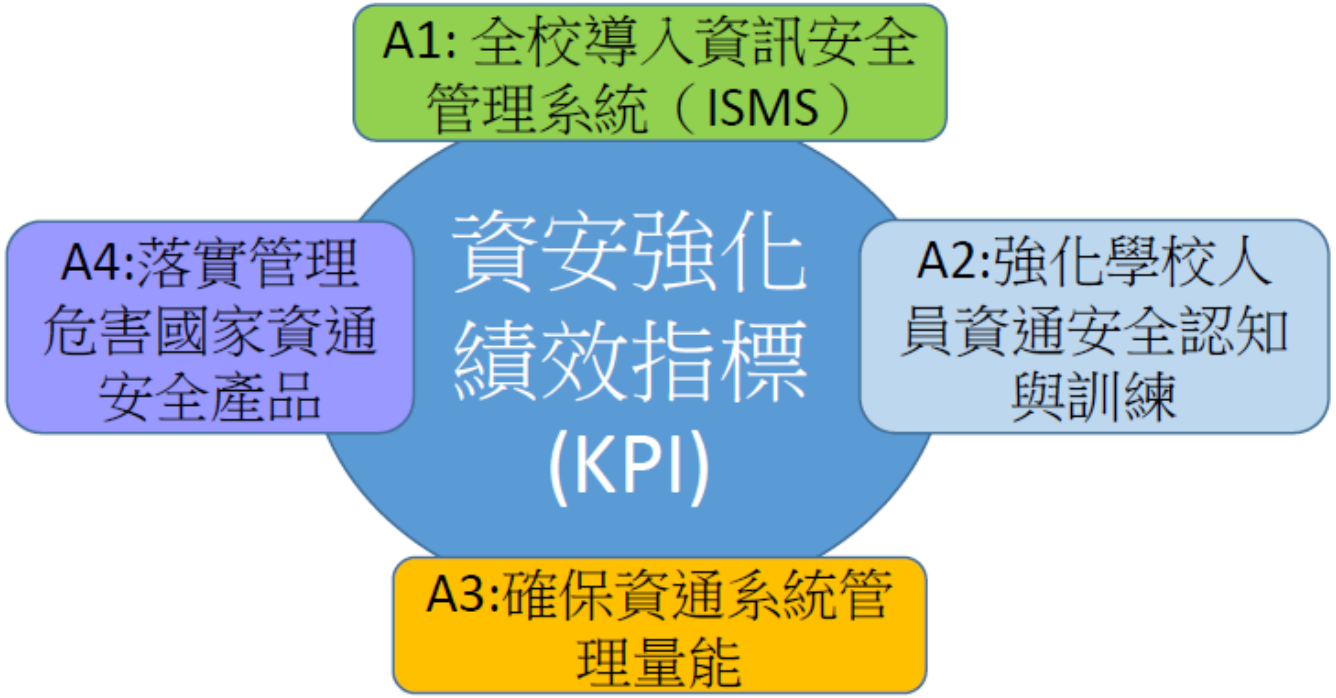
資訊資產盤點、風險評鑑暨業務持續運作演練教育訓練

報告單位：圖書暨資訊處

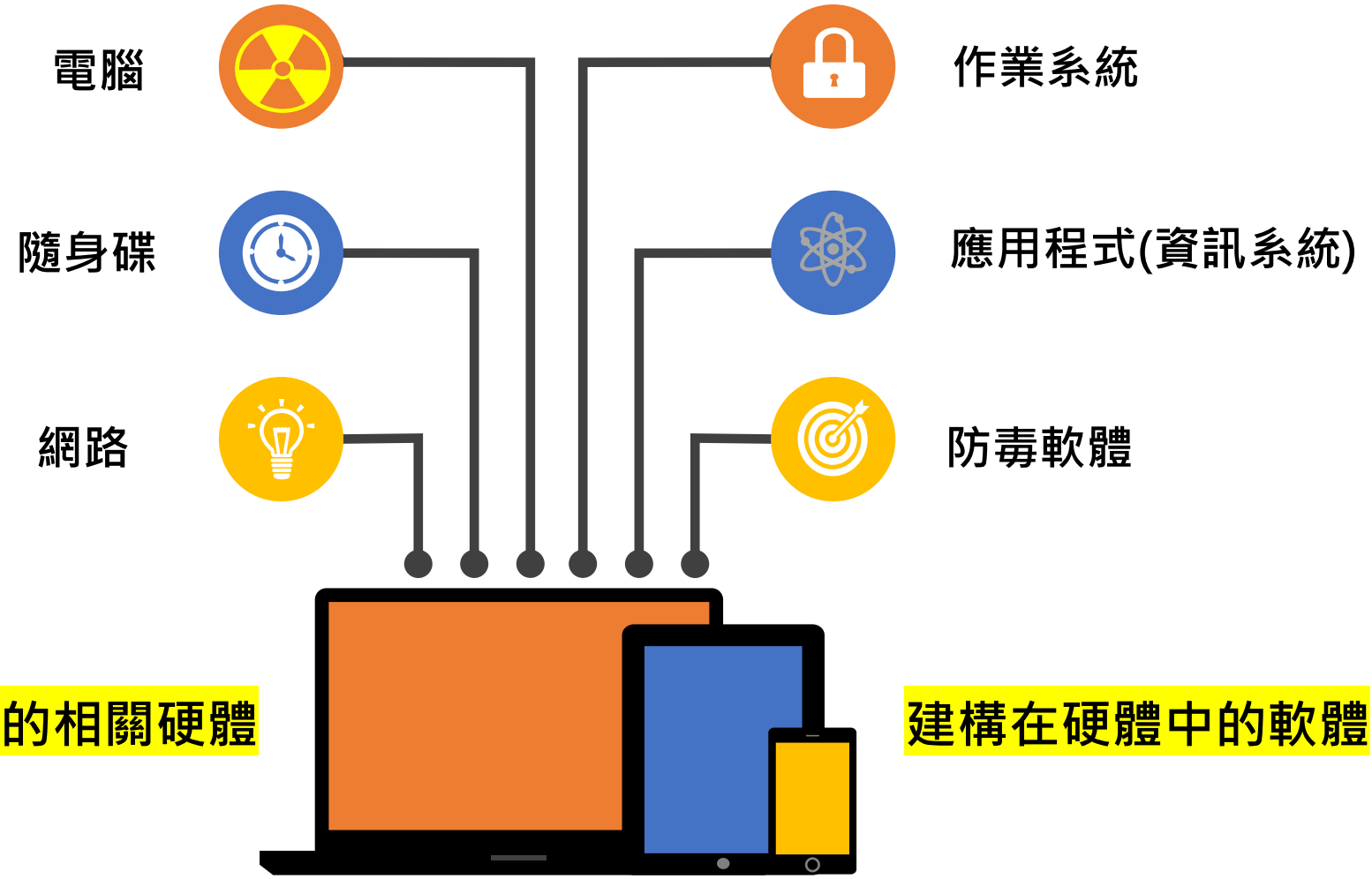
報告人:王彰偉

執行依據

- 資安專章指標**A1:全校導入ISMS(資訊安全管理系統)、A3:強化學校人員資通安全認知與訓練、A4:落實管理危害國家資通安全產品**
  - 資訊資產盤點(含IoT裝置盤點)
  - 風險評鑑
  - 內部稽核



何謂資訊資產



完成資料處理所需的相關硬體

建構在硬體中的軟體

業務執行所需的資料(電子檔)

何謂資訊資產

人員依業務敏感性，也須列為資訊資產，並進行分類

工讀生

協助資料繕打，公文傳送

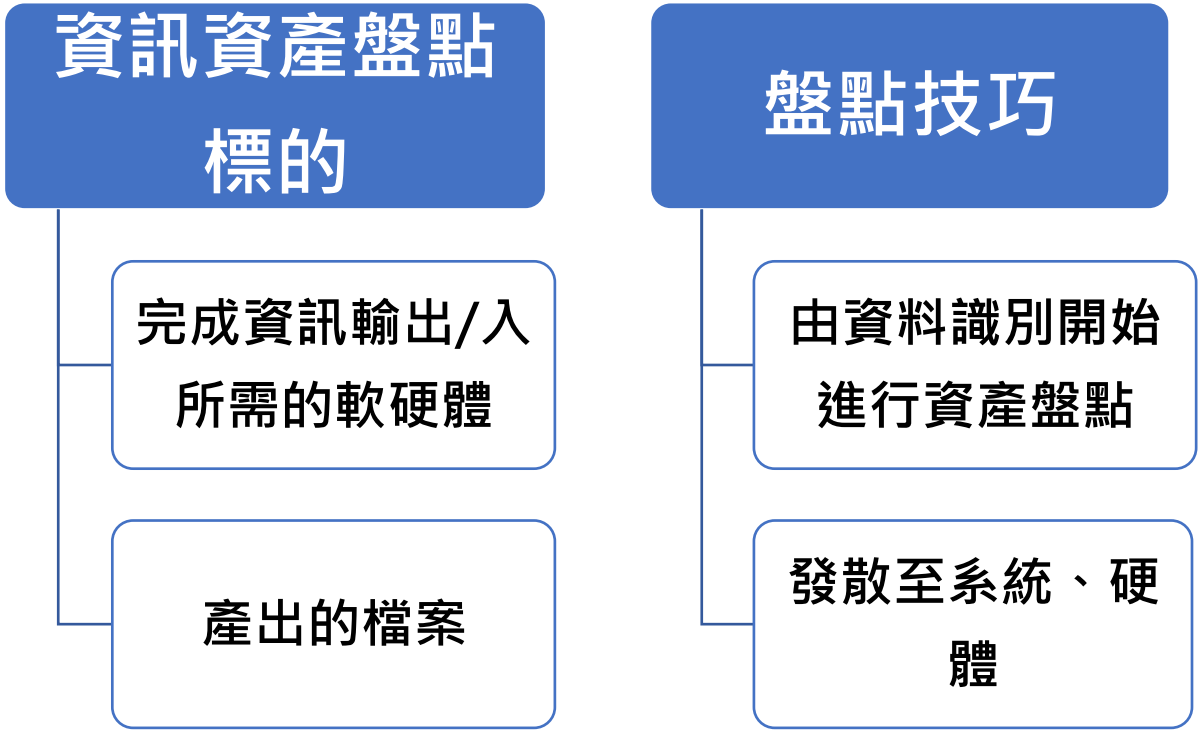
業務承辦人

業務執行人員

單位主管

可以碰觸到敏感等級更高資訊的人員

資訊資產盤點原則



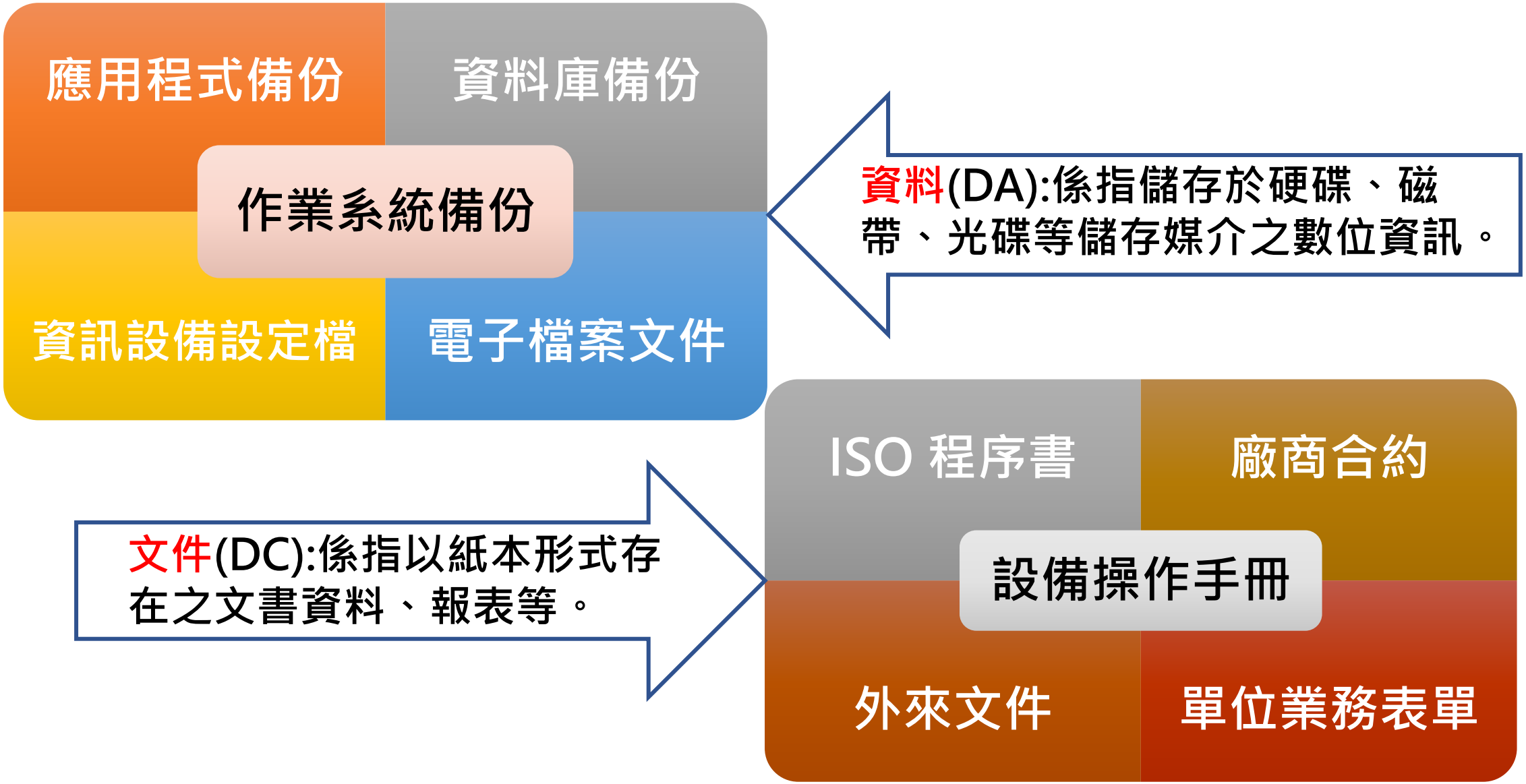
例如:提供服務的系統建構在主機上
使用者透過操作系統輸入資訊彙整產出資料
將這些資料儲存於特定媒體
以上這些皆屬資訊資產盤點範疇

資訊資產分類

須將IoT列入資訊資產盤點

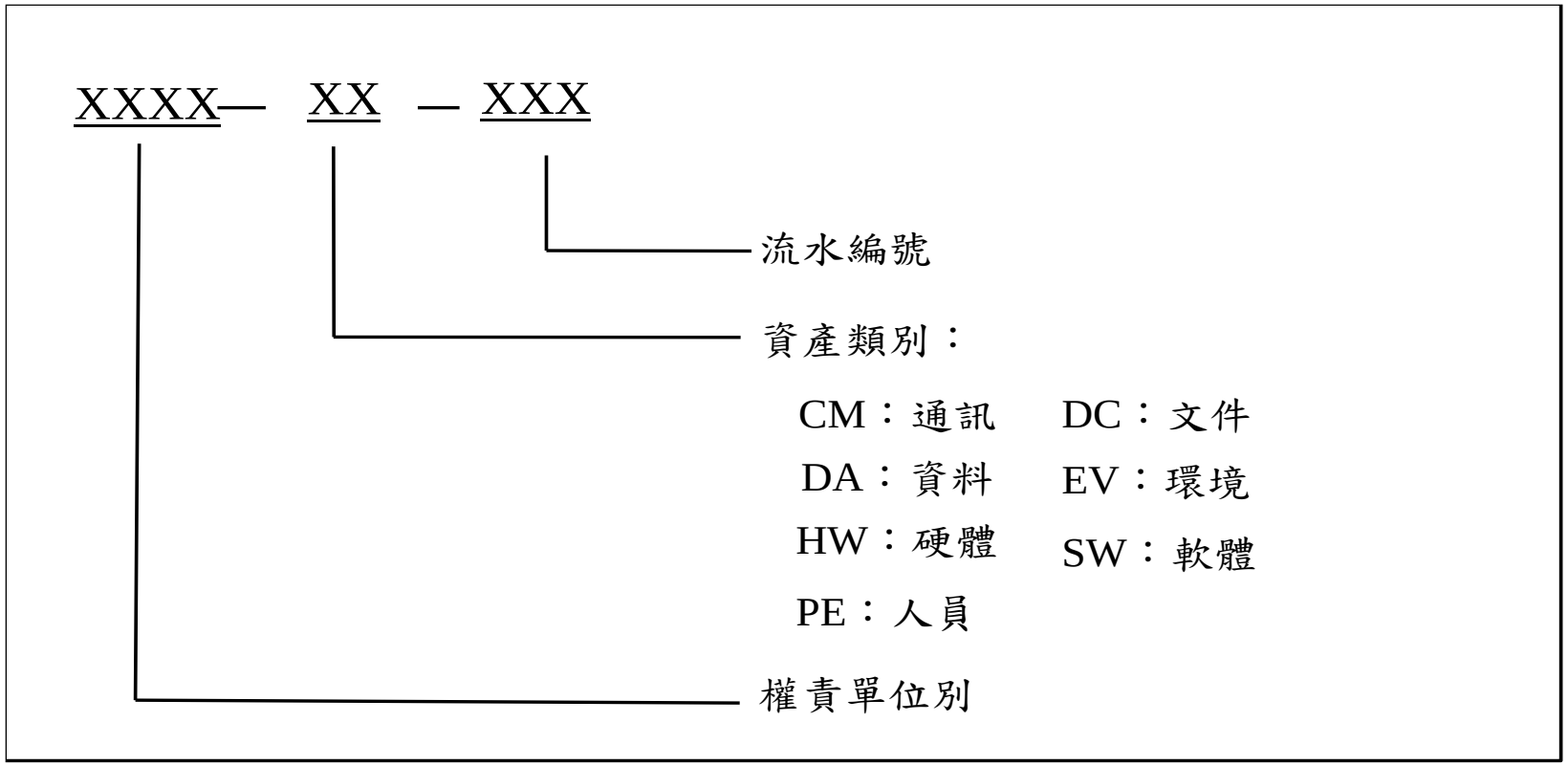

可攜式設備
主機設備
硬體(HW)
印表機
儲存設備


作業系統
windows、Linux
文書軟體
office
軟體(SW)
套裝軟體
考照輔導系統、輔助教學系統
工具軟體
繪圖軟體、壓縮軟體


應用程式備份
資料庫備份
作業系統備份
資訊設備設定檔
電子檔案文件
資料(DA):係指儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊。
文件(DC):係指以紙本形式存在之文書資料、報表等。
ISO 程序書
廠商合約
設備操作手冊
外來文件
單位業務表單

環境(EV):相關基礎設施及服務，包含辦公室實體、實體機房、電力、消防設施、網路攝影機等。

資訊資產編碼方式



資訊資產編碼方式圖

第1~4碼為權責單位別，第5~6碼為資產類別，第7~9碼為資訊資產流水編號。

權責單位別資訊

附件(五)

輔英科技大學各單位文件收發編碼一覽表

董事會					
0100					
校長室					
0200					
副校長室					
0300					
教務處	招生暨入學服務中心	進修業務組	課務註冊組	教師教學發展組	學生學習暨實習發展組
1000	1004	1005	1007	1008	1009
學務處	課外活動指導組	生活輔導組	諮商輔導中心	衛生保健組	職涯發展中心
1100	1101	1102	1104	1105	1106
服務學習中心	原住民族學生資源中心				
1108	1110				
總務處	出納組	營繕組	事務組	採購保管組	
1200	1202	1203	1204	1205	
研究暨產學發展處	研發業務組	產學合作組	創新育成中心		
1300	1304	1305	1306		
秘書室	稽核組	管考組			

劃室					
2400					
國際暨兩岸事務處	國際事務中心	兩岸事務中心	華語文中心		
2500	2501	2502	2503		
推廣教育中心	推廣業務組	教育服務組			
2600	2601	2602			
醫學與健康學院	醫學檢驗生物技術系	物理治療系	保健營養系	健康美容系	~~學士後牙科助理學位學程~~
6000	6002	6003	6004	6006	~~6007~~
環境與生命學院	環境工程與科學系	職業安全衛生系	應用化學及材料科學系	生物科技系	
6100	6101	6102	6103	6104	
人文與管理學院	應用外語系	休閒與遊憩事業管理系	師資培育中心	資訊科技與管理系	幼兒保育暨產業系
6300	6302	6304	6309	6310	6311
護理學院	護理系	健康事業管理系	助產與婦嬰健康照護系	高齡及長期照護事業系	
6400	6401	6402	6403	6404	
共同教育中心	語言教育組~~中心~~	博雅教育組	基本能力教育組		
6500	6501	6502	6503		
老化及疾病預					

教職員資訊服務/行政管理/ISO9002文件/程序書列表/4.5文件與資料管制/文件與資料管制程序書　頁次 16-17

群組化資訊資產

優點：

- 降低風險評鑑負擔，減少弱點、威脅的重複識別。

原則：

- 資訊資產價值相同。
- 資訊資產性質相同，且數量較多。
- 存在於相同的實體、邏輯環境。
- 遭遇弱點、威脅相同。
- 不需知道細部作業，即可進行風險鑑別。

群組化資訊資產

- 具共通性(相同資產價值及風險等級)
- 例如:辦公室行政作業電腦可登載為:

資產編號	資產類別	資產名稱	資產說明	擁有者	保管者	使用者	DA/DC類資產保存年限	大陸品牌	IoT	機密性	完整性	可用性	資產價值
1903-HW-004	HW	個人電腦	XX組辦公室電腦5部 HP Z220	XXX組	XXX組	XXX組				2	2	2	2

- 如為特殊業務用途，則須單獨填列

資產編號	資產類別	資產名稱	資產說明	擁有者	保管者	使用者	DA/DC類資產保存年限	大陸品牌	IoT	機密性	完整性	可用性	資產價值
1903-HW-001	HW	線上語言學習系統主機	HP DL-380	李四	李四	全校師生				3	2	3	3

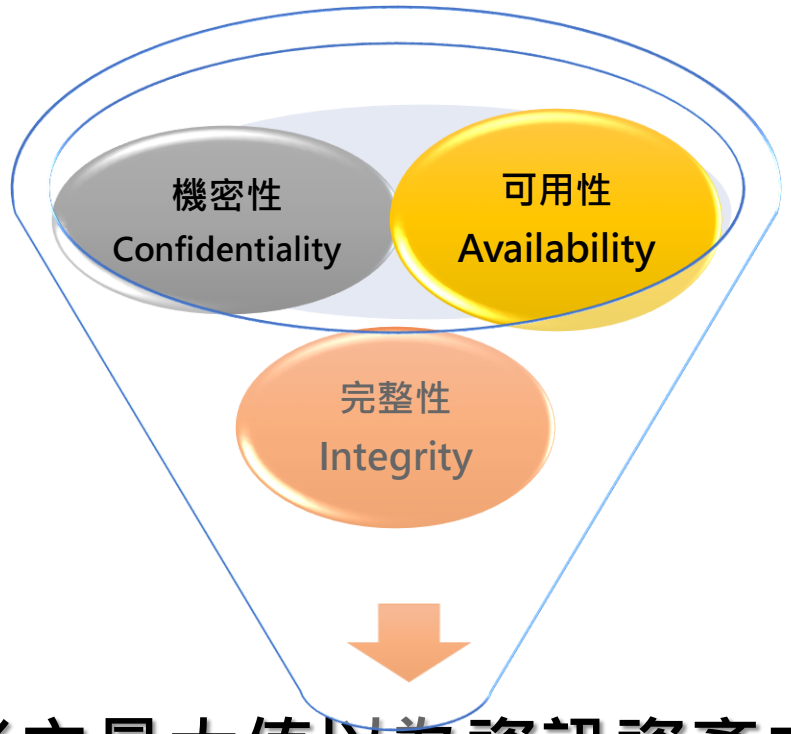
資產編號	資產類別	資產名稱	資產說明	擁有者	保管者	使用者	DA/DC類資產保存年限	大陸品牌	IoT	機密性	完整性	可用性	資產價值
1903-PE-001	PE	XX組行政人員	XX組7名(含組長)	XXX組	XXX組	XXX組				4	1	4	4
1903-PE-002	PE	工讀生	協助資料輸入整理等作業	XXX組	XXX組	XXX組				2	2	2	2
1903-DC-001	DC	一般文件（XX組）	歸檔電子公文、報表、活動文件	XXX組	XXX組	XXX組	依文件規定保存年限			1	1	1	1
1903-DC-002	DC	限閱文件（XX組）	財產移交清冊、計畫清冊	XXX組	XXX組	XXX組	依文件規定保存年限			2	2	1	2
1903-DC-003	DC	敏感文件（XX組）	各標案之規格書、簽約書、財產清冊、系統文件	XXX組	XXX組	XXX組	依文件規定保存年限			3	3	1	3
1903-SW-001	SW	作業系統（系統主機用）	Windows 作業系統	XXX組	XXX組	XXX組				2	2	2	2
1903-SW-002	SW	應用程式	office、Adobe PDF reader、7-ZIP	XXX組	XXX組	XXX組				1	1	1	1
1903-SW-003	SW	線上語言學習系統	空中美語線上學習系統	張三	張三	全校師生				1	2	2	2
1903-DA-001	DA	個人電腦資料（系統組）	辦公室個人電腦資料	XXX組	XXX組	XXX組	依業務需求			3	2	3	3
1903-HW-001	HW	線上語言學習系統主機	HP DL-380	李四	李四	全校師生				3	2	3	3

- **盤點原則:同質性資產群組化，例如辦公室行政用電腦5部，但若屬性不同，則應另外盤出，例如XX服務主機**
- **由硬體到軟體，擴展至業務流程無形資產(電子檔-以個資盤點資料為原則)及有形文件**

資產編號	資產類別	資產名稱	資產說明	擁有者	保管者	使用者	DA/DC類資產保存年限	大陸品牌	IoT	機密性	完整性	可用性	資產價值
1903-HW-002	HW	網路印表機	HP M72630	李四	李四	XXX組			●	1	1	1	1
1903-HW-003	HW	可攜式儲存媒體	創見 外接式硬碟1部	張文曉	張文曉	張文曉				1	1	1	1
1903-HW-004	HW	個人電腦	XX組辦公室電腦5部 HP Z220	XXX組	XXX組	XXX組				2	2	2	2
1903-HW-005	HW	網路附加儲存設備(Network Attached Storage, NAS)	Synology DS420+	XXX組	XXX組	XXX組			●	3	3	3	3
1903-CM-001	CM	網路集線器	ZYXEL GS-108B	王小明	王小明	XXX組				1	1	2	2
1903-CM-002	CM	無線網路基地台	TP-Link RE705X	王小明	王小明	XXX組		●	●	1	1	2	2
1903-EV-001	EV	監視錄影機	AVTECH AVN801	王小明	王小明	XXX組			●	1	1	1	1
1903-EV-002	EV	**環境監控系統**	JMC	王小明	王小明	XXX組			●	1	1	1	1

執行資訊資產填報時，請一併紀錄 廠牌、型號，如為大陸品牌，應特別標示，並依規定進行汰換

資產價值評核方法



- 機密性(confidentiality):
  - 資料不得被未經授權之個人、實體或程序所取得或揭露的特性。
- 完整性(Integrity)：
  - 確保資料無論是在傳輸或儲存的生命週期中，保有其正確性與一致性。
- 可用性(Availability)：
  - 當使用者需透過資訊系統進行操作時，資料與服務須保持可用狀況(能用)，並能滿足使用需求(夠用)。

取3者之最大值以為資訊資產之價值

依據FY-ISMS-B-007 資訊資產管理程序書辦理

機密性等級評估依據

評估標準	數值
此資訊資產無特殊之機密性要求	1
此資訊資產僅供組織內部人員或被授權之單位及人員使用	2
此資訊資產僅供組織內部相關業務承辦人員及其主管，或被授權之單位及人員使用	3
此資訊資產所包含資訊為組織或法律所規範的機密資訊	4

FY-ISMS-B-007 資訊資產管理程序書 6.3.2.1

完整性等級評估依據

評估標準	數值
該資訊資產本身完整性要求極低	1
該資訊資產本身具有完整性要求，當完整性遭受破壞時，不會對組織造成傷害	2
該資訊資產具有完整性要求，當完整性遭受破壞時會對組織造成傷害，但不至於太嚴重	3
該資訊資產具有完整性要求，當完整性遭受破壞時會對組織造成傷害，甚至造成業務終止	4

FY-ISMS-B-007 資訊資產管理程序書 6.3.2.2

可用性等級評估依據

評估標準	數值
該資訊資產可容許失效3天以上	1
該資訊資產可容許失效1天以上，3天以下	2
該資訊資產僅容許失效8小時以上，1天以下	3
該資訊資產僅容許失效8小時以下	4

FY-ISMS-B-007 資訊資產管理程序書 6.3.2.3

資訊資產價值評核注意事項

- 備份資料之機密等級與原有資料相當。
- 資產可用性需合理。
- 機密性評估
  - 資訊資產的機密等級。
  - 人員接觸機密的存取權。
- 完整性評估
  - 資訊資產無法提供完整系統服務或功能時，對組織營運的影響程度。
- 可用性評估
  - 多少(工作)小時內應回復至可運作狀態。

盤點實務

- 從硬體開始盤點(如伺服器、網路設備、儲存設備...等)。
- 再確認硬體中安裝哪些軟體(如作業系統、資料庫軟體、資訊系統...等)。
- 存放哪些資料(如作業所需資料、備份資料...等)。
- 核心系統專用的作業系統或資料庫軟體應獨立一項盤點。

盤點實務(續)

- **維持資訊系統服務正常運作有關的資訊資產**
  - **硬體類**
    - 成績系統主機、儲存設備(成績系統專用，如Storage或NAS)。
  - **網路類**
    - 網路設備(如防火牆、核心交換器、無線網路基地台、路由器...等)。
  - **軟體類**
    - 作業系統、成績系統、資料庫軟體...等。
  - **資料類**
    - 業務用資料電子檔、備份資料...等(可參考個資盤點表)。
  - **人員類**
    - 教、學務、行政系統操作/管理人員。

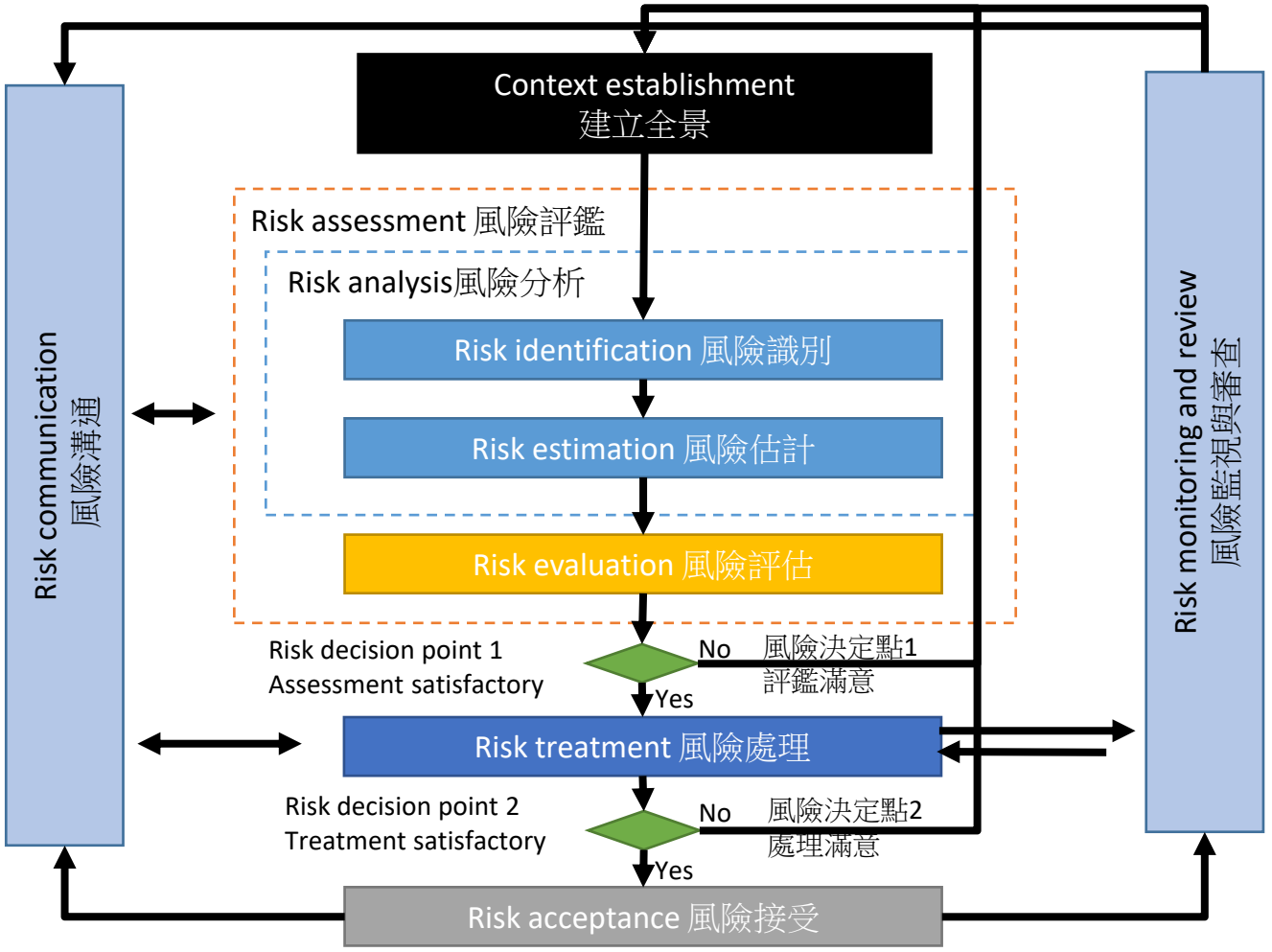
盤點實務(續)

- **軟體類應納入盤點項目**
  - **作業系統**
    - 如Windows 10、 Windows 11、Windows Server、Linux…等。
  - **資料庫軟體**
    - 如MS SQL、Oracle、My SQL…等。
  - **資訊系統**
    - 如成績系統、考照輔導系統、教學輔助系統、…等，大多為客製開發的系統。
  - **套裝軟體**
    - 如防毒軟體、壓縮軟體、繪圖軟體…等。

校園標準軟體清單

- windows 10
- windows 11
- office 2016、 office 2019、 office 2021
- Acrobat Reader
- 7-ZIP
- OfficeScan

風險評鑑

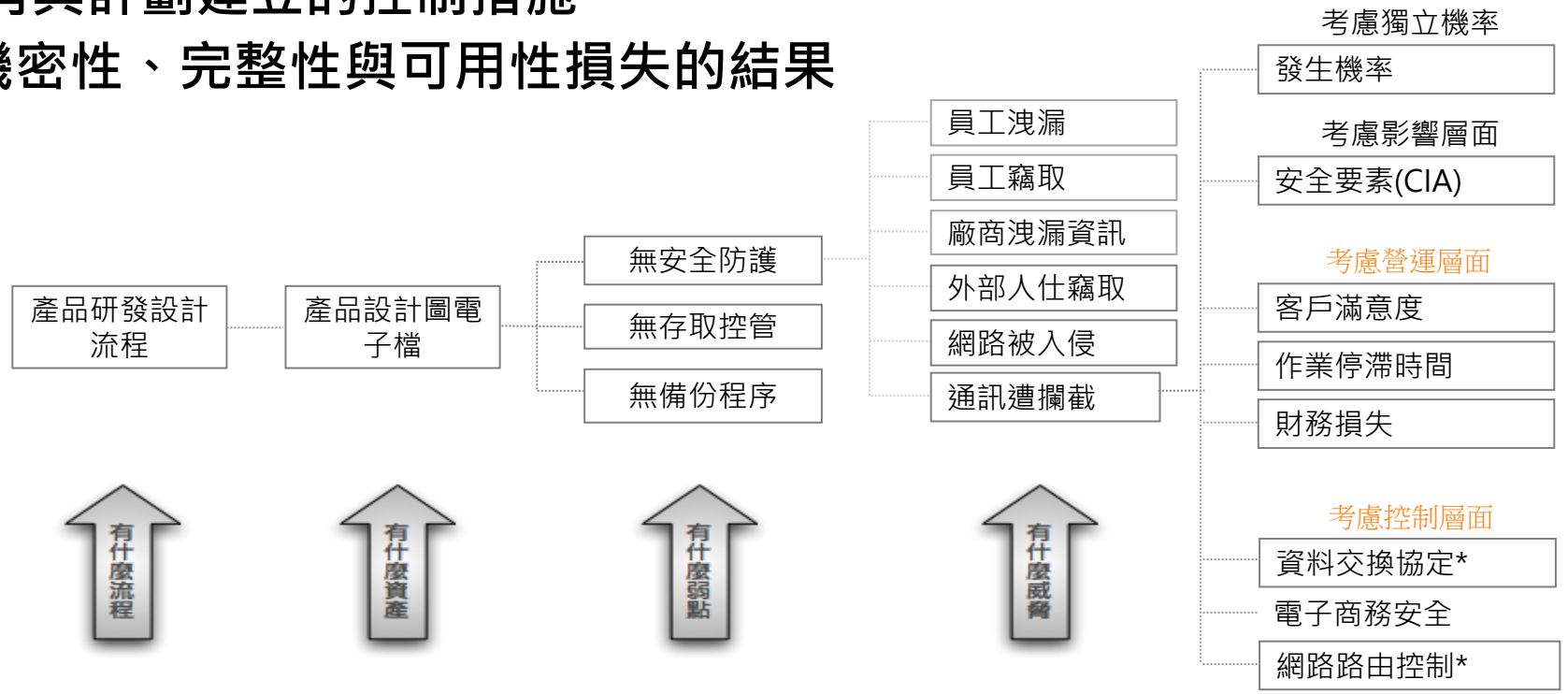


End of first subsequent iteration
結束首次或後續循環

Reference: ISO 27005:2011

風險識別

- 資產-識別範圍內各項資產
- 威脅-識別威脅與其來源
- 弱點-識別受威脅利用而造成資產危害的弱點
- 現有控制措施-識別現有與計劃建立的控制措施
- 結果(後果)-識別資產機密性、完整性與可用性損失的結果



風險

- 所謂「風險」乃是當「威脅」利用其相對應「脆弱性（弱點）」直接或間接造成組織一個或一群「資訊資產」受到損害的「可能性」。
- 風險主要運用「可能性」與「衝擊」的結合定義其特性。
- 「衝擊」指的是對組織或資訊資產產生的影響，可能是負面或正面(機會)。

威脅（Threat）

- 可能對系統或組織造成傷害之意外事件。
- 足以造成資訊資產危害之狀況或事件，例如：破壞、洩漏、篡改資料及阻斷服務而危害。
- 相對於資訊資產，威脅為外來的狀況。
- 威脅通常可以分為：不可抗力因素(例如：地震、颱風)、人為錯誤(例如：資料輸入錯誤、設備操作錯誤)、惡意行動(例如：駭客入侵、竊取資料)。
- 通常以發生可能性或機率進行評估。

威脅發生之可能性評估標準

評估標準	評估值
威脅每季可能發生機會或發生之可能性較低者	1
威脅每周可能發生機會或發生之可能性為中者	2
威脅每天可能發生機會或發生之可能性偏高者	3

弱點（Vulnerability）

- 因資訊資產本身狀況或所處環境之下，可能受到威脅利用而造成資產受到損害之因子。
- 存在於資訊資產或其他組成元件的弱點，如果被威脅利用，會造成危害，例如軟體測試不足、硬體設計缺失、內部控制程序不足等。
- 弱點存在於資訊資產本身，為資產之特性，例如：所在之地理位置、適用材質、使用、設計或管理方式。
- 優點也可能成為弱點，例如：攜帶方便之隨身碟或筆記型電腦。
- 通常以「被威脅利用之難易程度」進行評估。

弱點受到威脅利用之容易度評估標準

評估標準	評估值
該弱點需使用特殊技術或工具且作業時間極長，不容易被威脅利用	1
該弱點使用複雜技術或工具且作業時間長，容易被威脅利用	2
該弱點因使用簡易技術或工具且作業時間短，非常容易被威脅利用	3

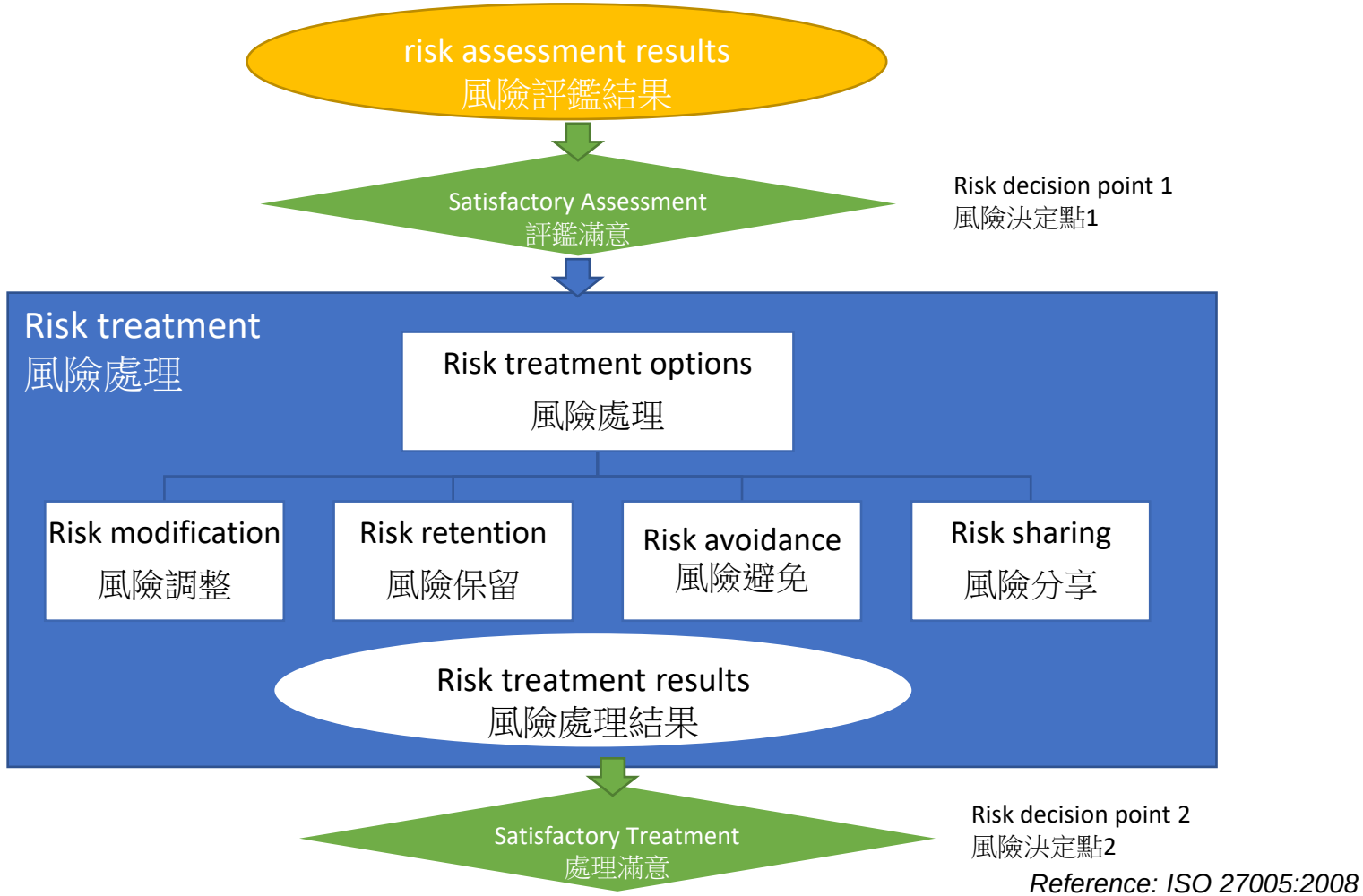
風險值的計算

- 風險值=（資訊資產價值 × 威脅等級 × 弱點等級）

可接受風險值

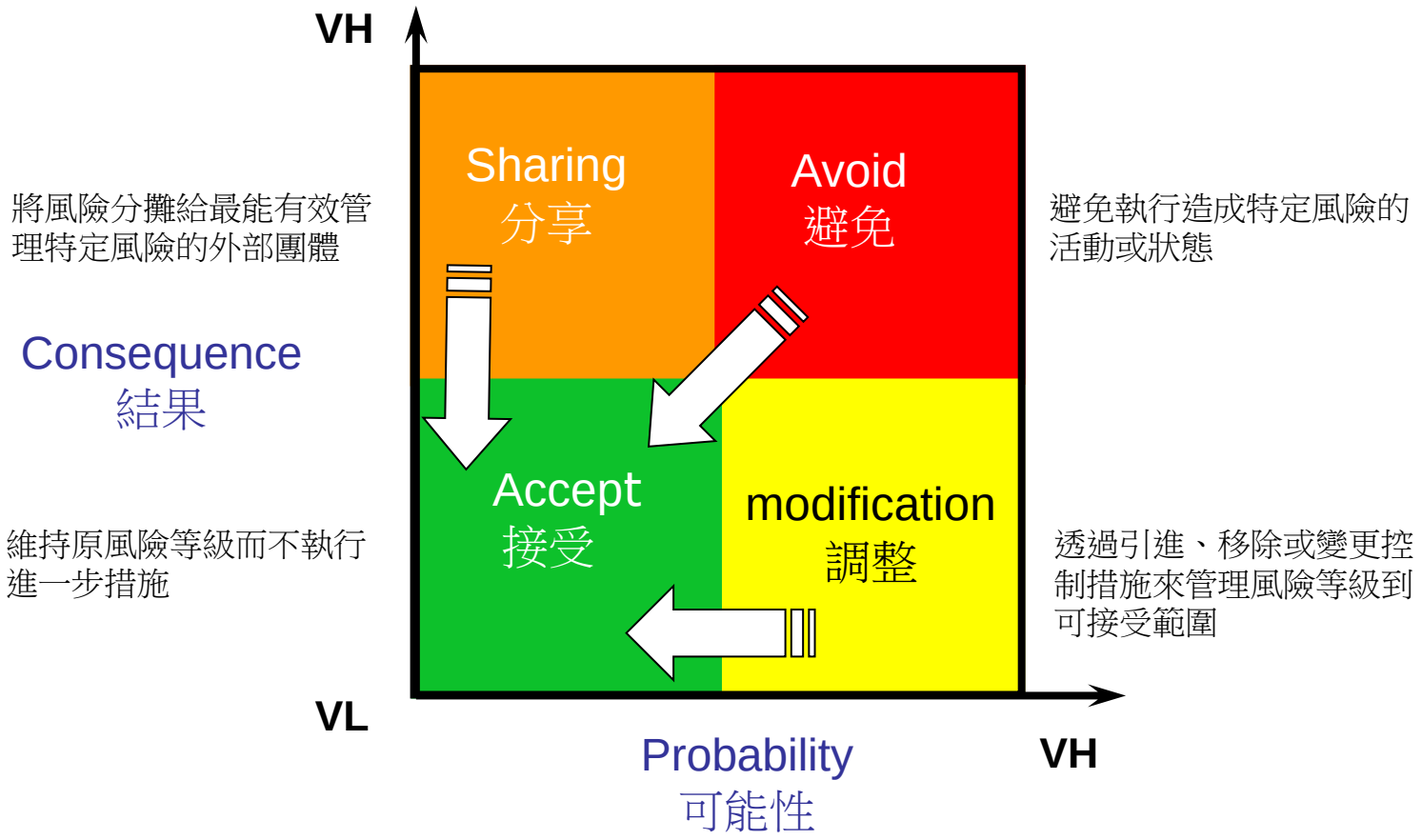
- 本校可接受風險值為**12**
- 執行風險評鑑後風險值為高於12以上者，應於風險改善計畫表提出處理建議方案

風險處理



Reference: ISO 27005:2008

風險處理原理


VH
Sharing
分享
Avoid
避免
Accept
接受
modification
調整
VL
VH
Consequence
結果
Probability
可能性
將風險分攤給最能有效管理特定風險的外部團體
避免執行造成特定風險的活動或狀態
維持原風險等級而不執行進一步措施
透過引進、移除或變更控制措施來管理風險等級到可接受範圍

風險處理原理

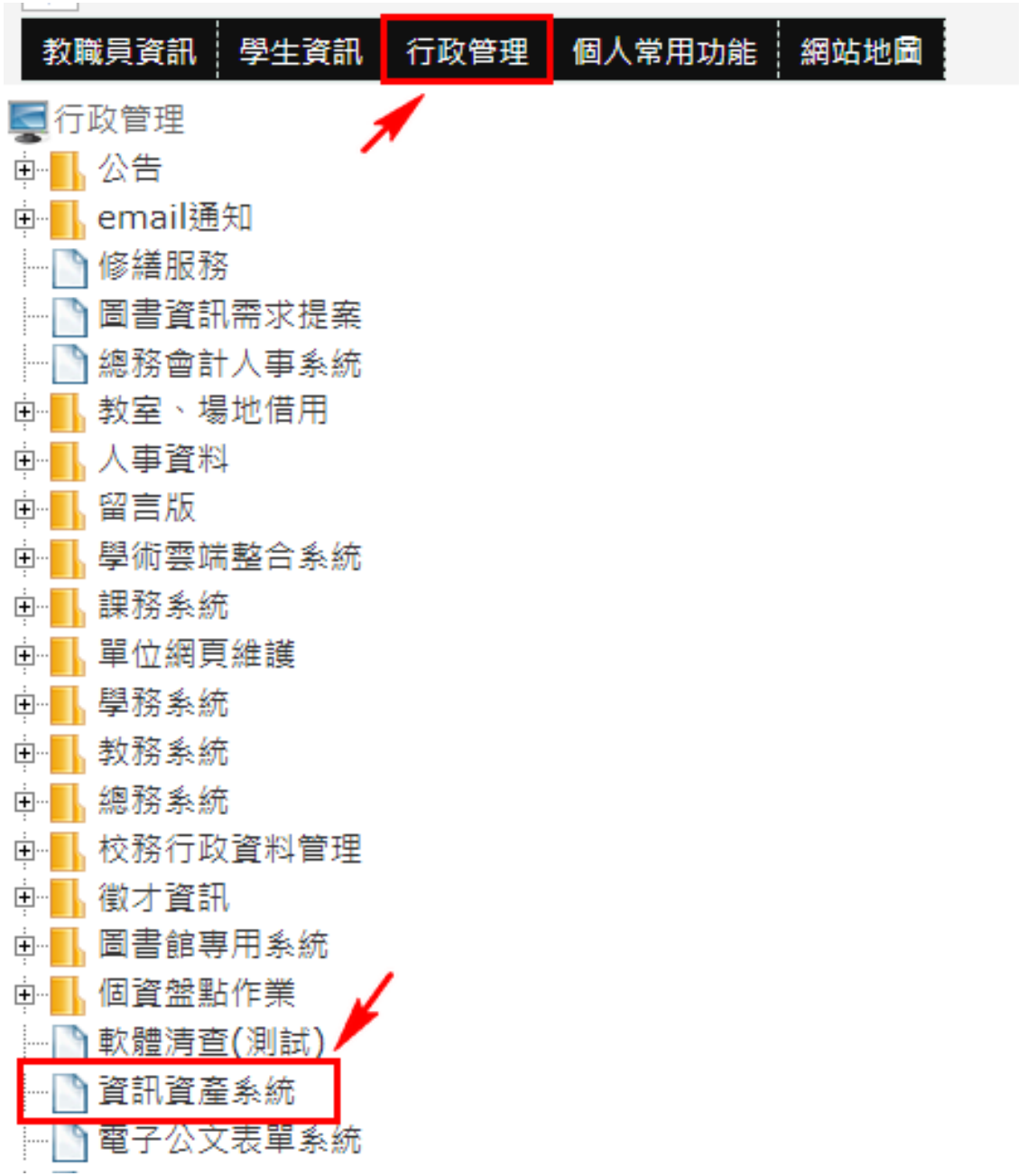
- 接受：風險在可容忍範圍內，得不作處理。
- 規避：風險在可容忍範圍外，處理成本高於利益時，採取不涉入或退出風險。
- 抑減：依風險評估結果，研議及採取適當內部控制或其他機制，降低風險發生之可能性及影響程度，將風險控制在可容忍範圍內。
- 移轉：藉由其他團體承擔或分擔部分風險，降低風險對機關之影響程度。

風險改善計畫表

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	資產擁有者(保管者)	預計改善時間與處理方式	與高風險資產之風險評鑑彙整表對照	風險擁有者確認

資訊資產盤點填報

教職員工資訊服務/行政管理/資訊資產系統



系統會依登入身份，自動帶入相關資料

功能說明

完整資訊資產清單資料

各類別詳細填報內容資料

主管審核狀態查詢

下拉方式選擇填報或匯出資訊資產類別

功能說明

透過檔案匯入資料

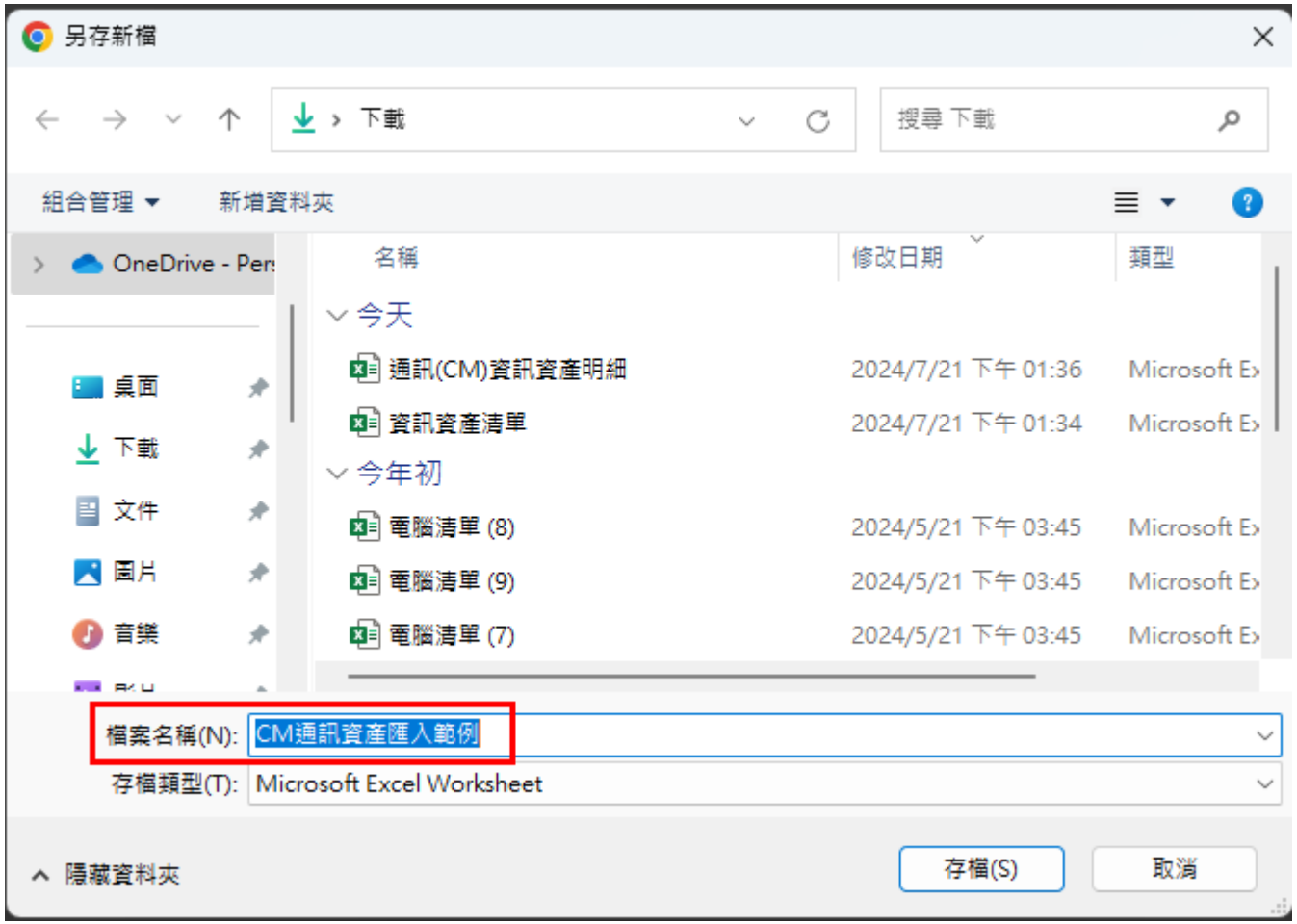
搜尋指定類別或狀態之資料

直接在系統上進行填寫

填寫步驟

- 勾選「資產類別」，下拉選擇所屬資產類別
- 點選「匯入」

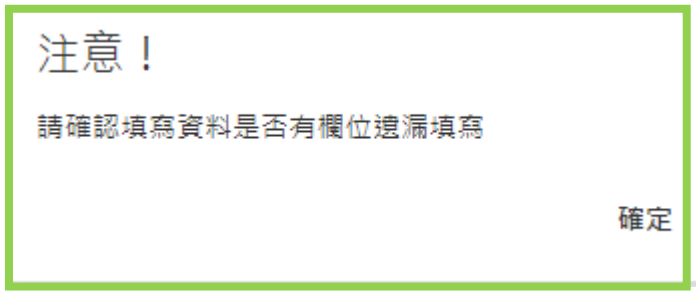
點選「範例下載」



將檔案儲存於電腦中，以便稍後填寫

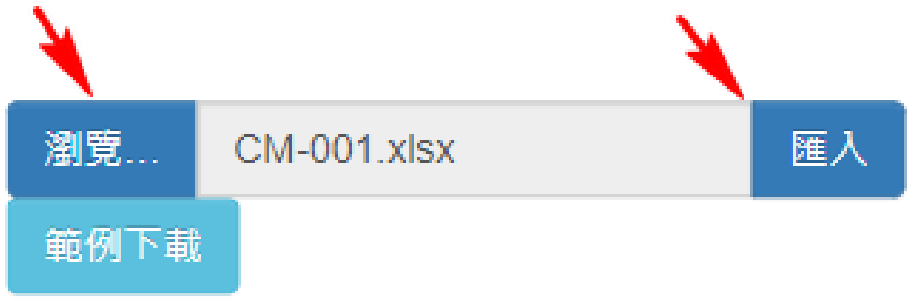
文件名稱：威脅及弱點評估表					機密等級：□一般 ■限閱 □敏感 □機密			
文件編號：FY-ISMS-D-009					版次：1.1			
紀錄編號：	112-				填表日期： 年 月 日			
資產編號：	1902-CM-001	資產類別：	通訊(CM)					
資產名稱：	無線網路基地台	資產說明：	TP-Link Archer BE230					
權責單位：	資訊組	保管者：	王彰偉		使用者：	資訊組		
DA/DC類 資產保存年限	無		是否大陸品牌		Y	是否IoT	Y	
資產價值：	1	機密性	1	完整性	1	可用性	1	
威脅	弱點	威脅等級 低(1)中(2)高(3)		弱點等級 低(1)中(2)高(3)			風險值	
風險類別:硬體								
範例(低輸入1、中輸入2、高輸入3)		1		2			2	
不當維護	不正確的使用軟體和硬體	1		3			3	
	文件化管理之缺乏或不足	1		1			1	
	缺乏有效的變更控制	1		1			1	
	缺乏監督機制	1		1			1	

- 各欄位請依現況進行填寫，有顏色的欄位皆須填寫!
- 每筆資產需自成一個檔案，才能匯入
- 填寫時請注意資產類別，不同類別會有不同評估條件



資料匯入

通訊(CM)資訊資產資料匯入



資訊資產清單

查詢條件

匯入 新增

資訊資產清單下載 資訊資產明細下載

搜尋

填寫年度： 112 資產類別： 請選擇 狀態： 請選擇

填寫年度	資產編號	自行編號	資產類別	資產名稱	資產說明	擁有者	保管者	使用者	DA/DC類資產保存年限	大陸品牌	IoT	機密性	完整性	可用性	資產價值	風險值	狀態	明細
112	1902-CM-001	1902-CM-001	CM	無線網路基地台	TP-Link Archer BE230	資訊組	王彰偉	資訊組	無	Y	Y	1	1	1	1	3	待審核	查看

主管審核

所有資訊資產需逐筆進行審核，主管欲執行審核時請點選「查看」

通訊(CM)資訊資產風險明細

審核通過

文件名稱：威脅及弱點評估表　　機密等級：□一般 ■限閱 □敏感 □機密

文件編號：FY-ISMS-D-009　　版次：1.1

紀錄編號：112 -029　　填表日期：113 年7/ 月7 日

資產編號：	CMTEST3	資產類別：	通訊				
資產名稱：	123	資產說明：	13				
權責單位：	123	保管者：	123	使用者：	123		
DA/DC類資產保存年限	213	是否大陸品牌	Y	是否IoT	Y		
資產價值：	3	機密性	1	完整性	2	可用性	3

威脅	弱點	威脅等級 低(1)中(2)高(3)	弱點等級 低(1)中(2)高(3)	風險值
風險類別:硬體				
範例(低輸入1、中輸入2、高輸入3)		1	2	6
不當維護	不正確的使用軟體和硬體	1	1	3
	文件化管理之缺乏或不足	2	2	12
	缺乏有效的變更控制	3	3	27
	缺乏監督機制	1	1	3
	專業訓練不足	2	2	12
	複雜的使用者介面	3	3	27
硬體失效	不正確的使用軟體和硬體	1	1	3
	沒有作好維護的工作	2	2	12
	缺乏有效變更控制	3	3	27
	缺乏硬體耗損控管	1	1	3
	專業訓練不足	2	2	12
	維護服務回應時間過長	3	3	27

關閉

確認資料無誤後點選「審核通過」

通訊(CM)資訊資產風險明細

文件名稱：威脅及弱點評估表　　機密等級：□一般 ■限閱 □敏感 □機密
文件編號：FY-ISMS-D-009　　版次：1.1
紀錄編號：112 -029　　填表日期：113 年7/ 月7 日

資產編號：	CMTEST3	資產類別：	通訊				
資產名稱：	123	資產說明：	13				
權責單位：	123	保管者：	123	使用者：	123		
DA/DC類資產保存年限	213	是否大陸品牌	Y	是否IoT	Y		
資產價值：	3	機密性	1	完整性	2	可用性	3

威脅	弱點	威脅等級 低(1)中(2)高(3)	弱點等級	
風險類別:硬體				
範例(低輸入1、中輸入2、高輸入3)		1		
不當維護	不正確的使用軟體和硬體	1	1	
	文件化管理之缺乏或不足	2	2	
	缺乏有效的變更控制	3	3	27
	缺乏監督機制	1	1	3
	專業訓練不足	2	2	12
	複雜的使用者介面	3	3	27
硬體失效	不正確的使用軟體和硬體	1	1	3
	沒有作好維護的工作	2	2	12
	缺乏有效變更控制	3	3	27
	缺乏硬體耗損控管	1	1	3
	專業訓練不足	2	2	12
	維護服務回應時間過長	3	3	27
風險類別:通訊				
	不正確的使用軟體和硬體	1	1	3

系統提示

審核資料成功

確認

業務持續運作計畫演練_網頁遭置換緊急應變措施

網頁遭竄改緊急應變原則(1/3)

- 參考行政院111年8月資安警戒專案相關會議指示，如發現所轄管系統網站內容遭竄改，應依下列原則辦理**緊急應變**：
  1. 原網站**立刻下架**。(注意亦須完成跡證保全及留存)
  2. **維護公告**網頁：**10分鐘內上架**。
  3. **靜態資訊**網頁：網站功能**無安全疑慮**的部分可先上架**恢復服務**，如純資訊公告、媒體播放等。
  4. 逐步**功能恢復**：網站每次**版更上線前弱點掃描**，確認**無重大安全性弱點**。(必要時加入人工測試)
  5. 全面修復上架。

根據111年全國大專院校資安長會議結論，參考行政院111年8月資安警戒專案相關會議指示

網頁遭竄改緊急應變原則(2/3)

網頁內容遭竄改

原網站
立刻下架

網頁遭竄改緊急應變原則(3/3)

維護公告頁面

電腦版面

手機版面

大專校院應辦事項(網頁遭竄改)

- 依資安法及「臺灣學術網路各級學校資通安全通報應變作業程序」規定，落實**資安事件通報**及**應變**作業(於**知悉1小時內完成通報**)。
  - 訂定內部作業規範且**適用範圍為全校**(含各行政單位、系所)。
  - 實施**教育訓練**或辦理演練，使相關人員確實熟悉作業程序。
- 針對網頁**遭竄改**事件：
  - **備妥應變機制**。請各行政單位、系所**盤點所管網站**，**事先建立維護公告**頁面及**切換機制**，以利及時應變。(發現網站內容遭竄改後10分鐘內切換為維護公告頁面)
  - **「行政單位、系所網頁遭竄改」**應納入學校**業務持續運作演練(BCP)**演練情境，並請相關單位**實際演練緊急應變**作業程序。

紀錄編號：　-

演練規劃表		
承辦人：王彰偉、張文曦、林上智 協辦單位：各單位資安暨個資窗口 規劃演練日期：113 年 07 月 31 日(星期三)、08 月 06 日(星期二)		
演練規劃項目		規劃內容
1	規劃演練目標與範圍	規劃演練目標：發現單位網站內容被竄改時，能在 10 分鐘內下架此網站。 範圍：RPAGE 學術 WEB 應用整合系統(單位網頁)。
2	規劃演練腳本	模擬單位網站內容被竄改，網站管理單位知悉通報流程，立即通知系統開發組管理人員於 10 分鐘內下架此網站。
3	規劃演練所需設備	無(依本校 FY-ISMS-B-016 業務持續運作管理程序書 6.4.3.2 項說明，採書面測試（Walk-through tests）方式辦理。
4	規劃演練所需系統	無(依本校 FY-ISMS-B-016 業務持續運作管理程序書 6.4.3.2 項說明，採書面測試（Walk-through tests）方式辦理。
5	規劃演練所需參與人員	各單位資安暨個資窗口同仁、系統開發組網站系統管理人員。
6	規劃演練時程及完成時限（完成時限參考衝擊分析）	演練時程：113 年 07 月 31 日、08 月 06 日。 完成時限：10 分鐘內。
7	規劃演練測試方式	1.模擬單位網站內容被竄改，進行通報作業。 2.以模擬畫面進行以下處理機制說明: A. 啟用獨立運作之網站主機(已事先完成網頁維修中之內容)。 B. 關閉網頁被竄改之網站站台。 C. 測試獨立運作之網站主機是否正常運作。 3.各單位參與演練人員填寫「資訊安全事件報告單」。
8	規劃演練成果的檢討時程	113 年 08 月 07 日 09 時 00 分
承辦人員		單位主管		資通安全長	

文件名稱：業務持續運作計畫演練活動紀錄　機密等級：□一般 □限閱 ■敏感 □機密
文件編號：FY-ISMS-D-043　版次：1.1

113 年度業務持續運作計畫演練腳本(113 年 7 月 31 日)

系統範圍：單位首頁

時間	動作	參與人員	地點	備註
113/07/31 11:00	演練開始	各單位資安暨個資窗口同仁	B502 電腦教室	
113/07/31 11:00~11:03	模擬單位網站內容被竄改。	各單位資安暨個資窗口同仁	B502 電腦教室	
113/07/31 11:03~11:10	以模擬畫面進行以下流程說明 1.單位網站內容被竄改，網站管理單位立即通知系統開發組管理人員 2.網站管理人員確認網頁內容被竄改後，關閉網頁被竄改之網站主機。 3.啟用獨立運作之網站主機(已事先完成網頁維修中之內容)，並將網頁被竄改之網站主機網域名稱的 IP 設定，調整為此獨立運作網站主機之 IP。 4.完成系統相關設定後，使用連線測試電腦測試獨立運作網站主機是否正常運行。 5.模擬演練完成後，關閉獨立運作網站主機、啟用原本之網站主機並復原已被竄改的學校首頁。 6.復原網站主機網域名稱的 IP 設定，並使用連線測試電腦進行測試，確保學校首頁運作正常。	各單位資安暨個資窗口同仁	B502 電腦教室	
113/07/31 11:10~11:30	1.填寫「資訊安全事件報告單」。 2.通知資訊安全官事件處理進度。	各單位資安暨個資窗口同仁	B502 電腦教室	「資訊安全事件報告單」

本文件為輔英科技大學圖書暨資訊處專有之財產，非經書面許可，不得透露或使用本文件，亦不得複印、複製或轉變成任何其他形式使用。

輔英科技大學 Fooyin University

https://www.fy.edu.tw

網站導覽 分機資訊 如何來輔英 聯絡我們 行事曆 English 簡體版 關鍵字

輔英科技大學
Fooyin University

關於輔英 學術單位 行政單位 境外招生 推廣教育 附設單位

招生資訊 校友貴賓 教職員工 學生專區 未來學生

- 招生資訊網
- 防疫專區
- 圖書服務Library
- 樂齡推廣
- 單位分機
- 單位信箱
- CIS形象識別
- 校園新聞總覽
- 職涯諮詢輔導
- 性別平等專區
- 智慧財產權專區

- 輔英科技大學校友總會
- 消除一切形式種族歧視國際公約(ICERD)專區
- 高雄市大寮區教育會
- 校務基金勸募平台
- 資訊安全與個資資料保護專區
- 輔英104
- 校園博覽會專區
- 鵬圖藝文展覽中心
- 校園影像館

- 如何來輔英
- 交通路線圖
- 輔英科大無障礙設施平面圖
- 企業徵才專區
- 校友資料庫
- 應屆畢業生\校友流向及雇主滿意度問卷調查

- 技術士技能檢定測試服務網
- 公、勞保員工人數統計
- 海外工作情形返國後調查問卷
- 身心障礙者權利
- 衛生福利部專區
- 科技部

哈哈！此網頁已被置換！

通報及處置流程

- 請立即通報「系統開發組」，分機#2830 協助將受影響站台下架
- 系統開發組於接獲通知後，會立即協助將受影響站台調整為「網站維護中」(參考畫面如下頁)
- 除進行通報外，請詳細檢查網站內容，確認受影響範圍(網頁、資料)
- 填寫「資訊安全事件報告單」(圖書暨資訊處/資訊服務/網路服務/作業表單--下載區)
- https://inf.fy.edu.tw/p/412-1079-10554.php?Lang=zh-tw
- 待完成影響範圍評估及事件調查後，進行網站資料復原或重建

網站維護中 Under Construction

不安全 | 140.127.86.45

匯入我的最愛 | 輔英科技大學 Fooyi...

~ Since 1958 ~

輔英科技大學
Fooyin University

網站維護中 Under Construction

聯絡我們

地址：83102 高雄市大寮區進學路151號　07-7811151

校園安全緊急聯絡電話：0933-608660(校安中心) 、校內分機：2911

本站建議使用 Google Chrome ，並設定 1280x 1024 解析度 以獲最佳瀏覽效果

通報人聯絡資料			
單位名稱	XX 系	通 報 人	張 XX
電　　話	07-7811151#0000	電子郵件	xx@fy.edu.tw
資訊安全事件通報事項			
發生時間	113 年 07 月 31 日 11 時 00 分		
設備資料	IP 位址（無；可免填）：140.127.86.110 Web 位址（無；可免填）：inf.fy.edu.tw/?Lang=zh-tw 設備廠牌、機型：VM 虛擬機 作業系統名稱、版本：CentOS 7(64-bit) 已裝置之安全機制：防毒軟體、端點防護		
資訊安全事件資料			
事件影響等級	□4 級	□3 級	■2 級　□1 級
事件分類	□非法入侵	□感染病毒	□阻斷服務　■其他
破壞程度	□系統當機	□資料庫毀損	■網頁遭篡改　□其他
事件說明	接獲通報發現系所網站內容被竄改。		
可能影響範圍及損失評估	因學校首頁與各單位網站皆使用相同(rpage)系統，故單位網站內容被竄改時，其他網站可能也會有類似問題。		
應變措施	下架被竄改之站台，啟用獨立運作網站讓網頁維護中之訊息公告周知。		
期望支援項目：			
解決辦法： 1.通報網站系統管理單位(系統開發組)協助下架被竄改的站台。 2.網站管理單位執行以下程序 ● 確認影響範圍，檢查站台內所有資料 ● 將受影響資料進行復原處理 ● 待站台服務復原後再次進行檢查			
解決時間	113 年 07 月 31 日 11 時 10 分		

承辦人員	權責主管	資通安全長

紀錄編號：　　-

通報人聯絡資料			
單位名稱	XX 系	通 報 人	張 XX
電　　話	07-7811151#0000	電子郵件	xx@fy.edu.tw
資訊安全事件通報事項			
發生時間	113 年 07 月 31 日 11 時 00 分		
設備資料	IP 位址（無；可免填）：140.127.86.110 Web 位址（無；可免填）：inf.fy.edu.tw/?Lang=zh-tw 設備廠牌、機型：VM 虛擬機 作業系統名稱、版本：CentOS 7(64-bit) 已裝置之安全機制：防毒軟體、端點防護		
資訊安全事件資料			
事件影響等級	□4 級	□3 級	■2 級　□1 級
事件分類	□非法入侵	□感染病毒	□阻斷服務　■其他
破壞程度	□系統當機	□資料庫毀損	■網頁遭篡改　□其他
事件說明	接獲通報發現系所網站內容被竄改。		
可能影響範圍及損失評估	因學校首頁與各單位網站皆使用相同(rpage)系統，故單位網站內容被竄改時，其他網站可能也會有類似問題。		
應變措施	下架被竄改之站台，啟用獨立運作網站讓網頁維護中之訊息公告周知。		

期望支援項目：

解決辦法：

1. 通報網站系統管理單位(系統開發組)協助下架被竄改的站台。
2. 網站管理單位執行以下程序(填報時這句話不用寫)
   - 確認影響範圍，檢查站台內所有資料
   - 將受影響資料進行復原處理
   - 待站台服務復原後再次進行檢查

解決時間	113 年 07 月 31 日 11 時 10 分

承辦人員	權責主管	資通安全長

內稽說明

預計執行時間:113年10月7 日

執行範圍:教務處

稽核計畫將於執行前通知