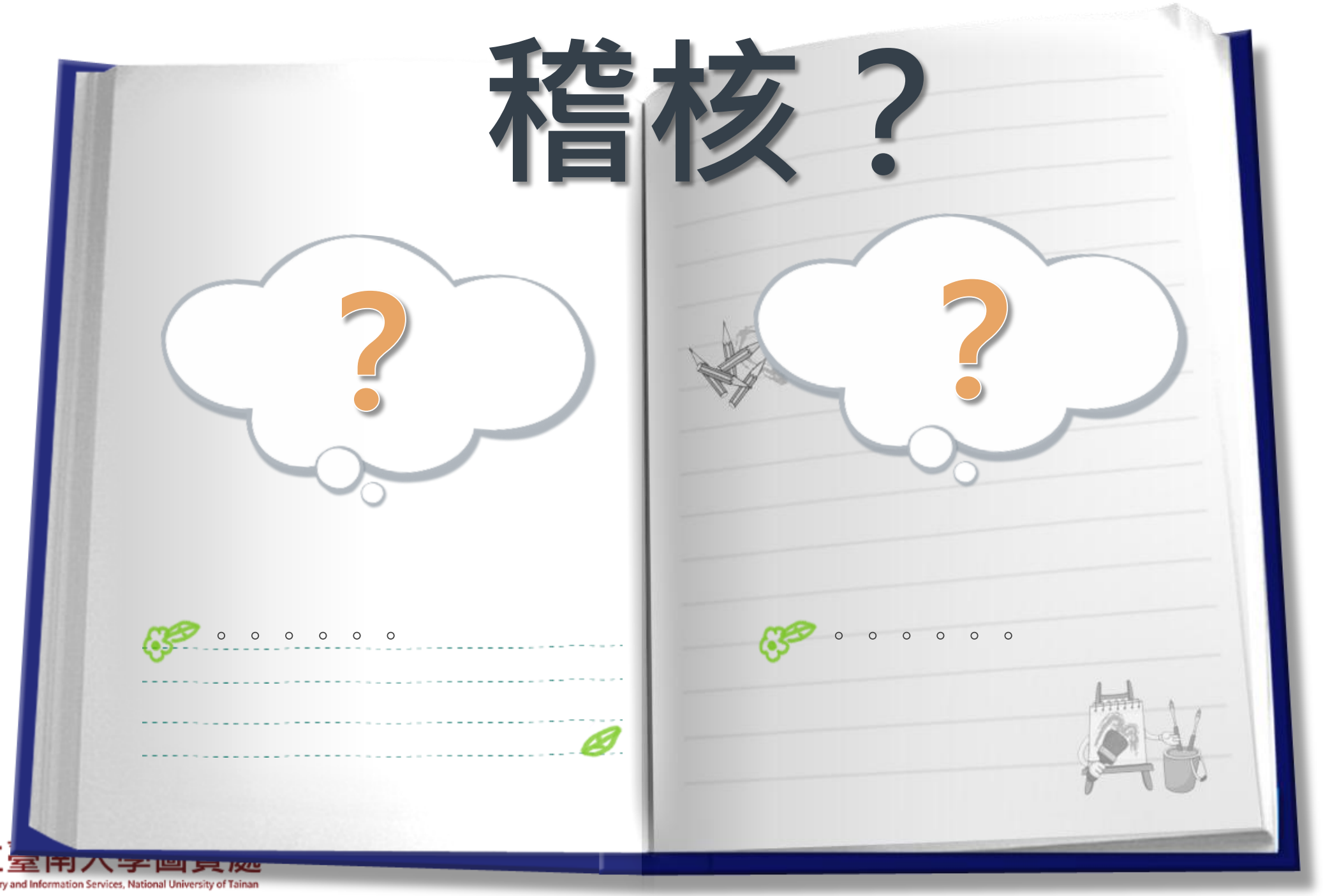
國立臺南大學
115年資安暨個資內部稽核作業說明會議

115年7月6日(星期一) 15：30

稽核？



資安例行作業檢視

Information Security

個資管理作業檢視

Personal Information Protection

資通安全作業
內部稽核

資安例行
作業檢視

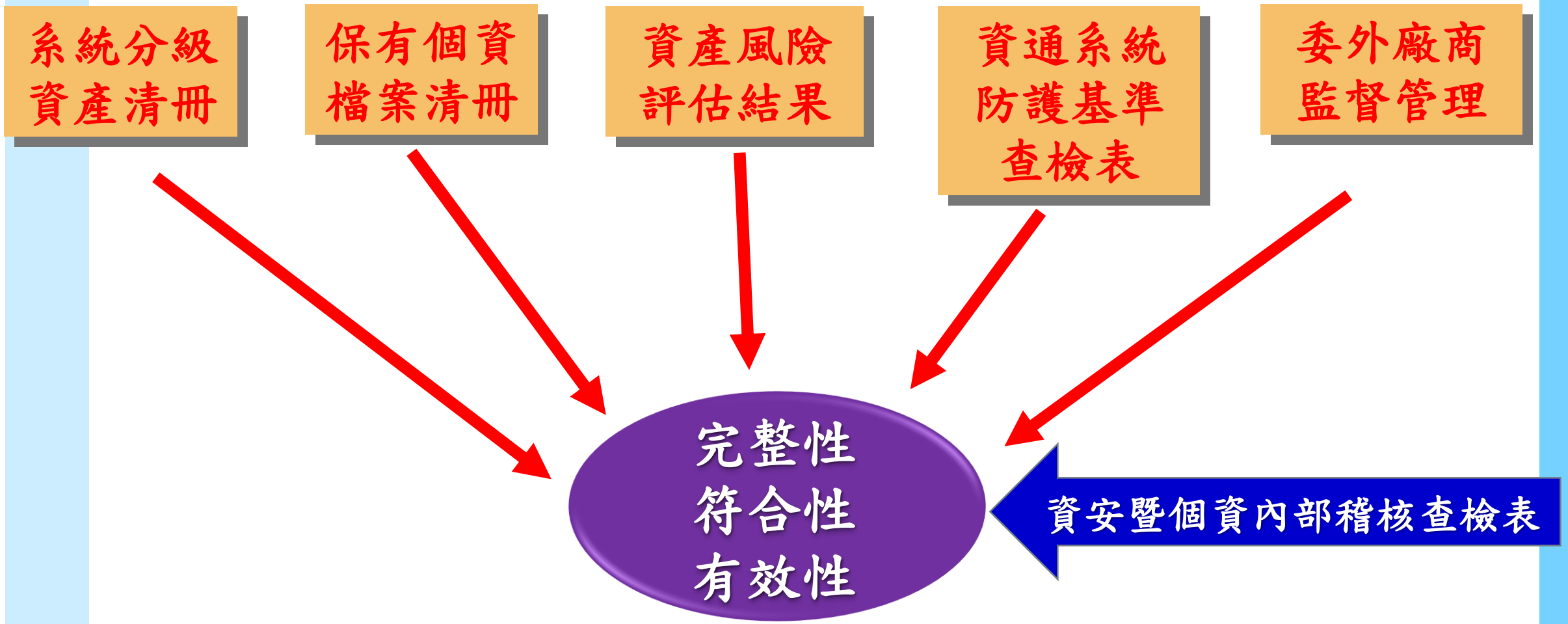
Information Security

個人資料保護
內部稽核

個資管理
作業檢視

Personal Information Protection

資安暨個資內部稽核重點



資安暨個資內部稽核檢視重點

ISMS資安稽核

稽核檢視重點

- 資訊資產清查結果
- 資訊資產風險評鑑結果
- 單位人員教育訓練時數
- 委外資通訊系統資安管理現況
- D051個人電腦查核表填報情況
- 稽核缺失持續改善情況

PIMS個資稽核

稽核檢視重點

- 保有個資檔案清查結果
- 保有個資檔案風險評鑑結果
- 個資蒐集法遵性檢核(告知聲明、最小化蒐集、定期銷毀)
- 委外資通訊系統個資保護管理
- 稽核缺失持續改善情況
- 資安暨個資內部稽核查檢表

資安暨個資內部稽核備查文件(1/2)

資產清冊

- D008資訊資產清單(表單填報系統)
- D011個人資料檔案清冊(保有個人資料檔案清查盤點系統)

風險評鑑

- D009威脅及弱點評估表(表單填報系統)
- D013個人資料檔案威脅及弱點評估表(表單填報系統)

安全維護

- D051個人電腦設定與軟體安裝查核表(表單填報系統)
- D054-資通系統防護基準查檢表-中級或普級
- 單位人員教育訓練時數資料

資安暨個資內部稽核備查文件(2/2)

查檢表

- 資安暨個資內部稽核查檢表(必備文件，稽核後收回。)
- D054資通系統防護基準查檢表-普級或中級(有委外系統)

委外管理

- 需求書或契約書，廠商資安作為紀錄文件及佐證資料。
- 廠商及維護人員保密切結書。

持續改善

- 矯正處理單改善追蹤情形(有如開立次要不符合事項)。
- 過往稽核缺失持續改善情形。

國立臺南大學一資安暨個資內部稽核查檢表

適用範圍：本校115年資安暨個資內部稽核各行政及教學單位

單位名稱(全銜)：＿＿＿＿＿＿＿＿填表人員：＿＿＿＿＿＿填表日期：115年　月

編號	查檢項目	查檢說明	自評結果	查檢結果
1	資訊資產暨個人資料風險評鑑作業(本文集)	1.個資處理人是否就已界定個人資料之範圍與蒐集、處理及利用流程，分析評估可能產生之風險及可能面臨的風險等級？ 2.資產管理人是否就資訊資產之分析評估可能產生之風險及可能面臨的風險等級？	□是 □否	□符合 □不符合
2	資訊資產暨個人資料盤點作業(A.8.1.1)	1.是否已識別資訊及資訊處理設施相關之資產，製作資訊資產之清冊，且每年至少清查一次所保有之資訊資產現況。 2.是否已確認蒐集個人資料之特定目的，依特定目的之必要性，界定所蒐集、處理及利用個人資料之類別或範圍及個人資料留存於單位之期間，且每年至少清查一次所保有之個人資料現況。	□是 □否	□符合 □不符合
3	已完成電腦作業系統帳號密碼設定(A.9.4.2)	1.應設定個人密碼(不可設為自動登入)、作業系統更新前檢查看是否需要輸入密碼。 2.至少每6個月更換一次密碼。 3.密碼長度至少8碼。 4.密碼應包含大小寫字母、數字、符號。	□是 □否	□符合 □不符合
4	已完成設定螢幕保護裝置，並啟動密碼設定(A.11.2.9)	1.設定螢幕保護裝置15分鐘以內，並勾選繼續執行後，顯示登入畫面。 2.離開座位時，應將電腦鎖定及設定螢幕保護裝置，並啟動密碼以保護電腦資料安全。	□是 □否	□符合 □不符合
5	無未授權軟體或來路不明軟體(A.12.2.1)	1.禁止使用非本校購買授權使用商用軟體。 2.禁止使用違反著作權法等來路不明軟體。 3.如有發現來路不明或未授權檔案，請移除。	□是 □否	□符合 □不符合
6	開啟系統或軟體自動更新功能(A.12.2.1)	應配合進行系統或軟體(例如 Windows、Java、Flash Player 、Adobe Reader 、7zip 等)更新，修補漏洞，保持更新至最新狀態，勿關閉系統自動更新程式。	□是 □否	□符合 □不符合
7	已安裝防毒軟體並更新病毒碼(A.12.2.1)	1.檢查電腦是否有安裝本校購買之正版防毒軟體並更新病毒碼至最新。 2.使用外來檔案，應先掃毒；勿任意移除或關閉防毒軟體。	□是 □否	□符合 □不符合
8	郵件軟體安全管理(A.12.6.2)	1.開啟郵件軟體中所有資訊夾郵件預覽功能。 2.開啟純電子郵件純文字模式。 3.不開啟或轉寄來路不明的電子郵件及其附件檔案或連結。	□是 □否	□符合 □不符合

編號	查檢項目	查檢說明	自評結果	查檢結果
9	已完成 google 瀏覽器安全設定 (A.18.1.1)	啟用標準防護模式	□是 □否	□符合 □不符合
10	是否瞭解禁止於上班時間瀏覽非公務用途網站(A.18.1.1)	上班時間禁止瀏覽非公務用途網站及暴力、色情、賭博、駭客、惡意網站，避免電腦中惡意或遭駭客入侵致使內部機密遭盜或資料外洩。	□是 □否	□符合 □不符合
11	ISMS 表單維護	D006 外部單位聯絡表	□是 □否	□適用 □不適用
		D008_資訊資產清單 *表單系統填報	□是 □否	□適用 □不適用
		D009 威脅及弱點評估表 *表單系統填報	□是 □否	□適用 □不適用
		D010_風險評鑑彙整表	□是 □否	□適用 □不適用
		D011 風險改善計畫表	□是 □否	□適用 □不適用
		D013_保密切結書	□是 □否	□適用 □不適用
		D014_人員職掌清冊	□是 □否	□適用 □不適用
		D015 離職人員移交流程表	□是 □否	□適用 □不適用
		D020 合約商保密切結書	□是 □否	□適用 □不適用
		D030_稽核消查結果報告 *表單系統填報	□是 □否	□適用 □不適用
		D036_業務流程衝擊分析表 *訂定管理之系統(組站)最大可容忍中斷時間(MTPD)、復原時間目標(RTO)及資料復原時間目標(RPO)	□是 □否	□適用 □不適用
		D040_資訊資產異動申請表	□是 □否	□適用 □不適用
		D042_適用法規清單	□是 □否	□適用 □不適用

編號	查檢項目	查檢說明	自評結果	查檢結果
		D051_個人電腦設定與軟體安裝查核	□是 □否	□適用 □不適用
12	PIMS 表單維護	D002_人員職掌清冊	□是 □否	□適用 □不適用
		D005_外部單位聯絡表	□是 □否	□適用 □不適用
		D011 個人資料檔案清冊	□是 □否	□適用 □不適用
		D013 個人資料檔案威脅及弱點評估表	□是 □否	□適用 □不適用
		D016_個人資料提供同意書	□是 □否	□適用 □不適用
		D017_隱私權政策聲明	□是 □否	□適用 □不適用
		D018 個人資料使用資訊服務申請表	□是 □否	□適用 □不適用
		D019 個人資料紀錄刪除申請單	□是 □否	□適用 □不適用
		D020_個人資料申訴事件紀錄單	□是 □否	□適用 □不適用
		D021_個人資料特定目的範圍變更需求同意書	□是 □否	□適用 □不適用
		D027_員工個人資料保密切結書	□是 □否	□適用 □不適用
		D031 假設消查結果報告 *表單系統填報(同 ISMS 之 D030)	□是 □否	□適用 □不適用

註：

一、 表單系統網址：https://system.nutn.edu.tw/form/fill

二、 ISMS 表單及 PIMS 表單請由文件管理系統下載，文件管理系統網址：https://system.nutn.edu.tw/doc/doc/

填表人員簽核：＿＿＿＿＿＿

查檢人員簽核：＿＿＿＿＿＿(稽核組長)

資安暨個資內部稽核查檢表

D054資通系統防護基準查檢表-普級

單位(組別)		管理人		填表日期	
系統名稱					
建置廠商			維護廠商		
版本類別	□公版　□機關自用			維護合約 □無 □有，至＿＿＿＿＿＿為止	
系統建置方式	□自行委外 □租用服務 □套裝軟體 □自行開發 □主管/上級機關提供 □其他＿＿＿＿＿＿				
填表人核章			單位主管核章		

1.系統環境資訊

作業系統	□Windows，版本: Windows Server 2019 □Mac OS，版本:＿＿＿＿ □Unix / Linux，版本:　□FreeBSD，版本: □其他，作業系統名稱　，版本: 註：請請寫出「種類」和「版本號碼」，如 Linux 請寫 CentOS 6.8、RHEL 6.8、Oracle Linux 6.8 或其他，而非只寫 Linux 6.8，以利查出 弱點漏洞資訊。
程式語言	□C/C++，版本:　□C#，版本:＿＿＿＿ □Java，版本:　□JavaScript，版本: □Python，版本:＿＿＿＿　□PHP，版本:＿＿＿＿ □Visual Basic .NET，版本:＿＿＿＿

	□其他，語言名稱＿＿＿＿＿＿，版本:＿＿＿＿＿＿ 註：請請填寫詳細版本，如 PHP 請寫 7.3.17 或其他，而非 PHP 7.0。
Web 伺服器	□無 □有： □Apache HTTP Server，版本:＿＿＿＿＿＿ □Apache Tomcat Server，版本:＿＿＿＿＿＿ □Microsoft IIS，版本：8.0＿＿＿＿＿＿ Nginx，版本: □其他，伺服器名稱　，版本: 註：請請填寫詳細版本，如 Tomcat 請寫 7.0.65 或其他，而非 Tomcat 7.0。
資料庫	□無 □有： □DB2，版本:＿＿＿＿＿＿　□Sqlite，版本:＿＿＿＿＿＿ Oracle，版本:　□MySQL，版本: PostgreSQL，版本: Microsoft Access，版本: □Microsoft SQL Server，版本:＿＿＿＿＿＿ □其他，資料庫名稱＿＿＿＿＿＿，版本:＿＿＿＿＿＿ 註：請請填寫詳細版本，如 Oracle Database 請寫 12.1.0.1，而非僅寫 12。
網站框架	□無 □有： Struts，版本:　□Spring，版本: ZK，版本:　□Django，版本: .Net Framework，版本:＿＿＿＿ □其他，網站框架名稱＿＿＿＿＿＿，版本:＿＿＿＿＿＿ 註：請請填寫詳細版本

	元件名稱	版本（須詳填實際版本）
軟體元件清單	jQuery	3.5.1
	alertify dataTables	0.3.11 1.10.15
	Combo Select	23/11/2014
	ClosedXML	0.94.2

2.控制措施查檢表

構面	控制措施	控制內容	檢閱檢視結果	備註
存取控制	帳號管理(CC101)	一、建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。	□是，具備以下程序： □帳號申請程序 □帳號建立程序 □帳號修改程序 □帳號啟用程序 □帳號停用程序 □帳號刪除程序 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、已逾期之臨時或緊急帳號應刪除或禁用。	□是，逾期之臨時或緊急帳號已刪除或禁用。 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		三、資通系統閒置帳號應禁用。	□是，資通系統閒置帳號已禁用。 □否，請於備註欄說明原因 □不適用，請於備註欄說明	

構面	控制措施	控制內容	檢閱檢視結果	備註
		四、定期審核資通系統帳號之建立、修改、啟用、停用及刪除。	□是，具備以下定期審核程序： □申請程序 □建立程序 □修改程序 □啟用程序 □停用程序 □刪除程序 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	最小權限(CC102)	一、採最小權限原則，僅允許使用者（或代表使用者行為之程序）依指派任務及業務功能，完成指派任務所需之授權存取。	□是，採最小權限原則授權存取 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	遠端存取(CC103)	一、對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化，使用者之遠端檢查作業應於伺服器端完成。	□是，組織有遠端存取 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、使用者之遠端檢查作業應於伺服器端完成。	□是， □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		三、應監控資通系統遠端連線。	□是，請於備註欄說明監控方式 □否，請於備註欄說明原因 □不適用，請於備註欄說明	

國立臺南大學「資通系統防護基準」控制措施自檢表-普級

文件編號：NUTN-ISMS-D054	版次：1.1	機密等級：限閱
紀錄編號：	填表日期：　年　月　日	

構面	控制措施	措施內容	檢測檢視結果	備註
	日誌紀錄內容(C0202)	一、資通系統產生之稽核紀錄(AuditLogs)應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用單一日誌紀錄機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。	□是，包含以下資訊： □事件類型 □發生時間 □發生位置 □任何與事件相關之使用者之身分識別 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	日誌儲存容量(C0203)	一、依據日誌儲存需求，配置所需之儲存容量。	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	日誌處理失效之回應(C0204)	一、資通系統於稽核處理失效時，應採取適當之行動。	□是， □關閉資通系統 □覆寫最舊的稽核紀錄 □停止產生稽核紀錄 □通知管理者進行故障排除作業 □其他，請於備註欄說明 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	時戳及校時(C0205)	一、資通系統應使用系統內部時鐘產生稽核紀錄(AuditLogs)所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、系統內部時鐘應定期與基準時間源進行同步。	□是，已定期與基準時間源進行同步 □否，請於備註欄說明原因 □不適用，請於備註欄說明	

國立臺南大學「資通系統防護基準」控制措施自檢表-普級

文件編號：NUTN-ISMS-D054	版次：1.1	機密等級：限閱
紀錄編號：	填表日期：　年　月　日	

構面	控制措施	措施內容	檢測檢視結果	備註
		四、資通系統應採用加密機制。	□是， □HTTPS □SSH □VPN □其他，請於備註欄說明 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		五、資通系統遠端存取之來源應為機關已預先定義及管理之存取控制點。	□是，遠端存取之來源已預先定義及管理存取控制點 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
事件日誌與可歸責性	記錄事件(C0201)	一、訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。	□是，記錄以下事件： □登入登出 □更改密碼 □登錄失敗 □資訊系統存取失敗 □其他，請於備註欄說明 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		三、應記錄資通系統管理者帳號所執行之各項功能。	□是， □否，請於備註欄說明原因 □不適用，請於備註欄說明	

國立臺南大學「資通系統防護基準」控制措施查檢表-普級

文件編號：NUTN-ISMS-D054	版次：1.1	機密等級：限閱
紀錄編號：	填表日期： 年 月 日	

構面	控制措施	措施內容	執行檢視結果	備註
		三、具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。	□是：帳戶鎖定機制為失敗達____次，則____分鐘內不得再登入 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		四、使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。	□是： □密碼長度____位字元以上 □已要求密碼組成複雜度 □最短效期____天 □最長效期____天 □其他：請於備註欄說明 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		五、密碼變更時，至少不可以與前三次使用過之密碼相同。	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		六、第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理。	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	鑑別資訊回饋(C0403)	一、資通系統應遮蔽鑑別過程中之資訊。	□是： □密碼輸入欄位預設以「*」顯示或不顯示 □使用憑證或QR碼進行鑑別 □其他：請於備註欄說明 □否，請於備註欄說明原因 □不適用，請於備註欄說明	

國立臺南大學「資通系統防護基準」控制措施查檢表-普級

文件編號：NUTN-ISMS-D054	版次：1.1	機密等級：限閱
紀錄編號：	填表日期： 年 月 日	

構面	控制措施	措施內容	執行檢視結果	備註
	日誌資訊之保護(C0206)	一、對日誌之存取管理，僅限於有權限之使用者。	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
營運持續計畫	資料備份(C0301)	一、訂定資料可容忍資料損失之時間要求。	□是，RPO設定為 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、執行資料備份。	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	系統備援(C0302)	一、訂定資通系統從中斷後至重新恢復服務之最大可容忍中斷時間要求（RTO）。	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
識別與鑑別	使用者之識別與鑑別(C0401)	一、資通系統應識別及鑑別使用者，並禁止使用者使用共用帳號。	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	身分驗證管理(C0402)	一、使用預設密碼登入系統時，應於登入後要求立即變更。	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、身分驗證相關資訊不以明文傳輸。	□是，使用____加密傳輸機制 □否，請於備註欄說明原因 □不適用，請於備註欄說明	

國立臺南大學「資通系統防護基準」控制措施查檢表-普級

文件編號：NUTN-ISMS-D054	版次：1.1	機密等級：限閱
紀錄編號：	填表日期： 年 月 日	

構面	控制措施	措施內容	執行檢視結果	備註
	系統發展生命週期部署與維運階段(C0505)	一、於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、資通系統不使用預設密碼。	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	系統發展生命週期委外階段(C0506)	一、資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約。	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	獲得程序(C0507)	一、識別資通系統使用之第三方軟體、服務、函式庫或其他元件。	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	系統文件(C0508)	一、應儲存與管理系統發展生命週期之相關文件。	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
系統與資訊完整性	漏洞修復(C0701)	一、系統之漏洞修復應測試有效性及潛在影響，並定期更新。	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	資通系統監控(C0702)	一、發現資通系統有被入侵跡象時，應通報機關特定人員。	□是，依機關作業程序通報 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	軟體及資訊完整性(C0703)	一、使用者輸入資料合法性檢查應置放於應用系統伺服器端。	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	

國立臺南大學「資通系統防護基準」控制措施查檢表-普級

文件編號：NUTN-ISMS-D054	版次：1.1	機密等級：限閱
紀錄編號：	填表日期： 年 月 日	

構面	控制措施	措施內容	執行檢視結果	備註
	非內部使用者之識別與鑑別(C0405)	一、資通系統應識別及鑑別非機關使用者（或代表機關使用者行為之程序）。	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
系統與服務獲得	系統發展生命週期需求階段(C0501)	一、針對系統安全需求（含機密性、可用性、完整性）進行確認。	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	系統發展生命週期開發階段(C0503)	一、應針對安全需求實作必要控制措施。	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		二、應注意避免軟體常見漏洞及實作必要控制措施。	□是， □源碼已防範OWASP所公布之最新OWASP TOP10安全風險 □已執行源碼檢測，並確認中、高風險弱點已修復 □其他控制措施：請於備註欄說明 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
		三、發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	
	系統發展生命週期測試階段(C0504)	一、執行「弱點掃描」安全檢測。	□是 □否，請於備註欄說明原因 □不適用，請於備註欄說明	

資安暨個資內部稽核產出文件

稽核產出文件

- 單位內部稽核查檢表
  - 各單位稽核前自評填寫，稽核後收回。
- 內部稽核表
  - 稽核人員稽核過程中紀錄稽核發現事項及佐證資料。
- 內部稽核報告
  - 稽核人員稽核結束後，提出稽核報告。

資通安全管理規範導入

- 資訊資產清查
- 系統分類分級
- 資產風險評鑑
- 完成教育訓練
- 委外系統監督
- 資安事件通報

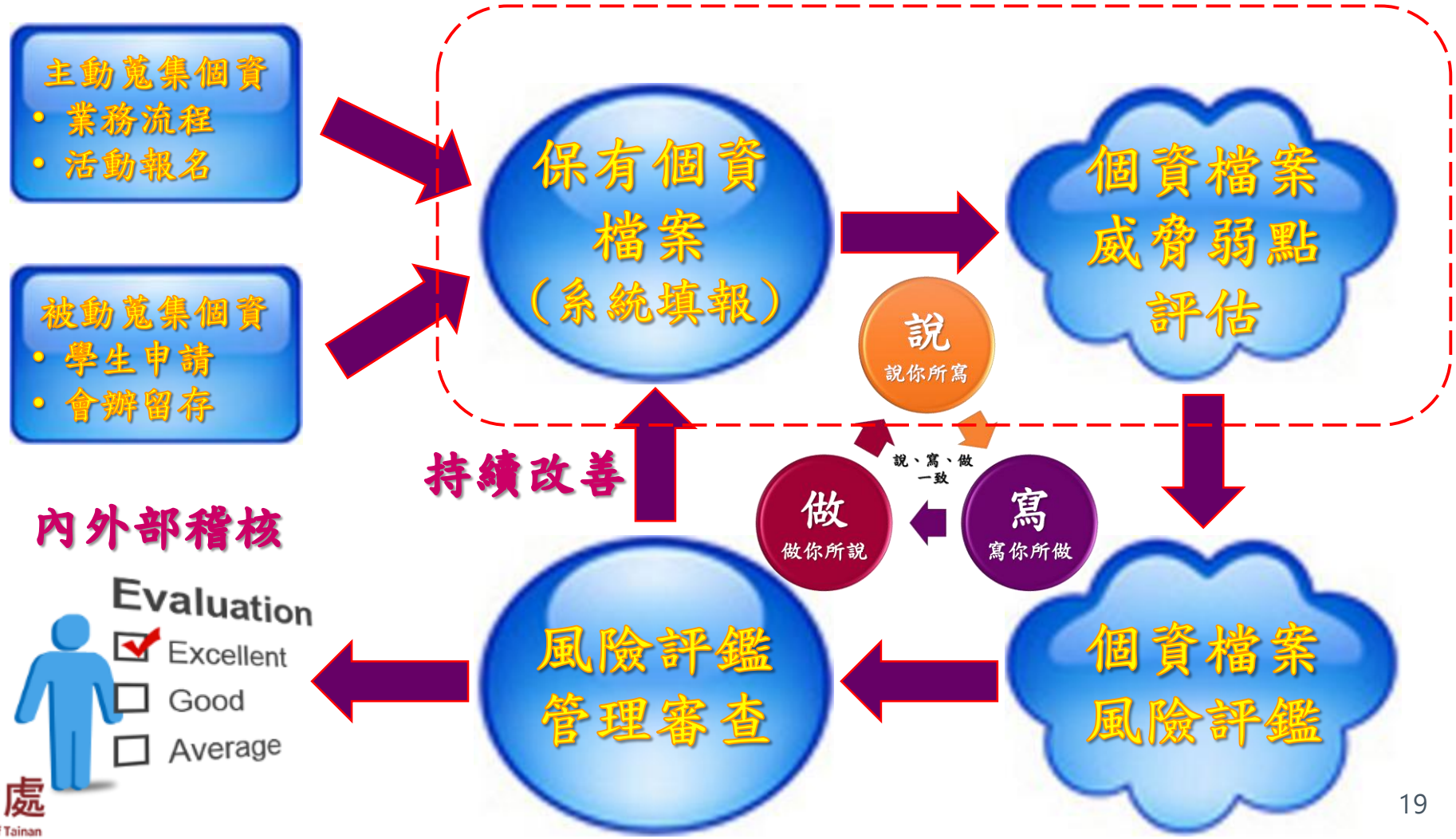
如果您是
稽核員或
稽核觀察員

- ◆有資訊系統→進行分類分級
- ◆有資訊資產→進行清查
- ◆針對資訊資產→進行風險評鑑
- ◆系統委外→委外管理監督作為
- ◆系統防護基準查檢表(D054)
- ◆資訊作業安全性(D051)
- ◆有無資安事件？
- ◆完成教育訓練？

個人資料管理規範導入

- 個資檔案清查
- 告知同意機制
- 個資風險評鑑
- 完成教育訓練
- 個資安全管理
- 落實定期銷毀

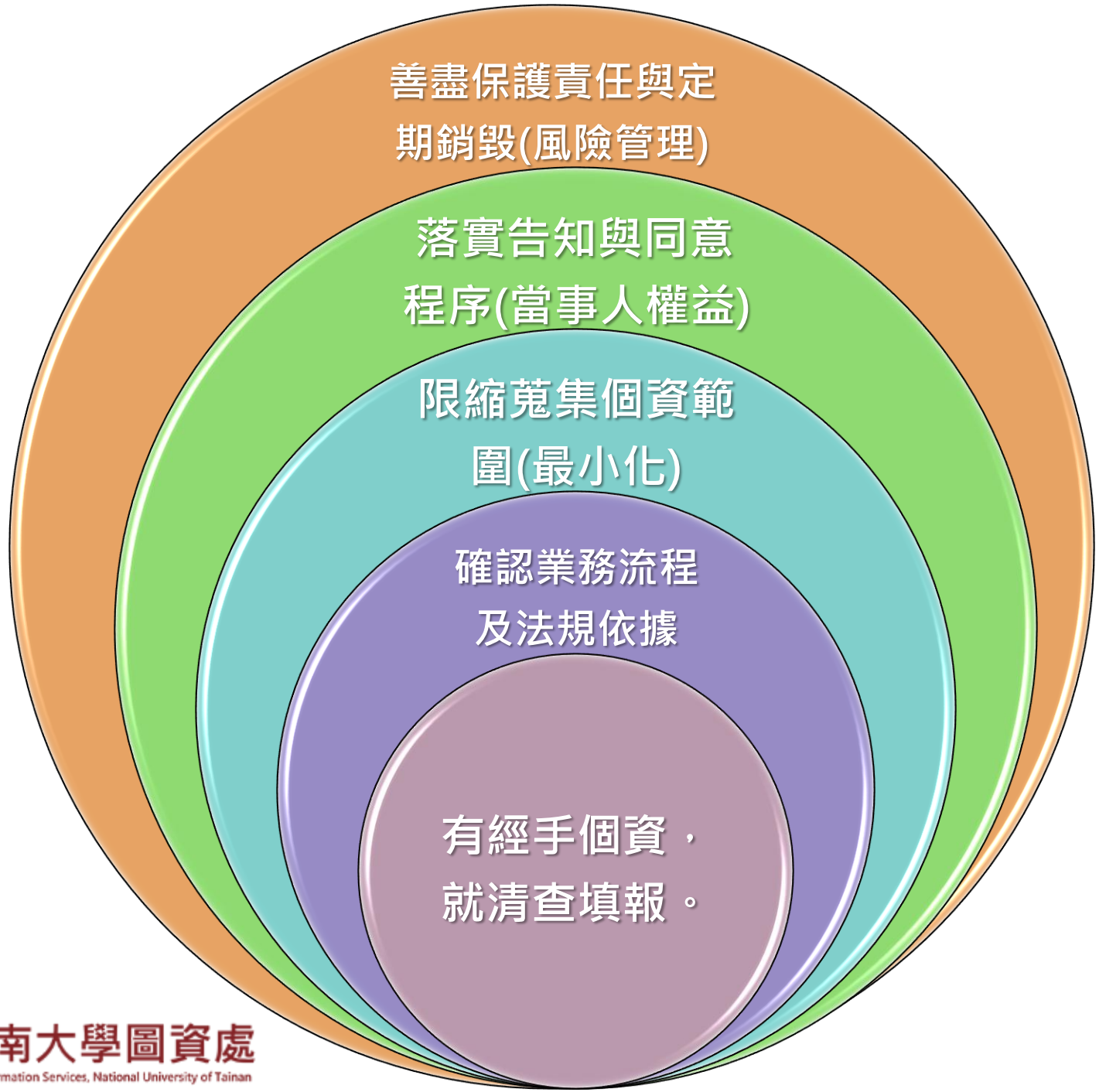
個人資料管理規範導入


主動蒐集個資
• 業務流程
• 活動報名
被動蒐集個資
• 學生申請
• 會辦留存
保有個資檔案（系統填報）
個資檔案威脅弱點評估
說
說你所寫
說、寫、做一致
寫
寫你所做
做
做你所說
持續改善
內外部稽核
Evaluation
Excellent
Good
Average
風險評鑑管理審查
個資檔案風險評鑑

維思

理管

資個



內部人員要求：
1、保密要求
2、教育訓練(含資安)
3、職掌權限與代理

系統維護廠商：
1、保密要求
2、監督管理
3、資料返還或銷毀

如果您是
稽核員或
稽核觀察員

- ◆有蒐集個資→個資檔案清查
- ◆個資蒐集→告知聲明
- ◆保有個資檔案→進行風險評鑑
- ◆個資蒐集、處理或利用依據？
- ◆個資安全管理作為？
- ◆系統個資委外管理作為？
- ◆有無個資外洩事件？
- ◆完成教育訓練？

國立臺南大學
115年
資安暨個資內部稽核作業
7月21日-22日教學單位
7月23日-24日行政單位

115 年資安暨個資內部稽核作業第一階段分組時間表(教學單位、圖資處資訊系統組及網路服務組)

日期	時間	第一組		第二組		第三組	
		受稽單位	稽核顧問	受稽單位	稽核顧問	受稽單位	稽核顧問
7 月 21 日 (星期二)	10:00-10:10	啟始會議 ◎視訊會議 https://meet.google.com/ems-quqa-dcy					陳俊茂 左寧生 郭家瑋
	10:10-10:30	管理階層訪談(B401 國際會議廳)					陳俊茂 左寧生 郭家瑋
	10:30-12:00	● 教育學院 ● 教育學系 ● 幼兒教育學系 ● 諮商與輔導學系	陳俊茂	● 特殊教育學系 ● 視覺藝術與設計學系 ● 體育學系 ● 數位學習科技學系	左寧生	● 環境與生態學院 ● 生態暨環境資源學系 ● 生物科技學系	郭家瑋
	12:00-14:00	中午休息					
	14:00-16:30	● 人文學院 ● 文化與自然資源學系 ● 英語學系 ● 國語文學系	陳俊茂	● 理工學院(含智慧製造在職學位學程) ● 材料科學系 ● 應用數學系	左寧生	● 戲劇創作與應用學系 ● 綠色能源科技學系 ● 資訊工程學系 ● 電機工程學系	郭家瑋
7 月 22 日 (星期三)	10:00-12:00	● 行政管理學系 ● 藝術學院 ● 音樂學系	陳俊茂	● 圖資處資訊系統組 ● 圖資處網路服務組	左寧生	● 管理學院(含 EMBA 碩士在職專班) ● 經營與管理學系	郭家瑋
	12:00-14:00	中午休息					
	14:00-16:30	● 學務處輔導中心 ● 圖資處讀者服務組 ● 圖資處館藏發展組 ● 校友服務中心	陳俊茂	● 總務長室 ● 總務處事務組 ● 總務處營繕組 ● 總務處文書組	左寧生	● 總務處出納組 ● 總務處保管組 ● 總務處環安組	郭家瑋

115 年資安暨個資內部稽核作業第二階段分組時間表(行政單位)

日期	時間	第一組		第二組		第三組	
		受稽單位	稽核顧問	受稽單位	稽核顧問	受稽單位	稽核顧問
7 月 23 日 (星期四)	10:00-12:00	● 李副校長室 ● 侯副校長室	陳俊茂	● 秘書室 ● 學務長室 ● 學務處生活輔導組	左寧生	● 體育室 ● 學務處課外活動指導組 ● 原住民族學生資源中心	郭家瑋
	12:00-14:00	中午休息					
	14:00-16:30	● 教務長室 ● 教務處企畫組 ● 教務處教學業務組	陳俊茂	● 學務處衛生保健組 ● 通識教育中心	左寧生	● 研究發展處計畫服務組 ● 研究發展處學術發展組 ● 國際事務處(含語文中心) ● 研究發展處創新育成中心	郭家瑋
7 月 24 日 (星期五)	10:00-12:00	● 教務處學籍成績組 ● 教務處數位學習中心 ● 教學與學習發展中心	陳俊茂	● 人事室 ● 主計室 ● 師資培育中心	左寧生	● 教務處進修推廣組 ● 特殊教育中心 ● 視障教育與重建中心	郭家瑋
	12:00-14:00	中午休息					
	14:00-16:00	稽核結果彙整					陳俊茂 左寧生 郭家瑋
	16:00	總結會議 ◎視訊會議 https://meet.google.com/ems-quqa-dcy					陳俊茂 左寧生 郭家瑋

稽核活動說明

› 本次稽核採行標準、程序及規範

- 資通安全管理法、個人資料保護法。
- 教育體系資通安全暨個人資料管理規範。
- 本校資通安全及個人資料管理規範稽核作業程序書。
- 本校所訂定之資通安全及個人資料管理政策及各項管理規定。

› 稽核範圍

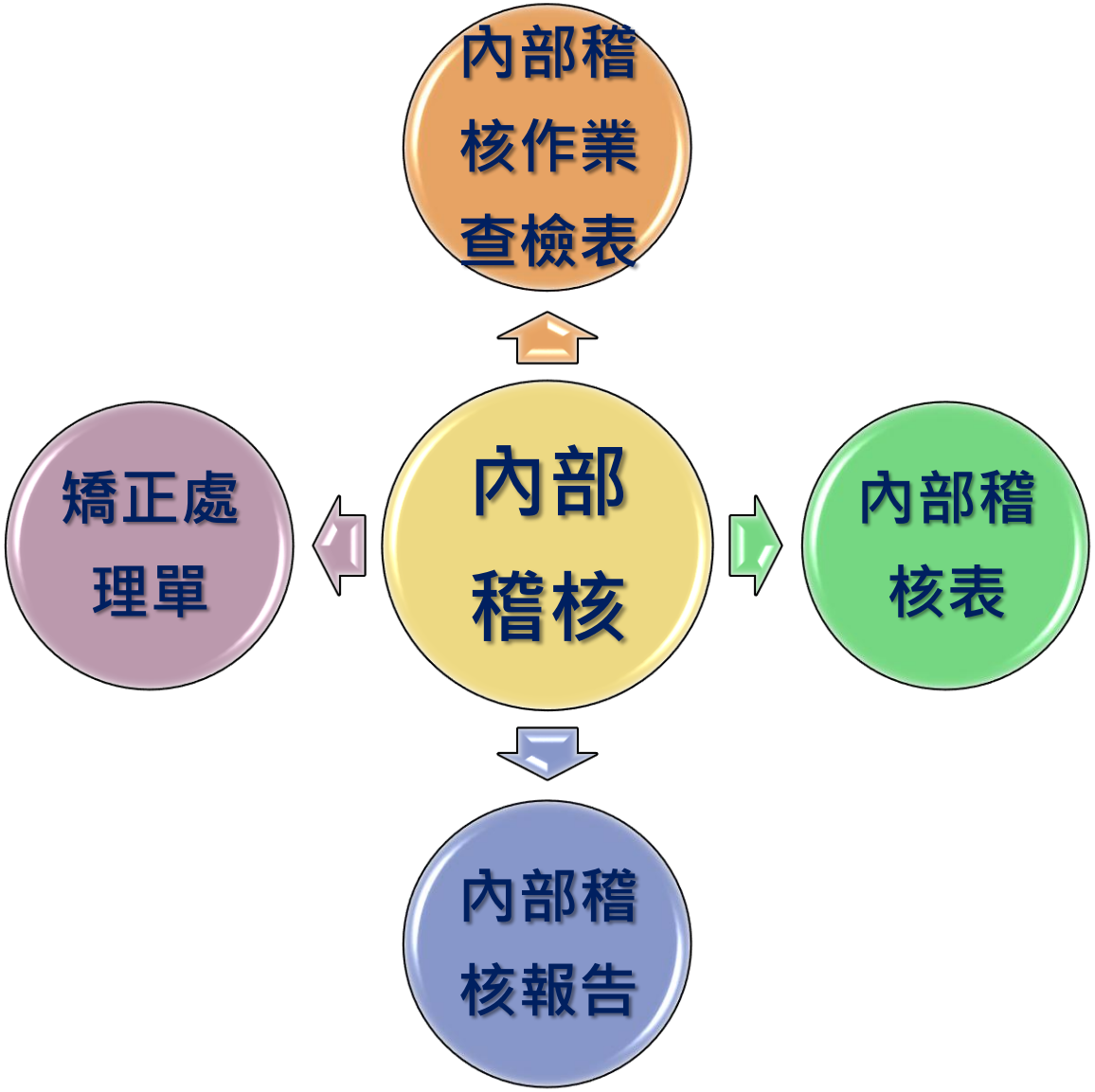
- 本校各行政及教學單位（含榮譽校區）涉及資訊安全管理之各項環境、人員及流程。
- 本校各行政及教學單位（含榮譽校區）涉及個資業務之人員及環境。

資安暨個資內部稽核小組成員

國立臺南大學 115 年資安暨個資內部稽核作業—南大稽核團隊名單

日期	時段	第一組 稽核顧問	第一組 圖資處	第一組 觀察員	第二組 稽核顧問	第二組 圖資處	第二組 觀察員	第三組 稽核顧問	第三組 圖資處	第三組 觀察員
115 年 7 月 21 日(星期二) 教學單位-全天	10:30-12:00	何冠龍	郭建宏	羅秀雲	左寧生	顏志榮	王律心	郭家瑋	許良維	柯美荷
	14:00-16:30	何冠龍	郭建宏	鄭雅容	左寧生	顏志榮	蔡宛庭	郭家瑋	許良維	吳佳靜
115 年 7 月 22 日(星期三) 教學單位—上午 行政單位—下午	10:00-12:00	何冠龍	王元良	吳怡靚 鄭雅方	左寧生	顏志榮	蔡宛庭 林純雅	郭家瑋	許良維	蔡佐穗
	14:00-16:30	陳俊茂	張育傑	徐英芬	左寧生	王惠民	蔡宛庭	郭家瑋	林芳彬	張昱隆
115 年 7 月 23 日(星期四) 行政單位—全天	10:00-12:00	陳俊茂	曾映鳳	許瑞玲 張筱青 陳可華 施明義	左寧生	蔡東樺	鄭嘉川 鄭汶琳 江姿慧 顏怡玄	郭家瑋	王元良	方淑玲 林芸安 陳柏欣 鄭雅方 方淑音
	14:00-16:30	陳俊茂	曾映鳳	呂季樺 趙善立	左寧生	蔡東樺	邱佳玉 吳怡靚	郭家瑋	王元良	林貴蘭 曾子旂
114 年 7 月 24 日(星期五) 行政單位—上午	10:00-12:00	陳俊茂	張育傑	張耀楚	左寧生	王惠民	蔡宛庭	郭家瑋	林芳彬	蔡月春

內部稽核檢視及產出文件



個人電腦設定與軟體安裝查核表

文件編號：NUTN-ISMS-D051	版次：1.8	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	電腦系統採帳號密碼設定	□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→帳戶鎖定閾值=3、帳戶鎖定/重設時間=10分鐘 帳戶之「密碼永久有效」不得勾選 ✓ 右鍵點選「本機」，選擇「電腦管理」， ✓ 點擊左方的「本機使用者和群組」，選擇「使用者」， ✓ 於任一個帳戶點按右鍵內下，確認「密碼永久有效」未勾選，再點擊確認即可。
4	刪除/關閉不必要帳號。	□是□否	如關閉 Guests
5	完成系統校時設定	□是□否	網路同步主機 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	15 分鐘以內啟動，並勾選「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	完整掃描及驅動掃描，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	無非法或未經授權軟體。	□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)。
15	Outlook 及 Mail2000 郵件	□是□	✓ 開啟 Microsoft Outlook：

個人電腦設定與軟體安裝查核表

文件編號：NUTN-ISMS-D051	版次：1.8	機密等級：限閱
紀錄編號：	填表日期： 年 月 日	

	預覽功能關閉		一、點選【檢視】→點選【版面配置】→點選【讀取窗格】→點選【關閉】。 二、點選【檢視】→點選【訊息預覽】→點選【關閉】。 ✓ 開啟 mail2000 網頁版→點選左側面板【個人設定】→點選控制面板【個人化設定】→點選左側面板【使用環境】→點選右側【郵件】標籤→「郵件自動預覽」點選【關閉】→點選【確定】存檔。

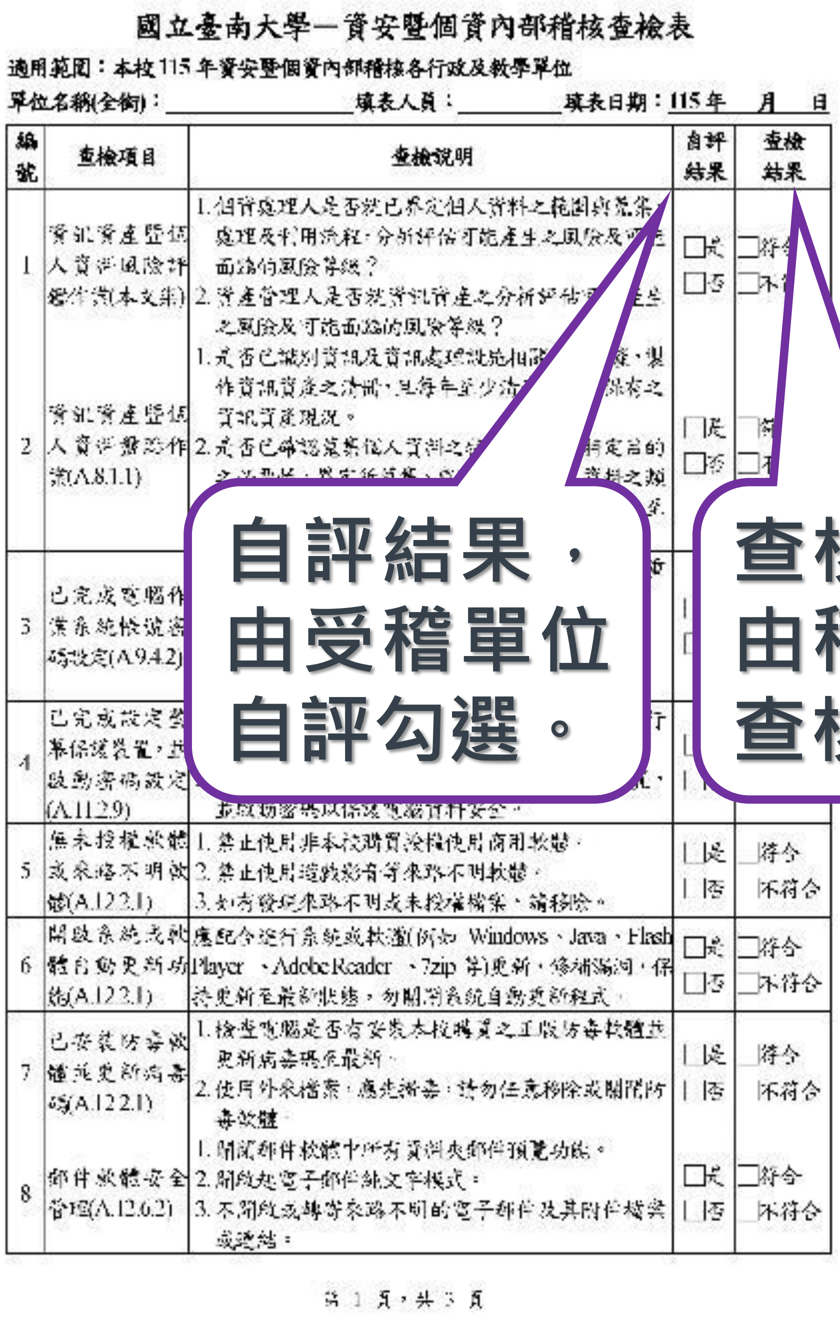
管理人	單位主管

內部稽核檢視文件

D051個人電腦設定與軟體安裝查核表，每人每半年檢核一次。(表單系統填寫)

內部稽核檢視文件

各單位資安暨個資承辦人員(資訊系統負責人)於稽核前完成自評(於「自評結果」欄位勾選)並填寫單位名稱、填表人員及日期等資訊後自行留存。(紙本填寫)



國立臺南大學—資安暨個資內部稽核查檢表

適用範圍：本校 115 年資安暨個資內部稽核各行政及教學單位

單位名稱(全銜)：________ 填表人員：________ 填表日期：115 年 月 日

編號	查檢項目	查檢說明	自評結果	查檢結果
1	資訊資產暨個人資料風險評鑑作業(本文集)	1. 個資處理人是否就已界定個人資料之範圍與蒐集、處理及利用流程，分析評估可能產生之風險及可能面臨的風險等級？ 2. 資產管理人是否就資訊資產之分析評估[illegible]產生之風險及可能面臨的風險等級？	□是 □否	□符合 □不符合
2	資訊資產暨個人資料盤點作業(A.8.1.1)	1. 是否已識別資訊及資訊處理設施相關[illegible]，製作資訊資產之清冊，且每年至少清[illegible]保存之資訊資產現況。 2. 是否已確認蒐集個人資料之[illegible]特定目的[illegible]資料之類[illegible]	□是 □否	□符合 □不符合
3	已完成電腦作業系統帳號密碼設定(A.9.4.2)	[illegible]	[illegible]	[illegible]
4	已完成設定螢幕保護裝置，且啟動密碼設定(A.11.2.9)	[illegible]	[illegible]	[illegible]
5	無未授權軟體或來路不明軟體(A.12.2.1)	1. 禁止使用非本校購買授權使用商用軟體。 2. 禁止使用違法影音等來路不明軟體。 3. 如有發現來路不明或未授權檔案，請移除。	□是 □否	□符合 □不符合
6	開啟系統及軟體自動更新功能(A.12.2.1)	應配合進行系統或軟體(例如 Windows、Java、Flash Player 、Adobe Reader 、7zip 等)更新，修補漏洞，保持更新至最新狀態，勿關閉系統自動更新程式。	□是 □否	□符合 □不符合
7	已安裝防毒軟體並更新病毒碼(A.12.2.1)	1. 檢查電腦是否有安裝本校購買之正版防毒軟體並更新病毒碼至最新。 2. 使用外來檔案，應先掃毒；請勿任意移除或關閉防毒軟體。	□是 □否	□符合 □不符合
8	郵件軟體安全管理(A.12.6.2)	1. 關閉郵件軟體中所有資料夾郵件預覽功能。 2. 開啟電子郵件純文字模式。 3. 不開啟或轉寄來路不明的電子郵件及其附件檔案或連結。	□是 □否	□符合 □不符合

第 1 頁，共 3 頁

自評結果，由受稽單位自評勾選。

查核結果，由稽核顧問查核後勾選。

編號	查檢項目	查檢規明	自評結果	查檢結果
9	已完成 google 瀏覽器安全設定 (A.18.1.1)	啟用標準防護模式	▎是 ▎否	符合 不符合
10	是否瞭解禁止於上班時間瀏覽非公務用途網站(A.18.1.1)	上班時間禁止瀏覽非公務用途網站及暴力、色情、賭博、駭客、惡意網站，避免電腦中毒或遭駭客入侵致使內部機敏資料遭竊或資料外洩。	▎是 □否	符合 □不符合
11	ISMS 表單維護	D0006 外部單位聯絡表	▎是 ▎否	適用 不適用
		D0008_資訊資產清單 *表單系統填報	▎是 ▎否	適用 不適用
		D0009 威脅及弱點評估表 *表單系統填報	▎是 ▎否	適用 不適用
		D0010_風險評鑑彙整表	□是 □否	□適用 □不適用
		D0011 風險改善計畫表	□是 □否	□適用 □不適用
		D0013_保密切結書	▎是 ▎否	適用 不適用
		D0014_人員職掌清冊	□是 □否	□適用 □不適用
		D0015 離職人員移交流程表	□是 □否	□適用 □不適用
		D0020 分約商保密切結書	□是 □否	□適用 □不適用
		D0030_稽核結果報告 *表單系統填報	▎是 ▎否	適用 不適用
		D0036_業務流程衝擊分析表 *訂定管理之系統(網站)最大可容忍中斷時間(MTPD)、復原時間目標(RTO)及資料復原時間目標(RPO)	□是 □否	□適用 □不適用
		D0040_資訊資產異動申請表	▎是 ▎否	適用 不適用
		D0042_適用法規清單	□是 □否	□適用 □不適用

編號	查檢項目	查檢規明	自評結果	查檢結果
		D0051_個人電腦設定與軟體安裝查核	▎是 ▎否	適用 不適用
12	PIMS 表單維護	D0002_人員職掌清冊	▎是 ▎否	適用 不適用
		D0005_外部單位聯絡表	□是 □否	□適用 □不適用
		D0011 個人資料檔案清冊	□是 □否	□適用 □不適用
		D0013 個人資料檔案威脅及弱點評估表	□是 □否	□適用 □不適用
		D0016_個人資料提供同意書	▎是 ▎否	適用 不適用
		D0017_隱私權政策聲明	□是 ▎否	□適用 不適用
		D0018 個人資料使用資訊服務申請表	□是 □否	□適用 □不適用
		D0019 個人資料紀錄刪除申請單	□是 ▎否	□適用 不適用
		D0020_個人資料申訴事件紀錄單	▎是 ▎否	適用 不適用
		D0021_個人資料特定目的範圍變更需求同意書	▎是 ▎否	適用 不適用
		D0027_員工個人資料保密切結書	□是 □否	□適用 □不適用
		D0031 稽核結果報告 *表單系統填報(同 ISMS 之 D0030)	□是 □否	□適用 □不適用

註：

一、 表單系統網址：https://system.nutn.edu.tw/formfill

二、 ISMS 表單及 PIMS 表單請由文件管理系統下載，文件管理系統網址：https://system.nutn.edu.tw/doc_doc/

填表人員簽核：_____

查驗人員簽核：_____(稽核組長)

資通安全管理制度內部稽核表	
文件編號：NUTN-ISMS-D038	版次：2.0　　[illegible]：限閱
紀錄編號：	填表日期：　　年　　月

稽核標準說明：

A：相關資通安全管理制度規範已建立，且落實執行

B：相關資通安全管理制度規範未建立，但已實施替代性資安控管措施

C：相關資通安全管理制度規範已建立，但未落實執行

D：相關資通安全管理制度規範未建立，且未實施替代性資安控管措施

E：不適用

稽核項目：教育體系資通安全管理規範本文

條款章節	條文	稽核結果 A	B	C	D	E	稽核事實
陸、	適用性聲明(Statement of Applicability)						
	ISMS 施行單位應依據適用單位等級選擇適用安全等級之控制措施，參考附錄 A 之控制措施，提出「ISMS 適用性聲明」。各等級機關(構)與學校適用之控制措施請參照「附錄 A 資通安全管理規範附件 1 各級教育機構適用控制項對照表」。附錄 A 控制措施之排除僅限適用範圍內資訊系統無需執行，且排除後不影響施行單位提供資通安全能力與責任之控制措施。 同時應參考「資訊系統分級與資安防護基準作業規定」，鑑別適用範圍內資訊系統之安全等級，經資訊系統分級與鑑別後，識別出具有等級為「高」者之資訊系統，應加入 A.14 系統獲取，開發及維護與 A 15 供應者關係等控制領域所有控制措施，並於該控制措施中述明適用之資訊系統。	☐	☐	☐	☐	☐	
＊1.1	**是否界定機關之核心業務，完成資通系統之盤點及分級，且每年至少檢視 1 次分級之妥適性？**	☐	☐	☐	☐	☐	
＊1.3	**是否將全部核心資通系統納入資訊安全管理系統(ISMS)適用範圍？**	☐	☐	☐	☐	☐	

＊為教育部　資通安全實地稽核項目檢核表(適用公務機關)」檢核項目

內部稽核產出文件

D038資通安全管理制度內部稽核(稽核顧問填寫)

個人資料管理制度內部稽核表		
文件編號：NUTN-PIMS-D023	版次：1.0	機密等級：限閱
紀錄編號：112-0001	填表日期：112 年 8 月	

稽核項目 － 規範本文

條款章節	條文				
陸、	適用性聲明(Statement of Applicability)				
	機關建置 ISMS 之教育體系機關(構)與學校可依據前揭所提及之適用等級選擇控制措施，參考附錄 A 之控制措施，提出「ISMS 適用性聲明」。各等級機關(構)與學校適用之控制措施請參照「附錄 A 資訊安全管理規範附件 1 各級教育機構適用控制項對照表」。附錄 A 控制措施之排除僅限適用範圍內資訊系統無需執行，且排除後不影響該機關(構)與學校提供資通安全能力與責任之控制措施。 教育機構如欲取得驗證，所有附錄 A 資訊安全管理規範內之控制項，除標註「建議」者外均應納入，同時應參考「資訊系統分級與資安防護基準作業規定」，盤別適用範圍內資訊系統之安全等級，經資訊系統分級與盤別後，識別出具有等級為「高」者之資訊系統，應加入 A.14 系統獲取、開發及維護與 A.15 供應者關係等控制領域所有控制措施，並於該控制措施中述明適用之資訊系統。	☐	☐	☐	
柒、	建置步驟及需求				
一、	組織全景				
	(一)施行機關(構)或學校應依據相關法令要求，行政院及教育主管機關所下達之重要決定或指導(包括但不限於主管機關之行政指導、重要會議決議事項等)、組織透過相關會議所做成之決議(包括但不限於主管會報、行政會議或校務會議等之決)，針對資通安全或個人資料安全之維護需求進行評估，並據此建立或調整資通安全與個人資料管理範圍與目標。	☐	☐	☐	
	(二)施行機關(構)或學校應依據決議事項確認其關注方(利害相關團體)與要求事項，並留存文件化紀錄。	☐	☐	☐	

內部稽核產出文件

D023個人資料管理制度內部稽核表。(稽核顧問填寫)

資通安全內部稽核

檢視資訊資產清查管理

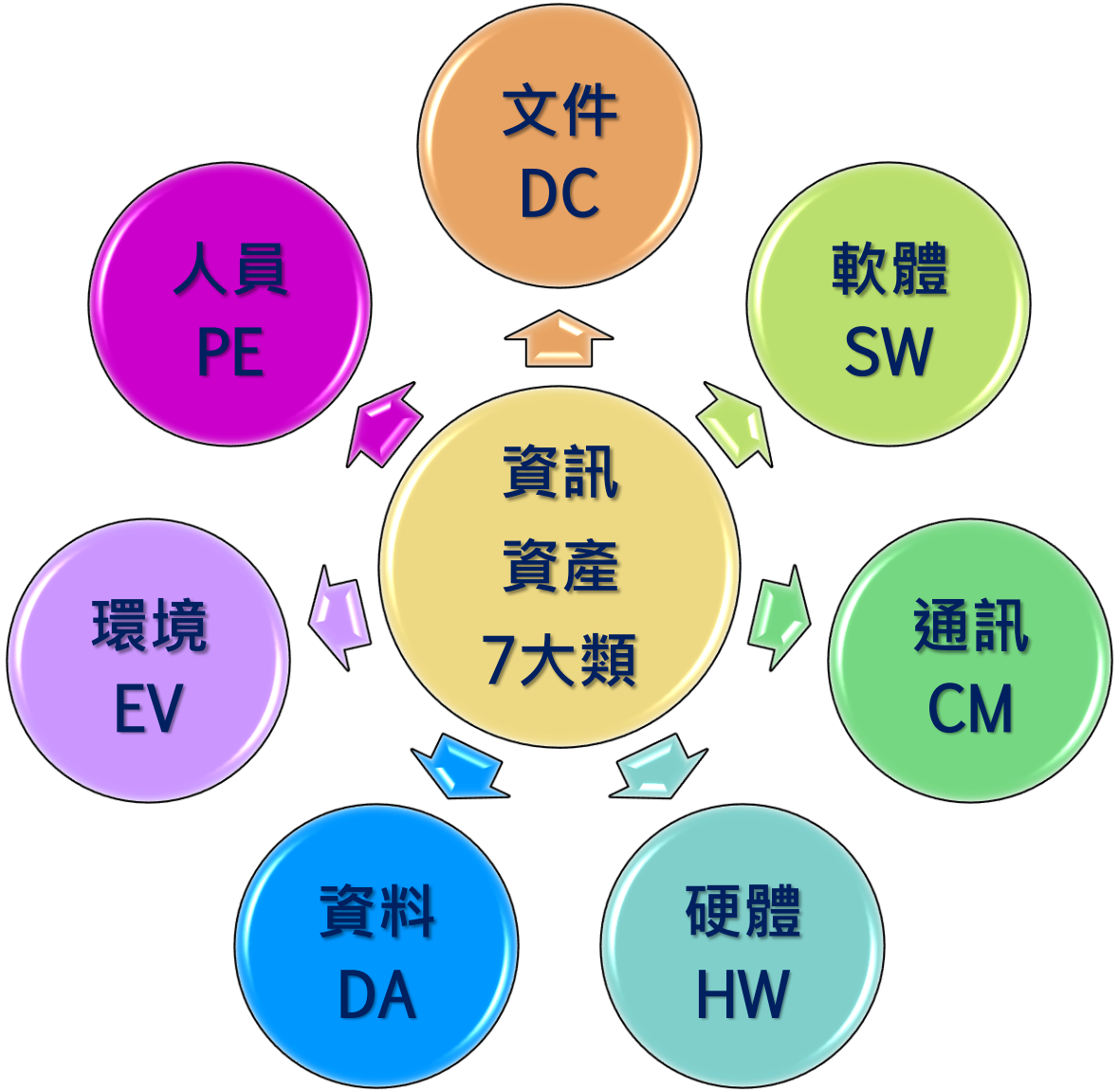
- 了解資訊資產現況
- 適切保護資訊資產
- 達成資通安全要求

保護資訊資產，避免遭受各種威脅及降低可能危害。

資訊資產依其性質不同，分為7類：文件DC、軟體SW、通訊CM、硬體HW、資料DA、環境EV、人員PE。

1. 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。
2. 軟體（Software / SW）：作業系統、應用系統程式、套裝軟體等，包含原始程式碼、應用程式執行碼等。
3. 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。
4. 硬體（Hardware / HW）：主機設備等相關硬體設施。
5. 資料（Data / DA）：儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊。
6. 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。
7. 人員（People / PE）：本校管理維護資通系統人員及其主管、各單位資訊系統負責人(資安及個資業務聯絡人)及其主管及本校資訊服務委外廠商。

資訊資產分類



各單位資訊資產清冊

資產編號	資產類別	資產名稱	資產說明
10200-HW-003	HW	筆記型電腦(行政文書)	ASUS15吋
10200-HW-004	HW	筆記型電腦(行政文書)	ASUS
10200-HW-005	HW	影印機	FUJI
10200-HW-006	HW	印表機	HP
10200-HW-001	HW	個人電腦(行政文書)	ASUS
10200-HW-002	HW	個人電腦(行政文書)	ASUS
10200-HW-007	HW	顯示器(戶外型LED顯示看板系統)	戶外型LED顯示看板
10201-HW-001	HW	個人電腦(系統管理)	廠牌ASUS
10201-HW-002	HW	個人電腦(行政文書)	廠牌ASUS
10201-HW-003	HW	筆記型電腦(行政文書)	廠牌ASUS
10201-EV-001	EV	租賃影印機	廠牌develop ineo+ 360i
10201-EV-002	EV	雷射印表機	廠牌HP M454dw
10201-SW-001	SW	電腦作業系統	Microsoft Windows 10
10201-PE-001	PE	副校長	一級主管
10201-PE-002	PE	計畫專任助理	高等教育深耕計畫專任助理

資訊資產價值鑑別

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

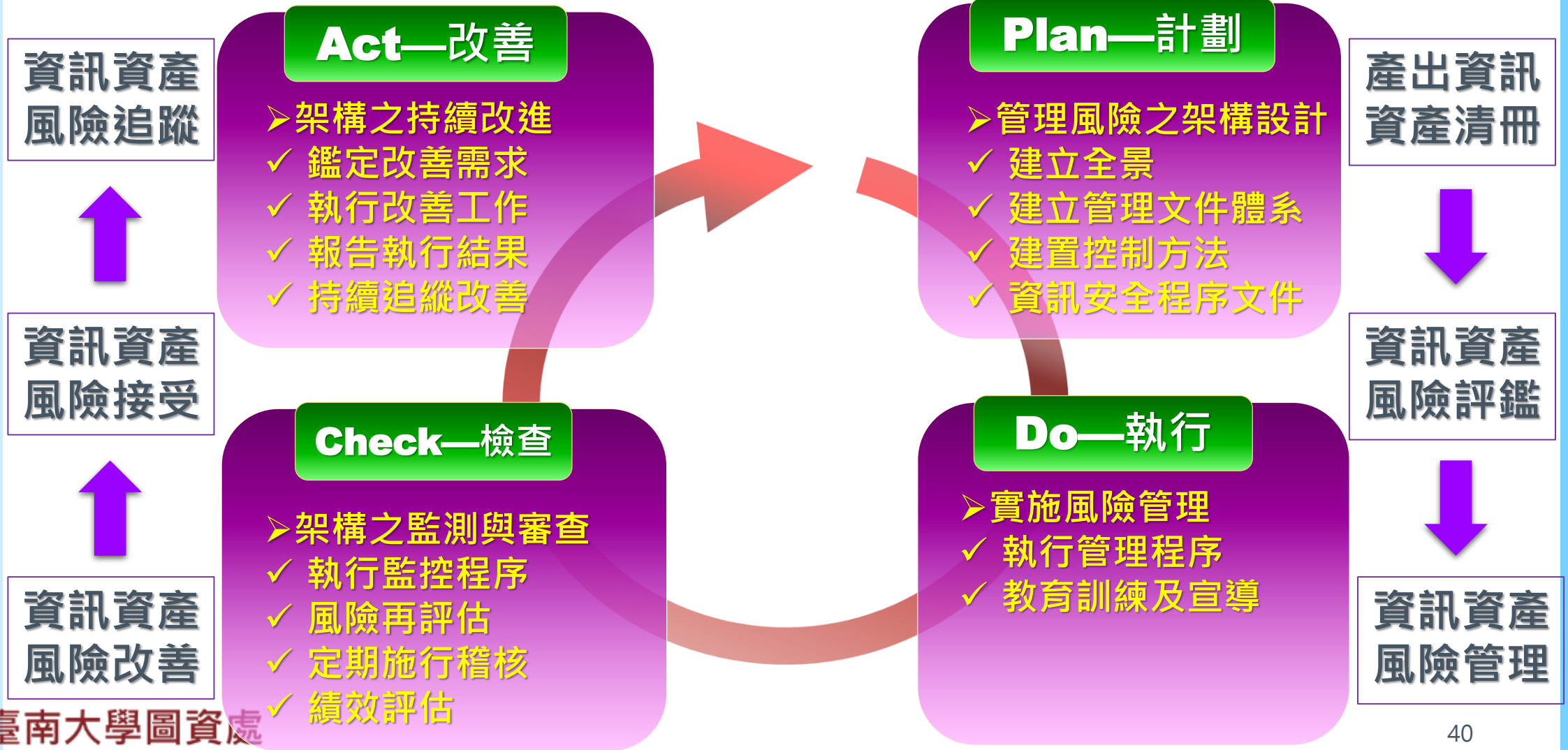
評估標準	數值
該資訊資產可容許失效3工作天以上	1
該資訊資產可容許失效8工作小時以上，3工作天以下	2
該資訊資產僅容許失效4工作小時以上，8工作小時以下	3
該資訊資產僅容許失效4工作小時	4

取3者之**最大值**
為資訊**資產價值**

產出資訊資產清冊，並確認資產價值。

資產編號	資產類別	資產名稱	資產價值
10200-HW-001	HW	個人電腦(行政文書)	3
10200-HW-002	HW	個人電腦(行政文書)	1
10200-HW-003	HW	筆記型電腦(行政文書)	1
10200-HW-004	HW	筆記型電腦(行政文書)	1
10200-HW-005	HW	影印機	1
10200-HW-006	HW	印表機	1
10200-HW-007	HW	顯示器(戶外型LED顯示看板系統)	1
10200-SW-001	SW	校務研究辦公室網站	1
10300-HW-001	HW	個人電腦(系統管理)	2
10300-HW-002	HW	個人電腦(系統管理)	2
10300-HW-003	HW	個人電腦(行政文書)	1
10300-HW-004	HW	個人電腦(行政文書)	1
10300-HW-005	HW	筆記型電腦(行政文書)	1

檢視資訊資產風險管理


Act—改善
➢架構之持續改進
✓ 鑑定改善需求
✓ 執行改善工作
✓ 報告執行結果
✓ 持續追縱改善
Plan—計劃
➢管理風險之架構設計
✓ 建立全景
✓ 建立管理文件體系
✓ 建置控制方法
✓ 資訊安全程序文件
Check—檢查
➢架構之監測與審查
✓ 執行監控程序
✓ 風險再評估
✓ 定期施行稽核
✓ 績效評估
Do—執行
➢實施風險管理
✓ 執行管理程序
✓ 教育訓練及宣導
資訊資產風險追蹤
資訊資產風險接受
資訊資產風險改善
產出資訊資產清冊
資訊資產風險評鑑
資訊資產風險管理

資訊資產風險定義

所謂「風險」乃是當「威脅」利用其相對應「脆弱性」，直接或間接造成組織或政府機關，一個或一群「資訊資產」受到漏失或損害的「可能性」。

風險主要運用兩個因素的結合定義其特性，分別為「可能性」與「衝擊」。

資訊資產風險威脅弱點評估

資產編號	資產類別	資產名稱	資產價值	衝擊值	可能性	風險值
10200-HW-001	HW	個人電腦(行政文書)	3	1	1	3
10200-HW-002	HW	個人電腦(行政文書)	1	1	1	1
10200-HW-003	HW	筆記型電腦(行政文書)	1	1	1	1
10200-HW-004	HW	筆記型電腦(行政文書)	1	1	1	1
10200-HW-005	HW	影印機	1	1	1	1
10200-HW-006	HW	印表機	1	1	1	1
10200-HW-007	HW	顯示器(戶外型LED顯示看板系統)	1	1	1	1
10200-SW-001	SW	校務研究辦公室網站	1	1	1	1
10300-HW-001	HW	個人電腦(系統管理)	2	1	1	2
10300-HW-002	HW	個人電腦(系統管理)	2	2	1	4
10300-HW-003	HW	個人電腦(行政文書)	1	1	1	1
10300-HW-004	HW	個人電腦(行政文書)	1	1	1	1
10300-HW-005	HW	筆記型電腦(行政文書)	1	1	1	1
10300-HW-006	HW	平板	1	1	1	1
10300-HW-007	HW	影印機	2	1	1	2
10300-HW-008	HW	印表機	1	1	1	1
10300-HW-009	HW	監視器	3	1	1	3

資訊資產 D009 威脅及弱點風險發生可能性及衝擊值評估說明

一、 威脅暨弱點評估

參考教育體系資通安全管理規範將各類資訊資產可能面臨之威脅與弱點項目，分別建立「威脅及弱點評估表」。

二、 事件發生機率與影響程度評估

(一) 依風險發生可能性評估表（表 1）評估各事件之可能性：

表 1 風險發生可能性評估表

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

(二) 依衝擊值評估表（表 2）評估各事件之衝擊：

表 2 衝擊值評估表

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

三、 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）

表

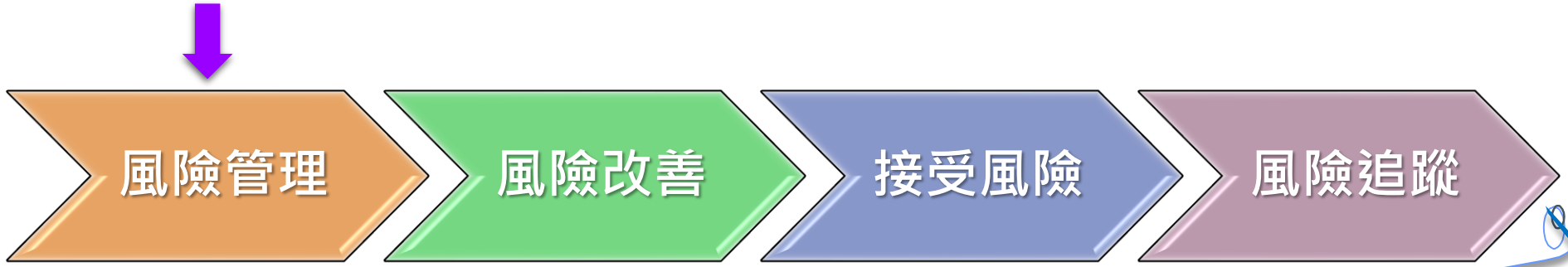
	版次：2.1	機密等級：限閱
	填表日期： 年 月 日	

	風險發生可能性			衝擊值				風險值
	1	2	3	1	2	3	4	

資訊資產風險值

資訊資產風險值的計算

- 評估事件發生可能性(機率)及衝擊值(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)



表單填報系統產「ISMS-D009威脅及弱點評估表」

紀錄編號：	115-0043	填表日期：	2026-05-27
資產編號：	11804-HW-002	資產名稱：	個人電腦(系統管理)
資產類別：	硬體	單位名稱：	圖資處網路服務組
資產價值：	2	填表人：	
資產描述：	公務用個人電腦		

資產類別	威脅	弱點	衝擊值	可能性	風險值
HW	未經授權存取或使用	未確實陪同外部人員或清潔人員執行相關作業	1	1	2
	未經授權存取或使用	缺乏監督與稽核機制	1	1	2
	硬體失效	缺乏硬體耗損控管	1	1	2
	硬體失效	缺乏有效變更控制	1	1	2
	硬體失效	維護服務回應時間過長	1	1	2
	電源供應中斷	不穩定的電壓	1	1	2

資安D009威脅及弱點評估表如有高於「可接受風險值」項目，須產出「D010風險評鑑彙整表」，並彙整相關綜合風險值，產出「D041風險評鑑報告」作為風險管理之依據。

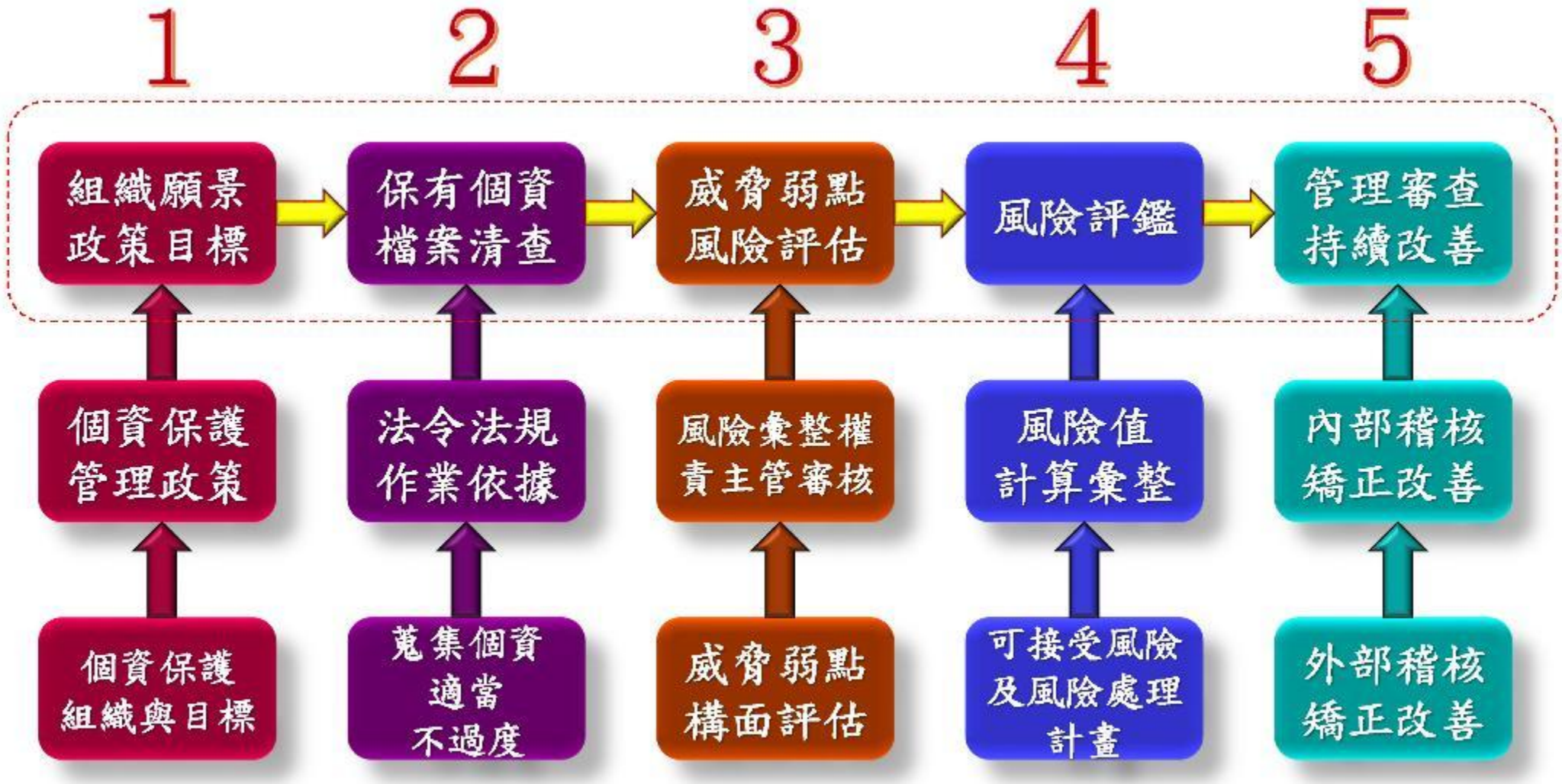
個資管理內部稽核

檢視保有個資檔案清冊

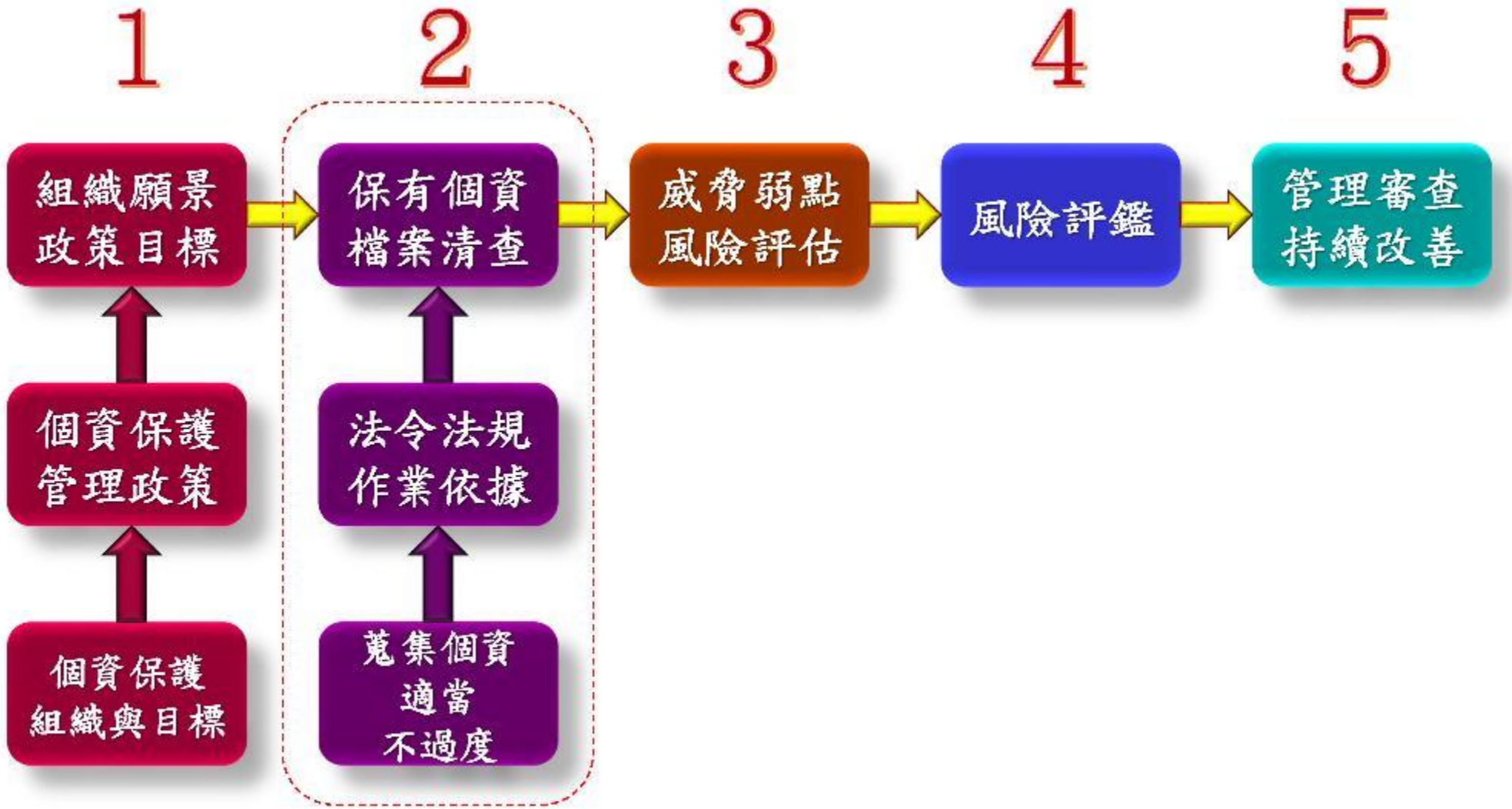
- 了解保有個資檔案現況
- 適切保護保有個資檔案
- 達成個資保護要求

保護保有個資檔案，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

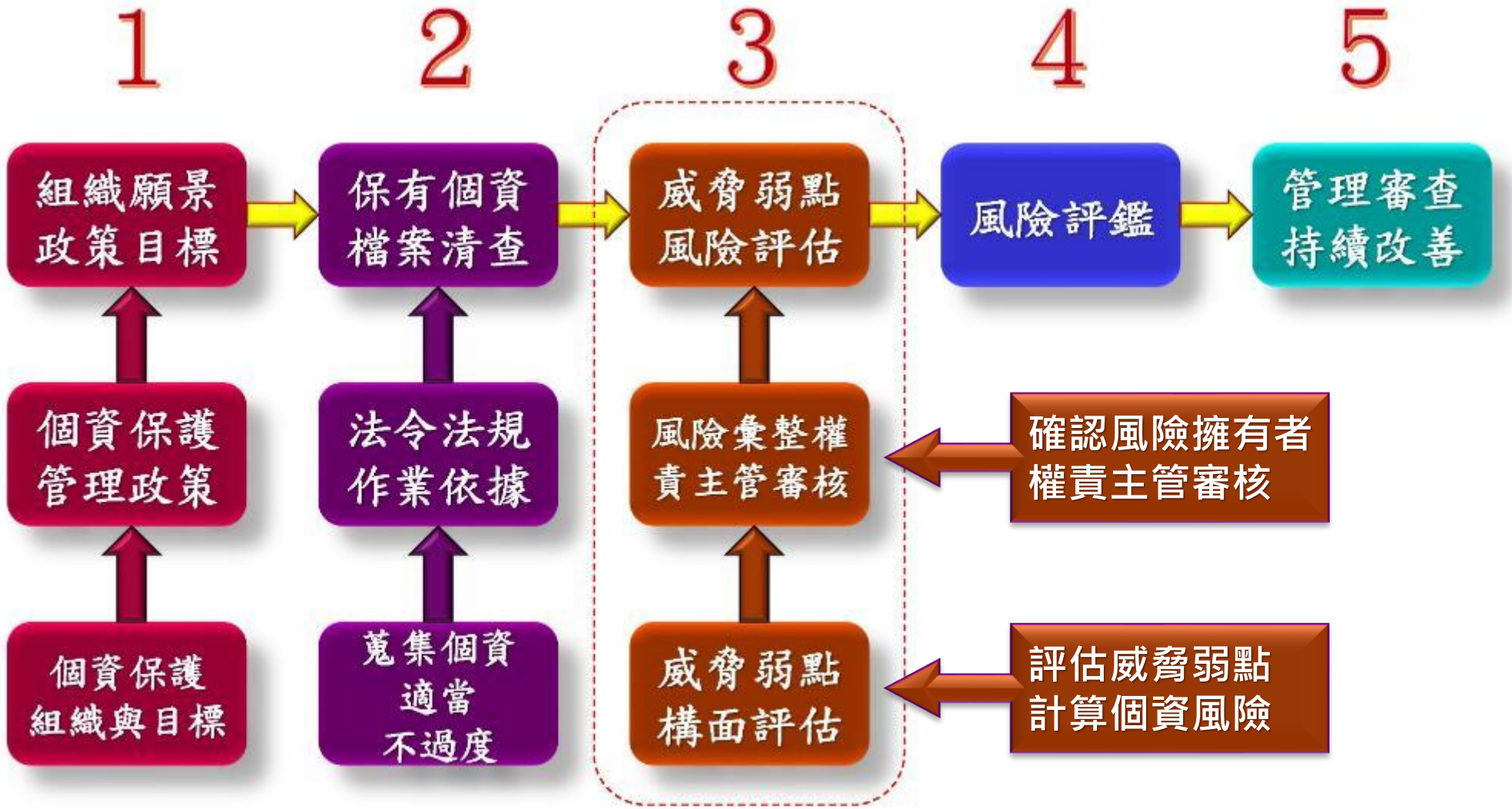
保有個資檔案清查作業流程



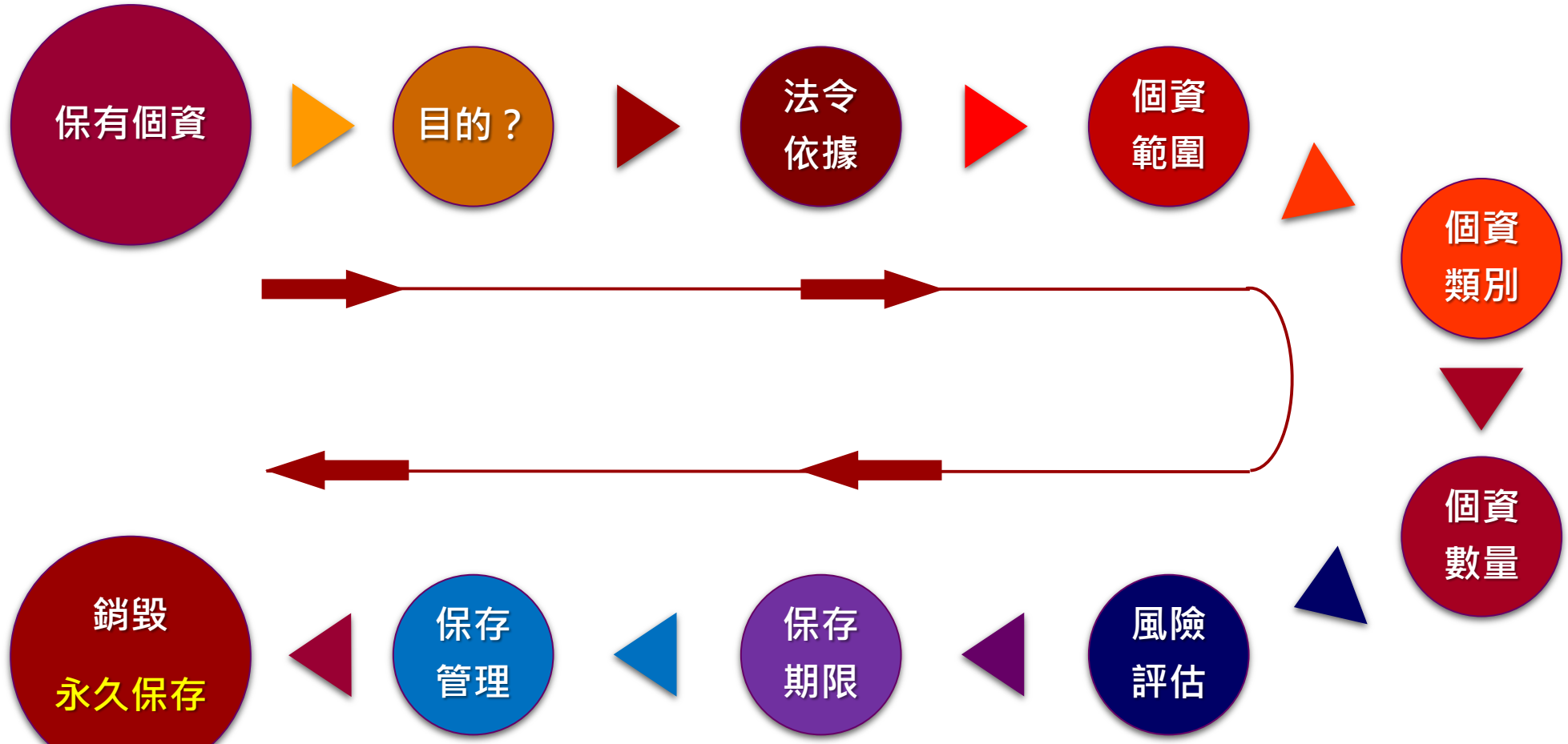
保有個資檔案清查作業流程



保有個資檔案清查作業流程



保有個資檔案清查作業流程



個資檔案稽核檢視重點

蒐集依據必須明確

資料類別與範圍須吻合

資料類別與範圍須吻合

國立臺南大學個人資料檔案清冊

單位：教務處教學業務組　　填報時間：115 年 4 月 23 日

個資資產編號	11102-0001
業務流程名稱	教師授課(超)鐘點作業
個人資料檔案名稱	教師授課(超)鐘點
資料形式	電子檔(資料庫)
法律依據或內部規定	依本校教師授課時數及支給超支鐘點費辦法
特定目的	〇〇二 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）
個人資料類別	C〇〇一 辨識個人者。 C〇〇二 辨識財務者。 C〇九一 資料主體所取得之財貨或服務。 C〇五一 學校紀錄。 C〇六五 工作、差勤紀錄。
個人資料範圍	教師職級,姓名,授課時數,學分數,超支鐘點
有否特種資料？何種特種資料？	否

個資檔案稽核檢視重點

蒐集	來源	當事人
	方式	直接
	單位	教學業務組
處理	方式	人事室及各系所登錄、內部傳遞
	單位	教學業務組、人事室、各系所
利用	期間	無
	地區	無
	單位	無
	方式目的	無
保存	單位	教學業務組、圖資處
	聯絡人	教學業務組之承辦人
	期限	60 年
銷毀	形式	請圖資處於資料庫刪除
	頻率	每年檢查，定期銷毀。
揭露	對象	無
	目的	無
	方式	無
	個資範圍	無
現有控制措施		系統設有帳密權限控管
資產價值		中度
個資數量		保有個資數量 5,001 筆~5 萬筆(含)以內。
重要性		中度

作業流程經手單位均應列出

保存期限須斟酌

碎紙或水銷...

每年銷毀

個資數量依保存期限每年調整

保有個資檔案清查作業系統

國立臺南大學個人資料檔案清冊

單位：教務處教學業務組　　　　填報時間：115年4月23日

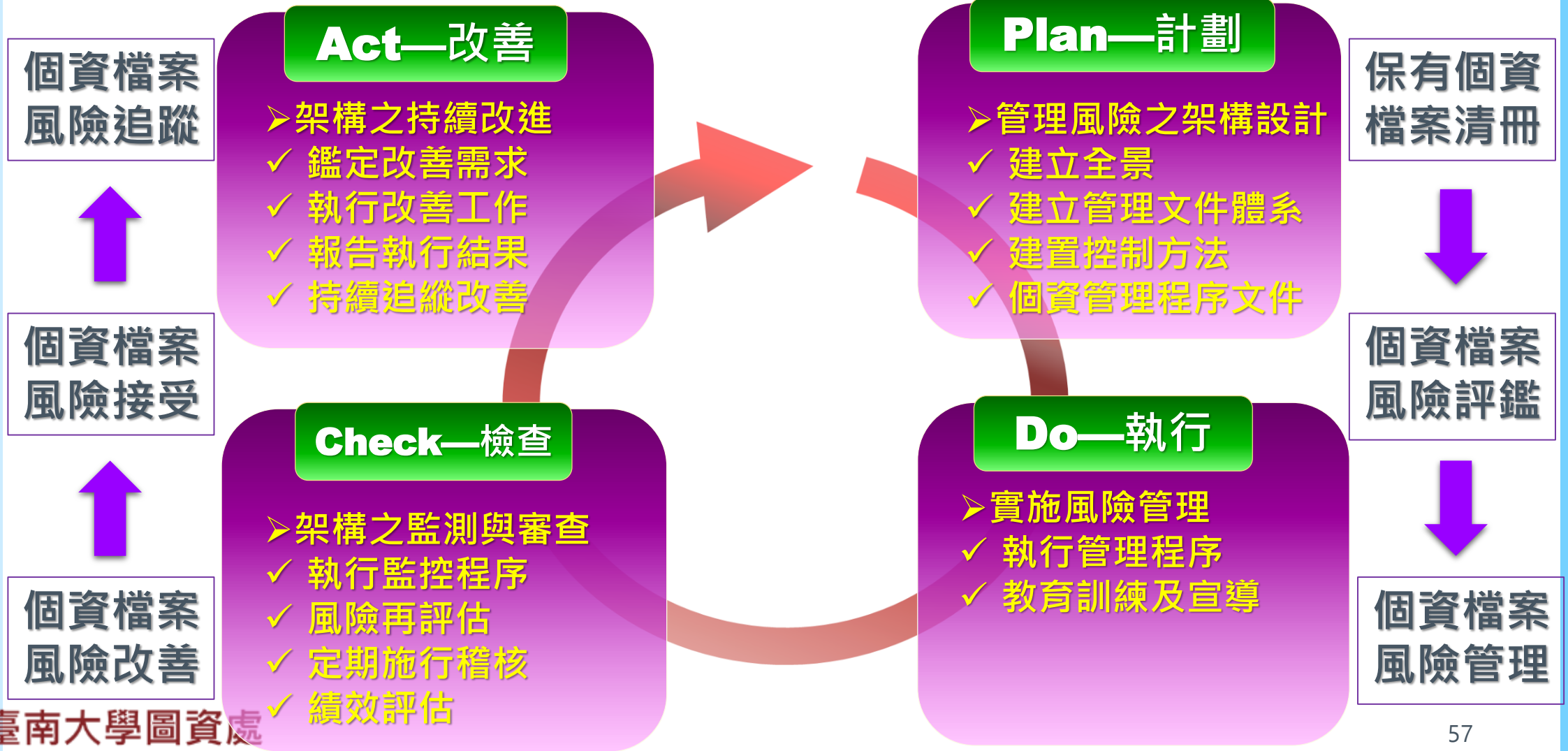
個資資產編號		11102-0001
業務流程名稱		教師授課(超)鐘點作業
個人資料檔案名稱		教師授課(超)鐘點
資料形式		電子檔(資料庫)
法律依據或內部規定		依本校教師授課時數及支給超支鐘點費辦法
特定目的		○○二 人事管理（包含甄選、離職及所屬員工基本資訊、現職、學經歷、考試分發、終身學習訓練進修、考績獎懲、銓審、薪資待遇、差勤、福利措施、褫奪公權、特殊查核或其他人事措施）
個人資料類別		C○○一 辨識個人者。 C○○二 辨識財務者。 C○九一 資料主體所取得之財貨或服務。 C○五一 學校紀錄。 C○六五 工作、差勤紀錄。
個人資料範圍		教師職級,姓名,授課時數,學分數,超支鐘點
有否特種資料？何種特種資料？		否
蒐集	來源	當事人
	方式	直接
	單位	教學業務組
處理	方式	人事室及各系所登錄，內部傳遞
	單位	教學業務組，人事室，各系所
利用	期間	無
	地區	無
	對象	無
	方式用途	無
保存	單位	教學業務組，圖資處
	保管人	教學業務組之承辦人
	期限	60年
銷毀	形式	期滿完成後資料庫刪除
	頻率	每年檢查，定期銷毀。
	對象	無
傳輸	目的	無
	方式	無
	接收範圍	無
現有控制措施		系統設有帳密權限控管
資產價值		中度
個資數量		保有個資數量 5,001 筆~5 萬筆(含)以內。
重要性		中度

國立臺南大學單位個人資料檔案清冊，第1頁，共2頁。

填報完成，產出個人資料檔案清冊。

國立臺
Office of Library and I

個資檔案風險管理PDCA



個人資料檔案風險定義

所謂「風險」乃是當「威脅」利用其相對應「脆弱性」，直接或間接造成組織或政府機關「個資檔案」發生外洩、竊取、不當使用等事故的「可能性」。

風險主要運用兩個因素的結合定義其特性，分別為「可能性」與「衝擊」。

個人資料檔案威脅及弱點評估樣態

國立臺南大學個人資料檔案威脅及弱點評估表—威脅與弱點樣態

106年10月18日(星期三)106年教育體系個人資料管理規範導入工作小組第6次會議決議通過
108年10月2日(星期三)、109年6月3日(星期三)及110年3月23日(星期二)導入工作小組會議決議不予修正
113年11月22日(星期五)資通安全暨個人資料管理規範導入工作小組113年第6次會議決議修正通過

作業階段	威脅	弱點
蒐集	未遵循法令法規	未告知個資法要求應告知事項
蒐集	資料外洩	缺乏安全防護機制
蒐集	未遵循法令法規	個資蒐集不符合免告知要件，且未取得當事人同意或告知要項不足
處理	未遵循法令法規	未主動或依當事人之請求更正或補充個人資料
處理	未遵循法令法規	未提供履行當事人權利機制
處理	未遵循法令法規	逾越特定目的與範圍未告知
處理	未遵循法令法規	個資被竊取、洩漏、竄改未於查明後告知
處理	個人資料被竊取、竄改、毀損、滅失或洩漏	未提供履行當事人權利機制
處理	個人資料被竊取、竄改、毀損、滅失或洩漏	逾越特定目的與範圍未告知
處理	個人資料被竊取、竄改、毀損、滅失或洩漏	個資被竊取、洩漏、竄改未於查明後告知
處理	個人資料被竊取、竄改、毀損、滅失或洩漏	缺乏實體保護
利用	未遵循法令法規	個資被竊取、洩漏、竄改未於查明後告知
利用	個人資料外洩	缺乏安全防護機制
利用	個人隱私資料遭不當公開	資料揭露未有審查機制
利用	使用錯誤的資料	未主動或依當事人之請求更正或補充個人資料
傳送	使用錯誤的資料	傳輸過程未有適當之保護
刪除/銷毀	誤刪除/銷毀資料	資料銷毀處理程序不當或不足

個人資料 D013 威脅及弱點風險發生可能性及衝擊值評估說明

一、 威脅及弱點影響分析

個人資料檔案之威脅及弱點評估依據「個人資料檔案威脅及弱點評估表」進行風險分析，本表係參酌「個人資料保護法」及相關規範內容與控管設計，以利評估組織在面臨個資風險時可能產生之影響程度。

二、 風險發生機率與影響程度評估

(一) 依風險發生可能性評估表（表 1）評估各事件之可能性：

表 1 風險發生可能性評估表

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

(二) 依衝擊值評估表（表 2）評估各事件之衝擊，並取其最大值：

表 2 衝擊值評估表

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）

三、 風險值的計算

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。

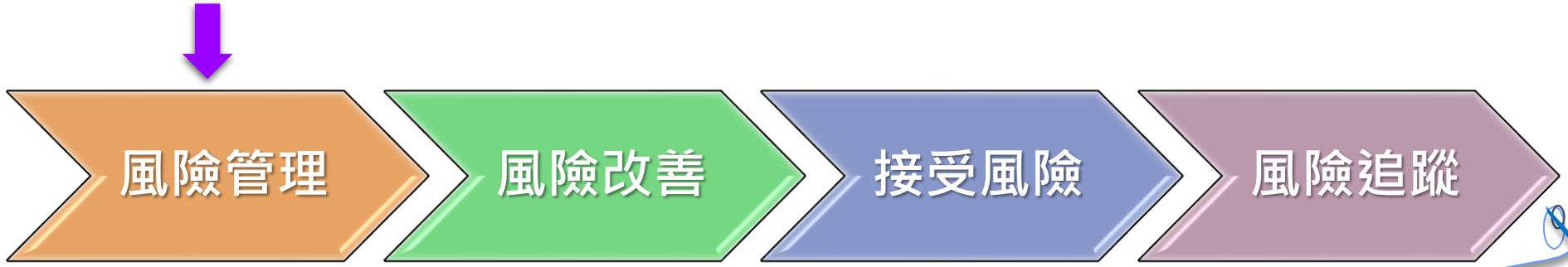
風險值=個資資產價值×衝擊值(MAX)×可能性值。

威脅	弱點	衝擊值	可能性	風險值
不熟悉法令	教育訓練不	1	1	2
個人資料被	缺乏稽核與	1	1	2
個人資料被	個資保護機	1	1	2
個人資料被	個資蒐集	1	1	2
個人資料被	人員離職或	1	1	2
個人隱私資	教育訓練不	1	1	2
個人隱私資	個資保護機	1	1	2
個人權益受	未提供當事	1	1	2
委託商違約	機關未對代	1	1	2
未遵循法令	未告知個資	1	1	2
未遵循法令	蒐集個資特	1	1	2
個資錯誤與	個資蒐集時	1	1	2

個人資料檔案風險值

個人資料檔案風險值的計算

- 評估事件發生可能性(機率)及衝擊值(影響程度)後，計算出風險值。
- **風險值** = (個資檔案價值 × 可能性評估值 × 衝擊值)



填報完成產出D013個人資料檔案威脅及弱點評估表

個資資產編號	流程名稱	個資檔案名稱	資料形式	資產價值	填表人	作業階段	威脅	弱點	衝擊值	可能性	風險值
103000002	教師升等審查	教師升等審查之申請人	電子檔(資料庫),紙	2		全階段	不熟悉法令法	教育訓練不足	1	1	2
103000002	教師升等審查	教師升等審查之申請人	電子檔(資料庫),紙	2		全階段	個人資料被竊	缺乏稽核監督	1	1	2
103000002	教師升等審查	教師升等審查之申請人	電子檔(資料庫),紙	2		全階段	個人資料被竊	個資保護機制	1	1	2
103000002	教師升等審查	教師升等審查之申請人	電子檔(資料庫),紙	2		全階段	個人資料被竊	個資蒐集、處	1	1	2
103000002	教師升等審查	教師升等審查之申請人	電子檔(資料庫),紙	2		全階段	個人資料被竊	人員離職或職	1	1	2
103000002	教師升等審查	教師升等審查之申請人	電子檔(資料庫),紙	2		全階段	個人隱私資料	教育訓練不足	1	1	2
103000002	教師升等審查	教師升等審查之申請人	電子檔(資料庫),紙	2		全階段	個人隱私資料	個資保護機制	1	1	2
103000002	教師升等審查	教師升等審查之申請人	電子檔(資料庫),紙	2		全階段	個人權益受損	未提供當事人	1	1	2
103000002	教師升等審查	教師升等審查之申請人	電子檔(資料庫),紙	2		全階段	委託商違法蒐	機關未對代表	1	1	2
103000002	教師升等審查	教師升等審查之申請人	電子檔(資料庫),紙	2		蒐集	未遵循法令法	未告知個資法	1	1	2
103000002	教師升等審查	教師升等審查之申請人	電子檔(資料庫),紙	2		蒐集	未遵循法令法	蒐集個資缺乏	1	1	2
103000002	教師升等審查	教師升等審查之申請人	電子檔(資料庫),紙	2		蒐集	個資錯誤影響	個資蒐集時無	1	1	2
103000002	教師升等審查	教師升等審查之申請人	電子檔(資料庫),紙	2		蒐集	過度蒐集面臨	個資蒐集超出	1	1	2
103000002	教師升等審查	教師升等審查之申請人	電子檔(資料庫),紙	2		蒐集	面臨當事人之	個資蒐集不符	1	1	2
103000002	教師升等審查	教師升等審查之申請人	電子檔(資料庫),紙	2		處理	未遵循法令法	未主動或依當	1	1	2

教育部資通安全實地稽核各單位應辦事項

- **資產**：清查正確性、完整性(物聯網(IoT)設備)
- **風險**：風險評鑑完整性、改善有效性
- **作為**：安全維護作為及應辦事項(物聯網(IoT)設備)
- **委外**：委外資安要求管理及佐證資料
- **訓練**：全員資安通識教育訓練

Q & A

THANK FOR YOUR ATTENTION