國立清華大學
個人資料生命週期與個資保護作業

2016.11.30

王俊凱 協理

財團法人中華民國國家資訊基本建設產業發展協進會
National Information Infrastructure Enterprise Promotion Association

NII 產業發展協進會
☏ (02) 2508-2353
✉台北市松江路 317 號 7 樓

課程大綱

1. 個人資料保護與ISMS
2. 個資保護實作
3. 個人資料管理制度介紹
4. 問題與討論

課程大綱

1. 個人資料保護與ISMS
2. 個資保護實作
3. 個人資料管理制度介紹
4. 問題與討論

落實安全維護措施(細則第12條)

保護標的：
防止個人資料被竊取、竄改、毀損、滅失或洩漏

1	配置管理之人員及相當資源
2	界定個人資料之範圍
3	個人資料之風險評估及管理機制
4	事故之預防、通報及應變機制
5	個人資料蒐集、處理及利用之內部管理程序
6	資料安全管理及人員管理
7	認知宣導及教育訓練
8	設備安全管理
9	資料安全稽核機制
10	使用紀錄、軌跡資料及證據保存
11	個人資料安全維護之整體持續改善

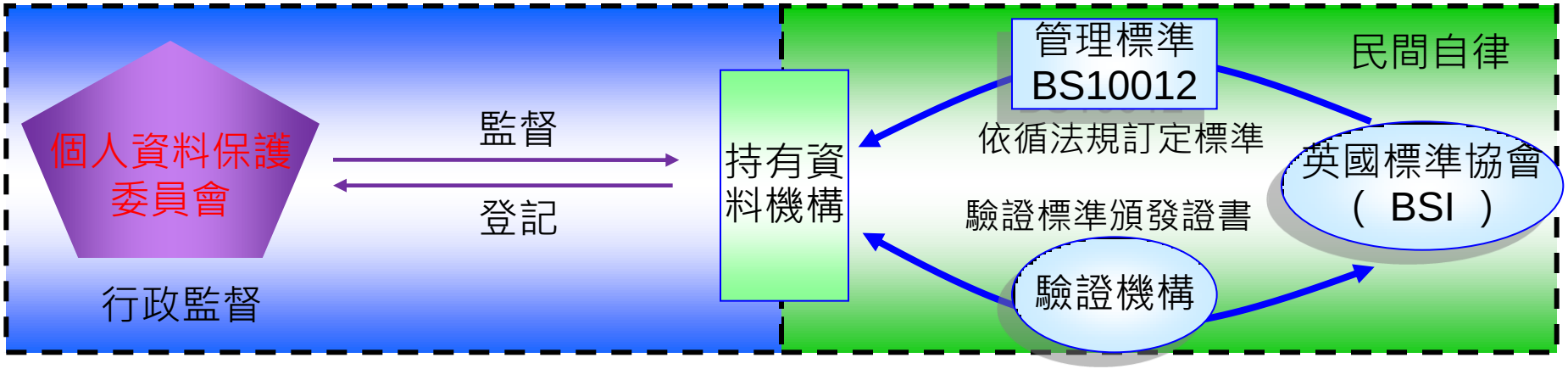
比例原則：必要措施以所須支出之費用與所欲達成之個人資料保護目的符合適當比例者為限。

此11項安全措施內容似參照英國 BS 10012:2009 及日本 JISQ 15001:2006 等個人資料管理系統之規範，以 P-D-C-A 循環之概念予以建立。

個人資訊管理標準BS 10012

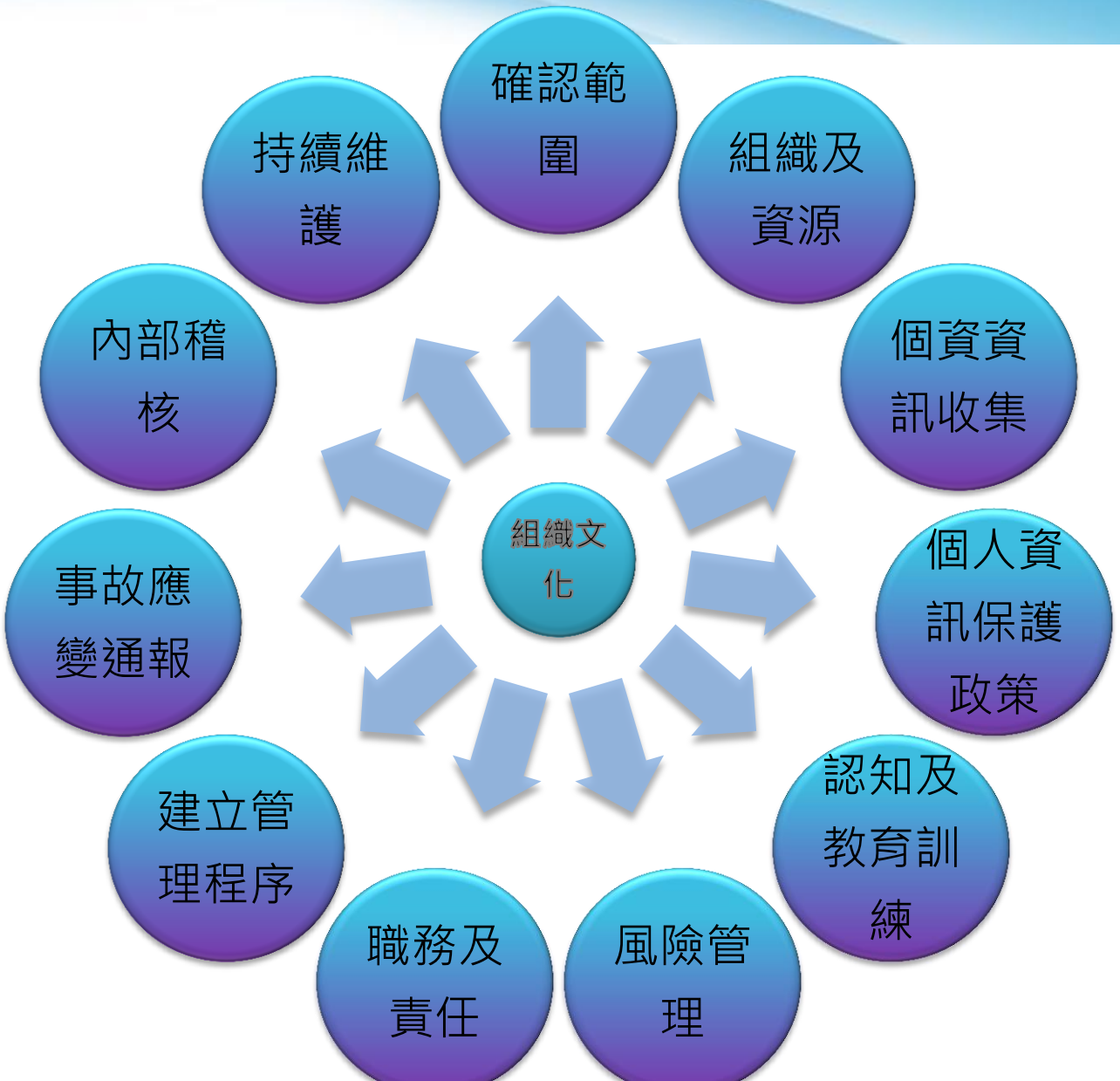
- 英國於1998年將歐盟之「個人資料保護指令」與「電子通訊隱私指令」內國法化為「個人資料保護法」（The Data Protection Act 1998）。並由個資保護委員（Information commissioner ）監督法令執行。
- 2001、2007修正擴大個人資料適用範圍，引發適用困擾。
- 英國標準協會（BSI）於2009年5月順應企業需要正式推出一套個人資料管理之標準（BS10012 ），協助企業遵循英國個人資料保護法。

英國個人資料保護法(The Data Protection Act)



資料參考來源：經濟部 www.nii.org.tw

BS10012要求


確認範圍
組織及資源
個資資訊收集
個人資訊保護政策
認知及教育訓練
風險管理
職務及責任
建立管理程序
事故應變通報
內部稽核
持續維護
組織文化

英國標準BS 10012(PIMS) V.S 國內個人資料保護法

BS 10012相關管理規範摘要	國內個人資料保護法相關管理規範摘要	
1.善盡告知義務	1.善盡告知義務	11.個資定義不同(未包含種族、政黨等)
2.依特定目的蒐集個資	2.依特定目的蒐集個資	12.提供閱覽或製給複製本
3.公正且合法使用個資	3.公正且合法使用個資	13.規範特種資料不得蒐集
4.保護個人隱私相關項目	4.保護個人隱私相關項目	14.區分公務機關與非公務機關之處理方式
5.確保存取控制之安全	5.確保存取控制之安全	15.具團體訴訟機制
6.確保資料之正確性	6.確保資料之正確性	
7.確保資料傳輸之安全	7.確保資料傳輸之安全	
8.確保個人修改之權利	8.確保個人修改之權利	
9.妥善處理抱怨與申訴	9.妥善處理抱怨與申訴	
10.落實委外安全管理	10.落實委外安全管理	

BS 10012與ISO 27001之關聯

BS 10012 (管理要求)

蒐集 → 處理 → 利用 → 傳輸 → 銷毀

BS 10012 (4.13)(安全議題--安全控管、儲存與處理、傳輸、存取控制、安全評估、資安事故管理）

ISO 27001(技術支援)

BS 10012與ISO 27001之關聯

課程大綱

1. 個人資料保護與ISMS
2. 個資保護實作
3. 個人資料管理制度介紹
4. 問題與討論

如何降低個資法之風險?

公務機關

- §28 公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權力者，負損害賠償責任。**但損害因天災、事變或其他不可抗力所致者**，不在此限。
- §18 公務機關保有個人資料檔案者，**應指定專人辦理安全維護事項**，防止個人資料被竊取、竄改、毀損、滅失或洩漏。
- §31 損害賠償，除依本法規定外，**公務機關適用國家賠償法之規定**，非公務機關適用民法之規定。
- “法定”職務範圍較大(細則第10條)
- **施行細則第十二條第二項說明「落實安全維護措施」有十一項。**

非公務機關

- §29 非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。**但能證明其無故意或過失者**，不在此限。
- §50 非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定受罰鍰處罰時，**除能證明已盡防止義務者外**，應並受同一額度罰鍰之處罰。
- §27非公務機關保有個人資料檔案者，**應採行適當之安全措施**，防止個人資料被竊取、竄改、毀損、滅失或洩露。
- §31 損害賠償，除依本法規定外，公務機關適用國家賠償法之規定，**非公務機關適用民法之規定**。
- “法定”義務範圍較小(細則第11條)
- **施行細則第十二條第二項說明「落實安全維護措施」有十一項。**

落實安全維護措施（細則第12條）

保護標的：
防止個人資料被竊取、竄改、毀損、滅失或洩漏

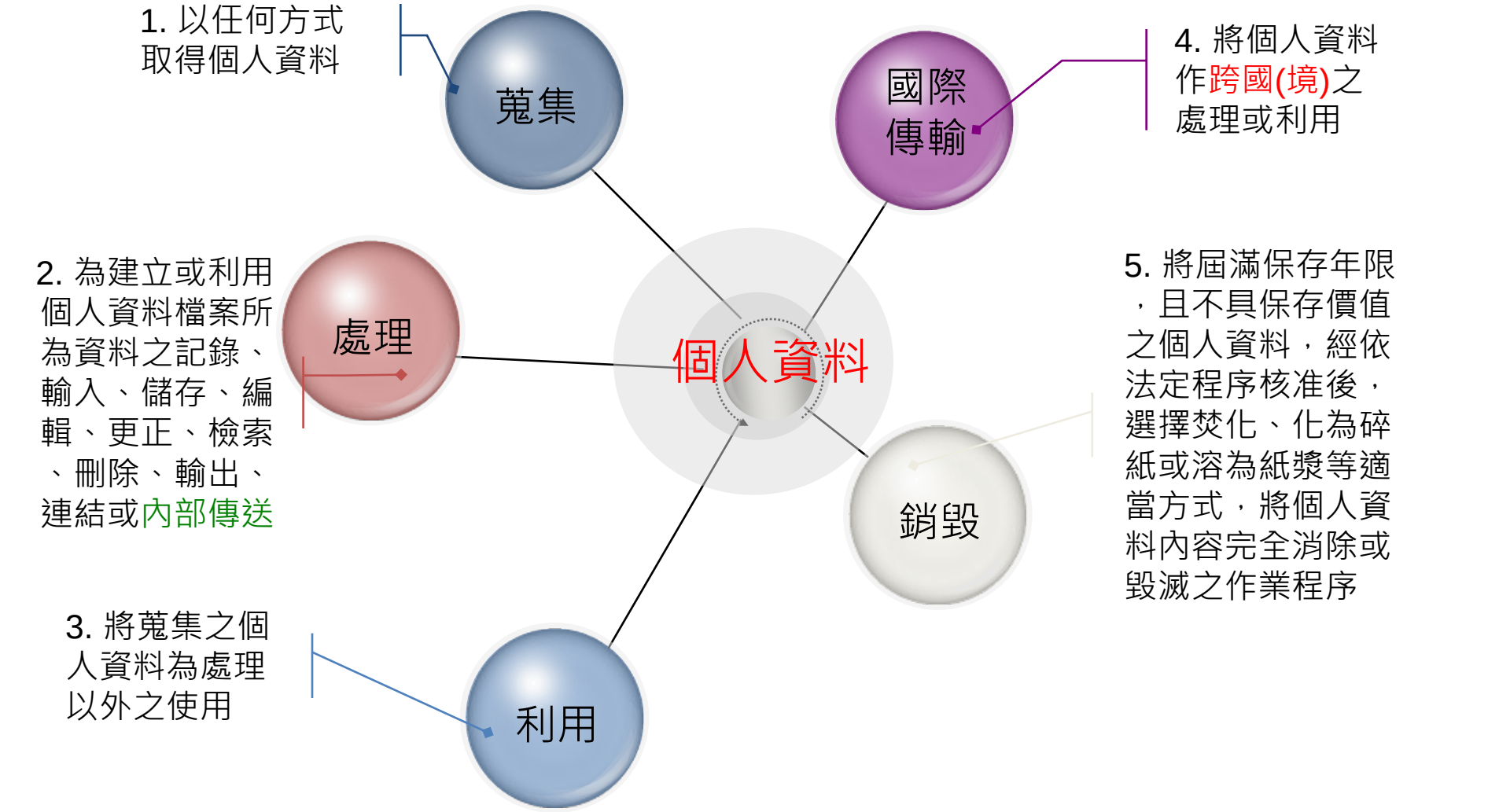
1	配置管理之人員及相當資源
2	界定個人資料之範圍
3	個人資料之風險評估及管理機制
4	事故之預防、通報及應變機制
5	個人資料蒐集、處理及利用之內部管理程序
6	資料安全管理及人員管理
7	認知宣導及教育訓練
8	設備安全管理
9	資料安全稽核機制
10	使用紀錄、軌跡資料及證據保存
11	個人資料安全維護之整體持續改善

比例原則：必要措施以所須支出之費用與所欲達成之個人資料保護目的符合適當比例者為限。

此11項安全措施內容似參照英國 BS 10012:2009 及日本 JISQ 15001:2006 等個人資料管理系統之規範，以 P-D-C-A 循環之概念予以建立。

個人資料檔案盤點作業(續)

(細則§12 /2項)



個人資料檔案盤點重點在於個資之生命週期

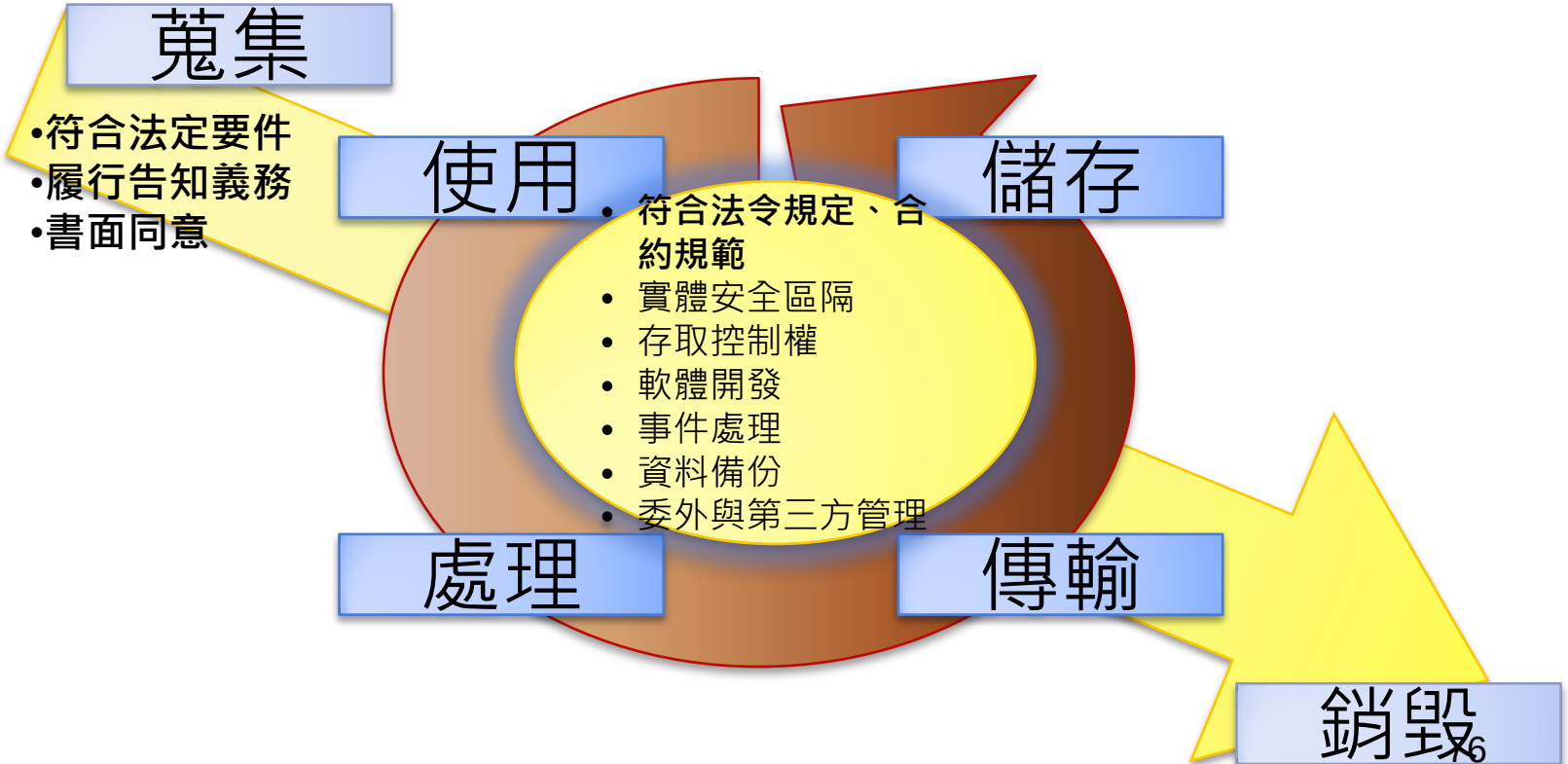
資產盤點及衝擊分析
（細則§12 /2項）

- 顧問藉由工作職掌進行作業流程訪談建立作業流程訪談記錄及個人資產清冊。
- 藉由清冊之內容依據定義之衝擊價值進行分析。

資產編號	流程名稱	個人資料檔案名稱	資料形式	法律依據	特定目的	個人資料類別	個人資料之範圍	有否特種資料？何種特種資料？	有無監督管理之非公務機關及其名稱	蒐集			處理 (指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送)		利用 (將蒐集之個人資料為處理以外之使用)				保存		銷毀		揭露			現有控制	衝擊值
										來源	方式	單位	方式	單位	期間	地區	對象	方式目的	保有單位及聯絡方式	期限	形式	頻率	對象	方式目的	個資範圍		

風險評鑑
（細則§12 /3項）

- 顧問藉由流程訪談中所獲知之現行管控方式，依據個人資料在不同的生命週期中，及不同的風險構面，進行風險評鑑。



個資風險判斷流程圖

個資法適用對象及範圍

第2條：包括各行各業及個人

第4條：受委託者視同委託機關

WHY?
特定目的
- 告知義務
- 法務部公告182項特定目的

WHO?
單位定性
- 公務機關
- 非公務機關

HOW?
執行行為
- 蒐集
- 處理
- 利用
- 傳輸
- 保存
- 銷毀

WHAT?
違法代價
- 通知義務
- 法律責任

不適用個資法之情況(個資法第51條第1項)

1.自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。

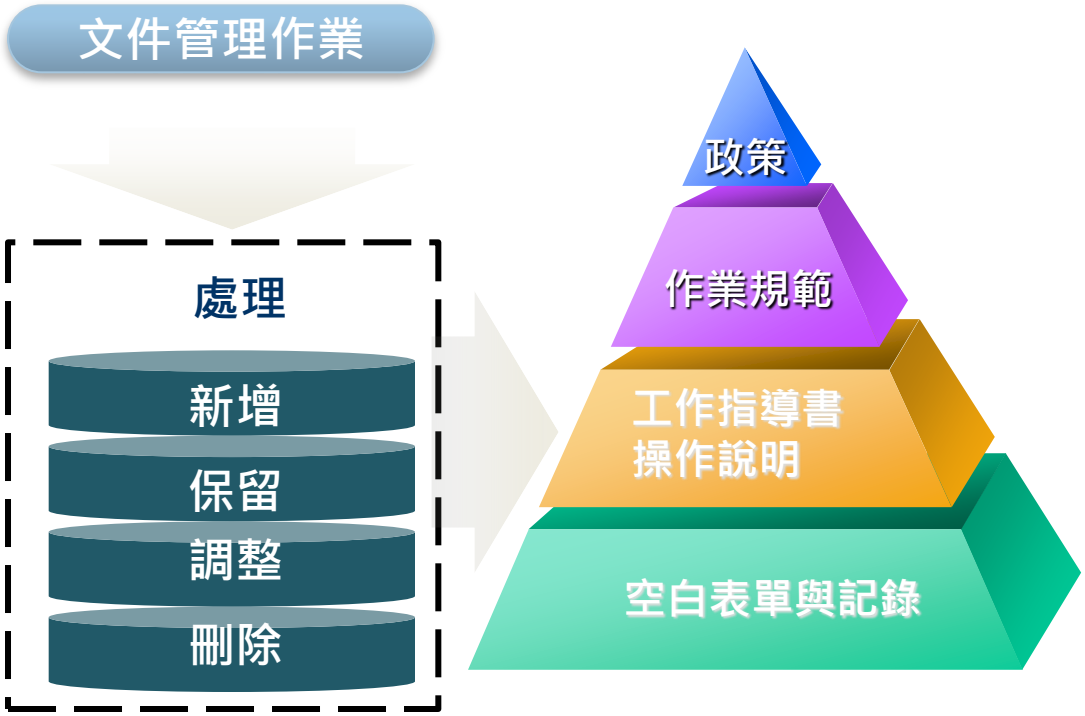
2.於公開場所或公開活動中所蒐集、處理或利用未與其他個人資料結合之影音資料。

風險處理
（細則§12 /3項）

- 依據風險評鑑的結果進行可接受風險分析，並將不可接受風險進行風險處理（依現況提供改善建議）。

建立管理制度
（細則§12 /5項）

- 依據個人資料保護法、施行細則及個人資訊管理制度（BS 10012）國際標準要求建立管理制度文件。



個資法 + BS10012:2009

蒐集

處理

利用

告知義務
特定目的
法律依據
書面同意

隱私權政策聲明書
個資保護管理政策
威脅及弱點評估表
個資生命週期管理

保存：適當安全維護措施

配置管理人員及相當資源
界定個人資料之範圍
個人資料風險評估及管理
事故預防通報及應變制度
蒐集處理及利用內部管理
資料安全管理與人員管理
認知宣導及教育訓練
設備安全管理
資料安全稽核
使用記錄軌跡及證據保存
安全維護之整體持續改善

個人 資料保護組織委員會
個人資料清冊
個人資料風險評鑑與管理
保護應變及處理作業辦法
個人資料生命週期管理
個人資料安全控管
認知宣導與教育訓練
個人資料安全控管
個人資料稽核作業
表單記錄及內稽底稿
個資矯正預防

安全維護計劃終止處理方法

當事人權利行使：個資法第3條

委外

預定蒐集處理利用個資範圍、類別及期間
適當安全維護措施
複委託/保留指示/補救措施

委外管理
實質審查/書面協議
委外廠商保密切結書
定期稽核

定期記錄

公正第三方驗證/第三方法律事務所適法性評估

教育部函文

主旨：檢送「教育體系個人資料安全保護基本措施及作法」(如附件)，請查照並轉知所屬(含所管非公務機關)。

說明：

一、本部為使所屬各機關(構)、各級學校及本部所管之各非公務機關可資參考之個人資料安全保護基本原則，故依據「個人資料保護法」、「個人資料保護法施行細則」(已包含個資法施行細則第12條第2項所列技術上及組織上等適當安全維護措施事等相關規定為基礎引申訂定之。

二、本行政指導臚列「人員管理」、「作業管理」、「物理環境管理」、「技術管理」「認知宣導及教育訓練」、「紀錄機制」六大面向之基本措施及作法。

三、本部所屬各機關(構)、各級學校及本部所管之各非公務機關可參考本行政指導之相關管理措施，以保護內部相關作業程序所產生或經手之各種形式（含書面或電子）之個人資料。

「教育體系個人資料安全保護基本措施及作法」配合重點

學校應依據「教育體系個人資料安全保護基本措施及作法」，辦理以下事項：

1. 人員管理措施
2. 作業管理措施
3. 物理環境管理措施
4. 技術管理措施
5. 認知宣導及教育訓練
6. 紀錄機制

人員管理措施

人員管理措施	說明及作法
一. 指定蒐集、處理及利用個人資料個別作業 (以下簡稱「作業」) 流程之負責人員。 二. 就個別作業設定所屬人員不同之權限並控管之，以一定機制管理其權限，且定期確認權限內容設定之適當與必要性。 三. 要求所屬人員負擔相關之保密義務。	一. 針對人員管理之部分，首先應先確認實際進行個人資料之蒐集、處理及利用之負責人員為何，方可確認相關管理程序之權責歸屬。 二. 各機關所屬人員與個人資料相關之各項作業，若有設定權限控管之必要，則應以一定機制管理之，並確認其權限設定是否適當或必要。避免人員取得不適當之權限，得以接觸非於作業必要範圍內之個人資料。 三. 各機關應要求其所屬人員負擔相關之保密義務，使所屬人員能明瞭其責任，必要時亦可以訂定契約條款之方式為之，以作為相關權責之紀錄。

作業管理措施

作業管理措施	說明及作法
一. 運用電腦或自動化機器相關設備蒐集、處理或利用個人資料時，訂定使用可攜式設備或儲存媒介物之規範。	一. 使用可攜式儲存媒體，可能提高處理個人資料之電腦及相關設備遭受惡意程式攻擊及個人資料外洩之風險，因此若有使用可攜式儲存媒體之情況，應訂定相關使用規範。
二. 針對所保有之個人資料內容，如有加密之需要，於蒐集、處理或利用時，採取適當之加密機制。	二. 針對個人資料處理之不同態樣，包括儲存、傳輸及備份之狀況，如資料有加密之必要，即應採取適當之加密機制。
三. 作業過程有備份個人資料之需要時，比照原件，依本法規定予以保護之。	三. 針對有備份必要之個人資料，除有必要時採取加密機制，儲存備份資料之媒體亦應以適當方式保管，且定期進行備份資料之還原測試，以確保備份之有效性。
四. 個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物，嗣該媒介物於報廢或轉作其他用途時，採適當防範措施，以免由該媒介物洩漏個人資料。	四. 儲存個人資料之媒體於廢棄或移轉與他人前，應確實刪除媒體中所儲存之資料，或以物理方式破壞之，以避免資料不當外洩。
五. 委託他人執行前款行為時，對受託人依本法施行細則第八條規定為適當之監督，並明確約定相關監督事項與方式。	五. 說明委託他人執行前款行為時，對受託人依本法施行細則第八條規定為適當之監督，並明確約定相關監督事項、方式、義務及責任。

物理環境管理措施及技術管理措施

物理環境管理措施	說明及作法
一. 依作業內容之不同，實施必要之門禁管理。 二. 妥善保管個人資料之儲存媒體。	在實體之物理環境管理方面，各機關亦應針對不同之作業內容、作業環境及個人資料之種類與數量，實施必要之門禁管理，以適當方式或場所保管個人資料之儲存媒體。

技術管理措施	說明及作法
一. 於電腦、相關設備或系統上設定認證機制，帳號及密碼使其具備一定安全之複雜度並定期更換密碼。 二. 於處理個人資料之電腦系統中安裝防毒軟體，並定期更新病毒碼。 三. 對於電腦作業系統及相關應用程式之漏洞，定期安裝修補之程式。 四. 具備存取權限之終端機不得安裝檔案分享軟體。 五. 定期檢查處理個人資料之資訊系統之使用狀況及個人資料存取之情形。	一. 認證機制使用密碼之方式時，並應有適當之管理方式，並定期測試權限機制之有效性。 二. 電腦系統中安裝防毒軟體，並定期更新病毒碼。 三. 避免惡意程式與系統漏洞對作業系統之威脅。 四. 檔案分享軟體之控制。 五. 檢查系統之使用狀況與個人資料存取之情形。

認知宣導及教育訓練與紀錄機制

認知宣導及教育訓練	說明及作法
各機關應對所屬人員施以認知宣導及教育訓練，使其明瞭個人資料保護相關法令之要求、所屬人員之責任範圍及各種作業程序。	為落實執行相關管理程序，各機關應透過認知宣導及教育訓練使所屬人員均能明瞭個人資料保護相關法令之要求、所屬人員之責任範圍及各種作業程序。

紀錄機制	說明及作法
一. 個人資料交付、傳輸之紀錄。 二. 確認個人資料正確性及更正之紀錄。 三. 提供當事人行使權利之紀錄。 四. 所屬人員權限新增、變動及刪除之紀錄。 五. 個人資料刪除、廢棄之紀錄。 六. 教育訓練之紀錄。	為確認所訂定之相關程序是否落實執行，以及釐清個人資料於蒐集、處理及利用過程之相關權責，各機關應保存相關紀錄以供查驗。

課程大綱

1. 個人資料保護與ISMS
2. 個資保護實作
3. 個人資料管理制度介紹
4. 問題與討論

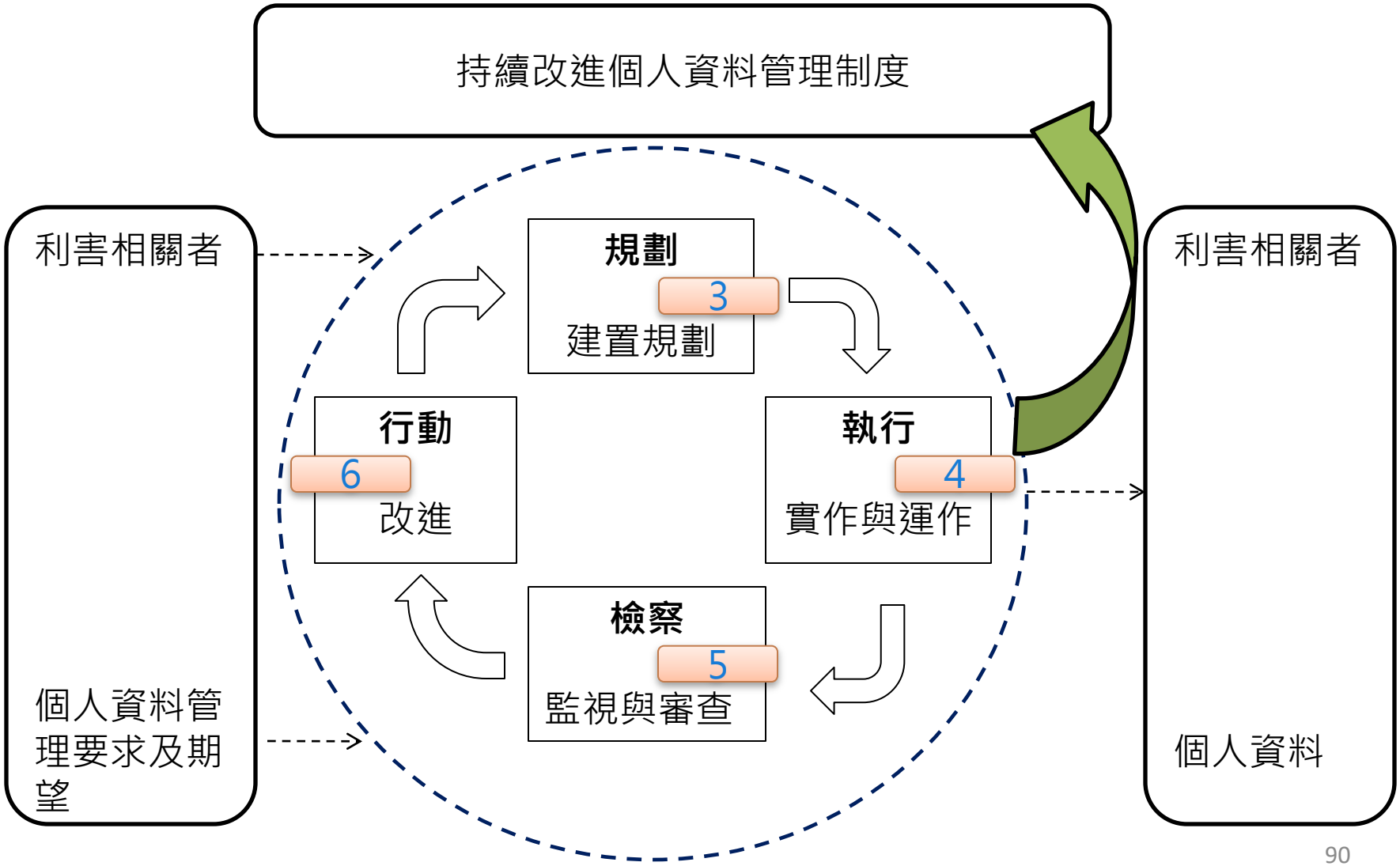
國內個資管理現況

ISO 29100	• 資訊機房個資管理框架標準，非適用全組織 • 個資法要求應全組織適用，且缺乏PDCA要求(施行細則)
符合性查驗	• 查核標準由各查核公司自訂 • 查核標準不一且缺乏PDCA要求(施行細則)
TIPIAS	• 電子商務(無店舖)業者自訂個資管理標準(經濟部商業司) • 標準制訂、顧問、驗證、訓練均同一單位，似缺乏獨立性
BS 10012	• 英國國家標準，法務部施行細則似參考此標準 • 需要修正英國個資定義以符合國內個資定義
ISO 27001	• 目前建置範圍侷限資訊單位或更小，管理制度面向需增加蒐集及部分利用階段適法性要求，另增加針對個資資產盤點及風險評鑑之要求(施行細則)

BS 10012 個人資料管理系統

- **BS 10012「資料保護–個人資訊管理系統之要求（Data protection–Specification for a personal information management system）」，其中，資料保護法案所要求應遵守的8項資料保護原則，非常適合各組織作為制定個人資料保護的參考，內容說明如下：**
  - 個人資料不可以非法或不公正方式蒐集、處理。
  - 個人資料應限於以特定目的之方式蒐集、處理。
  - 個人資料應以充分、相關，而非逾越其原本之目的處理。
  - 個人資料應求準確，並在必要時及時更新。
  - 個人資料之保存，不得超過其原定目的之保存期限。
  - 個人資料之處理，應依照當事人之權限及法令規範。
  - 組織應採取適當的資料保護技術和措施，防止個人資料遺失或毀壞。
  - 個人資料不得轉移到歐洲經濟區以外的國家或地區。

Plan-Do-Check-Act (PDCA) 循環



敏感性個人資料

與個人有關的個人資訊如：

- (a) 種族或人種,
- (b) 政治觀點,
- (c) 宗教或其他信仰,
- (d) 會員資格,
- (e) 身體或精神狀態,
- (f) 性生活,
- (g) 委員會或委員會的任何指控的罪行,
- (h) 任何犯罪的的訴訟，或已承認犯行，處置這類訴訟或任何此類訴訟的法院的判決。

Data Protection Act 1998 (DPA)[1]

規劃個人資料管理系統PIMS

- 3.1 建立和管理 PIMS
- 3.2 PIMS 的範圍和目標
- 3.3 個人資料管理政策
- 3.4 政策內容
- 3.5 職責和歸責性
- 3.6 資源提供
- 3.7 將PIMS嵌入組織文化

規劃個人資料管理系統PIMS

- **3.1 建立和管理 PIMS**
  - 組織應建立、實作、維護及持續改進PIMS以符合3.2～3.7的要求

- **3.2 PIMS 的範圍和目標**
  - a) 個人資料管理需求
  - b) 組織的目標與義務
  - c) 組織可接受的風險等級
  - d) 適用之法令、規章、契約(合約)與專業職責
  - e) 個人和其他利害關係人之利益

規劃個人資料管理系統PIMS

- **3.3 個人資料管理政策**
  - 組織應確保高階管理階層被附與發行及維護個人資料管理政策之責，而其政策中應明訂政策框架，並展現對於遵循個人資料保護法與好的實務的支持與承諾。

NOTE *Senior management might consist of the Board of Trustees/Directors, the Chief Executive and senior workers, the partners of the organization or the owner of a sole trader company.*

規劃個人資料管理系統PIMS

- **3.4 政策內容**
  - a) 僅於合法組織需求下，始得進行個人資料之處理
  - b) 僅針對特定目的蒐集必要的個人資料，且不過度的處理個人資料
  - c) 明確告知當事人其個人資料將如何被使用及被誰使用
  - d) 僅處理相關且適當的個人資訊
  - e) 公平與合法的處理個人資訊(參考 4.7);
  - f) 組織應維護一份個人資料清冊(參考 4.2);
  - g) 確保個人資料的正確性，並於必要時進行更新
  - h) 僅依法或合法的組織目的下保存個人資料

規劃個人資料管理系統PIMS

- i) 尊重當事人對其個人資料所能行使之權利，包含其申請閱覽權
- j) 確保所有個人資料安全
- k) 當組織將個人資料傳輸之非歐盟成員之國家時，應確保其具善良保護之機制
- l) 個人資料保護法令所允許之例外情形的應用
- m) 發展與建立PIMS，使個人資料保護政策能實行
- n) 鑑別內、外部利害關係者及其參與PIMS治理與運作的程度
- o) 於PIMS明確界定員工之責任和歸責性(參考3.5)

規劃個人資料管理系統PIMS

3.5 職責和歸責性

高階管理團隊應負起組織管理個人資料之責。(可參考4.1.1).

- **職責應包含：**
  - a) 核准個人資料管理政策
  - b) 依政策發展和施行PIMS
  - c) 應遵循政策執行安全及風險管理 (可參考4.13.1)
- **應指派一位或多位合適或具經驗的同仁負責日常個人資料管理政策的遵循(可參考4.1.2)**
- **藉由流程與程序的實行、適當的員工發展或對於不符合事項制訂管控程序，以確保所有同仁皆能遵循個人資料管理政策之要求**

規劃個人資料管理系統PIMS

- 3.6 資源提供
- 組織應決定並提供建立、實行、操作和維護PIMS的資源。

規劃個人資料管理系統PIMS

3.7 將PIMS嵌入組織文化

a) 透過持續的教育訓練與認知課程，以提高、強化與維持所有員工對PIMS的認知

b) 建立對PIMS認知訓練有效性評量程序

c) 對所有員工傳達以下的重要性：

- 1) 達成PIMS目標
- 2) 遵循政策
- 3) 對政策的持續改善

d) 確保每個員工都瞭解他們如何影響組織PIMS

PIMS的建置與運作

- **4.1 責任的配置(Key appointments)**
  - 4.1.1 高階管理階層
  - 4.1.2 遵循政策的日常職責
  - 4.1.3 資料保護代表
- **4.2 辨識及記錄個人資料的使用情況**
  - 4.2.1 組織應維護一份個人資料分類清冊
  - 4.2.2 具高風險的個人資料
- **4.3 認知及教育訓練**
- **4.4 風險評鑑**

PIMS的建置與運作

- **4.5 PIMS 持續更新**
- **4.6 通告**
- **4.7 公正與合法的處理**
  - 4.7.1 個人資料的蒐集與處理
  - 4.7.2 隱私公告與聲明之記錄
  - 4.7.3 隱私公告與聲明之取得
  - 4.7.4 隱私公告與聲明之可用性
  - 4.7.5 第三方

PIMS的建置與運作

- **4.8 個人資料處理的目的**
  - 4.8.1 處理準則
  - 4.8.2 新目的的同意
  - 4.8.3 資料分享
  - 4.8.4 資料配對
- **4.9 適當、相關且不過度**
  - 4.9.1 適當性
  - 4.9.2 相關且不過度
- **4.10 正確性**

PIMS的建置與運作

- **4.11 保留及處置**
- **4.12 個人的權利**
  - 4.12.1 個人的權利(符合法定時間限制)
  - 4.12.2 抱怨與申訴
- **4.13 安全議題**
  - 4.13.1 安全控制
  - 4.13.2 儲存及管理
  - 4.13.3 傳輸
  - 4.13.4 存取控制
  - 4.13.5 安全評估
  - 4.13.6 安全事故管理

PIMS的建置與運作

- 4.14 將個人資料傳輸於EEA(歐盟)之外
  (EEA=European Economic Area)
- 4.15 揭露予第三方
- 4.16 轉包處理
- 4.17 維護

PIMS的監控與審查

- **5.1 內部稽核**
  - 5.1.1 稽核計畫
  - 5.1.2 稽核員的挑選
  - 5.1.3 稽核需求
- **5.2 管理審查**
  - a)來自PIMS 使用者之回饋
  - b)由組織人員所辨識及提升之風險
  - c)稽核結果
  - d)程序審查之紀錄
  - e)資訊技術提升及替換之結果

5.2管理審查

- f)來自主管機關評估後之正式要求
- g)抱怨事件的處理
- h)已發生之資安事故及資料外洩事件

- 管理審查應提供所有可能造成PIMS變更之詳細資訊，其資料來源可為政策的調整、可能影響作業遵循之程序與技術。
- 當PIMS發生重大變更後，應立即執行稽核作業。

PIMS的改善

- **6.1 矯正與預防措施**
  - 6.1.1 概述
  - 6.1.2 預防措施
  - 6.1.3 矯正措施
- **6.2 持續改進**

教育體系資通安全暨個人資料管理規範2016年版附錄B修正說明

個人資料管理規範

- 本附錄列出之控制目標及控制措施乃參考BS 10012:2009第3節3.3至3.5、3.6，第4節4.1至4.3及4.7至4.17列出之管理原則，並考量「教育機構個人資料保護工作事項」、「私立專科以上學校及私立學術研究機構個人資料檔案安全維護實施辦法」，與「教育體系個人資料安全保護基本措施及作法等要求」，並配合教育體系與相關單位之屬性與特點，保留符合各層級單位之項目。除第4節4.6與我國個人資料保護法律規範不符而略去外，標準其它要求均已整合至本規範本文中，以建構完整的PDCA管理循環。
- 施行單位應完全遵循本附錄所列要求，並得考量自身的需求與特性，考慮增加其他必要之控制目標及控制措施。各控制項將標示遵循之個人資料保護法與施行細則條文，同時並將國際標準條文標號標註於，附件 1 附錄 B個人資料控制措施與各項標準對照表，以供參考。唯本附錄目標在對教育體系相關機構之個人資料管理產生引導作用，本規範之驗證作業目的為確認資通安全或個人資料管理系統有效執行，並無法律上免責的保證，教育體系機構如遇法律議題，其法規遵循性仍應由各機構提供符合性之法律證據與軌跡資料。
-
- 附註：控制項編號下(I/P)註記代表ISMS與PIMS可共用項目， 並以規範建置步驟與附錄A控制項編號進行對照，俾便施行單位進行PIMS的建置作業，同時導入ISMS則應考量適用該共用項目以符合ISMS與PIMS的要求。

B.1 個人資料管理政策

本章節主要的內容可參照下表：				規範 附錄 A	個資法
B.1 個人資料管理政策					
控制目標	B.1.1	個人資料管理方針		柒二(二) A5.1	
控制項	B.1.1.1 (I/P)	個人資料管理政策	核准並定期審查個人資料管理政策，展現管理階層對遵循個人資料保護法律及良好實務的承諾	柒二(二) A5.1.1 A.5.1.2	

B.2 個人資料管理組織

本章節主要的內容可參照下表：

				規範 附錄 A	個資法
B.2 個人資料管理組織					
控制目標	B.2.1	內部組織		柒二 A.6.1	§18 細§12
控制項	B.2.1.1 (I/P)	管理階層角色及責任	應由管理階層負責個人資料管理，確保個人資料保護法令及良好實務的遵循	柒二(一) A.6.1.1	細§12
	B.2.1.2 (I/P)	日常作業管理責任	指派合格或具經驗的人員，確保日常作業符合個人資料管理相關政策的要求	柒二(三) A.6.1.1	§18 細§12
	B.2.1.3 (I/P)	個人資料管理專人	建立各單位的個人資料管理窗口，協助個人資料相關日常作業的執行	柒二(三) A.6.1.1	§18 細§12

B.3 人員認知與訓練

本章節主要的內容可參照下表：

				規範 附錄 A	個資法
B.3 人員認知與訓練					
控制目標	B.3.1	個人資料管理認知與教育訓練		柒四(二) A.7.2.2	細 § 12
控制項	B.3.1.1 (I/P)	政策認知訓練	透過政策認知訓練使個人資料管理成為核心價值與績效管理的一部分	柒四(二) A.7.2.2	細 § 12
	B.3.1.2 (I/P)	認知與教育訓練	透過訓練與宣導，使所有員工了解處理個人資料時應有的責任	柒四(二) 柒四(三) A.7.2.2	細 § 12

B.4 個人資料之識別與風險管理

本章節主要的內容可參照下表：

				規範柒 附錄 A	個資法
B.4 個人資料之識別與風險管理					
控制目標	B.4.1	個人資料之識別與維護		A.8.1 A.8.2	細 § 12
控制項	B.4.1.1 (I/P)	個人資料清冊	清查並維護個人資料清冊	A.8.1.1	細 § 12
	B.4.1.2 (I/P)	高風險個人資料	應鑑別高風險個人資料	A.8.2.1 A.8.2.2	細 § 12
控制目標	B.4.2	個人資料之風險管理		柒三(二) 柒五(二) 柒五(三)	細 § 12
控制項	B.4.2.1 (I/P)	風險管理	確保組織瞭解，特定類型個人資料處理時任何相關風險。	柒三(二) 柒五(二) 柒五(三)	細 § 12

B.5 公正與合法的處理

本章節主要的內容可參照下表：

				規範 附錄 A	個資法
B.5 公正與合法的處理					
控制目標	B.5.1	蒐集與處理			§8, §9
控制項	B.5.1.1	蒐集與處理作業審查	定期審查作業流程，以確保公正且合法的蒐集與處理個人資料		§8, §9
控制目標	B.5.2	告知與同意			§8, §9 §17, §7, §15, §19
控制項	B.5.2.1	告知事項	告知事項應符合個人資料保護法令要求		§8, §9 §17
控制項	B.5.2.2	告知或同意作業程序	訂定管理程序，以確保告知作業之執行及執行證據保存		§8, §9 §17, §7, §15, §19

B.6 個人資料特定目的處理

本章節主要的內容可參照下表：				規範 附錄 A	個資法
B.6 個人資料特定目的處理					
控制目標	B.6.1	蒐集與處理特定目的			§15, §19 §16, §20
控制項	B.6.1.1	特定目的處理準則	個人資料僅於特定目的下處理與使用		§15, §19 §16, §20
	B.6.1.2	新特定目的同意	個人資料用於新增特定目的應取得當事人書面同意		§16, §20

B.6 個人資料特定目的處理

控制目標	B.6.2	資料分享與揭露		A.13.2	§15, §19 §16, §20
控制項	B.6.2.1 (I/P)	資料分享規劃與協議	資料分享應符合法令規範，簽訂資料分享協議取得合法使用承諾，並留存可供稽核紀錄	A.13.2.1 A.13.2.2 A.13.2.3	§15, §19 §16, §20
	B.6.2.2 (I/P)	資料揭露程序	訂定管理程序，以確保僅於合法且必要情況下揭露個人資料	A.13.2.1 A.13.2.3	§15, §19 §16, §20

B.6 個人資料特定目的處理

控制目標	B.6.3	資料比對			§15, §19
控制項	B.6.3.1	資料比對	透過資料比對而產出的個人資料，應確保其比對作業及使用，符合特定目的或法律要求		§15, §19

B.7 適當相關與正確性

本章節主要的內容可參照下表：

				規範 附錄 A	個資法
B.7 適當相關與正確性					
控制目標	B.7.1	適當性相關且不過度			
控制項	B.7.1.1	適當性管理	個人資料的蒐集與使用的適當性審查		
	B.7.1.2	相關且不過度管理	個人資料的蒐集與使用相關且不過度審查		
控制目標	B.7.2	個人資料正確性			§ 11
控制項	B. 7.2.1	正確性管理	整合個人資料的正確性管理至作業流程中		§ 11
	B. 7.2.2	錯誤資料的更正	應通知或更正提供予其他施行單位的個人資料的錯漏		§ 11
	B. 7.2.3	新流程的審查	審查新流程或系統，確保其可達成個人資料正確性的維持		§ 11

B.8 保存與處置

本章節主要的內容可參照下表：				規範 附錄 A	個資法
B.8 保存與處置					
控制目標	B.8.1	保存與銷毀		柒四(四) A.8.3 A.11.2	§ 11
控制項	B.8.1.1 (I/P)	資料保存與銷毀程序	施行單位應訂定個人資料保存與銷毀管理相關程序	柒四(四) A.8.3 A.11.2	§ 11

B.9 當事人權利

本章節主要的內容可參照下表：				規範 附錄 A	個資法
B.9 當事人權利					
控制目標	B.9.1	當事人權利行使			§3, §10 §11, §13 , §14
控制項	B.9.1.1	當事人權利行使程序	訂定管理程序，以確保當事人行使其法定權利		§3, §10 §11, §13 , §14
	B.9.1.2	抱怨與申訴流程	受理並正確處理個人資料相關抱怨與申訴案件		

B.10 資料安全議題

本章節主要的內容可參照下表：

				規範 附錄 A	個資法
B.10 資料安全議題					
控制目標	B.10.1	安全控管措施		A.8~A.14 A.18	細 § 12
控制項	B.10.1.1 (I/P)	個人資料控管措施	設定並審查個人資料蒐集、處理、儲存、傳輸與存取監控的安全控制措施或科技	A.8,A.11 A.12,A.13 A.14,A.18	細 § 12
	B.10.1.2 (I/P)	存取權限管理程序	以正式程序最小化授予並審查個人資料存取權限	A.8,A.9 A.10	細 § 12
	B.10.1.3 (I/P)	安全控制措施審查	定期審查安全控制措施的有效性	柒五(二) 柒六(二) A.18	細 § 12

B.10 資料安全議題

控制目標	B.10.2	安全事故管理		A.16 A.12	細§12
控制項	B.10.2.1 (I/P)	安全事故管理程序與紀錄	訂定管理程序，以妥善處理安全事故並留存可供後續追查的紀錄	A.16 A.12.4	細§12

B.11 國際傳輸

本章節主要的內容可參照下表：

				規範 附錄 A	個資法
B.11 國際傳輸					§ 21
控制目標	B.11.1	國際傳輸管理		A.13.2	§ 21
控制項	B.11.1.1	境外管理協議與保護	傳輸至我國境外的個人資料應受到良好的管理	A.13.2	
	B.11.1.2	傳輸法令遵循	個人資料的傳輸應符合我國相關法律要求		§ 21

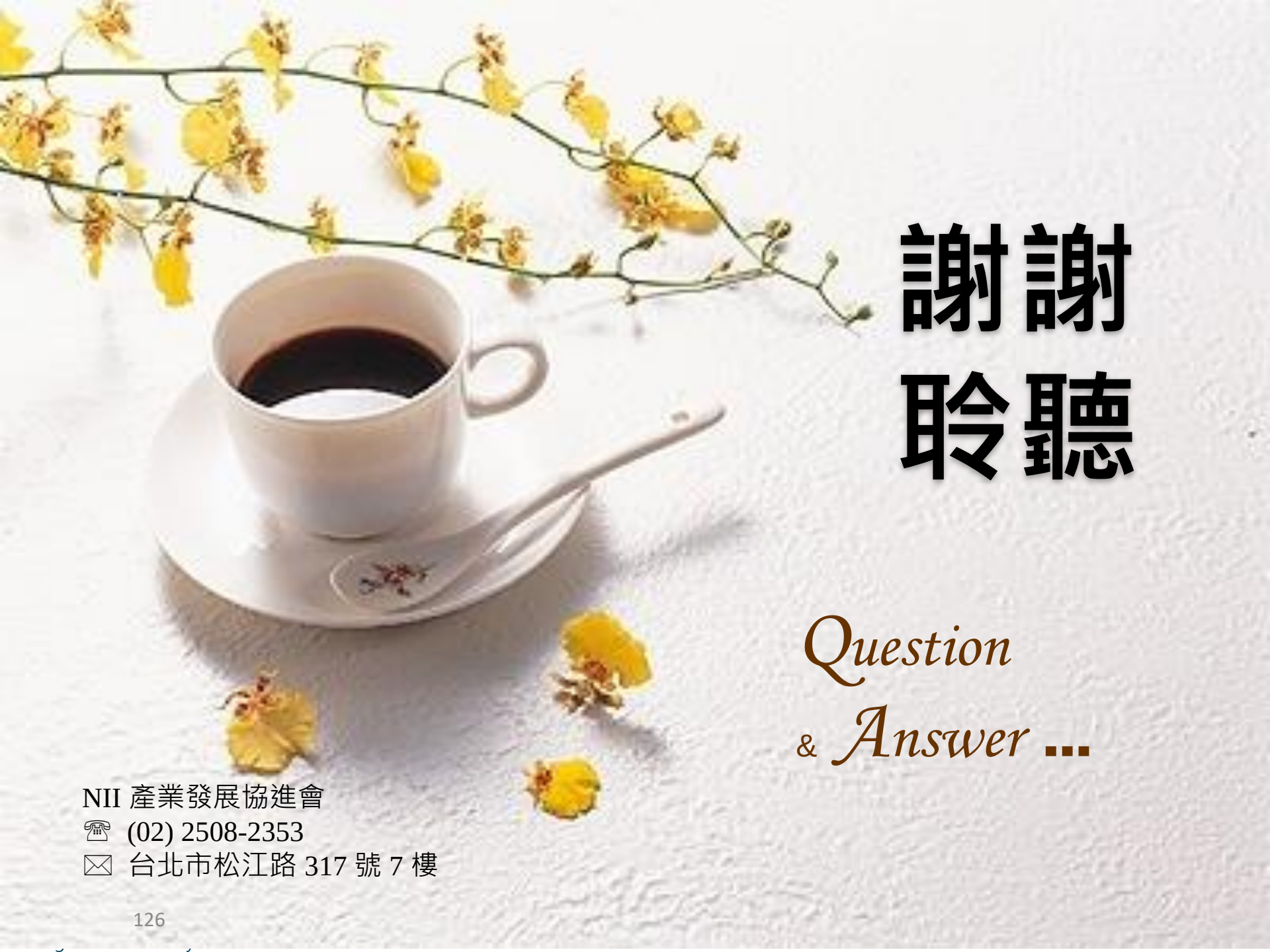
B.12 委外管理

本章節主要的內容可參照下表：

				規範 附錄 A	個資法
B.12 委外管理				A.15	細 § 8
控制目標	B.12.1	個人資料作業委外管理		A.15	細 § 8
控制項	B.12.1.1 (I/P)	委外管理程序	篩選及管理委外機構	A.15.1 A.15.2	細 § 8
	B.12.1.2 (I/P)	委外協議要項	於協議載明委外要求，以管理委外機構	A.15.1	細 § 8

課程大綱

1. 個人資料保護與ISMS
2. 個資保護實作
3. 個人資料管理制度介紹
4. 問題與討論



NII 產業發展協進會
☏ (02) 2508-2353
✉ 台北市松江路 317 號 7 樓