個人資料管理保護
內部稽核教育訓練

德諾科技服務

Agenda

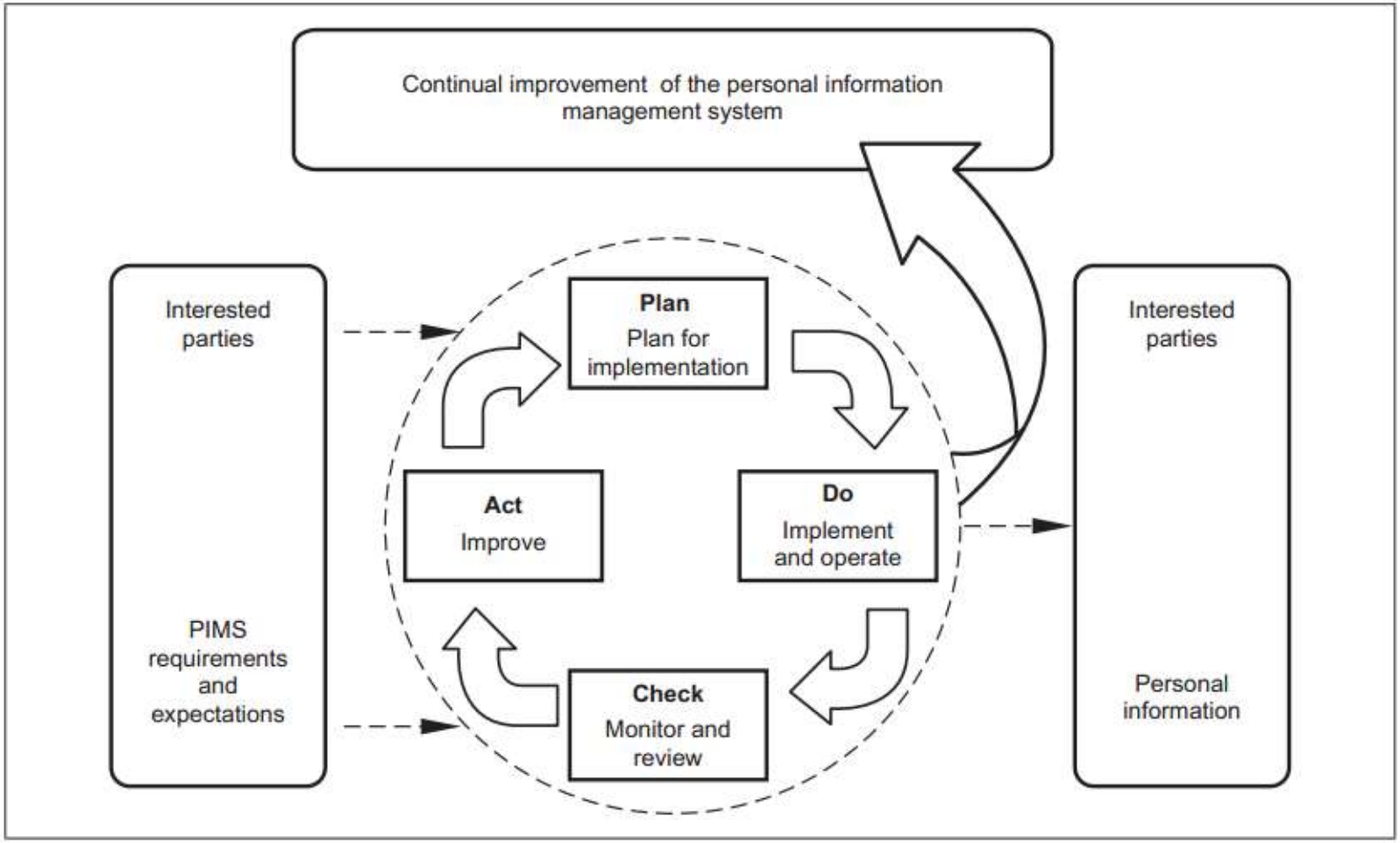
- P-D-C-A 簡介
- 稽核基本原理介紹
- 個資稽核的技巧
- 稽核的重點
- 實際稽核
- 稽核發現點與稽核報告

管理系統框架 – BS 10012

- **Contents**

P-D-C-A

Figure A.1 **PDCA cycle applied to the management of personal information**



重要應辦事項

- 個人資料保護政策
- 個人資料保護法施行細則第十二條第二項
  - 配置管理之人員及相當資源
  - 界定個人資料之範圍
  - 個人資料之風險評估及管理機制
  - 事故之預防、通報及應變機制
  - 個人資料蒐集、處理及利用之內部管理程序
  - 資料安全管理及人員管理
  - 認知宣導及教育訓練
  - 設備安全管理
  - 資料安全稽核機制
  - 使用紀錄、軌跡資料及證據保存
  - 個人資料安全維護之整體持續改善

稽核的目的

- 作業合法性檢查?
- 內控制度的建立與落實?
- 降低資訊處理風險?

內部稽核: 以 ISO 為例

政策

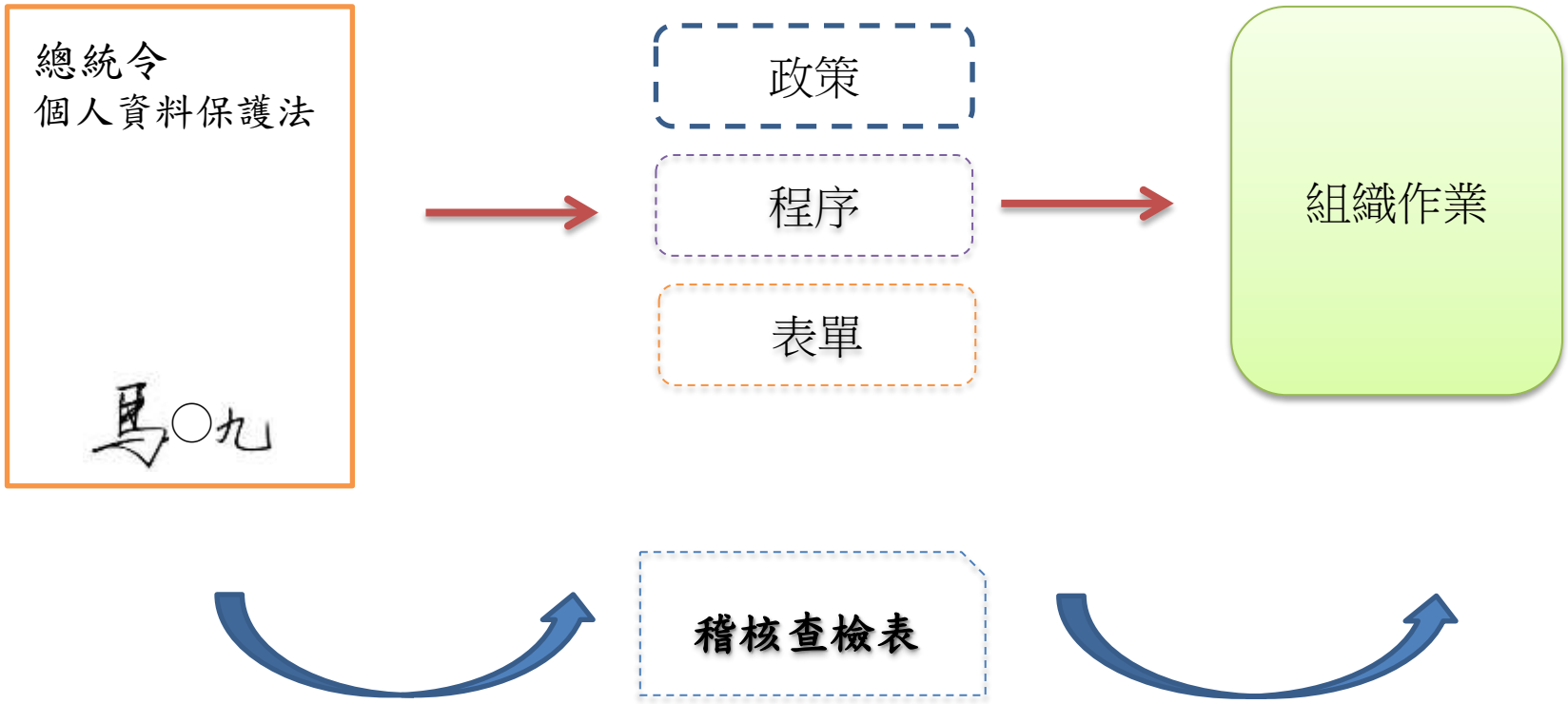
程序

表單

組織作業

稽核查檢表

內部稽核: 適法性查檢?



內部稽核: 管理制度?

總統令
個人資料保護法

馬○九

政策

程序

表單

組織作業

稽核查檢表

個人資料管理系統政策

高雄醫學大學個人資料保護管理政策

101.11.6　101 學年度第 1 次個人資料保護執行管理委員會審議通過
101.11.29 高醫秘字第 1011103292 號函公布

本校為了符合我國個人資料保護法之要求，本校將依以下原則蒐集、處理及利用當事人所提供的個人資料。

一、 本校將遵守個人資料保護法相關法令及本校所訂定之其他有關法令規範。

二、 本校將訂定個人資料保護管理相關之規範、作業準則以落實執行個人資料保護管理，並透過定期檢查、內部稽核或檢視之方式，持續改善之。

三、 本校於建置個人資料保護管理制度後，將公告全體人員周知以落實執行運作。

四、 本校於告知事項中將明示以下內容：本校將於利用目的範圍內，蒐集、處理及利用當事人所提供之個人資料，並於不逾越當事人提供個人資料之利用目的必要範圍內為處理、利用行為，亦將採取適切之個人資料保護措施。

五、 為維護當事人所提供之個人資料為正確且最新之狀態，將採取適切措施預防個人資料的被竊取、洩漏、竄改等侵害。並提升本校資訊安全相關措施以保護所蒐集、處理以及利用之個人資料，同時持續改善內部所建置之個人資料管理制度。於確認發生個資外洩事故時，將迅速採取緊急應變措施作為，並將事實通知當事人。

六、 本校於當事人提出有關其提供個人資料之查閱、複製、更正、刪除等之申請時，將依個資保護法之相關規定確實、迅速回應之。

個人資料檔案安全維護計畫

高雄醫學大學
個人資料檔案安全維護計畫

中華民國103年11月12日

目□次

個人資料管理稽核計畫書

個人資料管理稽核計畫書

個人資料管理稽核小組/稽核部門	個人資料管理代表

稽核目的	
稽核期間	
稽核期間	中華民國個人資料保護法及施行細則與其他個人資料相關法令法規 BS10012 個人資料管理系統標準
日期	
時間	
受稽部門	
稽核人員	

稽核範圍:	本年度	不定期
個人資料保護告知事項及同意內容之檢查		
個人資料盤點作業與公開作業之檢查		
個人資料保護法規盤點作業之檢查		
個人資料範圍界定作業之檢查		
個人資料風險評估與風險管理作業之檢查		
個人資料事故之預防、通報及應變作業之檢查		
個人資料蒐集、處理、利用行為之檢查		
個人資料安全維護作業之檢查		
認知宣導及教育訓練作業之檢查		
設備安全維護之檢查		
個人資料保護持續改善作業之檢查		
使用紀錄、軌跡資料及證據保存作業之檢查		
當事人抱怨及權利行使之各項檢查		
業務終止後個人資料處理程序作業之檢查		
個人資料委外處理程序作業之檢查		
個人資料保護審查管理作業		
其他		

個人資料管理組織代表或召集人	

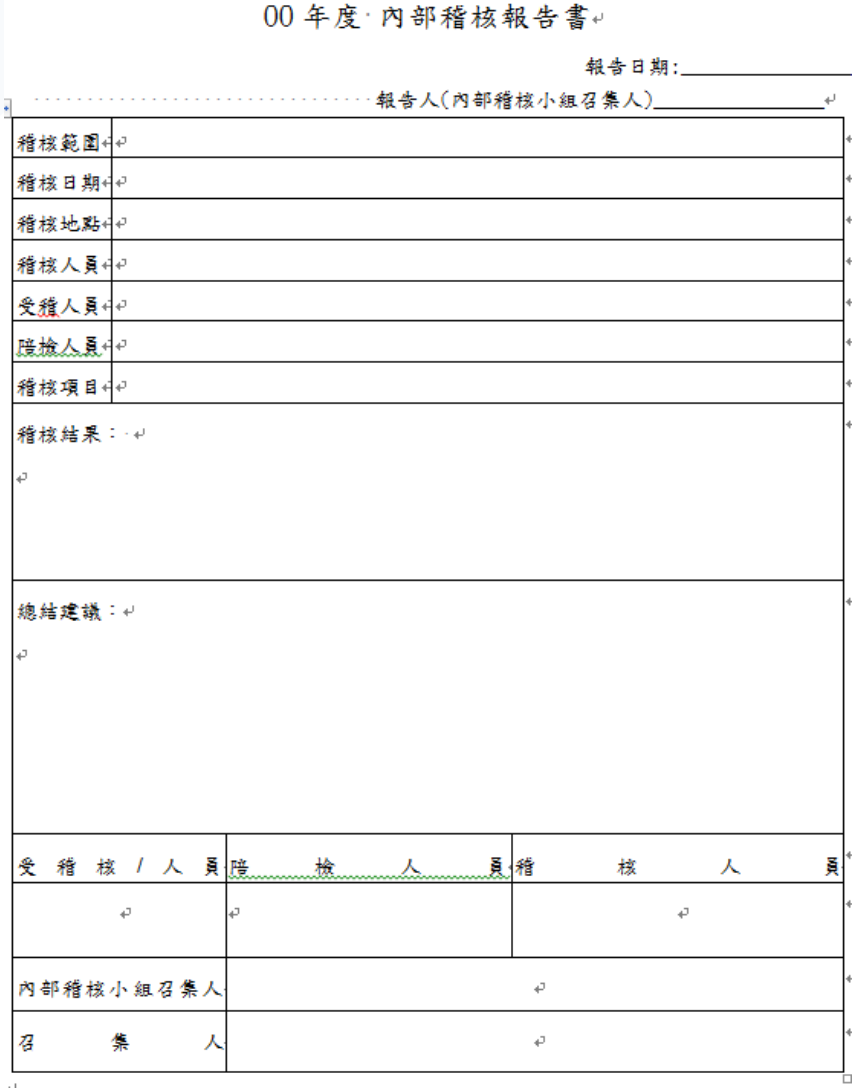
稽核查檢表

高雄醫學大學

個人資料管理稽核查檢表

序號	查‧‧‧檢‧‧‧細‧‧‧項	對應程序書	檢核表單	符合	不符合	不適用	說明
1	個人資料管理政策是否公告讓本校所有人員(包含員工、約聘雇人員、工讀生等)知悉？	個人資料保護管理政策					
2	是否訂定經校長核准宣告學生、教職員個人資料保護管理之政策?	個人資料保護管理政策					
3	個人資料管理政策每年是否進行審核，以符合個人資料保護法、主管機關規定之要求，確保個人資料管理實務作業之有效性?	個人資料保護管理政策					
4	是否已將個人資料保護管理執行委員會設置要點文件化，載明成立個人資料保護管理角色，同時清楚說明維護組織內部個人資料之管理作業權責?	個人資料保護管理政策					
5	各單位是否已指派個人資料保護管理人員?	個人資料保護管理政策					
6	是否已進行法規之清查並彙整成冊?	適用法規盤點程序					
7	是否定期檢視個人資料保護法及其他相關法令規範為最新之狀態，並公告更新?	適用法規盤點程序					
8	進行個人資料之新蒐集行為時，是否有程序或辦法規範新蒐集前之檢核作業，並留下相關檢核紀錄?	個人資料作業管理程序					
9	如有新蒐集行為時，是否於程序規範時間點內更新個人資料盤點表?	個人資料作業管理程序					
10	是否針對特種個人資料(醫療、基因、性生活、檢康檢查、犯罪前科)規範進行蒐集、利用及處理之檢核?	個人資料作業管理程序					
11	進行個人資料之新利用行為前，是否有程序或辦法規範利用合法性之檢核，並留下相關檢核紀錄?	個人資料作業管理程序					

個人資料管理稽核報告



00 年度 內部稽核報告書

報告日期:_____

報告人(內部稽核小組召集人)_____

稽核範圍	
稽核日期	
稽核地點	
稽核人員	
受稽人員	
陪檢人員	
稽核項目	
稽核結果：	
總結建議：	

受稽核人員	陪檢人員	稽核人員
內部稽核小組召集人		
召集人		

矯正措施單

▪ 附件十二、矯正措施單

矯正措施單

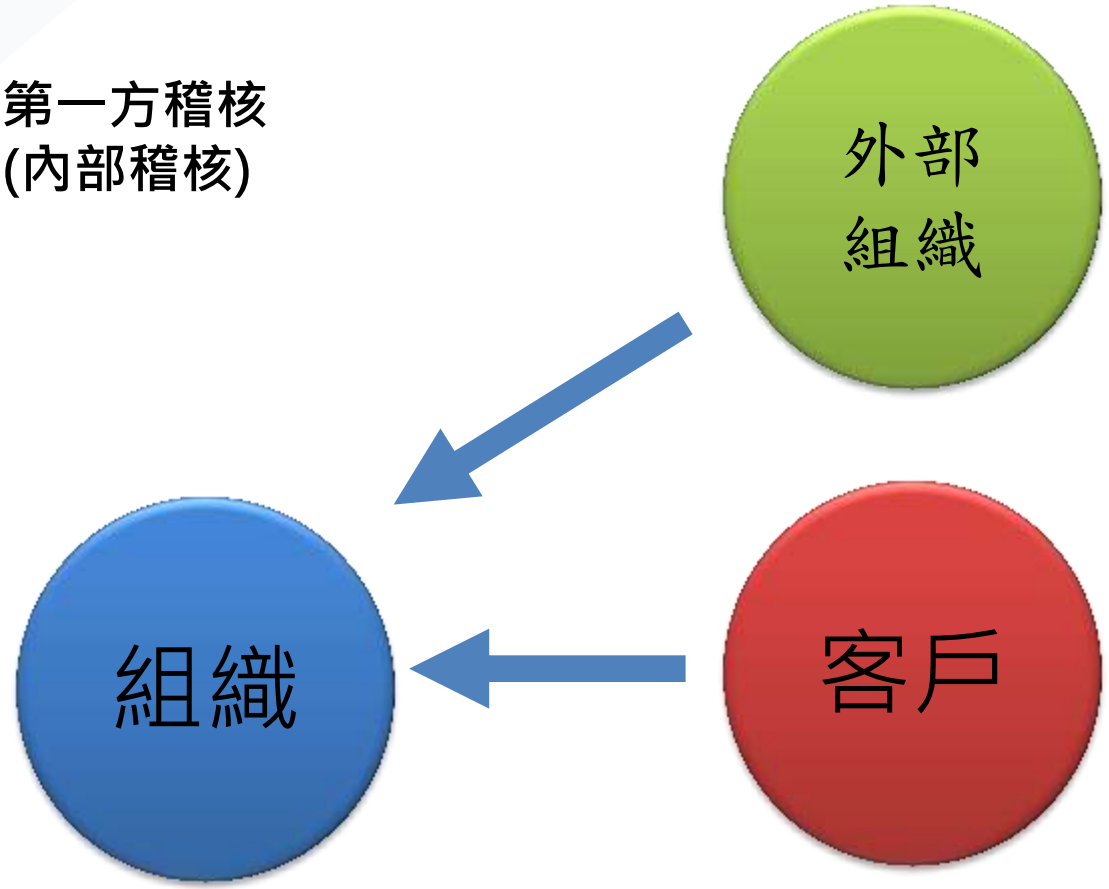
編號				年月日	
矯正措施執行單位		措施負責人(單位負責人)		提出糾正不符合人	

矯正計畫	「不符合內容」(記載為內部稽核報告書<糾正事項、要求改善指示事項>、機關外部糾正等)			
	「原因」(記載糾正事項發生的根本原因)			
	提出計畫日期:		核決計畫日期:	
	提出計畫人: (單位負責人)		計畫核決人: (個人資料保護管理負責人)	
	預定執行矯正措施完畢日期:		是否需要確認矯正措施:□是□否	
矯正措施執行結果	【執行矯正措施內容】			
	執行完畢日期:		核決日期:	
	提出計畫人: (單位負責人)		計畫核決人: (個人資料保護管理負責人)	
審核	【確認矯正措施效果及有效性】			
	執行日期:		核決日期:	
	報告人:		召集人	

稽核基本原理介紹

稽核形式

第一方稽核
(內部稽核)



第三方驗證稽核

ISO 的驗證

第二方稽核
(2nd Party audit)

客戶、上級、partner

稽核原理

3E

- Exist 存在
  - 文件、程序存在
- Execution 執行
  - 程序被執行
- Effectiveness 有效
  - 程序有效

2 段式稽核法

4.11 保存及銷毀　　個資保存及銷毀程序　　保存紀錄、銷毀紀錄

執行結果、紀錄

第一段稽核(文件審查)

包含任何法律要求以及組織要求的最小保存期限

- 個人資料作業管理程序
  - 個人資料保存管理
    - 各單位個資管理專人應負責查詢相關法律對於資料保存最小年限及最長年限之要求。

法規保存期限查詢紀錄

對象	法規名稱	最新版日期	保存內容	法律保存期限	
員工	**勞動基準法**	102.12.11.	勞工之姓名、性別、出生年月日、本籍、教育程度、住址、身分證統一號碼、到職年月日、工資、勞工保險投保日期、獎懲、傷病及其他必要事項	勞工離職後5年	第7條 Ⅰ雇主應置備勞工名卡，登記勞工之姓名、性別、出生年月日、本籍、教育程度、住址、身分證統一號碼、到職年月日、工資、勞工保險投保日期、獎懲、傷病及其他必要事項。 Ⅱ前項勞工名卡，應保管至勞工離職後五年。
			勞工之工資、工資計算項目、工資總額等事項	5年	第23條 Ⅰ工資之給付，除當事人有特別約定或按月預付者外，每月至少定期發給二次；按件計酬者亦同。 Ⅱ雇主應置備勞工工資清冊，將發放工資、工資計算項目、工資總額等事項記入。工資清冊應保存五年。
			勞工簽到簿或出勤卡	1年	第30條 Ⅰ勞工每日正常工作時間不得超過8小時，每二週工作總時數不得超過84小時。 Ⅱ前項正常工作時間，雇主經工會同意，如事業單位無工會者，經勞資會議同意後，得將其二週內二日之正常工作時數，分配於其他工作日。其分配於其他工作日之時數，每日不得超過二小時。但每週工作總時數不得超過48小時。 Ⅲ第1項正常工作時間，雇主經工會同意，如事業單位無工會者，經勞資會議同意後，得將八週內之正常工作時數加以分配。但每日正常工作時間不得超過八小時，每週工作總時數不得超過48小時。 Ⅳ第2項及第3項僅適用於經中央主管機關指定之行業。 Ⅴ雇主應置備勞工簽到簿或出勤卡，逐日記載勞工出勤情形。此項簿卡應保存1年。
	勞工退休金條例	96.7.4.	勞工名冊（包括勞工到職、離職、出勤工作紀錄、工資、每月提繳紀錄及相關資料）	自勞工離職之日起5年	第 21 條 Ⅰ雇主提繳之金額，應每月以書面通知勞工。 Ⅱ雇主應置備僱用勞工名冊，其內容應包括勞工到職、離職、出勤工作紀錄、工資、每月提繳紀錄及相關資料。

第二段稽核(實地審查)

- 個人資料作業管理辦法
  - 個人資料保存管理
    - 各單位個資管理專人應負責查詢相關法律對於資料保存最小年限及最長年限之要求
  - 法規保存期限查詢紀錄

- 稽核員發現點
  - 稽核員查證
    - 人事室辦識出
      - 員工資料應保存至勞工離職後5年
    - 實際查核
      - 離職員工資料為永久保存，未於勞工離職5年刪除
        - » 保留姓名、身分證字號、地址等欄位

稽核之目的、範圍

- 個資法為主?
- 合法 = 政策目標?
- 是否需要配合法令的查核?

Audit Process & Scope 稽核流程及範圍

- An audit programme which monitors and reviews the effectiveness and efficiency of the processing of personal information by the organization shall be planned, established and maintained, taking into account the policy.

  應計畫、建立、維護監視及審查組織處理個人資訊的有效性及效率的稽核計畫，並將組織的政策列入考量。

- The audit programme shall explicitly include any processing of high-risk personal information (see 4.2.2) and shall include any processing of personal information by other organizations (see 4.16).

  稽核計畫應該明確的包括任何處理高風險個人資訊(見 4.2.2) 及包括由其它組織所處理的個人資訊(見 4.1.6)

稽核計畫

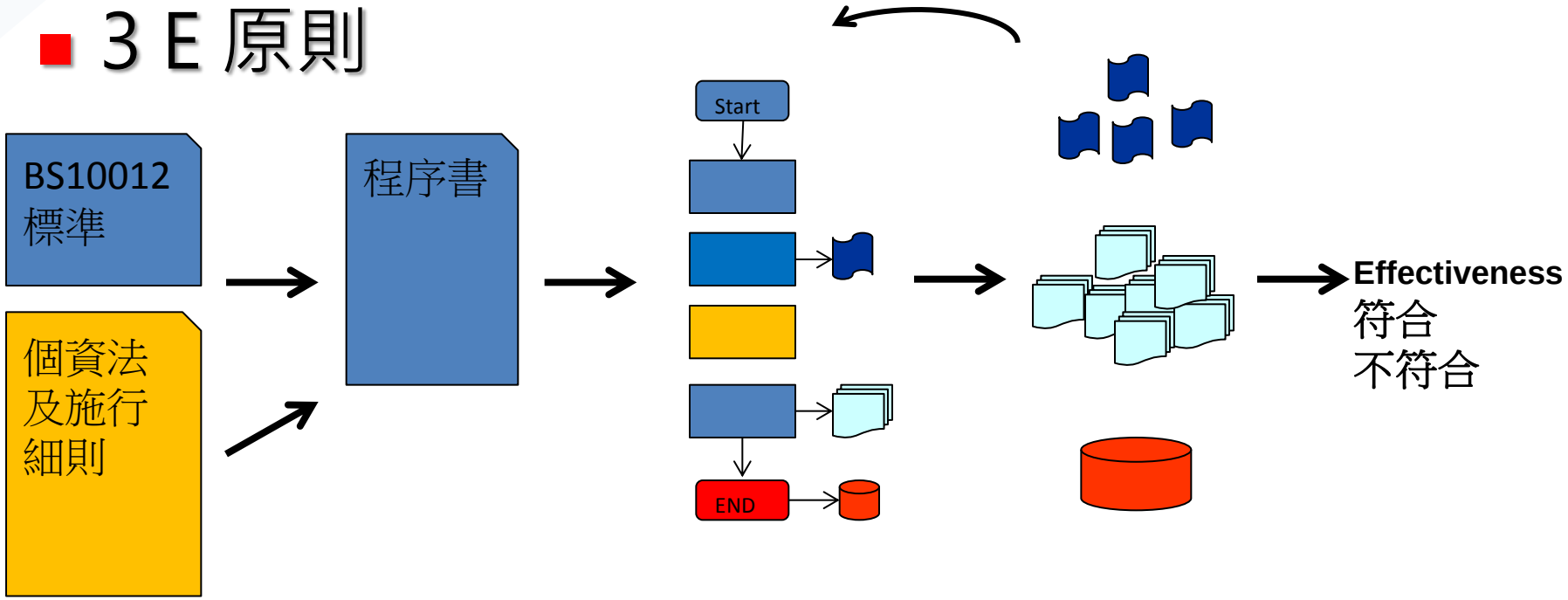
稽核計畫

地點	時程	受稽核單位	範圍/內容
XXX 會議室	09:00~09:10	全體人員	啟始會議
	09:40~10:00	個人資料保護安全執行委員會	個人資料保護安全政策
	10:30~12:00	教務處	
	12:00~13:30		中午休息
	13:30~14:20		
	14:20~14:50		
	15:10~15:40		
	16:30~17:00	內部稽核小組內部會議	稽核結果彙整
	17:00~17:30	全體	結束會議

抽樣及提問

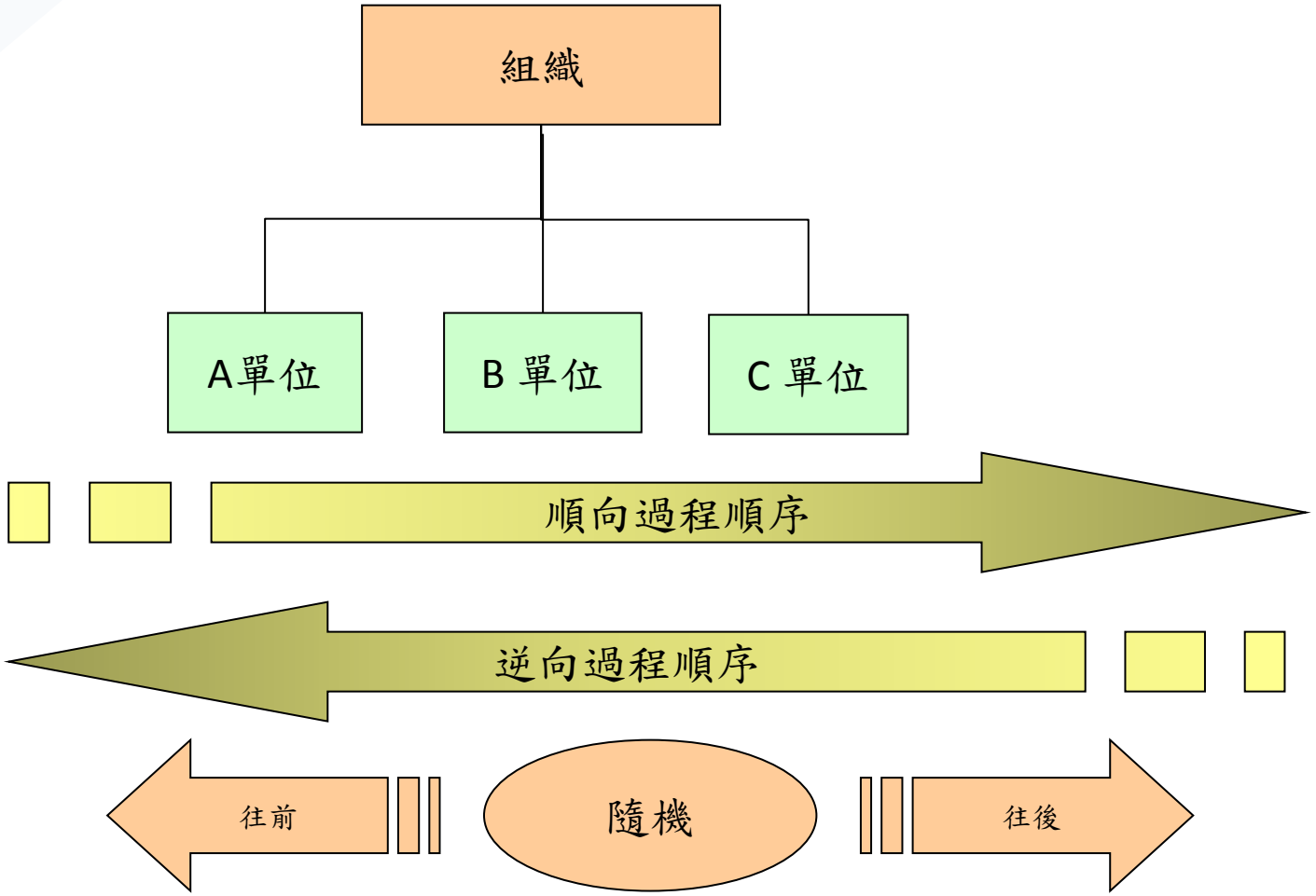
稽核標準流程

- P-D-C-A 過程導向中 D 的稽核方式
- 3 E 原則



文件審查 → 找出需查核流程或活動 → 抽樣 帶回流程

稽核技巧 – 流程抽樣



Check List and Questionnaire
稽核查檢表及稽核提問-1

- 查檢表
  - 功能:
    - 確保稽核員執行應稽核項目
    - 稽核作業能一致、有效
    - 稽核流程/軌跡安排
    - 時間安排
  - 格式
    - 為”是否”問題
    - 僅為稽核員使用
    - 不適用於稽核提問

程序規範

Yes/No 問題

稽核查檢表

高雄醫學大學

個人資料管理稽核查檢表

序號	查‧‧‧檢‧‧‧細‧‧‧項	對應程序書	檢核表單	符合	不符合	不適用	說明
1	個人資料管理政策是否公告讓本校所有人員(包含員工、約聘雇人員、工讀生等)知悉？	個人資料保護管理政策					
2	是否訂定經校長核准宣告學生、教職員個人資料保護管理之政策?	個人資料保護管理政策					
3	個人資料管理政策每年是否進行審核，以符合個人資料保護法、主管機關規定之要求，確保個人資料管理實務作業之有效性?	個人資料保護管理政策					
4	是否已將個人資料保護管理執行委員會設置要點文件化，載明成立個人資料保護管理角色，同時清楚說明維護組織內部個人資料之管理作業權責?	個人資料保護管理政策					
5	各單位是否已指派個人資料保護管理人員?	個人資料保護管理政策					
6	是否已進行法規之清查並彙整成冊?	適用法規盤點程序					
7	是否定期檢視個人資料保護法及其他相關法令規範為最新之狀態，並公告更新?	適用法規盤點程序					
8	進行個人資料之新蒐集行為時，是否有程序或辦法規範新蒐集前之檢核作業，並留下相關檢核紀錄?	個人資料作業管理程序					
9	如有新蒐集行為時，是否於程序規範時間點內更新個人資料盤點表?	個人資料作業管理程序					
10	是否針對特種個人資料(醫療、基因、性生活、檢康檢查、犯罪前科)規範進行蒐集、利用及處理之檢核?	個人資料作業管理程序					
11	進行個人資料之新利用行為前，是否有程序或辦法規範利用合法性之檢核，並留下相關檢核紀錄?	個人資料作業管理程序					

Check List and Questionnaire
稽核查檢表及稽核提問-2

- 稽核提問
  - 功能:
    - 協助稽核員完成稽核查檢表之判定
    - 可發展出一系列的問題而形成一稽核軌跡以確認在查檢表中某一特定的問題
  - 格式
    - 開放性問題
    - How, where, who, when, why, what, what if

稽核技巧 – 採用面談

1. 應讓被稽核者保持輕鬆，詢問簡短的問題
2. 說明面試的原因及記錄面談的內容
3. 以正確的態度，音調，肢體語言，及面部表情
4. 微笑、傾聽及看對方
5. 避免中斷
6. 避免優越性的評論
7. 適度的稱讚

稽核技巧 – 提問

- 稽核的品質高度可依賴於稽核員的提問技巧
- 適當的提問有助於稽核目的的達成
- 被稽核者不應對稽核問題感到壓力
- 所提問的問題應聚焦於正在稽核的區域及稽核的範圍內

稽核技巧 – 提問

- 一次只問單一的問題，不要問一連串的問題
- 聚焦於稽核範圍內被稽核者的工作
- 試著運用其專業語言或可理解的領域
- 提問開放性的問題
- 不要催促被稽核者

提問方法

- 開放式
  - 這類問題可得到更詳細的答案而非只有對或錯
    What, How, When, What if (假設性), Where, Why....
- 封閉式
  - 這類問題只需表達對或錯
- 引導式（“誘導式”）不允許
- 反覆式
  - 對類似的主題有多個問題

稽核查檢表設計

- 請依據各組分配到之”個人資料檔案安全維護計畫”內容，設計問項。

高雄醫學大學

個人資料管理稽核查檢表

序號	查檢細項	對應程序書	檢核表單	符合	不符合	不適用	說明
1	個人資料管理政策是否公告讓本校所有人員(包含員工、約聘雇人員、工讀生等)知悉？	個人資料保護管理政策					
2	是否訂定經校長核准宣告學生、教職員個人資料保護管理之政策?	個人資料保護管理政策					
3	個人資料管理政策每年是否進行審核，以符合個人資料保護法、主管機關規定之要求，確保個人資料管理實務作業之有效性?	個人資料保護管理政策					
4	是否已將個人資料保護管理執行委員會設置要點文件化，載明成立個人資料保護管理角色，同時清楚說明維護組織內部個人資料之管理作業權責?	個人資料保護管理政策					
5	各單位是否已指派個人資料保護管理人員?	個人資料保護管理政策					

稽核技巧 – 做筆記

- 記錄客觀的證據
- 記錄稽核發現點
- 為稽核報告做筆記
- 有助於記憶和追蹤
- 可能讓其他稽核員再度使用或稍後調查

筆記應記載事項

- D Document 文件 (程序書、標準)
- E Evidence 證據(抽樣...樣本編號)
- F Fact 事實 (大致發現狀況...，人事時地物)

稽核技巧 – 訪談

- 時間管理:
  - 定期檢查進度
  - 有效地管理延誤的事項

- 離開面試考量:
  - 結論是否有發現點
  - 取得稽核發現點的同意
  - 迅速離開稽核區域

稽核發現點

不符合事項的範例

陸、個人資料委外管理程序，委外業務承辦人員應以合約條款或書面確認方式，確認受委託者知悉本校委託蒐集、處理或利用之個人資料範圍、類別、特定目的及期間。

稽核中**觀察到** A單位與XYZ廠商簽訂之合約，未包括委託蒐集、處理或利用之個人資料範圍、類別、特定目的及期間之內容。

這表示稽核員有看到。
不只是聽說，也沒有任何懷疑，而是他們親自看見!

觀察事項/改進的機會

- **觀察事項是指:**

發現到一個事實可能在管理系統上有負面的影響

- **改進的機會點是指:**

- 建議
- 觀察到並非不符合的情形，但所達到的結果並不理想.

稽核發現點

- 評估在稽核工作中，分析觀察和分類所產生的紀錄證據。客觀的證據將提供真實的稽核報告。

- 確認事實成立，和被稽核者或稽核小組長討論所關切的事項，收集所有的證據，提供實際觀察的簡明紀錄，說明何時、何地、何事、何人、及如何。

想想看：

稽核發現，個人資料保護管理政策未依程序規定被審查和經由高階管理層核准，雖然這政策已被溝通和執行。

稽核報告及不符合事項報告

不符合報告

- 一個清楚且簡明的記錄說明:
  - 不符合事項的本質
  - 支持這不符合事項的證據
  - 所不符合的條款要求
  - 發現不符合事項的地點
  - 嚴重性或衝擊
- 使受稽核者清楚了解不符合事項的發現內容

不符合報告撰寫

- D Document 文件 (程序、標準)
- E Evidence 證據(抽樣...)
- F Fact 事實 (發現狀況...)

稽核報告書

稽核報告書

- 內部稽核作業之總結
  - 內部稽核執行日期
  - 內部稽核執行人員(稽核人員)
  - 受稽核單位
  - 稽核結果 (不符合事項撰寫)

個人資料管理稽核報告

個人資料管理稽核報告

查檢範圍	
查檢日期	
查檢地點	
稽核人員	
受稽人員	
陪檢人員	
查檢編號	
查檢項目	

稽核結果：

總結建議：

受稽核部門/人員	稽核分組（部門）/人員

個人資料管理稽核分組組長	
個人資料管理召集人	

稽核後續處理

矯正措施包括

- 未符合事項說明
  - 未符合事項提出人員應詳細說明未符合事項
- 原因分析
  - 根據未符合事項說明，權責單位主管應指派相關人員對於未符合事項進行分類及原因之分析
- 矯正措施
  - 針對原因分析提出解決方案

矯正措施單

矯正措施單

編號				年月日	
矯正措施執行單位		措施負責人（單位負責人）		提出糾正不符合人	

矯正計畫	「不符合內容」（記載為內部稽核報告書<糾正事項，要求改善指示事項>，機關外部糾正等）			
	「原因」（記載糾正事項發生的根本原因）			
	提出計畫日期：		核決計畫日期：	
	提出計畫人：（單位負責人）		計畫核決人：（個人資料保護管理負責人）	
	預定執行矯正措施完畢日期：		是否需要確認矯正措施：□是 □否	
矯正措施執行結果	【執行矯正措施內容】			
	執行完畢日期：		核決日期：	
	提出計畫人：（單位負責人）		計畫核決人：（個人資料保護管理負責人）	
審核	【確認矯正措施效果及有效性】			
	執行日期：		核決日期：	
	報告人：		召集人	