

ISMS與PIMS

吳國維
CEO, NIIEPA

大綱

- 個資法修正與何時實施？
- 個資法架構
- 施行細則說明（部分）
- **ISO27001/BS10012**
- 結語

大綱

- 個資法修正與何時實施？
- 個資法架構
- 施行細則說明（部分）
- ISO27001/BS10012
- 結語

“個人資料保護法” 與 “電腦處理個人資料管理辦法”

- 電腦處理個人資料保護法：84年8月11日制定公佈
- 個人資料保護法：99年5月26日修正公佈。
- 99年5月26日總統公佈日起，廢止許可登記制度。
- 其他法條施行日期，由行政院定之。
- 施行細則，由法務部定之。

何時施行？

- 總統於99年5月26日公佈
- 法務部預定完成施行細則之期間
- 11月25日之目標是否可以達成？
- 將由行政院訂定施行日期
- 今年十二月？明年六月？
- 自公佈日起，原有證照制度立即廢除
- 金融業目前已無個資法執照

保護個人資料的其他法律

- 民法18、195（**侵害人格權**）
 - 財產上的損害賠償
 - 精神慰撫金
 - 回復名譽的適當處分
- 刑法315、315-1、318-1（**妨害秘密罪**）
 - 有期徒刑 → 三年以下
 - 罰金 → 三萬元以下
- 通訊保障及監察法19、24、25（**秘密通信自由**）
 - 損害賠償
 - 有期徒刑 → 五年以下

新法修正重點

✧ 擴大適用主體：

- ✧ 現行法：公務機關與非公務機關（醫院、學校、電信業、金融業、證卷業、保險業、大眾傳播業、徵信業等八類行業
- ✧ 新法：打破行業別限制，包含各行各業及個人

✧ 擴大保護客體：

- ✧ 現行法：使用電腦或類似設備處理之個人資料檔案。
蒐集：為建立個人資料檔案而取得個人資料
- ✧ 新法：以任何方式（包含紙本）留存的資料
蒐集：以任何方式取得的個人資料

新法修正重點（續）

· 增訂告知義務：

· 直接搜集及間接搜集之告知義務

· 修正施行前非由當事人提供之個人資料，應自本法修正施行之日起一年內完成告知。

· 當事人拒絕行銷之權利

· 資料違法外洩之通知義務

· 加重罰則：

· 民事賠償：新台幣二千萬元→二億元

· 刑事處罰：新台幣伍萬元→一百萬
有期徒刑：三年以下→五年以下

大綱

- 個資法修正與何時實施？
- **個資法架構**
- 施行細則說明（部分）
- ISO27001/BS10012
- 結語

個資法架構

第一章 總則 (14)



第二章 (4)
公務機關對個人資料之
蒐集、處理及利用

第三章 (9)
非公務機關對個人資料之
蒐集、處理及利用

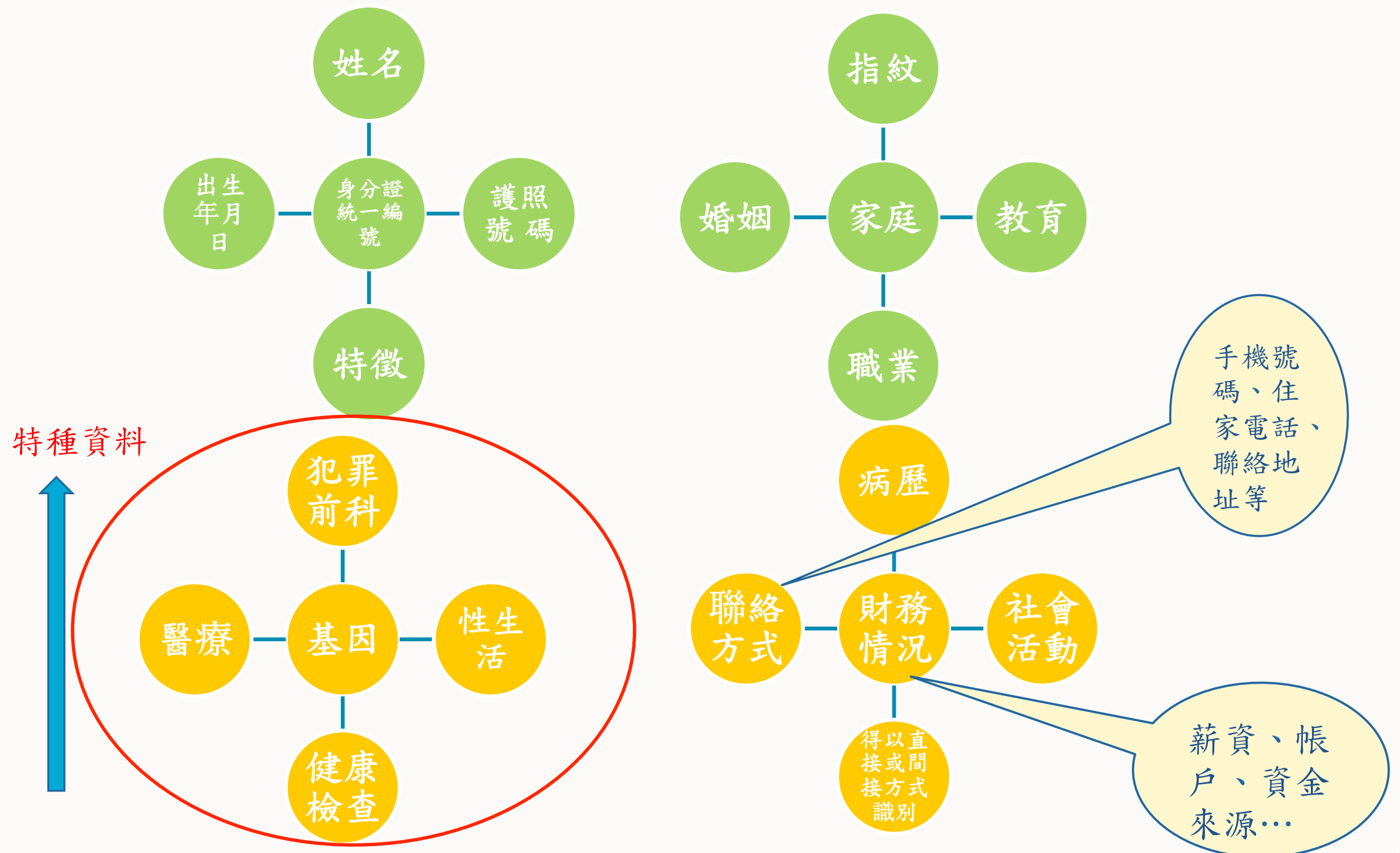


第四章 損害賠償及團體訴訟 (13)

第五章 罰則 (10)

第六章 附則 (6)

何謂個人資料？



何謂個人資料？

自然人的

- 姓名
- 出生年月日
- 身分證號碼
- 護照號碼
- 特徵
- 指紋
- 婚姻
- 家庭
- 教育
- 職業
- 病歷
- 聯絡方式
- 財務情況
- 社會活動

一般
資料

特種
資料

- 醫療
- 基因
- 性生活
- 健康檢查
- 犯罪前科

其他
資料

- 得以直接或間接方式識別該個人之資料

大綱

- 個資法修正與何時實施？
- 個資法架構
- 施行細則說明（部分）
- ISO27001/BS10012
- 結語

施行細則草案（一）

第五條 本法第二條第二款所稱個人資料檔案，包括備份檔案及軌跡資料。

第四條 本法第三條第二款所定個人資料檔案，包括備份檔案。

軌跡資料係指個人資料在蒐集、處理、利用過程中所產生非屬於原蒐集個資本體之衍生資訊（LOG FILES），包括（但不限於）資料存取人之代號、存取時間、使用設備代號、網路位址（IP）、經過之網路路徑…等，可用於比對、查證資料存取之適當性。因此，為符合本法個人資料保護與個人資料合理利用之立法意旨，個人資料檔案除備份檔案之外，亦應包括軌跡資料在內，爰增訂如上。

施行細則草案（二）

第六條 本法第二條第四款所稱刪除，指使已儲存之個人資料自個人資料檔案中消失。

前項規定，如為事後查核、比對或證明之需要而留存軌跡資料者，得不予刪除。

本法第二條第四款所稱內部傳送，係指公務機關或非公務機關本身內部之資料傳送。

第十條 本法第四條第五款所稱刪除，指依本法第十三條第三項規定，使已儲存之個人資料自個人資料檔案中消失而不復存在。

一、第一項配合本法條次，酌作文字修正。

二、刪除既指使已儲存之個人資料自個人資料檔案中消失，然如使個人資料自個人資料檔案中全部消失，將不利於電腦系統追查過往作業紀錄，為考量資訊安全與數位鑑識等證明作業之需要，乃增列由系統留存之必要軌跡資料，不在刪除之範圍內，爰規定如第二項。

三、第三項新增，明定內部傳送係指公務機關或非公務機關內部之資料傳送，例如公務機關內部各單位間之資料傳送，

施行細則草案（三）

第九條 本法所稱適當安全維護措施、安全維護事項或適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之必要措施。

前項必要措施，應包括下列事項：

- 一、成立管理組織，配置相當資源。
- 二、界定個人資料之範圍。
- 三、個人資料之風險評估及管理機制。
- 四、事故之預防、通報及應變機制。
- 五、個人資料蒐集、處理及利用之內部管理程序。
- 六、資料安全管理及人員管

一、本條新增。

二、本法所稱適當安全維護措施，參考德國聯邦個人資料保護法第九條規定，應係指技術上及組織上之必要措施，規定如第一項。

三、為確保個人資料檔案之合法且正當蒐集、處理或利用，應辦理安全維護之必要措施內容，且為與國際接軌，乃仿英國 BS10012：2009 及日本 JISQ15001：2006 等個人資料管理系統之規範，以 P-D-C-A 方法論予以建立，爰為第二項規定。

四、技術上與組織上之必要措施，如支出費用對公務機關或非公務機關而

施行細則草案（四）

理。

七、認知宣導及教育訓練。

八、設備安全管理。

九、資料安全稽核機制。

十、必要之使用紀錄、軌跡
資料及證據之保存。

十一、個人資料安全維護之
整體持續改善。

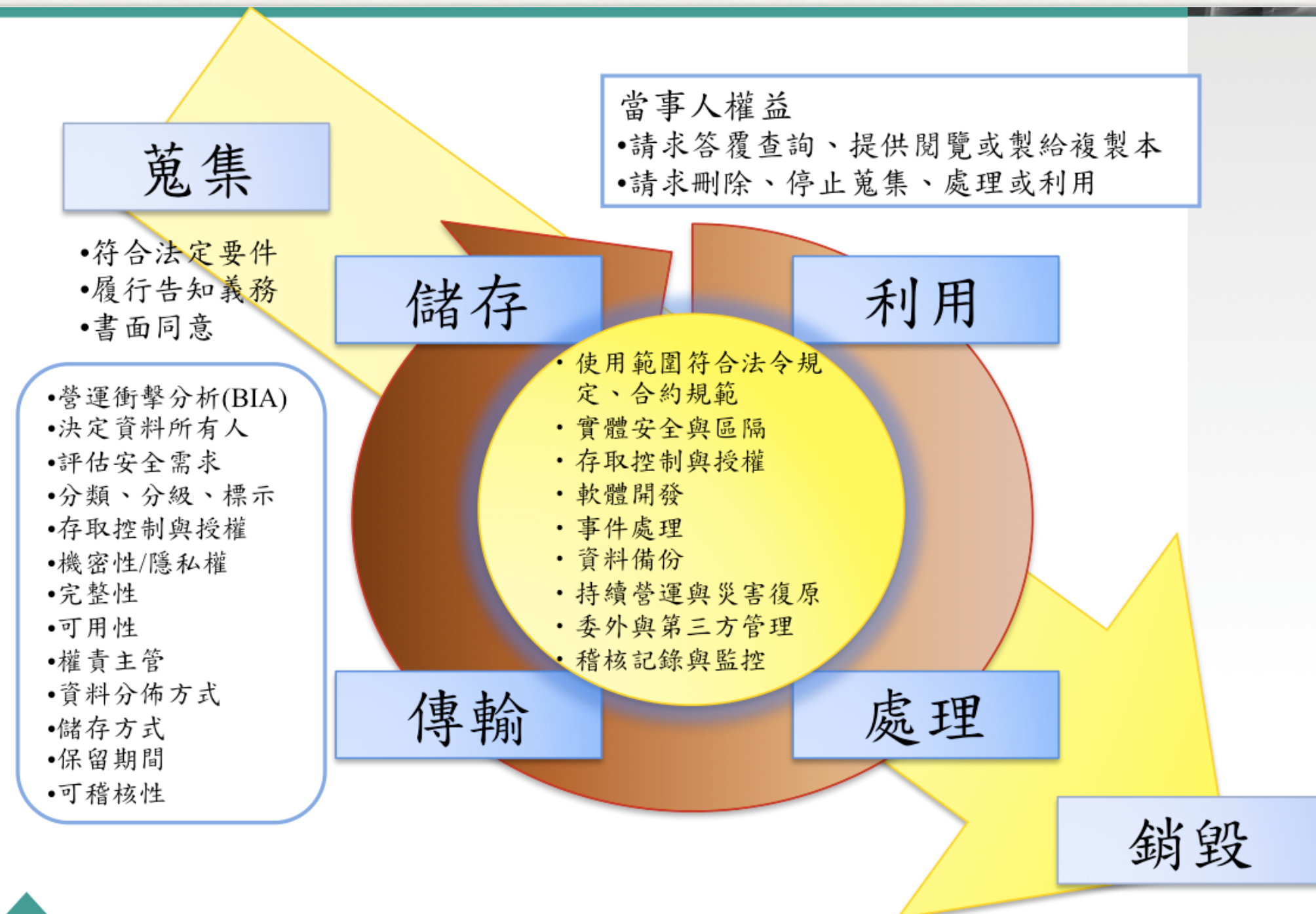
第一項必要措施，以
所須支出之費用與所欲達
成之個人資料保護目的符
合適當比例者為限。

言須耗費過鉅者，實已
與所欲達成之個人資料
保護目的間不符適當比
例，爰規定如第三項。

大綱

- 個資法修正與何時實施？
- 個資法架構
- 施行細則說明（部分）
- **ISO27001/BS10012**
- 結語

個人資料生命週期管理



學校個資之種類

教職員、學生 資料

姓名、電話、地址、
家長姓名、學生證號碼

校務行政資料

姓名、學生證號碼、成績
單、操行等

健康資料

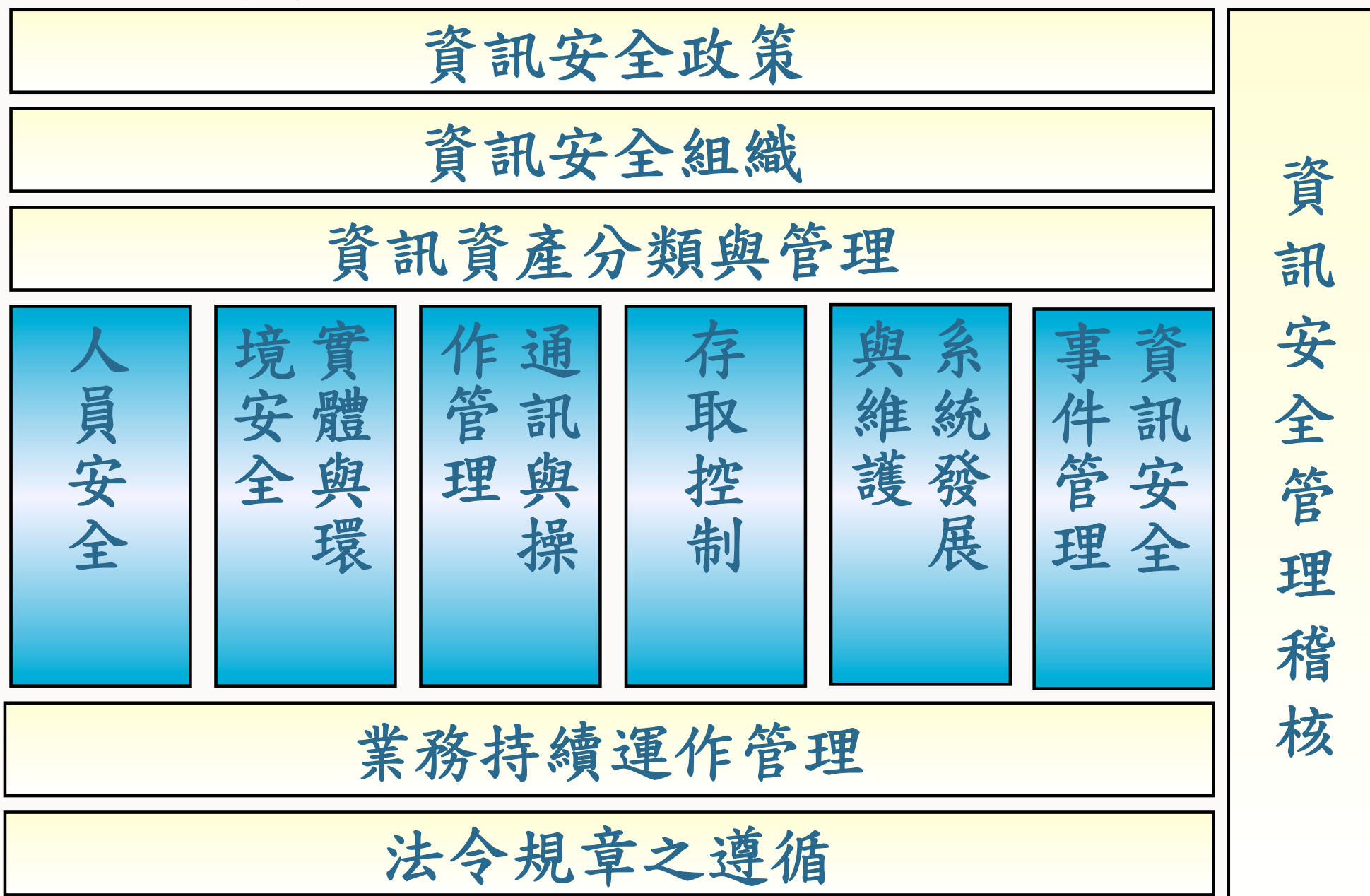
姓名、健康資料記錄

薪資資料

姓名、身分證字號、地
址、電話、薪資、級別

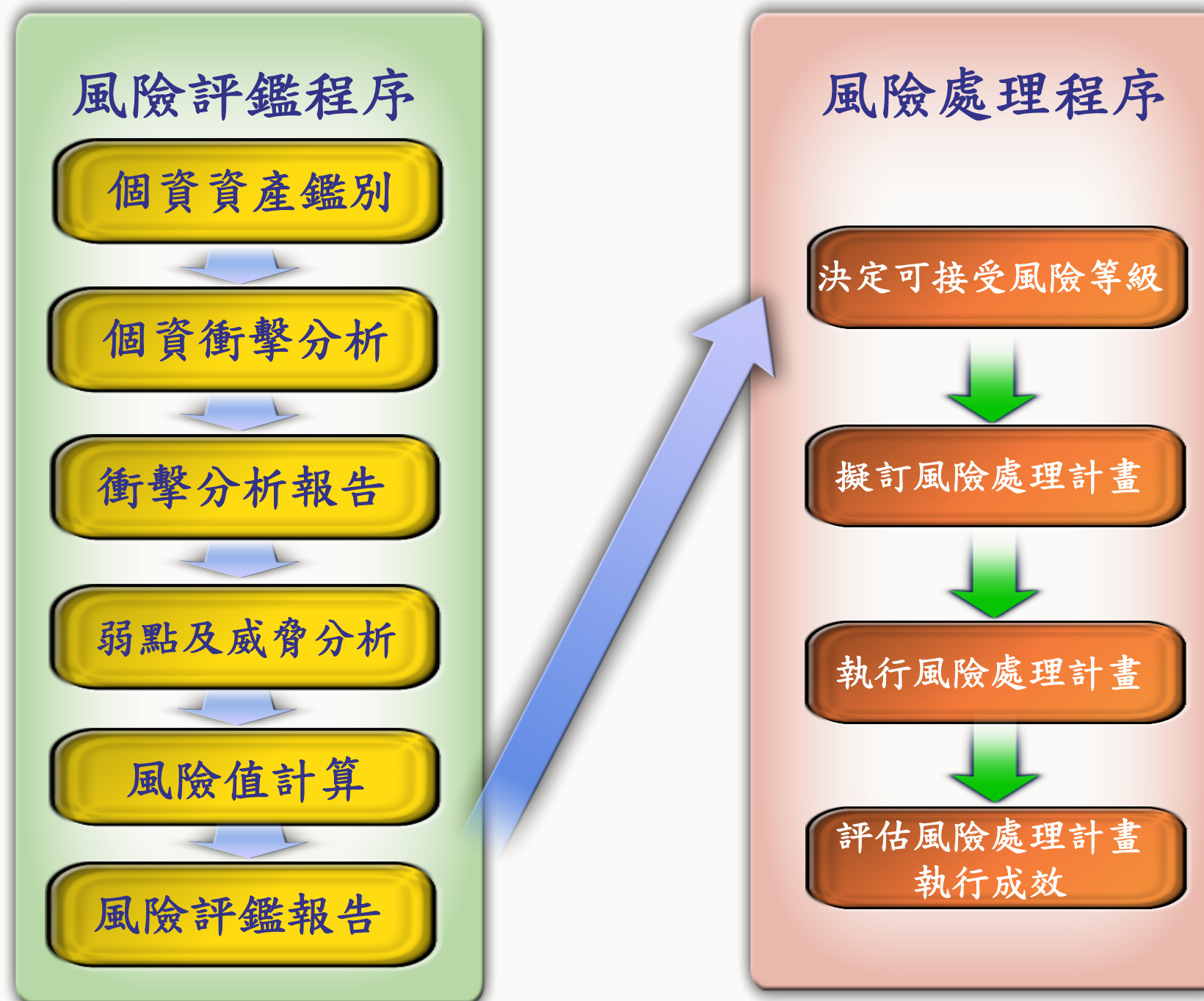
國際資訊安全、個資防護管理系統標準 – ISO 27001/PIMS

11領域、39控制目標、133控制要點



個人資料風險管理程序

- PIMS



國內個人資料保護法與BS10012

BS 10012相關管理規範摘要

- 1.善盡告知義務
- 2.依特定目的蒐集個資
- 3.公正且合法使用個資
- 4.保護個人隱私相關項目
- 5.確保存取控制之安全
- 6.確保資料之正確性
- 7.確保資料傳輸之安全
- 8.確保個人修改之權利
- 9.妥善處理抱怨與申訴
- 10.落實委外安全管理

國內個人資料保護法相關管理規範摘要

- 1.善盡告知義務
- 2.依特定目的蒐集個資
- 3.公正且合法使用個資
- 4.保護個人隱私相關項目
- 5.確保存取控制之安全
- 6.確保資料之正確性
- 7.確保資料傳輸之安全
- 8.確保個人修改之權利
- 9.妥善處理抱怨與申訴
- 10.落實委外安全管理

- 11.個資定義不同(未包含種族、政黨等)
- 12.提供閱覽或製給複製本
- 13.規範特種資料不得蒐集
- 14.區分公務機關與非公務機關之處理方式
- 15.具團體訴訟機制

英國標準BS10012(PIMS)
V.S. 國內個人資料保護法

BS 10012與ISO 27001之關聯

管理面

BS 10012

ISO 27001技術支援面

A.5 – 安全政策

A.6 – 資訊安全的組織

A.7 – 資產管理

A.8
人力資源安全

A.9
實體與環境安全

A.10
通訊與作業管理

A.12
資訊系統獲取、
開發、及維護

A.11 – 存取控制

A.13 – 資訊安全事故管理

A.14 – 營運持續管理

A.15 – 遵循性

BS 10012與ISO 27001之關聯

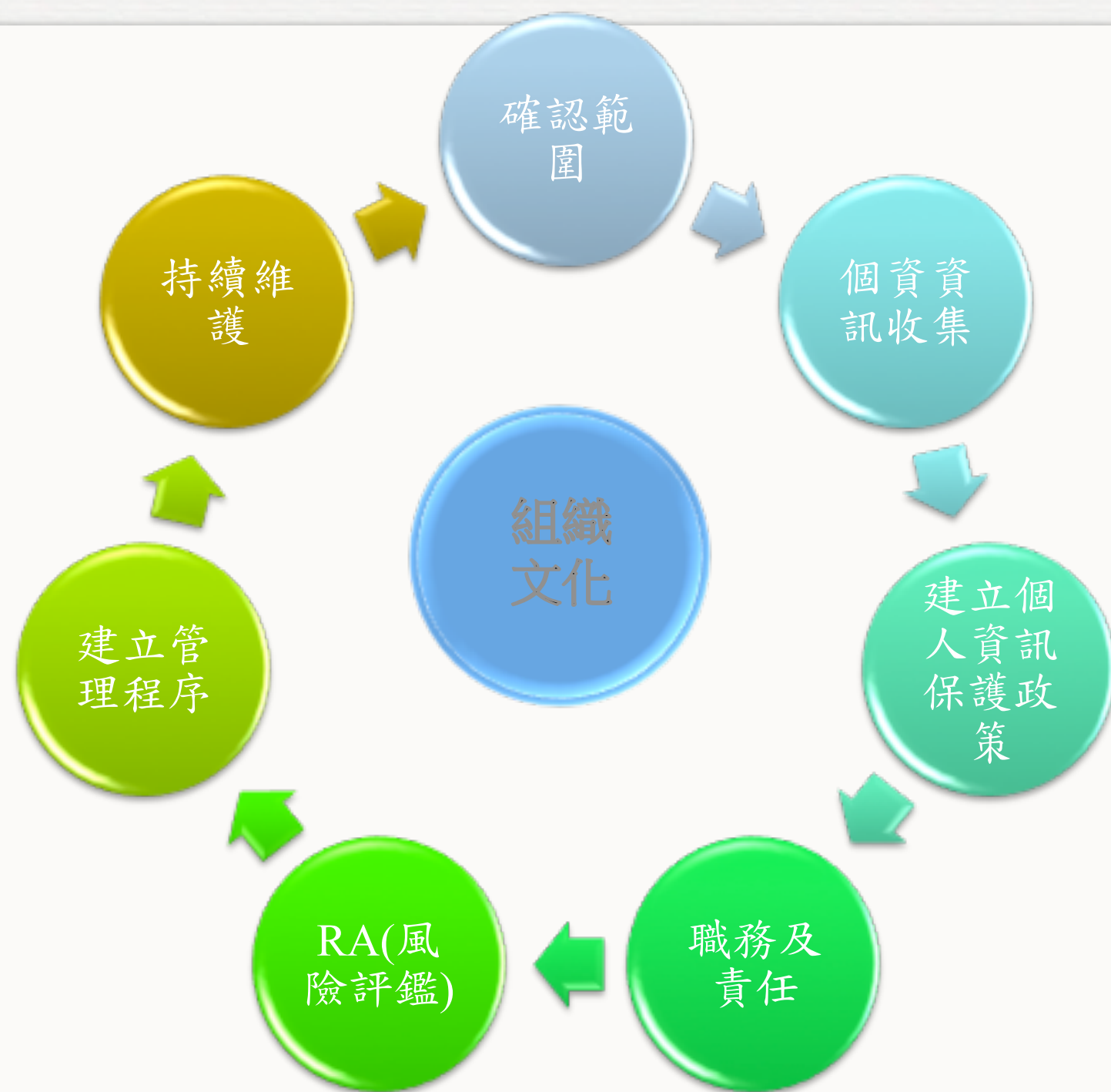
BS 10012 (管理要求)



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)

國際標準—BS10012



PIMS建置階段

建立PIMS 管理架構

- 前置準備
- 時程規劃
- 啟動會議
- 組織業務分析
- 制訂個人隱私政策
- 建立PIMS組織

風險評鑑 與管理作業

- 個資作業流程分析(PIA)
- 個資資產盤點
- 個資衝擊分析
- 威脅弱點分析
- 實體設備安全管控了解
- 風險評鑑作業程序建立
- 風險處理
- 現況診斷與改善建議

建置PIMS 管理系統

- 文件整合
- 政策文件改善及增修

制度落實 與稽核驗證

- PIMS事件緊急應變計畫
- 維護監控
- 稽核規劃
- 稽核追蹤
- 書面審查
- 實務審查
- 正式評鑑
- 改善建議

大綱

- 個資法修正與何時實施？
- 個資法架構
- 施行細則說明（部分）
- ISO27001/BS10012
- **結語**

特定目的修訂（一）

個人資料保護法「特定目的」建議修正彙整表（初稿）

壹、公務機關之特定目的（總類）

檔案管理

提報機關	現行特定目的	建議修正/增設特定目的	理由及特定目的具體內涵說明
國家安全會議	無	檔案管理	無

人事行政管理

提報機關	現行特定目的	建議修正/增設特定目的	理由及特定目的具體內涵說明
人事行政局	002 人事行政管理	002 人事行政管理 00201 人員基本資料管理 00202 現職資料管理 00203 學歷資料管理 00204 考試及分發資料管理 00205 終身學習及訓練進修資料管理 00206 經歷資料管理 00207 考績資料管理 00208 懲資料管理	一、現行「人事行政管理」無法充分描述本局進行人事行政管理之具體內涵，建議增列「人員基本資料管理」等 15 項子項目。惟增列內容係考量公務機關進行人事行政管理之需求，一般民間企業並不適用。 二、查公務人員任用法第 28 條規定略以，褫奪公權尚未復權者，不得任用為公務人員。為辦理任免作業所需，本局建置「褫奪公權人員資料庫」一種，爰建議增列「褫奪公權資料管理」1 項。 三、考量涉及國家安全或重大利益職務之公務人員

特定目的修訂（二）

提報機關	現行特定目的	建議修正/增設特定目的	理由及特定目的具體內涵說明
法務部行政執行署		(十八) 人事薪資系統管理	
消費者保護委員會		人事行政管理 (增設)	本會人事管理業務
原子能委員會	秘書行政管理： 2. 薪給管理及賦稅申報	無	辦理員工待遇給與、各項所得發放及員工及其他人員個人所得扣繳與申報。
原子能委員會	人事行政管理： 統籌人事行政管理業務	無	辦理委員聘請、職工員額管理、考試分發、任免、遷調、考績、獎懲、差勤、訓練、進修、待遇、福利、退撫、資遣、保險、獎金、加給等人事業務。
國軍退除役官兵輔導委員會	○七九 學生資料管理	○七九 學生(員)資料管理	一、職訓機構對於參訓學員之學習成效有管理義務。 二、上述學員資料管理與學生資料管理有別，建議酌作文字修正。
文化建設委員會		文化志工管理	本會為文化志工之中央目的事業主管機關，為業務需要，業已建置「全國文化志工資訊網」，提供全國各文化志工管理暨運用單位作為聯繫平台，並鼓勵文化志工個人加入網站會員，且有蒐集、處理及利用以下相關資料，爰擬增訂本項特定目的。 1. 志工保險資料 2. 志工通訊錄 3. 志工招募資料
文化建設委員會		文化替代役男管理	本會(含所屬機關)及全國各縣市文化局，為業務需

特定目的修訂（三）

提報機關	現行特定目的	建議修正/增設特定目的	理由及特定目的具體內涵說明
			要，設有文化服務替代役男，為期有效管理（ex: 專業訓練、培訓、分發、生活管理及督導考核）且各項資訊揭露，本會業已建置「文化服務替代役資訊網」網站，爰有蒐集、處理及利用役男之個資及兵籍資料，爰擬增訂本項特定目的。
宜蘭縣政府	096 其他地方政府事務	所得登錄報繳業務	本府給付個人款項，所為之個人所得資料蒐集登錄查詢處理，包括個人姓名、身分證字號、住址、所得款項及給付事由等，因現行特定目的項目籠統，爰另增設項目。
宜蘭縣政府	100 其他財政服務	核發薪餉業務	本府給付員工各項薪餉、獎金等，因現行特定目的項目籠統，爰予以明確增設。
宜蘭縣政府	100 其他財政服務	員工薪資相當實物配給、房租津貼免稅扣除額登記業務	為配合薪資所得總額減免申報，必須蒐集個人姓名、身分證、符合申報親屬出生年次及已申報親屬減列原因等，因現行特定目的項目籠統，爰予以明確增設。

會計

會計

提報機關	現行特定目的	建議修正/增設特定目的	理由及特定目的具體內涵說明
法務部行政執行署		（八）會計與相關服務	
消費者保護委員		會計與相關服務（增設）	本會會計業務

教育機構如何因應

- 法務部與教育部應儘早釐清相關事宜：
 - 如何可以符合新法規定？
 - 公務機關或非公務機關之認定
 - 特定目的之補充與公告
 - 施行細則中軌跡資料說明與確認納入的理由
 - 相關資料的處理原則（人二資料、健康檢查等）
 - 匯集學校疑問，提供諮詢服務。應以主管機關權限，作必要說明解釋，或作法律的增修（與法務部協調研擬修法方向與內容）。
 - 協助學校取得資源做好個資防護措施與教育訓練。

QUESTIONS?