證據說話——
內部稽核實務與軌跡紀錄管理

國立臺北商業大學 資訊與網路中心 徐國鈞 主任

目錄

01 稽核之基本定義、類型及流程

- 稽核基本定義
- 稽核類型
- 稽核流程

02 個人資訊管理系統 (PIMS) 稽核

- 內部稽核計畫架構
- 內稽底稿查核項目
- 矯正預防處理單填寫重點
- 實作練習：個資稽核常見缺失分析

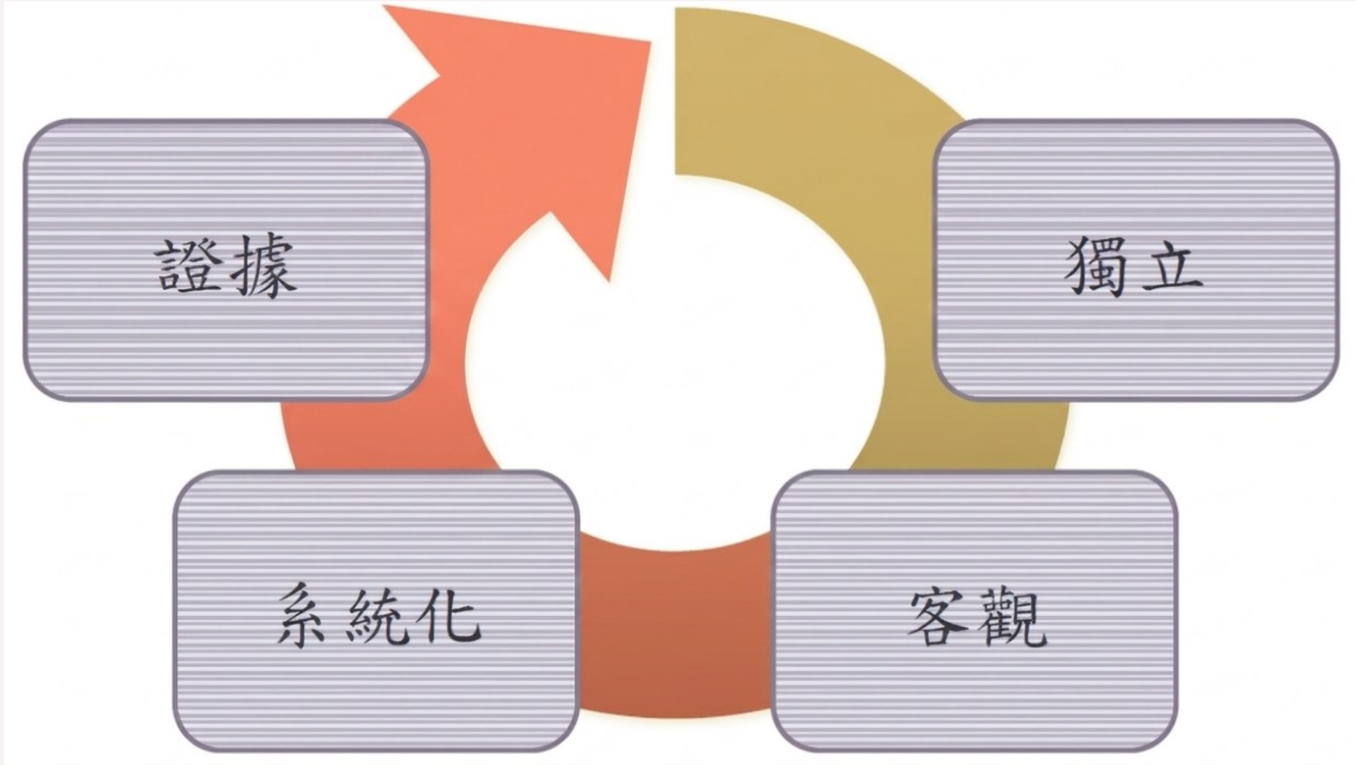
03 軌跡資料與證據留存

- 紙本調閱紀錄
- 系統存取 Log (日誌)
- 監視器畫面
- 同意書與合約

01 稽核之基本定義、類型及流程

稽核之基本定義、類型及流程

ISO 19011 所定義的**稽核**是指透過**系統化**、**文件化**及具**獨立性**的流程取得稽核證據，並透過**客觀**地評估，以鑑別其稽核準則所涵蓋的範圍是否達成。



稽核之基本定義、類型及流程

稽核類型：

內部稽核
(第一方)

- 由組織內部自行發起的稽核
- 確保管理制度的維護、發展及改善，以達成目標

委外稽核
(第二方)

- 由組織對其供應商或外包商所進行的稽核
- 評估供應商、外包商或下游單位是否符合契約要求或規定

外部稽核
(第三方)

- 由具有公信力且獨立的機構對組織進行稽核
- 驗證組織是否符合建立、施行並維護文件化之管理制度標準

稽核之基本定義、類型及流程

稽核流程：

前置作業

- 確認稽核範圍
- 進行稽核小組、人員任務分配

稽核作業

- 召開稽核起始會議
- 蒐集客觀證據
- 召開稽核總結會議

矯正追蹤作業

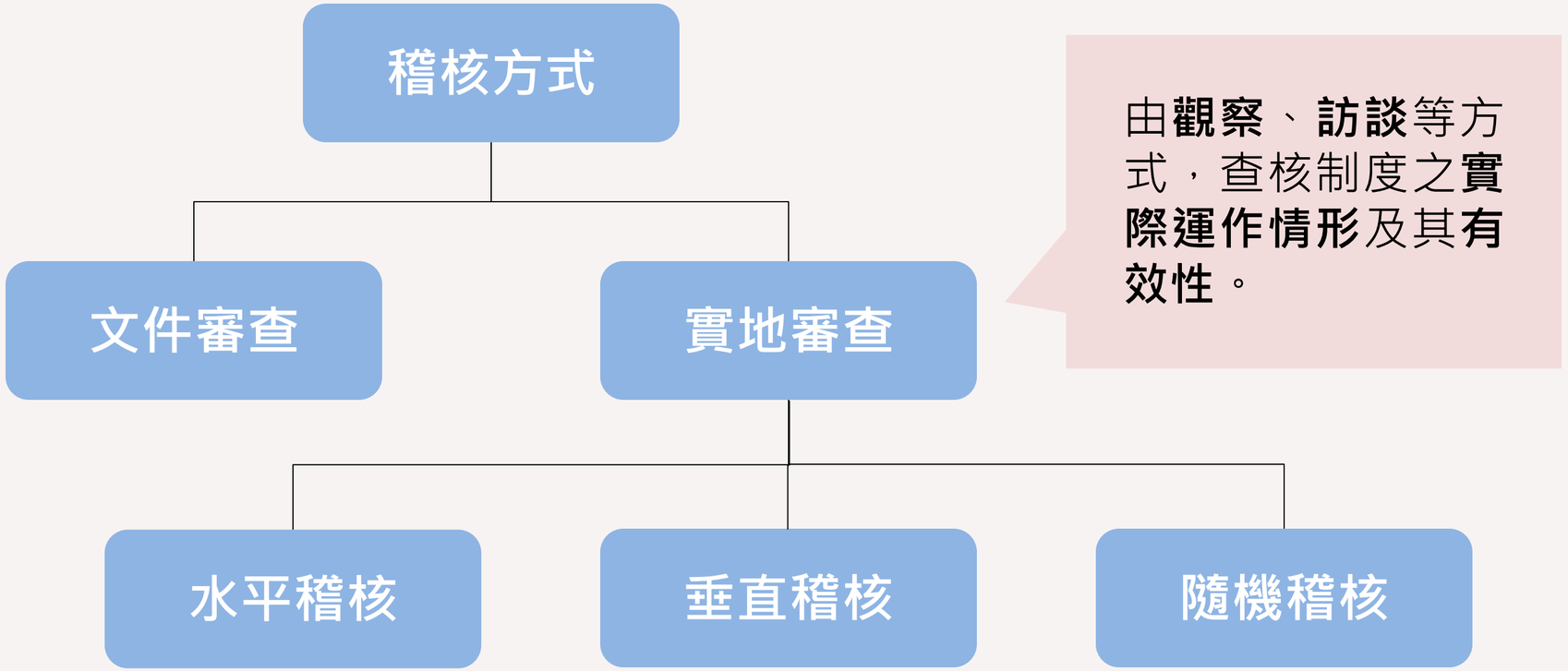
- 依稽核結果，針對受稽核單位進行矯正改善
- 改善追蹤

稽核前　　稽核中　　稽核後

稽核之基本定義、類型及流程

稽核方式：

檢視並確認相關制度是否符合**稽核準則**所訂之基本要求。



由**觀察**、**訪談**等方式，查核制度之**實際運作情形**及其**有效性**。

稽核之基本定義、類型及流程

實地審查：

水平稽核

依據**內稽底稿**或**查檢表**所列項目逐一提問，並依查檢表之設計於橫向欄位記錄稽核發現；確認該項查核完成後，再進行下一項查核。

垂直稽核

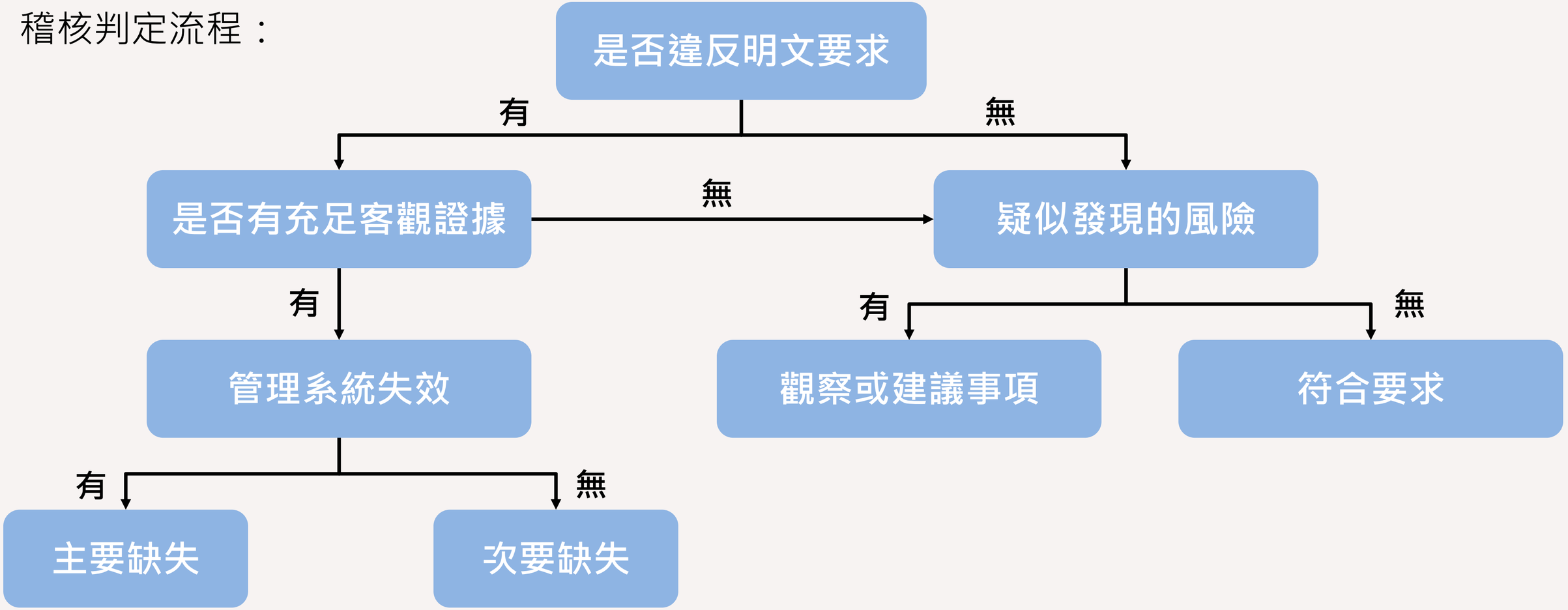
針對**特定議題**或**業務流程**，對相關人員或跨單位訪談對象進行查核，以追蹤並確認相關政策、規範、作業程序、管制措施及相關紀錄之落實情形。

隨機稽核

於稽核範圍內進行**抽樣查核**，例如以前次稽核日至本次稽核日期間之相關作業或紀錄為抽樣範圍。

稽核之基本定義、類型及流程

稽核判定流程：



稽核之基本定義、類型及流程

稽核判定類別：

主要缺失

- 部分程序、作業流程或實際實施情形已完全失效。必要要求項目中，有項目未予以任何實施。
- 多項次要不符合之累積已導致整體系統功能失效或崩潰。
- 前次稽核所列之次要不符合事項於本次稽核仍再度發生。
- 驗證標章或認證標章之使用方式不符規定。

次要缺失

- 部分程序、流程或操作上存在輕微偏離之情形。
- 單一、偶發且非連續性的不符合狀況。

稽核之基本定義、類型及流程

稽核判定類別：

觀察事項

- 雖未發現不符合稽核準則之具體證據，惟仍存在潛在風險，屬應予特別關注與審慎考量之事項。

建議事項

- 有助於組織管理系統持續精進之改善建議，並包含可供參考之業界良好實務。

稽核之基本定義、類型及流程

缺失開立原則：

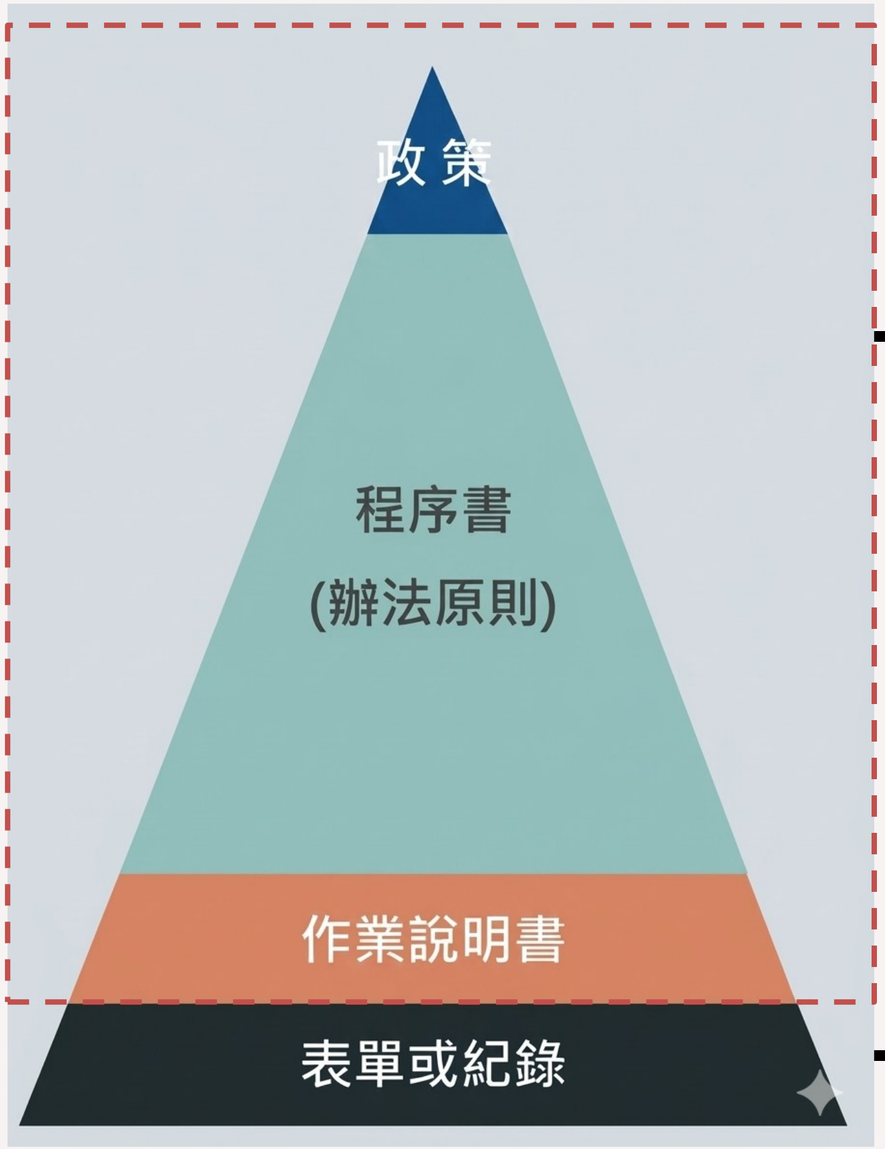
- **5W1H**

- 發生地點 (Where)
- 發生時間 (When)
- 在場人員或權責部門 (Who)
- 發生之事實或現象 (What)
- 構成不符合事項的原因 (Why)
- 如何發生 (How)

02 個人資訊管理系統 (PIMS) 稽核

個人資訊管理系統 (PIMS) 稽核

稽核依據：



要求文件化之資訊

- 內外部議題及利害關係人（關注方）之要求
- 管理政策
- 管理目標
- 個人資料流識別（含高風險）
- 隱私衝擊及風險評鑑流程（含風險評估及處理計畫）
- 隱私保護設計相關活動及其成果資訊
- 人員勝任能力之證據
- 管理審查資料（含有效性評估之佐證）
- 不符合項目及其矯正措施

- 管理制度執行之相關證據（包括個人資料之蒐集、處理、利用、資料分享及委外管理等事項）
- 當事人權利行使之相關紀錄
- 制度規劃與運作所需之外來文件

個人資訊管理系統 (PIMS) 稽核

權責：

資訊安全暨個人資料保護推動委員會

負責審核**「個人資料管理制度內部稽核計畫」**及**「個人資料管理制度內部稽核報告」**。

資訊安全暨個人資料保護稽核小組

負責擬訂**「個人資料管理制度內部稽核計畫」**、辦理**內部稽核作業**並產出**「個人資料管理制度內部稽核報告」**。

受稽單位

配合各項稽核作業。

個人資訊管理系統 (PIMS) 稽核

內部稽核計畫架構：

一、稽核目的與範圍

- 稽核目的：主動檢核校內個資管理制度 (PIMS) 執行現況，確認各單位是否落實法規要求，並發現潛在風險以進行改進。
- 稽核範圍：包含所有蒐集、處理，以及利用個資的單位（如教務處、學務處、資網中心），以及委外廠商的管理狀況 。

二、稽核頻率

- 稽核頻率：建議至少每年度辦理一次。

個人資訊管理系統 (PIMS) 稽核

內部稽核計畫架構：

三、稽核重點項目

- 技術安全：是否有採取隱碼機制 、加密機制，以及防止入侵對策。
- 作業程序：個資生命週期 (蒐集、處理、利用、刪除) 是否皆有適法依據與紀錄。
- 委外管理：委外契約是否包含違規責任、罰則，並要求廠商提供應變計畫。
- 事故應變：是否具備個資事故通報流程 、是否定期進行事故實體演練。
- 教育訓練：相關人員是否定期參與個資安全認知教育訓練。

個人資訊管理系統 (PIMS) 稽核

內部稽核計畫架構：

四、稽核團隊組成

為確保稽核過程之客觀性與獨立性，稽核作業應由非受稽單位人員執行。稽核團隊得以下列方式組成，以辦理各項個人資料保護稽核事務：

1. 聘請外部個資保護顧問協助執行稽核。
2. 由經審定具備資格之稽核人員擔任，例如具備 ISO/IEC 27701 個人資料隱私管理系統主導稽核員訓練證書，或已接受個人資料保護內部稽核相關訓練者。

個人資訊管理系統 (PIMS) 稽核

內部稽核計畫架構：

五、稽核結果之處理

- 異常發現紀錄：詳細記錄不符合項 (Non-conformity) 的事實與證據。
- 開立矯正措施單 (CAR)：要求受稽單位限期提出改善措施與預防措施。
- 追蹤改善：確認改善措施已確實執行且有效。
- 管理審查報告：將稽核結果彙報至「資安暨個資保護推動委員會」。

個人資訊管理系統 (PIMS) 稽核

內稽底稿查核項目 (節錄)：

一、界定個人資料之範圍

- 查核項目 (1)：是否已建立與維護一份個人資料檔案清冊？
- 稽核重點：以**「個人資料流」**所識別單位之個資資產
- 佐證資料：**個人資料檔案清冊**、**個人資料流程識別表**

- 查核項目 (2)：是否已公告本校保有個人資料檔案公開項目彙整表？
- 稽核重點：依個資法第 17 條，公開單位之**「個人資料檔案公開項目彙整表」**
- 佐證資料：**個人資料檔案公開項目彙整表**至少包含**個資檔案名稱**、**保有機關名稱及聯絡方式**、**個資檔案保有依據及特定目的**，以及**個人資料之類別**

個人資訊管理系統 (PIMS) 稽核

內稽底稿查核項目 (節錄)：

二、個人資料保護之風險評估及管理機制

- 查核項目 (1)：是否已建立與執行風險評鑑作業，以確保本校能瞭解在處理各種特定類型之個人資料所可能產生的風險？
- 稽核重點：組織之**個資風險評鑑**的評估方式
- 佐證資料：**個人資料風險評鑑表 (包含衝擊影響 / 可能性 / 風險值)**

- 查核項目 (2)：是否已定義可接受風險與進行高風險處理及風險再評鑑？
- 稽核重點：如何定義「可接受風險」方式；高風險項目處理的狀況；風險「再評鑑」的方式及結果
- 佐證資料：**可接受風險值評估紀錄**、**高風險處理紀錄 (風險改善計畫)**、**再評鑑評估紀錄**

個人資訊管理系統 (PIMS) 稽核

內稽底稿查核項目 (節錄)：

三、個人資料蒐集、處理及利用之內部管理程序

- 查核項目 (1)：蒐集、處理及利用個人資料時，是否已符合「適當、相關且符合資料極小化」的原則？
- 稽核重點：由業務職掌，了解所設計的機制或表單是否符合**「適當、相關且符合資料極小化」**之原則
- 佐證資料：**「適當、相關且符合資料極小化」之討論、審核紀錄**

- 查核項目 (2)：是否維護個人資料之正確且保持更新？
- 稽核重點：當事人資料變更之處理機制，以證明資料之處理、利用時為正確資料
- 佐證資料：**當事人變更紀錄**、**業管單位處理紀錄**

個人資訊管理系統 (PIMS) 稽核

內稽底稿查核項目 (節錄)：

三、個人資料蒐集、處理及利用之內部管理程序

- 查核項目 (3)：是否已建立與執行相關程序，以確保組織保留個人資料所需的保存期限？
- 稽核重點：保存期限設定之佐證
- 佐證資料：個人資料檔案清冊中的**「保有依據」**

- 查核項目 (4)：是否已建立並實作個人資料檔案銷毀作業，當特定目的消失或保存期限屆滿時，合理地銷毀個人資料檔案？
- 稽核重點：屆滿個資銷毀之現況
- 佐證資料：**個資銷毀紀錄**、**委外銷毀之協議**、**保密文件**

個人資訊管理系統 (PIMS) 稽核

內稽底稿查核項目 (節錄)：

三、個人資料蒐集、處理及利用之內部管理程序

- 查核項目 (5)：是否已建立與執行相關程序，確保當個人資料以電子或人工方式在組織內外傳輸的過程中，皆施予合適之控管措施，進而提供資料傳遞之安全防護？
- 稽核重點：電子或紙本個資傳輸控管方式
- 佐證資料：**電子**：Email 加密；**紙本**：專人親送、彌封等

個人資訊管理系統 (PIMS) 稽核

內稽底稿查核項目 (節錄)：

四、資料安全管理及人員管理

- 查核項目 (1)：是否對存放於系統上之備份資料已定期執行回復測試？個人資料的授權與存取作業是否已在合法目的下執行？
- 稽核重點：了解系統之相關管控措施，如備份、授權存取、帳號清查等
- 佐證資料：**系統之管控執行紀錄**

個人資訊管理系統 (PIMS) 稽核

內稽底稿查核項目 (節錄)：

四、資料安全管理及人員管理

- 查核項目 (2)：是否已建立與執行委外安全管理？是否定期審查或稽核委外廠商有關個資安全之遵循性？與委外廠商之契約是否已考慮個人資料保護要求？
- 稽核重點：委外狀況或項目；監督責任之履行；合約內容之個資管控要求
- 佐證資料：**委外合約**、**保密切結書**、**監督紀錄**

- 查核項目 (3)：針對可攜式、行動裝置或雲端服務，是否已建立並執行相關管理規定？
- 稽核重點：可攜式、行動裝置或雲端服務相關管控規定
- 佐證資料：**實地隨機抽查**是否符合規定

個人資訊管理系統 (PIMS) 稽核

內稽底稿查核項目 (節錄)：

五、認知宣導與教育訓練

- 查核項目 (1)：是否已進行教育訓練或觀念宣導等方式來強化組織內人員對於個資安全的意識？辦理個人資料保護認知宣導活動完畢後，是否留存相關紀錄備查？
- 稽核重點：依要求規劃、執行、評估教育訓練
- 佐證資料：**教育訓練簽到表**等相關紀錄

個人資訊管理系統 (PIMS) 稽核

內稽底稿查核項目 (節錄)：

六、設備安全管理

- 查核項目 (1)：所有涉及個人資料的資訊設備、文件與紀錄，是否皆位於良好實體環境安全管制之區域，且攜出入實體環境皆有管制？
- 稽核重點：依要求管理實體環境
- 佐證資料：**檔案櫃上鎖照片**、**人員出入紀錄表**等相關紀錄

個人資訊管理系統 (PIMS) 稽核

內稽底稿查核項目 (節錄)：

七、使用紀錄、軌跡資料，以及證據保存

- 查核項目 & 佐證資料：

1. 提供當事人行使權利之紀錄
2. 建立並維持當事人同意紀錄及其保存機制
3. 所有涉及個人資料的伺服器作業系統、應用系統、資料庫權限，任何存取紀錄皆已妥善保存
4. 資料正確性及更正之紀錄
5. 個人資料刪除、銷毀之紀錄
6. 文件化程序或機制或紀錄
7. 隱私權公告紀錄，如公告時間或公告版本，予以當事人易於了解
8. 個人資料管理安全事故處理相關紀錄等

個人資訊管理系統 (PIMS) 稽核

內稽底稿查核項目 (節錄)：

八、個人資料安全維護之整體持續改善

- 查核項目 (1)：是否定期舉辦管理審查會議？是否已建立與執行矯正處理措施，並持續追蹤確認？
- 稽核重點：管理審查辦理狀況；內外稽矯正情況；年度目標達成情況
- 佐證資料：**管理審查紀錄**、**內外稽矯正及追蹤紀錄**、**年度目標評估及追蹤紀錄**

個人資訊管理系統 (PIMS) 稽核

矯正預防處理單填寫重點 (節錄)：

https://docs.google.com/spreadsheets/d/184xjw4ow5lW4yzqKJkkhJEnMRZ5OiilDpY6Rd6Yj508/edit?usp=sharing

<table>
<tr><td>提出單位</td><td></td><td>提出人員</td><td></td><td>提出日期</td><td></td></tr>
<tr><td>處理單位</td><td></td><td>處理人員</td><td></td><td>處理日期</td><td></td></tr>
<tr><td colspan="3">缺失分類：
內部稽核：□建議　□缺失
外部稽核：□建議　□觀察
□次要缺失　□主要缺失</td><td colspan="3">事件來源：
□稽核作業　□個資事故
□自行發現　□其它：</td></tr>
<tr><td>問題或缺失說明</td><td colspan="5">(詳加說明事件來源所揭示之問題事項)</td></tr>
<tr><td>原因分析</td><td colspan="5">(請就現行作業方式導致本次事件發生之原因，予以明確說明)</td></tr>
<tr><td rowspan="2">矯正措施</td><td colspan="5">(用以控制事件擴大或降低其影響程度之處置作法)</td></tr>
<tr><td>預定完成日期：</td><td>追蹤人：</td><td>追蹤日期：</td><td colspan="2">確認結果：</td></tr>
<tr><td rowspan="2">預防措施</td><td colspan="5">(旨在消除事件成因，並防止同類事項再次發生之矯正措施)</td></tr>
<tr><td>預定完成日期：</td><td>追蹤人：</td><td>追蹤日期：</td><td colspan="2">確認結果：</td></tr>
</table>

實作練習：個資稽核常見缺失分析

案例1 親師溝通與個資過度蒐集（紙本與程序）：

情境：某班級導師為建立家長聯絡網，要求全班學生填寫「家庭狀況調查表」，內容包含家長的身分證字號、職業、年收入及病史。

實作任務：檢視該調查表是否符合個資法「最小化原則」？

實作練習：個資稽核常見缺失分析

案例1 親師溝通與個資過度蒐集（紙本與程序）：

稽核發現（缺失點）：

- 蒐集範圍過大：親師聯絡通常不需要「身分證字號」與「精確年收入」，此舉違反比例原則。
- 告知義務缺失：表單下方未註明個資蒐集的目的、利用期間及當事人權利（如：可要求刪除）。
- 存放環境不安：導師將回收的紙本隨手放在辦公桌上，且辦公室門禁未管制，學生可輕易翻閱。

正確作法：

重新設計表單，僅保留必要聯繫資訊，並加上個資告知條款，紙本必須入櫃上鎖。

實作練習：個資稽核常見缺失分析

案例2 成績單傳送與權限漏洞（數位軌跡）：

情境：教務處職員為了方便，將全校學生的「期末成績大表（含姓名、學號、成績）」上傳至 Google Drive 雲端資料夾，並設定為「知道連結的人皆可檢視」，隨後將連結貼在校內教職員群組。

實作任務：分析此種分享方式的風險，並檢查系統 Log 能否追蹤洩密來源？

實作練習：個資稽核常見缺失分析

案例2 成績單傳送與權限漏洞（數位軌跡）：

稽核發現（缺失點）：

- 存取控制失效：設定為「公開連結」意味著連結一旦外流，全世界都能看見，不具備身分驗證。
- 缺乏軌跡紀錄：由於是公開連結，系統 Log 僅會顯示「匿名使用者」存取，發生外洩時無法追蹤是哪位教職員將連結流出。
- 敏感資料未加密：檔案本身未設密碼，且包含全校學生個資。

正確作法：

應限定特定帳號（限定教職員 E-mail）存取，並開啟「禁止下載/列印」功能，且檔案應加密處理。

實作練習：個資稽核常見缺失分析

案例3 委外「線上學習平台」的監管缺失（委外管理）：

情境：學校向某科技公司採購「數位學習平台」，並將全校學生的姓名、身分證字號匯入該系統以建立帳號。

實作任務：檢查學校對該廠商的「年度監督」紀錄。

實作練習：個資稽核常見缺失分析

案例3 委外「線上學習平台」的監管缺失（委外管理）：

稽核發現（缺失點）：

- 合約漏洞：檢視合約發現，未載明「廠商發生資安事件時的通報時限」及「合約終止後資料如何銷毀」。
- 缺乏實地或書面稽核：學校保存五年紀錄中，完全沒有廠商的「資安自我檢查表」或「弱點掃描報告」。
- 權限黑洞：廠商工程師為了維修方便，直接使用一個「萬用管理帳號」進出資料庫，學校卻無此存取紀錄。

正確作法：

補足委外合約中的個資處理協議，並要求廠商每年回傳資安檢核報告，且所有遠端維護必須申請並記錄個人身分。

03 軌跡資料與證據留存

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **紙本調閱紀錄**

1. 實體機房進出登記表：

確保所有進入機房的行為皆可追溯，防止未授權的硬體更動或資料竊取。

必填欄位：日期與時間 (進場/出場)；進場人員姓名 (若是外部廠商需註明公司名稱)；進場事由 (如：更換硬碟、系統維護、例行檢查)；陪同人員 (機房通常要求「雙人進出」，需有一名內部員工陪同)。

稽核重點：檢查員會抽查特定的「系統維護日誌」，比對當時是否真有對應的人員在機房內。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **紙本調閱紀錄**

2. 紙本文件調閱申請單 (含主管核准簽名)：

建立「知其必要」的證據軌跡，證明敏感紙本文件 (如客戶契約、人事檔案) 未被隨意翻閱。

必填欄位：申請人單位及姓名；文件名稱/編號；調閱目的；主管核准簽名 (證明程序合規)；歸還日期與簽收。

稽核重點：確認是否有「逾期未還」的情況，以及調閱程序是否早於實際拿到文件的時間。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **紙本調閱紀錄**

3. 訪客登記簿：

管理辦公室整體的邊界安全，區分「內部員工」與「外部人員」。

必填欄位：

身分驗證：訪客需出示證件 (如身分證、駕照) 供櫃檯比對，並登記證件末三碼 (符合個資法最小化原則)。

標示配戴：登記後應發放「訪客證」，並要求全程配戴於胸前顯眼處。

被訪人確認：訪客不能自行進入，必須由該業務承辦人 (被訪人) 親自到櫃檯帶領。

禁止區域規範：登記簿後方可加註「訪客禁區須知」(如：辦公區嚴禁拍照、禁止操作未授權設備)。

稽核重點：檢查員會查看登記簿是否有漏填 (例如有進場沒出場)，或訪客停留時間是否異常過長。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **系統存取 Log (軌跡資料)**

1. 身分驗證：

這是最基礎的「門禁卡」。除了記錄誰進來了，「失敗紀錄」更是資安防禦的重點，可用於偵測暴力破解攻擊。

關鍵紀錄欄位：

使用者帳號、來源 IP 與設備名稱、時間戳記至秒、結果代碼 (成功、密碼錯誤、帳號遭停用、多因子驗證 MFA 失敗)。

實務建議：

應設定告警機制。例如：同一 IP 在 1 分鐘內登入失敗超過 5 次，系統應自動鎖定並發送通知給資安管理員。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **系統存取 Log (軌跡資料)**

2. 特權帳號：

「管理者」擁有最高權限，其行為必須受到最嚴格的監控。這類日誌稱為「操作日誌」 ，用以預防「內部舞弊」或「帳號遭盜用後的大規模破壞」。

關鍵紀錄欄位：

權限變更、設定異動、高風險操作。

實務建議：

推動「代行權限」制度，管理者執行高風險指令時，系統應要求輸入「工單編號」或「審核代碼」，以便日後與申請文件比對。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **系統存取 Log (軌跡資料)**

3. 存取行為：

這是行政檢查 (特別是個資法檢查) 的重中之重。僅有登入紀錄是不夠的，稽核員會要求證明：「當員工進到資料庫後，他看了哪些個資？有沒有大量帶走？」

關鍵紀錄欄位：

查詢：針對身分證字號、病歷、薪資等敏感欄位的查詢行為；匯出：將查詢結果存成 CSV 或 Excel 的動作；大量存取：短時間內讀取超過常規數量的行為。

實務建議：

查詢結果應預設遮罩（如：A123***789），若要查看明文或匯出，必須觸發「二次審核」或留下「專項事由說明」；若資料庫本身效能負荷不了詳細日誌，建議導入第三方稽核工具來側錄所有 SQL 指令。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **監視器畫面**

1. 機房影像監控：

機房是資訊心臟，監控重點在於「設備接觸」與「操作行為」。影像必須能清楚辨識進入者的面貌，以及其在機房內停留的位置 (如：在哪個機櫃前操作)。

監控要點：

機櫃前後門：確認是否有未授權插拔硬碟、接取 USB 或筆電的行為。

環控設備：避免人員誤觸空調、電力開關或滅火系統。

實務建議：

應具備動態偵測錄影功能，節省硬碟空間，但需確保人員進入前 5 秒至離開後 5 秒皆有完整截錄

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **監視器畫面**

2. 文件庫房影像監控：

針對存放機密合約、個人資料申請書、傳票等紙本資料的區域。此處影像旨在防止「未經授權的攜出」或「現場翻拍」。

監控要點：

存取動線：記錄人員領取文件與歸還文件的完整過程。

禁止行為偵測：監控是否有在內使用手機拍攝文件或影印資料的動作。

實務建議：

庫房內應維持足夠照明，避免夜間或昏暗環境下影像模糊，導致檢查時無法辨識人員身分。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **監視器畫面**

3. 出入口影像監控：

包含大樓門廳、辦公區入口及後門。這是建立「人員軌跡」的第一道數據，用來與訪客登記簿或門禁刷卡紀錄進行交叉比對。

監控要點：

尾隨進場：檢查是否有人趁前面同事刷卡時溜進場。

異常時段進出：記錄非上班時間、週末或假日的進出人員。

實務建議：

鏡頭角度應設在與人眼平視或略高處，確保能清楚拍攝面部，且需涵蓋門禁讀卡機位置。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **同意書與合約**

1. 客戶個資蒐集同意書：

這是合規的起點。根據個資法，蒐集資料前必須明確告知並取得同意。檢查員會核對你的資料庫欄位 (如：出生年月日、電話) 是否超出了同意書宣稱的範圍。

核心要素：

告知義務：包含蒐集目的、類別、利用期間、地區、對象及方式。

當事人權利：明確告知客戶可以要求查詢、閱覽、製給複製本、補充、更正、停止蒐集或刪除。

勾選機制：必須是「主動勾選」或「簽名」，不可預設同意。

實務建議：

若為數位同意書，系統需記錄「點擊同意時的 IP」與「精確時間戳記」作為保存五年的電子軌跡。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **同意書與合約**

2. 員工保密協定：

用於建立內部人員的法律約束力。證明公司已盡到「管理責任」，若發生員工洩密，公司可舉證已事先告誡並要求保密，從而釐清公司與個人的法律責任。

核心要素：

保密範圍：定義哪些資訊屬於機密 (如：薪資、技術規格、客戶清單)。

離職後義務：約定離職後仍需負擔保密義務的期限。

違約賠償：明確違反協定時的法律後果與賠償機制。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **同意書與合約**

2. 員工保密協定：

實務建議：

除了入職簽署，建議每年進行「資安宣導」並讓員工簽署當年度的復訓確認書，這在行政檢查中能展現公司有持續落實教育訓練。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **同意書與合約**

3. 委外廠商的資安合約與個資處理協議：

當將資料交給雲端商、物流商或廣告商處理時，仍負有監管責任。

核心要素：

複委託限制：廠商若要再轉包給其他公司，必須事先取得你的書面同意。

安全性要求：要求廠商必須具備加密儲存、定期掃毒、人員權限控管等措施。

稽核權力：合約須載明「甲方有權派員或委託第三方至乙方 (廠商) 處所進行實地檢查」。

事故通報：明確規定廠商若發生資安事件，必須在幾小時內通報你公司。

軌跡資料與證據留存

依據個人資料保護法及相關資安維護計畫，以下紀錄應至少妥善保存五年：

- **同意書與合約**

3. 委外廠商的資安合約與個資處理協議：

實務建議：

行政檢查時，檢查員常會問：「你們怎麼監督委外廠商？」此時除了拿出合約，若能附上「年度委外稽核報告」，專業度會大幅提升。

感謝聆聽