個人資料保護與管理第三方稽核
暨委外管理教育訓練

PIMS

全球之領導者與創新者

提供檢驗、鑑定、測試及驗證服務

課程大綱

- 個人資料安全稽核機制
- 教育體系作業查核重點
- 驗證稽核流程介紹
- 委外管理暨查核要項

PIMS

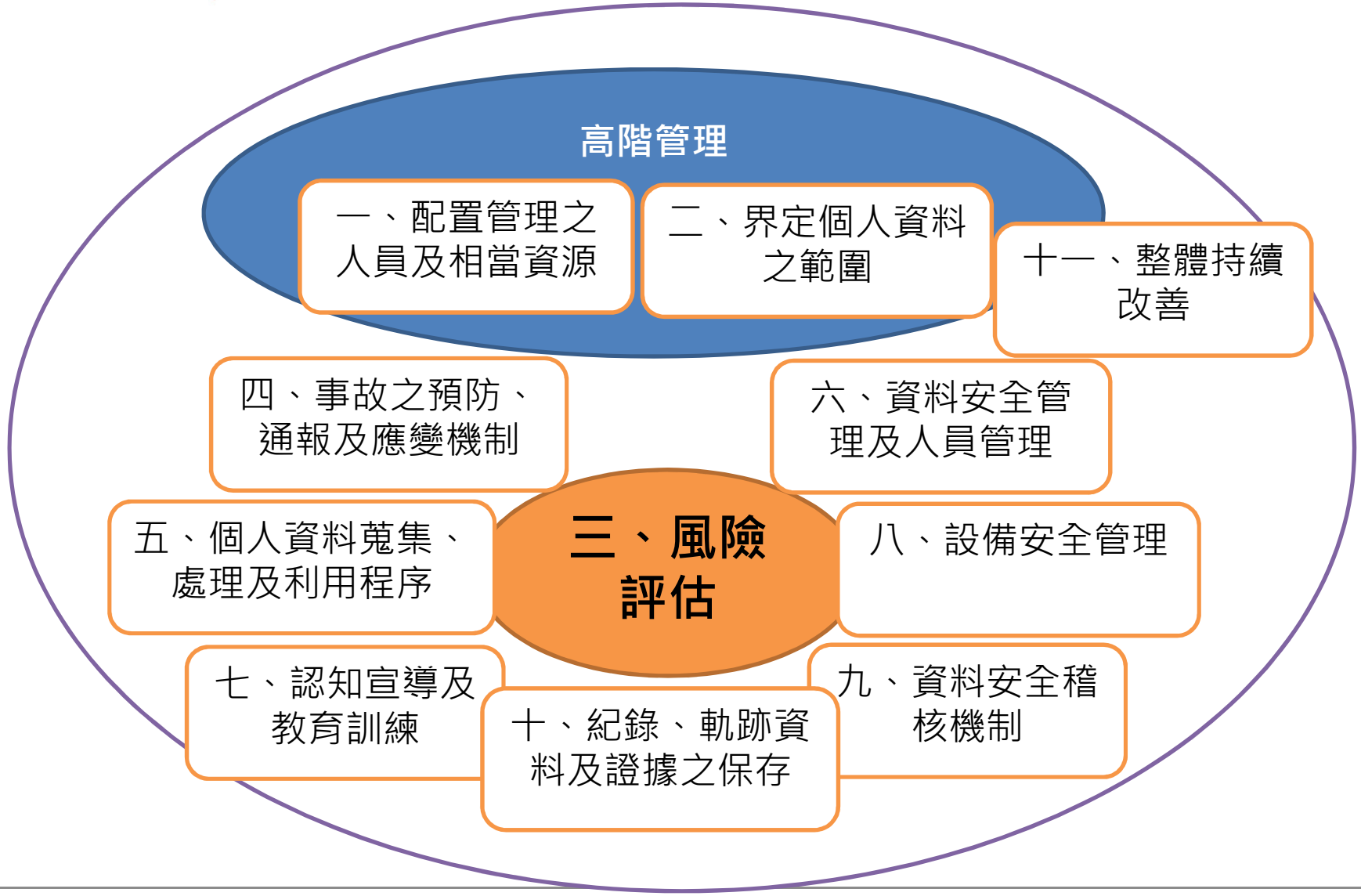
Tutor
講師

PIMS

個人資料安全稽核機制

PIMS

施行細則第十二條第二項
適當安全維護措施(共十一項)



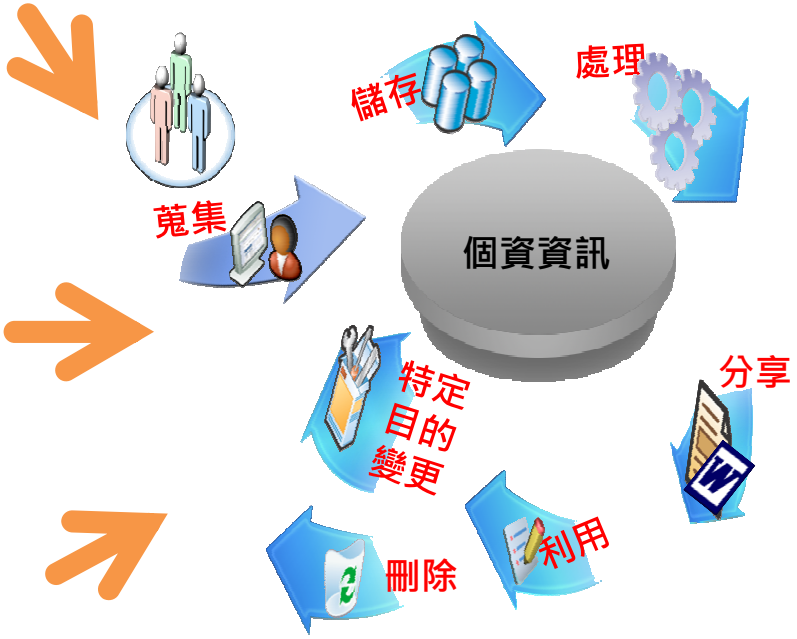
PIMS

個資法安全維護事項 VS BS10012 VS ISO 27001

個資法安全維護事項	BS10012:2009	ISO 27001:2005	ISO 27001:2013
配置管理之人員及相當資源	3.6 資源提供	4.2 建立與管理ISMS	5.3組織角色、責任與授權 7.1 資源
界定個人資料之範圍	3.2 PIMS的範圍與目標	4.2建立與管理ISMS	4.3決定資訊安全管理系統範圍
個人資料之風險評估及管理機制	4.4風險評鑑	4.2建立與管理ISMS	6.1風險與機會處理措施
事故之預防、通報及應變機制	4.6 通知 / 4.7公平與合法的處理 /4.13安全議題	4.2建立與管理ISMS/ A.13資訊安全事故管理 /A.14營運持續管理	6.1風險與機會處理措施(附錄A all) A.16資訊安全事故管理 / A.14A.17營運持續管理 資訊安全層面
個人資料蒐集、處理及利用之內部管理程序	4.8個人資料處理的特定目的/ 4.9 適當、相關且不過度/ 4.10正確性/ 4.11保存與處置/ 4.12個人權利/ 5.2管理審查		
資料安全管理及人員管理	4.13安全議題	4.2建立與管理ISMS /A.7資產管理 /A.8人力資源安全	A.7人力資源安全/A.8資產管理
認知宣導及教育訓練	3.7將PIMS納入組織文化/ 4.3訓練與認知	5.2訓練、認知及能力 / A.8人力資源安全	7.3 Awareness 認知/ A.7人力資源安全
設備安全管理	4.13安全議題	A7資產管理 /A9實體環境安全	A.11 實體及環境 安全
資料安全稽核機制	5.1內部稽核	6內部稽核	9.2 內部稽核/ A.18.2.3技術遵循性審查
必要之使用紀錄、軌跡資料及證據之保存		4.3.3紀錄管制 /A.10通訊與作業管理	7.5 文件化資訊/ A.12.4 存錄及監視
個人資料安全維護之整體持續改善	6改進PIMS	4.2.4維持與改進ISMS /8 ISMS 之改進	10改善

PIMS

資料安全稽核機制



PIMS

透過資料安全稽核確保個資資訊達到機密性完整性可用性的要求

個人資訊(隱私)損害風險

- 隱私侵害活動可能包含下列:

廣告或間諜程式	盜用	勒索	機密性破壞	網路犯罪	資料正確性損害	歧視
意外暴露	詐騙	身份盜竊	入侵	控制措施失效	資料遺失	資料誤用
	網路釣魚	色誘	垃圾郵件	未授權電話銷售	第三方未授權分享	

- 其他重要的影響因素

識別性	資料欄位組合	使用情境	保護義務	個資存取與儲存

資料來源: ISO/IEC CD 29101 Information technology — Security techniques — A privacy reference architecture

PIMS

降低個人資訊(隱私)損害風險

- 管理者應決定安全維護措施，來保護個資與個資處理流程免於可能的隱私損害。
- 隱私風險評鑑應決定個資項目的風險等級。
- 潛在損害包含個資當事人可能受到的衝擊，以及個資管理者在維護個資時所面臨的負面影響。
- 個資管理者應透過定期隱私風險評鑑，及個資極小化與減緩活動來降低隱私風險。

資料來源: ISO/IEC CD 29101 Information technology — Security techniques — A privacy reference architecture

PIMS

提出個人資訊(隱私)保護要求

- 個人資訊(隱私)安全要求影響因素：

個資隱私與保護的法令法規要求	產業法規、專業標準與組織政策	業務應用與使用	其他影響資通訊系統設計因素

- ICT應用作業共通考量
  - 整合所有個資存取與儲存記錄(含軌跡與備份紀錄)
  - 識別與描述所有個資資訊
  - 維護個資存取權限清單
  - 日常稽核紀錄的具體需求評估應納入系統設計
  - 隱私控制設計宜包含備份與封存的安全性
  - 流程隱私控制的使用宜具一致性
  - 系統記憶刪除或處理活動軌跡應納入安全與隱私政策遵循。
  - 資料架構應識別單位間的個資分享與處理流程，並依個案狀況決定資料架構與資任歸屬。
  - 各系統宜考量隱私資料查詢紀錄的需求與容量。

資料來源: ISO/IEC CD 29101 Information technology — Security techniques — A privacy reference architecture

PIMS

個人資訊(隱私)處理生命週期控制考量(I)

- **蒐集-從個人取得資訊**
  - 尊重個資當事人隱私偏好與法律權利，及相關法令的隱私保護要求。
  - 僅取得必要資訊，並避免未授權獲得個資。
- **傳輸-傳輸、散播及揭露個資**
  - 各個涉及資料傳輸的單位應同意並維護其權責。
  - 除個資當事人或法令要求，應避免傳輸敏感性個資。
  - 跨國境傳輸應特別加以控制。
- **利用-蒐集、傳輸、儲存與銷毀以外的資料處理活動。**
  - 限制目的內使用，且除法令要求外應有書面同意。
  - 目的外使用是嚴重的議題，不能進行無書面同意的目的外使用。

資料來源: ISO/IEC CD 29101 Information technology — Security techniques — A privacy reference architecture

PIMS

個人資訊(隱私)處理生命週期控制考量(II)

- **儲存-可用不同形式或地點進行存放**
  - 儲存之資料應能識別為個資，資料儲存應有識別文件，如標籤。
  - 敏感性資料應避免儲存，除需儲存應有個資當事人同意，並有保護。
- **報廢-刪除、匿名化(anonymized)、封存、毀壞、歸還或丟棄**
  - 預備報廢資料應禁止使用，並匿名化。
  - 報廢資料應依據個資當事人或法令要求，以及相關保存期限進行處理。

資料來源: ISO/IEC CD 29101 Information technology — Security techniques — A privacy reference architecture

PIMS

教育體系作業查核重點

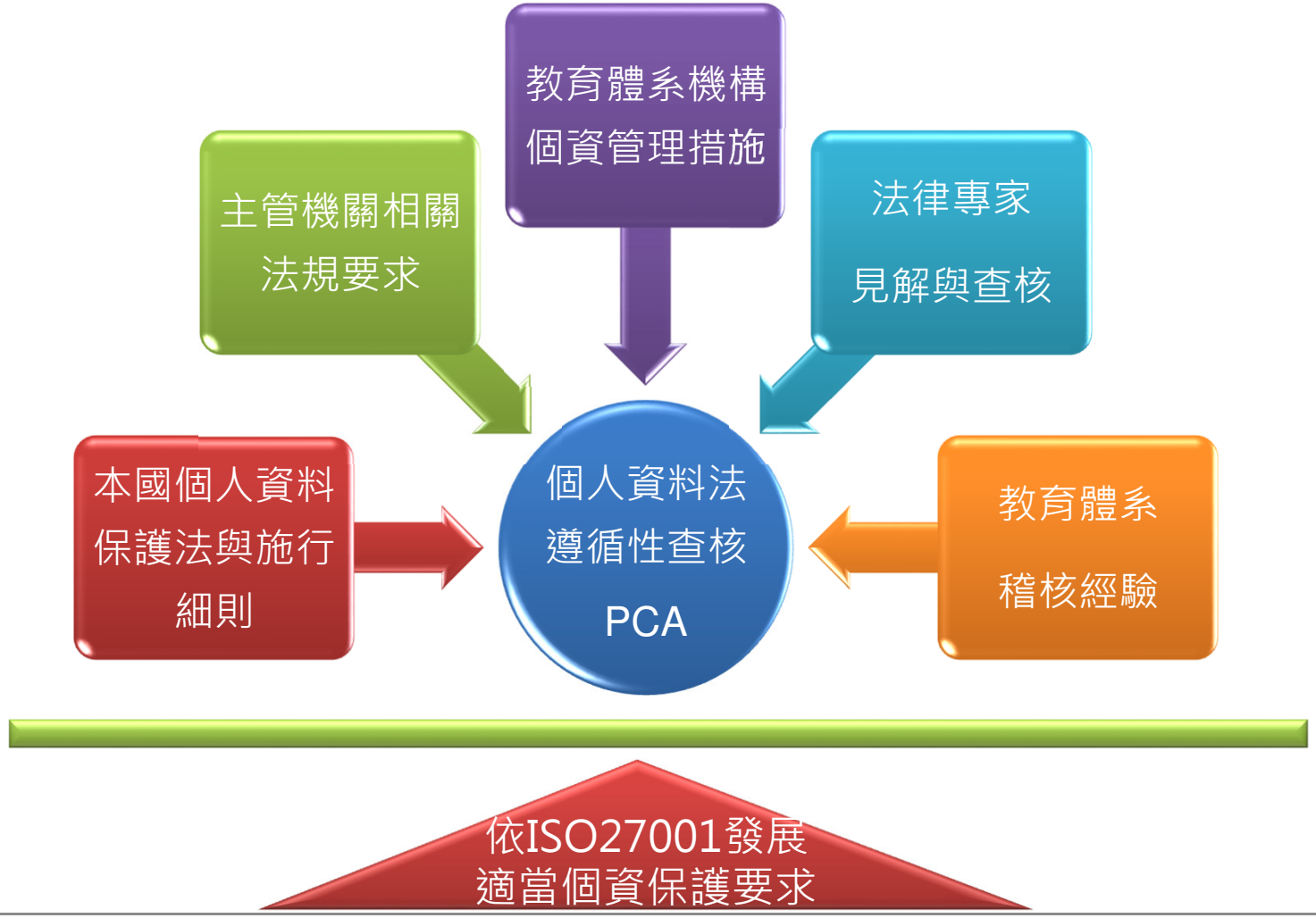
PIMS

個資管理系統成效確認之重要性

- **進行個資管理系統建置與輔導作業，建議管理系統建置完成專案末期時，可考量輔以階段性成效確認作業，理由如下：**
  - 專業驗收
  - 藉由客觀事實，積極對外彰顯本組織於個資管理良善管理責任之有效性，應符合：
    - 中華民國個資相關法規之遵循性
    - 符合國際標準與趨勢

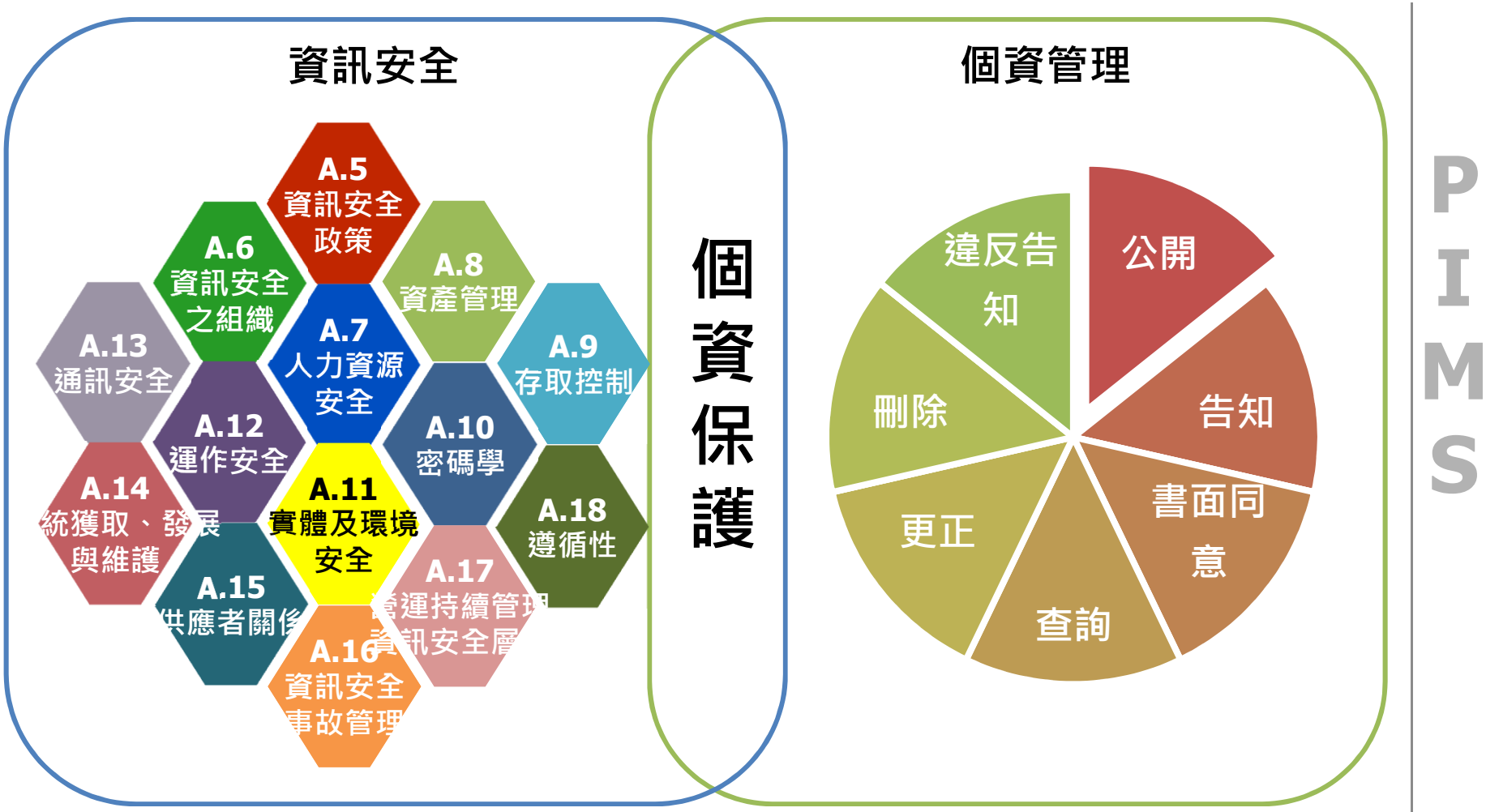
PIMS

個資法規遵循性查核(PCA)依據準則



PIMS

個資與資安管理


資訊安全
A.5 資訊安全政策
A.6 資訊安全之組織
A.7 人力資源安全
A.8 資產管理
A.9 存取控制
A.10 密碼學
A.11 實體及環境安全
A.12 運作安全
A.13 通訊安全
A.14 統獲取、發展與維護
A.15 供應者關係
A.16 資訊安全事故管理
A.17 營運持續管理
A.18 遵循性
個資保護
個資管理
公開
告知
書面同意
查詢
更正
刪除
違反告知
PIMS

個人資料蒐集、處理及利用管理程序稽核

確認個人資料特定目的 → 是否符合免告知事項 → 是否符合15,19條特定目的與特定情形 → 如目的外，檢視是否符合16,20條目的外利用要件

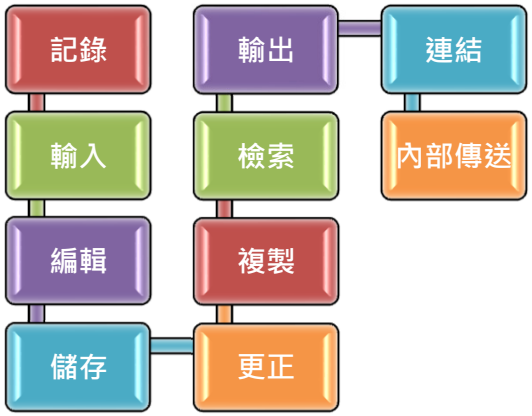
蒐集

公告事項

個資蒐集

書面同意

處理



內部管理程序應配合機關現有行政流程與資安要求

利用

資料提供

研究統計

郵遞物流

PIMS

教育體系個人資料安全保護基本措施及作法

- 人員管理措施
- 作業管理措施
- 物理環境管理措施
- 技術管理措施
- 認知宣導及教育訓練
- 紀錄機制

PIMS

技術遵循性稽核

WHEN YOU NEED TO BE SURE

SGS

必要之使用紀錄、軌跡資料及證據之保存

個資蒐集

記錄　輸出　連結
輸入　檢索　內部傳送
編輯　複製
儲存　更正

個資處理

紀錄、軌跡資料

資料利用

證據與鑑識

犯罪現場
被害人　嫌疑人
物證

軌跡資料收集

- 考量項目
  - 涵蓋度
  - 完整性
  - 保存時間(至少5年)
  - 保護能力
- 資源：Storage設備
- 管理機制：監控、稽核
- 數位鑑識之證據力

PIMS

個人資訊稽核需求—資料外洩可能性

多人共同
使用單一帳號

使用者權限遭竄改

正式資料測試
產生資料外洩

內部人員
竊取業務資料

未授權人員
執行資料存取

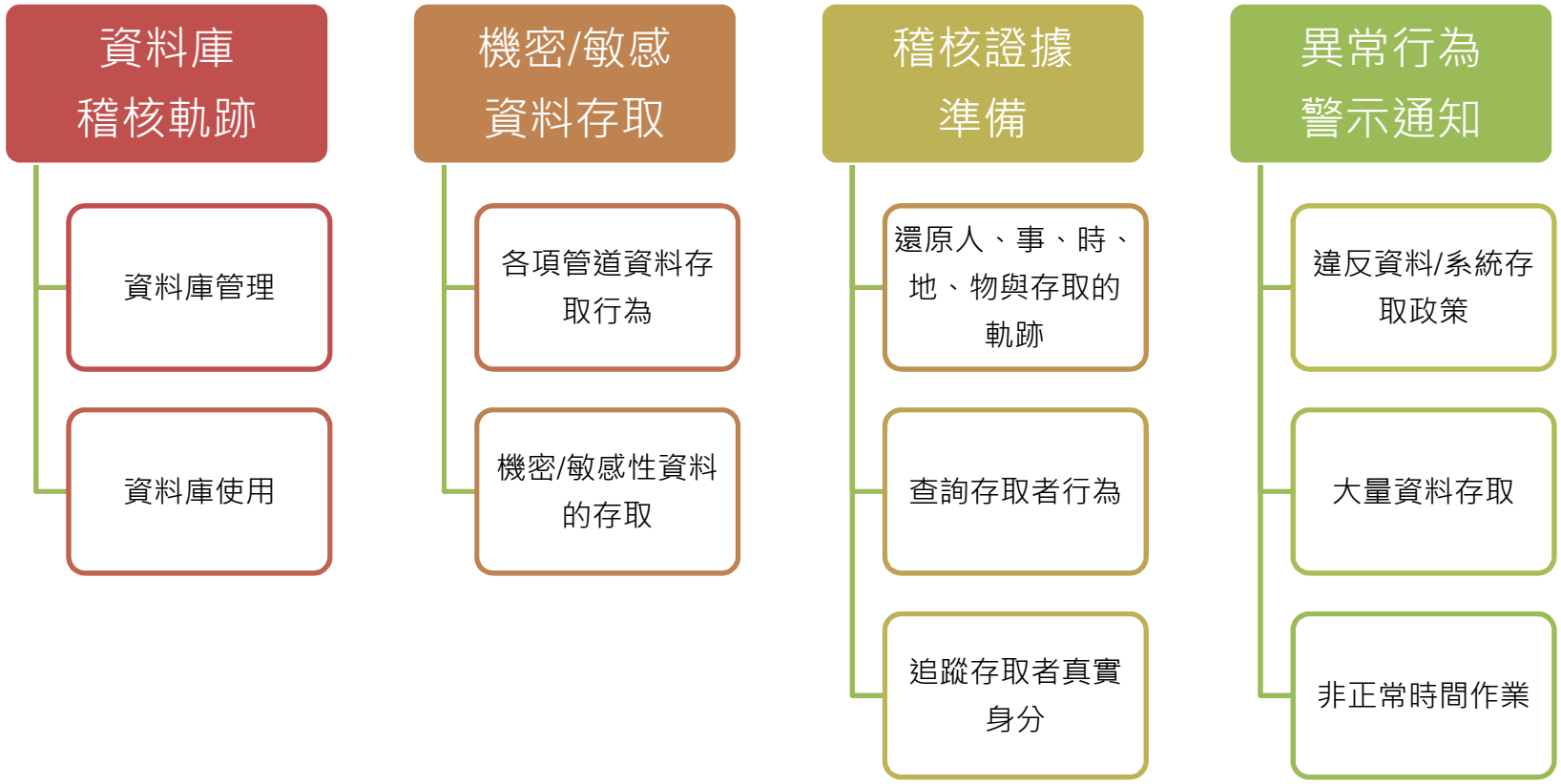
未授權傳遞外部單位

委外廠商洩漏資料

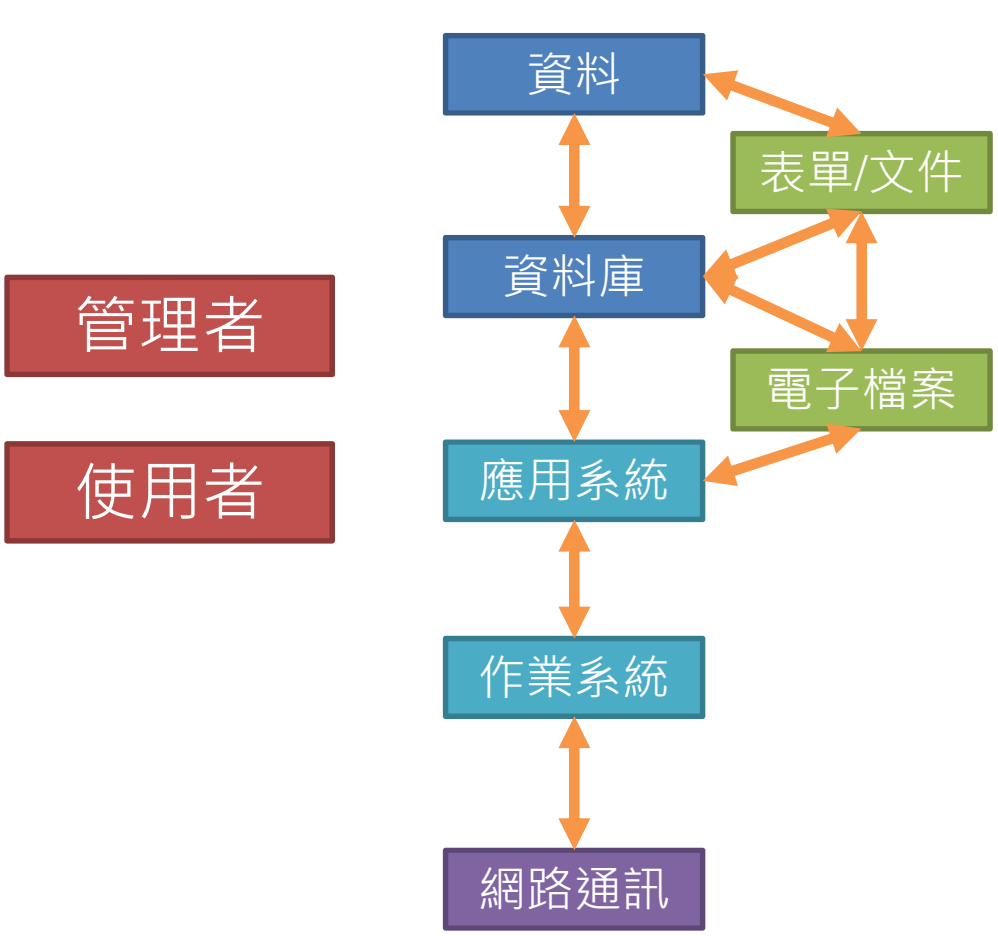
內部人員
執行目的外利用

PIMS

個人資訊技術稽核重點


資料庫
稽核軌跡
資料庫管理
資料庫使用
機密/敏感
資料存取
各項管道資料存取行為
機密/敏感性資料的存取
稽核證據
準備
還原人、事、時、地、物與存取的軌跡
查詢存取者行為
追蹤存取者真實身分
異常行為
警示通知
違反資料/系統存取政策
大量資料存取
非正常時間作業
PIMS

資料稽核軌跡留存要項



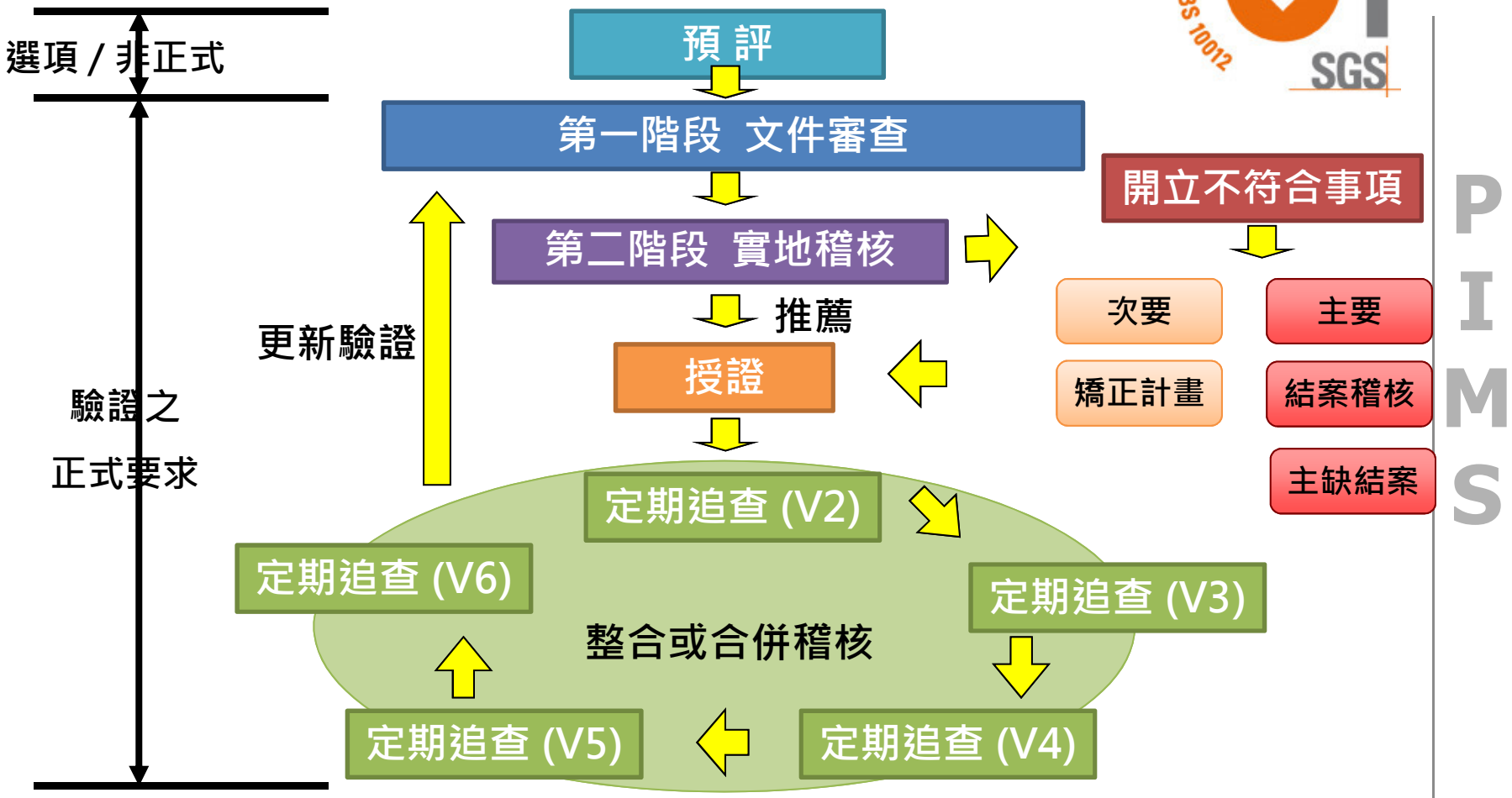
軌跡內容	
應用系統名稱	執行時間
使用者ID	來源IP
目的地IP	DB使用者
SQL指令	資料內容

PIMS

驗證稽核流程介紹

PIMS

制度檢核—驗證過程
BS10012/ISO 29100/ISO 27018



Audit Criteria 稽核準則

- 管理系統標準要求
  - BS 10012:2009/2017
- 個人資訊管理相關政策要求
- 個人資訊管理相關程序、條例、規範等要求
- 法令、法規、主管機關要求、行政命令
- 個人資訊管理系統要求
- 合約要求
- 產業行為規範

PIMS

第一階段 文件審查

- **目的**
  - 確認文件整備是否符合標準
  - 設計稽核計畫
  - 發展稽核查檢表
- **審查事項**
  - 個資管理政策與目標之聲明文件
  - 個人資訊管理系統程序文件
  - 組織及流程相關文件
    - 個人資訊流程/個人資訊清冊
    - 風險評鑑/安全評鑑報告
    - 個人資訊檔案保存期限表
    - 程序書、工作指導書
  - 流程審查
- **稽核計畫**

PIMS

組織與其環境

- **稽核員將確認組織瞭解其個人資訊管理要求，如**
  - 識別利害相關團體，以及其議題與期望
  - 建立個資管理與營運目標的連結
  - 識別適用的法令法規要求
  - 識別適切的活動、資產與資源
  - 執行適當的風險評鑑
  - 正確的決定PIMS範圍

PIMS

文件審查稽核發現說明

- **Critical audit findings關鍵稽核發現**

  本項稽核發現未加以適當處置，可能會造成第二階段的主要不符合事項。

- **Non critical audit findings非關鍵稽核發現**

  本項稽核發現未加以適當處置，可能會造成第二階段的弱點(如次要不符合事項或觀察事項)。

PIMS

第二階段 實地審查

目的

- 確認個人資訊管理系統符合性

審查事項

- 全流程全條款查核
- 依稽核標準確認其符合性
- 流程方式進行
- 抽樣手法
- 抽樣內部流程紀錄為證據

PIMS

定期追查

- **目的**
  - 確認管理系統的持續有效

- **審查事項**
  - 稽核人天較少
  - 重新抽樣確認前次稽核發現
  - 僅部分流程或條款

- **審查方式**
  - 依稽核標準確認其符合性
  - 流程方式進行
  - 抽樣手法
  - 抽樣內部流程紀錄為證據

PIMS

實地審查/定期追查 稽核發現說明

- **Major nonconformity (Major CAR) 主要不符合**
  - 個人資訊管理系統過程, 程序或運作的全面失效
  - 對應標準之某一要求完全缺乏
  - 許多的小失誤, 其集合效應導致系統之失效
  - 對個人資訊產生立即性的危害(機密性、完整性、可用性、法規遵循性)
- **Minor nonconformity (Minor CAR) 次要不符合**
  - 在特定流程、程序或運作過程中較不嚴重的失誤
- **Observation (OBS) /Opportunity for Improvement (OFI)觀察事項與改善建議**
  - 好的意見或可嘉惠組織中其他領域
  - 值得關切的部分
  - 改進的建議

PIMS

稽核行程- 配合安排

- 請準備一間不受干擾的會議室，供討論及書寫報告
- 請準備簡單午餐即可
- 請在會議室內準備簡便與充分的茶水飲料
- 為各組安排最少一位的陪審人員全程陪同。
- 請準備一份個人資訊管理文件一覽表

PIMS

個資稽核常見發現事項

- **個資盤點不完整**
  - 個資檔案個人資料流向與保存期限與實際作業未能符合
  - 部分個資檔案未列入個人資料檔案清冊，盤點未落實
- **保存期限不一致或永久保存**
  - 個資檔案的保存與銷毀程序未符合要求
- **告知主體與對象未適切**
  - 個資檔案同意書內未符合個資法告知事項
- **新目的/資料分享管理未完成**
  - 資料分享於非屬學校的第三人時未簽訂資料分享協議取得合法使用承諾
- **個資安全控制不足**
  - 委外廠商涉及個資檔案合約要求未包含個資安全維護事項
  - 個人資訊系統或資料庫帳號與權限控管未符合要求

PIMS

委外管理暨查核要項

PIMS

個人資訊委外管理要求—個資法

個資法施行細則第八條

- 受委託蒐集、處理或利用個人資料之法人、團體或自然人，依委託機關應適用之規定為之。前項情形，當事人行使本法之權利，應向委託機關為之。
- 委託機關應定期確認受託者執行之狀況，並將確認結果記錄之。

一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。	二、受託者就第十二條第二項採取之措施。	三、有複委託者，其約定之受託者。
四、 受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。	五、委託機關如對受託者有保留指示者，其保留指示之事項。	六、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。

PIMS

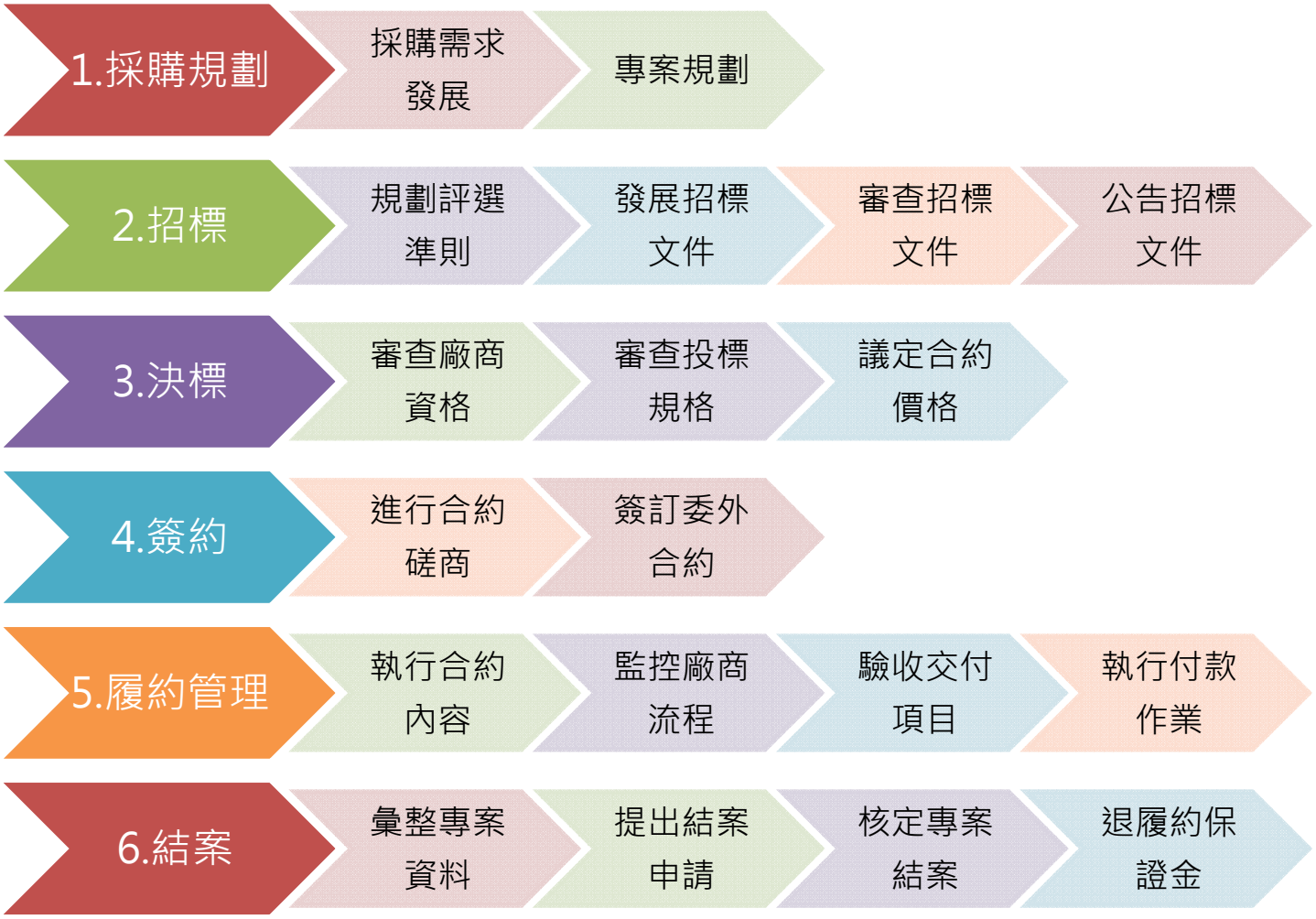
個人資訊委外管理要求— BS10012

4.16 分包處理

- 僅選擇可符合組織技術、實體及組織面安全要求；
- 其他組織處理個資前，評鑑其實施之安控措施，或於簽約前對該組織安控措施實行稽核；
- 應簽訂正式書面協議請組織依照要求提供服務，並要求對處理之個資實施適當之安控措施；
- 所簽訂契約中，應載明在存取個人資訊期間，定期稽核其安控措施執行；
- 需在合約義務規範下，取得組織同意後，方能使用分包商來處理個人資訊；
- 其他組織與其分包商之合約，需要求該分包商至少實施與其他組織一樣的安控措施及其他條款；及
- 與其他組織(包括向下展開的任何分包商)所簽訂契約中應明確陳述，當契約終止時，相關之個人資訊應銷毀、交還組織或交給組織指定之其他組織。

PIMS

個人資訊委外管理流程



PIMS

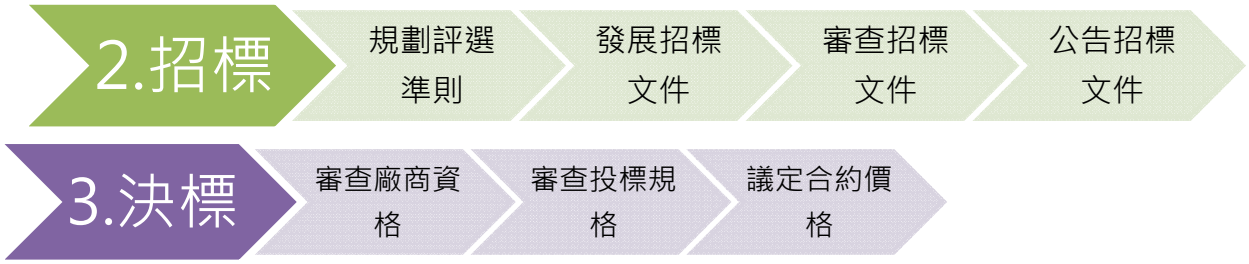
個人資訊委外管理作業—採購規劃

1.採購規劃 | 採購需求發展 | 專案規劃

- 確認預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間
- 確認應遵循之個資相關法令法規
- 委外單位技術、實體及組織面安全要求
- 委外單位應採取之個人資訊安全維護事項

PIMS

個人資訊委外管理作業—招標/決標



- 確認評選準則中之個人資訊管理要求
- 確認招標文件內個人資訊管理要求
- 評鑑其安控措施，或於簽約前實行安控措施稽核

PIMS

個人資訊委外管理作業—簽約

4.簽約 | 進行合約磋商 | 簽訂委外合約

- 簽訂正式書面協議依要求提供服務，並對處理之個資實施適當安控措施；
- 正式書面協議中，應載明在存取個人資訊期間，定期稽核其安控措施執行；
- 書面協議中應載明受託者或其受僱人違反本個資法或相關法規命令時，應向委託單位通知之事項及補救措施。

PIMS

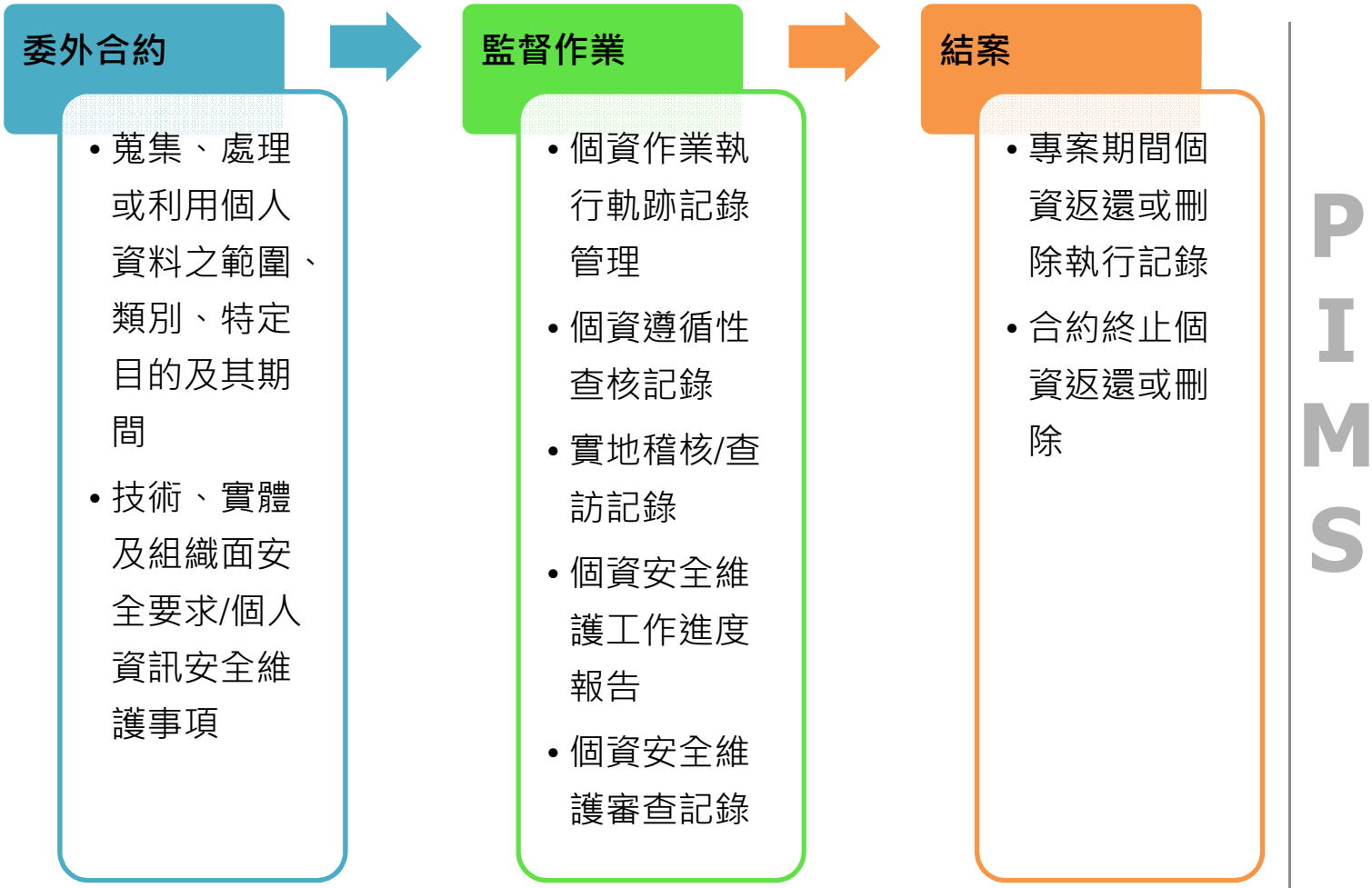
個人資訊委外管理作業—履約管理/結案

5.履約管理	執行合約內容	監控廠商流程	驗收交付項目	執行付款作業
6.結案	彙整專案資料	提出結案申請	核定專案結案	退履約保證金

- **分包商**
  - 應經委託單位同意後，方能使用分包商處理個人資訊
  - 受託單位與分包商之合約，應要求該分包商至少實施相同之安控措施及其他條款
- **合約期間應依約定進行監督作業**
  - 實地稽核/查訪
  - 定期提交個資安全維護工作進度報告
  - 定期進行專案/個資安全維護審查會議
- **委託關係終止或解除時，個人資料載體應依合約返還或刪除**

PIMS

個人資訊委外流程查核


委外合約
• 蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間
• 技術、實體及組織面安全要求/個人資訊安全維護事項
監督作業
• 個資作業執行軌跡記錄管理
• 個資遵循性查核記錄
• 實地稽核/查訪記錄
• 個資安全維護工作進度報告
• 個資安全維護審查記錄
結案
• 專案期間個資返還或刪除執行記錄
• 合約終止個資返還或刪除
PIMS

個人資訊委外查核可行方式

	第一者稽核	第二者稽核	第三者稽核
	委外單位自評	客戶查核	驗證稽核
稽核人員	受託廠商稽核單位	委託單位 (或經授權者)	第三者認證稽核
受稽對象	內部單位	供應商或分包商	驗證範圍之內部單位
稽核目的	■組織變動 ■外部法令法規	■執行能力 ■安全問題	■取得證書 ■客戶要求
稽核依據	■法令法規 ■組織內部規章 / 程序	■合約 ■行業特定標準 ■法律法規	■法令法規 ■組織內部規章 / 程序 ■合約 ■行業特定標準
稽核強度	較無強制力	具強制力	具強制力
稽核深度	最深層	以合約範圍為準	以驗證範圍為準

PIMS

Q & A

PIMS

THANKS FOR YOUR COOPERATION

PIMS