TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

國立臺南大學

111年資訊安全暨個人資料管理規範導入顧問輔導服務案
課程名稱：資通安全與個資保護管理實務

授課日期：111年8月17日
授課講師：德欣寰宇科技股份有限公司 資安顧問 吳懿仁

簡報大綱

一	個資保護管理實務
二	資通安全管理實務
三	課程結論

個資保護管理實務

個資保護管理系統(Personal Information Management System, PIMS)

- 規範組織蒐集、處理及利用個人資訊時的保護機制。透過導入標準提供的基礎架構，建立符合規畫—執行—稽核—處理（Plan–Do–Check–Act, PDCA）精神的系統化管理制度。

個資保護管理實務

管理政策 | 適用聲明 | 推動組織 | 文件管制

人員管理 | 教育訓練 | 矯正改善 | 內部稽核

個人資料盤點 | 個人資料風險評鑑

蒐集/處理/利用 | 儲存/銷毀

委商管理 | 當事人權益 | 個資事故

本校PIMS制度文件清單-1~3階

政策　程序書　作業說明書

序號	階層	文件編號及名稱
1	一階	A001個人資料保護管理政策
2	二階	B001個人資料保護組織程序書
3		B002個人資料文件管理程序書
4		B003個人資料檔案風險評鑑與管理程序書
5		B004個人資料蒐集、處理、利用與安全管理程序書
6		B005個人資料當事人之權利聲明
7		B006個人資料稽核作業程序書
8		B007個人資料保護矯正管理程序書
9		B008個人資料檔案安全維護計畫
10		B009業務終止後個人資料處理方法
11	三階	C001個人資料安全控管作業說明書
12		C002個人資料保護緊急應變處理作業說明書

本校PIMS制度文件清單-4階

表單或紀錄

序號	編號及名稱
1	D001個人資料保護組織成員表
2	D002人員職掌清冊
3	D003外來文件一覽表
4	D004適用法規清單
5	D005外部單位聯絡表
6	D006目標達成計畫與量測表
7	D007個人資料保護管理審查會議紀錄
8	D008文件調閱申請單
9	D009文件修訂建議表
10	D010個人資料管理制度文件列表
11	D011個人資料檔案清冊
12	D012個人資料檔案威脅暨弱點分析評分構面表
13	D013個人資料檔案威脅及弱點評估表
14	D014個人資料檔案風險評鑑彙整表

序號	編號及名稱
15	D015個人資料檔案風險處理計畫
16	D016個人資料提供同意書
17	D017私權政策聲明
18	D018個人資料使用資訊服務申請表
19	D019個人資料紀錄銷毀申請單
20	D020個人資料申訴事件紀錄單
21	D021個人資料特定目的範圍變更需求同意書
22	D022個人資料管理制度內部稽核計畫
23	D023個人資料管理制度內部稽核表
24	D024個人資料管理制度有效性量測表
25	D025個人資料管理制度內部稽核報告

序號	編號及名稱
26	D026個人資料管理制度矯正處理單
27	D027員工個人資料保密切結書
28	D028合約商保密切結書
29	D029資訊服務申請表
30	D030帳號清查紀錄表
31	D031帳號清查結果報告
32	D032校務系統密碼變更申請表
33	D033個人資料侵害事故通報與紀錄表
34	D034個人資料管理會議紀錄
35	D035校務資訊系統資料整合應用申請表
36	D036教育訓練簽到表
37	D037個人資料侵害事故應變演練計畫

個人資料保護管理政策

一. 政策目的-最高指導原則及管理目標。

二. 個人資料之蒐集與處理-不過度蒐集與處理，符合特定目的。

三. 個人資料之利用及國際傳遞-特定目的內利用、特定目的外利用之同意、國際傳輸規定。

四. 個人資料之調閱與異動-當事人權益。

五. 個人資料之例外應用-當事人權益外之請求，例如司法、警政、公權、緊急救助。

六. 個人資料之保護-個資保護作為集大成並濃縮內容。

七. 利害關係人之參與及期許-內外部關注方議題回饋、定期執行管理審查。

八. 施行-因應時勢變遷或法令修正等，予以適當修訂，個資推動組織審核後公告，修正時亦同。

個人資料保護組織程序書

一. 組織全景識別與建立-識別利害關係人要求與期望，定期審查。

二. 推動組織建立-個資長(DPO)、個資委員會組成、幕僚單位成立。

三. 各推動組織權責-工作、任務、責任。

四. 內外部關注方聯繫-業務主管機關、法規主管機關、警消、委外廠商聯繫清單。

五. 個資保護目標達成-可預期、可量化、符合目標。

六. 資源提供-個人資料保護所需資源提供。

七. 組織能力-組織人員能力要求、特殊教育訓練、培訓證明。

八. 個資保護宣導、持續改善。

九. 管理審查-定期/非定期開會、必要討論議題。

十. 法規遵循-識別適用之法律。

個人資料保護組織程序書

一. 組織全景識別與建立-識別利害關係人要求與期望，定期審查。

二. 推動組織建立-個資長(DPO)、個資委員會組成、幕僚單位成立。

三. 各推動組織權責-工作、任務、責任。

四. 內外部關注方聯繫-業務主管機關、法規主管機關、警消、委外廠商聯繫清單。

五. 個資保護目標達成-可預期、可量化、符合目標。

六. 資源提供-個人資料保護所需資源提供。

七. 組織能力-組織人員能力要求、特殊教育訓練、培訓證明。

八. 個資保護宣導、持續改善。

九. 管理審查-定期/非定期開會、必要討論議題。

十. 法規遵循-識別適用之法律。

個人資料文件管理程序書

一. 文件架構-管理制度文件架構定義。
二. 審查權責-文件修訂權責。
三. 文件管制-專人保護、調閱申請、注意文件版本、文件版本控制。
四. 表單或記錄管制-PIMS執行過程紀錄、系統記錄、調閱申請、專人保護。
五. 文件製作及修訂-文件修訂流程、修訂紀錄記載。
六. 文件發行-發行流程、如何讓同仁取得與知悉最新版本文件與表單。
七. 文件保管-專人保護、文件列表。
八. 文件廢止-文件修訂流程，如何讓同仁知悉文件不在適用於組織。
九. 文件版控、編碼、版面-版本原則、紀錄編碼原則、文件封面格式。

個人資料檔案風險評鑑與管理程序書

一. 分類-電子、紙本。

二. 盤點-定期/非定期執行，誰來執行。

三. 隱私衝擊分析-衝擊高低/資產價值對應個人資料範圍。(方法論)

四. 風險評鑑-定期/非定期執行，誰來執行。

五. 風險識別-威脅/脆弱影響。(方法論)

六. 風險值計算-(方法論)

七. 風險評鑑報告產出-誰來彙整，誰來報告。

八. 風險評鑑管理-可接受風險值/風險處理/風險改善追蹤。

九. 威脅弱點-檢討是否適用組織。

個人資料蒐集、處理、利用與安全管理程序書

一. 個人資料蒐集-告知事項、個人資料提供同意書、隱私權政策聲明、適當不過度。

二. 個人資料處理

三. 個人資料利用

四. 個人資料傳輸

五. 個人資料儲存

六. 個人資料銷毀

七. 當事人申訴

八. 委外管理

九. 向第三方揭露個資

個人資料當事人之權利聲明

一. 個資聯絡窗口-誰來擔任窗口協助當事人行使權利。

二. 當事人可行使權利事項-查詢、閱覽、複本、補充、更正、停止蒐集處理利用、刪除。

三. 當事人行使權利方式-申請表單、流程、拒絕情形。

四. 個資特定目的與範圍變更-申請表單、流程

個人資料當事人之權利聲明

一. 個資聯絡窗口-誰來擔任窗口協助當事人行使權利。

二. 當事人可行使權利事項-查詢、閱覽、複本、補充、更正、停止蒐集處理利用、刪除。

三. 當事人行使權利方式-申請表單、流程、拒絕情形。

四. 個資特定目的與範圍變更-申請表單、流程。

個人資料稽核作業程序書

一. 稽核團隊-組成、能力、資格。

二. 稽核活動-定期/非定期。

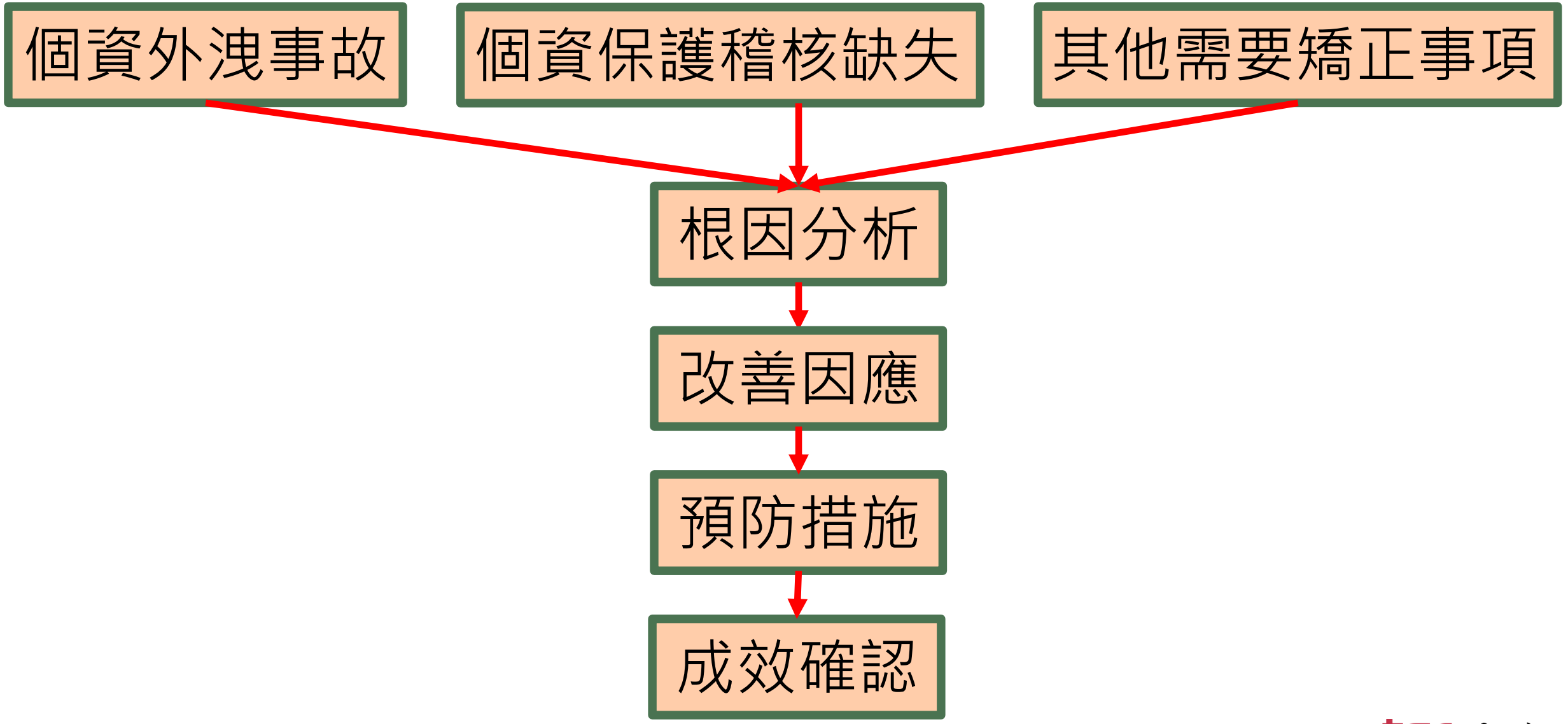
三. 稽核計畫-擬定稽核計畫、計畫核准層級。

四. 符合程度判定標準-符合/不符合/不適用。

五. 稽核報告-稽核底稿、稽核發現彙整、報告核准層級。

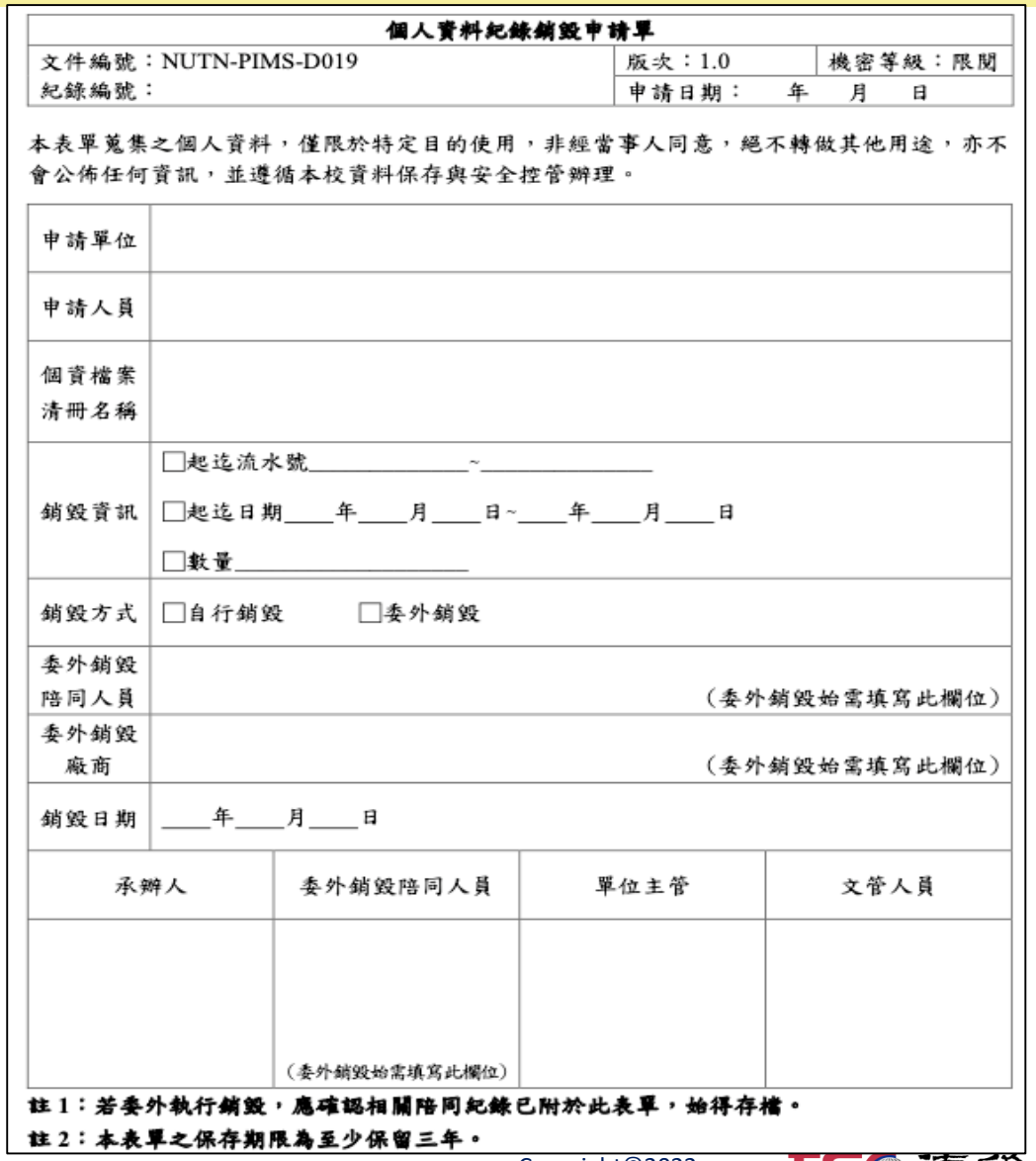
六. 稽核結果後續追蹤。

個人資料保護矯正管理程序書



業務終止後個人資料處理方法

- 儲存應注意保存年限，不必要的複本盡量降低產生之數量與份數。
- 紙本資料儲存應注意環境與安全問題，例如：溫濕度、消防設備、門禁管制、上櫃上鎖、進出紀錄等；電子資料儲存應注意設備安全與存取控制問題，例如：設備資安漏洞更新、資料存取權限、加密儲存等。
- 超過保存年限或業務不需要再使用之個人資料應規劃銷毀或刪除作業。
- 紙本資料可造冊確認銷毀之數量及範圍，並留存相關銷毀紀錄，例如：拍照、錄影、銷毀人員及監銷人員確認；電子資料應留存儲存媒體銷毀紀錄、電子檔案刪除過程與結果截圖。



個人資料紀錄銷毀申請單

文件編號：NUTN-PIMS-D019	版次：1.0	機密等級：限閱
紀錄編號：	申請日期：　年　月　日	

本表單蒐集之個人資料，僅限於特定目的使用，非經當事人同意，絕不轉做其他用途，亦不會公佈任何資訊，並遵循本校資料保存與安全控管辦理。

申請單位	
申請人員	
個資檔案清冊名稱	
銷毀資訊	□起迄流水號＿＿＿＿＿＿＿＿~＿＿＿＿＿＿＿＿ □起迄日期＿＿＿年＿＿＿月＿＿＿日~＿＿＿年＿＿＿月＿＿＿日 □數量＿＿＿＿＿＿＿＿＿＿
銷毀方式	□自行銷毀　□委外銷毀
委外銷毀陪同人員	（委外銷毀始需填寫此欄位）
委外銷毀廠商	（委外銷毀始需填寫此欄位）
銷毀日期	＿＿＿年＿＿＿月＿＿＿日

承辦人	委外銷毀陪同人員	單位主管	文管人員
	（委外銷毀始需填寫此欄位）		

註 1：若委外執行銷毀，應確認相關陪同紀錄已附於此表單，始得存檔。

註 2：本表單之保存期限為至少保留三年。

個人資料保護緊急應變處理作業說明書

一. 個資事故通報及受理程序。
二. 個資事故應變流程。
三. 判斷是否為個資事故及影響程度及範圍。
四. 記錄個資事故過程紀錄。
五. 應變措施及演練作業。
六. 確認狀況排除。
七. 檢討及改善。

資通安全管理實務

資訊安全管理系統(Information Security Management System,ISMS)

- 透過制度化的管控措施，降低組織面對的威脅和弱點，以風險管理的概念保護組織資訊資產的機密性、完整性及可用性。

資通安全管理實務

管理政策 | 適用聲明 | 推動組織 | 文件管制

人員管理 | 教育訓練 | 矯正改善 | 內部稽核

資訊資產盤點 | 資訊資產風險評鑑

實體安全 | 網路安全 | 系統安全 | 存取安全

委商安全 | 業務永續 | 資安事故

本校ISMS制度文件清單-1~2階/相對應表單

文件編號	文件名稱	相關表單編號	相關表單名稱
A001	資通安全政策	D012	適用性聲明書
		D042	適用法規清單
B001	文件管理程序書	D001	文件修訂建議表
		D002	資通安全管理文件列表
		D003	外來文件一覽表
		D004	文件調閱申請單
B002	資通安全組織程序書	D003	外來文件一覽表
		D005	資通安全組織成員表
		D006	外部單位聯絡表
		D007	ISMS有效性量測表
		D028	資通安全管理審查會議記錄
		D043	資通安全會議記錄
		D053	目標達成計畫與量測表
B003	資訊資產管理程序書	D008	資訊資產清單
		D040	資訊資產異動申請表
B004	風險評鑑與管理程序書	D009	威脅及弱點評估表
		D010	風險評鑑彙整表
		D011	風險改善計畫表
		D012	適用性聲明書
		D028	資通安全管理審查會議記錄
		D041	風險評鑑報告
B005	人員安全與教育訓練程序書	D013	保密切結書
		D014	人員職掌清冊
		D015	離職人員移交流程表
		D016	教育訓練簽到表
		D025	資訊服務申請表

文件編號	文件名稱	相關表單編號	相關表單名稱
B006	實體安全管理程序書	D008	資訊資產清單
		D017	人員進出機房紀錄表
		D018	設備進出紀錄表
		D019	異常事件紀錄表
		D020	合約商保密切結書
		D049	機電與消防設備檢查紀錄表
B007	通信與作業管理程序書	D019	異常事件紀錄表
		D021	系統與網路檢查紀錄表
		D022	網路安全設備進出規則申請表
		D023	網路安全設備設定備份確認表
		D026	校務系統密碼變更申請表
		D033	弱點處理報告單
B008	資訊作業委外安全管理程序書	D017	人員進出機房紀錄表
		D020	合約商保密切結書
		D025	資訊服務申請表
B009	存取控制管理程序書	D025	資訊服務申請表
		D029	帳號清查紀錄表
		D030	帳號清查結果報告
		D045	設備密碼授權紀錄單
		D051	個人電腦設定與軟體安裝查核表
		D052	伺服器及網路設備系統設定查核表

文件編號	文件名稱	相關表單編號	相關表單名稱
B010	系統開發與維護程序書	D031	系統需求申請表
		D032	系統測試與驗收報告
		D034	系統上線及緊急復原計畫表
		D047	系統程式碼清冊
		D048	系統資料庫說明
		D050	軟體安裝及異動記錄單
B011	資通安全事件管理程序書	D035	資通安全事件報告單
B012	業務永續運作管理程序書	D036	業務流程衝擊分析表
		D037	業務永續運作計畫演練活動紀錄
B013	資通安全稽核作業程序書	D038	資通安全管理制度內部稽核表
		D039	矯正處理單
		D027	資通安全內部稽核報告
B014	矯正管理程序書	D039	矯正處理單

***備註：表單紀錄使用時機有定期跟非定期，使用時可透過電子檔程序書搜尋功能找到表單所屬之程序書，了解使用或更新時機。**

本校ISMS制度文件清單-3階/相對應表單

文件編號	文件名稱	相關表單編號	相關表單名稱
C001	人員資通安全守則	D025	資訊服務申請表
		D013	保密切結書
C002	一般使用者資通安全指南		
C003	業務永續運作計畫	D037	業務永續運作計畫演練活動紀錄
C004	關鍵業務障礙偵測與復原作業程序	D035	資通安全事件報告單
		D006	外部單位聯絡表
C005	資通安全管理制度內部稽核計畫	D038	資通安全管理制度內部稽核表
		D039	矯正處理單
C006	業務承辦人員資通安全指南		
C007	資訊資產異動作業說明書	D008	資訊資產清單
		D040	資訊資產異動申請表
C008	日常操作管理作業說明書		
C009	機房進出管理作業說明書		

4 密碼使用要點

4.1 應保護密碼，維持密碼的機密性，使用者應至少每 6 個月更換密碼一次，並禁止重複使用相同的密碼。

4.2 應避免將密碼記錄在書面上，或張貼於個人電腦、螢幕或其它容易洩漏秘密之場所。

4.3 當有跡象顯示系統及密碼可能遭破解時，應立即更改密碼。

4.4 密碼的長度最少應有 8 位長度，且應符合密碼設置原則。

4.5 密碼設置原則，應儘量避免使用如下等易猜測或公開資訊為設定：

4.5.1 年、月、日等時間資訊。

4.5.2 個人姓名、出生日或身分證字號。

4.5.3 機關、單位名稱、識別代碼或是其他相關事項。

4.5.4 電腦主機名稱、作業系統名稱、或電腦上使用者的名稱。

4.5.5 電話號碼。

4.5.6 使用者識別碼、使用者姓名、群組名稱或是其他系統識別碼。

4.5.7 重複出現兩個字以上的識別字碼。

4.5.8 以全部數字或是全部字母組成密碼。

4.5.9 英文或是其他外文的常用字彙。

4.5.10 常用專有名詞。

4.5.11 地方名稱。

取自 人員資通安全守則V1.4 有關密碼設置使用要點

3階文件內容屬細部作業操作流程，說明如何實作完成2階文件之要求，可以思考想成細部SOP、補充實際作業說明或法規之施行細則。

委外廠商作業資通安全要求

「資訊作業委外安全管理程序書」

- 委外人員執行業務時，應遵守政府及本校資通安全與個人資料保護相關法令規定，若違反時（如電腦洩密、盜取個人資料...等），依契約及相關法令辦理。
- 委外廠商需提供完整之工作說明書或專案管理計畫書，內容包含專案目標、範圍、時程、組織、管理機制、服務水準、變更要求等。
- 委外廠商專案計畫主持人或重要成員（如專案經理、專案工程師、專案服務人員等）非經本校同意，不得更換。
- 重要系統之委外廠商應訂定緊急應變與回復標準程序，以確保本校資訊業務之持續運作。

資通安全管理法

第九條

- 公務機關或特定非公務機關，於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

資通安全管理法施行細則-第四條（1/9）

一.受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。

➢說明：

第一款所稱第三方，係指通過我國標準法主管機關委託機構認證之機構，其驗證標準可為國際、國家或團體標準。

注意：

通過第三方驗證的認證範圍需為業務之相關程序、人員、設備及環境。

資通安全管理法FAQ-完善之資通安全管理措施

6.4. 何謂完善的資通安全管理措施?	除遵行機關自定之資通安全防護及控制措施所要求之項目外，機關得依委託之項目個案判斷， 並可於採購、委外招標時，納入相關需求並列為評分項目。 例如: 1.應用系統委外開發:可考慮廠商的開發環境是否安全，程式的測試資料是否合宜等。 2.SOC 監控委外:可考量蒐集的資料是否做好相當之管理及防護。

第三方驗證-主管機關委託機構認證之機構

- 財團法人全國認證基金會https://www.taftw.org.tw/

查詢認證名錄（1/3）

查詢認證名錄（2/3）

查詢認證名錄（3/3）

關於TAF | 焦點訊息 | 認證申請 | 認證名錄 | 合作關係 | 文件專區 | 聯繫我們

查詢 重設

➤ 前往驗證機構客戶名錄

認證編號	領域	驗證機構名稱	地址	電話	傳真	聯絡人
MS001	管理系統	台灣檢驗科技股份有限公司	新北市五股區(新北產業園區)五工路136之1號	02-22993279		李仁燮
MS004	管理系統	香港商英國標準協會太平洋有限公司台灣分公司	台北市內湖區基湖路37號2樓	02-26560333#100		蒲樹盛
MS012	管理系統	艾法諾國際股份有限公司	桃園市桃園區中平路102號20樓之2	03-2208080		Myriam Augereau-Landais
MS013	管理系統	環奧國際驗證有限公司	臺北市信義區松德路161號12樓之2	02-2726-0262		謝淑櫻
MS014	管理系統	香港商漢德技術監督服務亞太有限公司台灣分公司	台北市大安區敦化南路二段333號9樓A1室	02-23780578		任駿

回頂部

共 5 筆資料 ,第 1/1 頁, 每頁顯示 10

1

tsc 海航 TSC CAPITAL GROUP The Bridge to the Asia Pacific Region

資通安全管理法施行細則-第四條（2/9）

二.受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

➢說明：

為確保受託者辦理受託業務之程序及環境具安全性，並得妥善執行受託業務，爰為第一款及第二款規定。

注意：證照是否有維持其有效性。

資通安全專業證照清單

資通安全專業證照清單

證機構(單位)	管理類(18)	技術類(92)
經 TAF 或國際認證機構認可之資安相關管理系統驗證機構[1]	1.ISO/IEC 27001:2013 Information Security Management System(ISMS) Auditor/ Lead Auditor 2.ISO 22301 Business Continuity Management System(BCMS) Auditor/Lead Auditor 3.ISO/IEC 29100 Lead Privacy Implementer Information technology — Security techniques — Privacy framework (111 年 3 月 15 日停止認定) 4.ISO/IEC 27701:2019 Privacy Information Management System Lead Auditor Lead Auditor Lead Auditor 相關證照應具有效性，除提出證照外，尚須提供當年度至少 2 次實際參與該證照內容有關之稽核經驗證明。	

稽核經驗可以稽核員或觀察員身份，參與內部稽核、外部稽核或針對資訊系統委外廠商之稽核，均可納入稽核經驗次數計算。

資通安全管理法施行細則-第四條（3/9）

三.受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。

➢說明：

- 委託機關應依受託業務之性質，決定是否允許受託者就受託業務為複委託；如允許複委託，應注意得複委託之範圍與對象，及複委託之對象應具備之資通安全維護措施，爰為第三款規定。

資通安全管理法施行細則-第四條（4/9）

四.受託業務涉及國家機密者，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。

➢說明：

- 考量國家機密牽涉國家之安危或重大利益，應嚴加保護。

資通安全管理法施行細則-第四條（5/9）

五. 受託業務包括客製化資通系統開發者，受託者應提供該資通系統之安全性檢測證明；該資通系統屬委託機關之核心資通系統， 或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測；涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

- 注意：

  安全檢測如：弱點掃描及滲透測試，委託之第三方應由機關指定。

資通安全管理法施行細則-第四條（6/9）

六. 受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。

➢ 說明：

- 受託者執行受託業務，有違反資通安全相關法令之情形，或知悉資通安全事件時，為避免損害擴大，應立即將相關情狀通知委託機關，並採行諸如啟動備援、回復運轉、損害管制等適當之補救措施，爰為第六款規定。
- 注意：於合約或於需求說明書內要求（可參考資訊服務採購契約範本）。

資訊服務採購契約範本

- 廠商提供服務，如違反資通安全相關法令、知悉機關或廠商發生資安事件時，均必須於1小時內通報機關，提出緊急應變處置，並配合機關做後續處理；必要時，得由資通安全管理法主管機關於適當時機公告與事件相關之必要內容及因應措施，並提供相關協助。

資通安全管理法施行細則-第四條（7/9）

七.委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行契約而持有之資料。

➢說明：

- 為確保對於受託業務相關資料及系統之保護，受託者於委託關係結束時，應返還、移交、刪除或銷毀為履行契約所持有之資料，爰為第七款規定。
- 注意：保留執行紀錄(如：銷毀單或切結書)。

資通安全管理法施行細則-第四條（8/9）

八.受託者應採取之其他資通安全相關維護措施。

➢說明：

- 委託機關就委外辦理之業務，得要求受託者依業務之性質及內容，調整其須具備之資通安全相關維護措施，爰為第八款規定。
- 注意：資通安全相關維護措施(如：應用系統委外開發：可考慮廠商的開發環境是否安全，程式的測試資料是否合宜等)。

資通安全管理法施行細則-第四條（9/9）

九.委託機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

➢說明：

- 為確保受託業務執行之妥適性， 委託機關應定期檢視執行狀況；於知悉受託者發生可能影響受託業務之資通安全事件時，亦應確認受託業務之執行情形，爰為第九款規定。
- 注意：於合約或於需求說明書內要求（可參考資訊服務採購契約範本）。

資訊服務採購契約範本

- 機關得定期或不定期派員檢查或稽核廠商提供之服務是否符合本契約之規定，廠商應以合作之態度在合理時間內提供機關相關書面資料，或協助約談相關當事人。上述提供機關相關書面資料，以法令規定或契約約定者為限，其檢查或稽核得以不預告之方式進行之，廠商不得拒絕。

補充-附表十、資通系統防護基準

系統與服務獲得	系統發展生命週期委外階段	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**。

資通系統開發、維運及管理安全要求-需求申請

「系統開發與維護程序書」

- 申請單位對於系統開發或變更的需求應由業務負責人員先提出具體需求描述，並與承辦單位承辦人員充分討論後確立需求內容。

- 承辦單位承辦人員針對需求內容進行必要的系統分析與評估後，提出「系統需求申請表」送承辦單位負責人員與主管簽核，完成需求確認。若評估後續測試時需使用真實資料進行測試，應於此階段一併取得授權。

系統測試與驗收

「系統開發與維護程序書」

- 測試不應在線上營運系統執行，測試環境與線上環境應予以分開。

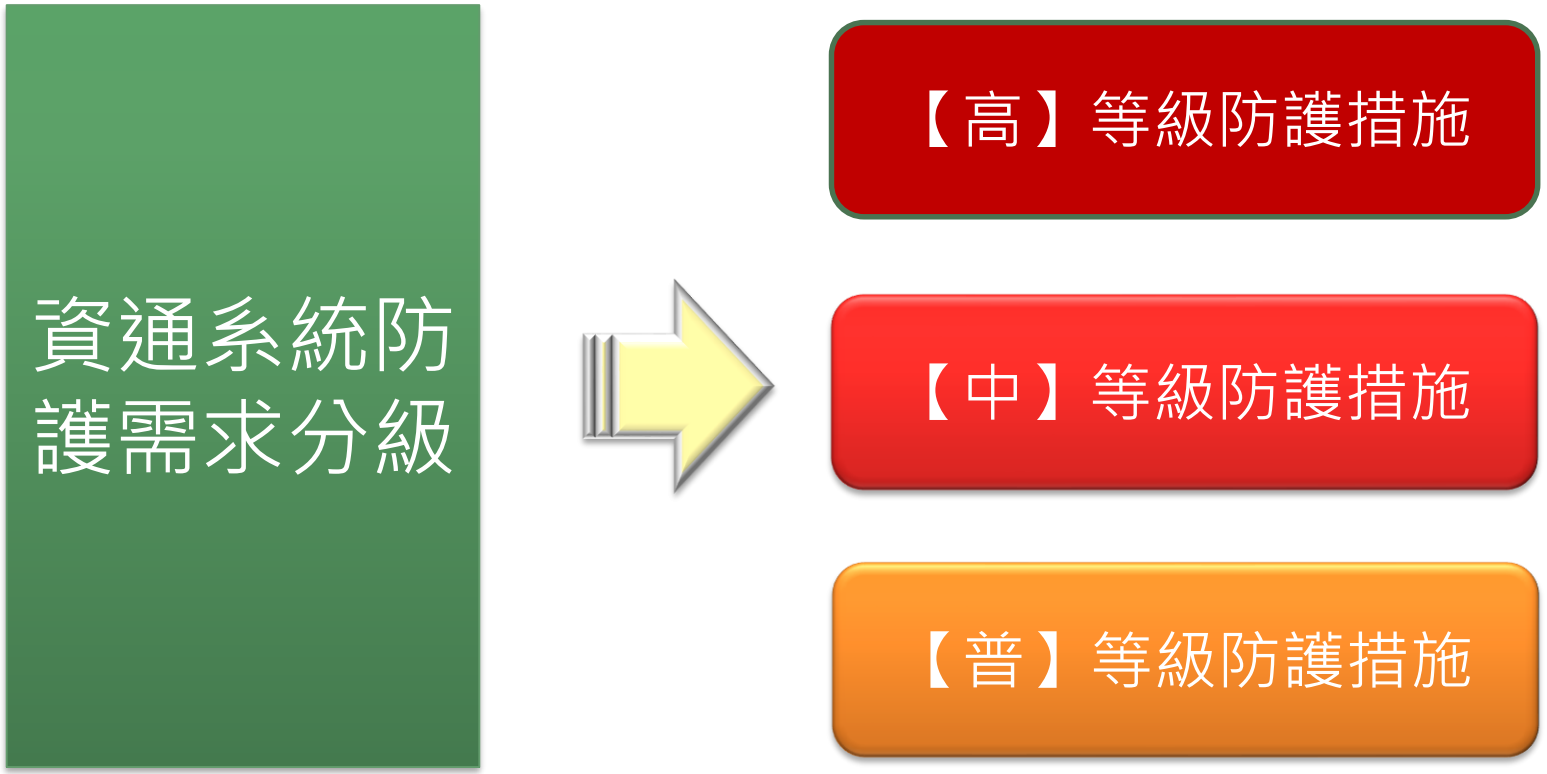
- 系統開發或變更需求完成後，承辦單位承辦人員應準備「系統測試與驗收報告」，並通知申請單位進行聯合測試。

- 測試結果若系統功能已滿足所提需求，申請單位負責人員於「系統測試與驗收報告」中填寫測試驗收結果，經單位主管簽核後完成驗收作業。

資通安全責任等級分級辦法

- 第11條

各機關自行或委外開發之資通系統應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表十所定資通系統防護基準執行控制措施。



核心系統認定

- 前條第一項第一款所定核心業務，其範圍如下:
- 一、公務機關依其組織法規，足認該業務為機關核心權責所在。
- 二、公營事業及政府捐助之財團法人之主要服務或功能。
- 三、各機關維運、提供關鍵基礎設施所必要之業務。
- 四、各機關依資通安全責任等級分級辦法第四條第一款至第五款或第五條第一款至第五款涉及之業務。
- 前條第一項第六款所稱核心資通系統，指支持核心業務持續運作必要之系統，或依資通安全責任等級分級辦法附表九資通系統防護需求分級原則之規定， 判定其防護需求等級為高者。

備份管理及人員作業安全檢視 - A.12.3備份

- 目標：防範資料漏失

控制措施	稽核重點
資訊備份	1. 建立並實作備份政策 2. 定期測試備份回復 3. 一般人員對機敏資料的備份方式 防護基準普級以上：營運持續計畫 - 系統備份

作業安全管理及人員作業安全檢視 - A.12.4存錄及監視

- 目標：紀錄事件並產生證據

控制措施	稽核重點
事件存錄	1. 依防護基準及「各機關資通安全事件通報及應變處理作業程序」產出並留存稽核軌跡紀錄。 2. 保護稽核軌跡紀錄：另行備份（Log Server、NAS、燒錄光碟……）、設定存取權限 3. 各單位系統帳號權限清查紀錄 4. 各單位監視器影像紀錄 5. 參考：存取控制程序書、使用者帳號及權限管理作業說明書
日誌資訊之保護	
管理者及操作者日誌	
鐘訊同步	機關內有統一校時（系統、設備及紀錄）

跡證保存

各機關資通安全事件通報及應變處理作業程序

資通安全責任等級	保存範圍	保存項目
A	機關應保存全部資通系統與各項資通及防護設備最近六個月之日誌紀錄。	1. 作業系統日誌(OS event log) 2. 網站日誌(web log) 3. 應用程式日誌(AP log) 4. 登入日誌(logon log)
B	機關應保存全部核心資通系統與相連之資通及防護設備最近六個月之日誌紀錄。	
C	機關應保存全部核心資通系統最近六個月之日誌紀錄。	

附表十、資通系統防護基準

記錄事件	一應定期審查機關所保留資通系統產生之日誌。 二、等級「普」之所有控制措施。	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。 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。 三、應記錄資通系統管理者帳號所執行之各項功能。

作業安全管理及人員作業安全檢視 - A.12.5運作中軟體之控制

- 目標：確保運作中系統之完整性

控制措施	稽核重點
對運作中系統之軟體安裝	系統安裝新軟體或升級新版本前評估測試程序及造成不良影響之對策： 1. 技術性檢測 2. 保留舊版本 3. 還原策略……

作業安全管理及人員作業安全檢視 - A.12.6技術脆弱性管理

- 目標：防範對技術脆弱性之利用

控制措施	稽核重點
技術脆弱性管理	**1. 系統、軟體更新狀態(包含公用電腦)** **2. 弱點掃描、滲透測試結果及修補報告**
對軟體安裝之限制	**無未經允許安裝之軟體(包含公用電腦)**

存取控制與網路安全管理 - A.9.1存取控制之營運要求事項

- 目標：限制對資訊及資訊處理設施之存取

控制措施	稽核重點
存取控制措施	文件化及審查存取控制措施： 帳號申請、權限異動、特權帳號管理、存取權限與資訊分級一致.....
對網路及網路服務之存取	僅提供使用者存取已被授權使用之網路及網路服務

存取控制與網路安全管理 - A.9.2使用者存取控制管理

- 目標：限制對資訊及資訊處理設施之存取

控制措施	稽核重點
使用者註冊及註銷	1. 帳號權限管理程序及程序 2. 新增及移除之帳號 3. 所有帳號之權限設定
使用者存取權限之配置	
具特殊存取權限之管理	1. 是否僅有必要人員配置特權帳號（admin、root……） 2. 共用帳號管理：禁止、經常或使用後立即變更密碼……
使用者之秘密鑑別資訊的管理	管理配置之密碼（預設或暫時密碼）：安全傳送方式、配置前確認使用者身分、強制使用後立即變更……
使用者存取權限之審查	定期清查帳號權限
存取權限之移除或調整	人員離職或異動時權限調整

存取控制及權限檢視與網路安全管理 - A.9.3使用者責任

- 目標：令使用者對保全其鑑別資訊負責

控制措施	稽核重點
秘密鑑別資訊之使用	1. 避免密碼留存（禁止手寫、儲存或需有安全控制） 2. 密碼長度及複雜度 3. 不建議多系統共用同一組密碼

存取控制及權限檢視與網路安全管理 - A.9.4系統及應用存取控制

- 目標：防止系統及應用遭未經授權存取

控制措施	稽核重點
資訊存取限制	1. 限制特定使用者可存取之資料或系統 2. 控制使用者存取權限（讀取、寫入、刪除、異動）
保全登入程序 (同防護基準識別與鑑別)	1. 連續登入失敗3次即鎖定15分鐘 2. 保留登入成功及失敗之紀錄 3. 登入過程不明文顯示輸入密碼 4. 限制連線時間或經過特定時間無動作即終止連線 5. 其他非通行碼驗證方式（生物辨識或實體金鑰）
通行碼管理系統 (同防護基準識別與鑑別)	1. 強制要求使用者使用合格之密碼 2. 強制要求首次登入立即變更暫用密碼 3. 密碼記憶，不與前3代重複

營運持續管理安全要求

「業務永續運作管理程序書」

- 本校應實施業務永續運作管理作業，結合預防和復原控制措施，將業務災害或故障（如自然災害、意外、設備故障和蓄意行為等）所造成之中斷情形降低到可接受的範圍。

- 應分析業務災害或故障對組織之衝擊，並發展和實施「業務永續運作計畫」，確保能在所需時間內恢復業務運作。「業務永續運作計畫」亦應持續維護並定期演練。

影響業務營運的因素

電腦惡意攻擊
- 惡意網頁
- 垃圾電子郵件
- 植入木馬/後門程式
- 攻擊系統弱點或漏洞
- 間諜軟體
- 阻斷服務攻擊

天然災變
- 地震
- 颱風/焚風
- 雷擊

意外事故
- 火災
- 停電
- 管線破裂
- 危險物品散出

其他事件
- 軟/硬體失效
- 人為操作疏失
- 人員意外或離職
- 員工盜賣資產
- 惡意競爭
- 嚴重特殊傳染病

災害、營運持續演練計畫

§ 災害演練(火災、地震、停電...)

§ 營運持續演練計畫

有機房範例

- 網路骨幹服務持續計畫
- 電力持續計畫
- 空調持續計畫

……等可供參考

無機房範例

- 資訊系統持續計畫
- 業務持續計畫

……等可供參考

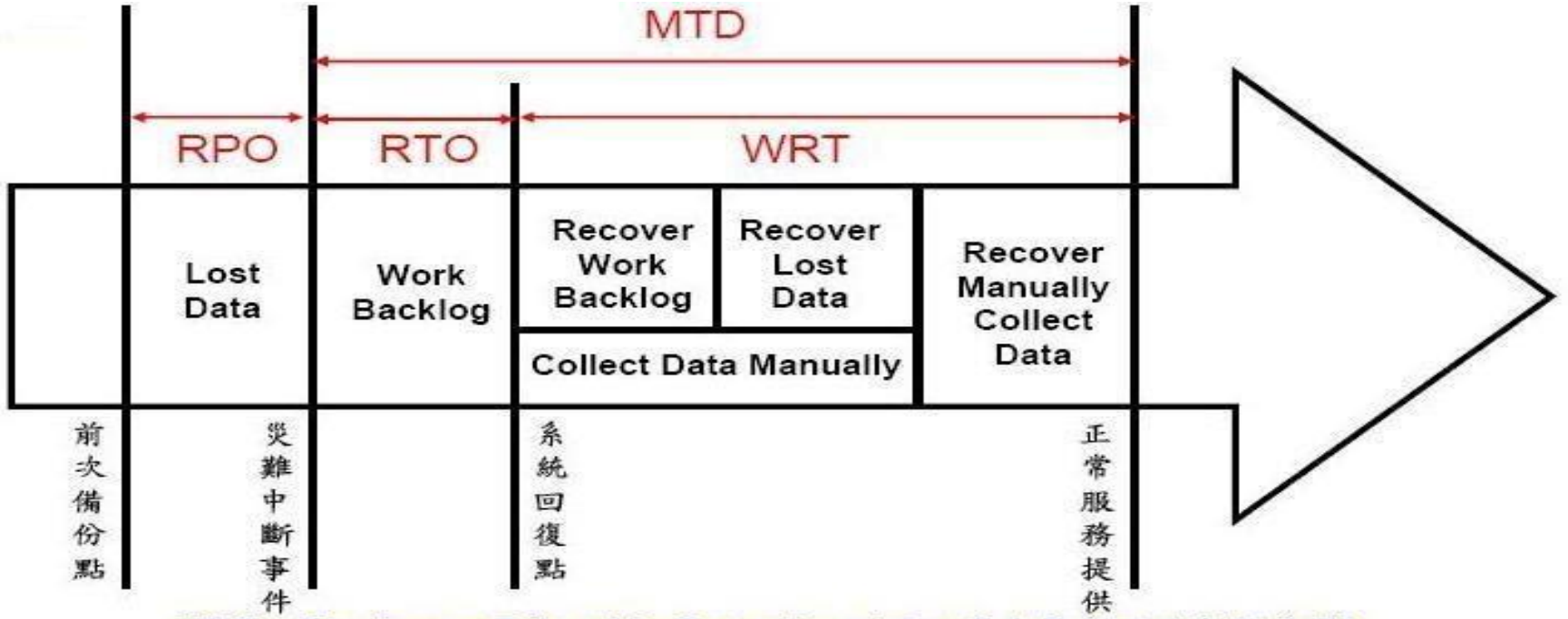
營運衝擊分析

- 營運衝擊分析
  （Business Impact Analysis, BIA）：
  檢視整體營運流程並分析影響程度，重大故障或災害發生時，以確保持續營運規劃能發揮最大效益。
- 鑑別組織的產品或服務，在中斷事件發生時，哪些產品或服務會影響到組織的營運。

名詞解釋

- 資料回復點(Recovery Point Objectives, RPO)：
  中斷事件發生後，足以回復至正常運作之資料時點。
- 最大可容忍服務中斷時間 (Maximum Tolerable Downtime, MTD)：
  業務從事故發生到恢復正常運作之時間區段。
- 系統回復時間（Recovery Time Objective, RTO）：
  業務從事故發生後系統重建復原的時間區段。
- 資料復原時間(Work Recovery Time, WRT):
  業務從系統重建復原後並將資料及設定復原至可正常運作之時間。

BIA之因子關係圖



- MTD – Maximum Tolerable Downtime (可以忍受最大服務中斷時間)
  Maximum Tolerable period of Disruption
- RPO – Recovery Point Objective (資料回復點)
- RTO – Recovery Time Objective (系統回復時間)
- WRT – Work Recovery Time (資料復原時間)

業務持續策略

- 在業務持續計畫範圍內，對每一支援關鍵產品及服務的活動，組織應該：
  a) 評估如果活動中斷，隨時間推移所造成的影響
  b) 通過識別以下內容，為每一活動建立最大可容忍服務中斷時間（MTD）：
     - 自中斷開始，活動需要被恢復的最大期限
     - 活動需要恢復到的最低水準（RTO）
     - 恢復到正常水準的時間跨度
  c) 識別任何相互依賴的活動、資產、用於支持的基礎建設與資源，這些也需要得到持續的維護或隨時間進行的恢復。

資安事故安全要求-參考依據

- 「資通安全管理法」
- 「資通安全事件通報及應變作業辦法」
- 「資通安全事件管理程序書」
- 「個人資料保護緊急應變處理作業說明書」

通報程序

「資通安全事件管理程序書」

- 疑似資通安全事件發生時，發現人員應依事件歸屬通報權責單位，並副知直屬主管
- 權責單位於收到通知後，研判是否為資通安全事件。
- 權責單位於發生資通安全事件時，應立即填具「資通安全事件報告單」

資訊安全事件回應

- 規劃事件回應可以使組織隨時準備面對各種已知及未知的威脅，並建立一個可靠的方式在最短的時間內識別各項資安事件。

- 行政院訂頒「資通安全事件通報及應變辦法」，將資通安事件影響等級分為4個級別，由重至輕分別為「4級」、「3級」、「2級」及「1級」

- 公務機關知悉資通安全事件後，應於一小時內依主管機關指定之方式及對象，進行資通安全事件之通報。

資通安全事件分級（1/4）

- 第一級資通安全事件:

一.非核心業務資訊遭輕微洩漏。

二.非核心業務資訊或非核心資通系統遭輕微竄改。

三.非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成機關日常作業影響。

資通安全事件分級（2/4）

- 第二級資通安全事件:

一.非核心業務資訊遭嚴重洩漏， 或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

二.非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

三.非核心業務之運作受影響或停頓，無法於可容忍中斷時間內 回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

資通安全事件分級（3/4）

- 第三級資通安全事件:

一.未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

二.未涉及關鍵基礎設施維運之核心業務資訊或核心 資通系統遭嚴重竄改，或一般公務機密、敏感資 訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

三.未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓， 於可容忍中斷時間內回復正常運作。

資通安全事件分級（4/4）

- 第四級資通安全事件:

一.一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或國家機密遭洩漏。

二.一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或國家機密遭竄改。

三.涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作。

資安法規定時限

- 公務機關知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業，並依主管機關指定之方式及對象辦理通知事宜：

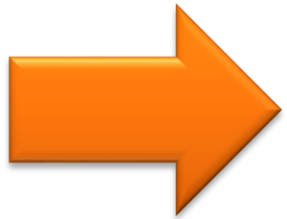
一、二級資安事件為72小時內完成。

三、四級資安事件為36小時內完成。

事故管理

- 事故管理可以讓組織為面臨意外安全事故做好預先的準備，並減少對IT資產造成損害的持續時間和嚴重性。

- 事故處理有助組織於事故發生後儘早恢復正常的營運服務，並最大程度地減少對各項業務營運的影響，從而確保維持正常服務所需的服務質量。

資安事件發生  **營運持續**

ISMS-檢討與改善

「資通安全事件管理程序書」

- 安全事件確認處理完成後，權責單位應檢討現行管理措施之完整性，並適當修訂相關作業管理規範或建置控制措施。必要時，應召開檢討會議。

- 權責單位應依「矯正管理程序書」規定處理，以避免類似安全事件重複發生。

個資事故通報及受理程序

- 當發生個資外洩時必須告知當事人並留下通報紀錄，若有通報而無相關通報記錄，事後將究責。
- 接獲個資事故通報後，需依所通報之內容進行處理，並填寫本校「個人資料侵害事故通報與紀錄表」
- 當違反個資法規定，導致個人資料被竊取、洩漏、竄改或其他侵害者，應於查明後以適當方式通知當事人
- 應建立通報機制，確保所使用的方式(例如電話、簡訊、郵寄、email等)可以通知到當事人，並留下紀錄

個資事故通報及受理程序

- 各單位於發現個資遭侵害時，應通知個人資料管理窗口，由個人資料管理窗口與個資保護執行小組判斷是否發生個資事故。

- 個人資料管理窗口接獲相關個資案件通知時，應立即協同相關人員蒐集相關跡證，初步判斷是否發生個資事故及其影響程度與範圍。

PIMS-檢討與改善

「個人資料保護緊急應變處理作業說明書」

- 個資事故確認處理完成後，事故發生單位應檢討現行安全控制措施之完整性，並適當修訂相關作業管理規範或建置控制措施，且於必要時召開檢討會議。

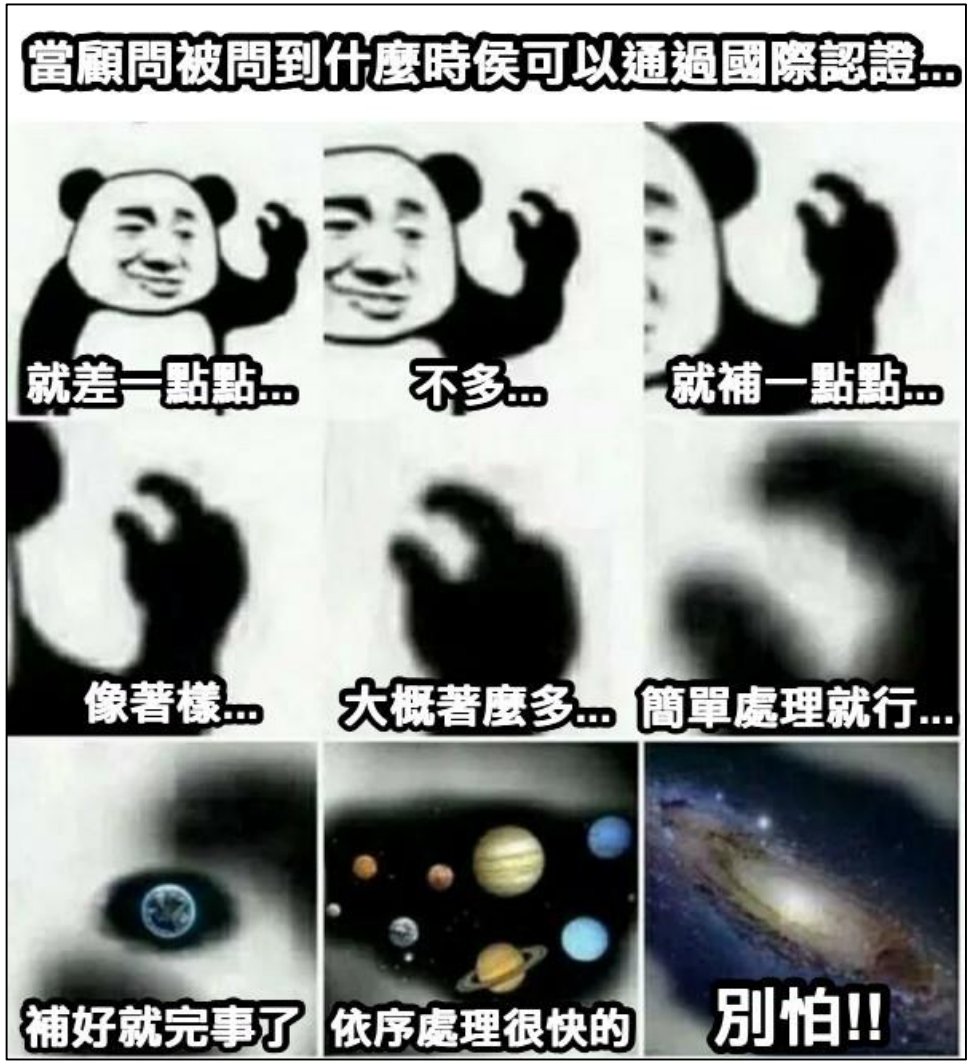
- 事故發生單位應於事故處理完畢後，進行相關矯正預防措施，避免同類型之個資事故重複發生。

課程結論

資安管理制度-稽核常見的情境...

完全不準備 V.S 做好萬全準備

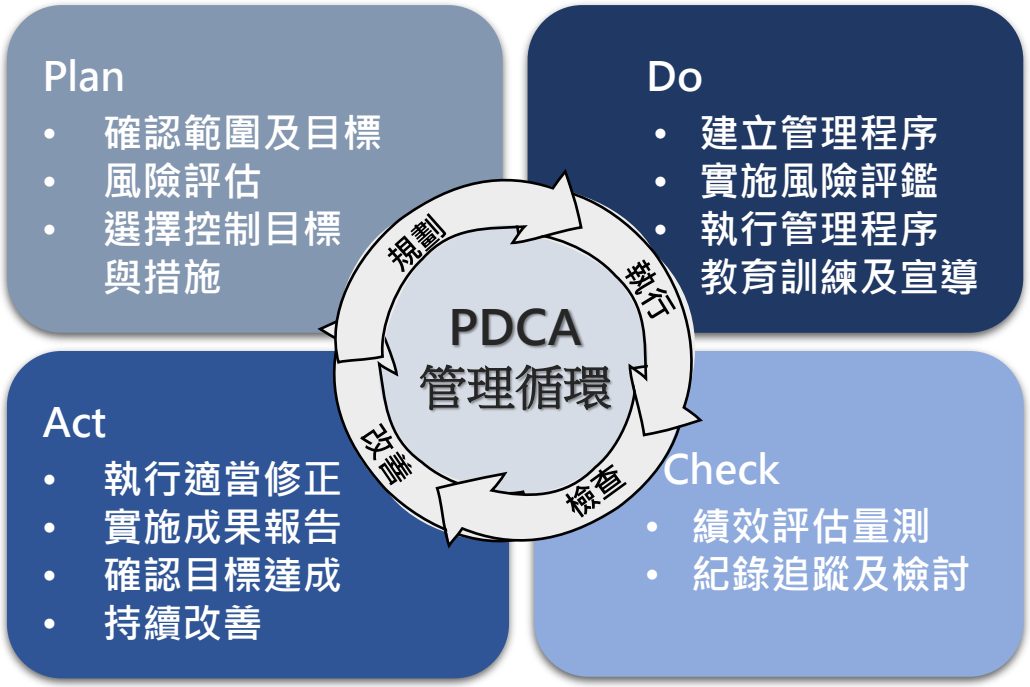
資安管理制度-國際認證與矯正時常見的情境...



課程結論

管理制度運行應保持說、寫、做一致，透過文件化作業展現制度落實執行的過程；組織人員及委外廠商應配合管理程序文件中所訂定之各種控管措施融入日常維運，並按實際需求及外部環境之變化，持續改善並強化各項管控作業，以期達到資通安全與個資保護永續經營的目標。

管理制度沒有100分，組織投入資源維運管理制度，應積極配合各項安全管理控制措施，不怕被開立缺失與改善建議，應考慮這過程中是否有讓組織推行制度健全的方式與機會，降低營運中所產生的風險！



TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

問題與討論

請掃描QR code填寫課後評量

https://forms.gle/wM1wCXbchcMCwEJWA

TSC CAPITAL GROUP

The Bridge to the Asia Pacific Region

感謝您的參與

歡迎於活動後與講師討論您的任何疑問

本公司的臉書粉絲團及部落格可以找到更多資訊

TSC – FB Site

TSC – Blog Site