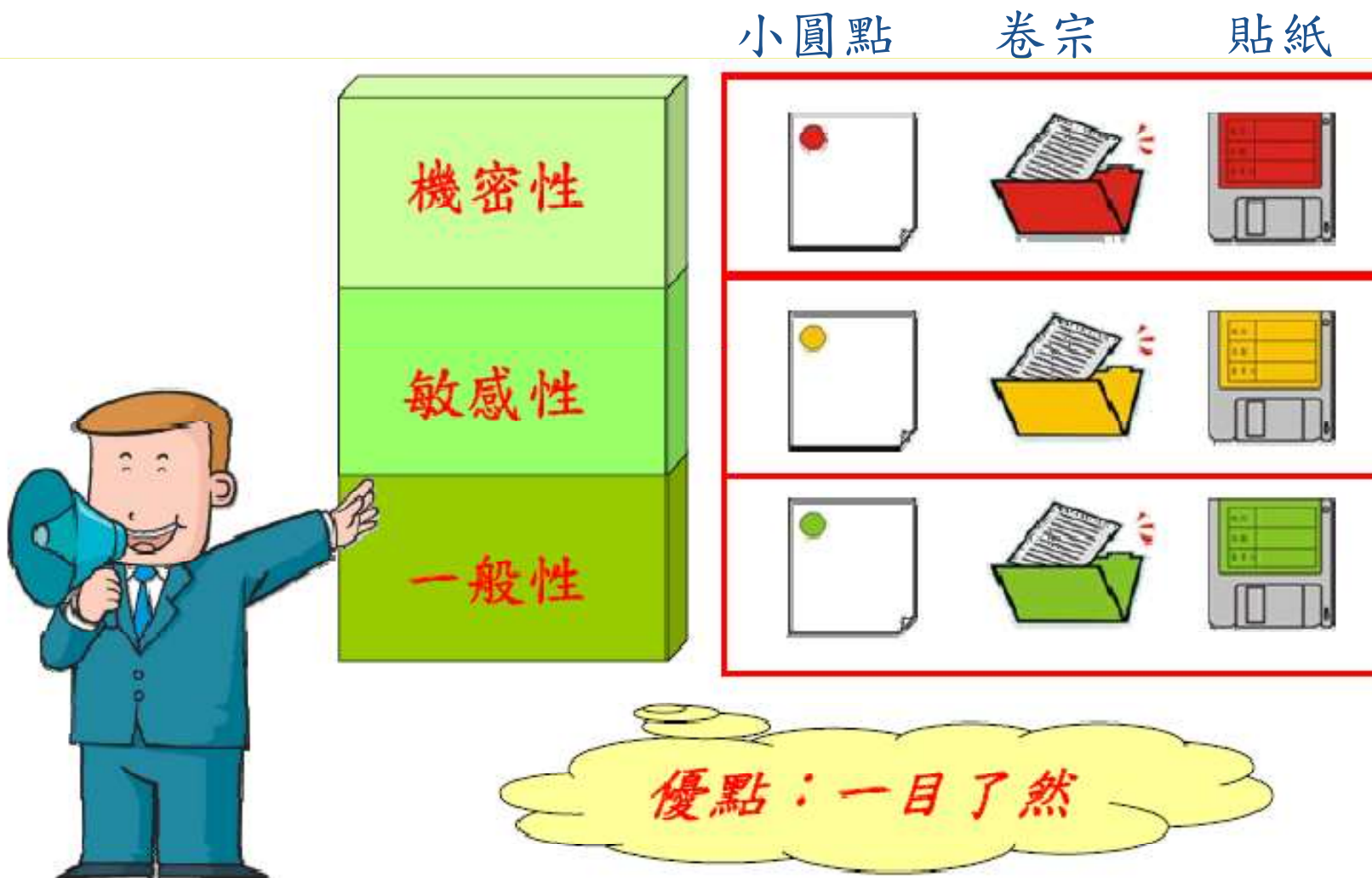


分級的範例與規範

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：

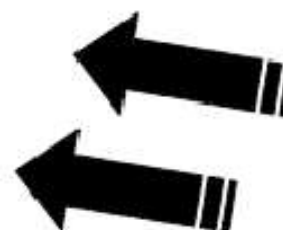


2. 資訊標示 (1) - 顏色標示



資訊標示的安全考量

過於清楚的標示



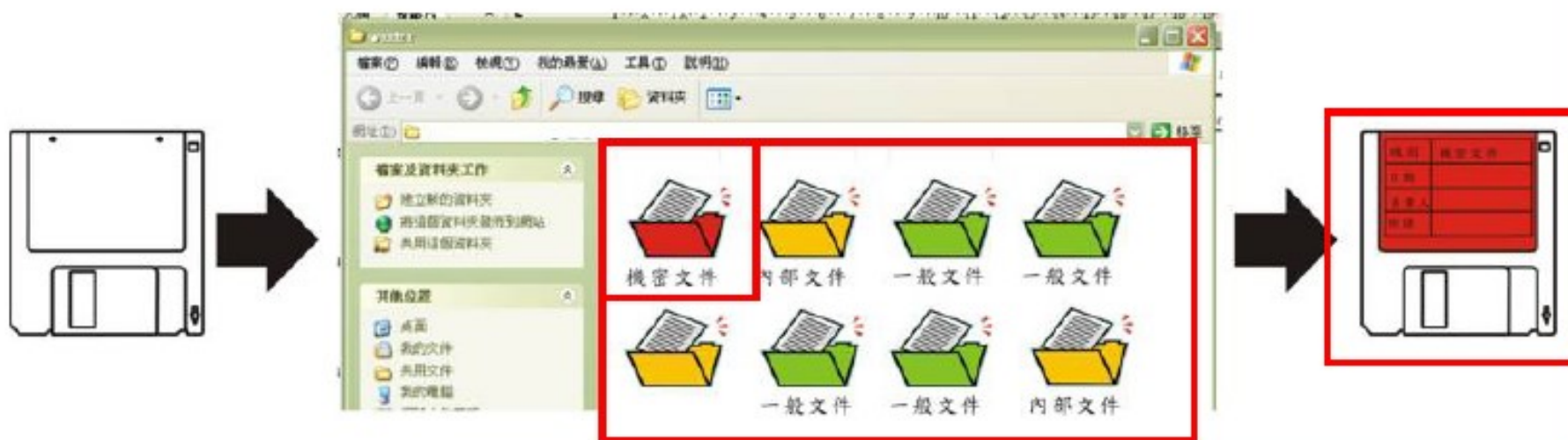
易引起外部人員犯罪動機

資訊標示 (2) - 編碼標示



資訊標示 (3) - 複合式標示

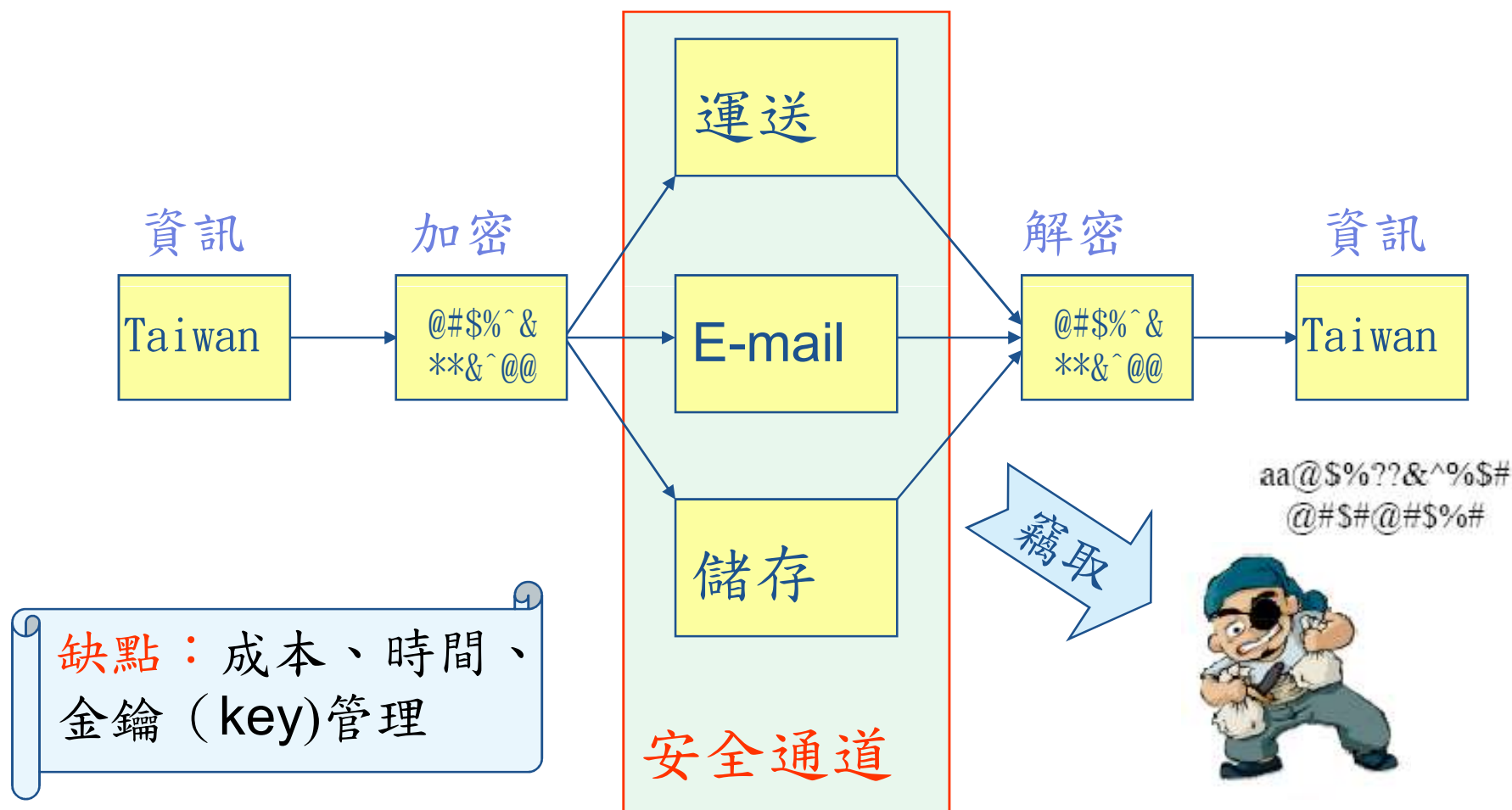
文件中包含多種級別的檔案時



文件標示以中最高的等級為準

3. 資訊加密

- 資訊加密是資訊安全最核心的措施





4. 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





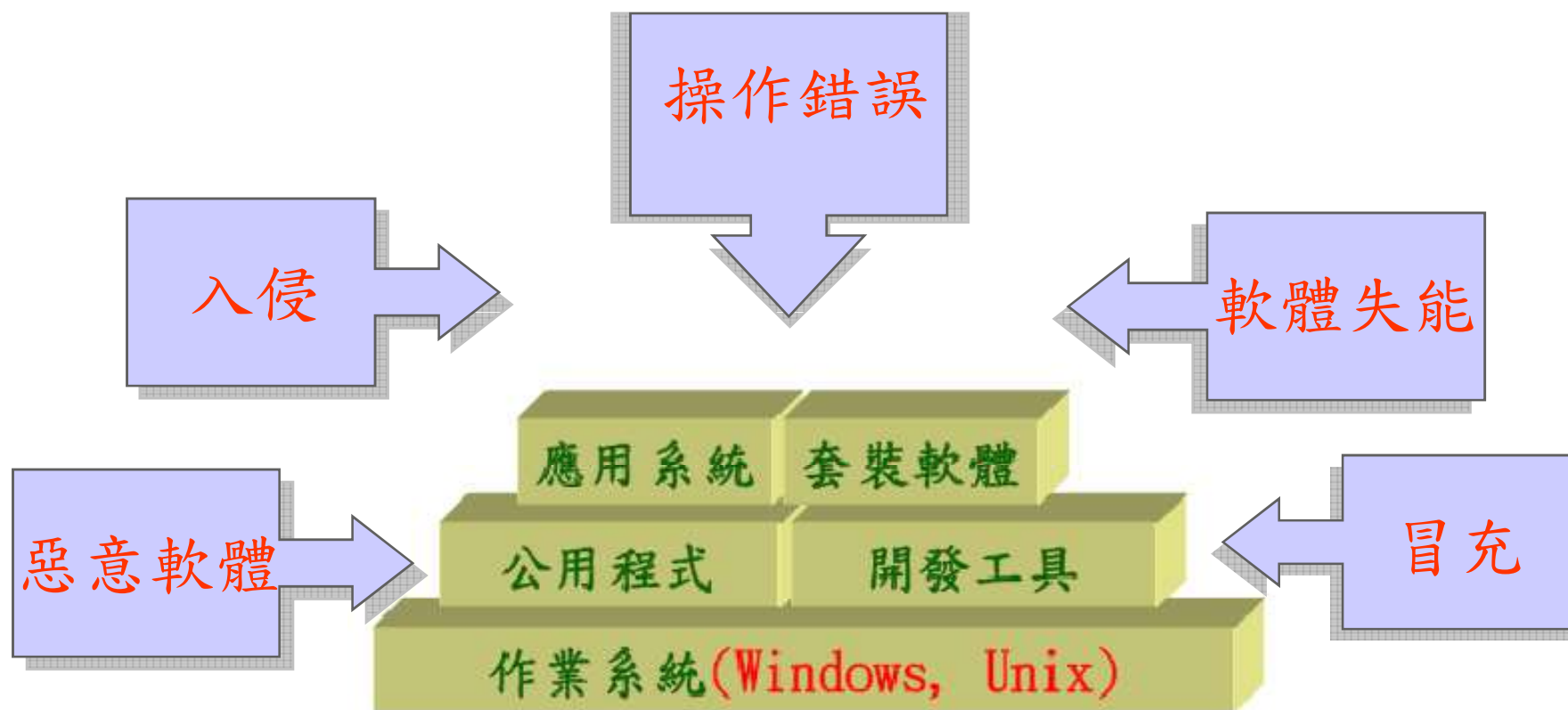
第五章 軟體資產(電腦系統)



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

使用合法軟體並更新系統漏洞



1. 使用**原版軟體**，確保無後門程式，確保符合法令要求。
2. 不安裝不明軟體(**shareware**)，沒有版權問題但可能暗藏後門。
3. 不任意下載不明資料與檔案。
4. 更新**電腦系統漏洞**。
 - (1) 自動偵測更新
 - (2) 定期更新



正確使用通行 (password)

1. 避免將通行碼寫在紙上
2. 選用較嚴謹的通行碼，最少8碼：
 - (1) 容易記
 - (2) 不要使用個人資訊當做通行碼
 - (3) 數字、字元併用

較差的通行碼：12345678

Tony+6285

較佳的通行碼：t6o25n8y

3. 定期更改通行碼。



使用防毒軟體



1. 安裝**防毒軟體**並定期/自動更新**病毒碼**。
2. 設定防毒軟體**常駐執行**。
3. 定期**掃描**重要業務作業的系統軟體與資料內容。
4. 外來檔案在使用前**檢查**是否有病毒。
5. 在使用前**檢查**所有電子郵件附件和下載檔案有無惡意軟體。
6. 遭病毒攻擊後，立即**通報**。



建立救援磁片與軟體備份

中毒、毀損、遭竄改

- 建立救援磁片

- 協助系統異常排除
- 協助系統復原

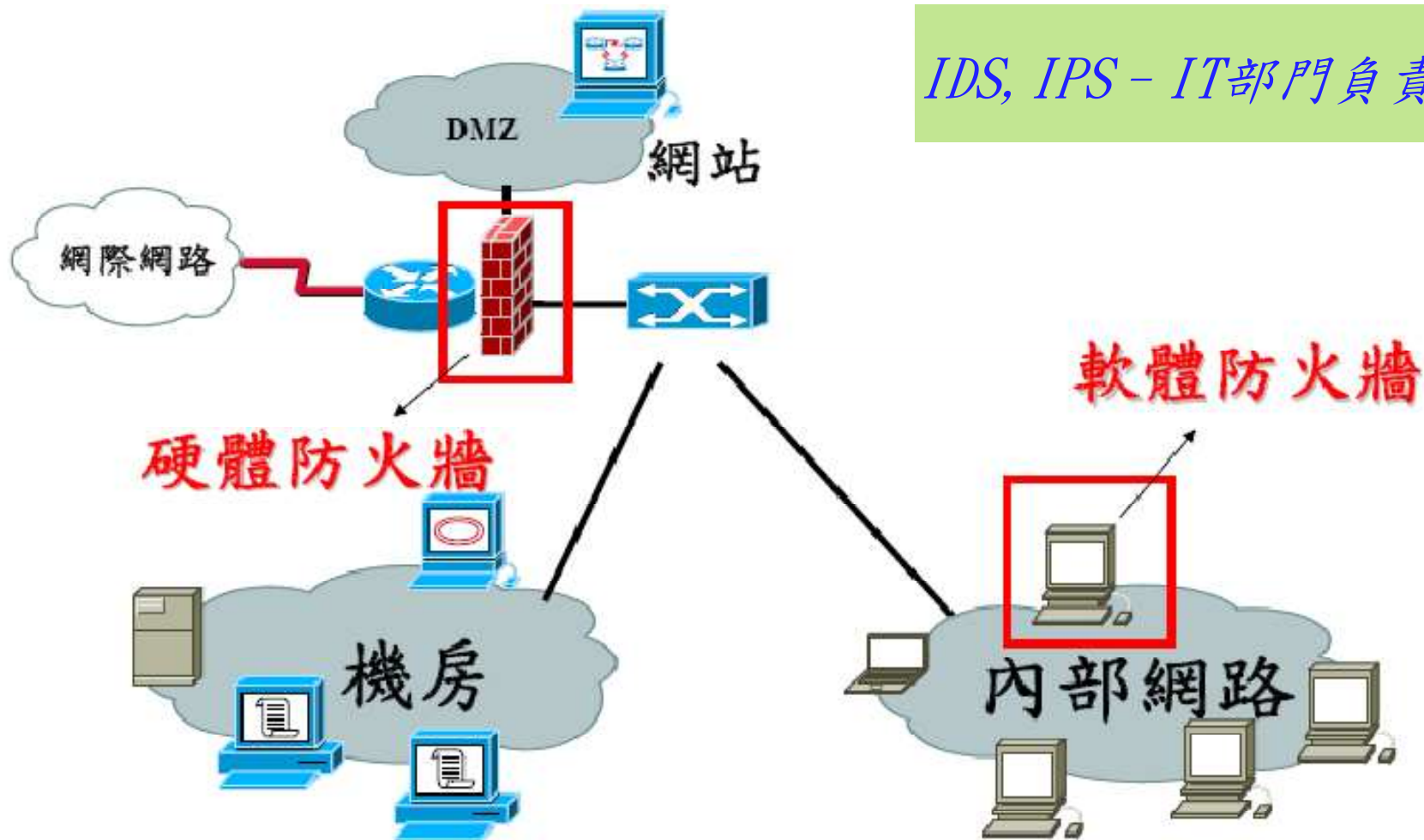


- 軟體備份

- 含設定參數
- 加速災害復原速度
- 多人系統的帳號與權限設定，透過系統備份，可省下許多時間



安裝防火牆或偵測系統



IDS, IPS – IT部門負責



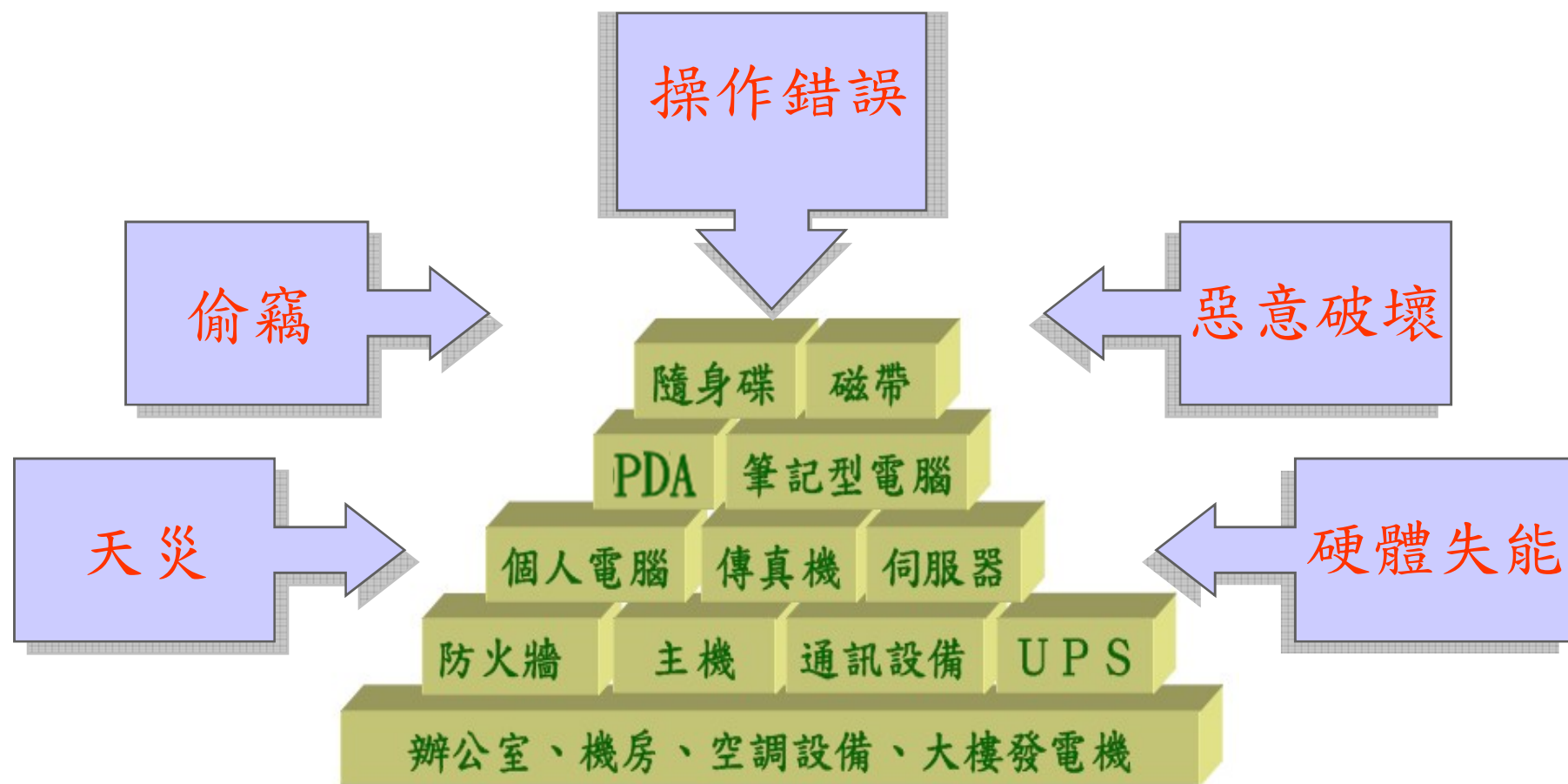
第六章 實體資產



實體-資產範例



實體-常見資安威脅





實體-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

5. 再利用(re-use)與報廢

6. 建立備份/備援機制





實體防護



- 重要設備應放置在**安全區域**。

例如：主機應該鎖在機房、重要資料則應鎖進保險箱。

- 可移動式設備應**上鎖**。

例如：筆記型電腦、PDA、外接式硬碟等。

- 筆記型電腦於公司外場所使用，應盡可能讓筆記型電腦**不離開視線**。



門禁管制

- 嚴格執行人員進出管制。
- 訪客應配帶**識別證**，無正式員工陪同不得自行走動。
- 單位內遇有可疑人士應進行確認。
- 資產攜出應出具**核准文件**。
- 重要設施區域（機房）應**隨時上鎖**。



工作區域作業規則



- 在機房或資訊設備旁，**禁止**吸菸與放置飲料。
- 除非經授權，否則**不允許使用拍照、錄影、錄音**和其他可用來記錄的設備（照相手機也應該避免）。
- 離開時關閉門窗。



保養維護(1/2)

- 日常清潔保養（通常由使用者執行）的工作項目有：
 - 自行清點設備有無短缺
 - 簡單清潔擦拭，減少灰塵
 - 電腦元件間連接線整理有序
- 定期保養維護的工作項目有：
 - 設備內部清潔
 - 到期電腦零件更換
 - 系統與檔案重整
 - 通常由技術人員執行

灰塵堆積，容易造成過熱或短路唷！



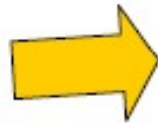


保養維護 (2/2)

設備定期保養維護表

資產名稱	編號	保養類別	保養人	工作說明	下次保養日期
伺服器	C102311	月保養	張山	1.清潔 2.系統檢查 3.檔案整理 4. xxx	2005.12.01
xxx	xxx	季保養	xxx		
xxx	xxx	年保養	xxx		

再利用 (re-use)

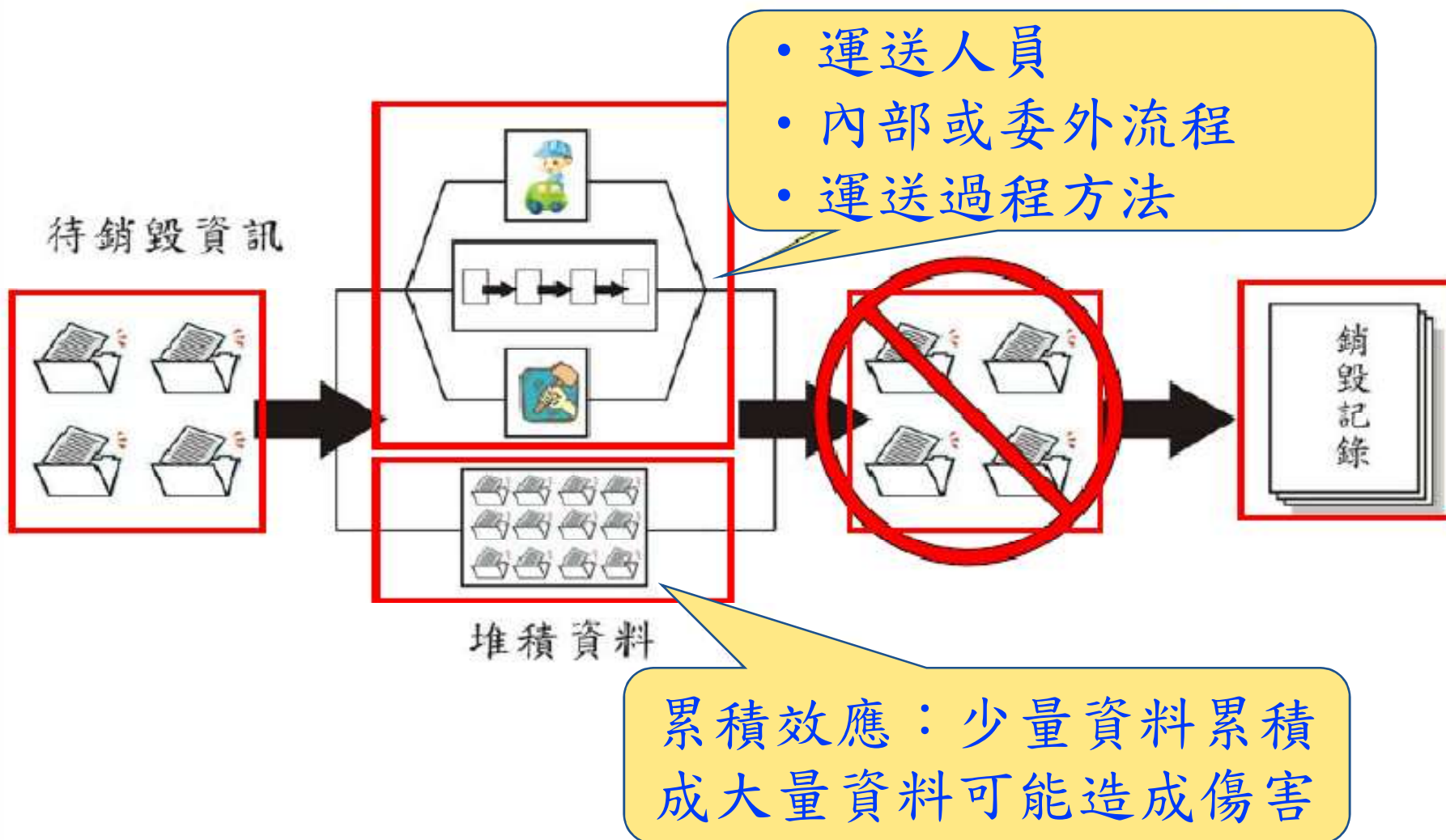


重要資料移除

1. 格式化硬碟，重新安裝
2. 移交原版軟體(含安裝序號)
3. 清點原有配備
4. 異動交接登記



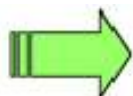
銷毀作業-資安議題



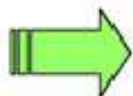
銷毀方式



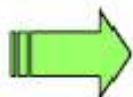
銷毀方式



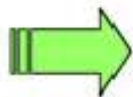
文件：絞碎、焚毀



磁碟、硬碟：拆解



光碟、磁片：破碎



電腦設備：拆解



建立備份/備援機制

備份

- 耗材備份
- 零件備份
- 系統備份

災害緊急 應變演練

- 消防演練
- 災害處理與災後復原演練

備援 機制

- 系統備援
- 機房備援





第七章 人員



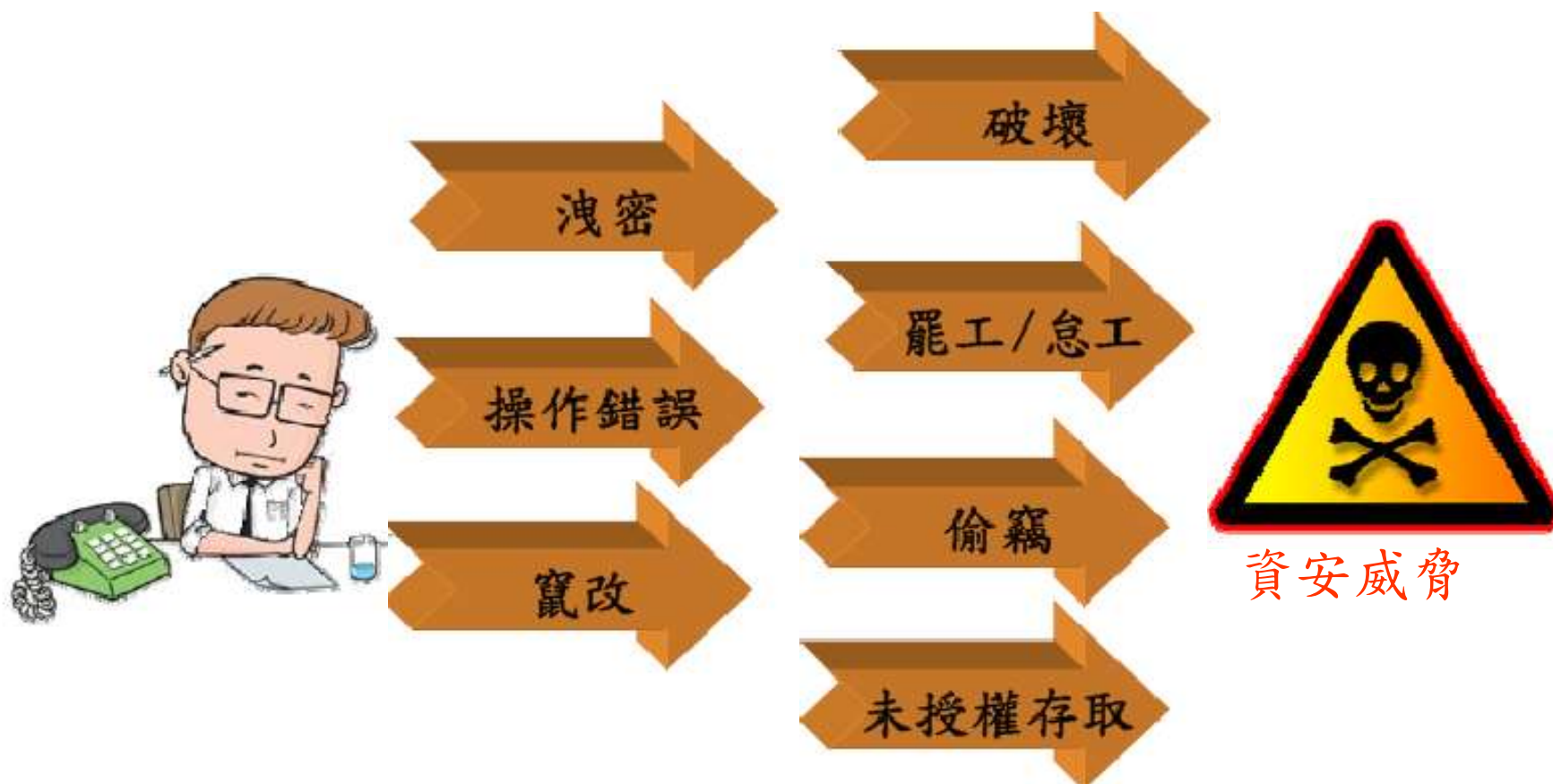
人員

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

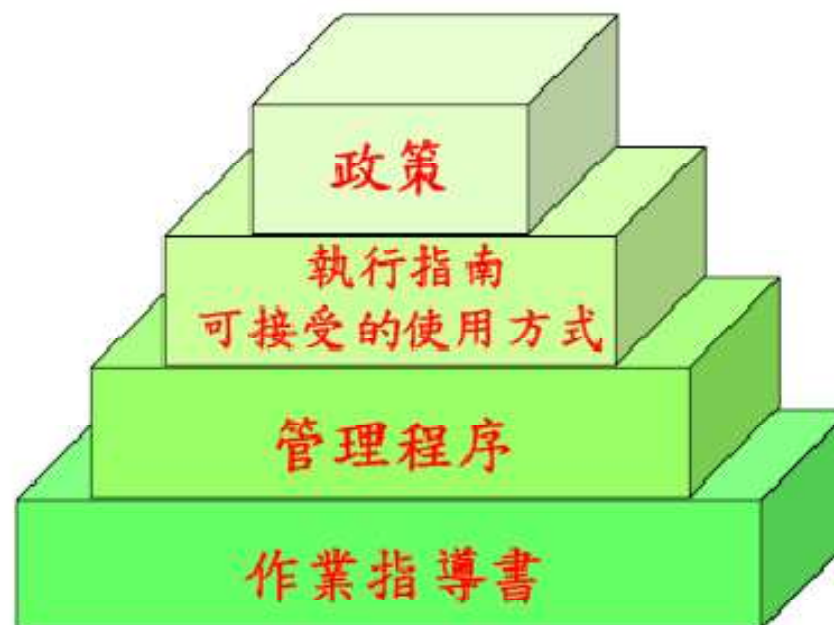


第八章 資安措施

資安措施-制度化



欲有效落實資安施，需加以制度化

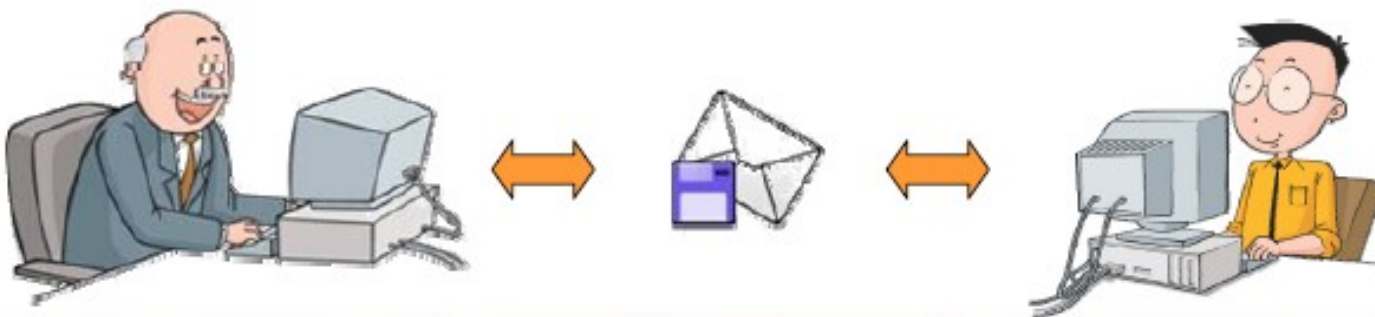


訓練與宣導

資產可接受的使用方式

電子郵件(e-mail)的使用規定(rule)

- 禁止使用電子郵件傳送私人、色情、危害組織或國家安全的資訊。
- 所有電子郵件開啟前應執行病毒掃描
- 禁止使用電子郵件傳送機密資訊，包括系統帳號與通行碼。





第九章 稽核與改進



稽核

資 訊 安 全 內 部 稽					
稽核項目	ISO27001	受稽單位		稽核員	
章節	稽核要點	稽核結果			
		符合	不符合		
A.8	資產管理				
A.8.1	資產責任 是否有建立書面程序識別組織資產及定義 適切的保護責任。				
A.8.1.1	資產清冊 是否已明確識別與資訊及資訊處理設施有 關的資產，並制作與維護上述資產的清冊。				



持續改進管理措施

從稽核結果

從資安事件中學習

吸收資安專家建議





第十章 結論

結論



- **資訊資產管理**是建立資訊安全最根本的工作。
- 資訊資產包含資訊、軟體、實體、技術服務，人員與無形資產。
- **資產清冊**可以有效幫助資產登錄與管理。
- **資訊安全分級**能幫助組織用有限的成本達成較佳的資安措施。
- 資訊資產管理應瞭解資產可能的威脅並加以防護。
- 資訊資產管理制度應持續改進，不斷提昇資訊安全。



Q&A 問題與討論

～如有任何問題・歡迎隨時來電詢問～

SafeLink

博創資訊科技股份有限公司

臺中市西屯區國安一路208巷6號

TEL : 886-4-25250535

FAX : 886-4-24615268

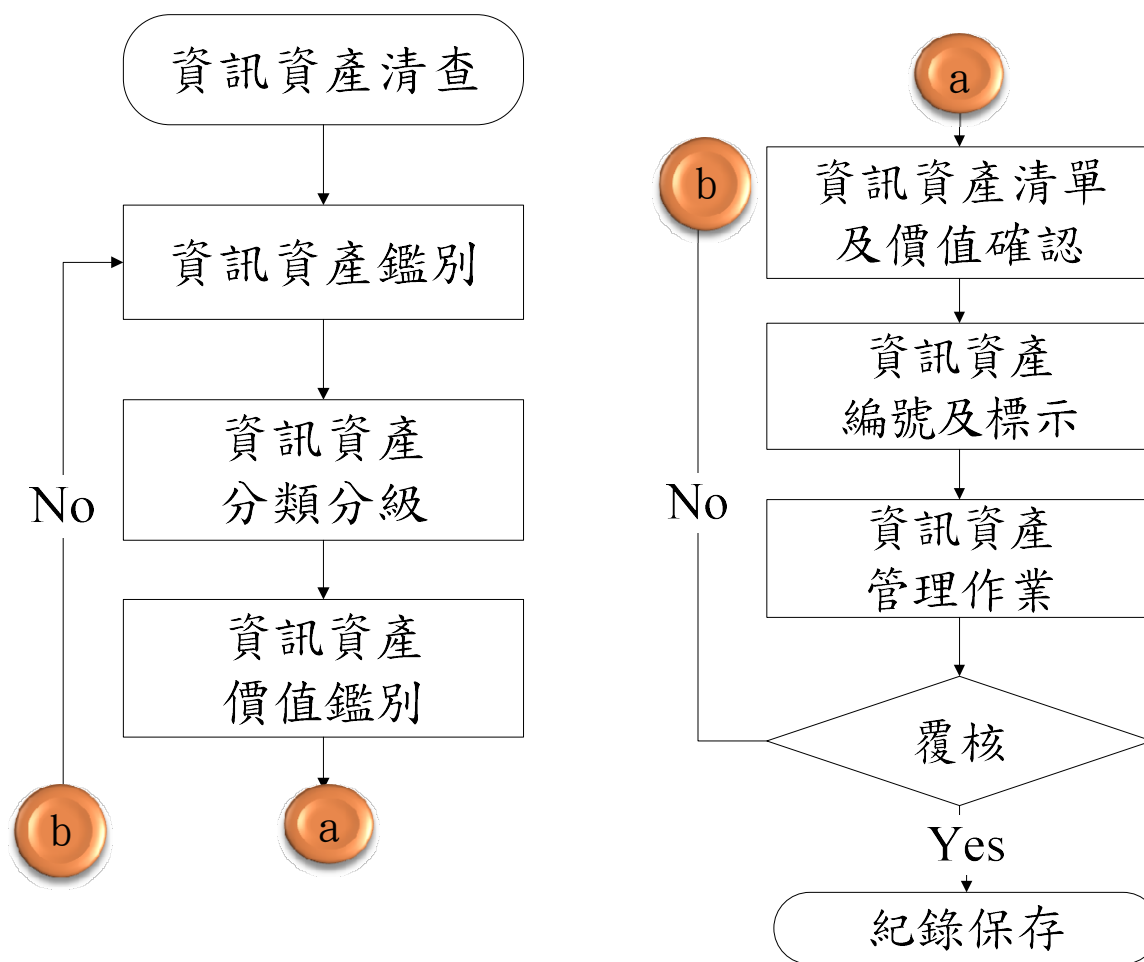
<http://www.safelink.com.tw/>

E-mail: sam@safelink.com.tw





資訊資產

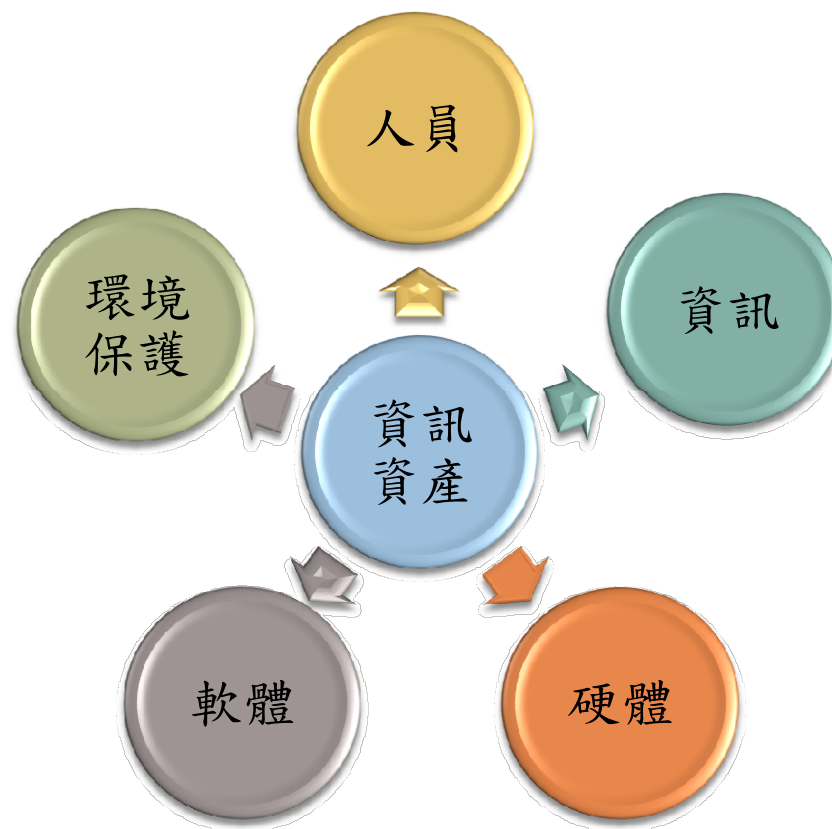




資訊資產

資訊資產價值評估標準

依資訊資產之特性，分成人員與非人員（含硬體、軟體、資訊及環境保護類）兩大類，其各所對應之機密性、完整性及可用性之定義與價值評估標準





資訊資產

大分類	小分類	範例
人員類	編制內人員	正式編制人員、臨時人員、工讀生、專案人員、委外廠商.....等。
	臨時鐘點人員	
	委外廠商駐點人員	
	委外廠商	
資訊類	作業文件	資料庫與資料檔案、備份資料、原始程式碼、網路架構圖 系統文件、操作或支援程序、使用手冊、教育訓練教材、 管理制度文件、緊急應變&復原計畫、營運持續計畫 (BCP)、稽核日誌、契約與協議、報表、表單記錄..... 等。
	系統文件	
	契約	
	資訊紀錄 (電子/紙本)	
	系統紀錄 (Log)	
硬體類	個人電腦	<u>一般硬體</u> ：包含電腦設備（伺服器、筆記型電腦、個人電腦、工作站）、CD/DVD 燒錄器、CD/DVD光碟機、磁帶機、軟碟機、投影機、PDA、印表機.....等。
	可攜式電腦	
	伺服器	
	資安設備	<u>通訊設備</u> ：集線器、橋接器、網路交換器、路由器、數據機、電話自動交換機 (PBX)、網路纜線、防火牆、入侵偵測系統、視訊會議設備、傳真機、手機。
	網路設備	
	可攜式儲存媒體	
	電腦保護設施	<u>儲存媒體</u> ：CD/DVD（空白）、硬碟（無資料）、磁片（空白）、磁帶（空白）、移動式硬碟（空白）、錄音/影帶（無資料）.....等。
	其他硬體	



資訊資產



大分類	小分類	範例
軟體類	作業系統	應用系統軟體、作業系統軟體、開發工具、套裝軟體、公用程式、防火牆軟體、防毒軟體、驗證軟體、資料庫管理系統（DBMS）、加密軟體、文件管理系統、內部開發程式、內部發展系統……等。
	應用系統	
	套裝軟體	
	軟體開發工具	
	資通安全系統	
環境保護類	一般辦公區域	建築類：電腦機房、會議室、辦公室、監控室、接待區、交貨區/裝載區……等。
	特殊辦公區域	
	資訊機房	環境保護設施：不斷電系統、第二電力供應迴路、穩壓器、機櫃、避雷裝置、警報系統、備用發電系統、環境控制系統（火偵測、熱偵測、水偵測、溫濕度偵測、自動消防滅火系統）……等。
	倉庫/庫房	
	建築保護設施	

資訊資產-機密等級區分

分級	評估標準說明
機敏	■ 含機密或敏感資訊，僅提供<u>少數</u>相關業務<u>承辦人員</u>及其<u>主管</u>或<u>被授權</u>之<u>單位</u>及<u>人員</u>使用。 ■ 發生資通安全事件可能造成<u>未經授權</u>之資訊<u>揭露</u>，對機關之營運、資產或信譽等方面將產生<u>非常嚴重或災難性</u>之影響。 ■ 資訊資產存取權限須經由<u>高階主管</u>核准同意。
內部使用	■ 含部分敏感資訊，僅供組織<u>內部人員</u>或<u>被授權</u>之<u>外部單位</u>使用。 ■ 發生資通安全事件可能造成<u>未經授權</u>之資訊<u>揭露</u>，對機關之營運、資產或信譽等方面將產生<u>嚴重</u>之影響。 ■ 資訊資產存取權限須經由單位<u>權責主管</u>核准同意。
一般	■ 為一般性資料可對外公開，但須<u>遵守</u>相關<u>發布流程</u>。 ■ 發生資通安全事件可能造成<u>未經授權</u>之資訊<u>揭露</u>，對機關之營運、資產或信譽等方面將產生<u>有限</u>之影響。 ■ 資訊資產存取權限只須經由資訊資產<u>使用者</u>同意。



資訊資產-人員類

等級	量化值	機密性	完整性
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）。	- 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	其工作執掌可存取內部使用類資料及一般類資料。	- 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	其工作執掌僅可存取一般類資料。	- 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。 - 僅影響少數承辦人的作業。



資訊資產-人員類

等級	量化值	可用性
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，<u>可容忍</u>替換時間為<u>4小時</u>。 - 業務高度仰賴該員，且一旦該員無法作業時，將<u>影響對外</u>所提供的<u>服務</u>作業。以內
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，<u>可容忍</u>替換時間為<u>12小時</u>。 - 業務仰賴該員，且一旦該員無法作業時，將<u>影響多數部門</u>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，<u>可容忍</u>替換時間為<u>24小時</u>。 - 業務仰賴該員，且一旦該員無法作業時只<u>影響少數承辦人員</u>作業，其工作可暫時委由他人替代。

資訊資產

-硬體、軟體、資訊及環境保護類

等級	量化值	機密性
高	3	- 機密或敏感性資訊處理設施與系統資源，僅開放給<u>必要知道的人</u>使用。 <u>發生資通安全事件可能造成未經授權之資訊揭露</u>，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。
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<u>內部人員</u>使用。 <u>發生資通安全事件可能造成未經授權之資訊揭露</u>，對機關之營運、資產或信譽等方面將產生嚴重之影響。
低	1	- 不限制使用資訊處理設施與系統資源等。 <u>發生資通安全事件可能造成未經授權之資訊揭露</u>，對機關之營運、資產或信譽等方面將產生有限之影響。

資訊資產資訊資產

-硬體、軟體、資訊及環境保護類

等級	量化值	完整性
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<u>顯著的衝擊</u>。 - 發生資通安全事件可能造成資訊<u>錯誤或遭竄改</u>等情事，對機關之營運、資產或信譽等方面將產生<u>非常嚴重或災難性之影響</u>。
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<u>輕微的衝擊</u>。 - 發生資通安全事件可能造成資訊<u>錯誤或遭竄改</u>等情事，對機關之營運、資產或信譽等方面將產生<u>嚴重之影響</u>。
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<u>衝擊可以忽略者</u>。 - 發生資通安全事件可能造成資訊<u>錯誤或遭竄改</u>等情事，對機關之營運、資產或信譽等方面將產生<u>有限之影響</u>。

資訊資產資訊資產

-硬體、軟體、資訊及環境保護類

等級	量化值	可用性
高	3	- 僅容許<u>短暫時間</u>（4小時內）<u>無法使用</u>，作業停頓期間極易產生客訴事件，使本公司<u>受到損害者</u>。 - 作業<u>完全仰賴</u>資訊資產，且一旦服務<u>中斷</u>時將<u>影響全組織對外</u>所提供的服務作業。 <u>發生資通安全事件可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。</u>
中	2	- 容許<u>較長時間</u>（8小時內）<u>無法使用</u>，會造成部份人員之抱怨，使本公司受到<u>輕微損害者</u>。 - 作業<u>仰賴</u>資訊資產，且一旦服務<u>中斷</u>時將<u>影響部門運作</u>。 <u>發生資通安全事件可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響。</u>
低	1	- 容許<u>長時間</u>（1天以上）<u>無法使用</u>，作業停頓期間可利用其他替代方案，<u>不致造成本公司之損失</u>。 - 作業<u>仰賴</u>資訊資產，且一旦服務<u>中斷</u>時將<u>影響少數承辦人作業</u>。 <u>發生資通安全事件可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。</u>