ISMS簡介

1. ISMS架構及導入流程
2. 組織全景、目標制訂與量測
3. 系統盤點、資產盤點、風險評鑑
4. 績效評估、改善

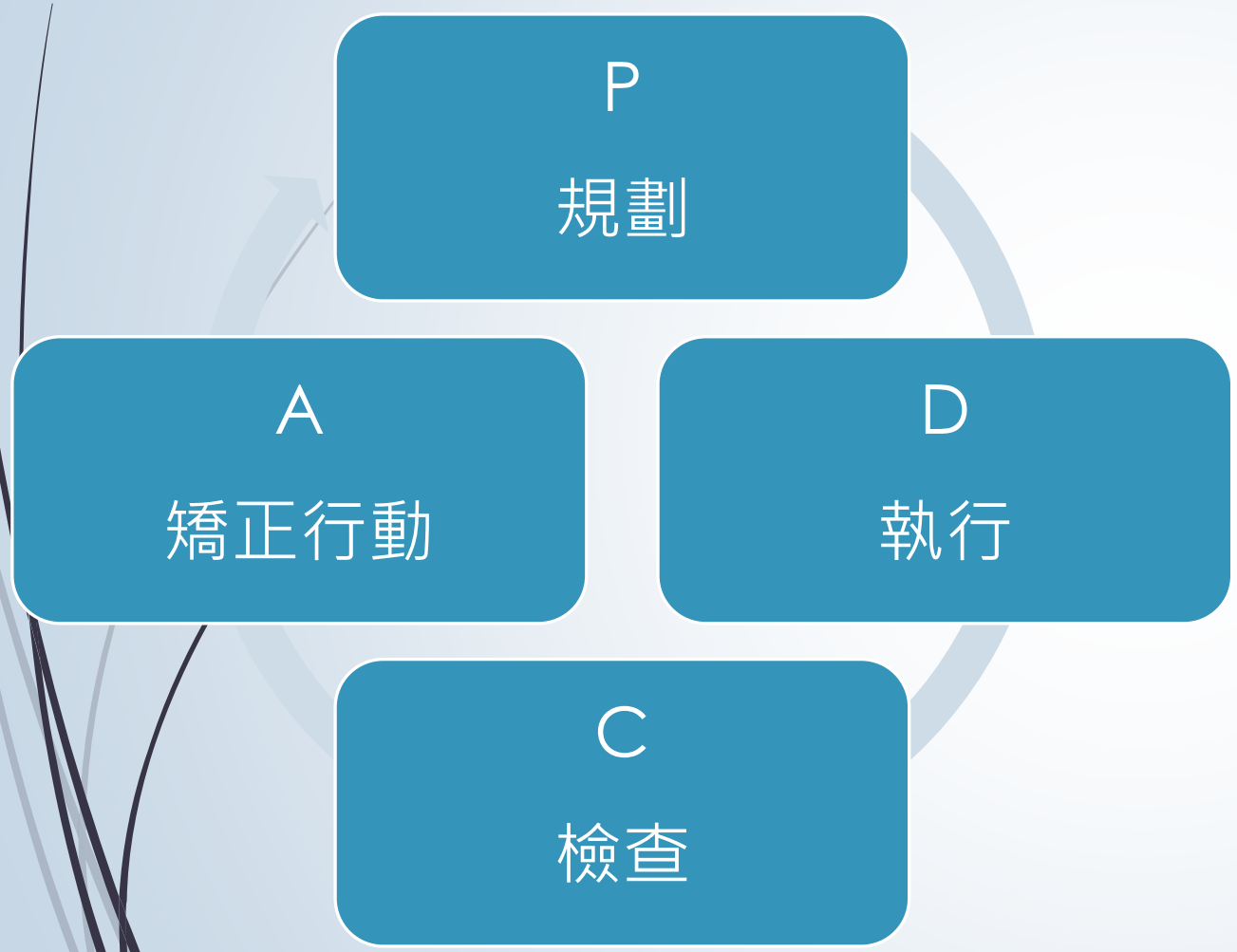
1 ISMS架構及導入流程

2 組織全景、目標制訂與量測

3 系統盤點、資產盤點、風險評鑑

4 績效評估、改善

ISMS架構



P、D、C、A	條款
P	4.組織全景 5.領導作為 6規劃 7支援 8運作
D	A5組織 A6人員 A7實體 A8技術
C	9績效評估
A	10改善

- 4.組織全景(為何要做)
- 5.領導作為(老闆要不要做)
- 6.規劃(訂定範圍)
- 7.支援(需要資源、人力、能力)
- 8.運作(高風險資產先處理)
- 9.績效評估(稽核、量測)
- 10.改善(矯正行動)

- A5組織
- A6人員
- A7實體
- A8技術(資產)

1 ISMS架構及導入流程

2 **組織全景、目標制訂與量測**

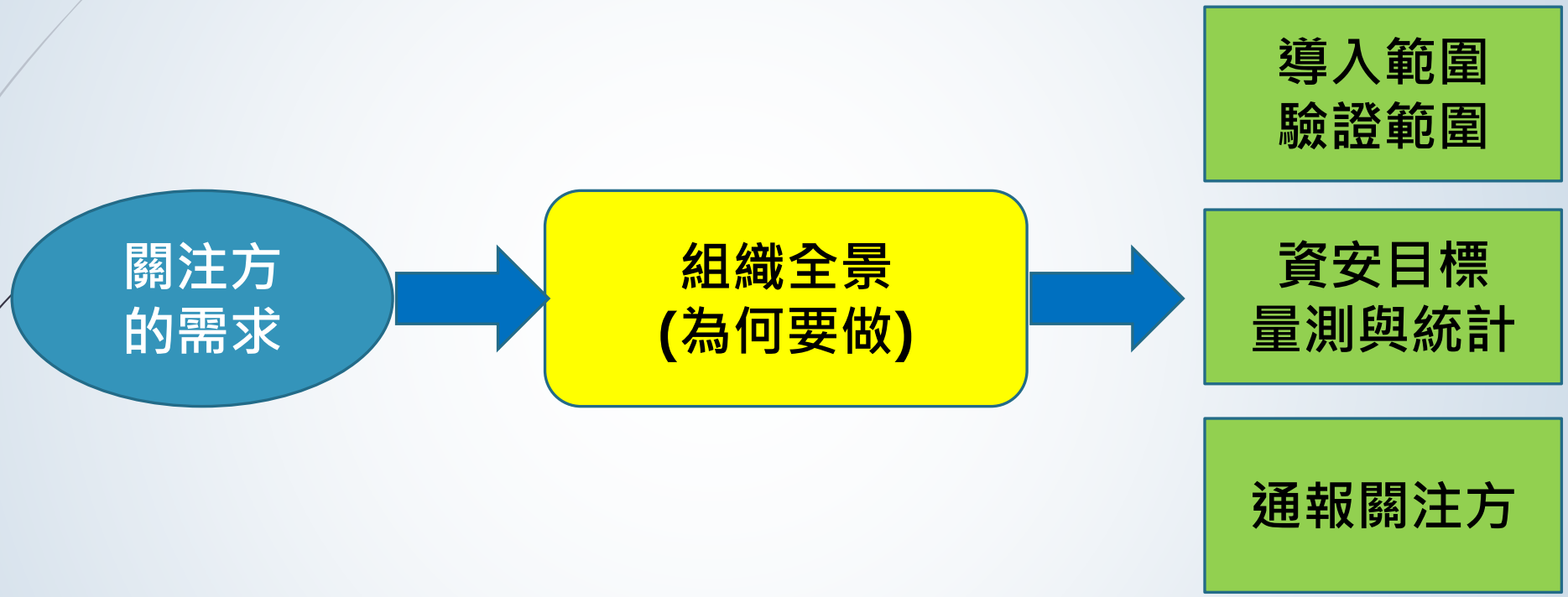
3 系統盤點、資產盤點、風險評鑑

4 績效評估、改善

組織全景

- 4.1　瞭解組織及其全景
  - 組織應決定與其目的有關且影響達成其資訊安全管理系統預期成果能力之**外部及內部議題**。
- 4.2　瞭解關注方之需求及期望
  - "組織應決定下列事項：(a)與資訊安全管理系統有關之關注各方。(b)此等關注方之相關要求事項。(c)此等要求事項中之哪些要求事項，將透過資訊安全管理系統因應。"
- 4.3　決定資訊安全管理系統之範圍
  - "組織應決定資訊安全管理系統之邊界及適用性，以建立其範圍。於決定此範圍時，組織應考量下列事項：(a)4.1中所提及之外部及內部議題。(b)4.2中所提及之要求事項。(c)組織執行之活動與其他組織執行的活動間之介面及相依性。範圍應以文件化資訊提供。"
- 4.4　資訊安全管理系統　　組織應依本標準之要求事項，建立、實作、維持及持續改善資訊安全管理系統，包括所需過程及其互動。

組織全景、目標制訂與量測



組織全景

- 法規的要求(主管機關的要求、鋼性要求)
  - 資通安全管理法：公務機關(A、B級需驗證，C級需導入)
  - 上市上櫃公司資通安全管控指引
  - 金融控股公司及銀行業內部控制及稽核制度實施辦法
  - 保險業內部控制及稽核制度實施辦法
  - 證券暨期貨市場各服務事業建立內部控制制度處理準則
  - 電子支付機構內部控制及稽核制度實施辦法
  - 農漁會信用部內部控制及稽核制度實施辦法
  - (特定行業)個人資料檔案安全維護管理辦法

組織全景

- 導入範圍當然是全組織，那一些需要納入驗證範圍
  - 支持核心業務的(系統)或(服務)
  - 占公司主要營運獲利來源
  - 法規要求(金融業者須將公文系統納入驗證)
  - 公司未來的核心業務的(系統)或(服務)
  - 發生重大事件的(系統)或(服務)

組織全景

- 公務機關(含特定非公務機關)
- 核心業務(組織法所規範)系統或服務
- 資通系統防護基準為高等級系統

核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間
		□為主管機關指定之關鍵基礎設施 □為主管機關核定資通安全責任等級A級或B級機關所涉業務 □為本機關依組織法執掌，足認為重要者	財務損失： 民眾生命財產損失： 經濟發展受阻： 影響其他機關業務運作(相依性)： 違反法遵義務： 機關信譽： 其他：	

組織全景

- 來自於關注方的需求
  - 外部關注方
    - 主管機關
    - 學生家長
    - 學生
  - 內部關注方
    - 高階主管
    - 內部同仁
- **關注方的其他需要注意**
  - 聯繫通道及方式(演練須納入)
  - 與關注方溝通需要留下證據(2022版，要求)

量測

核心系統	量測指標	頻率	評量機制	執行	審核
單一登入系統	系統所提供資訊無外洩，系統提供之資訊外洩事件每年應 1 件(含)以下。	每季	檢視及統計相關執行紀錄(如資安事件通報單)。	技術發展組	技術發展組組長
	系統所提供資訊無缺漏，系統提供之資訊缺漏事件每年應 1 件(含)以下。	每季	檢視及統計相關執行紀錄(如資安事件通報單)。	技術發展組	技術發展組組長
	針對非天災、電力中斷、火災引起之資通安全事故，導致本校使用核心資通系統、網際網路服務停頓，每年小於 2 次(含)，每次不得超過可接受系統中斷時間(MTPD)。	每季	檢視及統計相關執行紀錄（如機房工作日誌、相關維護／保養報告）。	技術發展組	技術發展組組長
	遇資通安全事件時，須按照「資通安全事件通報及應變辦法」辦理，違反事件發生次數每年應 2 件(含)以下。	每季	檢視及統計相關執行紀錄(如資安事件通報單)。	技術發展組	技術發展組組長
	業務持續運作演練，全部核心資通系統每 2 年辦理 1 次，違反事件發生應為 1 件(含)以下。	每年	檢視及統計相關執行紀錄(如演練報告)。	技術發展組	技術發展組組長

1 ISMS架構及導入流程

2 組織全景、目標制訂與量測

3 **系統盤點、資產盤點、風險評鑑**

4 績效評估、改善

資通系統盤點及分級表

資通系統盤點及分級表

機密等級：□一般 ■限閱 □敏感

文件編號：ISMS-215-01　　版　　次：1.0

紀錄編號：　　填表日期：　年　月　日

單位名稱	資通系統	系統網址	資訊資產	最大可容忍中斷時間	資通系統主要功能	是否為核心資通系統	資通系統防護需求分級自評 參考【附表九 資通系統防護需求分級原則】					管理單位	承辦人	承辦人聯絡電話	承辦人電子郵件	系統維護單位/廠商	服務對象	是否介接SSO	是否限制校內連線	防護基準符合性	系統所在位置
							機密性	完整性	可用性	法律遵循	系統等級										
單位盤點	填寫資通系統名稱	填寫系統網址	提供該系統服務之設備均需列出	以小時為單位	提供○○服務	是/否	普/中/高	普/中/高	普/中/高	普/中/高	普/中/高	○○處/○○組	承辦人姓名	聯絡電話	聯絡電子郵件	系統維護廠商名稱	校內/校外	是/否	是/否	是/否	校內/校外
1																					
2																					
3																					
4																					
5																					
6																					
7																					
8																					
9																					

是否為核心資通系統

- 一定需要使用該系統方能執行核心業務者 — 是
- 不一定需要使用該系統即可執行核心業務者 — 否
- 非核心業務相關系統 — 否

資通系統防護需求分級原則

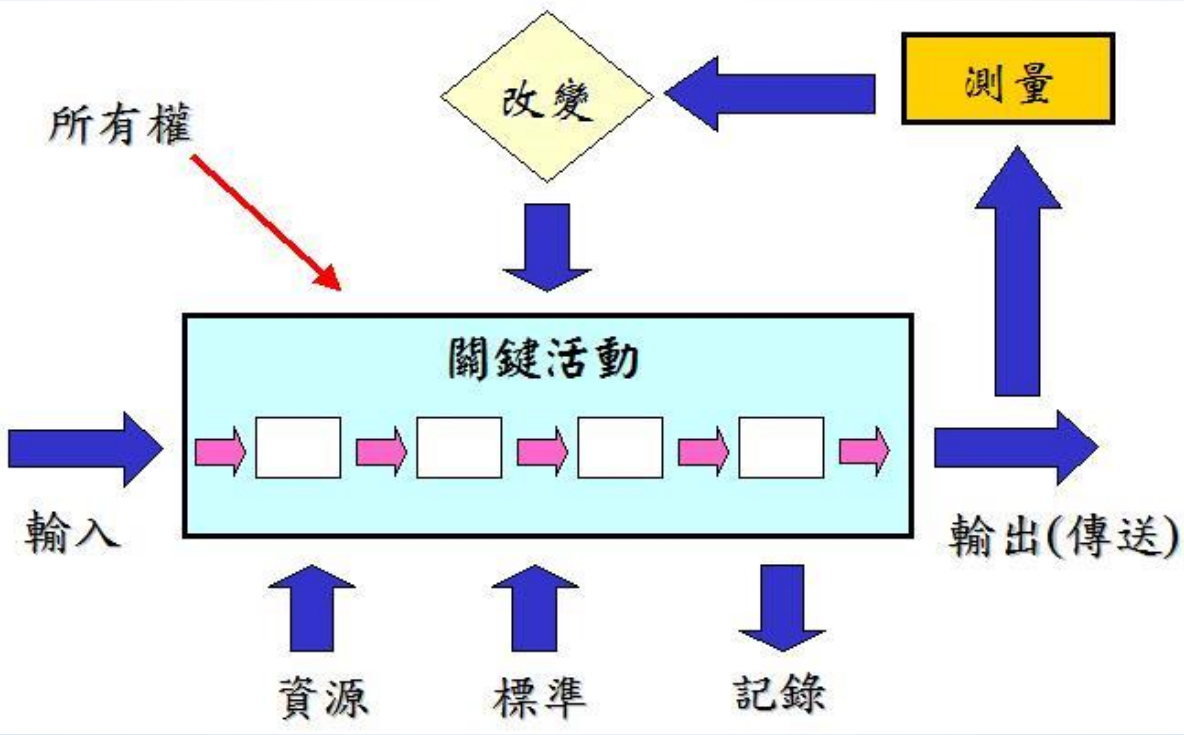
防護需求等級 / 構面	高	中	普
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面**將產生非常嚴重或災難性之影響**。 含有機密資料	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面**將產生嚴重之影響** 含有個人資料或敏感以上等級資料	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面**將產生有限之影響** 無個人資料或敏感以上等級資料
完整性	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面**將產生非常嚴重或災難性之影響**。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事對機關之營運、資產或信譽等方面**將產生嚴重之影響**。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事對機關之營運、資產或信譽等方面**將產生有限之影響**。

資通系統防護需求分級原則

構面 \ 防護需求等級	高	中	普
可用性	發生資通安全事件致資通系統受影響時，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**。 最大可容忍中斷時間為小於半日。	發生資通安全事件致資通系統受影響時，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**。 最大可容忍中斷時間為半日以上(含)、小於1日。	發生資通安全事件致資通系統受影響時，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**。 最大可容忍中斷時間1天以上(含)。
法律遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或**影響他人合法權益或機關執行業務之公正性及正當性，使機關所屬人員負刑事責任**。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或**影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處**。	其他資通系統設置或運作於法令有相關規範之情形。

資訊資產鑑別作業

- 資產鑑別
  - 資產鑑別主要是以業務流程為主軸，由作業流程 / 資產負責人審視其業務相關之資產，並以鑑別資產以及其他與資訊安全管理有關的資產與相對應之資產價值。



資訊資產鑑別作業

- 資產類別
  - 資產類別之分類，主要是針對資訊資產進行歸類，以便後續資產價值之識別及風險評鑑作業
- 資產分類
  - 資訊類資產
    - 資料經過處理後成為有特殊價值的資訊，或以文件形式存在的資產
  - 實體類資產
    - 為執行所負責的業務流程所使用之硬體設備。
  - 軟體類資產
    - 為有效執行所負責的業務流程而建置的軟體作業與應用程式

資訊資產鑑別作業

- 資產分類
  - 服務類資產
    - 以服務形式(合約)存在之資產。
  - 人員類資產
    - 管理、執行或提供支援給所負責的業務流程之人員。
    - 單位所有具**權限**人員。

資訊資產鑑別作業(續)

- 資產分類標準表

資產類別	資產項目
資訊類資產	一　業務資料檔案，例如：XX業務檔案。 二　系統資料檔案，例如：資料庫檔案、應用程式檔案及備份檔案等。 三　電子化儲存之文件檔案，例如：系統或軟體使用手冊及教育訓練教材等。 四　書面管理文件，例如：系統文件、使用手冊、各種程序及指引辦法等。 五　書面紀錄，例如：申請表單及採購等。
實體類資產	一　電腦設備，例如：伺服器、工作站、個人主機、筆記型電腦及PDA等。 二　通訊設備，例如：路由器、網路交換器、數據機、傳真機、印表機及影印機等。 三　儲存媒體，例如：隨身碟、磁帶、磁帶機、磁帶櫃、光碟及光碟機等。 四　其他支援設備，例如：監視器、不斷電系統、空調系統、消防系統、環控系統及機房用發電機等。
軟體類資產	一　系統軟體，例如：校務系統、官網系統等。 二　資料庫軟體，例如：ORACLE、SQL Server等。 三　套裝軟體，例如：Windows 10、 Office 等。
服務類資產	一　一般維運支援性服務，例如：中華電信網路專線、市電系統、供水服務等。 二　委外服務，例如：XX公司網路安全服務、XX公司設備主機維護服務等。
人員類資產	一　內部同仁，例如：資訊處同仁、專案工作人員及計畫約聘人員等。 二　外部(常駐型)人員，例如：XX公司駐點人員等。

名詞說明

- 資產負責人員
  - 鑑別資產之價值
  - 評估當鑑別的風險發生時，其潛在的衝擊影響
  - 評估所鑑別的風險，其實際發生的可能性
  - 參與安全防護對策之討論與決策
- 風險當責者(資產風險擁有者)
  - 業務流程中，具有決定的人。
  - 決定安全防護對策的實施，及對殘餘資訊安全風險的接受。
- 角色(何人)、工作說明

資產清冊

資通資產清冊

機密等級：□一般 ■限閱 □敏感

文件編號：ISMS-203-01　　版　　次：4.0

紀錄編號：　　填表日期：　年　月　日

	資產識別			基本資料					人員識別			
項次	資產類別	資產項目	資產編號	資產名稱	數量	資通系統	系統分級(普中高)	放置地點	使用人	業務流程／資產負責人員	審核主管	備註
1	資訊類	業務資料檔案	(單位)-I-XXX	00系統產出檔案		00系統		(辦公室)	(可使用到的人)	(開帳號的人)	(業務承辦單	
2	資訊類	系統資料檔案	(單位)-I-XXX	00系統資料庫檔案		00系統		(000機房)	(00處人員)	(盡量寫人名)		
3	資訊類	電子化儲存之文件檔案	(單位)-I-XXX	00系統操作手冊電子檔案		00系統		(000庫房)	(000組人員)			
4	文件類	書面管理文件	(單位)-D-XXX	00系統操作手冊		00系統			(本校同仁)			
5	文件類	書面紀錄	(單位)-D-XXX	00系統使用紀錄紙本		00系統			(一般民眾)			
6	實體類	電腦設備	(單位)-H-XXX	Server(廠牌型號)		00系統			(連線機關、學校)			
7	實體類	電腦設備	(單位)-H-XXX	PC(廠牌型號)		網際網路連線						
8	實體類	通訊設備	(單位)-H-XXX	防火牆(廠牌型號)		網際網路連線						
9	實體類	通訊設備	(單位)-H-XXX	網路交換器(廠牌型號)		網際網路連線						
10	實體類	通訊設備	(單位)-H-XXX	事務機(廠牌型		網際網路連線						
11	實體類	通訊設備	(單位)-H-XXX	監視器(廠牌型號)		(先留白)						
12	實體類	通訊設備	(單位)-H-XXX	無人機(廠牌型號)		是否有配合之系統						

資訊資產鑑別作業

- 資產價值鑑別
  - 資產價值鑑別，主要鑑別資產本身之價值，其鑑別方式為將各項資產分類依「機密性、完整性、可用性、法律遵循性」進行資產價值評鑑。
- 資產價值
  - 資產總價值 = **Max**(機密性價值、完整性價值、可用性價值、法律遵循性)

資產等級

防護需求 等級 構面	高(3)	中(2)	普(1)
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，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。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響
完整性	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，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。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事對機關之營運、資產或信譽等方面將產生有限之影響。

資產等級

防護需求 等級 構面	高(3)	中(2)	普(1)
可用性	發生資通安全事件致資通系統受影響時，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。	發生資通安全事件致資通系統受影響時，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。	發生資通安全事件致資通系統受影響時，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。
法律遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	其他資通系統設置或運作於法令有相關規範之情形

資產關係

- 建立與全景風險的關係(系統分級所建立之系統)
- 系統包含5類資產
- 共同使用資產另外列舉，自建系統，如VM、網路
- 說明人員所管理的系統，將影響風險值
- 單一資產之資產價值(CIA)不得大於全景風險(資訊系統分級)中(CIA)，若大於全景風險(資訊系統分級)者，需修正全景風險(資訊系統分級)

風險鑑別與評鑑

- 風險鑑別主要是針對風險機率及衝擊性進行鑑別，鑑別方式是假定資產失效無法提供服務情況下，其資產對組織之衝擊及機率影響程度，並依影響等級進行評鑑。
- 風險值計算：

  單一資產風險值(1~27)=資產總價值X脆弱性利用難易度X威脅發生可能性

脆弱性利用難易度

等級	脆弱性利用難易度分級原則
普(1)	·僅限深入了解脆弱性技術，並於特定條件或環境下方能利用脆弱性 ·不會損害資訊及資通系統資產，或是受到損害後能立即回復 ·必須運用特殊的方法才能利用脆弱性進行攻擊 ·威脅來源必須花費長時間(可能需一個月以上)的資料蒐集，突破各層防護，才能接觸到關鍵資訊 ·攻擊成功：可能要1~數個月以上 ·可能之原因 —管理防護機制完備並落實實施(例如流程控管、存取權限、通行碼政策、變更管理、稽核及應用系統經過完整測試等皆落實進行) —資訊或處理設備的使用手冊完整或說明清晰 —使用者或管理者受過完整教育訓練，對資訊處理設備操作熟練 —使用者或管理者對資訊處理程序熟悉 —技術性防護機制完備(例如資訊採用加密保護、網路區隔並採用安全設備監控系統效能、容量及安全事件；有效管理入侵/病毒/木馬、備援線路) —可被利用的方法的技術層次高或技術不容易取得實體環境的特性(例如劃分安全區域並實施監控與出入管控、環境溫濕度控管、建築物或防護設施材質等)讓威脅源被杜絕

脆弱性利用難易度

等級	脆弱性利用難易度分級原則
中(2)	·具備了解脆弱性技術知識，方能利用脆弱性 ·資訊及資通系統資產受到損害，且無法立即回復 ·不需用特殊的方法就能利用脆弱性進行攻擊 ·已實施保護的機制，威脅來源必須花費一段時間(可能是數天)進行資料蒐集始能接觸到關鍵資訊▪ 攻擊成功：可能是數天以上 ·可能之原因 —已建立管理防護機制但未落實(例如流程控管、存取權限、通行碼政策、變更管理、稽核及應用系統測試等) —資訊或處理設備的使用手冊過於簡單或說明不詳細 —使用者或管理者雖受過教育訓練，但對資訊處理設備操作不熟練 —使用者或管理者對資訊處理程序不熟悉 —雖實施技術性防護機制(例如資訊採用加密保護、網路區隔並採用安全設備、監控系統效能、容量及安全事件；有效管理入侵/病毒/木馬、備援線路)但是設定或防護能力不足 —可被利用的方法的技術層次高但技術容易取得 —實體環境的特性(例如未劃分安全區域出入管控、環境溫濕度控管不足及建築物或防護設施材質等)讓威脅源存在

脆弱性利用難易度

等級	脆弱性利用難易度分級原則
高(3)	·任何人不需具備任何能力均能有意或無意的利用脆弱性 ·資訊及資通系統資產受到嚴重損害，影響或中斷資產相關業務運作，或導致資訊及資通系統資產消失無法復原 ·利用簡易的方法就能利用脆弱性進行攻擊 ·未實施保護或保護機制無效，威脅來源於短期內即可攻擊成功 ·攻擊成功：可能是一天內到數天 ·可能之原因 —管理防護機制缺乏(例如流程控管、存取權限、通行碼政策、變更管理、稽核及應用系統測試等)-缺乏資訊或處理設備的操作手冊或手冊錯誤 —使用者或管理者未受過教育訓練，或對資訊處理設備操作不熟練 —使用者或管理者對資訊處理程序不了解 —缺乏技術性防護機制(例如資訊採用加密保護、網路區隔並採用安全設備、監控系統效能、容量及安全事件；有效管理入侵/病毒/木馬、備援線路) —可被利用的方法其技術層次低且容易取得 —實體環境的特性(例如未劃分安全區域出入管控、環境溫濕度控管不足及建築物或防護設施材質等)讓威脅源持續存在

威脅發生可能性

等級	威脅發生可能性等級分級原則
普(1)	·事件或威脅雖然沒發生過，但有可能發生 ·平均每年發生不到1次 ·平均每月人為阻止事件或威脅發生不到1次
中(2)	·平均每年可能發生 1 次以上，低於6次 ·平均每月人為阻止事件或威脅發生1~3次
高(3)	·平均每年可能發生 6 次(含)以上 ·平均每月人為阻止事件或威脅發生超過4次(含)以上

風險鑑別與評鑑

- 風險值計算
  - 風險值計算是由資產價值等級、衝擊程度等級及可能性等級值三個因子所構成，其計算方式為
    風險值＝資產價值等級＊脆弱性利用難易度＊威脅發生可能性
  - 範例：
    資產價值等級為2，脆弱性利用難易度為2，威脅發生可能性等級為1
    2＊2＊1＝4

風險評鑑彙整表

機密等級：□一般 ■限閱 □敏感

文件編號：ISMS-204-01　　版　　次：2.0

紀錄編號：　　填表日期：　年　月　日

	資產識別			資產價值識別					風險值計算		
項次	資產類別	資產項目	資產編號	機密性(1-3)	完整性(1-3)	可用性(1-3)	法遵性(1-3)	資產價值	威脅發生可能性(1-3)	脆弱性利用難易度(1-3)	風險值
1											
2											
3											

風險鑑別與評鑑

- 決定臨界風險值

1	1	2	3
1	1	2	3
2	2	4	6
3	3	6	9

2	1	2	3
1	2	4	6
2	4	8	12
3	6	12	18

3	1	2	3
1	3	6	9
2	6	12	18
3	9	18	27

1	1
2	3
3	3
4	3
6	6
8	1
9	3
12	3
18	3
27	1

風險評鑑報告

- 監控和審查
  - 資產的維護和對資產價值認知的責任由資產管理人負責，應至少每年審查一次，有任何關於本單位業務流程的改變或架構變更時，或新服務上線前，必需重新進行相關部分的風險評鑑。
  - 組織結構的改變，可能導致業務流程權責的變化。責任的移交應包括業務流程的風險評鑑。

1 ISMS架構及導入流程

2 組織全景、目標制訂與量測

3 系統盤點、資產盤點、風險評鑑

4 **績效評估、改善**

稽核的類型

- 第一方(First party):目的在確認資訊安全管理系統的管制目標、控制措施、過程及程序，符合標準及相關法令、法規之要求，並有效的實施與維持。
- 第二方(Second party)：由對組織的績效或成效有利害關係的個人或團體所執行之稽核(合併稽核、聯合稽核、利害關係者的稽核)。
- 第三方(Third party)：驗證單位稽核以驗證所申請之認證標準符合性稽核為主，通過驗證單位稽核可獲頒證書。

資安法中的各種稽核

第一方稽核

機關內部資安稽核

A：每年2次
B：每年1次
C：每2年1次

第二方稽核

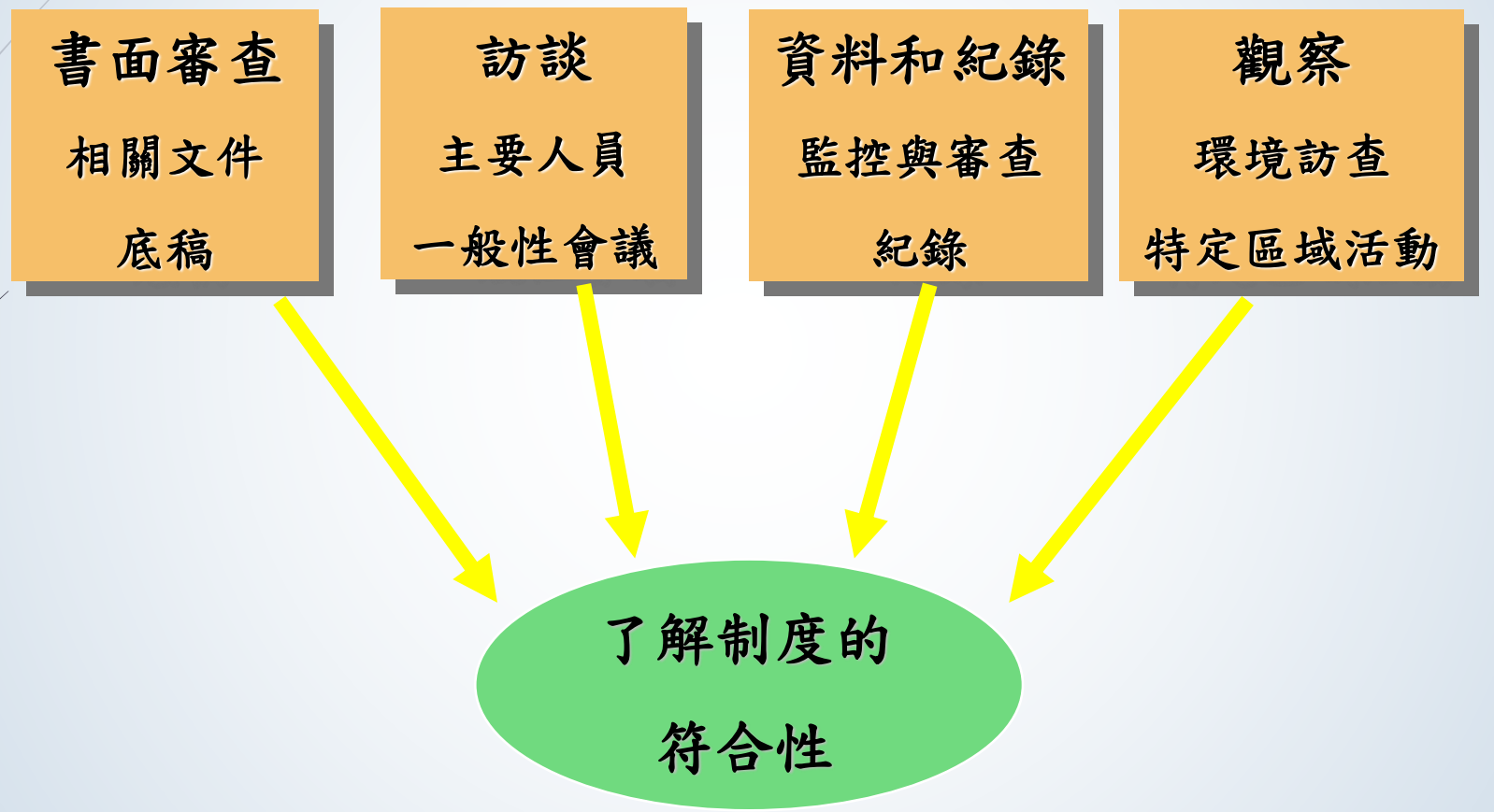
- 上級機關對所屬機關
- 監督機關對行政法人
- 中央目的事業主管機關對特定非公務機關
- 資安法主管機關對特定非公務機關
- 機關對受託者

第三方稽核

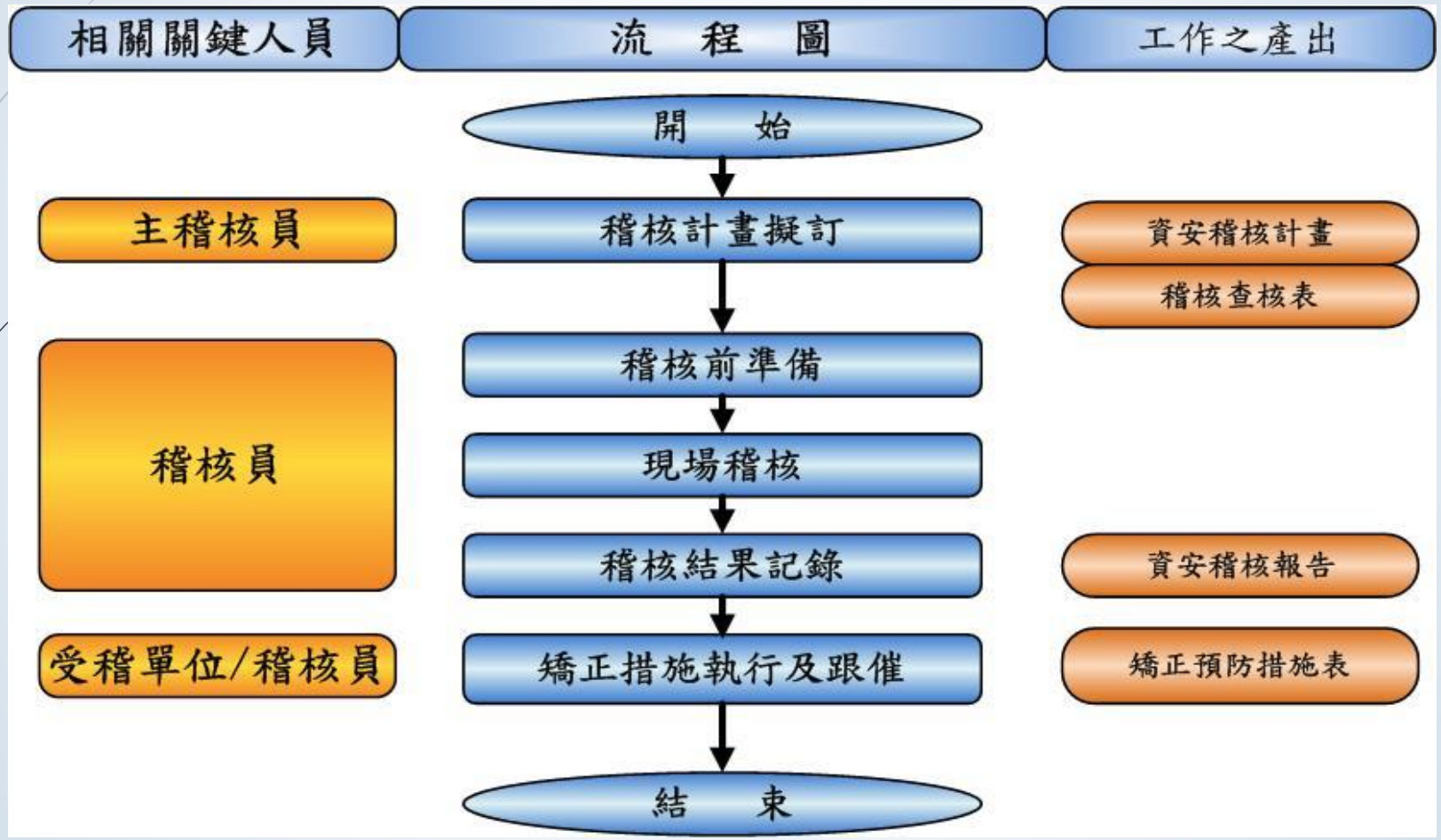
資訊安全管理系統(ISMS)驗證

目的：檢視**全機關資通安全管理法及其子法**相關**法遵事項符合情形**

稽核方式


書面審查
相關文件
底稿
訪談
主要人員
一般性會議
資料和紀錄
監控與審查
紀錄
觀察
環境訪查
特定區域活動
了解制度的
符合性

稽核流程


相關關鍵人員
流　程　圖
工作之產出
開　始
主稽核員
稽核計畫擬訂
資安稽核計畫
稽核查核表
稽核前準備
稽核員
現場稽核
稽核結果記錄
資安稽核報告
受稽單位/稽核員
矯正措施執行及跟催
矯正預防措施表
結　束

內部稽核查檢表

引導

輔助記憶

連貫性

查檢表
提醒我們稽核抽樣

資通安全維護計畫內部稽核查核表

國立中正大學000年度資通安全維護計畫內部稽核查核表

稽單位：□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□稽核日期：□□年□□月□□日

項次	稽核項目	資通安全稽核檢核項目	自評情形					
			符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
一	資通安全推動組織							
1	資安業務聯繫窗口	一級單位任命資安管理窗口(兼任)至少一位						(內簽紀錄)
2	小組成員	是否各二級單位皆派員參加，或由一級單位管理窗口兼任						(名冊)
二	資訊及資通系統之盤點							
1	資通系統分級	每年至少完成清查所業管之資通系統一次						ISMS-215-01 資通系統盤點及分級表
2	防護基準	每年檢視上述系統，已經完成控制措施					(未完成者，需說明何時能完成)	ISMS-215-03 資通系統防護基準查檢表
3	核心業務系統	1. 業務涉及公務機關捐助、資助或研發之國家核心科技資訊之安全維護及管理					(符合檢查項目者，需通過第三方 ISMS 驗證，須提出驗證規劃)	ISMS-215-01 資通系統盤點及分級表

委商稽核表

委外廠商查核項目表

受稽廠商：美思科法顧問股份有限公司
填表日期：113年03月04日

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
1.資通安全政策之推動及目標訂定	1.1 是否定義符合組織需要之資通安全政策及目標？	■	□	□	已訂定資通安全政策及目標資通安全管理政策。
	1.2 組織是否訂定資通安全政策及目標？	■	□	□	政策及目標符合業主之需求。資通安全管理政策。
	1.3 組織之資通安全政策文件是否由管理階層核准並正式發布且轉知所有同仁？	■	□	□	依規定按時進行教育訓練之宣達。
	1.4 組織是否對資通安全政策、目標之適切性及有效性，定期作必要之審查及調整？	■	□	□	定期進行政策及目標之檢視、調整。
	1.5 是否隨時公告資通安全相關訊息？	■	□	□	將資安訊息公告於布告欄。
2.設置資通安	2.1 是否指定適當權責之高階主管負責資通安全管理之協調、推動及督導等事項？	■	□	□	指派洪協理擔任資安長。資通安全推行組織人員名冊。

矯正

- 不符合事項發生時，組織應有下列作為：
  - (a)對不符合事項反應，並於適用時，採取下列作為：
    - (1)採取行動，以控制並矯正之。
    - (2)處理其後果。
  - (b)藉由下列作為，評估對消除不符合事項之原因的行動之需要，使其不再發生且不於他處發生：
    - (1)審查不符合事項。
    - (2)判定不符合事項之原因。
    - (3)判定是否有類似之不符合事項存在，或可能發生。
  - (c)實作所有所需行動。
  - (d)審查所有所採取矯正措施之有效性。
  - (e)必要時，對資訊安全管理系統進行變更。

矯正

- 矯正措施應切合所遇到不符合事項之影響。應具備文件化資訊，以作為下列事項之證據：
  - (f)不符合事項之性質及後續採取的所有行動。
  - (g)所有矯正措施之結果。
- 矯正時機
  - 資通安全管理系統目標之有效性無法達成。
  - 風險管理控制措施。(短期間無法完成)
  - 內部/外部稽核不符合事項。
  - 發生業務持續運作計畫中未考慮之重大災難事件。
  - 發生資安事件時。

不符合事項和起因(根因)

不符合事項

實際操作和書面政策程序不一致

資訊安全風險沒有完全管理或降低

根本原因通常是缺少：

1.組織結構
2.教育、訓練、認知
3.資源
4.紀律
5.管理承諾

未能鑑別脆弱點威脅及風險

追蹤行動(follow up)

- 同意一個執行矯正措施的現實計畫
- 追蹤行動
  - 書面審查(off-site review)：根據被稽核者所提供的書面證據，審查後將NCRs結案
  - 現場稽核(On-site Audit)：安排現場稽核以確認矯正措施的有效性
- 計畫定期的追查稽核(Surveillance Audit)

矯正措施單

矯正措施單					
文件編號	ISMS-214-01	機密等級	限閱	版次	2.1

紀錄編號：　　　　　　　　　　　　　　填表日期：　年　月　日

提出單位	美商科技顧問公司	提出人員	OOO	提出日期	稽核那一天
處理單位	受稽核單位	處理人員	誰被開缺失	填寫日期	
事件來源： ■內部稽核 □外部稽核 □資通安全事件 □自行提出 □其他			事件分類： □主要缺失□次要缺失□觀察□建議 （外部稽核所發現之問題，缺失與事件項目需填寫本欄位）		
問題或缺失說明	(查核表中待改善事項)				
原因分析					

矯正措施處理方式	矯正性措施：（消除缺失或潛在風險之根本原因，防止類似事件發生） 預訂完成日期：　年　月　日		
承辦人	(單位的管理窗口)	單位主管	(一級)
追蹤紀錄(第一次)	□結案 □未結案，說明： 追蹤人：□□□□□□□□□□□□□□□□□□□□追蹤日期：　年　月　日		
追蹤紀錄(第二次)	□結案 □未結案，說明： 追蹤人：□□□□□□□□□□□□□□□□□□□□追蹤日期：　年　月　日		

管理審查(維護計畫版)

- 管理審查議題應包含下列討論事項
  - ✓ 過往管理審查議案之處理狀態
  - ✓ 與資訊安全管理系統有關之內外部議題變更，如法令變更、上級機關要求、資通安全推動小組決議事項等
  - ✓ 資通安全維護計畫內容之適切性
  - ✓ 資訊安全績效之回饋，包括：
    - 資通安全政策及目標之實施情形
    - 資通安全人力及資源之配置之實施情形
    - 資通安全防護及控制措施之實施情形
    - 內外部稽核結果
    - 不符合項目及矯正措施
  - ✓ 風險評鑑結果及風險處理計畫執行進度
  - ✓ 重大資通安全事件之處理及改善情形
  - ✓ 利害關係人之回饋
  - ✓ 持續改善之機會