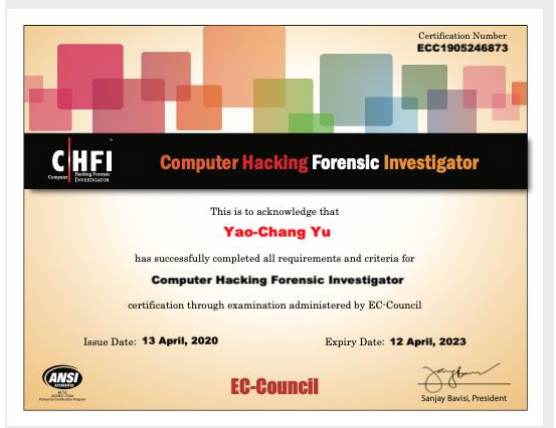
資產鑑別與風險評鑑方法

于燿彰 博士

2023/08/07

講師簡介



- 學歷:
  1. 國立成功大學 工程科學所 博士
  2. 密蘇里大學堪薩斯城校區 資訊工程所 碩士
- 經歷：
  1. 財團法人電信技術中心 資通安全組 副組長
  2. Hermes-Infortech Inc. 資深資安顧問/講師
  3. 鼎智國際技術服務有限公司 技術長/資深資安顧問
  4. USIS INC. 創辦人/技術長/資深資安顧問 （現任）
  5. 鑑智實相科技股份有限公司 協同創辦人/執行長（現任）
  6. 鑑智實相科技股份有限公司（馬來西亞分公司）協同創辦人/技術長（現任）
  7. 國立成功大學工程科學所 兼任助理教授 （現任）
- 專長:
  1. 網路通訊協定安全
  2. 資訊安全
  3. 管理系統(資訊安全、IT服務、營運持續)
  4. 資安產品測試 (ISO/IEC 15408)
  5. 密碼模組測試(FIPS 140-2)
  6. 實體環境安全
  7. 密碼學
- 稽核員資格：
  1. ISO/IEC 27001稽核員
  2. ISO/IEC 17025稽核員
  3. BS 10012稽核員
- 聯絡資訊:

  Email: avis.y@ustar-is.com

大綱

- 風險評鑑的目的
- ISMS風險評鑑要求
- PIMS風險評鑑要求
- ISMS資產鑑別、風險評鑑及風險處理
- PIMS資產鑑別、風險評鑑及風險處理
- D051_個人電腦設定與軟體安裝查核表操作簡介

風險評鑑的目的

不要寄望於敵人可能不來，而要寄希望於我們時刻都要做好禦敵準備，不要寄希望於敵人不會來攻擊，而要寄希望於我們已經無懈可擊。

孫子兵法

風險評鑑的目的

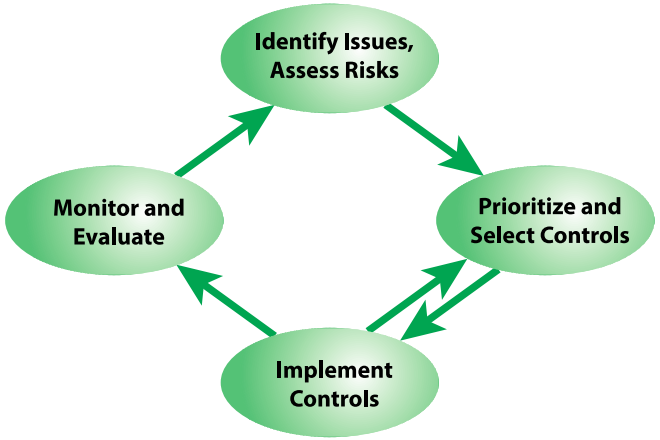
- 風險評鑑之目的主要在分析企業組織在其活動的環境中可能面臨的風險，例如：
  1. 企業投資風險
  2. 生產環境風險
  3. 產品安全風險
  4. IT環境風險
  5. OT環境風險
  6. 資訊安全風險
  7. 隱私風險
  8. …
- 透過有效的風險管控降低風險的發生的機會。（風險處理）

風險管理建立

類別	考慮或標準
風險管理的目的	• 法律的合規性 • 業務持續計畫 • 事故影響計畫 • 描述產品、服務或機制的資訊安全要求
風險評估準則	• 業務資訊流程的戰略價值 • 資訊資產重要性 • 法律、監管要求以結合約業務。 • 可用性、機敏性和完整性對營運和業務的重要性。 • 利害相關者的期望和看法以及對商譽或聲譽的影響。
影響標準	• 受影響的資訊資產的分類級別。 • 違反資訊安全 • 營運受損 • 損害業務和財務價值 • 計畫和截止日期中斷 • 聲譽受損 • 違反法律、法規和合約要求。
風險接受標準	• 確認風險可接受值。 • 不同風險可接受值，可能適用於不同類別的風險。 • 可能包括未來額外處置的要求。

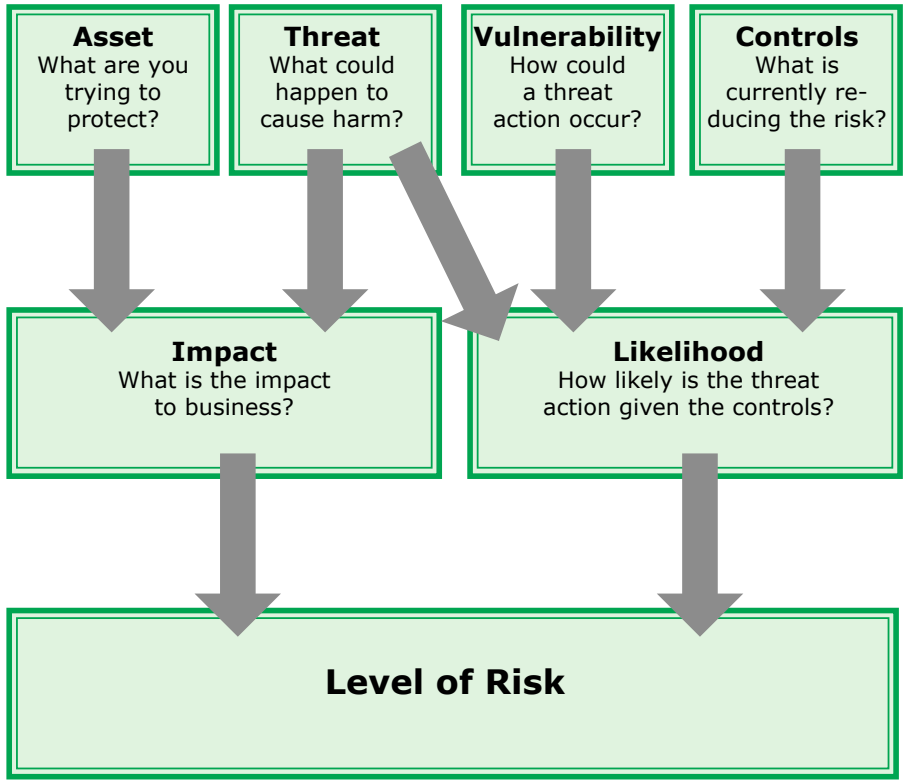
風險管理

- National Institute of Standards and Technology (NIST) Cybersecurity SP 800-37, *Risk Management Framework for Information Systems and Organizations*, 說明:
  - 風險管理包括組織資產評估的規範，結構化和靈活的流程； 安全和隱私控制的選擇，實施和評估； 系統和控制授權； 和持續監控。
  - 它還包括企業級活動，以幫助組織更好地準備在系統上執行風險管理框架。



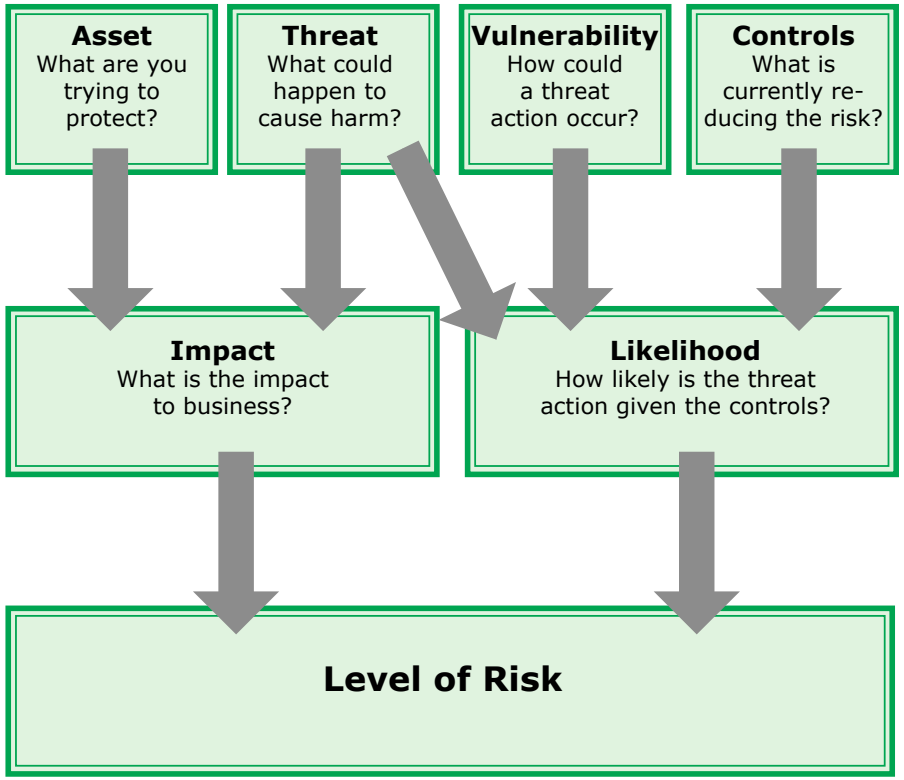
確定風險等級的普遍接受的方法（1/3）

- 在確定影響(Impact)時考慮兩個因素：
  - 資產
    - 編制組織資產的清單，其中包括資產的逐項列出以及每個資產的分配值。
    - 其中包括聲譽和商譽等無形資產，以及數據庫，設備，業務計劃和人員等有形資產。
  - 威脅
    - 對於每項資產，確定可能降低該資產價值的潛在威脅。
- 然後，針對每種資產，確定發生威脅行動的成本或損失值對業務的影響。



確定風險等級的普遍接受的方法（2/3）

- 在確定可能性(Likelihood)時考慮三個要素：
  - 威脅
    - 對於每項資產，確定哪些威脅是相關的並且需要考慮的
  - 弱點
    - 對於資產的每種威脅，請確定對該威脅的脆弱性級別（即，專門針對資產確定如何採取威脅措施）
  - 控制
    - 確定當前有哪些安全控制措施可以降低風險
- 根據威脅行動的可能性和相應控制措施的有效性，確定威脅行動可能造成損害的可能性



確定風險等級的普遍接受的方法（3/3）

- 風險等級被確定為威脅發生帶來的**影響(Impact)**與威脅發生的**可能性(Likelihood)**組合。

威脅和弱點

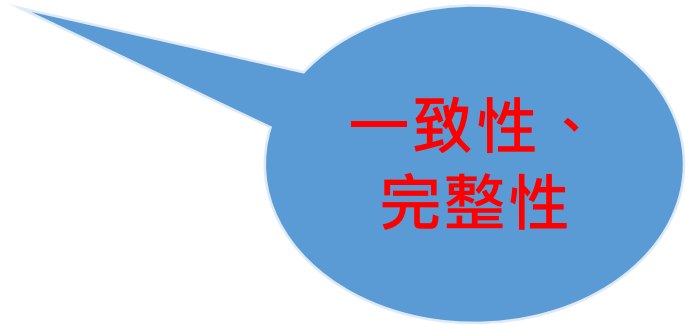
- Threats and vulnerabilities need to be considered together
  - Threat
    - The potential for a threat agent to intentionally or accidentally exploit a vulnerability
    - 威脅代理有意或無意利用弱點的可能性
  - Vulnerability
    - A weakness in a system’s security procedures, design, implementation, or internal controls
    - 系統的安全程序，設計，實施或內部控制方面的弱點

威脅/弱點-範例

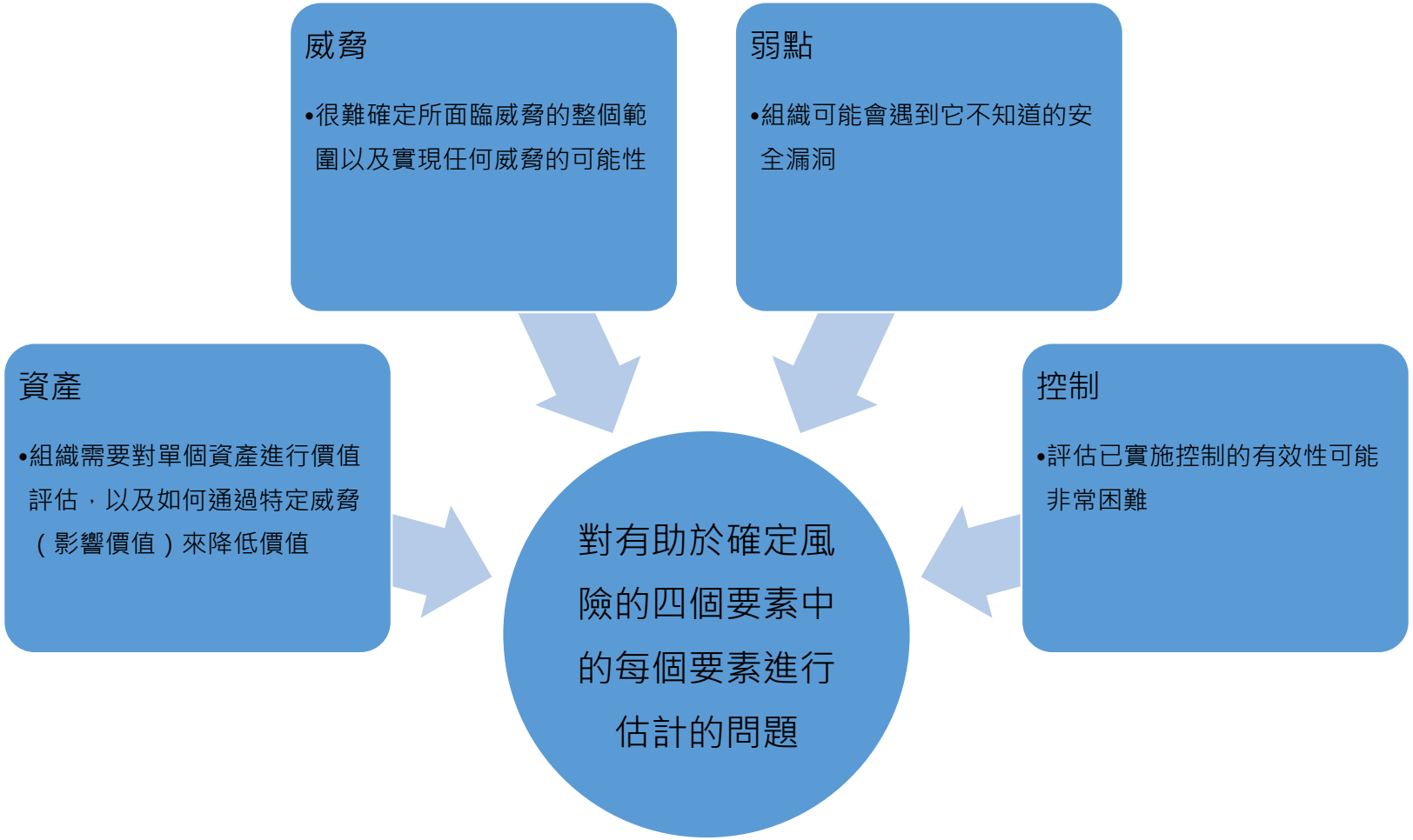
- 風險描述 1：在過馬路時邊走邊滑手機，因而未注意路況所以產生意外事故。
- 風險描述 2：在過馬路時邊走邊滑手機，因而未注意路況所以被路過的轎車撞上。
- 風險描述 3：在過馬路時邊走邊滑手機，因而未注意路況所以被路過的轎車撞上而造成腹腔出血，有生命危險。

風險評估面臨的挑戰

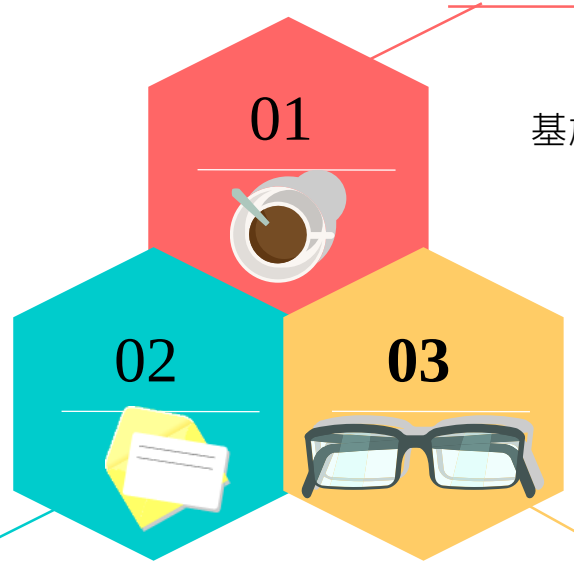
- 組織在確定風險級別時面臨的挑戰分為兩類：
  - 估計難度
  - 預測難度



風險評估


威脅
•很難確定所面臨威脅的整個範圍以及實現任何威脅的可能性
弱點
•組織可能會遇到它不知道的安全漏洞
資產
•組織需要對單個資產進行價值評估，以及如何通過特定威脅（影響價值）來降低價值
控制
•評估已實施控制的有效性可能非常困難
對有助於確定風險的四個要素中的每個要素進行估計的問題

風險評鑑方法論



ISO/IEC 27005 IS Risk Management

基於資訊資產盤點進行風險評鑑

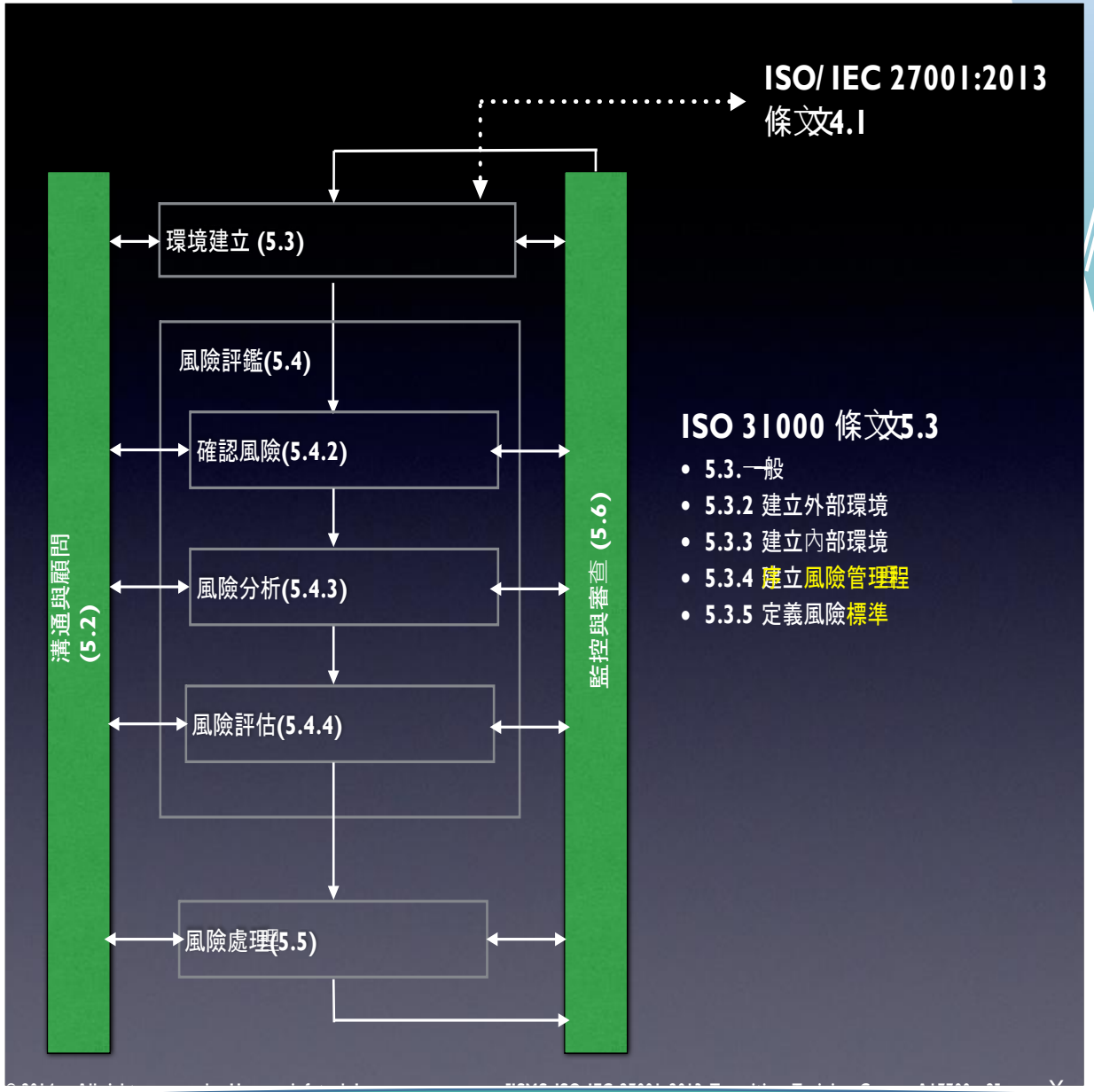
基於組織環境背景及其活動進行風險評鑑

ISO31000 (Risk Management)

NIST SP 800-37 (CSF)

基於組織環境及資訊資產進行風險評鑑

風險評鑑


ISO/ IEC 27001:2013
條文4.1
環境建立 (5.3)
風險評鑑(5.4)
確認風險(5.4.2)
風險分析(5.4.3)
風險評估(5.4.4)
風險處理(5.5)
溝通與顧問 (5.2)
監控與審查 (5.6)
ISO 31000 條文5.3
• 5.3.一般
• 5.3.2 建立外部環境
• 5.3.3 建立內部環境
• 5.3.4 建立風險管理過程
• 5.3.5 定義風險標準

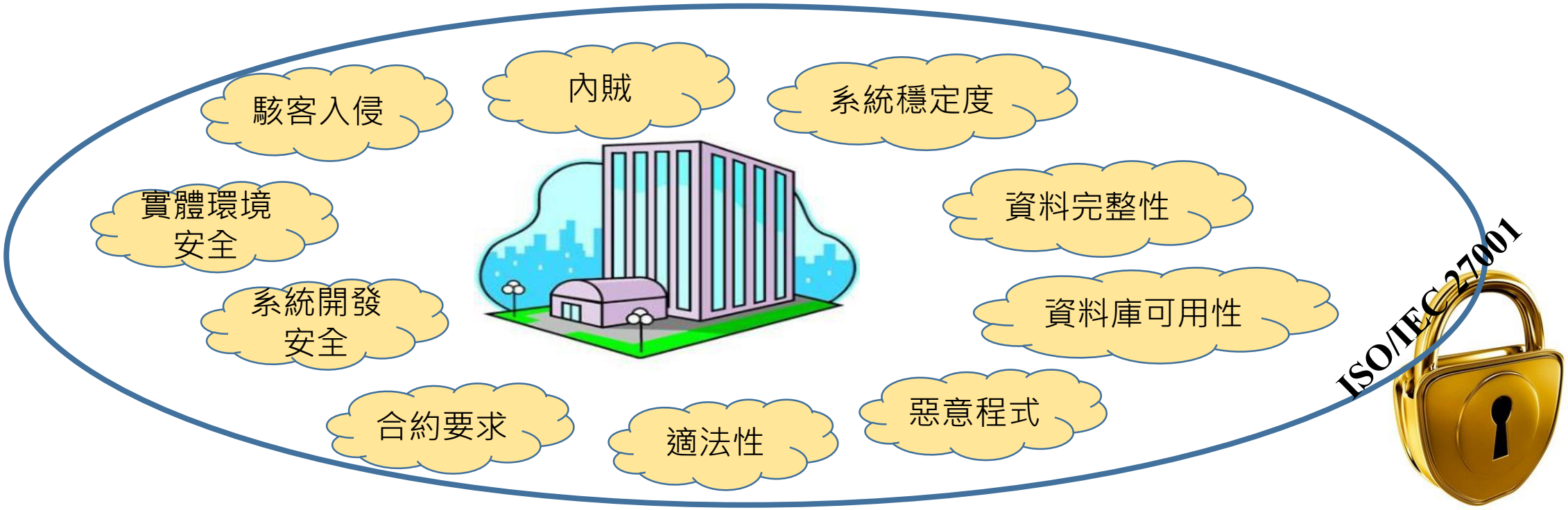
ISMS風險評鑑要求

資訊安全管理系統（ISMS）

- ISMS (Information Security Management System) 是一套有系統地分析和管理資訊安全風險的方法。
- 要達到 100% 的資訊安全是一種過高的期望，資訊 安全管理的目標是透過控制方法，把資訊風險降低 到可接受的程度內。

ISO/IEC 27001的目的

以系統化的方式分析企業資訊資產在其營運的環境中可能面臨的資訊安全風險，進而將資訊安全風險控制在可接受範圍內。



從標準上來看風險評鑑

6. 規劃

6.1 因應風險及機會之行動

6.1.1 一般要求

於規劃資訊安全管理系統時，組織應考量 4.1 所提及之議題及 4.2 所提及之要求事項，並決定需因應之風險及機會，以達成下列事項。

(a) 確保資訊安全管理系統達成其預期成果。

(b) 預防或減少非所欲之影響。

(c) 達成持續改善。

組織應規劃下列事項。

(d) 因應此等風險及機會之行動。

(e) 執行下列事項之方法。

(1) 將各項行動整合及實作於其資訊安全管理系統過程之中。

(2) 評估此等行動之有效性。

6.1.2 資訊安全風險評鑑

組織應定義及應用資訊安全風險評鑑過程於下列事項中。

(a) 建立及維持包括下列準則之資訊安全風險準則。

(1) 風險接受準則。

(2) 履行資訊安全風險評鑑之準則。

(b) 確保重複之資訊安全風險評鑑產生一致、有效及適於比較之結果。

(c) 識別資訊安全風險。

(1) 應用資訊安全風險評鑑過程，以識別資訊安全管理系統範圍內與漏失資訊之機密性、完整性及可用性相關聯之風險。

(2) 識別風險擁有者。

(d) 分析資訊安全風險。

(1) 評鑑若 6.1.2(c)(1)中所識別之風險實現時，可能導致之潛在後果。

(2) 評鑑 6.1.2(c)(1)中所識別之風險發生的實際可能性。

(3) 決定風險等級。

(e) 評估資訊安全風險。

(1) 以 6.1.2(a)中所建立之風險準則，比較風險分析結果。

(2) 訂定已分析風險之風險處理優先序。

組織應保存關於資訊安全風險評鑑過程之文件化資訊。

PIMS風險評鑑要求

5.4.1 Actions to address risks and opportunities

5.4.1.1 General

The requirements stated in ISO/IEC 27001:2013, 6.1.1 along with the interpretation specified in 5.1, apply.

5.4.1.2 Information security risk assessment

The requirements stated in ISO/IEC 27001:2013, 6.1.2 apply with the following refinements:

ISO/IEC 27001:2013, 6.1.2 c) 1) is refined as follows:

The organization shall apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability, within the scope of the PIMS.

The organization shall apply privacy risk assessment process to identify risks related to the processing of PII, within the scope of the PIMS.

The organization shall ensure throughout the risk assessment processes that the relationship between information security and PII protection is appropriately managed.

NOTE The organization can either apply an integrated information security and privacy risk assessment process or two separate ones for information security and the risks related to the processing of PII.

ISO/IEC 27001:2013, 6.1.2 d) 1) is refined as follows:

The organization shall assess the potential consequences for both the organization and PII principals that would result if the risks identified in ISO/IEC 27001:2013, 6.1.2 c) as refined above, were to materialize.

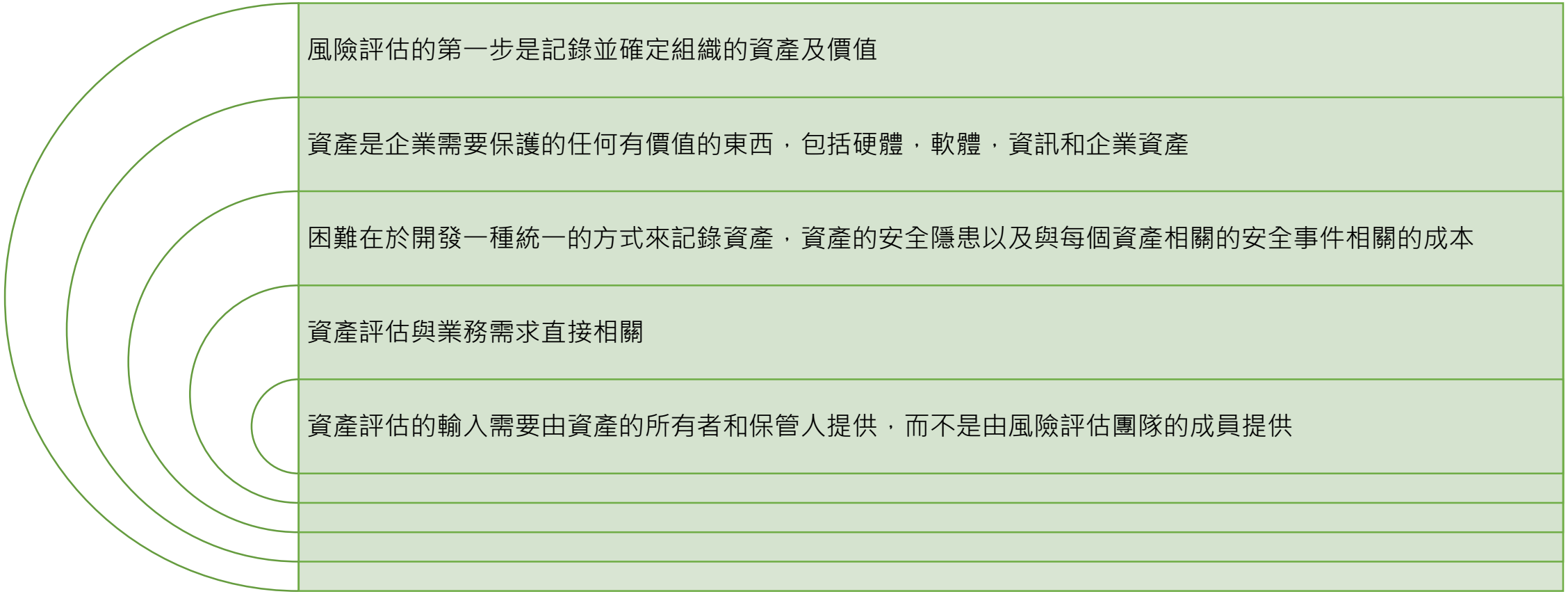
ISMS資產鑑別、風險評鑑及風險處理

A.8 資產管理		
A.8.1 資產責任		
目標：識別組織之資產並定義適切之保護責任。		
A.8.1.1	資產清冊	控制措施 應識別與資訊及資訊處理設施相關聯之資產，並製作及維持此等資產之清冊。
A.8.1.2	資產擁有權	控制措施 清冊中所維持之資產應具擁有者。
A.8.1.3	資產之可被接受使用	控制措施 對與資訊及資訊處理設施相關聯之資訊及資產，應識別、文件化及實作可被接受使用之規則。
A.8.1.4	資產之歸還	控制措施 所有員工及外部使用者於其聘用、契約或協議終止時，應歸還其據有之全部組織資產。

A.8.2 資訊分級		
目標：確保資訊依其對組織之重要性，受到適切等級的保護。		
A.8.2.1	資訊之分級	控制措施 資訊應依法律要求、價值、重要性及對未經授權揭露或修改之敏感性分級。
A.8.2.2	資訊之標示	控制措施 應依組織所採用之資訊分級方案，發展及實作一套適切的資訊標示程序。
A.8.2.3	資產之處置	控制措施 應依組織所採用之資訊分級方案，發展及實作處置資產之程序。

A.8.3 媒體處置		
目標：防止儲存於媒體之資訊被未經授權之揭露、修改、移除或破壞。		
A.8.3.1	可移除式媒體之管理	控制措施 應依組織所採用之資訊分級方案，實作管理可移除式媒體之程序。
A.8.3.2	媒體之汰除	控制措施 當不再需要媒體時，應使用正式程序加以安全汰除。
A.8.3.3	實體媒體傳送	控制措施 應保護含有資訊之媒體於傳送時，不受未經授權的存取、誤用或毀損。

資產鑑別


風險評估的第一步是記錄並確定組織的資產及價值
資產是企業需要保護的任何有價值的東西，包括硬體，軟體，資訊和企業資產
困難在於開發一種統一的方式來記錄資產，資產的安全隱患以及與每個資產相關的安全事件相關的成本
資產評估與業務需求直接相關
資產評估的輸入需要由資產的所有者和保管人提供，而不是由風險評估團隊的成員提供

資訊資產管理作業

- 依據：國立臺南大學 資訊資產管理程序書
- 文件編號：NUTN-ISMS-B003
- 版次：1.7

資訊資產管理作業-定義

- 資訊資產權責單位：
  - 對該項資訊資產具有判斷資產價值、決定存取權限或新增、刪除、修改權限之單位，同時也是資訊資產的擁有單位。
- 資訊資產保管單位：
  - 依據權責單位之需求標準，執行資訊資產日常保護、異動與維護之執行單位。
- 資訊資產使用單位：
  - 因業務需求，經授權可直接或間接使用該資訊資產之單位。

資訊資產管理作業-權責

- 資通安全官：
  - 負責定期審議資訊資產清單及價值評估結果，並督導相關活動之進行。
- 資通安全暨個人資料管理規範導入工作小組：
  - 負責定期辦理資訊資產異動調查與彙整，提供最新之資訊資產清單，並陳報資通安全暨個人資料保護推動委員會。
- 資訊資產權責單位：
  - 負責所管轄內資訊資產之存取授權，並評估與審核資訊資產分類分級及價值之結果，得另指定資訊資產保管單位。
- 資訊資產保管單位：
  - 對於指定資訊資產，具有落實資訊資產權責單位所委託之保護管理責任。
- 資訊資產使用單位：
  - 對於資訊資產之使用，必須依據權責單位要求，並具有正確使用操作之責任。

資訊資產鑑別

- 資訊資產鑑別
  - 各資訊資產權責單位應鑑別所管轄之資訊資產，並建立「資訊資產清單」。
  - 各資訊資產權責單位應定期更新與維護所管轄之資訊資產清單。
  - 資訊資產清單由各權責單位提供彙整，資通安全暨個人資料管理規範導入工作小組負責彙整決議，以確保資訊資產編號及清單之完整性。

資訊資產分類

- 文件（Document / DC）：以紙本形式存在之文書資料、報表等相關資訊，包含公文、列印之報表、表單、計畫等紙本文件。
- 軟體（Software / SW）：作業系統、應用系統程式、套裝軟體等，含原始程式碼、應用程式執行碼等。
- 通訊（Communication / CM）：網路設備、網路安全設備及提供資訊傳輸、交換之線路或服務。
- 硬體（Hardware / HW）：主機設備等相關硬體設施。
- 資料（Data / DA）：儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊。
- 環境（Environment / EV）：相關基礎設施及服務，包含辦公室實體、實體機房、電力、消防設施等。
- 人員（People / PE）：全體同仁及委外廠商。

資訊資產價值鑑別

- 資訊資產價值將依據資訊資產之機密性、完整性及可用性評估之後，取3者之最大值為資訊資產價值，各項評估標準如下：

機密性

評估標準	數值
一般：此資訊資產無特殊機密性要求	1
限閱：此資訊資產含敏感資訊，但無特殊之機密性要求，且僅供組織內部人員或被授權之外部單位使用	2
敏感：此資訊資產僅供內部相關業務承辦人員存取	3
機密：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

完整性

評估標準	數值
資產本身完整性要求極低	1
資產本身具有完整性要求，但是完整性被破壞不會對組織造成傷害	2
資產具有完整性要求，且完整性被破壞會對組織造成傷害，但不至於太嚴重	3
資產具有完整性要求，且完整性被破壞會對組織造成傷害，甚至會造成業務終止	4

可用性

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

資訊資產編號及標示

- 資訊的標示應涵蓋實體與電子格式的資訊資產。
  - 除「資通安全管理制度文件」外的資訊資產編碼方式，第1~5碼為權責單位別，第6~7碼為資產類別，第8~10碼為資訊資產流水編號。
  - 已列入機密等級分類的資訊資產及系統之輸出資料，應明確標示其機密等級，避免其機密性遭破壞。
- 實體設備之重要等級標示方式
  - 實體設備之重要等級應以不同顏色標籤區分(資產價值2為藍色標籤，資產價值3為黃色標籤，資產價值4為紅色標籤)。

覆核

- 權責單位每年至少進行1次資產盤點與資訊資產清單覆核，以更新及確保資訊資產清單的正確性及完整性。
- 當範圍內有以下的狀況發生之時，則實施不定期的覆核，以更新及確保資訊資產清單的正確性及完整性：
  - 有新增、變更或移除資訊資產。
  - 系統有重大異動。
  - 作業環境改變。

文件編號：NUTN-ISMS-D008	版次：1.5	機密等級：限閱
紀錄編號：	填表日期：　　年　　月　　日	

資產編號	資產類別	資產名稱	數量	資產說明	權責單位	保管單位	使用單位	機密性	完整性	可用性	資產價值

風險評鑑與管理程序書

- 依據：國立臺南大學 風險評鑑與管理程序書
- 文件編號：NUTN-ISMS-B004
- 版次：4.0

風險評鑑及處理權責

- 資通安全暨個人資料保護推動委員會：負責可接受風險值、風險評鑑結果、風險改善計畫與控制措施之核定。
- 資通安全暨個人資料管理規範導入工作小組：負責相關資訊資產風險評鑑結果之複核，並針對風險值超過可接受風險值之資訊資產，採取適當之控管措施以控管之，以及產出「風險改善計畫表」。
- 權責單位主管：負責所屬單位業務範圍之風險評鑑結果審核作業，亦是該業務之風險擁有者。
- 資訊資產權責單位：負責執行資訊資產之威脅與弱點評估、風險值計算等程序項目。

威脅及弱點評估表

資產編號	資產類別	資產名稱	資產價值	威脅	弱點	風險發生可能性			衝擊值				風險值
						1	2	3	1	2	3	4	

機率

評估標準	評估值
每年發生次數小於等於 1 次	1
每年發生次數為 2 至 3 次	2
每年發生次數大於等於 4 次	3

影響（衝擊）

評估標準	評估值
無傷害 1.對組織無任何影響 2.資料無損毀，組織資料可正常提供 3.組織可容許該風險造成服務失效 3 工作天以上	1
低度傷害 1.該風險對組織造成的衝擊（含組織聲譽及財務影響）為可接受範圍 2.資料損毀或遭竄改，組織資料可供回復 3.組織可容許該風險造成服務失效 8 工作小時以上，3 工作天以下	2
中度傷害 1.該風險對組織造成一定程度的衝擊（含組織聲譽及財務影響） 2.資料損毀或遭竄改，組織有備份資料可供回復 3.組織可容許該風險造成服務失效 4 工作小時以上，8 工作小時以下	3
重大傷害 1.該風險對組織造成重大的衝擊（含組織聲譽及財務影響） 2.資料損毀或遭竄改且組織無任何備份資料可供復原 3.組織可容許該風險造成服務失效 4 工作小時	4

風險值的計算

- 評估事件發生機率及影響程度後，計算出風險值。

  風險值= (資訊資產價值 × 可能性評估值 × 衝擊值)

風險彙整表（註：風險可接受值）

風險評鑑彙整表

文件編號：NUTN-ISMS-D010	版次：1.2	機密等級：限閱
紀錄編號：	填表日期：　　年　　月　　日	

資產編號	資產類別	資產名稱	資產說明	權責單位	資產價值	風險事件		風險值	風險再評鑑			
						威脅	弱點		資產價值	威脅等級	弱點等級	風險值

風險改善計畫表

風險改善計畫表		
文件編號：NUTN-ISMS-D011	版次：1.2	機密等級：限閱
紀錄編號：	填表日期：　　年　　月　　日	

教育體系資通安全管理規範控制目標	現況說明	風險改善建議措施	教育體系資通安全管理規範條文	建議權責單位	預計改善時間及處理方式	與高風險之風險評估彙整表對照

PIMS資產盤點、風險評鑑及風險處理

6.5 Asset management

6.5.1 Responsibility for assets

6.5.1.1 Inventory of assets

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.1.1 applies.

6.5.1.2 Ownership of assets

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.1.2 applies.

6.5.1.3 Acceptable use of assets

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.1.3 applies.

6.5.1.4 Return of assets

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 8.1.4 applies.

6.5.2 Information classification

個人資料檔案風險評鑑與管理程序書

- 依據：國立臺南大學 個人資料檔案風險評鑑與管理程序書
- 文件編號：NUTN-PIMS-B003
- 版次：2.0

定義

- 個人資料
  - 泛指自然人之姓名、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、社會活動等。

參閱：個人資料保護法第一章第二條第一項
112年05月31日

個人資料資產分類

- 本校個人資料資產分為電子與紙本兩類別，其分類說明如下：
  - 電子資料(Data；DA)：係指儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊，包含公文、報表、表單、計畫書、合約、外來文件及資料庫資料等電子檔案。
  - 紙本資料(Document；DC)：係指以紙本形式存在之文書資料、報表等相關資訊，包含公文、列印之報表、表單、計畫、文件等紙本資料。

個人資料檔案鑑別

- 資通安全暨個人資料管理規範導入工作小組應進行組織業務個資盤點作業，並視實際狀況進行內容調整。
- 依據作業流程分析結果，執行個人資料檔案鑑別作業，並建立「個人資料檔案清冊」。
- 本校除每年執行一次個人資料檔案鑑別作業外，亦應於下列情形發生時，針對變動範圍內的作業程序與個人資料檔案進行個人資料檔案鑑別作業：
  - 營運組織變更。
  - 作業流程改變。

個人資料資產之群組歸納原則

- 依據各單位識別出之個資資產進行分類，再從分類中群組化，以避免遺漏重要資產，群組歸納原則如下：
  - 個資資產價值相同。
  - 個資資產性質相同。
  - 個資欄位要相同且資產數量較多。

個人資料檔案風險評鑑

- 鑑別個人資料檔案資產價值。
- 個人資料檔案風險評鑑作業應於每年內部稽核活動前執行，資通安全暨個人資料管理規範導入工作小組可視實際狀況，決定執行之時機與範圍。除每年執行一次外，亦應於下列情形發生時，針對變動範圍內的作業程序與個人資料檔案進行風險評鑑：
  - 營運組織變更。
  - 作業流程改變。
  - 新增或變更個人資料檔案。
  - 發生重大個資外洩事件。

個資資產價值評估分析

資產價值	個人資料範圍
4	自然人之姓名或國民身分證統一編號(或護照號碼）及特種個人資料。
3	1. 含自然人之姓名及國民身分證統一編號(或護照號碼)，但不含特種個人資料。 2. 含自然人之姓名或國民身分證統一編號(或護照號碼)及財務情況(如：薪資、局帳號)，但不含特種個人資料。
2	1. 含自然人之姓名或國民身分證統一編號(或護照號碼)，但不包含特種資料。 2. 含自然人之姓名及員工編號(或學號)，但不含特種個人資料。
1	不含自然人之姓名及國民身分證統一編號(或護照號碼)。

風險發生機率與影響程度評估

評估標準	評估值
每年發生次數小於等於 1 次	1
每年發生次數為 2 至 3 次	2
每年發生次數大於等於 4 次	3

項目 / 評估值	財務影響	對當事人損害程度
1	保有個資數量 500 筆(含)以內，全數外洩或處理不當，造成財務影響。	個人資料檔案機敏等級低，資料外洩對不致影響個人權益或僅導致個人權益輕微受損。(如：個資資產價值「1」者)
2	保有個資數量逾 500 筆~5,000 筆(含)以內，全數外洩或處理不當，造成財務影響。	資料外洩資料外洩可能導致個人隱私遭冒犯，當事人個人權益部份受損。(如：含身分證號、財務資訊，個資資產價值「2」者)
3	保有個資數量逾 5,000 筆~5 萬筆(含)以內，全數外洩或處理不當，造成財務影響。	資料外洩資料外洩可能導致個人隱私遭冒犯，當事人個人權益嚴重受損。(如：含身分證號、財務資訊，個資資產價值「3」者)
4	保有個資數量逾 5 萬筆，全數外洩或處理不當，造成財務影響。	資料外洩將造成個人身心受到危害、社會地位受到損害、或衍生財物損失，當事人個人權益非常嚴重受損。(如：含特種個資、特種身分、輔導紀錄等，個資資產價值「4」者)

風險值計算

- 評估個人資料檔案威脅及弱點對構面因子所產生之影響，計算出風險值。

風險值 =個資資產價值×衝擊值(MAX)×可能性值。

風險評鑑頻率

- 每年應至少執行1次風險評鑑。
- 當作業環境、作業流程變更或系統重大異動時，應不定期執行風險評鑑。

D051_個人電腦設定與軟體安裝查核表操作簡介

D051_個人電腦設定與軟體安裝查核表

個人電腦設定與軟體安裝查核表		
文件編號：NUTN-ISMS-D051	版次：1.4	機密等級：限閱
紀錄編號：	填表日期：　　年　　月　　日	

管理人員	
設備資料	1. 資訊資產名稱：＿＿＿＿＿＿＿＿＿＿財產序號：□□□□□□ 2. 作業系統：□Windows＿＿＿＿(請填寫版本) □其他＿＿＿＿＿＿

	查　核　項　目	結果	檢查說明
1	電腦系統帳號密碼設定	□是□否	系統重新開機查看是否需要登入帳號
2	完成稽核原則設定	□是□否	執行 CMD：gpedit.msc 電腦設定→Windows 設定→安全性設定→本機原則→稽核原則→每個項目的「成功/失敗」全部開啟
3	完成密碼原則設定	□是□否	執行 CMD：gpedit.msc ✓ 電腦設定→Windows 設定→安全性設定→帳戶原則→密碼原則→密碼最長有效期=180天、密碼最小長度=8 ✓ 電腦設定→Windows 設定→安全性設定→帳戶原則→帳戶鎖定原則→帳戶設定閥值=3、帳戶鎖定/重設時間=10 分鐘
4	刪除/關閉不必要帳號。	□是□否	如關閉 Guests
5	完成鐘訊校時設定	□是□否	鐘訊同步主機 140.133.2.81 或 time.windows.com
6	關閉自動播放(CD-ROM、USB)	□是□否	✓ 方法一：執行 CMD：gpedit.msc→電腦設定→系統管理範本→Windows 元件→自動播放原則 ✓ 方法二：左下角 Windows 設定→裝置→自動播放→為所有媒體與裝置使用自動播放功能→關閉
7	帳號密碼無置於顯而易見之處	□是□否	桌面上無任何可見易得的帳號密碼資訊
8	完成螢幕保護程式設定	□是□否	10 分鐘以內啟動，並點選「密碼保護」
9	安裝防毒軟體，防毒軟體病毒碼已更新至最新版。	□是□否	□Kaspersky □Windows Defender □其他＿＿＿＿＿＿
10	防毒軟體設定定期掃描	□是□否	完整掃描及弱點掃描，並修復掃描到的問題。
11	開啟 WINDOWS 系統自動更新程式	□是□否	確實進行軟體更新，修補漏洞，保持更新至最新狀態。
12	無非法及未經授權軟體。	□是□否	✓ 查看控制台→新增/移除程式、查看程式集。 ✓ 如有發現來路不明或未授權檔案，請立即移除。例如 winrar、teamviewer、AnyDesk ✓ 如有 P2P 分享軟體，請立即移除。
13	其他軟體之更新	□是□否	Office 應用程式、Adobe Acobat Reader、Java 更新、其他合法軟體的更新狀況
14	電腦檔案及 Mail2000 郵件之刪除	□是□否	電腦檔案及 Mail2000 郵件刪除後，務必立即清理資源回收桶(垃圾桶)。

管理人	檢核人	單位主管	資通安全官

1.電腦系統帳號密碼設定

- 檢查說明：
  - 系統重新開機查看是否需要登入帳號。

2.完成稽核原則設定

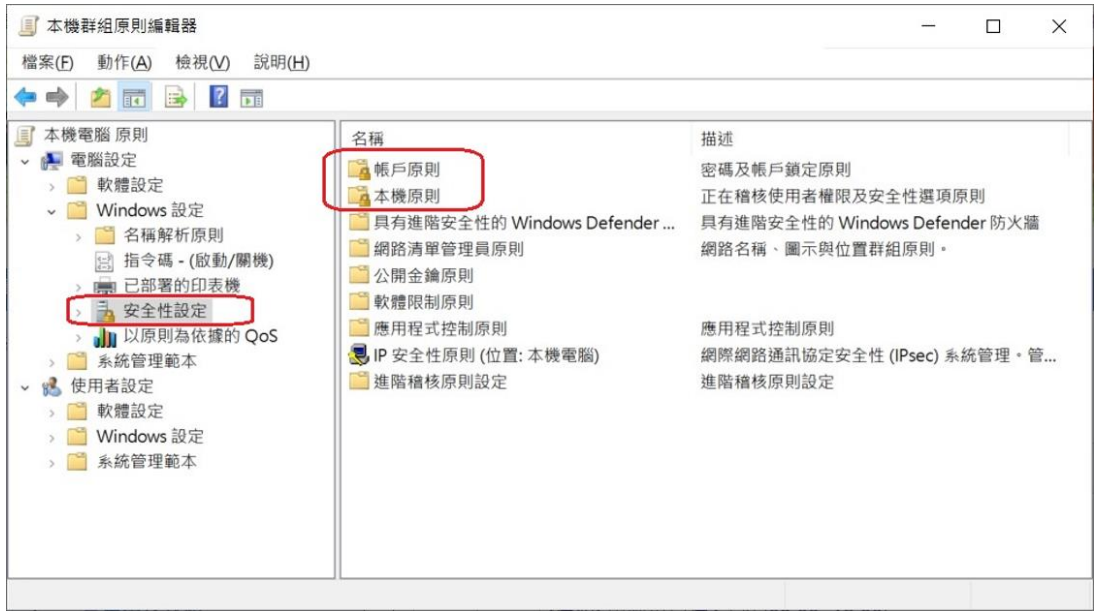
- 檢查說明：
  - 執行CMD：gpedit.msc
  - 電腦設定→Windows設定→安全性設定→本機原則→稽核原則→每個項目的「成功/失敗」全部開啟。

3.完成密碼原則設定

- 檢查說明：
  - 執行CMD：gpedit.msc
  - 電腦設定→Windows設定→安全性設定→帳戶原則→密碼原則→密碼最長有效期=180天、密碼最小長度=8 。
  - 電腦設定→Windows設定→安全性設定→帳戶原則→帳戶鎖定原則→帳戶設定閥值=3、帳戶鎖定/重設時間=10分鐘。

◆項次2、3執行步驟說明

- 於Windows視窗「搜尋列」輸入gpedit.msc後按enter鍵。
- 出現「本機群組原則編輯器」畫面，點選『電腦設定→Windows設定→安全性設定』進行變更設定 。

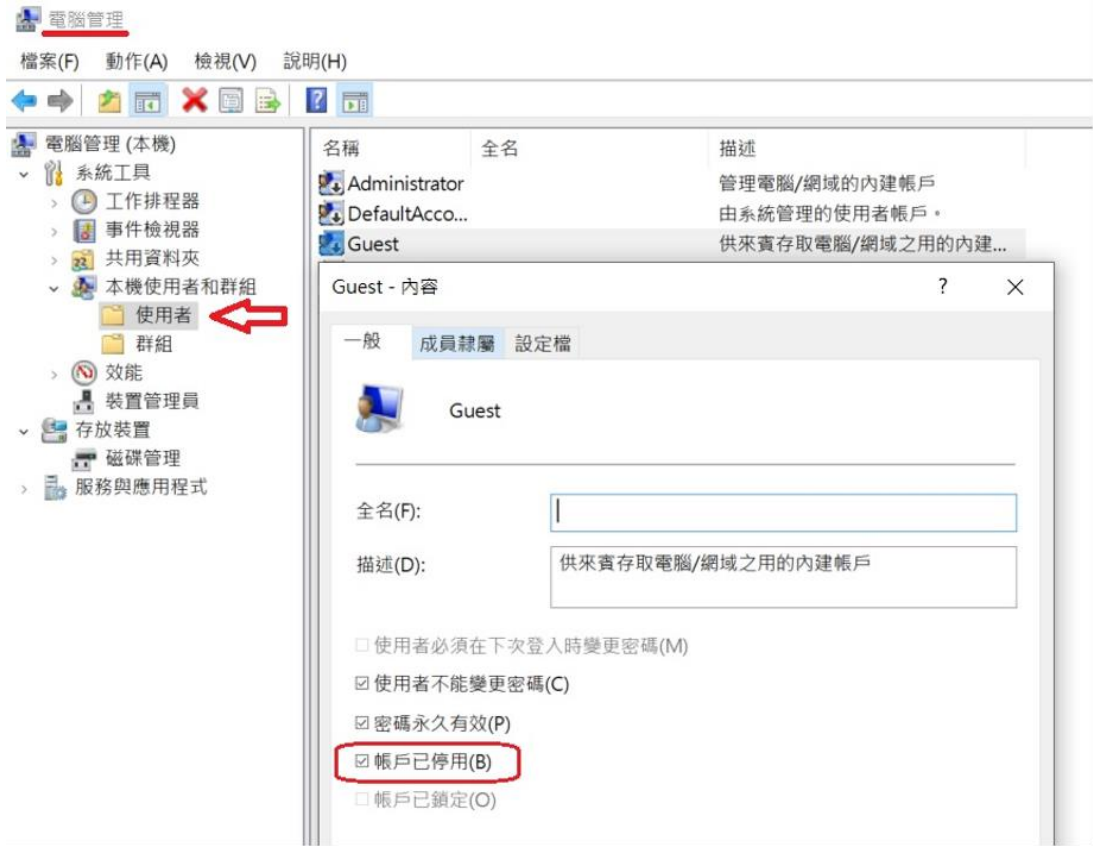


4.刪除/關閉不必要帳號

- 檢查說明：
  - 如關閉Guests。

◆項次4執行步驟說明

- 點選執行「開始 / Windows系統管理工具 / 電腦管理」。
- 出現右方畫面，點選本機使用者和群組之使用者，點選Guest帳號，確認Guest帳號已停用。



5.完成鐘訊校時設定

- 檢查說明：
  - 鐘訊同步主機140.133.2.81或time.windows.com。

◆項次5執行步驟說明

- 開啟控制台，點選在「日期和時間」，切換至「網際網路時間」。
- 點選「變更設定」，設定網際網路時間時間伺服器。（140.133.2.81或time.windows .com）。

6.關閉自動播放（CD-ROM、USB）

- 檢查說明：
  - 方法一：執行CMD：gpedit.msc→電腦設定→系統管理範本→Windows元件→自動播放原則（參考項次2、3之步驟）。
  - 方法二：左下角Windows設定  →裝置→自動播放→為所有媒體與裝置使用自動播放功能→關閉。

7.帳號密碼無置於顯而易見之處

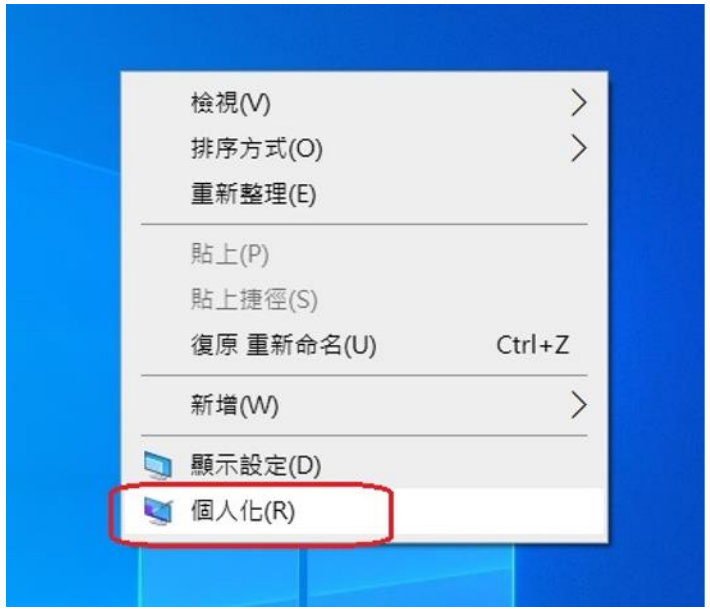
- 檢查說明：
  - 桌面上無任何可見易得的帳號密碼資訊。

8.完成螢幕保護程式設定

- 檢查說明：
  - 10分鐘以內啟動，並點選「密碼保護」。

◆項次8執行步驟說明（1/2）

- 於電腦桌面點按滑鼠右鍵，出現選單點選「個人化」。
- 點選「鎖定畫面」，再點選「螢幕保護設定」。設定等候時間為10分鐘，並勾選「繼續執行後，顯示登入畫面」。



◆項次8執行步驟說明（2/2）

9.安裝防毒軟體，防毒軟體病毒碼已更新至最新版

- 檢查說明：
  - 啟動Windows Defender

◆項次9執行步驟說明

- 點選執行「設定 / 更新與安全性 / Windows安全性 / 防火牆與網路保護」。
- 確認防火牆已開啟。

10.防毒軟體設定定期掃描

- 檢查說明：
  - 完整掃描及弱點掃描，並修復掃描到的問題。

◆項次10執行步驟說明

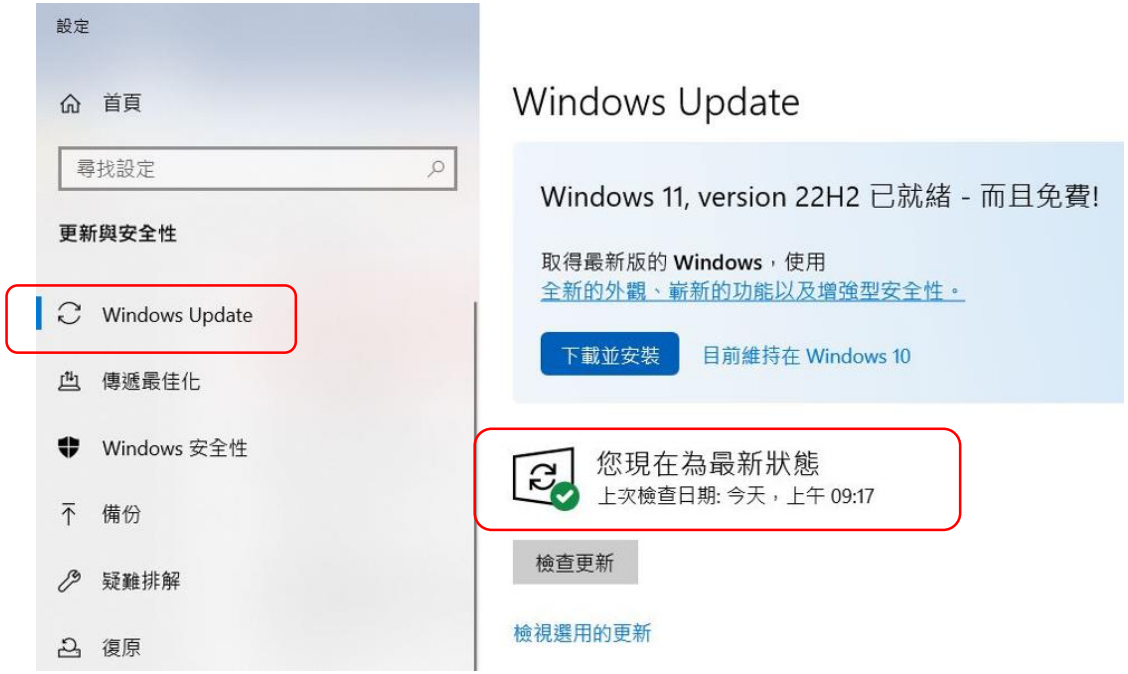
- 點選執行「設定 / 更新與安全性 / Windows安全性 / 病毒與威脅防護」。
- 確認「沒有目前的威脅」。

11.開啟WINDOWS系統自動更新程式

- 檢查說明：
  - 確實進行軟體更新，修補漏洞，保持更新至最新狀態。

◆項次11執行步驟說明

- 點選執行「設定 / 更新與安全性 / WindowsUpdate。
- 點選「檢查更新」，確認「現在為最新狀態」。



12.無非法及未經授權軟體

- 檢查說明：
  - ➢ 查看控制台→新增/移除程式、查看程式集。
  - ➢ 如有發現來路不明或未授權檔案，請立即移除。例如winrar、teamviewer、AnyDesk
  - ➢ 如有P2P分享軟體，請立即移除。

✓ 著作權法第91-1條...侵害他人之著作財產權者，處三年以下有期徒刑、拘役，或科或併科新臺幣五十萬元以下罰金。

13.其他軟體之更新

- 檢查說明：
  - Office應用程式、Adobe Acobat Reader、Java更新、其他合法軟體的更新狀況。

14.電腦檔案及Mail2000郵件之刪除

- 檢查說明：
  - 電腦檔案及Mail2000郵件刪除後，務必立即清理資源回收桶（垃圾桶）。

附錄

大專校院類檔案保存年限基準表

			等相關文件		序銷毀		
	200206	學籍管理	學籍表、成績冊及評量表、學籍異動資料、新生名冊、畢(結)業生名冊、公費生名冊等相關資料	永久	機關永久保存		
	200207	成績及學分管理	成績繳交、更正、考核、抵免及學分抵免等相關文件	20 年	依規定程序銷毀		
	200208	註冊服務					
	-1		學生入學、轉學、轉系(組、科、班、所)、休學、保留入學資格、國外學歷之處理、認定、申請及通知等相關文件	10 年	依規定程序銷毀		
	-2		學生退學及開除學籍之認定、處理及通知等相關文件	20 年	屆期後鑑定		

法規內容

法規名稱：	個人資料保護法之特定目的及個人資料之類別 英
公發布日：	民國 85 年 08 月 07 日
修正日期：	民國 101 年 10 月 01 日
法規體系：	常用法規 > 憲法暨其關係法規
立法理由：	立法總說明 條文對照表.PDF

1 代號　修正特定目的項目

○○一　人身保險

○○二　人事管理（包含甄選、離職及所屬員工基本資訊、現職、學經歷、考試分發、終身學習訓練進修、考績獎懲、銓審、薪資待遇、差勤、福利措施、褫奪公權、特殊查核或其他人事措施）

○○三　入出國及移民

○○四　土地行政

○○五　工程技術服務業之管理

○○六　工業行政

○○七　不動產服務

○○八　中小企業及其他產業之輔導

○○九　中央銀行監理業務

○一○　公立與私立慈善機構管理

○一一　公共造產業務

○一二　公共衛生或傳染病防治

○一三　公共關係

○一四　公職人員財產申報、利益衝突迴避及政治獻金業務

○一五　戶政

○一六　文化行政

○一七　文化資產管理

○一八　水利、農田水利行政

○一九　火災預防與控制、消防行政

○二○　代理與仲介業務

○二一　外交及領事事務

○二二　外匯業務

○二三　民政

○二四　民意調查

○二五　犯罪預防、刑事偵查、執行、矯正、保護處分、犯罪被害人保護或更生保護事務

○二六　生態保育

○二七　立法或立法諮詢

○二八　交通及公共建設行政

○二九　公民營（辦）交通運輸、公共運輸及公共建設

○三○　仲裁

○三一　全民健康保險、勞工保險、農民保險、國民年金保險或其他社會保險

○三二　刑案資料管理

○三三　多層次傳銷經營

○三四　多層次傳銷監管

○三五　存款保險

○三六　存款與匯款

○三七　有價證券與有價證券持有人登記

○三八　行政執行

○三九　行政裁罰、行政調查

○四○　行銷（包含金控共同行銷業務）

○四一　住宅行政

代　號　識別類：

C○○一　辨識個人者。

例如：姓名、職稱、住址、工作地址、以前地址、住家電話號碼、行動電話、即時通帳號、網路平臺申請之帳號、通訊及戶籍地址、相片、指紋、電子郵遞地址、電子簽章、憑證卡序號、憑證序號、提供網路身分認證或申辦查詢服務之紀錄及其他任何可辨識資料本人者等。

C○○二　辨識財務者。

例如：金融機構帳戶之號碼與姓名、信用卡或簽帳卡之號碼、保險單號碼、個人之其他號碼或帳戶等。

C○○三　政府資料中之辨識者。

例如：身分證統一編號、統一證號、稅籍編號、保險憑證號碼、殘障手冊號碼、退休證之號碼、證照號碼、護照號碼等。

代　號　特徵類：

C○一一　個人描述。

例如：年齡、性別、出生年月日、出生地、國籍、聲音等。

C○一二　身體描述。

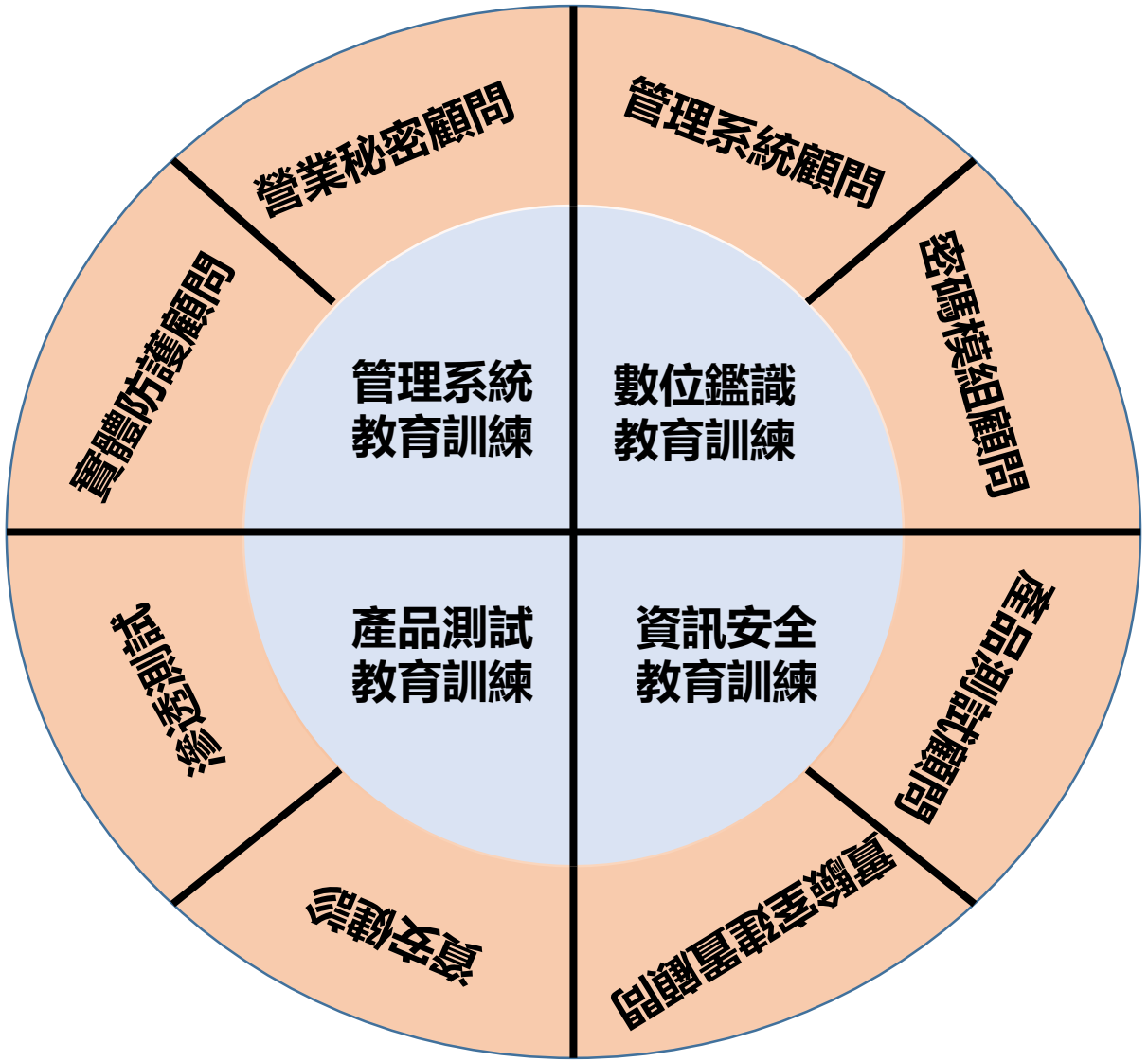
例如：身高、體重、血型等。

C○一三　習慣。

例如：抽煙、喝酒等。

C○一四　個性。

Q/A


營業秘密顧問
管理系統顧問
密碼模組顧問
實體防護顧問
管理系統
教育訓練
數位鑑識
教育訓練
產品測試
教育訓練
資訊安全
教育訓練
滲透測試
資安健診
實體安全實驗室
產品測試實驗室

優士創造您的資安優勢