【內部使用】

文件編號：ICST-C-023

101年度

雲端資安防護整合服務委外服務案

個資保護實務導入試行報告

(V2.0)

執行單位：財團法人資訊工業策進會

中華民國102年5月

報告摘要

報告名稱	個資保護實務導入試行報告
資訊等級	☐機密　☐密　☒內部使用　☐普通
相關撰稿人	江衍勳、盧玲朱、林子群
閱讀對象	☒一般主管　☒資安人員　☒資訊人員　☒一般使用者

內容摘要：

本報告主要目的為實務導入「個人資料保護參考指引」，以評估參考指引之可行性、適用性及有效性，乃遴選 2 個政府機關進行實務導入作業。

本報告適用於一般主管、資安人員及資訊人員，以瞭解資安參考指引文件之導入方式與實施重點，藉由參考本報告的附件相關產出內容，方便閱讀者據以實施，讓參考指引實際導入有依循的方向。

本報告導入方法分成四階段，分別為「開始」、「文件導讀」、「參考指引導入」及「結案」。

本次導入作法係於開始階段由個案 A 先挑選 5 個不同性質的資訊系統，經討論後決定由「A1 系統」執行導入；個案 B 則自行遴選「B1 業務」執行導入。接著在第 2 階段，導讀個人資料保護參考指引的重點，以加速導入機關對參考指引的瞭解。第 3 階段實務導入參考指引規劃與執行階段，最後對導入機關之資訊系統與參考指引之適用性提出改善建議，於結案階段彙整說明。

關鍵詞	個人資料、個人資料保護

目　次

圖 目 次

表 目 次

1. 前言

1.1. 導入目的

技服中心於 100 年度完成「個人資料保護參考指引」編訂，為強化指引之可行性、適用性及有效性，乃遴選 2 個政府機關進行實務導入作業(以下簡稱本專案)。

1.2. 導入個案

個案 A：○○資訊單位。

個案 B：○○資訊單位。

1.3. 導入依據

本次導入驗證之參考指引為「個人資料保護參考指引」[3]。

1.4. 章節架構

本報告共分為 8 個章節，說明如下：

- 第 1 章「前言」，描述本專案欲達成的目標、參與導入個案、導入依據的內容及簡述本份文件的章節架構與各章節的摘要說明。
- 第 2 章「導入執行方式」，描述欲達成導入目標，規劃具體執行步驟為「開始」、「文件導讀」、「參考指引導入」及「結案」4 個階段。
- 第 3 章「導入個案 A」，執行 4 個階段的導入步驟，遴選「A1 系統」為導入目標，並依據「個人資料保護參考指引」所描述的各個階段，詳實記錄導入過程中的輸入與產出結果。

- 第 4 章「導入個案 B」，執行 4 個階段的導入步驟，遴選「B1 系統」為導入目標，並依據「個人資料保護參考指引」所描述的各個階段，詳實記錄導入過程中的輸入與產出結果。
- 第 5 章「改善建議」，描述導入過程中，導入個案與顧問對「個人資料保護參考指引」所彙整之整體改善建議，做為「個人資料保護參考指引」之修訂方向參考。
- 第 6 章「結論」，描述導入過程中，提供導入個案綜合性建議與結論，以呼應本專案之目標，驗證參考指引的適用性與有效性。
- 第 7 章「參考文獻」，詳列本報告所參考的文件或資料。
- 第 8 章「附件」，詳列本次實務導入結果與相關表單範例。

2. 導入執行方式

為使導入步驟有所依循，茲規劃具體執行步驟為「開始」、「文件導讀」、「參考指引導入」及「結案」4 個階段，每個階段之重點工作詳見圖 1 所示。

資料來源：本計畫整理

圖1　參考指引導入實施步驟圖

2.1.「開始」

2.1.1. 前置作業

為利於專案順利進行，由導入之機關與顧問協商作業執行細節，並召開「導入啟動會議」，由顧問說明導入執行方式、時程及討論雙方應配合事項。

2.1.2. 訂定個資風險等級

2.1.2.1. 個資風險等級基準值

本次導入個資風險等級以「含有個資類別」、「NIST SP800-122 之衝擊等級」及「資訊系統分類分級與鑑別機制」影響構面等 3 個面向，分別檢討其風險等級，再採最高原則評定為該個資之風險等級，其中「資訊系統分類分級與鑑別機制」影響構面，則依資安會報所頒「資訊系統分類分級與鑑別機制參考手冊」(以下簡稱鑑別機制)[2]之 6 大構面中，「資料保護受到損害」、「影響法律規章遵循」及「損害本機關信譽」3 者作綜合考量。

2.1.2.2. 衝擊分析

本次導入依據為「個人資料保護參考指引」之衝擊分析，以該個資項目之衝擊分析檢核表內容檢視個資可能之衝擊。

2.1.2.3. 風險評估

針對組織所擁有個資項目的機密性、完整性及可用性等構面向，進行個資風險評估作業，以瞭解個資項目之風險等級，並彙整相關個資衝擊分析結果，做為後續擬訂安全控制措施之依據。

2.1.2.4. 決定資訊系統範疇與邊界

本次導入個案 A 將由 10~20 個含個資系統遴選 1 個做為導入目標，遴選方式依個資風險等級基準值與衝擊分析檢核表部分欄位，進行風險等級分析，以風險等級最高者-「A1 系統」做為導入目標，並據以討論導入系統範疇與邊界，未來該單位其他系統可依本次導入相關程序與方法實作。

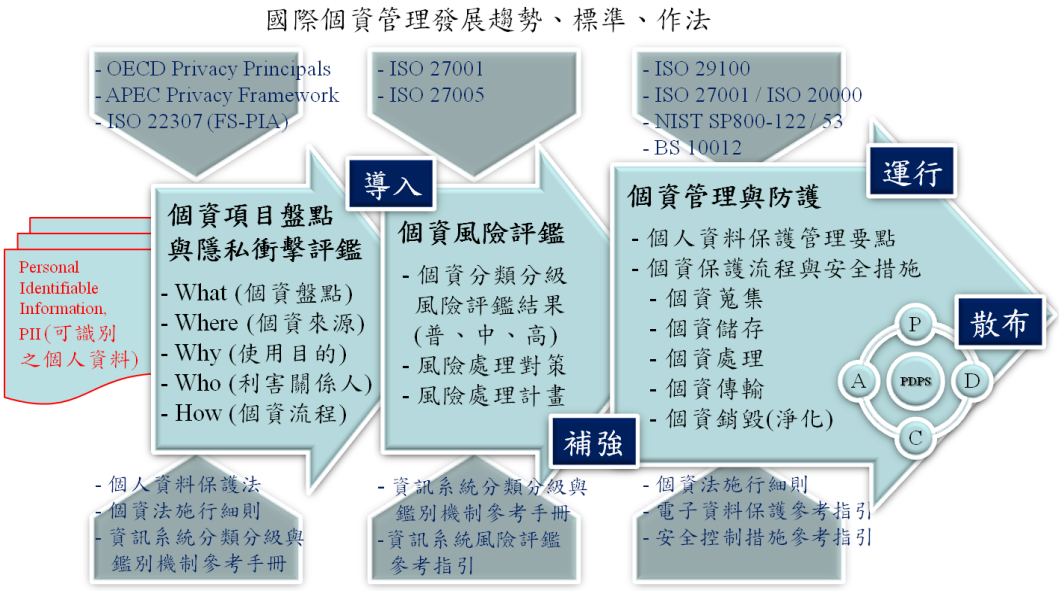
個案 B 為展現對導入計畫之支持與承諾，由該機關自行篩選 2~3 個業務或系統列為導入候選對象，再經討論後，自行遴選 1 個含個資業務-「B1 業務」，做為導入目標。

2.2.「文件導讀」

由導入顧問透過簡報說明個資國際發展趨勢、我國個資相關規範、個人資料保護參考指引簡介及資訊安全管理制度(ISMS)與個資保護整合建議。導讀重點如下：

2.2.1. 個資保護發展趨勢與標準規範

個資管理對任何組織而言，需要隨時因應內外部趨勢、法律、規範及環境的變化，進行調整與持續提升改善。運用許多管理制度常見的規劃(Plan)-執行(Do)-檢核(Check)-改善(Act)的 PDCA 循環，對組織而言是非常適切之作法。因此 PDPS 的方法中也加入當個資管理與防護運行後的持續改善活動建議，並期待藉由此項政府機關實作，將相關良好實務推廣散布至其他非公務機關參考運用，因此在導讀中，導入顧問亦說明國內外個資保護發展趨勢與相關標準規範之關係，詳見圖 2。



資料來源：本計畫整理

圖2　個資保護發展趨勢與標準規範

2.2.2. 個資國際相關規範

2.2.2.1. OECD 隱私保護及個人資料之國際傳輸指導方針

經濟合作發展組織(Organization for Economic Co-operation and Development, OECD)於 1980 年發布之「隱私保護及個人資料之國際傳輸指導方針(Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data)」[8]，已成為國際組織(如 APEC 等)與國家制定其相關隱私保護綱領、原則之參考。OECD 隱私保護及個人資料之國際傳輸指導方針明列 8 大原則如下：

- 限制蒐集原則(Collection Limitation Principle)：例如僅蒐集執行活動所需之最小範圍內容之個資，明確列出限制蒐集之個資類別或內容等。
- 資料品質原則(Data Quality Principle)：例如所蒐集之個資必須明確與蒐集目的有關，且應保持個資內容之正確性與完整性，當個資內容有異動時即時進行更新。
- 目的明確化原則(Purpose Specification Principle)：例如採用正面表列的方式明確說明對個資進行蒐集之目的，而非概括性用語或類似「...等用途」的說明方式。
- 限制利用原則(Use Limitation Principle)：例如對於個資之處理、利用及國際傳輸等活動，明確設定程序管控，不逾越特定蒐集目的以外之利用。
- 安全保護原則(Security Safeguards Principle)：例如對於個資之處理、利用及國際傳輸等活動中所潛在的揭露風險，建立合適的安全控制措施，如對個資檔案進行加密、設定存取權限及防火牆保護等。
- 公開原則(Openness Principle)：例如組織主動對外公開所擁有之個資檔案名稱、法律依據、特定目的、保存期間及聯絡窗口等資訊。

- 個人參與原則(Individual Participation Principle)：例如當事人對於個資自主權之行使像是查閱、更正及要求刪除個資內容等之規範。

- 責任原則(Accountability Principle)：例如建立個資管理組織人員之職責職掌，使相關人員能夠依循相關政策與程序進行個資管理活動。

2.2.2.2. APEC 隱私保護綱領

亞太經濟合作會議(Asia-Pacific Economic Cooperation, APEC)「隱私保護綱領(Privacy Framework)」[9]緣起於 APEC 1998 年電子商務行動計畫，要實踐電子商務相關技術與政策，必須建立安全、保密且可信賴的通訊、資訊及傳輸系統，並重視隱私議題。此外，非必要性地限制或增加資訊流動規定，也會對全球性的商業經濟活動造成負面影響。因此，有必要發展一套可保護個資與兼顧全球經濟發展活動的隱私制度，促進 APEC 會員經濟體之個資蒐集、存取、利用或處理的組織發展，並執行有關個資存取與利用的全球化標準程序，因而制定 APEC 隱私保護綱領，其內容與 OECD 1980「隱私保護與個人資料之國際傳遞指導方針」的核心價值相符，包括 9 項 APEC 隱私保護原則。

- 預防損害(Preventing Harm)

  包括指派組織內負責個資管理之專責人員角色、建立適當之管理機制，以及當發生個資事故時之即時通知與處理措施等。

- 告知(Notice)

  符合法令要求與個資當事人需求之告知程序與形式，包括告知之時機、方式、應涵蓋的內容、確認方式及例外處理原則等。

- 蒐集限制(Collection Limitations)

明確定義個資類別與其相關之蒐集限制條件、進行蒐集之依據、當事人同意之方式及有效期限之設定等。

●個人資料之利用(Uses of Personal Information)

須符合蒐集目的與範圍內之利用，明確定義例外處理原則等。

●當事人自主(Choice)

當事人對其個資進行查詢、閱覽、製給複製本、補充或更正、要求停止蒐集、處理或利用及刪除等權利須予以保障，並在適當時限內回應等。

●個人資料之完整性(Integrity of Personal Information)

依據當事人自主或蒐集時限屆滿等需求，即時維護個資之完整性與保存狀態等。

●安全管理(Security Safeguards)

採行適當之安全措施，以防止個資遭受到竊取、竄改、毀損、遺失或洩漏等情況。

●查閱和更正(Access and Correction)

依據當事人自主對於個資查閱或更正之需求適時回應，此外須公告所蒐集個資之檔案名稱、蒐集組織與聯絡人資訊、保有之依據及特定目的、個資類別等資訊，以提供公眾進行查閱等。

●責任(Accountability)

規範當個資進行傳輸時，相關處理組織與人員之角色與責任，以避免個資之不當運用，同時保障當事人之隱私權等。

2.2.2.3. ISO 22307 金融服務-隱私衝擊分析(ISO 22307 Financial services-Privacy impact assessment)

- 公布日期: 2008 年 5 月 1 日。
- 由於電腦與網路的快速發展，促進金融服務組織能夠比以往更快速地記錄、保存及處理大量的當事人資料，同時也帶來對於個人隱私權侵犯的衝擊影響。而金融服務組織在運用當事人個資時，除了考量法規命令的要求外，亦要評估相關金融系統在開發與更新時，是否有妥善保護與避免不當使用當事人的資料，以提升對當事人的作業流程與服務。
- 為確保符合 OECD 隱私原則，組織應建立適當的隱私政策與實作方式，透過標準化的隱私衝擊評估活動，協助組織識別與隱私有關的風險，包括如何降低這些風險，協助組織建立隱私政策與實作方法。
- 由於隱私保護的要求在不同國家有所不同，此標準化的隱私衝擊評估工具，特別適用於含有跨境金融交易的全球性銀行。
- 金融機構隱私衝擊分析主要涵蓋領域
  - 起始隱私告知：包括評估在應用系統需求分析、設計、開發、測試及上線運作各階段活動中，對於隱私保護之措施與作法是否適當。
  - 年度隱私告知：對當事人定期性告知最新隱私政策內容。
  - 隱私告知之內容：例如蒐集組織名稱、目的、蒐集之內容及將被使用之方式等。
  - 退出(opt-out)/選定(opt-in)政策與告知：例如透過明顯標示提醒當事人可方便自主選擇對隱私之蒐集、處理及利用等方式是否接受或拒絕。

– 變更告知：例如當所蒐集之個資或隱私內容之處理、利用目的或方式，和原本蒐集目的已有變更不同時，是否能即時告知當事人並取得同意。

– 傳遞方式：評估應用系統在傳遞個資檔案時，是否已建立適合的保護機制，例如加密的傳輸管道、權限及密碼控管等。

– 揭露至非分支機構的第三方之限制：例如在蒐集目的告知時，即正面表列出參與之相關第三方，以及相關之執行方式與範圍等。

– 再揭露與再使用資料之限制：例如對於是否即時告知當事人並取得同意後方可進行之管控措施。

– 服務提供者與聯合行銷的退出(opt-out)/選定(opt-in)之例外要求。

– 處理與服務交易的退出(opt-out)/選定(opt-in)與告知之例外要求。

– 退出(opt-out)/選定(opt-in)與告知之其他例外要求。

2.2.2.4. BS 10012 資料保護-個資管理系統規格(BS 10012:2009 Data protection-Specification for a Personal Information Management System)

- 公布日期：2009 年 5 月。
- 目的：提供一個保持與提升符合資料保護之法規與良好實踐之架構。
- 應用「Plan」、「Do」、「Check」及「Act」循環，持續提升管理系統維運要求。
- 主要依循英國資料保護法(The DPA-The Data Protection Act 1998)，DPA 係依據歐洲經濟區(European Economic Area, EEA)的 European Directive(95/46/EC)所制定。個資在 DPA 稱為 Personal Data，BS 10012 則以 Personal Information 代表。

●DPA 由英國資訊專員辦公室(Information Commissioner)負責資料保護相關規劃、管理、教育及監督等事宜。

●BS 10012:2009 中 8 項資料保護原則

– 公平與合法的處理：例如依據個資法之規範進行個資管理。

– 僅獲取符合符定目的的資料，並於後續處理資料時不逾越這些目的。

– 適當、相關、不過度：應用限制蒐集原則，僅蒐集所需最少的個資。

– 正確與更新：提供當事人自主權利行使時的管道和便利的方式。

– 不保留超出所需的時間：明確定義相關個資檔案之保存期限，和到達期限後之處理方式。

– 處理程序符合法律賦予個人的權利，包括有關存取的權利。

– 保持安全。

– 未經適當的保護措施不得傳輸至 EEA 以外的國家。

●BS 10012:2009 標準架構

– 簡介(Introduction)：說明個資管理系統(Personal Information Management System, PIMS)係提供維護與改善的框架(framework)，以符合個資保護相關法律與實務要求。

– 範圍(Scope)：說明本標準係提供一個共通基礎以管理個人資料，故適用於各種型態的組織。

– 名詞定義與縮寫(Terms, definitions and abbreviations)：定義標準中所提及之各項名詞與縮寫，例如稽核(audit)、程序(procedure)等。

– 規劃 PIMS(Planning for a personal information management system)：說明規劃階段包括的活動項目，本階段的目的為提供 PIMS 實施的方向與支援，以符合個資保護與實務的要求。

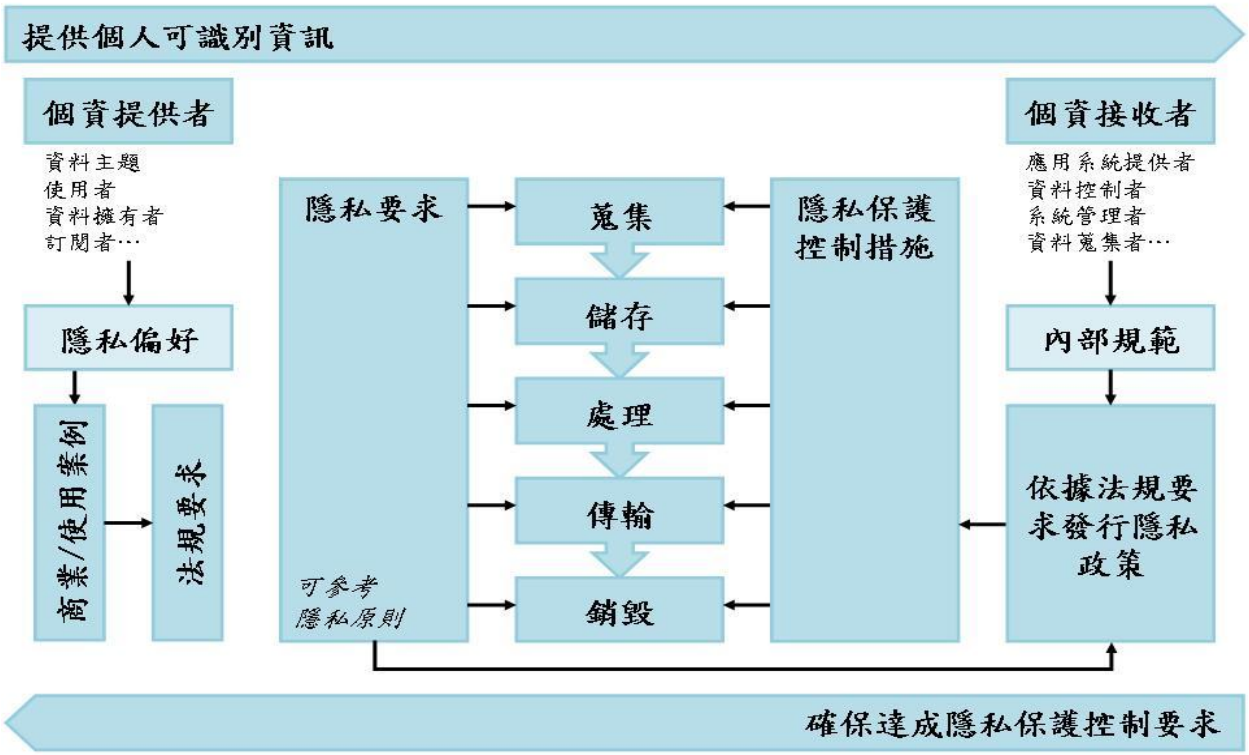
– 建置與運作 PIMS(Implementing and operating the PIMS)：說明建置與運作階段包括的活動項目，本階段的目的在於確保組織依照政策中的要求，指派適當的權責人員。

– 監督與檢視 PIMS (Monitoring and reviewing the PIMS)：說明監督與檢視階段包括的活動項目，本階段的目的為確保 PIMS 的效率與有效性受到適時的監督與檢視。

– 改善 PIMS(Improving the PIMS)：說明改善階段包括的活動項目，本階段的目的是藉由矯正行動的實施以改善 PIMS 的效率與有效性。

2.2.2.5. ISO/IEC 29100 資訊科技-安全技術-隱私框架(Information technology-Security techniques-Privacy framework)

- 公布日期: 2011 年 12 月 15 日。
- 規劃個資提供者與接收者之間，有關個資蒐集、儲存、處理、傳輸及銷毀等作業流程內容，詳見圖 3。



資料來源：Rannenberg, K. (WG5 Convener), Sténuit, C. (Co-editor 24760), Yamada, A. (Editor 24761), and A.S. Weiss (Editor 29100/29101) (2007) Working Group 5 Identity Management and Privacy Technologies Within ISO/IEC JTC 1/SC 27-IT Security Techniques (Presentation), 2007-09-30，本報告中文化翻譯

圖3　ISO/IEC 29100 隱私框架示意圖

2.2.2.6. NIST SP800-122

- 公布日期：2010 年 4 月。
- 目的：過去幾年來，包括數百萬筆個資紀錄遺失的資安事故層出不窮，因而對個人與組織造成傷害，如身分竊取、詐騙、信任感喪失、法律責任及矯正成本等。因此，保護個資的機密性實有其必要性，故美國國家標準與技術局(National Institute of Standards and Technology, NIST)制定本文件，

主要提供聯邦政府機關及其相關委外單位，於執行個資保護時之參考建議，其他組織亦可參照運用。

- 目標：本文件除說明個資防護的重要性外，並以風險為基礎，建議各項防護措施與事故回應計畫(Incident Response Plan)。

- 文件架構：本文件共分為 5 個章節，第 1 章介紹文件的目的與範圍、使用對象及文件架構；第 2 章描述何謂個資，並如何找出組織所維護的個資；第 3 章說明當個資遭到不當的存取、使用及揭露時，如何決定衝擊等級因素；第 4 章提供保護個資機密性的控制措施，以降低個資被洩漏的風險；第 5 章提出如何發展個資事故回應計畫，並整合至組織現有的事故回應計畫中。

- 主要內容：

  – 個資辨識。

  – 個資運用。

  – 個資分類。

  – 個資保護。

  – 個資事故回應計畫。

  – 密切協調。

2.2.3. 我國個資相關規範

「電腦處理個人資料保護法」於 84 年 8 月 11 日公布施行，當初規範非公務機關之適用主體有行業類別之限制，僅限於徵信業、醫院、學校、電信業、金融業、證券業、保險業及大眾傳播業等八行業，一般行業與個人均不受規範，保護之客體亦只限於經電腦處理之個資，不包括非經電腦處理

之個資，對於保護個資隱私權益之規範顯有不足，故法務部自 90 年起即積極進行相關修法工作，於整理國內學界與實務界之修法意見，並參酌各國個資保護之立法例，經召開多次公聽會與研討會後，研擬「電腦處理個人資料保護法修正草案」，報請行政院審查，行政院院會業於 93 月 9 月 8 日通過，並函送立法院審議。

法務部所擬電腦處理個人資料保護法修正草案(修正後名稱為「個人資料保護法」)，歷經多年來審查、協商及立法院「屆期不續審」再重報，終於在 99 年 4 月 27 日三讀修正通過，使個資法在保障個人隱私資料，並兼顧新聞自由平衡下邁向新的里程碑，個資法強化個資揭露、查詢及更正等的自主控制，同時也將「亞太經濟合作論壇(APEC)隱私保護綱領」所揭示的預防損害、告知及蒐集限制等 9 項原則納入規範，以迎接個資保護全球化時代的來臨。

本次修法重點：

●擴大保護客體。

●普遍適用主體。

●增修行為規範。

●強化行政監督。

●促進民眾參與。

面對個資法之施行，政府機關即將面對的主要衝擊如下：

●保護客體範圍擴大。

●作業流程調整需求。

●舉證與處罰之預防。

依據個資法第五十六條本法施行日期，由行政院定之。其施行日期經法務部於 101 年 9 月 26 日完成施行細則修訂頒布後，由行政院頒布本法除第 6 條、第 54 條外施行日期為 101 年 10 月 1 日。

有關個人資料保護法施行細則修正要點，摘要說明如下：

- 為明確以間接方式識別該個人資料之意義及提供不能識別該個人資料之判斷標準；病歷、醫療、基因、性生活、健康檢查及犯罪前科之概念；刪除、內部傳送、當事人自行公開、已合法公開之個人資料、資料經過處理後或依其揭露方式無從識別特定當事人等概念，增列相關定義性規定，以資衡平個人資料保護與個人資料合理利用。
- 為保護個人資料之隱私權，個人資料檔案除了備份檔案之外，亦應包括軌跡資料在內。
- 受委託蒐集、處理或利用個人資料之法人、團體或自然人，依個資法第四條規定，於個資法適用範圍內視同委託機關，係指以委託機關為權責歸屬機關，增訂委託人之適當監督義務規定。
- 增訂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之事項內容規定。
- 增訂個資法所稱書面意思表示之方式及單獨所為之書面意思表示之意涵。
- 增訂個資法規定告知之方式。

此外，施行細則第 12 條所述之必要措施，共計 11 項：

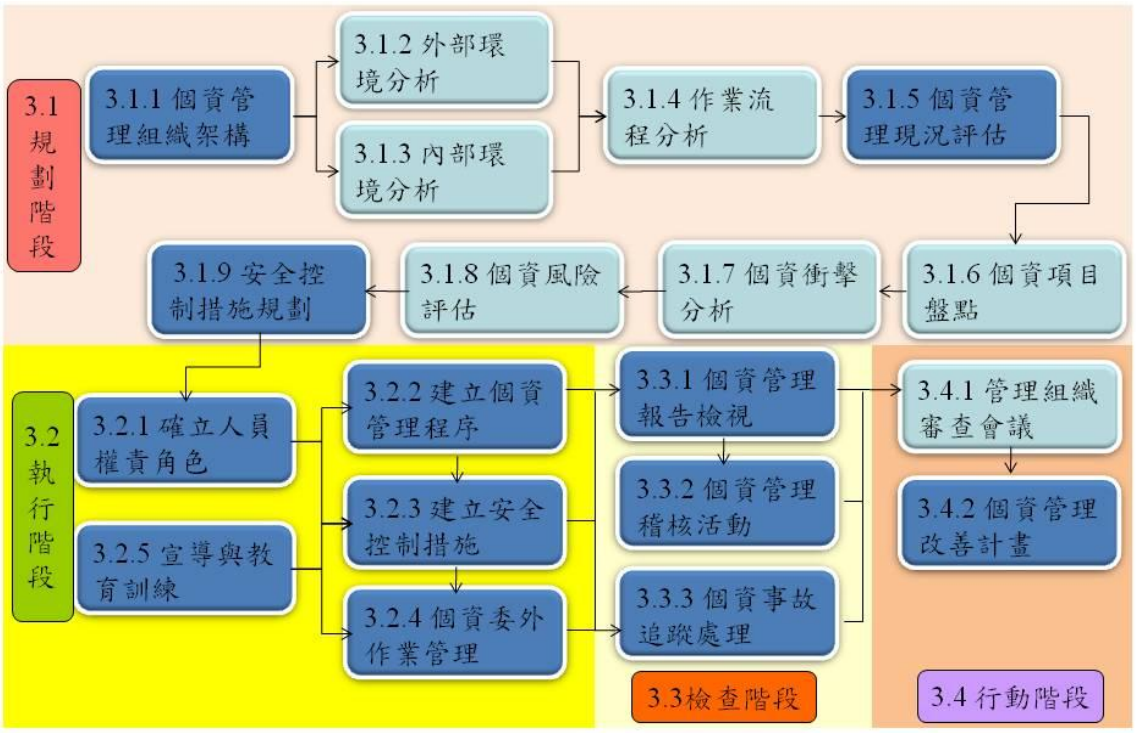
- 成立管理組織，配置相當資源：專人、專責組織負責個資保護相關事宜。

- 界定個人資料之範圍：即進行個資盤點，必須知道誰使用那些資料並且存放在什麼位置，包括紙本和電子個資。
- 個人資料之風險評估及管理機制：應針對個人資料進行風險評估，並提供相關管理機制。
- 個資資料蒐集、處理及利用之內部管理程序：制定個資保護相關的執行程序與標準作業流程。
- 資料安全管理及人員管理：說明對個資應該採取何種 IT 科技與系統進行保護；人員存取個資的權限管制等。
- 資料安全稽核機制：對於存放個資的 IT 系統定期進行資料稽核。
- 認知宣導及教育訓練：對於同仁應施行適當的個資宣導與訓練。
- 必要之使用紀錄、軌跡資料及證據之保存：IT 設備或者紙本資料個資存取控制的紀錄、日誌檔(Log)等，都必須完整保留，這些都可能是舉證的證據力。
- 設備安全管理：針對各種保存個資的載具或系統，應定期的維護與更新。
- 事故之預防、通報及應變機制：規範個資事故發生後的通報應變流程。
- 個人資料安全維護之整體持續改善：針對個資保護不足之處持續更新。

2.2.4. 個資保護管理建置流程

個資保護管理建置流程，遵循國際標準管理系統的 PDCA 循環分為規劃、執行、檢查及行動 4 個階段，每個階段分別有不同的活動(Activity)，例如個資管理組織架構、個資項目盤點、個資衝擊分析、個資風險評估、建立個資管理程序及建立安全控制措施等。其中每項活動中有不同的任務(Task)需要執行，而過程中可能需要各種不同資訊的提供，再輔以各種執行手法

與相關工具，完成該項任務，任務如有產出將可能成為其他任務或活動執行時所需參考之資訊。例如在「個資管理組織架構」活動中，需要進行「瞭解組織現行架構(含單位別與功能性)和人員角色職責」之任務，因此，必須先瞭解「單位組織圖、管理制度架構圖、角色職責分工定義」等資訊，並透過「資料蒐集、人員訪談」方式，達成該項任務之目的，最後再進一步去定義「個資管理組織」架構，個資保護管理建置流程之整體發展架構，詳見圖 4。



資料來源：本計畫整理

圖4　個資保護管理建置流程之整體發展架構

●規劃階段

– 活動：個資管理組織架構

依據組織的需求與特性，規劃後續進行個資管理活動所需之功能性組織架構，以及架構中相關人員的角色職責，以利溝通協調運作。同時擬定組織的個資管理政策與要點，做為後續執行個資管理活動的最高指導原則。

– 活動：外部環境分析

瞭解組織外部環境對於個資的相關需求，例如個資法與其施行細則、國際隱私保護原則及個資管理標準等，並識別與分析和組織間有個資往來活動之外部利害關係人，例如當事人、供應商、委外廠商或人員、合作組織及策略聯盟等。

– 活動：內部環境分析

識別與分析組織內部現行和個資有關的管理制度內容、應用範圍、單位或人員等資訊。然後彙整個資內外部環境與利害關係人之分析結果，做為組織規劃與建置後續個資保護管理各階段範圍的參考。

– 活動：作業流程分析

依據組織所規劃後續各階段建置個資管理的範圍，進行相關服務目錄與服務等級協議、業務作業流程及委外作業流程的分析，以明確定義各階段範圍涵蓋那些與個資有關之流程或應用系統。

– 活動：個資管理現況評估

本項為選擇性活動，組織可透過個資管理整體準備度評估問卷，對個資管理的現況進行評估，以瞭解目前在個資管理相關領域準備度較為不足之處，並針對主要差異項目進行提升與改善，亦可將準備度評估結果，做為未來提升比較之參考基準。

– 活動：個資項目盤點

盤點組織所擁有之個資項目內容，包括個資項目之類別、目的、來源、欄位、數量、型態、相關的生命週期活動及相關利害關係人等，以利後續進行個資之衝擊分析、衝擊評鑑、保護及管理等活動。

– 活動：個資衝擊分析

藉由適當的衝擊評估與分析活動，瞭解個資項目或針對處理大量個資之應用系統，所可能面臨之個資洩露的弱點與威脅，及可能造成組織的衝擊與損失，以便及早採取可行之防範對策或行動方案，避免個資洩露事故之發生。

– 活動：個資風險評估

針對組織所擁有個資項目，依據其個資類別(如一般個資或特種個資)與數量、個資之機密性/完整性/可用性被破壞時，會對組織/資產/人員造成的傷害等構面，進行個資風險評估作業，以瞭解個資項目的衝擊等級，並彙整相關個資衝擊分析結果，做為後續規劃安全控制措施之參考依據。

– 活動：安全控制措施規劃

組織於進行個資風險評估後，依法規命令與組織可運用之資源，並參考個資保護技術安全控制項目基準值建議表，規劃組織內不同衝擊等級之個資保護技術方案與管理程序。

●執行階段

– 活動：確立人員權責角色

依據組織內個資項目的生命週期，建立組織人員對應各階段活動的個資存取權責與角色，以確保組織對個資的蒐集、處理及利用等活動，符合

相關法規命令與組織的個資管理政策，同時做為個資管理程序與安全控制措施的運作基礎。

– 活動：建立個資管理程序

依據個資相關法規命令、組織個資管理政策，建立組織之個資管理流程與程序，降低個資洩露或違反相關法規命令的風險。

– 活動：建立安全控制措施

依據個資相關法規命令、組織個資管理政策及個資安全控制措施規劃，建立組織相關個資管理安全控制措施，降低個資洩露或違反相關法規命令的風險。

– 活動：個資委外作業管理

針對個資委外作業，依據個資相關法規命令、組織個資管理政策及個資安全控制措施規劃，透過相關委外契約要求及稽核活動，確保委外作業建立必要的個資管理流程、程序及安全控制措施。

– 活動：宣導與教育訓練

依據組織個資管理之目標與需求，建立並實施個資管理相關人員訓練計畫。

●檢查階段

– 活動：個資管理報告檢視

運用 PDCA 機制，依據個資管理政策與目標，定期與不定期檢視個資管理活動與紀錄，或進行趨勢分析。針對可能無法達到或未達到目標之項目，適時提出矯正預防行動方案，以持續提升組織個資管理成效。

– 活動：個資管理稽核活動

運用 PDCA 機制，規劃定期與不定期對組織個資管理，包括個資委外作業活動的稽核，以發掘未落實執行之活動或潛在改善之機會。針對稽核發現提出矯正預防行動方案，以持續提升組織個資管理成效。

– 活動：個資事故追蹤處理

因應個資事故通報與處理回應，包括對於個資事故可能需要之數位證據與數位鑑識處理上的需求等，建立相關作業程序與人員職責角色分派，並與組織相關之資安事故程序予以整合運作，以發揮流程運作之效率。

●行動階段

– 活動：管理組織審查會議

針對設定期間個資管理相關重要議題與績效，進行階段性審查，並與相關利害關係人溝通個資管理的成效。對重大計畫或議題進行決策，並提供後續個資管理活動所需之相關資源。

– 活動：個資管理改善計畫

運用 PDCA 機制，分析並彙整相關可提升個資管理活動的潛在機會，提出個資管理改善計畫，追蹤檢視執行成果，持續改善提升組織的個資管理系統。

2.3.「參考指引導入」

本專案 2 個導入機關將各選取 1 個資訊系統或個資業務，依據個資保護管理建置流程的步驟執行：規劃階段與執行階段，作法詳述如下：

2.3.1. 規劃階段

規劃階段主要先針對組織內個資管理現況、內外環境的個資需求及組織作業流程中可能與個資相關項目，進行整體瞭解，並架構出個資管理所需之功能性組織,再整合前項個資管理整體準備度與主要風險領域評估的結果、個資盤點整理出之個資流程與項目及應用系統個資衝擊分析結果等，進行個資衝擊分析與個資風險評估，藉此瞭解組織所蒐集、處理及利用相關個資之風險等級，並對應至適當的安全控制項目基準值，做為發展技術控制措施，後續個資管理與防護實作的依據。

本階段之活動包括個資管理組織架構、作業流程分析、個資項目盤點、個資衝擊分析、個資風險評估及安全控制措施規劃。

2.3.1.1. 個資管理組織架構

為展現組織對個資保護的承諾與決心，導入單位應成立個資管理組織，由各部門代表參與，明確界定該組織內相關角色職掌，並且由專人擔任個資保護聯絡窗口，做為統一的個資管理溝通管道。

個資管理組織架構之任務，包括瞭解組織現行架構(含單位別與功能性)與人員角色職責、定義個資管理組織、定義個資管理組織人員角色職責、建立個資管理政策與要點及發布個資管理組織架構。有關每項任務內容，說明如下：

●瞭解組織現行架構(含單位別與功能性)與人員角色職責

可蒐集單位組織圖、管理制度架構圖及角色職責分工定義等相關資料，再配合人員訪談方式，瞭解各部門的作業內容是否與個資相關或持有個資。

●定義個資管理組織

應有高層主管擔任召集人，並由跨部門人員(建議由部門主管)參與。對於已導入 ISMS 的單位，可考量將 ISMS 與個資適當整合成一個管理組織。

此外，當個資管理涵蓋範圍超過資訊單位的業管範圍時，建議考量由其他適當部門主辦與協調，進行個資管理活動之推動。

●定義個資管理組織人員角色職責

在個資管理組織中，應明確描述各人員的角色與職掌，並建議由個資保護專責人員擔任此功能性組織之溝通協調。該組織人員可包括召集人、個資保護專責人員、個資聯絡窗口、個資保護規劃小組、個資保護應變小組、個資保護文件管制小組及稽核小組等，有關個資管理組織與角色職責分工範例詳見表 1。

表1　個資管理組織與角色職責分工範例

組織架構角色	工作職掌
召集人	▪擔任個資與隱私保護之召集人，統籌決策及組織資訊安全與個資與隱私保護管理業務之資源整合運用 ▪每年審核並頒行個資保護與隱私政策 ▪指派個資管理推動組織架構所需之角色人員，如個資保護專員、個資保護聯絡窗口、資訊服務管理組個資保護工作組長等 ▪核定個資管理文件的制定、修訂及廢止 ▪定期或不定期審核個資與隱私保護計畫 ▪審核內部稽核之稽核計畫與稽核報告 ▪審核個資管理推動所須之資源及計畫，並編列相關預算，如人員任用及教育訓練計畫等
個資保護專責人員	▪協助召集人推行個資管理 ▪依相關法規命令辦理安全維護及保管事項 ▪傳達召集人之決策，以貫徹個資管理 ▪協調各組使組織相關個資保護之運作更落實

組織架構角色	工作職掌
	▪彙集、轉陳各組之意見、資料，供召集人做最佳決策 ▪協助追蹤、管理個資保護稽核所提相關建議事項 ▪定期蒐集、分析及陳報個資相關通報及執行狀況之報告
個資聯絡窗口	▪機關對外之個人資料保護業務聯繫協調 ▪個人資料安全事故通報 ▪重大個人資料外洩事件單一聯繫窗口 ▪接受與回覆當事人依法提出個人資料權利之請求事宜
個資保護規劃小組	▪協助召集人與個資保護專責人員推行執行個資管理活動 ▪傳達召集人之決策，以貫徹個資管理 ▪執行各組工作使相關個資保護之運作更落實 ▪轉陳各組之意見、資料予個資保護專員彙整供召集人進行決策 ▪協助追蹤、管理個資保護稽核所提相關建議事項 ▪定期蒐集、分析及陳報個資相關通報及執行狀況之報告
個資保護應變小組	▪個人資料事故處理與應變相關資源之規劃與取得 ▪個人資料事故通報、處理及應變相關活動內外部聯繫與協調 ▪個人資料事故證據之保存、鑑識及調查分析 ▪個人資料事故之公關與客服處理 ▪個人資料事故通報、處理及應變相關活動之教育訓練與演練 ▪個人資料事故通報、處理及應變目標與程序之持續改善提升
個資保護文件管制小組	▪核定之個資保護文件登錄、發行、保存等相關管理工作

組織架構角色	工作職掌
各單位專責人員	▪落實個資與隱私保護相關作業規範 ▪配合執行或參加個資與隱私保護相關教育訓練 ▪執行管理階層於個資與隱私保護之決策及交辦事項 ▪配合召集人或所授權人員執行風險審查包括： ➢ 鑑別與盤點單位之個資項目 ➢ 鑑別個資項目潛在風險與提出需求 ➢ 鑑別個資項目所須之安控機制 ➢ 各類隱私事故之報告與處理 ➢ 參與並推廣個資管理與隱私保護觀念教育訓練
委外廠商與相關人員	▪遵循組織制定之個資保護與隱私政策與相關作業規範 ▪配合組織辦理之個資與隱私保護管理稽核活動
稽核小組	▪研提年度個資與隱私保護管理稽核計畫 ▪配合年度稽核計畫執行相關稽核活動並提供改善建議事項予召集人

資料來源：本計畫整理

●建立個資管理政策與要點

個資管理政策與要點為組織內對個資管理之最高指導原則，應於核定後公告至所有同仁，並納入一階文件進行維護管理。政策內容包括目的、目標、原則及適用範圍；要點包括個資管理組織架構說明、個資範圍、如何蒐集/處理/利用個資、當事人行使權利之處理及個資檔案安全維護等。

●發布個資管理組織架構

個資管理組織架構經核定後，應將此組織架構、個資管理政策與要點，透過電子郵件、內部網站或書面文件等方式，公告通知所有同仁。

2.3.1.2. 作業流程分析

當組織決定各階段的導入範圍後，接下來應著手分析該範圍內與個資相關流程與應用系統，因此，藉由分析服務目錄、服務等級協議、業務作業流程及委外作業流程的過程，才能準確掌握組織所擁有的個資項目。

作業流程分析之任務，包括：

●分析服務目錄與服務等級協議(Service Level Agreement , SLA)

所謂服務目錄(Service Catalog)係組織提供所有服務項目的列表，這些服務不只是對外的服務，也包括組織內各單位對內部其他單位所提供的服務，例如資訊部門提供之機房維運服務等。另外 SLA 為服務提供者與服務使用者之間的協議，載明使用者要求及提供者承諾，通常 SLA 涵蓋項目包括服務正常運作時間、隱私權、安全及備份程序等。從服務目錄與 SLA 中，發掘可能與個資有關的服務或安全要求，以瞭解目前是否還有不足之處。例如，SLA 中載明針對包括個資的資料應定期進行備份，但卻未定義該備份資料應具有適當的存取控制措施等。

●分析業務作業流程

就如同導入資訊安全管理制度一樣，從業務作業流程面著手分析，較能夠找出與該業務相關之個資項目，並針對該項目進行適當保護。通常分析業務作業流程，可從與該業務作業管理相關之文件程序與規範著手，例如，人事作業中之招募程序，當對外招募人員時，會收到應徵人員之履歷資料，其中即包括應徵者之個資。

●分析委外作業流程

對於承接包政府機關委外作業之廠商，如有執行個資蒐集、處理及利用等相關作業時，雖屬非公務機關，但因受公務機關委託，其應遵守之規範與

限制，比照公務機關辦理。因此，政府機關於辦理委外作業時，應瞭解該作業是否包括個資項目，除自我要求遵守個資法規定外，更須要求委外廠商亦須遵守個資法。例如，可於契約中要求對委外廠商定期或不定期執行個資管理稽核作業，以確保廠商落實個資保護相關規定。

●定義和個資相關之流程與應用系統範圍

透過服務目錄與流程分析，掌握與個資相關之作業流程與應用系統清單，後續可提供個資項目盤點活動使用。

2.3.1.3. 個資項目盤點

個資項目盤點主要目的在盤點組織所擁有之個資項目內容，包括個資項目的類別、目的、來源、欄位、數量、型態、相關生命週期活動及相關利害關係人等，以利後續進行個資之個資衝擊分析、個資風險評估、保護及管理等活動。

個資項目盤點之任務，包括識別不同作業流程之個資項目、識別個資項目之類別、依據及目的、識別個資項目相關生命週期活動、識別個資項目與外部利害關係人之關聯及完成個資項目盤點。有關每項任務內容，說明如下：

●識別不同作業流程之個資項目

進行個資盤點時，首先分析服務目錄與服務等級協議中，各服務內容之作業流程與應用系統清單，並經由訪談方式識別含個資之業務或服務作業流程，填註於個資流程分析表(詳見表 2)。

●識別個資項目之類別、依據及目的

組織應將識別出之個資項目，依個資法與其施行細則所規定之個資管理應完成事項清單、行政命令、準則，識別個資項目之蒐集範圍、類別、蒐集依據及蒐集目的，做為未來通知利害相關人之依據，詳見表 3 與表 4。

●識別個資項目相關生命週期活動

個資法對於個資管理相關活動分為蒐集、處理、利用及國際傳輸等階段，分別定義如下：

– 蒐集：指以任何方式取得個人資料。

– 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：指將蒐集之個人資料為處理以外之使用。

– 國際傳輸：指將個人資料作跨國（境）之處理或利用。

另參考 ISO/IEC 29100 隱私框架草案架構，對於個資提供者與接收者之間，從個資的蒐集到銷毀階段，可分為數個細部階段，其中特將銷毀階段納入考量，建議政府機關除考量個資法對於個資管理相關活動外，宜將刪除或銷毀納入考量。個資項目生命週期詳見表 5。

表2　個資流程分析表

業務或服務作業流程		個人資料檔案名稱	是否為個資流程
服務目錄或流程名稱	子流程名稱		

資料來源：本計畫整理

表3　個資項目蒐集範圍

業務或服務作業流程		個人資料檔案名稱	姓名	生日	身分證號	護照號碼	特徵	指紋	婚姻	家庭	教育	職業	病歷	醫療	基因	性生活	健康檢查	犯罪前科	聯絡方式	財務情況	社會活動	直接識別	間接識別	間接識別的欄位
服務目錄或流程名稱	子流程名稱																							

資料來源：本計畫整理

表4　個資項目基本資料表

業務或服務作業流程		個人資料檔案基本資料					
服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	保有單位	檔案型態	保有依據	特定目的	個人資料類別

資料來源：本計畫整理

表5　個資項目生命週期

業務或服務作業流程		個人資料檔案名稱	個人資料檔案生命週期活動									
服務目錄或流程名稱	子流程名稱		蒐集方式	蒐集者	蒐集介面	儲存位置	複本或備份或異地備援位置	法定保存期限	自訂保存期限	連結或內部傳送對象與方式	刪除或銷毀方式	國際傳輸對象與方式

資料來源：本計畫整理

●識別個資項目與外部利害關係人之關聯

個資與隱私保護之利害關係人包括當事人、組織內部人員、委外人員、供應者及其他可能接觸到組織所屬個資之相關人員。本階段主要就個資項目盤點結果所識別出之個資項目，清查其與外部利害關係人在其不同生命週期的型態、相關文件、支援系統及彼此間之關聯，以做為建立委外管理控制之依據，詳見表 6。

表6　個資項目利害關係人

業務或服務作業流程		個人資料檔案名稱	利害關係人				
服務目錄或流程名稱	子流程名稱		當事人	組織內部	委外	供應者	其他

資料來源：本計畫整理

●完成個資項目盤點

綜整個資項目基本資料與利害關係人，完成個資項目盤點(詳見表 7)，做為後續個資衝擊分析與評鑑之依據。

表7　個資項目盤點表

業務或服務作業流程		個人資料檔案基本資料						利害關係人				
服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	保有單位	檔案型態	保有依據	特定目的	個人資料類別	當事人	組織內部	委外	供應者	其他

資料來源：本計畫整理

2.3.1.4. 個資衝擊分析

個資衝擊分析主要目的，在於瞭解個資在蒐集、處理及利用過程中，是否已符合組織所處環境的法規命令與個資保護政策等遵循性要求。

個資衝擊分析之任務，包括設計個資衝擊分析檢核表、進行個資項目個資衝擊分析及完成個資衝擊分析。有關每項任務內容，說明如下：

●設計個資衝擊分析檢核表

個資衝擊分析檢核表主要就個資在蒐集、處理及利用過程中，是否提供當事人相關權利(如查詢、閱覽及複製等)與定期審視個資保護管理措施等機制，設計檢核表，內容詳見附件 1_個資項目個資衝擊分析檢核表。

●進行個資項目個資衝擊分析

組織應依據個資項目盤點所完成之個人資料檔案名稱，各別填寫個資項目個資衝擊分析檢核表，並彙整所有檢核表內容至個資項目衝擊分析表(詳見附件 2_個資項目衝擊分析表)。

●完成個資衝擊分析

組織應依據上述個資項目衝擊分析表，討論相關改善方式，並撰寫個資衝擊分析報告，做為未來改善計畫之依據。

2.3.1.5. 個資風險評估

個資風險評估係針對組織所擁有個資項目的機密性、完整性及可用性等構面向，進行個資風險評估作業，以瞭解個資項目之風險等級，並彙整相關個資衝擊分析結果，做為後續擬訂安全控制措施之依據。

個資風險評估之任務，包括設計個資項目之個資風險等級基準值、分析個資項目個資性之風險等級及完成個資風險評估。有關每項任務內容，說明如下：

●設計個資項目之個資風險等級基準值

組織應依個資流程分析，藉由設計問卷與實地訪談，確認組織存在那些個資項目，以及這些項目是以何種形式存在(是以系統或者表單存在)與擁有之個資類別 (如一般個資或特種個資)。

另組織應就法律層面上洩露不同類別與數量個資時的違法性風險、保護可識別之個資的機密性、資訊資產之影響構面等，設計個資風險等級基準值。基準值設計可依據含有個資類別、NIST SP800-122「個人可識別資訊機密性保護指引」之衝擊等級判定方式，以及「資訊系統分類分級與鑑別機制」影響構面與個資項目價值對應等 3 個層面。含有個資類別係以在法律層面上，洩露不同類別與數量個資時的違法性風險，政府機關應依個資洩露筆數所造成之風險程度不同，以及個資法對於不當揭露個資時，在法律責任上之每筆賠償金額，訂定適當筆數做為數量之級距建議。在 NIST SP800-122「個人可識別資訊保護指引」之衝擊等級判定方式，係參考美國 NIST SP800-122(Guide to Protecting the Confidentiality of Personally Identifiable Information)做為技術性控制措施，該文件主要提供以風險為基礎的方法與指導方針，來協助保護可識別之個人資料的機密性。「資訊系統分類分級與鑑別機制」影響構面與個資項目價值對應，係依據鑑別機制之影響構面等級，進行對個資項目價值之對應。個資風險等級基準值建議，詳見表 8。

表8　個資風險等級基準值建議表

參考項目	個資風險等級		
	普	中	高
含有個資類別	未具有任何個資，或僅含有姓名、公務電話、公務傳真、公務E-mail 等公務個資，且公務個資筆數不超過特定筆數(依機關需求自行訂定)	含有一般個資，如姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業等「個人資料保護法」定義之個人資料數量在特定筆數(依機關需求自行訂定)以下，或公務個資數量超過特定筆數(依機關需求自行訂定)(含)以上	含有特種個資，如有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個資，或含有一般個資之資料筆數超過特定筆數(依機關需求自行訂定) (含)以上
NIST SP800-122「個人可識別資	若個資之機密性、完整性及可用性被破壞時會對本機關組織、資	若個資之機密性、完整性及可用性被破壞時會對本機關組織、資	若個資之機密性、完整性及可用性被破壞時會對本機關組織、資產或

參考項目	個資風險等級		
	普	中	高
訊機密性保護指引」之衝擊等級判定方式	產或人員造成有限的傷害(可能輕微影響本機關聲譽、但不會造成任何財務損失或遭受訴訟之情事)	產或人員造成傷害(可能會影響本機關聲譽、財務損失或遭受訴訟，但不至於對本機關業務之持續運作造成重大影響)	人員造成重大傷害(非常可能嚴重影響本機關聲譽、重大財務損失或重大訴訟，且可能造成本機關主要業務中止)
「資訊系統分類分級與鑑別機制」影響構面與個資項目價值對應	「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信譽」三者影響構面之安全等級皆為普或安全等級為中者不超過一項	「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信譽」三者影響構面的安全等級皆無高，且其中二項安全等級為中	「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信譽」三者影響構面之安全等級皆為中，或「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信譽」三者影響構面之其中一項安全等級為高者

資料來源：本計畫整理

「資訊系統分類分級與鑑別機制」影響構面與個資項目價值對應之安全等級設定原則詳見表 9。

表9　鑑別機制安全等級設定原則建議表

安全等級 影響構面	普 (等級 1)	中 (等級 2)	高 (等級 3)
1.資料保護受到損害	一般性資料 資料若外洩或遭竄改，不致影響個人權益或僅導致個人權益【輕微】受損	敏感性資料 資料若外洩或遭竄改，將導致個人權益【嚴重】受損之資料	機密性資料 資料若外洩或遭竄改，將危及國家安全、導致個人權益【非常嚴重】受損或造成極大規模之個人權益嚴重受損
2.影響法律規章之遵循程度	資訊系統運作、資料保護、資訊資產使用等須依循相關規範辦理，否則將導致機關違反法律規章並伴隨【輕微】不良後果	資訊系統運作、資料保護、資訊資產使用等須依循相關規範辦理，否則將導致機關違反法律規章並伴隨【嚴重】不良後果	資訊系統運作、資料保護、資訊資產使用等須依循相關規範辦理，否則將導致機關從【根本上】違反法律規章
3.損害組織信譽	若資訊系統發生資訊安全事故，將導致機關形象、信譽受到【輕微】損害	若資訊系統發生資訊安全事故，將導致機關形象、信譽受到【嚴重】損害	若資訊系統發生資訊安全事故，將導致機關形象、信譽受到【非常嚴重】損害

資料來源：資訊系統分類分級與鑑別機制參考手冊

●分析個資項目個資性之風險等級

每個個資項目應依個資風險等級基準值建議，就其含有個資類別、NIST SP800-122「個人可識別資訊機密性保護指引」之衝擊等級判定方式，以及「資訊系統分類分級與鑑別機制」影響構面與個資項目價值對應等 3 個層面之個資風險等級，填註 PIA/RA 安全控制項目基準值，詳見表 10。

表10 PIA/RA 安全控制項目基準值

業務或服務作業流程		個人資料檔案名稱	含有個資類別	NIST SP800-122「個人可識別資訊機密性保護指引」之衝擊等級判定方式	「資訊系統分類分級與鑑別機制」影響構面與個資項目價值對應
服務目錄或流程名稱	子流程名稱				

資料來源：本計畫整理

●完成個資風險評估

個資風險等級評估，係依據 PIA/RA 安全控制項目基準值之組織含有個資類別、NIST SP800-122「個人可識別資訊機密性保護指引」之衝擊等級判定方式，以及「資訊系統分類分級與識別機制」影響構面與個資項目價值進行對應，採最高原則方式判別，填註個資項目個資風險評估表，詳見表 11，主要區分為普、中、高。例如在個資類別評等為「中」，在 NIST SP800-122「個人可識別資訊機密性保護指引」之衝擊等級評等為「普」，在「資訊

系統分類分級與識別機制」影響構面評等為「高」，則其個資風險等級採最高原則應為「高」。

依所述之判定原則，評估每個個資項目之風險等級，即完成個資項目個資風險評估表內容，以做為檢討安全控制措施規劃之依據。

表11 個資項目個資風險評估表

業務或服務作業流程			個人資料檔案名稱	PIA/RA 安全控制項目基準值			個資性之風險等級
編號	服務目錄或流程名稱	子流程名稱		含有個資類別	NIST SP800-122「個人可識別資訊機密性保護指引」之衝擊等級判定方式	「資訊系統分類分級與鑑別機制」影響構面與個資項目價值對應	

資料來源：本計畫整理

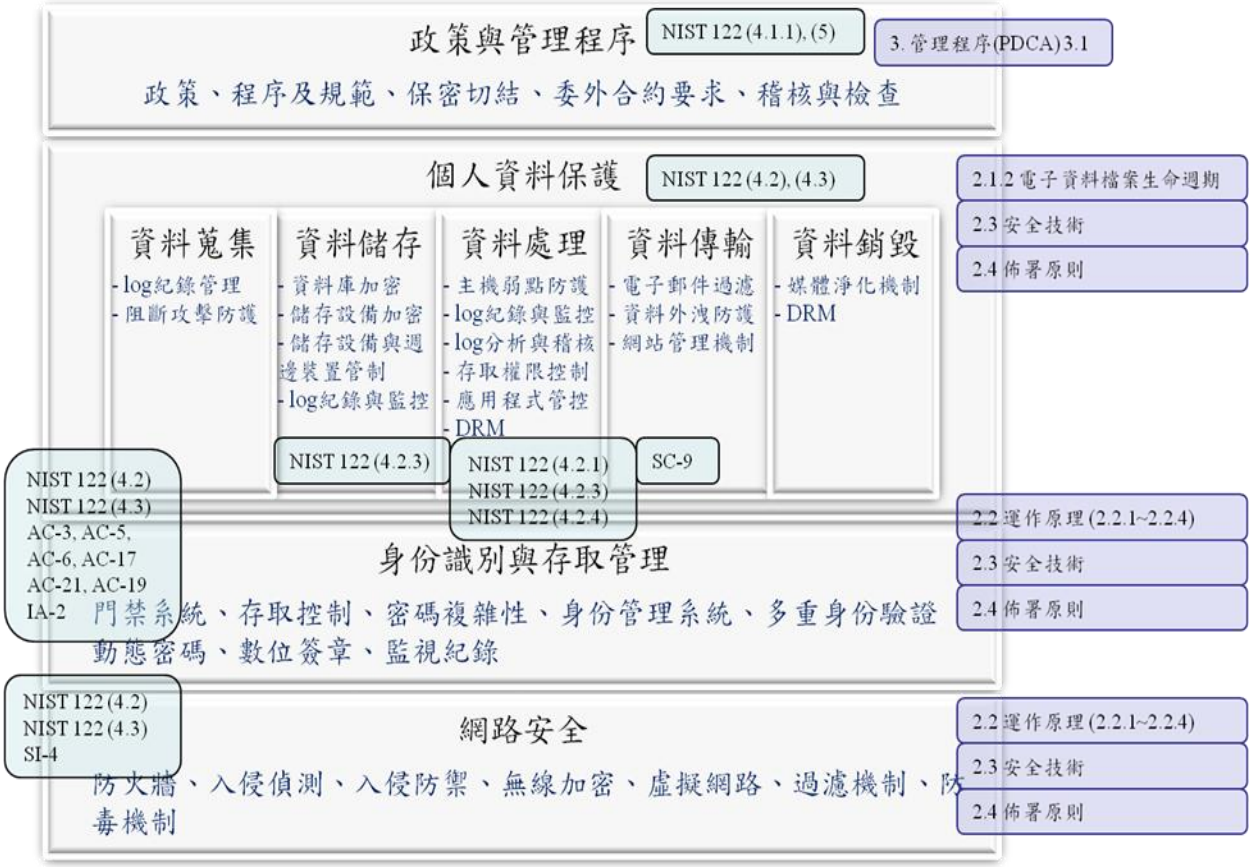
2.3.1.6. 安全控制措施規劃

安全控制措施規劃，係依據個資風險評估對於組織所擁有個資項目不同的風險等級，規劃不同風險等級個資保護技術方案與控制方法。

安全控制措施規劃之任務，包括規劃組織安全控制措施、評估所需資源及確認組織安全控制措施規劃內容。有關每項任務內容，說明如下：

●規劃組織安全控制措施

個資管理之防護技術架構，包括對於個資保護生命週期不同階段活動之安全措施項目、整體環境之身分識別與存取管理以及基礎設施網路安全管理等，整體架構詳見圖 5。



資料來源：本計畫整理

圖5　個資管理防護技術架構

依此架構，參考美國國家標準與技術局訂定之 NIST SP800 系列資訊安全相關指引(包括 NIST SP800-122 個人可識別資訊機密性保護指引、NIST

SP800-53 安全控制指引)、國際 ISO 27001 資訊安全管理標準及「電子資料保護參考指引」，並參考 NIST SP800-122 安全控制之普、中、高分級，綜整為個資保護技術安全控制項目基準值建議。個資保護技術安全控制項目基準值建議，請參閱個人資料保護參考指引表 17，由於個人資料之存在方式區分為紙本與電子檔案，其所需安全控制措施不同，經彙整個資保護技術安全控制項目基準值建議，依紙本與電子檔案需求，訂定技術安全控制措施基準值評估表詳見附件 3_個資項目技術安全控制措施基準值評估表。

●評估所需資源

組織應依據衝擊影響層面排定優先處理順序，再依組織個人資料保護管理要點、個資衝擊分析及個資風險評估所評估之個資風險等級，參考個資保護安全控制項目基準值建議表與「電子資料保護參考指引」，考量組織所負責任務的類別與性質、服務對象、內部資源及經費預算等因素，評估在有限資源下，需優先進行處理之安全控制措施，並列出要達到此業務目標與需求之安全控制措施所需資源。

●確認組織安全控制措施規劃內容

組織應依規劃所需之安全控制措施，排除組織目前已實作或已計畫實施中之控制措施，檢查所有應處理之衝擊，是否皆有合適之安全控制措施或應加強之安全控制措施，並訂定未來應建立之安全控制措施，經核定後做為實作安全控制措施依據。

2.3.2. 執行階段

執行階段為組織於評量個資整體環境、衝擊分析及衝擊評鑑後，依上階段的規劃結果，執行各項個資管理措施。

本階段之活動，包括確立人員權責角色、建立個資管理程序、建立安全控制措施、個資委外作業管理及宣導與教育訓練。

2.3.2.1. 確立人員權責角色

在處理個資時，需確認組織內外及相關人員之權責角色，並依照其權責給予所應具備之權限，在發生個資事故時，便可儘速釐清可能洩露之管道。

確立人員權責角色之任務，包括識別個資管理相關人員或群組角色、建立個資項目生命週期活動與個資管理角色之對應表、識別對應表內個資管理角色細部權責定義需求、完成人員權責角色定義及轉換個資管理人員權責角色定義至相關應用系統權限定義。有關每項任務內容，說明如下：

●識別個資管理相關人員或群組角色

針對各單位之工作內容與特性，應瞭解在個資處理過程中，有那些角色、人員及系統使用權限，釐清其相互關係，包括內部/外部使用者、管理者及供應商。

●建立個資項目生命週期活動與個資管理角色之對應表

依據個資檔案名稱與識別之個資管理角色，列出各管理者之個資使用情形，包括蒐集、建立、讀取、更新、列印、刪除及轉出等，並將上述資料填入個資項目與個資管理角色對應表，詳見表 12。

表12 個資項目與個資管理角色對應表

個資管理角色 / 個人資料檔案	計畫承辦窗口							單位秘書							文件管理人員							委外廠商窗口						
	蒐集	建立	讀取	更新	列印	刪除	轉出	蒐集	建立	讀取	更新	列印	刪除	轉出	蒐集	建立	讀取	更新	列印	刪除	轉出	蒐集	建立	讀取	更新	列印	刪除	轉出

資料來源：本計畫整理

●識別對應表內個資管理角色細部權責定義需求

根據已完成之個資項目與個資管理角色對應表，與各單位進行訪談，瞭解其角色與權限是否符合最小權限原則。

●完成人員權責角色定義

依照與各單位訪談結果，調整個資項目與個資管理角色對應表。

●轉換個資管理人員權責角色定義至相關應用系統權限定義

完成個資項目與個資管理角色對應表，依其權責角色修正系統或檔案使用權限。以組織現行業務，填寫個資項目與個資管理角色對應表。實務情形若有涉及代理人，則應詳列代理人之權限。

2.3.2.2. 建立個資管理程序

為因應個資法之要求，組織需訂定個資保護政策，宣告對外網站之隱私權保護政策，明確規範內部的保護機制，檢視組織內部現行管理制度是否符合個資保護要求，同時一併檢討修正現行管理制度相關之程序書與執行表單。

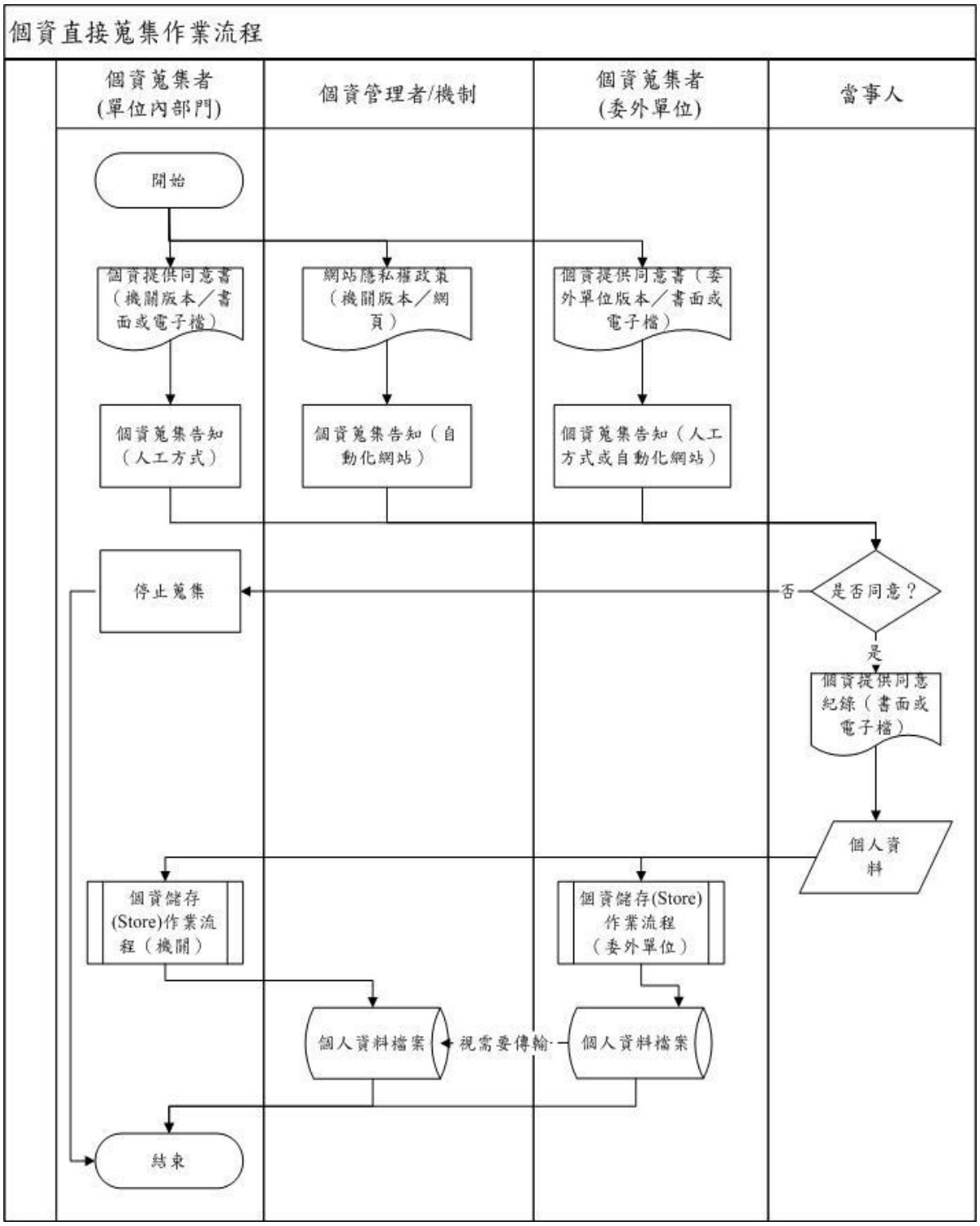
組織於業務作業需求須蒐集個資時，應訂定個資蒐集作業流程，確認個資蒐集符合特定目的，同時設計個資同意書範本，以利於蒐集個資時使用。於蒐集資料之流程中，檢視所涉及之管理作業流程與程序書，符合組織之個資保護政策，修定相關文件資料內容。本階段之管理重點為清楚定義管理權責、依據法令與流程進行個資分類，以及落實公開與告知等隱私管理原則。例如針對短期持有(如行銷或抽獎目的)的個人資料，應透過蒐集程序告知當事人後續的個資處理與利用方式；當業務終止時，該項業務所擁有的個人資料是否依刪除/銷毀/淨化程序處理；對於久未利用或是太舊的個資，

應檢討是否透過蒐集程序取得，並視檢討結果決定是否補行告知當事人，以取得個資的後續處理與利用，或依刪除/銷毀/淨化程序處理等。

建立個資管理程序之任務，包括設計個資生命週期作業流程、設計個資事故管理作業流程、設計個資管理稽核作業流程及修訂組織內部管理制度文件。有關每項任務內容，說明如下：

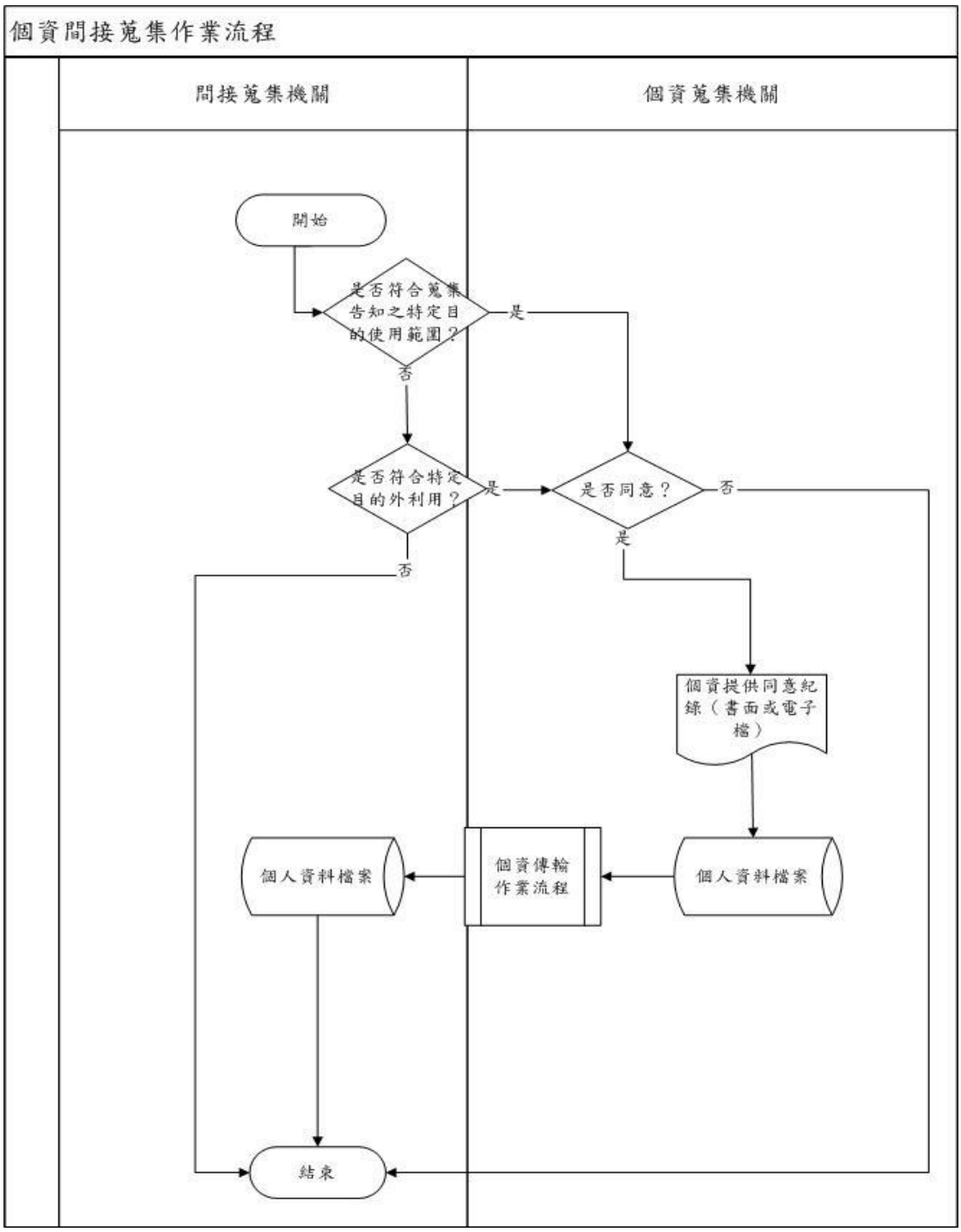
●設計個資生命週期作業流程

在施行細則草案規定之必要措施中，必須設計「個資資料蒐集、處理及利用之內部管理程序」。因此，組織應就所擁有的個資項目，設計相關作業流程，並調整相關管理作業程序書與使用人員權限，有效管制處理階段之個資安全，個資生命週期相關作業流程，詳見圖 6~圖 12。



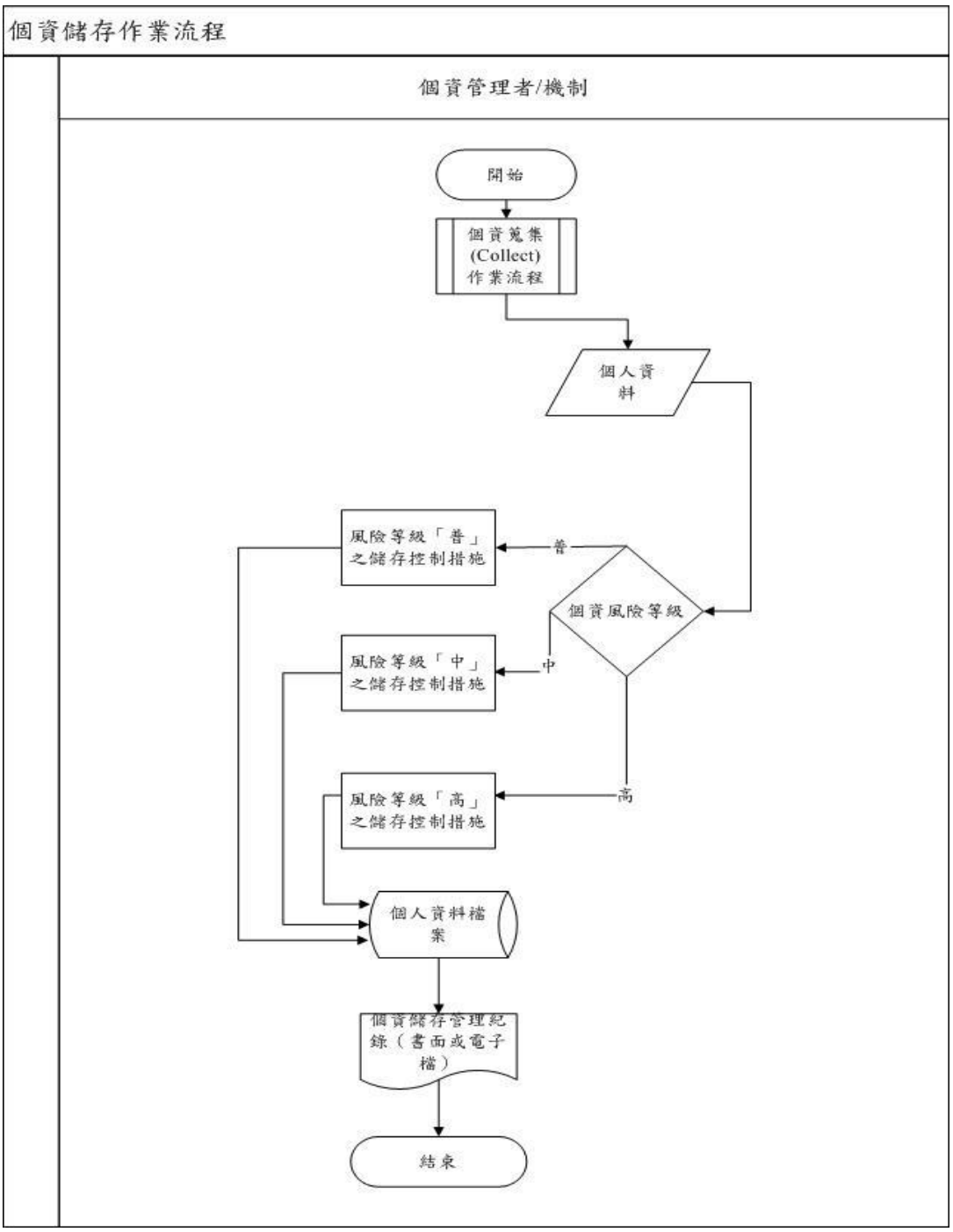
資料來源：本計畫整理

圖6　個資直接蒐集作業流程範例



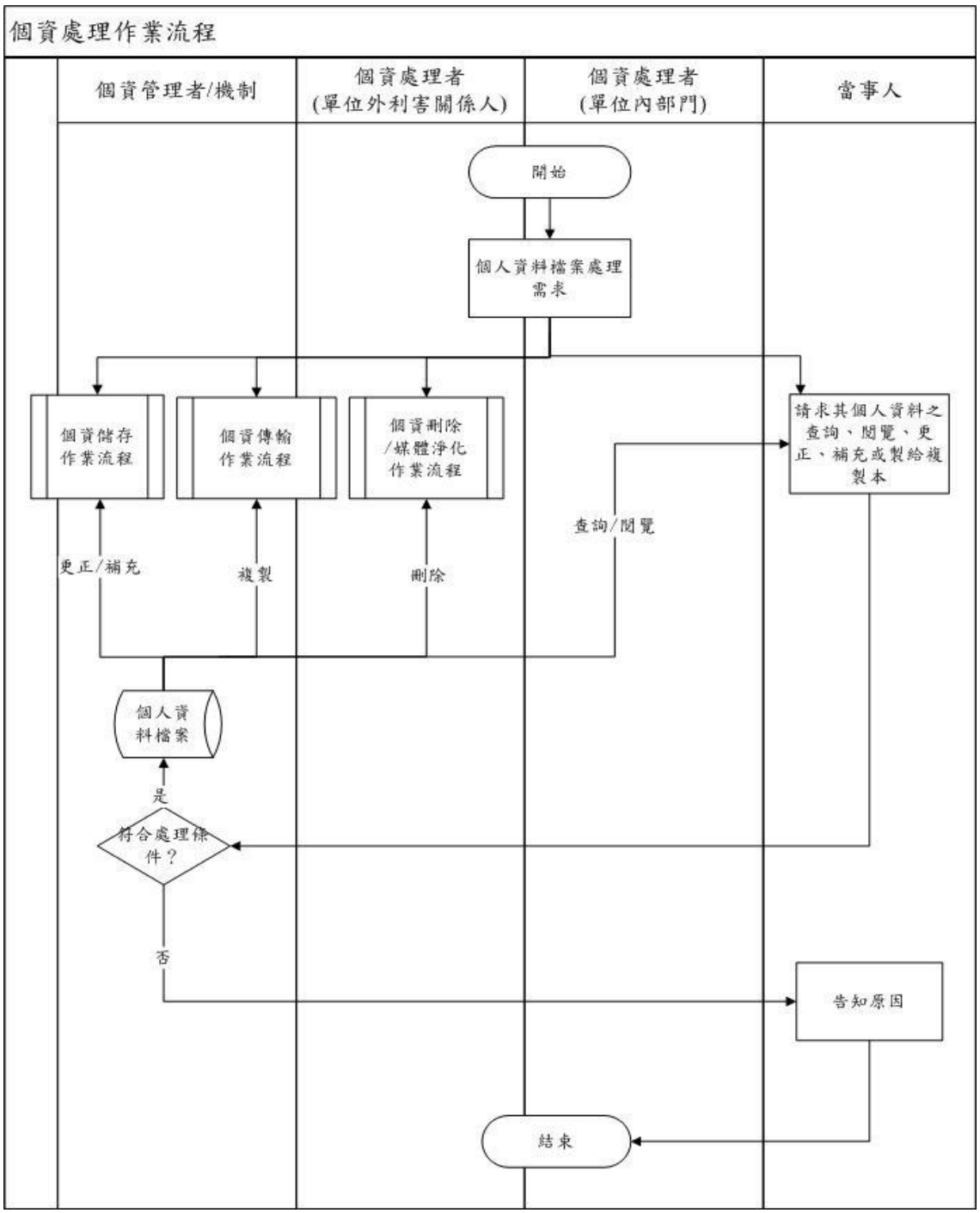
資料來源：本計畫整理

圖7　個資間接蒐集作業流程範例



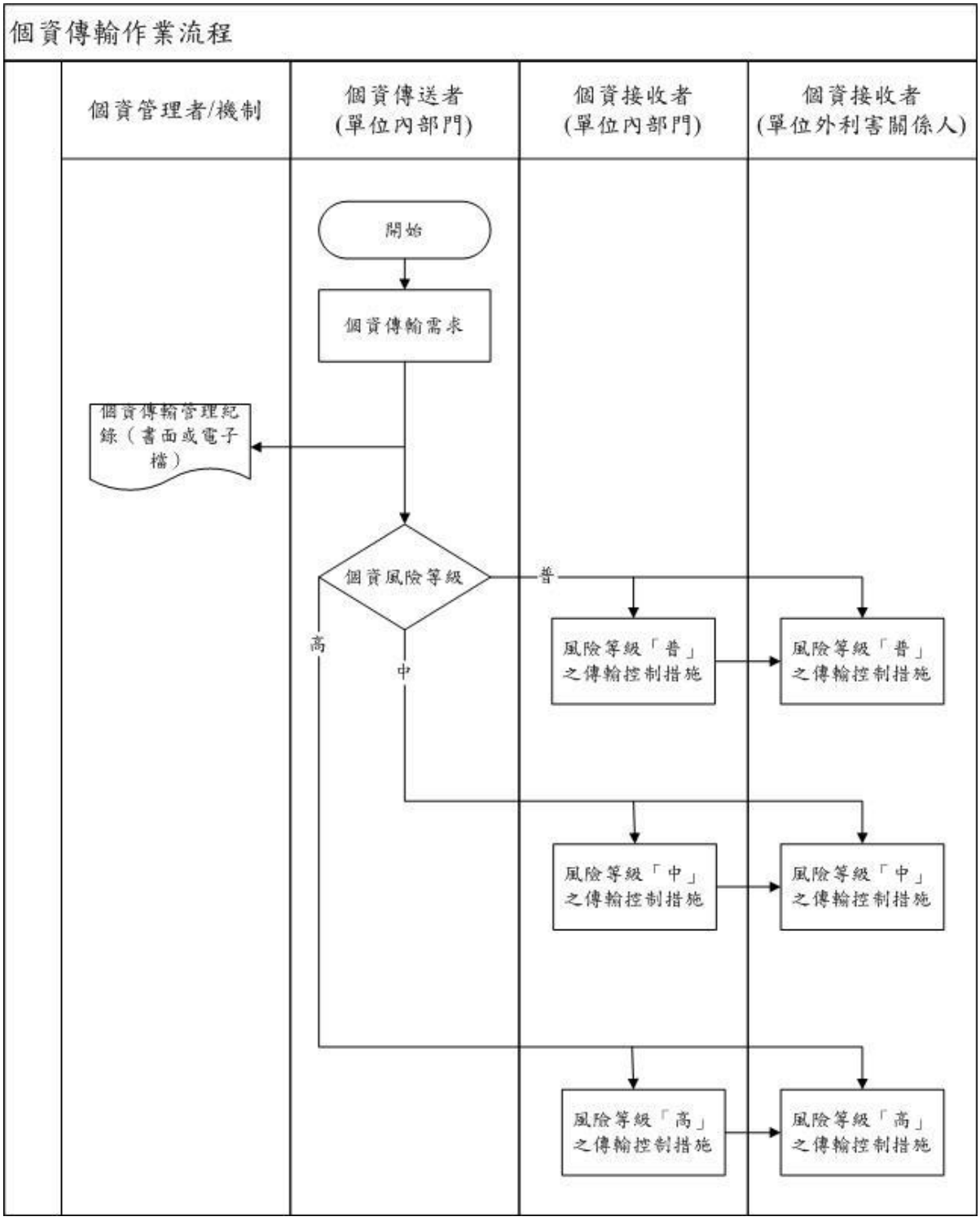
資料來源：本計畫整理

圖8　個資儲存作業流程範例



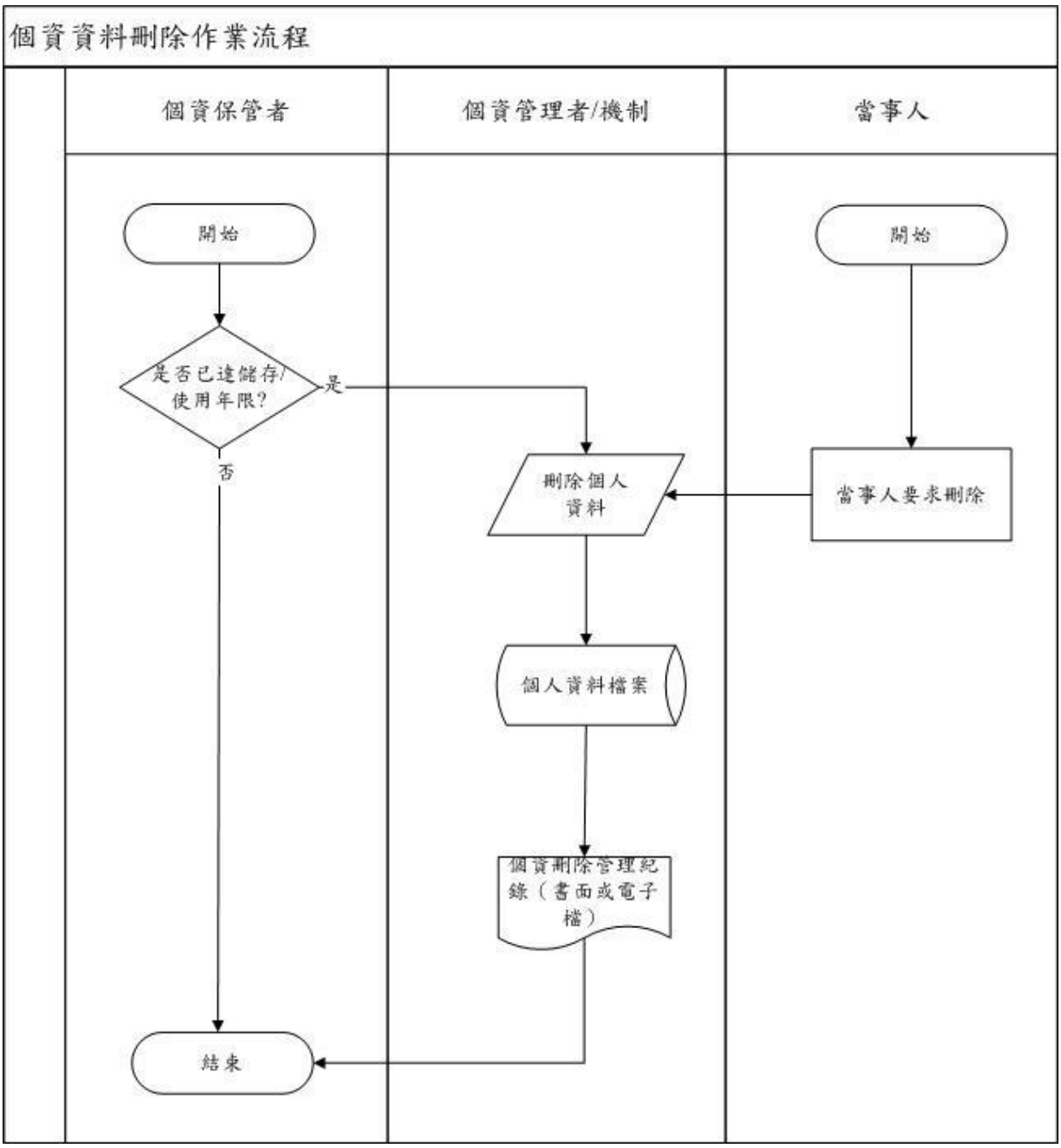
資料來源：本計畫整理

圖9　個資處理作業流程範例



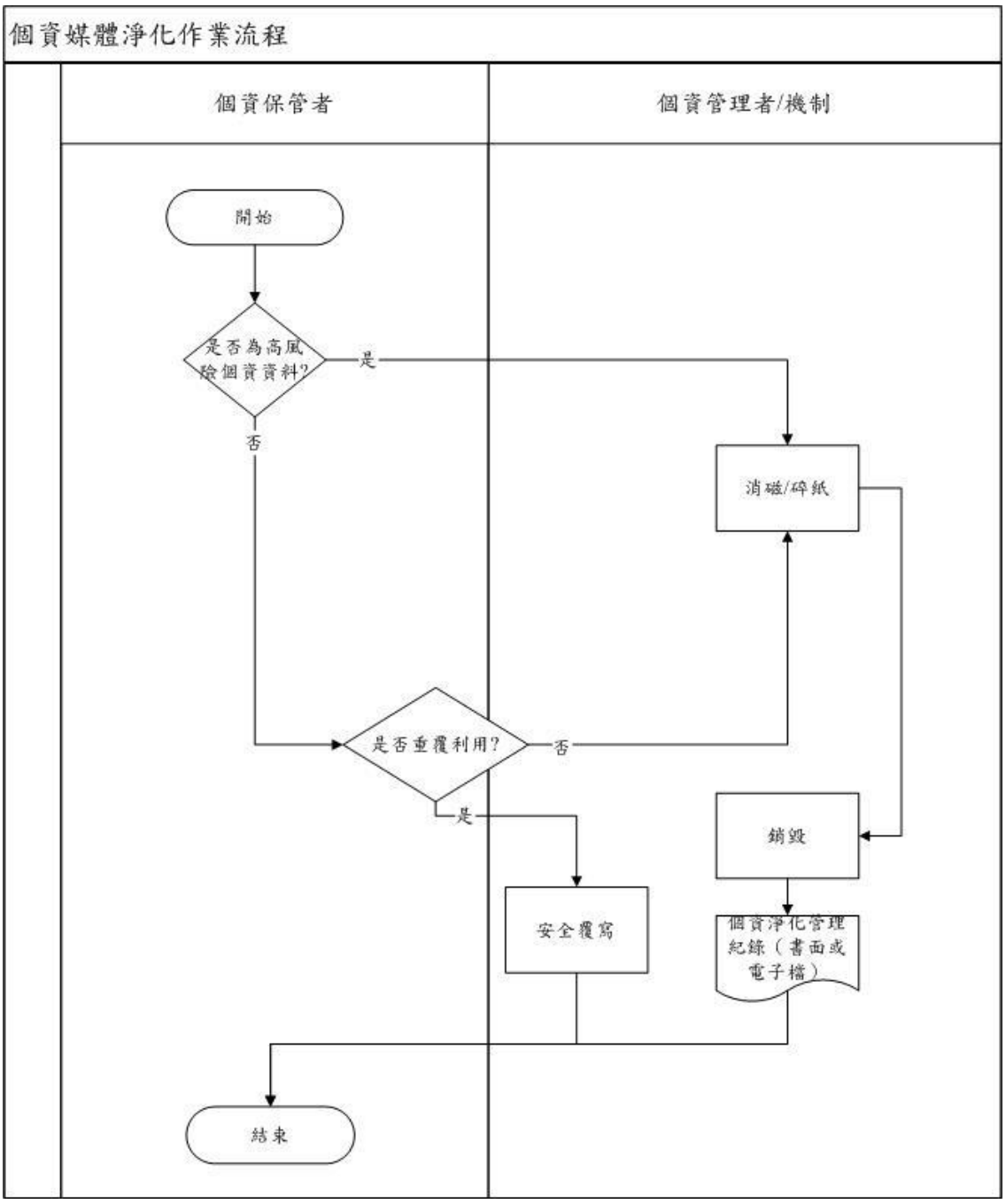
資料來源：本計畫整理

圖10 個資傳輸作業流程範例



資料來源：本計畫整理

圖11 個資刪除作業流程範例



資料來源：本計畫整理

圖12 個資淨化作業流程範例

組織若需於網站或網頁中蒐集個資，應於網站中載明隱私權政策，詳見表13；於蒐集個資時，應請個資擁有者簽署個資提供同意書，詳見表14，明確告知蒐集個資的目的與用途；同時保有個資擁有者需異動與調閱之權利，包括個資補充、資料更正、製給複製本、停止蒐集、處理或利用及資料刪除等時機之用途，詳見表15與表16。

表13 隱私權政策範例(適用於網站)

隱私權政策範例

最後更新日期：xxx 年 xx 月 xx 日

個人資料的蒐集

OO 機關(以下簡稱「本機關」)根據本網站所提供下列服務，將蒐集個人資料：

1、資安教育訓練

2、資安系列競賽

3、資安推廣活動

本機關蒐集的資料如下：

1、真實姓名、身分證字號、職稱、地址、電話、E-mail 電子郵件。

2、我們也蒐集一些不代表您個人，但與您個人相關之訊息，例如您一次瀏覽本網站的頁數，以及伺服器自行產生的相關紀錄，如您使用連線設備的 IP 位置、使用時間、使用的瀏覽器、瀏覽與點選資料紀錄等。本網站會對於個別連線者的瀏覽器予以標示，除非您願意告知您的個人資料，否則在此情況下本網站不會將此項紀錄和您對應。

個人資料的選擇

當您申請需要註冊的特定服務時，我們會要求您提供個人資料。如果此資訊的使用方式與當初蒐集的目的不同，我們會在使用前先徵求您的同意。

如果個人資料的使用用途與本【隱私權政策】或特定服務的隱私權通知所述不同，我們將提供有效的方法，讓您選擇不將個人資料用於這些用途。除非已事先徵得您的同意，否則我們不會蒐集敏感資訊或將之用於與本【隱私權政策】和/或增補服務隱私權通知未涉及之目的。

您可以拒絕向本機關提供個人資料，不過我們可能因此無法為您提供這些服務。

資訊的使用

本網站只有在下列情形下，會向其他機關或個人分享個人資料：

1、已事先徵得您的同意，分享任何機密的個人資料前，我們都會先徵求您的同意。

2、內部分析與研究用途：我們會使用您的資料做為內部統計分析與研究報告用途。

3、委外業務：我們將您的資料提供予負責執行[資安教育訓練]業務且與本機關簽訂委外合約之委外廠商，本機關在合約中要求委外廠商僅可在為本機關執行服務、且無關自身利益的情形下使用您的資料，並遵守本【隱私權政策】和其他適用的任何保密和安全措施。

4、法律要求：本機關於必要時將遵循中華民國法律、命令、傳票、裁判、判斷及處分要求的內容，提供適當的資訊予法定機構，這有可能包括您的個人資料。

5、組織調整：如果本機關因應組織改造所進行之組織調整，我們將確保對涉及這些調整的所有個人資料保密，並在個人資料移轉且被另一隱私權政策約束之前通知您。

Cookies

Cookies 是伺服端為了區別使用者的不同喜好，由瀏覽器寫入使用者硬碟的一些簡短資訊，雖然 Cookies 會識別使用者的電腦，但是無法識別使用者的身分。您也可以透過在您的瀏覽器中選擇修改您對於 Cookies 的接受程度，如果您選擇拒絕所有的 Cookies，您可能無法正常使用部分個人化服務，或是完成[活動或訓練報名業務]。

為了提供更好、更個人化的服務以及方便您參與個人化的互動活動，Cookies 會在您註冊或登入時建立，並在您登出時修改其狀態。

共用資料政策

除本政策的規定外，本網站不會任意出售、交換或出租任何您的個人資料予其他團體或個人。

但是本網站可能為了提供您其他服務或優惠權益(例如[資安推廣之抽獎活動])需要與提供該服務或優惠之第三者共用您的資料，本機關與第三者共用您的個人資料時，本網站將於活動網頁加註資料共用對象說明。

傳送商業或電子郵件之政策

本網站將在事前或註冊登錄取得您的同意後，傳送商業性或電子郵件給您。本網站除了在該資料或電子郵件上註明是由本網站發送，也會在該資料或電子郵件上提供您能隨時停止接收這項服務。或提供您其他服務或優惠權，需要與提供該服務或優惠的第三者傳送商業性資料或電子郵件時，我們將會在活動時提供充分的說明，並且在第三者傳輸之前通知您，您可

以自由選擇是否接受這項特定服務或活動。

資訊安全

我們會採取適當的安全措施，來防止未經授權的資料存取、竄改、披露或損毀，其中包括就資料的蒐集、儲存、處理慣例及安全措施進行內部審查，並以實體的安全措施，防止我們儲存個人資料的系統遭到未經授權的存取。

我們只允許本機關的員工和提供特定服務之委外廠商存取個人資料，因為他們需要這些資訊來提供、開發或改善我們的服務。上述人員都必須遵守保密義務，否則可能會遭到懲戒，包括解僱和刑事起訴等。

資料正確性

本機關處理您的個人資料時，會嚴格遵守當初蒐集資訊的目的以及本【隱私權政策】或任何適用的特定服務隱私權通知。我們會審查我們的資料蒐集、儲存及處理慣例，以確保僅蒐集、儲存及處理提供或改善我們的服務所需的個人資料。我們會採取合理的措施來確保所處理之個人資料的正確性、完整性及即時性，但我們仰賴使用者在必要時更新或修正其個人資料。

查閱和更新個人資料

當您使用本機關服務時，我們會儘量讓您有權查閱自己的個人資料，並讓您修正不正確的資訊，或依您的要求，將法律並未規定需要保留或依合法商業用途不需保留的資料刪除。處理此類要求之前，我們會要求個別使用者證明身分，並指明要查閱、修正或移除的資訊，我們可能會拒絕處理過度重複、經常性、需要過多技術支援、危害其他使用者隱私權、 非常不切實際(例如，索取儲存於備份磁帶上的資訊)或是根本不必要的查閱要求。除非需要大量的技術支援，否則我們會免費讓使用者查閱和修正自己的個人資料。我們有部分服務採用不同的程序來查閱、修正或刪除使用者個人資

料。如需這些程序的詳細資訊，請參閱此等服務的特定隱私權通知或常見問題。

自我保護措施

請妥善保管您的任何個人資料，不要將任何個人資料提供給任何人或其他機構。在您使用完本網站所提供的各項服務功能後，務必記得登出，若您是與他人共享電腦或使用公共電腦，切記要關閉瀏覽器視窗，以防止他人讀取您的個人資料或信件。

本政策之修正

由於社會環境及法令規定變遷或科技技術進步，本網站將採用最新技術與法規以盡全力保護您的網路隱私，並且定期審查本網站是否遵守本【隱私權政策】，故本網站有權不定時修訂與公布本【隱私權政策】以合時宜。

為保障您的權益，我們不會在未經您同意的情況下，削減本【隱私權政策】賦予您的權利，即使有變更，多半也只是小幅修正。無論如何，我們會將【隱私權政策】的所有變更都公布在此網頁上，如果是重大變更，我們將提供更明確的通知(某些服務甚至會以電子郵件通知【隱私權政策】的變更)。

本【隱私權政策】的每個版本都會在網頁上方標示生效日期，我們也會將本【隱私權政策】的存檔版本封存，供您檢閱。也請您隨時上網參閱本項聲明。

隱私權保護政策諮詢

如果您有任何本【隱私權政策】或其他關於隱私權管理或本機關使用個人資料的問題，請與我們聯絡，本機關個人資料保護聯絡窗口資訊如下：

個人資料保護服務專線 ： _____

傳真專線電話：_____

諮詢服務時間：_____

若上述回覆或處理方式無法滿足需求或有任何訴怨內容，請連繫本機關使用者訴怨電子信箱：_____

資料來源：本計畫整理

表14 個資提供同意書範例

個人資料提供同意書範例

為保障您的權益，請於申請接受 OO 機關（以下簡稱「本機關」）所提供之_____服務(以下簡稱「本服務」)前，詳細閱讀本同意書所有內容。

當您勾選「我同意」並簽署本同意書時，表示您已閱讀、瞭解並同意接受本同意書之所有內容及其後修改變更規定。若您未滿二十歲，應於您的法定代理人閱讀、瞭解並同意本同意書之所有內容及其後修改變更規定後，方得使用本服務，但若您已接受本服務，視為您已取得法定代理人之同意。，並遵守以下所有規範。

一、基本資料之蒐集、更新及保管

1.本機關蒐集您的個人資料在中華民國個人資料保護法與相關法令之規範下，依據本機關【隱私權政策】，蒐集、處理及利用您的個人資料。

2.請於申請時提供您本人正確、最新及完整的個人資料。

3.本機關因執行業務所需蒐集您的個人資料包括姓名、出生年月日、國民身

分證統一編號、連絡方式（包括但不限於電話號碼、E-MAIL 或居住地址）及 OOOOO。

4.若您的個人資料有任何異動，請主動向本機關申請更正，使其保持正確、最新及完整。

5.若您提供錯誤、不實、過時或不完整或具誤導性的資料，本機關保留隨時終止您接受使用_____服務資格的權利。

6.您可依中華民國個人資料保護法，就您的個人資料行使以下權利：

(1)請求查詢或閱覽

(2)製給複製本

(3)請求補充或更正

(4)請求停止蒐集、處理及利用

(5)請求刪除

但因本機關執行職務或業務所必須者，本機關得拒絕之。若您欲執行上述權利時，請參考本機關【隱私權政策】之個人資料保護聯絡窗口聯絡方式與本機關連繫。

二、蒐集個人資料之目的

1.本機關為執行以下業務需蒐集您的個人資料：

(1)資安教育訓練

(2)資安系列競賽

(3)資安推廣活動

2.當您的個人資料使用方式與當初本機關蒐集的目的不同時，我們會在使用前先徵求您的書面同意，您可以拒絕向本機關提供個人資料，不過我們可能因此無法為您提供服務。

命資料利用對象為本機關、本機關簽訂委外合約之委外廠商_____及主管機關_____，個人資料處理方式包括個人資料之蒐集、建立、傳送、轉變、儲存、封存與銷毀等資料生週期。資料使用範圍僅限中華民國境內（包括臺澎金馬地區），本機關_____利用您的個人資料期間為永久使用，委外廠商_____利用您的個人資料期間預設為 2 年，若委外廠商_____因業務需要需延長個人資料使用期間，我們將遵循前項原則，本機關會先徵求您的書面同意後始延長資料使用期限。

三、基本資料之保密

1.您的個人資料受到本機關【隱私權政策】之保護及規範。請閱讀【隱私權政策】以查閱本機關完整隱私權保護政策。

四、同意書之效力

1.當您勾選「我同意」並簽署本同意書時，即表示您已閱讀、瞭解並同意本同意書之所有內容，您如違反下列條款時，本機關得隨時終止對您提供之一切服務。

2.本機關保留隨時修改本同意書規範之權利，本機關將於修改規範時，將於本機關網頁公告修改之事實，不另作個別通知。如果您不同意修改的內容，請勿繼續接受本服務。否則將視為您已同意並接受本規範該等增訂或修改內容之拘束。

3.您在接受本機關提供的_____服務之前，應仔細閱讀本同意書條

款。如您不同意本同意書條款或其更新之內容，您可以放棄接受本機關提供的服務；您一旦接受本同意書，即視為您已瞭解並完全同意本同意書各項條款內容。

4.您自本同意書取得的任何建議或資訊，無論是書面或口頭形式，除非本同意書條款有明確規定，均不構成本同意書條款以外之任何保證。

九、準據法與管轄法院

1.本同意書之解釋與適用，以及與本同意書有關的爭議，均應依照中華民國法律予以處理，並以臺灣臺北地方法院為第一審管轄法院。

□ 我已閱讀並且接受上述同意書內容

當事人簽名_____(請親簽)

年　　月　　日

資料來源：本計畫整理

表15 個人資料異動申請書範例

<table>
<tr><td rowspan="2">申請人姓名
(請檢附證件)</td><td></td><td>申請人簽名</td><td>(請親簽)</td></tr>
<tr><td>☐當事人 ☐代理人(與當事人關係_____)</td><td>承辦人</td><td>承辦人姓名
_____
核對身分確認，☐本人 ☐非本人</td></tr>
<tr><td>申請目的
(請勾選一項)</td><td colspan="3">☐資料補充 ☐資料更正 ☐製給複製本 ☐停止蒐集、處理或利用
☐資料刪除
原因(請詳述)：
_____
_____</td></tr>
<tr><td>檔案名稱</td><td colspan="3"></td></tr>
<tr><td>資料項目
(請勾選)</td><td>☐當事人所有個資
☐姓名
☐身分證字號</td><td>☐出生年月日
☐戶籍地址
☐通訊方式</td><td>☐_____
☐_____
☐_____</td></tr>
<tr><td>資料說明</td><td colspan="3"></td></tr>
<tr><td colspan="4">以下由 OO 機關人員填寫</td></tr>
</table>

資訊型態	☐紙本，名稱_____ ☐電子檔，檔名_____ ☐資料庫，名稱_____ ☐其他： _____	
處理方式		
保管人	科長	主管

資料來源：本計畫整理

表16 個資調閱申請書範例

<table>
<tr><td rowspan="2">申請人姓名
(請檢附證件)</td><td colspan="4"></td></tr>
<tr><td colspan="2">□當事人 □代理人(與當事人關係_____)</td><td>連絡電話</td><td></td></tr>
<tr><td>調閱目的
(請詳述)</td><td colspan="4"></td></tr>
<tr><td>資訊型態</td><td colspan="4">□紙本 □電子檔(PDF) □電子檔(DOC) □電子檔(PPT)
□電子檔(XLS) □電子檔(其他：) □其他：</td></tr>
<tr><td>調閱對象</td><td colspan="4">姓名(個人)：_____；範圍(非特定對象)：_____</td></tr>
<tr><td>調閱項目
(請勾選)</td><td>□身分證字號
□姓名
□出生年月日</td><td>□通訊電話
□通訊住址
□戶籍地址</td><td colspan="2">□_____
□_____
□_____</td></tr>
<tr><td colspan="2">保管人</td><td>科長</td><td colspan="2">主管</td></tr>
<tr><td colspan="2"></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="5">說明：
1.資料申請者為組織單位時，不得做為個人使用。
2、資料申請者同意對於個資的運用與保密，如有違反「中華民國個人資料保護法」之相關規定者，悉依該法第五章之相關罰則辦理。</td></tr>
</table>

資料來源：本計畫整理

●設計個資事故管理作業流程

於現行資安事故通報應變程序與流程中，檢視並調整作業程序，以符合個資法規與政策要求。

組織若尚未訂定事故管理程序，可參考國家資通安全通報應變網站之「資安事件通報應變機制說明」，訂定個資事故通報應變處理程序。

●設計個資管理稽核作業流程

依照個資作業流程、作業程序書(蒐集、處理及傳輸)及事故通報與作業程序文件，訂定個資內部稽核作業程序，或於現行稽核作業程序中，檢討調整個資檢核項目，至少一年需執行一次稽核作業。

●修訂組織內部管理制度文件

依據個資作業流程，檢視並綜整組織內部管理制度文件，同時重新發布更新版之管理制度文件。

2.4.「結案」

藉由參考指引導入過程，將導入機關與導入顧問所發現指引描述語意不清或未交代事項，致使過程中無法順利執行的意見，彙整於結案會議中說明，並據以修正「個人資料保護參考指引」。

3. 個案 A 導入執行情形

3.1.「開始」

3.1.1. 決定系統範圍與前置作業

3.1.1.1. 機關背景介紹

個案 A 於 81 年 2 月成立資訊單位，負責行政業務電腦化相關推動事宜，業務職掌如下：

- 關於本府資訊應用系統之規劃分析及辦理事項。
- 關於資訊作業委外服務案件之規劃及簽辦事項。
- 關於資訊軟硬體及網路之管理維護及應用事項。
- 關於資訊業務之推廣及教育事項。

其工作項目包括：

- 全球資訊網管理維護。
- 辦理本府地理資訊系統建置。
- 公文系統管理維護。
- 員工資訊網管理維護。
- 資通訊安全管理。
- 目錄服務系統(DS)管理維護。
- 資料備份及回復系統管理維護。
- 本府區域網路及行政骨幹網路管理維護。

●府內個人電腦及周邊設備管理維護。

●電子郵件系統管理維護。

●市府電腦機房管理維護。

●提供本府及所屬機關業務電腦化諮詢及協助，以推動單位業務電腦化。

●辦理本府及所屬機關員工電腦基礎教育訓練，提高員工資訊素養，善用資訊工具，以利推動電子化政府服務。

3.1.1.2. 前置作業

為利於導入專案順利進行，個案 A 與導入顧問先期協商導入作業執行細節後，該府先行檢討全府各局處業務具個資項目計 13 個單位 20 項業務，列為導入候選對象，並召開「導入啟動會議」，由導入顧問說明與討論相關前置作業內容，並由導入計畫團隊簽具保密切結，詳見附件 4_個案 A 保密切結書，會議相關事項說明於后：

●參與單位：

個案 A、行政院研究發展考核委員會(以下簡稱行政院研考會)及技服中心。

●內容：

說明導入工作計畫書，包括導入計畫目的與範圍、導入指引的執行方式、導入活動人員、導入計畫團隊、導入計畫時程及雙方配合事項。啟動會議簡報與導入工作計畫書詳見附件 5_個案 A 導入啟動會議簡報與附件 6_個案 A 導入工作計畫書。

●結論：

本專案計劃訂於 101 年 10 月 12 日起每周四下午，執行「個人資料保護參考指引」實務導入作業，總共導入期程約為十三週。本案擬選定一項個資業務，進行導入試行，但專案會議期間個案 A 先行檢討之 23 項個資業務相關系統負責人將全程參與。

3.1.1.3. 訂定個資風險等級

3.1.1.3.1. 個資風險等級基準值

本次導入個資風險等級以含有個資類別、NIST SP800-122 之衝擊等級及「資訊系統分類分級與鑑別機制」影響構面等 3 個面向，分別檢討其風險等級，再採最高原則評定為該個資之風險等級，其中「資訊系統分類分級與鑑別機制」影響構面，則依鑑別機制之 6 大構面中，「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信譽」3 者作綜合考量。經與導入機關討論，本專案個資風險等級基準值評定方式，以參考指引之個資風險等級基準值建議表為基準，做部分修正，詳見表 17。

表17 個資風險等級基準值

參考項目	個資風險等級		
	普	中	高
含有個資類別	未具有任何個資，或僅含有姓名、公務電話、公務傳真、公務E-mail等公務個資，且公務個資筆數不超過5,000筆	含有一般個資，如姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業等「個人資料保護法」定義之個人資料數量在5,000筆以下，或公務個資數量超過5,000筆(含)以上	含有特種個資，如有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個資，或含有一般個資之資料筆數超過5,000筆(含)以上
NIST SP800-122「個人可識別資訊機密性保護指引」之衝擊等級	若個資之機密性、完整性及可用性被破壞時會對本機關組織、資產或人員造成有限的傷害(可能輕微影響本機關聲譽、但不會造	若個資之機密性、完整性及可用性被破壞時會對本機關組織、資產或人員造成傷害(可能會影響本機關聲譽、財務損失	若個資之機密性、完整性及可用性被破壞時會對本機關組織、資產或人員造成重大傷害(非常可能嚴重影響本機關聲譽、重大財

參考項目	個資風險等級		
	普	中	高
判定方式	成任何財務損失或遭受訴訟之情事)	或遭受訴訟，但不至於對本機關業務之持續運作造成重大影響)	務損失或重大訴訟，且可能造成本機關主要業務中止)
「資訊系統分類分級與鑑別機制」影響構面與個資項目價值對應	「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信譽」三者影響構面之安全等級皆為普或安全等級為中者不超過一項	「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信譽」三者影響構面的安全等級皆無高，且其中二項安全等級為中	「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信譽」三者影響構面之安全等級皆為中，或「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信譽」三者影響構面之其中一項安全等級為高者

資料來源：本計畫整理

其中「資料保護受到損害」、「影響法律規章遵循」及「損害本機關信譽」三者影響構面之安全等級設定原則，如下：

資料保護受到損害：以資料機密性與完整行受導損害之影響考量，詳見表18。

表18 資料保護受到損害安全等級設定原則

安全等級	設定原則
普 (等級 1)	▪(資料機密性)一般性資料；資料外洩不致影響個人權益或僅導致個人權益輕微受損 ▪(資料完整性)資料遭竄改不致影響個人權益或僅導致個人權益輕微受損
中 (等級 2)	▪(資料機密性)敏感性資料；資料外洩將導致個人權益嚴重受損，如： ▪涉及個人出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、聯絡方式、財務情形、社會活動及其他得以直接或間接識別個人之資料。 ▪具有敏感屬性之個人資料，如：中途輟學學生、收養兒童等資料，資料外洩可能導致個人隱私遭冒犯。 ▪(資料完整性)資料遭竄改將導致個人權益嚴重受損。
高 (等級 3)	▪(資料機密性)機密性資料；資料外洩將危及國家安全、導致個人權益非常嚴重受損、或造成極大規模之個人權益嚴重受損，如： ➢ 凡涉及國家安全之外交、情報、國境安全、財稅、經濟、金融、醫療等重要機敏系統。 ➢ 特殊屬性之個人資料(如：臥底警員、受保護證人、被害人等資料)，資料外洩可能會使相關個人身心受到危害、

安全等級	設定原則
	社會地位受到損害、或衍生財物損失等情形。 ➢ 涉及個人之醫療、基因、性生活、健康檢查、犯罪前科等資料，資料外洩將使個人權益非常嚴重受損。例如：醫療資訊系統、刑案資訊整合系統等。 ▪極大規模(如：全國性)之涉及個人出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、聯絡方式、財務情形、社會活動及其他得以直接或間接識別個人之資料。例如：戶役政資訊系統、護照管理系統等。 ▪(資料完整性)資料遭竄改將危及國家安全、導致個人權益非常嚴重受損、或造成極大規模之個人權益嚴重受損。

資料來源：本計畫整理

影響法律規章遵循：以系統運作、資料保護及資訊資產使用等，違反法律規章所可能影響之後果為考量，詳見表 19。

表19 影響法律規章遵循安全等級設定原則

安全等級	設定原則
普 (等級 1)	▪系統運作、資料保護、資訊資產使用等須依循相關規範辦理，否則將導致機關違反法律規章並伴隨輕微不良後果，如： ➢ 依使用授權年限購買之資訊系統或軟體：授權年限到期，必須停止使用，否則將涉及違反契約及智慧財產權相關法令之遵循性。 ▪全球資訊網：必須符合智慧財產權相關法令尊重他人智慧結晶，並遵守兒童及少年福利法、電腦網路內容分級處理辦法進行資訊內容管理，否則將涉及違反法律之遵循性。

安全等級	設定原則
中 (等級 2)	▪系統運作、資料保護、資訊資產使用等須依循相關規範辦理，否則將導致機關違反法律規章並伴隨嚴重不良後果，如： ➢ 政府電子採購網：依「政府採購法」第 27 條規定，機關辦理公開招標或選擇性招標，應將招標公告或辦理資格審查之公告刊登於政府採購公報或公開於資訊網路。因此，若系統資料遭竄改導致公告資料錯誤，將影響採購作業透明化。
高 (等級 3)	▪系統運作、資料保護、資訊資產使用等須依循相關規範辦理，否則將導致機關從根本上違反法律規章，如： ➢ 機密性資料：依「國家機密保護法施行細則」第 28 條第 4 款規定，國家機密之保管方式直接儲存於資訊系統者，須將資料以政府權責主管機關認可之加密技術處理，該資訊系統並不得與外界連線。因此，機關若未依循規定儲存資料，將涉及從根本上違反法律之遵循性。 ▪醫療機構醫囑暨電子病歷系統：依「醫療機構電子病歷製作及管理辦法」第 3、4 條規定，電子病歷資訊系統之建置、電子病歷之製作及貯存應符合相關規定。因此，機關若未依循相關規定進行系統建置維運及資料儲存，將涉及從根本上違反法律之遵循性。

資料來源：本計畫整理

損害組織信譽：以系統發生資訊安全事故，導致機關形象、信譽受到損害情形為考量，詳見表 20。

表20 損害組織信譽安全等級設定原則

安全等級	設定原則
普 (等級 1)	若系統發生資訊安全事故，將導致機關形象、信譽受到輕微損害，如：導致區域性媒體報導負面新聞、造成多位民眾電話抱怨等情形。
中 (等級 2)	若系統發生資訊安全事故，將導致機關形象、信譽受到嚴重損害，如：導致全國性媒體報導負面新聞、造成民眾至機關抗議或陳情等情形。
高 (等級 3)	若系統發生資訊安全事故，將導致機關形象、信譽受到非常嚴重損害，如：導致國際性媒體報導負面新聞、造成民眾大規模遊行抗爭等情形。

資料來源：本計畫整理

3.1.1.3.2. 衝擊分析

本專案導入目標所採用之個資項目衝擊分析方法，經討論沿用「個人資料保護參考指引」之衝擊分析檢核表(詳見附件 1_個資項目個資衝擊分析檢核表)，做為檢視該個資項目之可能衝擊。

3.1.1.3.3. 風險評估

本專案個資風險等級評估，係依據 PIA/RA 安全控制項目基準值之組織含有個資類別、NIST SP800-122「個人可識別資訊機密性保護指引」之衝擊等級判定方式及「資訊系統分類分級與識別機制」影響構面與個資項目價值進行對應，採最高原則方式判別，並彙整相關個資衝擊分析結果，做為後續擬訂安全控制措施之依據。

3.1.1.4. 決定資訊系統範疇與邊界

導入機關為展現對導入計畫之支持與承諾，依啟動會議決議由個案 A 內部先行檢討具個資業務/系統計 20 個，以各局處推選 1 個業務/系統，做為導入專案的初選系統，計有「A1 系統」、「A2 系統」、「A3 系統」、「A4 系統」及「A5 系統」等 5 個資訊系統。

經導入顧問與導入機關之系統負責人，依據個資風險等級基準值與衝擊分析檢核表部分欄位，進行風險等級分析，以風險等級最高者做為導入目標，詳見表 21，討論期間 A1 系統負責人提議以該系統為導入目標，故決議以 A1 系統做為本專案導入目標，未來該機關其他系統亦可依本次導入相關程序與方法實作。

表21 導入系統遴選表

業務/資訊系統名稱	業務屬性	具特種個資	保有量	處理量/年	個人資料欄位	資料保護受到損害
A1 系統	支援性業務	No	1,560,000	312,000	3	中
A2 系統	支援性業務	No	180,000		5	中
A3 系統	支援性業務	No			2	中
A4 系統	支援性業務	No	25,000	不多	2	中

業務/資訊系統名稱	業務屬性	具特種個資	保有量	處理量/年	個人資料欄位	資料保護受到損害
A5 系統	支援性業務	No		6,000	3	中

資料來源：本計畫整理

3.1.1.5. 決定導入專案成員

導入機關為展現對導入計畫之支持與承諾，依啟動會議決議，除導入目標之系統負責人外，個案 A 內部先行檢討具個資業務/系統之 20 個系統負責人，皆應全程參與本專案，惟討論時以所選取之導入目標為重點。

3.2.「**文件導讀**」

3.2.1.「個人資料保護參考指引」導讀

於 101 年 10 月 12 日與 28 日導讀「個人資料保護參考指引」，由導入顧問透過簡報說明個資國際發展趨勢、我國個資相關規範、個人資料保護參考指引簡介及資訊安全管理制度(ISMS)與個資保護整合建議。主要內容同 2.2。

3.3.「**參考指引導入**」

由導入顧問與個案 A 遴選結果之 A1 系統負責人，依據 3.1「開始」階段所訂定之個資風險等級基準值評估、個資衝擊分析及個資風險評估原則，針對所遴選之 A1 系統依參考指引規畫階段與執行階段執行導入。

3.3.1. 作業流程分析

由於從業務作業流程面著手分析，較能夠找出與該業務相關之個資項目，並針對該項目進行適當保護，針對所挑選之「A1 系統」，於 101 年 10 月 18 日請系統負責人從與該業務作業管理相關之文件程序與規範著手，清查該系統所含個資項目。

3.3.2. 個資項目盤點

個資項目盤點主要目的在盤點組織所擁有之個資項目內容，包括個資項目的類別、目的、來源、欄位、數量、型態、相關生命週期活動、相關利害關係人等，以利後續進行個資之個資衝擊分析、個資風險評估、保護及管理等活動。

本專案個資項目盤點之任務，包括識別不同作業流程之個資項目、識別個資項目之類別、依據及目的、識別個資項目相關生命週期活動、識別個資項目與外部利害關係人之關聯及完成個資項目盤點。有關每項任務導入情形，說明如下：

●識別不同作業流程之個資項目

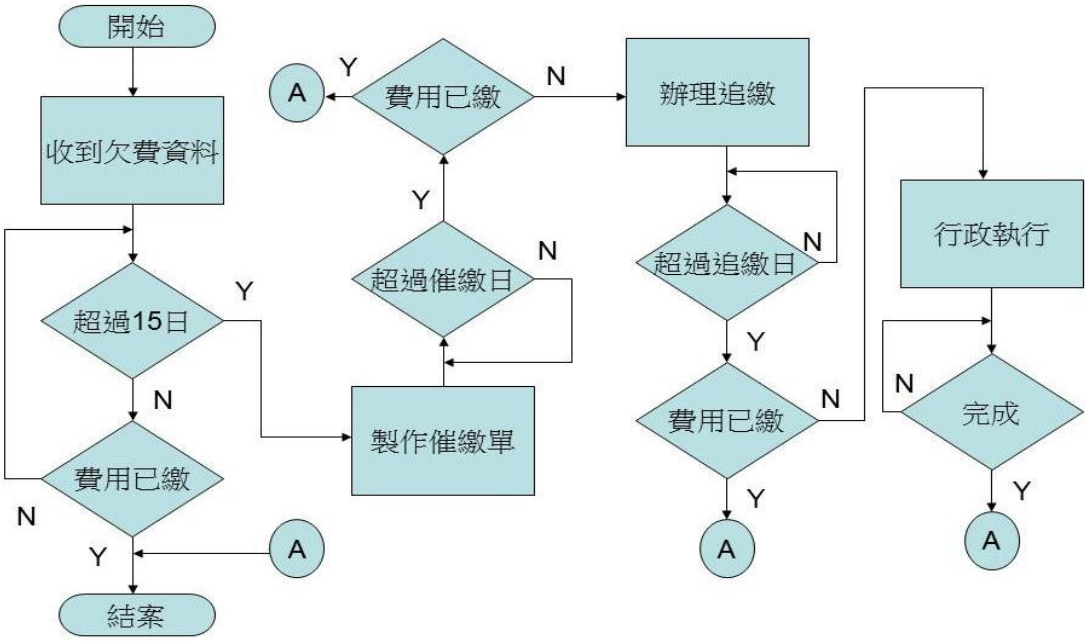
「A1 系統」負責人依作業流程分析，進行個資盤點結果詳見表 22。

表22 A1 系統個資流程分析表

業務或服務作業流程		個人資料檔案名稱	是否為個資流程
服務目錄或流程名稱	子流程名稱		
A1 系統	車主車戶籍資料查詢	E110110220.A.V.big	是
A1 系統	催繳單列印	實體紙本	是

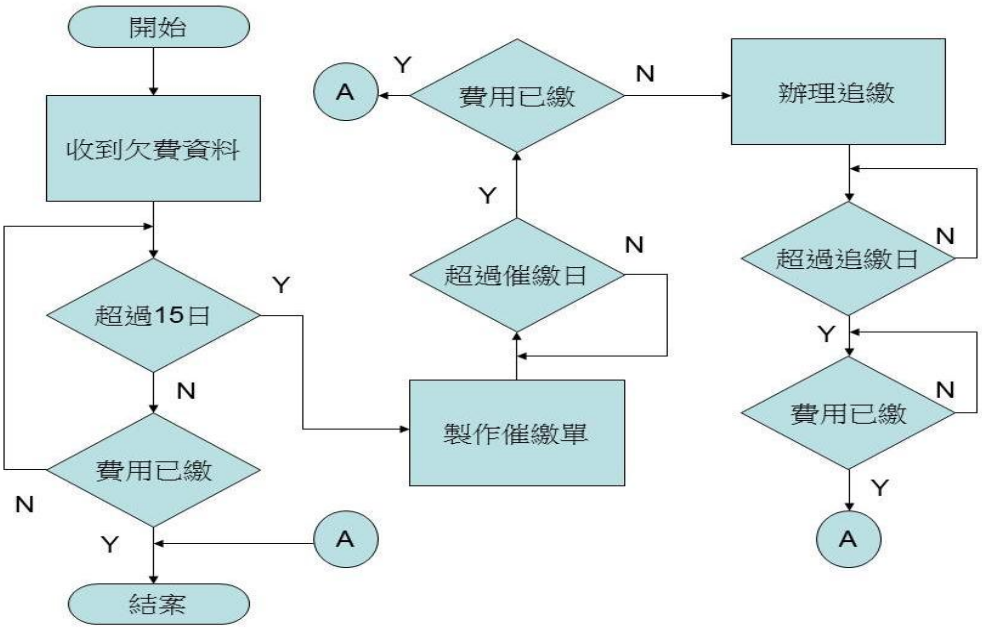
資料來源：本計畫整理

經由導入顧問以訪談方式了解該系統作業流程，由導入顧問繪製該系統作業流程圖，再與系統負責人確認，詳見圖 13、圖 14。



資料來源：本計畫整理

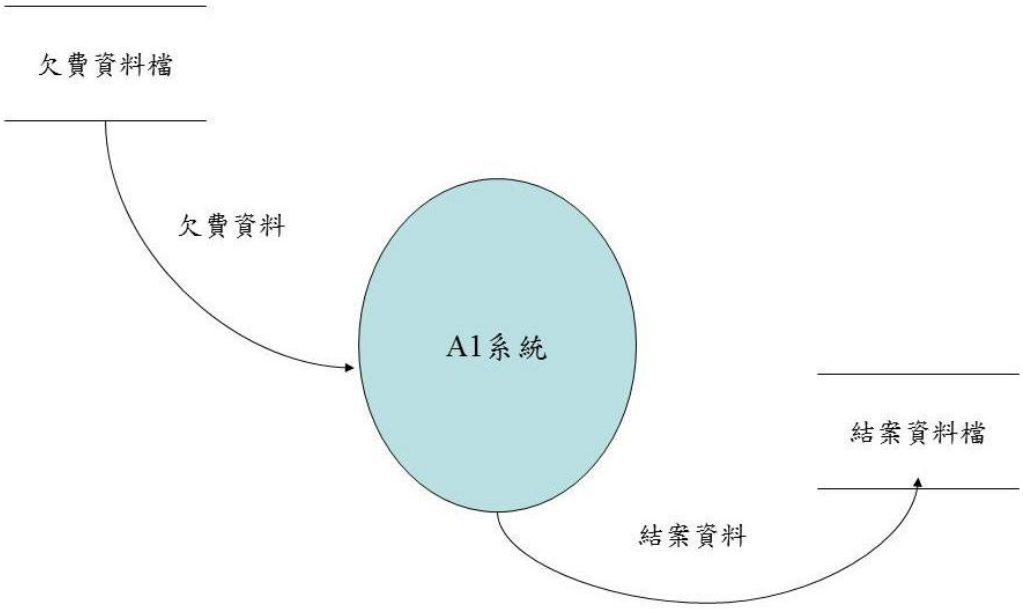
圖13 A1 系統作業流程圖 1



資料來源：本計畫整理

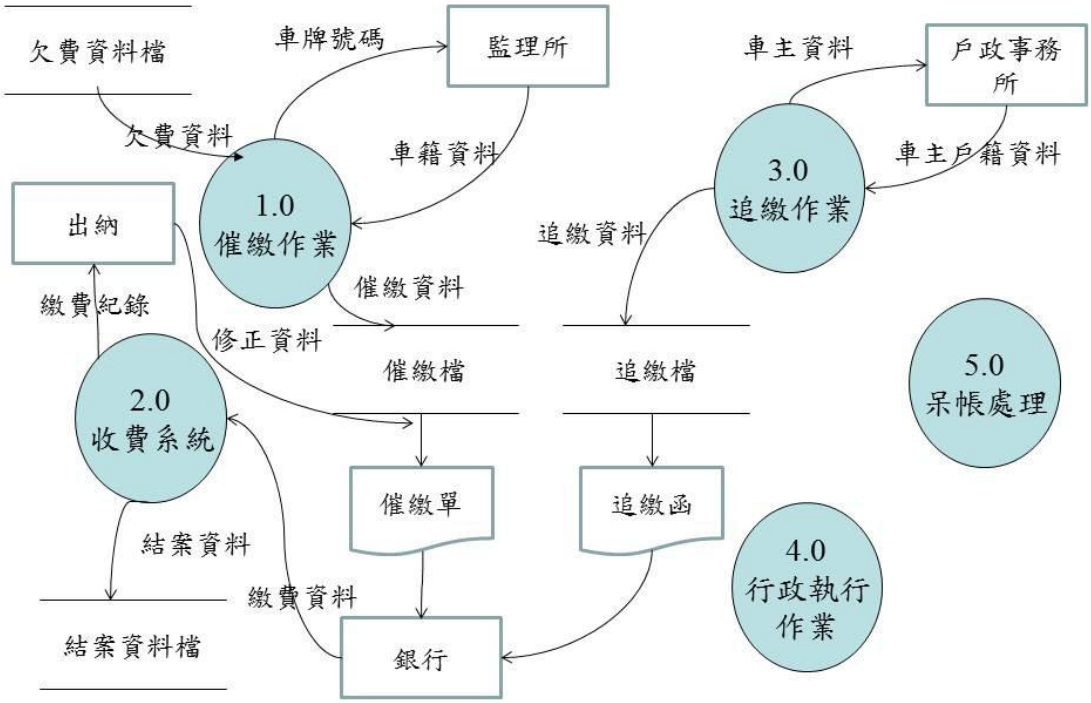
圖14 A1 系統作業流程圖 2

續由導入顧問依該系統作業流程圖繪製資料流程圖,再與系統負責人確認，詳見圖 15~圖 18。



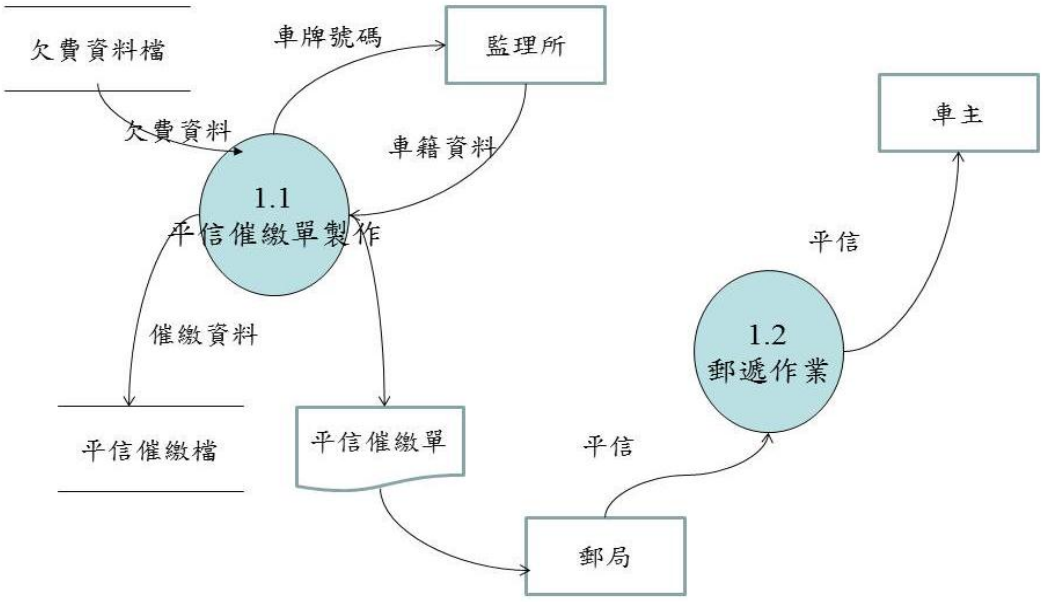
資料來源：本計畫整理

圖15 A1 系統資料流程圖(0 層)



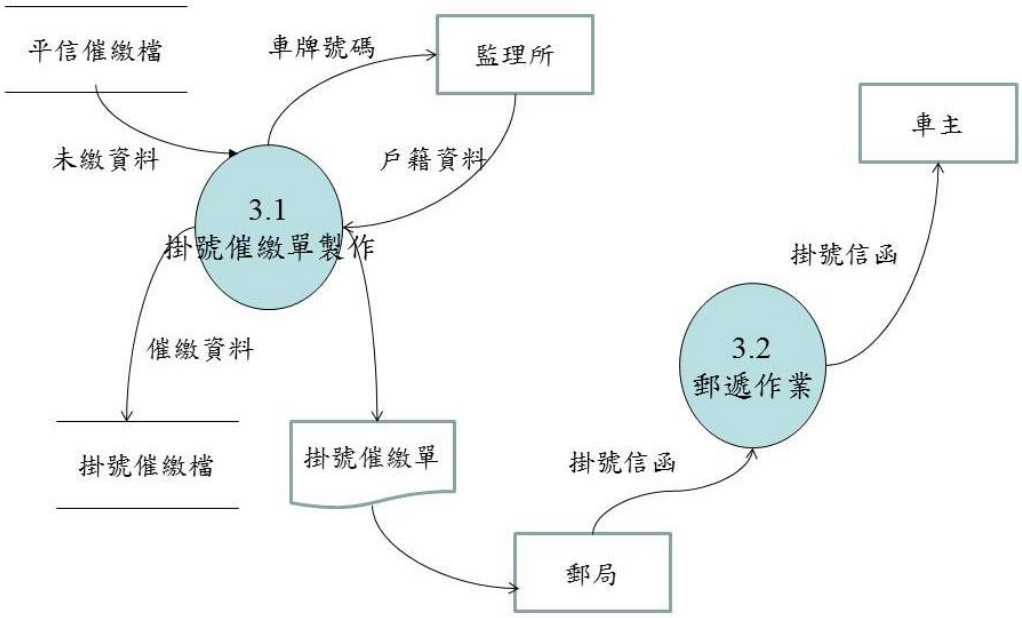
資料來源：本計畫整理

圖16 A1 系統資料流程圖(1 層)



資料來源：本計畫整理

圖17 A1 系統資料流程圖(2 層)-1



資料來源：本計畫整理

圖18 A1 系統資料流程圖(2 層)-2

依所繪製資料流程圖，進行個資盤點修正結果詳見表 23。

表23 A1 系統個資流程分析修正表

業務或服務作業流程		個人資料檔案名稱	是否為個資流程
服務目錄或流程名稱	子流程名稱		
A1 系統	平信催繳作業	欠費資料檔	否
A1 系統	平信催繳作業	平信催繳 (E110110220.A.V.big)	是
A1 系統	平信催繳作業	平信催繳單	是
A1 系統	收費系統	結案資料檔	是
A1 系統	掛號催繳作業	未繳資料檔	否
A1 系統	掛號催繳作業	掛號催繳檔 (E110110220.A.B.big)	是
A1 系統	掛號催繳作業	掛號催繳單	是

資料來源：本計畫整理

3.3.2.1. 識別個資項目之類別、依據及目的

A1 系統系統負責人將識別出之個資項目，依個資法與其施行細則所規定之個資管理應完成事項清單、行政命令、準則，識別個資項目之蒐集範圍、類別、蒐集依據及蒐集目的，經導入顧問協助完成個資項目蒐集範圍與個資項目基本資料表，做為未來通知利害相關人之依據，詳見表 24 與表 25。

表24 A1 系統個資項目蒐集範圍

業務或服務作業流程		個人資料檔案名稱	姓名	生日	身分證號	護照號碼	特徵	指紋	婚姻	家庭	教育	職業	病歷	醫療	基因	性生活	健康檢查	犯罪前科	聯絡方式	財務情況	社會活動	直接識別	間接識別	間接識別的欄位
服務目錄或流程名稱	子流程名稱																							
A1 系統	平信催繳作業	平信催繳檔	Y		Y														Y					
A1 系統	平信催繳作業	平信催繳單	Y																Y					
A1 系統	收費系統	結案資料檔	Y																Y					

業務或服務作業流程		個人資料檔案名稱	姓名	生日	身分證號	護照號碼	特徵	指紋	婚姻	家庭	教育	職業	病歷	醫療	基因	性生活	健康檢查	犯罪前科	聯絡方式	財務情況	社會活動	直接識別	間接識別	間接識別的欄位
服務目錄或流程名稱	子流程名稱																							
A1 系統	掛號催繳作業	掛號催繳檔	Y																Y					
A1 系統	掛號催繳作業	掛號催繳單	Y																Y					

資料來源：本計畫整理

表25 A1 系統個資項目基本資料表

業務或服務作業流程		個人資料檔案基本資料					
服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	保有單位	檔案型態	保有依據	特定目的	個人資料類別
A1 系統	平信催繳作業	平信催繳檔	停車管理科	數位檔		'018	C001,C003
A1 系統	平信催繳作業	平信催繳單	停車管理科	實體紙本		'018	C001
A1 系統	收費系統	結案資料檔	停車管理科	數位檔		'018	C001,C003
A1 系統	掛號催繳作業	掛號催繳檔	停車管理科	數位檔		'018	C001,C003
A1 系統	掛號催繳作業	掛號催繳單	停車管理科	實體紙本		'018	C001

資料來源：本計畫整理

3.3.2.2. 識別個資項目相關生命週期活動

由導入顧問先行說明個資項目相關生命週期各欄位內涵，並協助系統負責人完成個資項目生命週期詳見表 26。

表26 A1 系統個資項目生命週期

業務或服務作業流程		個人資料檔案名稱	個人資料檔案生命週期活動									
服務目錄或流程名稱	子流程名稱		蒐集方式	蒐集者	蒐集介面	儲存位置	複本或備份或異地備援位置	法定保存期限	自訂保存期限	連結或內部傳送對象與方式	刪除或銷毀方式	國際傳輸對象與方式
A1 系統	平信催繳作業	平信催繳檔	間接	催繳人員	FTP 上傳下載	資料庫、催繳人員電腦	資料庫備份	N/A	六年	與催繳程式連結	整個檔案刪除,資料庫刪除結案資料	N/A
A1 系統	平信催繳作業	平信催繳單	間接	催繳人員	系統自行產生	費用繳交後條碼聯回市府	倉庫	N/A	六年	承辦人送郵局交寄	焚毀	N/A

業務或服務作業流程		個人資料檔案名稱	個人資料檔案生命週期活動									
服務目錄或流程名稱	子流程名稱		蒐集方式	蒐集者	蒐集介面	儲存位置	複本或備份或異地備援位置	法定保存期限	自訂保存期限	連結或內部傳送對象與方式	刪除或銷毀方式	國際傳輸對象與方式
A1 系統	收費系統	結案資料檔	間接	催繳人員	系統自行產生	資料庫	資料庫備份	N/A	六年	與收費程式連結	資料庫刪除結案資料	N/A
A1 系統	掛號催繳作業	掛號催繳檔	間接	催繳人員	FTP 上傳下載	資料庫、催繳人員電腦	資料庫備份	N/A	六年	與催繳程式連結	整個檔案刪除,資料庫刪除結案資料	N/A
A1 系統	掛號催繳作業	掛號催繳單	間接	催繳人員	系統自行產生	費用繳交後條碼聯回市府	倉庫	N/A	六年	承辦人送郵局交寄	焚毀	N/A

資料來源：本計畫整理

3.3.2.3. 識別個資項目與外部利害關係人之關聯

由導入顧問先行說明個資項目利害關係人各欄位內涵，並協助系統負責人完成個資項目利害關係人，詳見表 27。

表27 A1 系統個資項目利害關係人

業務或服務作業流程		個人資料檔案名稱	利害關係人				
服務目錄或流程名稱	子流程名稱		當事人	組織內部	委外	供應者	其他
A1 系統	平信催繳作業	平信催繳檔	車主,公務員	資訊組	系統委外開發	無	
A1 系統	平信催繳作業	平信催繳單	車主,公務員	資訊組	無	透過郵差寄送	
A1 系統	收費系統	結案資料檔	車主,公務員	資訊組	系統委外開發	無	
A1 系統	掛號催繳作業	掛號催繳檔	車公務員	資訊組	系統委外開發	無	
A1 系統	掛號催繳作業	掛號催繳單	車主,公務員	資訊組	無	透過郵差寄送	

資料來源：本計畫整理

3.3.2.4. 完成個資項目盤點

綜整個資項目基本資料與利害關係人，完成個資項目盤點(詳見表 28)，做為後續個資衝擊分析與評鑑之依據。

表28 A1 系統個資項目盤點表

業務或服務作業流程		個人資料檔案基本資料						利害關係人				
服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	保有單位	檔案型態	保有依據	特定目的	個人資料類別	當事人	組織內部	委外	供應者	其他
A1 系統	平信催繳作業	平信催繳檔	停車管理科	數位檔		'018	C001,C003	車主,公務員	資訊組	系統委外開發	無	
A1 系統	平信催繳作業	平信催繳單	停車管理科	實體紙本		'018	C001	車主,公務員	資訊組	無	透過郵差寄送	
A1 系統	收費系統	結案資料檔	停車管理科	數位檔		'018	C001,C003	車主,公務員	資訊組	系統委外開發	無	
A1 系統	掛號催繳作業	掛號催繳檔	停車管理科	數位檔		'018	C001,C003	車主,公務員	資訊組	系統委外開發	無	
A1 系統	掛號催繳作業	掛號催繳單	停車管理科	實體紙本		'018	C001	車主,公務員	資訊組	無	透過郵差寄送	

資料來源：本計畫整理

3.3.3. 個資衝擊分析

個資衝擊分析的主要目的，在於瞭解個資在蒐集、處理及利用過程中，是否已符合組織所處環境的法規命令與個資保護政策等遵循性要求。A1 系統負責人依「個資項目個資衝擊分析檢核表」(詳見附件 1_個資項目個資衝擊分析檢核表)，檢討該系統個資項目衝擊分析，經彙整所有檢核表內容完成個資項目衝擊分析表，做為未來改善計畫之依據，詳見表 29 與表 30。

表29 A1 系統個資項目衝擊分析表(1)

服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	欄位 1	欄位 2	欄位 3	欄位 4	欄位 5	欄位 6	欄位 7	欄位 8
A1 系統	平信催繳作業	平信催繳檔	>50,000	>50,000	1-5	不適用	N/A	六年	是	否
A1 系統	平信催繳作業	平信催繳單	>50,000	>50,000	1-5	不適用	N/A	六年	是	否
A1 系統	收費系統	結案資料檔	>50,000	>50,000	1-5	不適用	N/A	六年	是	否

服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	欄位 1	欄位 2	欄位 3	欄位 4	欄位 5	欄位 6	欄位 7	欄位 8
A1 系統	掛號催繳作業	掛號催繳檔	>50,000	>50,000	1-5	不適用	N/A	六年	是	否
A1 系統	掛號催繳作業	掛號催繳單	>50,000	>50,000	1-5	不適用	N/A	六年	是	否

資料來源：本計畫整理

表30 A1 系統個資項目衝擊分析表(2)

欄位 9	欄位 10	欄位 11	欄位 12	欄位 13	欄位 14	欄位 15	欄位 16	欄位 17	欄位 18
0. 無確認	否		不適用	不適用	不適用	不適用	否	否	是
0. 無確認	否		不適用	不適用	不適用	不適用	否	否	是
0. 無確認	否		不適用	不適用	不適用	不適用	否	否	是
0. 無確認	否		不適用	不適用	不適用	不適用	否	否	是
0. 無確認	否		不適用	不適用	不適用	不適用	否	否	是

欄位說明：

欄位 1：目前保有多少數量(筆數)的個人資料？

欄位 2：每年大約會處理多少數量(筆數)的個人資料？

欄位 3：每筆資料中包含的個人資料欄位數量為多少？

欄位 4：於蒐集個資前是否主動公告其所依循之法源、機構或合約?

欄位 5：法定保存期限

欄位 6：自定保存期限

欄位 7：於執行個資蒐集相關業務/專案前是否已完成系統安全計畫？

欄位 8：是否透過商業廣告方式取得或使用已公開之個資？

欄位 9：如何確認個資內容之正確性？

欄位 10：除執行業務外，是否利用所蒐集之個資進行資料搜尋、分析或統計等用途?

欄位 11：前項問題之回應若為是，這些活動是否已告知當事人?

欄位 12：當事人是否具有同意、拒絕提供個資之權利？

欄位 13：當事人是否具有隨時要求停止蒐集、處理或利用該個資之權利？

欄位 14：於個資蒐集之初是否告知當事人得利用個資之利害關係方與其利用方式等資訊？

欄位 15：是否限制利害相關方利用個資之方式與禁止其從事與原訂利用方式無關之活動？

欄位 16：是否有方式提供當事人查詢或請求閱覽個資或製給複製本？

欄位 17：是否有方式提供當事人更正或補充其個資？

欄位 18：是否定期審視或稽核以確保個資之蒐集、利用及處理皆遵循已訂定之管理規範？

資料來源：本計畫整理

3.3.4. 個資風險評估

本專案 A1 系統負責人針對所擁有個資項目的機密性、完整性及可用性等構面向，依前置作業所擬之個資風險等級基準值(詳見表 17)，進行個資風險評估作業，以瞭解個資項目之風險等級，做為後續擬訂安全控制措施之依據，經彙整相關個資衝擊分析結果採最高原則，評定結果本系統風險等級為「高」詳見表 31。

表31 A1 系統風險評估表

服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	含有個資類別	NIST SP800-122「個人可識別資訊機密性保護指引」之衝擊等級判定方式	「資訊系統分類分級與鑑別機制」影響構面與個資項目價值對應	風險等級
A1 系統	平信催繳作業	平信催繳檔	高	普	普	高
A1 系統	平信催繳作業	平信催繳單	高	普	普	高
A1 系統	收費系統	結案資料檔	高	普	普	高
A1 系統	掛號催繳作業	掛號催繳檔	高	普	普	高
A1 系統	掛號催繳作業	掛號催繳單	高	普	普	高

資料來源：本計畫整理

3.3.5. 安全控制措施選取

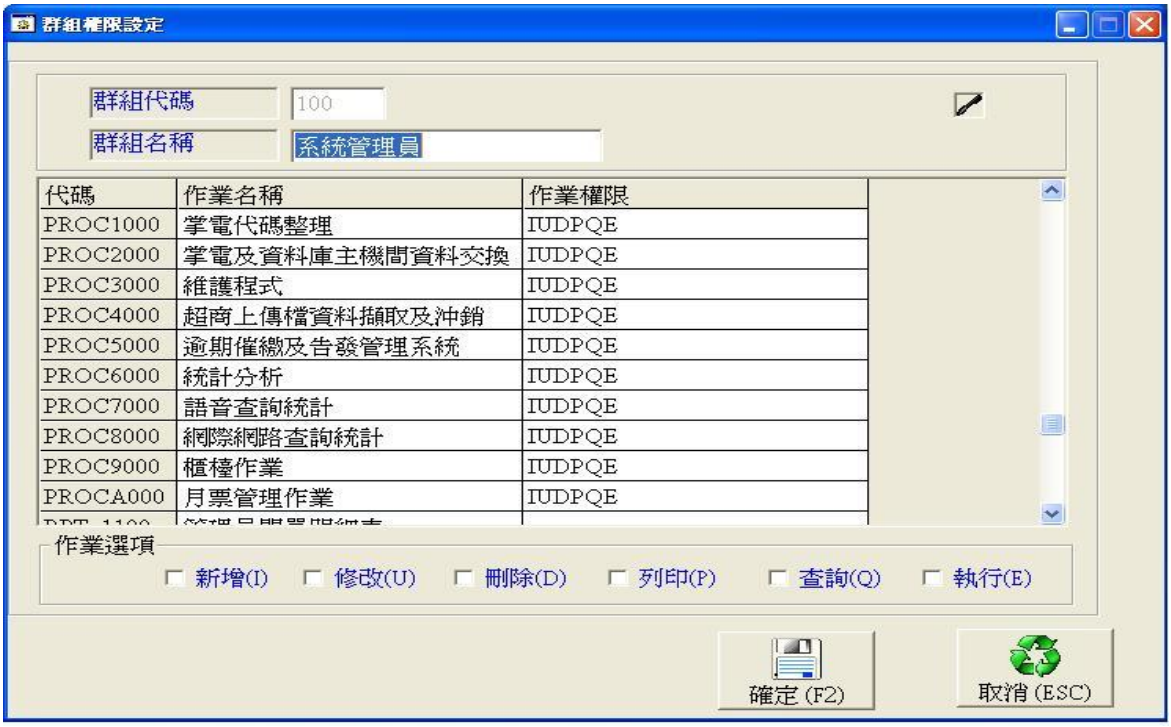
本專案技術安全控制措施採用個資項目技術安全控制措施基準值評估表(詳見附件 3_個資項目技術安全控制措施基準值評估表)，A1 系統之個資項目其檔案格式有紙本與電子檔案 2 種，由於紙本檔案之平信催繳單與掛號催繳單所需安全維護相同，且風險安全等級相同，故該 2 個資項目之安全控制措施整併為同一表格；電子檔案之平信催繳檔、結案資料檔及掛號催繳檔存在於同一伺服器，且風險安全等級相同，故該 3 個資項目之安全控制措施整併為同一表格，經系統負責人先行選取所需安全控制措施，再由導入顧問協助完成紙本與電子檔案安全控制措施選取，詳見附件 7_個案 A 紙本安全控制措施與附件 8_個案 A 電子檔安全控制措施。

3.3.6. 個資人員權責角色

在處理個資時，需確認組織內外及相關人員之權責角色，並依照其權責給予所應具備之權限，在發生個資事故時，便可儘速釐清可能洩露之管道。

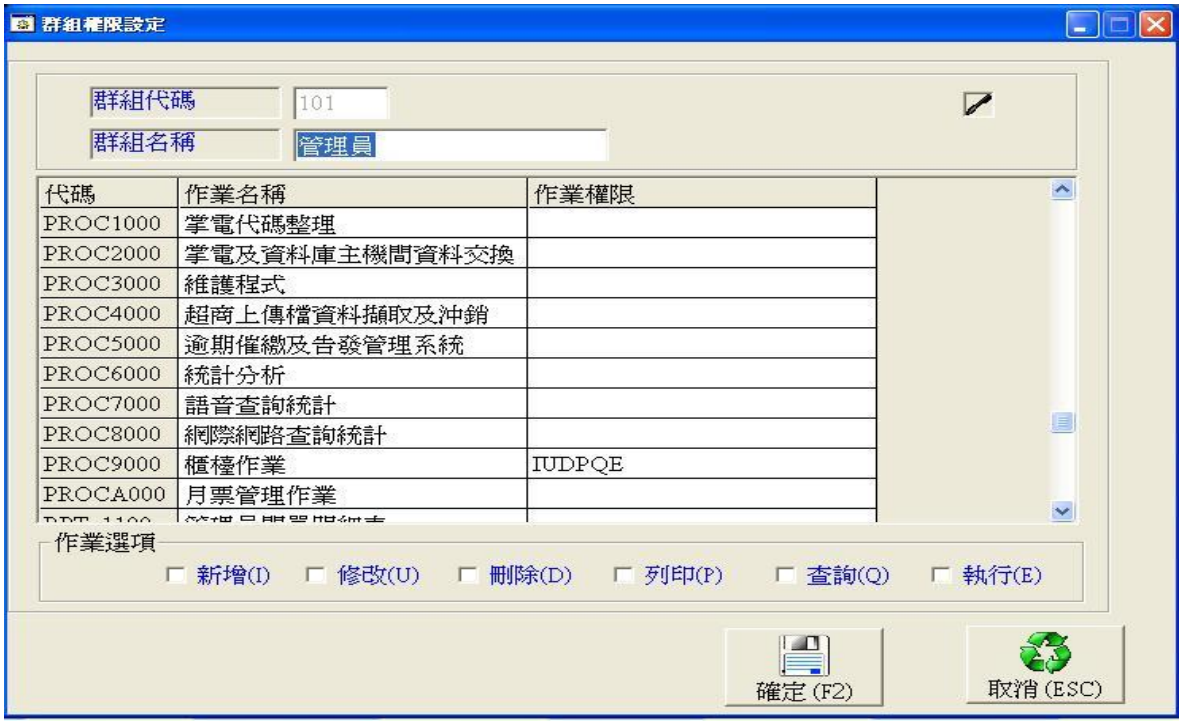
確立人員權責角色之任務，包括識別個資管理相關人員或群組角色、建立個資項目生命週期活動與個資管理角色之對應表、識別對應表內個資管理角色細部權責定義需求、完成人員權責角色定義及轉換個資管理人員權責角色定義至相關應用系統權限定義。

A1 系統於設計之初，即依人員權責角色規劃之任務訂定相關群組角色，計分為系統管理員、管理員及稽核員 3 種，詳見圖 19~圖 21，再依相關作業人員所擔任任務賦予作業人員權責，範例詳見圖 22。



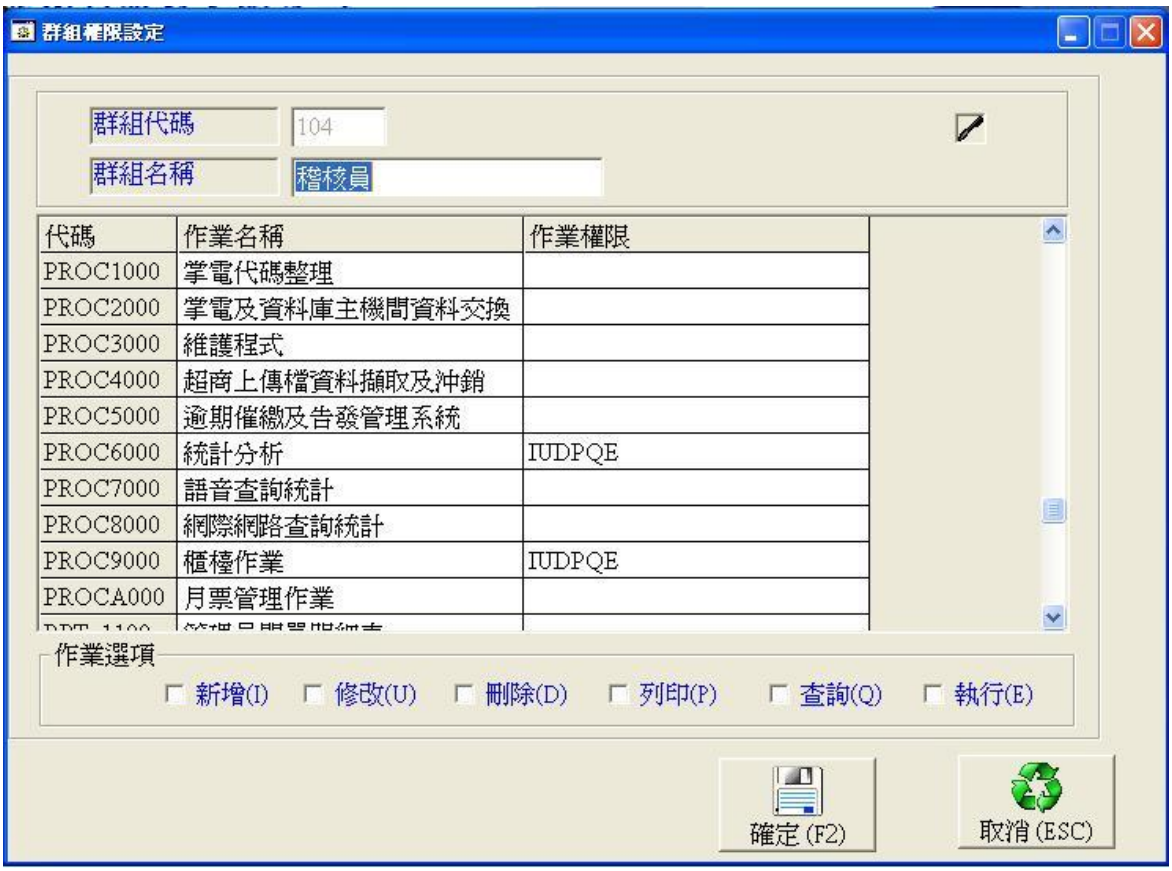
資料來源：本計畫整理

圖19 系統管理員群組權限



資料來源：本計畫整理

圖20 管理員群組權限



資料來源：本計畫整理

圖21 稽核員群組權限

資料來源：本計畫整理

圖22 作業人員個人權限

3.3.7. 建立個資管理程序

組織於業務作業需求需蒐集個資時，應訂定個資蒐集作業流程，確認個資蒐集符合特定目的，同時設計個資同意書範本，以利於蒐集個資時使用。於蒐集資料之流程中，檢視所涉及之管理作業流程與程序書，符合組織之個資保護政策，修定相關文件資料內容。本階段之管理重點為清楚的管理權責定義、依據法令與流程進行個資分類及落實公開與告知等隱私管理原則。

建立個資管理程序之任務，包括設計個資生命週期作業流程、設計個資事故管理作業流程、設計個資管理稽核作業流程及修訂組織內部管理制度文件。

鑒於個人資料保護法於 101 年 10 月 1 日正式施行，個案 A 於 101 年 10 月 8 日頒布個案 A 個人資料保護管理要點，詳見附件 9_個案 A 個人資料保護管理要點。另個案 A 個人資料管理其他相關程序現正由法務室研擬中，導入顧問亦就個人資料之蒐集、處理、利用及傳輸標準作業程序(詳見附件 10_個人資料之蒐集、處理、利用及傳輸標準作業程序)與個人資料之盤點、公開作業程序(詳見附件 11_個人資料之盤點、公開作業程序)提供範例供個案 A 參酌。另導入顧問亦說明委外作業管理(請參閱 3.3.8)、以資安事故通報範例說明個資通報應變應注意事項及稽核計畫(詳見附件 12_資安事故通報與紀錄表範例~附件 15_稽核紀錄範例)，並說明個資管理相關程序宜併入現行資安管理程序。

3.3.8. 委外作業管理

個案 A 之應用系統幾乎是採委外開發，委外作業雖是由外部第三方執行，但仍需符合組織個資防護要求，故於委外作業流程中，應檢視並要求第三方於處理個資作業時，必須具備個資安全保護措施，同時保留稽核之權利，

故於導入期間由導入顧問說明機關個資系統委外時，應於委外需求說明書中增列個資需求說明如后：

- 承包廠商應建立隱私保護政策，承包廠商與承包廠商人員應遵循本機關的隱私權政策、個人資料保護與管理辦法、及相關個人資料保護與管理要求，承包廠商與承包廠商人員，應對本專案相關個人資料檔案負保護與管理責任，並符合個人資料保護法等相關法規命令要求。
- 承包廠商須提供參與本案人員個人資料保護與管理教育訓練，並舉行測驗，教育訓練內容須包括人員對個人資料保護的認知，個人資料檔案蒐集、處理及利用的作業要求等，教育訓練內容及測驗卷送本機關備查。
- 未經本機關事先書面同意，承包廠商不得將本專案相關個人資料檔案攜出履約地點。若有事先經本機關書面允許之情形，承包廠商應於本專案終止前將相關個人資料檔案交還本機關，同時承包廠商不得對任何交還之個人資料檔案進行複印、複製、攝錄影及拍照等各式保存行為。
- 承包廠商應建立個資事故之正式通報程序及管道，並訂定通報後應採行之處理措施，如相關個人資料遭受侵害時，承包廠商應依事前訂定之通報管道立即通報本機關。
- 本機關於本專案有效期間暨專案合約正式終止後一年內，得不定期至承包廠商場所稽核其對於本專案相關個人資料蒐集、處理及利用情形，以防個人資料外洩或遭受侵害，確保個人資料保護與管理之要求。

3.4.「結案」

本專案依導入實施步驟執行 4 階段導入，各階段執行情形詳見圖 23，並於導入過程完成後，邀請個案 A 全體參與人員，針對參考指引之內容與導入

方法，進行導入所見的意見進行彙整，於結案會議中說明，結案簡報詳見附件 16_個案 A 導入結案會議簡報。

資料來源：本計畫整理

圖23 參考指引導入執行情形

4. 個案 B 導入執行情形

4.1.「開始」

4.1.1. 決定系統範圍與前置作業

4.1.1.1. 機關資訊作業背景介紹

個案 B 資訊單位負責資訊業務推動相關事宜，業務職掌如下：

- 整體資訊業務發展目標及策略之研擬。
- 資訊業務之整體規劃、訓練及研究發展。
- 資訊應用系統之規劃、開發及維護。
- 資訊作業與資料庫環境之建置、維護及管理。
- 電腦與網路環境之建置、操作及管理。
- 資通安全作業之規劃及辦理。
- 與其他機關間資訊交換之協調。
- 附屬機構資訊業務之查核。
- 其他有關資訊事項。

4.1.1.2. 前置作業

為利於導入專案順利進行，個案 B 與導入顧問先期協商導入作業執行細節後，個案 B 將篩選 2-3 個業務或系統，經討論後列出優先次序，列為導入候選對象，並召開「導入啟動會議」，由導入顧問說明與討論相關前置作業內容，並由導入計畫團隊簽具保密切結，詳見附件 17_個案 B 保密切結書，會議相關事項說明於后：

●參與單位

個案 B 與技服中心。

●內容

說明導入工作計畫書，包括導入計畫目的與範圍、導入指引的執行方式、導入活動人員、導入計畫團隊、導入計畫時程及雙方配合事項。啟動會議簡報與導入工作計畫書,詳見附件 18_個案 B 導入啟動會議簡報與附件 19_個案 B 導入工作計畫書。

●結論

本專案計劃訂於 101 年 11 月 1 日起每週三下午，執行「個人資料保護參考指引」實務導入作業，總共導入期程約為十三週。本案擬選定一項包含個資項目之業務，進行導入試行。

導入系統/業務之選取,若能選取與業務部門相關且於導入期間邀請業務部門共同參與，對參考指引之適用性與可用性將較有助益。

4.1.1.3. 訂定個資風險等級

4.1.1.3.1. 個資風險等級基準值

本次導入個資風險等級以含有個資類別、NIST SP800-122 之衝擊等級及「資訊系統分類分級與鑑別機制」影響構面等 3 個面向，分別檢討其風險等級，再採最高原則評定為該個資之風險等級，其中「資訊系統分類分級與鑑別機制」影響構面，則依鑑別機制之 6 大構面中，「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信譽」3 者作綜合考量。經與導入機關討論，本專案個資風險等級基準值評定方式，依照參考指引之個資風險等級基準值建議表為基準，執行相關內容同表 8。

其中「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信譽」三

者影響構面之安全等級之安全等級設定原則，如下：

●資料保護受到損害：以資料機密性與完整行受導損害之影響考量，詳見表32。

表32 資料保護受到損害安全等級設定原則

安全等級	設定原則
普 (等級 1)	▪(資料機密性)一般性資料；資料外洩不致影響個人權益或僅導致個人權益輕微受損 ▪(資料完整性)資料遭竄改不致影響個人權益或僅導致個人權益輕微受損
中 (等級 2)	▪(資料機密性)敏感性資料；資料外洩將導致個人權益嚴重受損，如： ➢ 涉及個人出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、聯絡方式、財務情形、社會活動及其他得以直接或間接識別個人之資料 ➢ 具有敏感屬性之個人資料，如：中途輟學學生、收養兒童等資料，資料外洩可能導致個人隱私遭冒犯 ▪(資料完整性)資料遭竄改將導致個人權益嚴重受損
高 (等級 3)	▪（資料機密性）機密性資料；資料外洩將危及國家安全、導致個人權益非常嚴重受損、或造成極大規模之個人權益嚴重受損，如： ➢ 凡涉及國家安全之外交、情報、國境安全、財稅、經濟、金融、醫療等重要機敏系統

安全等級	設定原則
	▪特殊屬性之個人資料(如：臥底警員、受保護證人、被害人等資料)，資料外洩可能會使相關個人身心受到危害、社會地位受到損害、或衍生財物損失等情形 ▪涉及個人之醫療、基因、性生活、健康檢查、犯罪前科等資料，資料外洩將使個人權益非常嚴重受損。例如：醫療資訊系統、刑案資訊整合系統等 ▪極大規模(如：全國性)之涉及個人出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、聯絡方式、財務情形、社會活動及其他得以直接或間接識別個人之資料。例如：戶役政資訊系統、護照管理系統等 ▪(資料完整性)資料遭竄改將危及國家安全、導致個人權益非常嚴重受損、或造成極大規模之個人權益嚴重受損

資料來源：本計畫整理

●影響法律規章遵循：以系統運作、資料保護、資訊資產使用等，違反法律規章所可能影響之後果為考量，詳見表 33。

表33 影響法律規章遵循安全等級設定原則

安全等級	設定原則
普 (等級 1)	▪系統運作、資料保護、資訊資產使用等須依循相關規範辦理，否則將導致機關違反法律規章並伴隨輕微不良後果，如： ➢ **依使用授權年限購買之資訊系統或軟體：**授權年限到期，必須停止使用，否則將涉及違反契約及智慧財產權相關法令之遵循性 ➢ **全球資訊網：**必須符合智慧財產權相關法令尊重他人智

安全等級	設定原則
	慧結晶，並遵守兒童及少年福利法、電腦網路內容分級處理辦法進行資訊內容管理，否則將涉及違反法律之遵循性
中 (等級 2)	▪系統運作、資料保護、資訊資產使用等須依循相關規範辦理，否則將導致機關違反法律規章並伴隨嚴重不良後果，如： ➢ **政府電子採購網**：依「政府採購法」第 27 條規定，機關辦理公開招標或選擇性招標，應將招標公告或辦理資格審查之公告刊登於政府採購公報或公開於資訊網路。因此，若系統資料遭竄改導致公告資料錯誤，將影響採購作業透明化
高 (等級 3)	▪系統運作、資料保護、資訊資產使用等須依循相關規範辦理，否則將導致機關從根本上違反法律規章，如： ➢ **機密性資料**：依「國家機密保護法施行細則」第 28 條第 4 款規定，國家機密之保管方式直接儲存於資訊系統者，須將資料以政府權責主管機關認可之加密技術處理，該資訊系統並不得與外界連線。因此，機關若未依循規定儲存資料，將涉及從根本上違反法律之遵循性。 ➢ **醫療機構醫囑暨電子病歷系統**：依「醫療機構電子病歷製作及管理辦法」第 3、4 條規定，電子病歷資訊系統之建置、電子病歷之製作及貯存應符合相關規定。因此，機關若未依循相關規定進行系統建置維運及資料儲存，將涉及從根本上違反法律之遵循性

資料來源：本計畫整理

●損害組織信譽：以系統發生資訊安全事故，導致機關形象、信譽受到損害情形為考量，詳見表 34。

表34 損害組織信譽安全等級設定原則

安全等級	設定原則
普 (等級 1)	▪若系統發生資訊安全事故，將導致機關形象、信譽受到輕微損害，如：導致區域性媒體報導負面新聞、造成多位民眾電話抱怨等情形
中 (等級 2)	▪若系統發生資訊安全事故，將導致機關形象、信譽受到嚴重損害，如：導致全國性媒體報導負面新聞、造成民眾至機關抗議或陳情等情形
高 (等級 3)	▪若系統發生資訊安全事故，將導致機關形象、信譽受到非常嚴重損害，如：導致國際性媒體報導負面新聞、造成民眾大規模遊行抗爭等情形

資料來源：本計畫整理

4.1.1.3.2. 衝擊分析

本專案導入目標所採用之個資項目衝擊分析方法，經討論沿用「個人資料保護參考指引」之衝擊分析檢核表(詳見附件 1_個資項目個資衝擊分析檢核表)，做為檢視該個資項目之可能衝擊。

4.1.1.3.3. 風險評估

本專案個資風險等級評估，係依據 PIA/RA 安全控制項目基準值之組織含有個資類別、NIST SP800-122「個人可識別資訊機密性保護指引」之衝擊等級判定方式，以及「資訊系統分類分級與識別機制」影響構面與個資項目

價值進行對應，採最高原則方式判別，並彙整相關個資衝擊分析結果，做為後續擬訂安全控制措施之依據。

4.1.1.4. 決定資訊系統範疇與邊界

導入機關為展現對導入計畫之支持與承諾，自行遴選「B1 業務」，做為導入目標。

4.2.「文件導讀」

4.2.1.「個人資料保護參考指引」導讀

於 101 年 11 月 14 日導讀「個人資料保護參考指引」，由導入顧問透過簡報說明個資國際發展趨勢、我國個資相關規範、個人資料保護參考指引簡介及資訊安全管理制度(ISMS)與個資保護整合建議。主要內容同 2.2。

4.3.「參考指引導入」

由導入顧問與個案 B 遴選之「B1 業務」，由 BA 與 BB 二單位共同執行，依據 3.1「開始」階段所訂定之個資風險等級基準值評估、個資衝擊分析及個資風險評估原則，針對所遴選之「B1 業務」依參考指引規畫階段與執行階段執行導入。

4.3.1. 作業流程分析

由於從業務作業流程面著手分析，較能夠找出與該業務相關之個資項目，並進行適當保護。針對所挑選之「B1 業務」，於 101 年 11 月 21 日請業務負責人，從與該業務作業管理相關之文件程序與規範著手，清查該系統所含有之個資項目。

4.3.2. 個資項目盤點

個資項目盤點主要目的在盤點組織所擁有之個資項目內容，包括個資項目的類別、目的、來源、欄位、數量、型態、相關生命週期活動及相關利害關係人等，以利後續進行個資之個資衝擊分析、個資風險評估、保護及管理等活動。

本專案個資項目盤點之任務，包括識別不同作業流程之個資項目、識別個資項目之類別、依據及目的、識別個資項目相關生命週期活動、識別個資項目與外部利害關係人之關聯及完成個資項目盤點。有關每項任務導入情形，說明如下：

4.3.2.1. 識別不同作業流程之個資項目

「B1 業務」負責人依作業流程分析，進行個資盤點結果詳見表 35、表 36。

表35 B1 業務－BA 單位個資流程分析表

業務或服務作業流程		個人資料檔案名稱	是否為個資流程
服務目錄或流程名稱	子流程名稱		
B1 業務	清單報送作業	報送清單	是
B1 業務	清單報送作業	清單電子檔	是
B1 業務	清單建檔作業	清單	是
B1 業務	清單建檔作業	專案資料庫	是
B1 業務	專案資料異動作業	專案資料	是
B1 業務	專案提前作業	專案提前資料	是
B1 業務	專案展延作業	專案展延資料	是

業務或服務作業流程		個人資料檔案名稱	是否為個資流程
服務目錄或流程名稱	子流程名稱		
B1 業務	專案催收作業	專案催收資料	是

資料來源：本計畫整理

表36 B1 業務－BB 單位個資流程分析表

業務或服務作業流程		個人資料檔案名稱	是否為個資流程
服務目錄或流程名稱	子流程名稱		
B1 業務	專案提前申報作業	專案提前檔案	是
B1 業務	產生資料明細	資料計算明細檔案	是
B1 業務	申報資料	資料計算明細表	是
B1 業務	資料審核作業	資料庫	是

資料來源：本計畫整理

4.3.2.2. 識別個資項目之類別、依據及目的

B1 業務負責人將識別出之個資項目，依個資法與其施行細則所規定之個資管理應完成事項清單、行政命令、準則，識別個資項目之蒐集範圍、類別、蒐集依據及蒐集目的，經導入顧問協助完成個資項目蒐集範圍與個資項目基本資料表，做為未來通知利害相關人之依據，詳見表 37~表 40。

表37 B1 業務－BA 單位個資項目蒐集範圍

業務或服務作業流程		個人資料檔案名稱	姓名	生日	身分證號	護照號碼	特徵	指紋	婚姻	家庭	教育	職業	病歷	醫療	基因	性生活	健康檢查	犯罪前科	聯絡方式	財務情況	社會活動	直接識別	間接識別
服務目錄或流程名稱	子流程名稱																						
B1 業務	清單報送作業	報送清單	Y		Y				Y											Y			
B1 業務	清單報送作業	清單電子檔	Y		Y				Y											Y			
B1 業務	清單建檔作業	清單	Y		Y				Y											Y			
B1 業務	清單建檔作業	專案資料庫	Y		Y				Y											Y			
B1 業務	專案資料異動作業	專案資料	Y		Y				Y											Y			
B1 業務	專案提前作業	專案提前資料	Y		Y															Y			

業務或服務作業流程		個人資料檔案名稱	姓名	生日	身分證號	護照號碼	特徵	指紋	婚姻	家庭	教育	職業	病歷	醫療	基因	性生活	健康檢查	犯罪前科	聯絡方式	財務情況	社會活動	直接識別	間接識別
服務目錄或流程名稱	子流程名稱																						
B1 業務	專案展延作業	專案展延資料	Y		Y															Y			
B1 業務	專案催收作業	專案催收資料	Y		Y															Y			

資料來源：本計畫整理

表38 B1 業務－BB 單位個資項目蒐集範圍

業務或服務作業流程		個人資料檔案名稱	姓名	生日	身分證號	護照號碼	特徵	指紋	婚姻	家庭	教育	職業	病歷	醫療	基因	性生活	健康檢查	犯罪前科	聯絡方式	財務情況	社會活動	直接識別	間接識別
服務目錄或流程名稱	子流程名稱																						
B1 業務	專案提前申報作業	專案提前檔案	Y		Y															Y			
B1 業務	產生資料明細	資料計算明細檔案	Y		Y															Y			
B1 業務	申報資料	資料計算明細表	Y		Y															Y			
B1 業務	資料審核作業	資料庫	Y		Y															Y			

資料來源：本計畫整理

表39 B1 業務－BA 單位個資項目基本資料表

業務或服務作業流程		個人資料檔案基本資料					
服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	保有單位	檔案型態	保有依據	特定目的	個人資料類別
B1 業務	清單報送作業	報送清單	BA 單位	實體紙本	略	177	C001，C003，C021，C084
B1 業務	清單報送作業	清單電子檔	BA 單位	數位檔	略	177	C001，C003，C021，C084
B1 業務	清單建檔作業	清單	BA 單位	實體紙本	略	177	C001，C003，C021，C084
B1 業務	清單建檔作業	專案資料庫	BA 單位	數位檔	略	177	C001，C003，C021，C084
B1 業務	專案資料異動作業	專案資料	BA 單位	實體紙本	略	177	C001，C003，C021，C084
B1 業務	專案提前作業	專案提前資料	BA 單位	實體紙本	略	177	C001，C003，C084
B1 業務	專案展延作業	專案展延資料	BA 單位	實體紙本	略	177	C001，C003，C084

業務或服務作業流程		個人資料檔案基本資料					
服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	保有單位	檔案型態	保有依據	特定目的	個人資料類別
B1 業務	專案催收作業	專案催收資料	BA 單位	實體紙本	略	177	C001，C003，C084

資料來源：本計畫整理

表40 B1 業務－BB 單位個資項目基本資料表

業務或服務作業流程		個人資料檔案基本資料					
服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	保有單位	檔案型態	保有依據	特定目的	個人資料類別
B1 業務	專案提前申報作業	專案提前檔案	BB 單位	數位檔	略	177	C001
B1 業務	產生資料明細	資料計算明細檔案	BB 單位	數位檔	略	177	C001
B1 業務	申報資料	資料計算明細表	BB 單位	實體紙本	略	177	C001
B1 業務	資料審核作業	資料庫	BB 單位	數位檔	略	177	C001

資料來源：本計畫整理

4.3.2.3. 識別個資項目相關生命週期活動

由導入顧問先行說明個資項目相關生命週期各欄位內涵，並協助業務負責人完成個資項目生命週期詳見表 41、表 42。

表41 B1 業務－BA 單位個資項目生命週期

業務或服務作業流程		個人資料檔案名稱	蒐集方式	蒐集者	蒐集介面	儲存位置	複本或備份或異地備援位置	法定保存期限	自訂保存期限	連結或內部傳送對象與方式	刪除或銷毀方式	國際傳輸對象與方式
服務目錄或流程名稱	子流程名稱											
B1 業務	清單報送作業	報送清單	間接	BA 單位	公文	檔案室	無	N/A	99 年	BB 單位	依檔管局規定進行銷毀	N/A
B1 業務	清單報送作業	清單電子檔	間接	BA 單位	公文	BA 單位	無	N/A	3 個月	BB 單位	刪除檔案	N/A
B1 業務	清單建檔作業	清單	間接	BA 單位	公文	檔案室	無	N/A	99 年	BB 單位	依檔管局規定進行銷毀	N/A
B1 業務	清單建檔作業	專案資料庫	間接	BA 單位	公文	主機	中區備援中心	N/A	99 年	BB 單位	依個案 B 應用系統廢止程序辦理	N/A
B1 業務	專案資料異動作業	專案資料	間接	BA 單位	公文	檔案室	無	N/A	30 年	BB 單位	依檔管局規定進行銷毀	N/A
B1 業務	專案提	專案提	間接	BA 單位	公文	檔案室	無	N/A	30 年	BB 單位	依檔管局規定進行銷毀	N/A

業務或服務作業流程		個人資料檔案名稱	蒐集方式	蒐集者	蒐集介面	儲存位置	複本或備份或異地備援位置	法定保存期限	自訂保存期限	連結或內部傳送對象與方式	刪除或銷毀方式	國際傳輸對象與方式
服務目錄或流程名稱	子流程名稱											
	前作業	前資料										
B1 業務	專案展延作業	專案展延資料	間接	BA 單位	公文	檔案室	無	N/A	30 年	BB 單位	依檔管局規定進行銷毀	N/A
B1 業務	專案催收作業	專案催收資料	間接	BA 單位	公文	檔案室	無	N/A	30 年	BB 單位	依檔管局規定進行銷毀	N/A

資料來源：本計畫整理

表42 B1 業務－BB 單位個資項目生命週期

業務或服務作業流程		個人資料檔案名稱	蒐集方式	蒐集者	蒐集介面	儲存位置	複本或備份或異地備援位置	法定保存期限	自訂保存期限	連結或內部傳送對象與方式	刪除或銷毀方式	國際傳輸對象與方式
服務目錄或流程名稱	子流程名稱											
B1 業務	專案提前申報作業	專案提前檔案	間接	BB 單位	e-mail	承辦人 PC		N/A	N/A			無
B1 業務	產生資料明細	資料計算明細檔案	間接	BB 單位		承辦人 PC		N/A	N/A			無
B1 業務	申報資料	資料計算明細表	間接	BB 單位	公文	檔案室		N/A	99 年	BA 單位	依檔管局規定進行銷毀	無
B1 業務	資料審核作業	資料庫	間接	BB 單位	e-mail 公文	INTRA SERVER	北區備援	N/A	99 年		依業務處理規範辦理	無

資料來源：本計畫整理

4.3.2.4. 識別個資項目與外部利害關係人之關聯

由導入顧問先行說明個資項目利害關係人各欄位內涵，並協助業務負責人完成個資項目利害關係人，詳見表 43、表 44。

表43 B1 業務－BA 單位個資項目利害關係人

業務或服務作業流程		個人資料檔案名稱	利害關係人				
服務目錄或流程名稱	子流程名稱		當事人	組織內部	委外	供應者	其他
B1 業務	清單報送作業	報送清單	民眾	BB 單位、檔案室	無	信差、快遞、郵局	
B1 業務	清單報送作業	清單電子檔	民眾	BB 單位	無	信差、快遞、郵局	
B1 業務	清單建檔作業	清單	民眾	BB 單位、檔案室	無	信差、快遞、郵局	
B1 業務	清單建檔作業	專案資料庫	民眾	資訊單位	無	信差、快遞、郵局	
B1 業務	專案資料異動作業	專案資料	民眾	BB 單位、檔案室	無	信差、快遞、郵局	
B1 業務	專案提前作業	專案提前資料	民眾	BB 單位、檔案室	無	信差、快遞、郵局	
B1 業務	專案展延作業	專案展延資料	民眾	BB 單位、檔案室	無	信差、快遞、郵局	
B1 業務	專案催收作業	專案催收資料	民眾	BB 單位、檔案室	無	信差、快遞、郵局	

資料來源：本計畫整理

表44 B1 業務－BB 單位個資項目利害關係人

業務或服務作業流程		個人資料檔案名稱	利害關係人				
服務目錄或流程名稱	子流程名稱		當事人	組織內部	委外	供應者	其他
B1 業務	專案提前申報作業	專案提前檔案	民眾		無		
B1 業務	產生資料明細	資料計算明細檔案	民眾		無	無	
B1 業務	申報資料	資料計算明細表	民眾	BA 單位、檔案室	無	信差、快遞、郵局	
B1 業務	資料審核作業	資料庫	民眾	資訊單位	無	無	

資料來源：本計畫整理

4.3.2.5. 完成個資項目盤點

綜整個資項目基本資料與利害關係人，完成個資項目盤點詳見表 45、表 46，做為後續個資衝擊分析與評鑑之依據。

表45 B1 業務－BA 單位個資項目盤點表

業務或服務作業流程		個人資料檔案基本資料						利害關係人				
服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	保有單位	檔案型態	保有依據	特定目的	個人資料類別	當事人	組織內部	委外	供應者	其他
B1 業務	清單報送作業	報送清單	BA 單位	實體紙本	略	177	C001，C003，C021，C084	民眾	BB 單位、檔案室	無	信差、快遞、郵局	
B1 業務	清單報送作業	清單電子檔	BA 單位	數位檔	略	177	C001，C003，C021，C084	民眾	BB 單位	無	信差、快遞、郵局	
B1 業務	清單建檔作業	清單	BA 單位	實體紙本	略	177	C001，C003，C021，C084	民眾	BB 單位、檔案室	無	信差、快遞、郵局	
B1 業務	清單建檔作業	專案資料庫	BA 單位	數位檔	略	177	C001，C003，C021，C084	民眾	資訊單位	無	信差、快遞、郵局	
B1 業務	專案資料異動作業	專案資料	BA 單位	實體紙本	略	177	C001，C003，C021，C084	民眾	BB 單位、檔案室	無	信差、快遞、郵局	
B1 業務	專案提前作業	專案提前資料	BA 單位	實體紙本	略	177	C001，C003，C084	民眾	BB 單位、檔案室	無	信差、快遞、郵局	

業務或服務作業流程		個人資料檔案基本資料						利害關係人				
服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	保有單位	檔案型態	保有依據	特定目的	個人資料類別	當事人	組織內部	委外	供應者	其他
B1 業務	專案展延作業	專案展延資料	BA 單位	實體紙本	略	177	C001，C003，C084	民眾	BB 單位、檔案室	無	信差、快遞、郵局	
B1 業務	專案催收作業	專案催收資料	BA 單位	實體紙本	略	177	C001，C003，C084	民眾	BB 單位、檔案室	無	信差、快遞、郵局	

資料來源：本計畫整理

表46 B1 業務－BB 單位個資項目盤點表

業務或服務作業流程		個人資料檔案基本資料						利害關係人				
服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	保有單位	檔案型態	保有依據	特定目的	個人資料類別	當事人	組織內部	委外	供應者	其他
B1 業務	專案提前申報作業	專案提前檔案	BB 單位	數位檔	略	177	C001	民眾		無		
B1 業務	產生資料明細	資料計算明細檔案	BB 單位	數位檔	略	177	C001	民眾		無	無	
B1 業務	申報資料	資料計算明細表	BB 單位	實體紙本	略	177	C001	民眾	BA 單位、檔案室	無	信差、快遞、郵局	
B1 業務	資料審核作業	資料庫	BB 單位	數位檔	略	177	C001	民眾	資訊單位	無	無	

資料來源：本計畫整理

4.3.3. 個資衝擊分析

個資衝擊分析的主要目的係瞭解個資於蒐集、處理及利用過程中，是否已符合組織所處環境的法規命令與個資保護政策等遵循性要求。B1 業務負責人依「個資項目個資衝擊分析檢核表」(詳見附件 1_個資項目個資衝擊分析檢核表)，檢討該業務個資項目衝擊分析，經彙整所有檢核表內容完成個資項目衝擊分析表，做為未來改善計畫之依據，詳見表 47~表 50。

4.3.4. 個資風險評估

個案 B 依據個資風險等級基準值建議表為基準(詳見表 8)，調整含有個資類別之風險等級，做為個案 B 適用之個資風險等級基準值建議表為基準，詳見表 51。

表47 B1 業務－BA 單位個資項目盤點表(1)

服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	目前保有多少數量(筆數)的個人資料？	每年大約會處理多少數量(筆數)的個人資料？	每筆資料中包含的個人資料欄位數量為多少？	於蒐集個資前是否主動公告其所依循之法源、機構或合約?	法定保存期限	自定保存期限	於執行個資蒐集相關業務/專案前是否已完成系統安全計畫？	是否透過商業廣告方式取得或使用已公開之個資？
B1 業務	清單報送作業	報送清單	5,000-50,000	1-500	1-5	不適用	N/A	99 年	是	不適用
B1 業務	清單報送作業	清單電子檔	1-500	1-500	1-5	不適用	N/A	3 個月	是	不適用
B1 業務	清單建檔作業	清單	5,000-50,000	1-500	1-5	不適用	N/A	99 年	是	不適用
B1 業務	清單建檔作業	專案資料庫	5,000-50,000	1-500	1-5	不適用	N/A	99 年	是	不適用
B1 業務	專案資料異動作業	專案資料	5,000-50,000	1-500	1-5	不適用	N/A	30 年	是	不適用
B1 業務	專案提前作業	專案提前資料	5,000-50,000	1-500	1-5	不適用	N/A	30 年	是	不適用
B1 業務	專案展延作業	專案展延資料	1-500	1-500	1-5	不適用	N/A	30 年	是	不適用
B1 業務	專案催收作業	專案催收資料	500-5,000	1-500	1-5	不適用	N/A	30 年	是	不適用

資料來源：本計畫整理

表48 B1 業務－BA 單位個資項目盤點表(2)

個人資料檔案名稱	如何確認個資內容之正確性？	除執行業務外，是否利用所蒐集之個資進行資料搜尋、分析或統計等用途?	前項問題之回應若為是，這些活動是否已告知當事人?	當事人是否具有同意、拒絕提供個資之權利？	當事人是否具有隨時要求停止蒐集、處理或利用該個資之權利？	於個資蒐集之初是否告知當事人得利用個資之利害關係方與其利用方式等資訊？	是否限制利害相關方利用個資之方式與禁止其從事與原訂利用方式無關之活動？	是否有方式提供當事人查詢或請求閱覽個資或製給複製本？	是否有方式提供當事人更正或補充其個資？	是否定期審視或稽核以確保個資之蒐集、利用及處理皆遵循已訂定之管理規範？
報送清單	0. 無確認	否	不適用	不適用	不適用	不適用	不適用	不適用	不適用	是
清單電子檔	0. 無確認	否	不適用	不適用	不適用	不適用	不適用	不適用	不適用	是
清單	0. 無確認	否	不適用	不適用	不適用	不適用	不適用	不適用	不適用	是
專案資料庫	0. 無確認	否	不適用	不適用	不適用	不適用	不適用	不適用	不適用	是
專案資料	3. 與其他來源進行交叉比對	否	不適用	不適用	不適用	不適用	不適用	不適用	不適用	是
專案提前資料	3. 與其他來源進行交叉比對	否	不適用	不適用	不適用	不適用	不適用	不適用	不適用	是
專案展延資料	3. 與其他來源進行交叉比對	否	不適用	不適用	不適用	不適用	不適用	不適用	不適用	是
專案催收資料	3. 與其他來源進行交叉比對	否	不適用	不適用	不適用	不適用	不適用	不適用	不適用	是

資料來源：本計畫整理

表49 B1 業務－BB 單位個資項目盤點表(1)

服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	目前保有多少數量(筆數)的個人資料？	每年大約會處理多少數量(筆數)的個人資料？	每筆資料中包含的個人資料欄位數量為多少？	於蒐集個資前是否主動公告其所依循之法源、機構或合約?	法定保存期限	自定保存期限	於執行個資蒐集相關業務/專案前是否已完成系統安全計畫？	是否透過商業廣告方式取得或使用已公開之個資？
B1 業務	專案提前申報作業	專案提前檔案	5,000-50,000	5,000-50,000	1-5	不適用	N/A	N/A	是	不適用
B1 業務	產生資料明細	資料計算明細檔案	5,000-50,000	5,000-50,000	1-5	不適用	N/A	N/A	是	不適用
B1 業務	申報資料	資料計算明細表	5,000-50,000	5,000-50,000	1-5	不適用	N/A	99 年	是	不適用
B1 業務	資料審核作業	資料庫	5,000-50,000	5,000-50,000	1-5	不適用	N/A	99 年	是	不適用

資料來源：本計畫整理

表50 B1 業務－BB 單位個資項目盤點表(2)

個人資料檔案名稱	如何確認個資內容之正確性？	除執行業務外，是否利用所蒐集之個資進行資料搜尋、分析或統計等用途?	前項問題之回應若為是，這些活動是否已告知當事人?	當事人是否具有同意、拒絕提供個資之權利？	當事人是否具有隨時要求停止蒐集、處理或利用該個資之權利？	於個資蒐集之初是否告知當事人得利用個資之利害關係方與其利用方式等資訊？	是否限制利害相關方利用個資之方式與禁止其從事與原訂利用方式無關之活動？	是否有方式提供當事人查詢或請求閱覽個資或製給複製本？	是否有方式提供當事人更正或補充其個資？	是否定期審視或稽核以確保個資之蒐集、利用及處理皆遵循已訂定之管理規範？
專案提前檔案	3. 與其他來源進行交叉比對	否	不適用	不適用	不適用	不適用	不適用	不適用	不適用	是
資料計算明細檔案		否	不適用	不適用	不適用	不適用	不適用	不適用	不適用	是
資料計算明細表		否	不適用	不適用	不適用	不適用	不適用	不適用	不適用	是
資料庫	3. 與其他來源進行交叉比對	否	不適用	不適用	不適用	不適用	不適用	不適用	不適用	是

資料來源：本計畫整理

表51 個案 B 個資風險等級基準值

參考項目	個資風險等級		
	普	中	高
含有個資類別	**1.僅公務用聯絡資料，如公務用聯絡電話、傳真、E-mail 等 2.一般個資僅含姓名與聯絡方式，筆數不超過 5,000 筆**	**含有一般個資，如姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業等「個人資料保護法」定義之個人資料數量不超過 50,000 筆**	**含有特種個資，如有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個資，或含有一般個資之資料筆數超過 50,000 筆 (含)**
NIST SP800-122「個人可識別資訊機密性保護指引」之衝擊等級判定方式	若個資之機密性、完整性及可用性被破壞時會對本機關組織、資產或人員造成有限的傷害(可能輕微影響本機關聲譽、但不會造成任何財務損失或遭受訴訟之情事)	若個資之機密性、完整性及可用性被破壞時會對本機關組織、資產或人員造成傷害(可能會影響本機關聲譽、財務損失或遭受訴訟，但不至於對本機關業務之持續運作造成重大影響)	若個資之機密性、完整性及可用性被破壞時會對本機關組織、資產或人員造成重大傷害(非常可能嚴重影響本機關聲譽、重大財務損失或重大訴訟，且可能造成本機關主要業務中止)
「資訊系統分類分級與鑑別機制」影響構面與個資項目價值對應	「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信譽」三者影響構面之安全等級皆為普或安全等級為中者不超過一項	「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信譽」三者影響構面的安全等級皆無高，且其中二項安全等級為中	「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信譽」三者影響構面之安全等級皆為中，或「資料保護受到損害」、「影響法律規章遵循」、「損害本機關信譽」三者影響構面之其中一項安全等級為高者

資料來源：本計畫整理

本專案B1 業務負責人針對所擁有個資項目的機密性、完整性及可用性等構面向，依前置作業所擬之個資風險等級基準值(詳見表 51)，進行個資風險評估作業，以瞭解個資項目之風險等級，做為後續擬訂安全控制措施之依據，經彙整相關個資衝擊分析結果採最高原則，評定結果本業務風險等級為「中」詳見表 52~表 53。

表52 B1 業務－BA 單位風險評估表

服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	含有個資類別	NIST SP800-122「個人可識別資訊機密性保護指引」之衝擊等級判定方式	「資訊系統分類分級與鑑別機制」影響構面與個資項目價值對應	風險等級
B1 業務	清單報送作業	報送清單	中	中	中	中
B1 業務	清單報送作業	清單電子檔	中	中	中	中
B1 業務	清單建檔作業	清單	中	中	中	中
B1 業務	清單建檔作業	專案資料庫	中	中	中	中
B1 業務	專案資料異動作業	專案資料	中	中	中	中
B1 業務	專案提前作業	專案提前資料	中	中	中	中
B1 業務	專案展延作業	專案展延資料	中	中	中	中
B1 業務	專案催收作業	專案催收資料	中	中	中	中

資料來源：本計畫整理

表53 B1 業務－BB 單位風險評估表

服務目錄或流程名稱	子流程名稱	個人資料檔案名稱	含有個資類別	NIST SP800-122「個人可識別資訊機密性保護指引」之衝擊等級判定方式	「資訊系統分類分級與鑑別機制」影響構面與個資項目價值對應	風險等級
B1 業務	專案提前申報作業	專案提前檔案	中	中	中	中
B1 業務	產生資料明細	資料計算明細檔案	中	中	中	中
B1 業務	申報資料	資料計算明細表	中	中	中	中
B1 業務	資料審核作業	資料庫	中	中	中	中

資料來源：本計畫整理

4.3.5. 安全控制措施選取

本專案技術安全控制措施採用個資項目技術安全控制措施基準值評估表(詳見附件 3_個資項目技術安全控制措施基準值評估表)，B1 業務之個資項目其檔案格式有紙本與電子檔案 2 種,BA 單位紙本檔案包含報送清單、清單、專案資料、專案提前資料、專案展延資料及專案催收資料，所需安全維護相同且風險安全等級相同，故該 6 個資項目之安全控制措施整併為同一表格。BA 單位電子檔案包含清單電子檔(磁片)與專案資料庫，其風險安全等級相同，故該 2 個資項目之安全控制措施整併為同一表格。BB 單位紙本僅有資料計算明細表，故其安全控制措施表格只含一項個資項目。BB 單位電

子檔包含專案提前檔案、資料計算明細檔案及資料庫，其風險安全等級相同，故該 3 個資項目之安全控制措施整併為同一表格。

經業務負責人先行選取所需安全控制措施，再由導入顧問協助完成紙本與電子檔案安全控制措施選取，詳見附件 20_BA 單位－個資項目技術安全控制措施基準值評估表(紙本)~附件 23_BB 單位－個資項目技術安全控制措施基準值評估表(電子檔)。

4.3.6. 個資人員權責角色

在處理個資時，需確認組織內外及相關人員之權責角色，並依照其權責給予所應具備之權限，在發生個資事故時，便可儘速釐清可能洩露之管道。

確立人員權責角色之任務，包括識別個資管理相關人員或群組角色、建立個資項目生命週期活動與個資管理角色之對應表、識別對應表內個資管理角色細部權責定義需求、完成人員權責角色定義及轉換個資管理人員權責角色定義至相關應用系統權限定義。

BA 單位所擁有之專案資料庫於設計之初，即依人員權責角色規劃其使用權限，目前僅有 BA 單位與 BB 單位承辦人擁有其執行權限，詳見表 54。

BB 單位所擁有之資料庫於設計之初，即依人員權責角色規劃其使用權限，再依相關作業人員所擔任任務賦予作業人員權責。目前擁有其使用權限包含經辦人員、彙總人員及系統管理者，其權限分配詳見表 55。

表54 專案資料庫個資項目個資管理角色對應表

個資管理角色 / 個人資料檔案	BA 單位承辦人					BB 單位承辦人				
	新增	查詢	修改	列印	刪除	新增	查詢	修改	列印	刪除
專案資料庫	■	■	■	■	■	□	■	□	□	□

資料來源：本計畫整理

表55 資料庫使用者權限

系統使用者	授權作業	備註
經辦人員	申報資料入檔 產生下個月份明細 明細查詢及列印 例外處理 資料查詢 產生彙總資料 檔案更改	每位經辦人員僅能處理自己負責之機構資料。 (每一家機構,僅授權一位經辦人員可處理左列之各項作業)
彙總人員	資料維護 機構資料維護 彙總表 金鑰更新紀錄	彙總人員未涉及個資 依規定金鑰至少每5年應更換一次，更新電腦亦須重新產生金鑰
系統管理者	系統使用者資料維護	僅能維護系統使用者權限

資料來源：本計畫整理

4.3.7. 建立個資管理程序

組織於業務作業需求蒐集個資時，應訂定個資蒐集作業流程，確認個資蒐集符合特定目的，同時設計個資同意書範本，以利於蒐集個資時使用。於蒐集資料之流程中，檢視所涉及之管理作業流程與程序書，符合組織之個資保護政策，修定相關文件資料內容。本階段之管理重點為清楚的管理權責定義、依據法令與流程進行個資分類及落實公開與告知等隱私管理原則。

建立個資管理程序之任務，包括設計個資生命週期作業流程、設計個資事故管理作業流程、設計個資管理稽核作業流程及修訂組織內部管理制度文件。

鑒於個人資料保護法於 101 年 10 月 1 日正式施行,個案 B 頒布個案 B 個人資料保護管理要點詳見附件 24_個案 B 個人資料保護管理要點，同時修定個案 B 資訊業務處理規範，訂定個資事故通報暨處理作業程序草案，以及個案 B 委託辦理資料處理資訊安全約定事項等個人資料保護相關規定。導入顧問說明個人資料之蒐集、處理、利用及傳輸標準作業程序、委外作業管理、稽核計畫及個資通報應變應注意事項。委外作業管理內容請參考 4.3.8，稽核計畫與個資通報應變相關表單詳見附件 12_資安事故通報與紀錄表範例~附件 15_稽核紀錄範例。

除說明個資管理相關程序外,同時協助檢視現行個資管理文件請參考表 56，並建議個資相關管理文件宜與現行管理文件結合，以利同仁使用。

表56 個資管理文件檢視建議

文件名稱	建議事項
個案 B 資訊業務處理規範	1.個資紙本與電子檔之儲存、傳輸、刪除及銷毀作業，分散於資訊業務處理規範中，可考量增加個資處理作業對照表，以利同仁使用，或加強相關教育訓練 2.資料交換或傳輸原則訂定「不得用電子郵件傳送個人資料或其他機敏資料。但法令或主管機關另有規定者，依其規定。」，但現行業務有個資傳輸需求，宜考量調整相關規範 3.委外處理宜增加對委外廠商之作業要求，包含教育訓練、通報應變、稽核及個資處理 4.於資訊安全管理制度之內部查核中，增加個資稽核人員資格；如 BS 10012 個人資料管理系統主導稽核員課程或其他個人資料保護相關課程
個資事故通報暨處理作業程序(草案)	宜考量是否需建立個資事故通報等級與限制通報時間
個案 B 委託辦理資料處理資訊安全約定事項	1.於資訊系統使用之權限管理，應保留存取紀錄 2.系統測試使用資料，避免使用正式資料，若需使用應具保護措施 3.承包廠商應建立資通安全事件及個資事故之通報應變處理程序及管道。 4.於發生個人資料事故經查明後，應以適當方式儘速通知本行並討論通知當事人之方式

資料來源：本計畫整理

4.3.8. 委外作業管理

委外作業雖是由外部第三方執行，但仍需符合組織個資防護要求，故於委外作業流程中，應檢視並要求第三方於處理個資作業時，必須具備個資安

全保護措施，同時保留稽核之權利，故於導入期間由導入顧問說明機關個資系統委外時，應於委外需求說明書中增列個資需求說明如后：

- 承包廠商應建立隱私保護政策，承包廠商與承包廠商人員應遵循本機關的隱私權政策、個人資料保護與管理辦法、及相關個人資料保護與管理要求，承包廠商與承包廠商人員，應對本專案相關個人資料檔案負保護與管理責任，並符合個人資料保護法等相關法規命令要求。

- 承包廠商須提供參與本案人員個人資料保護與管理教育訓練，並舉行測驗，教育訓練內容須包括人員對個人資料保護的認知，個人資料檔案蒐集、處理及利用的作業要求等，教育訓練內容及測驗卷送本機關備查。

- 未經本機關事先書面同意，承包廠商不得將本專案相關個人資料檔案攜出履約地點。若有事先經本機關書面允許之情形，承包廠商應於本專案終止前將相關個人資料檔案交還本機關，同時承包廠商不得對任何交還之個人資料檔案進行複印、複製、攝錄影及拍照等各式保存行為。

- 承包廠商應建立個資事故之正式通報程序及管道，並訂定通報後應採行之處理措施，如相關個人資料遭受侵害時，承包廠商應依事前訂定之通報管道立即通報本機關。

- 本機關於本專案有效期間暨專案合約正式終止後一年內，得不定期至承包廠商場所稽核其對於本專案相關個人資料蒐集、處理及利用情形，以防個人資料外洩或遭受侵害，確保個人資料保護與管理之要求。

4.4.「結案」

本專案依導入實施步驟，執行開始、文件導讀、指引導入及結案 4 階段導入步驟，有關專案導入時程對照關係詳見表 57，其執行成果說明如后:

表57 專案時程對照表

項次	作業項目	預定時程	實際時程
1(一)	啟動會議	101 年 11 月 1 日	101 年 11 月 1 日
2(二)	文件導讀	101 年 11 月 14 日	101 年 11 月 14 日
3(三)	個資項目盤點與討論	101 年 11 月 21 日	101 年 11 月 21 日
4(三)	個資項目盤點與討論 個資衝擊分析	101 年 11 月 28 日	101 年 11 月 28 日
5(三)	第一次專案管理會議 個資衝擊分析 個資風險評估	101 年 12 月 5 日	101 年 12 月 5 日
6(三)	個資風險評估	101 年 12 月 12 日	101 年 12 月 12 日 調整為安全控制措施選取
7(三)	安全控制措施選取 確立人員權責角色	101 年 12 月 26 日	101 年 12 月 26 日
8(三)	第二次專案管理會議 建立個資管理程序	102 年 1 月 2 日	102 年 1 月 2 日
9(三)	建立個資管理程序	102 年 1 月 9 日	102 年 1 月 9 日
10(四)	整體建議	102 年 1 月 16 日	102 年 1 月 23 日
11(四)	結案	102 年 1 月 23 日	102 年 1 月 31 日

資料來源：本計畫整理

- 個案 B 依遴選之「B1 業務」，盤點出 BA 單位 8 項個資項目，BB 單位 4 項個資項目。
- 依據盤點之個資項目，填寫相關個資內容，包含 5 項個人資料檔案基本資訊、5 項利害關係人、21 項個人資料欄位、10 項個人資料檔案生命週期活動。
- 執行 18 項隱私衝擊分析。

●依照個資風險評估基準表執行三個類別之風險評估，包含個資類別、NIST SP800-122「個人可識別資訊機密性保護指引」之衝擊等級判定方式，以及「資訊系統分類分級與鑑別機制」影響構面與個資項目價值對應之風險評估；個案 B 並據此建立個資風險評估基準表詳見表 51。

●執行安全控制措施檢視

– BA 單位電子檔(65 項)：清單電子檔、專案資料庫。

– BA 單位紙本(12 項)：報送清單、清單、專案資料、專案提前資料、專案展延資料及專案催收資料。

– BB 單位電子檔(65 項)：專案提前檔案、資料計算明細檔案及資料庫。

– BB 單位紙本(12 項)：資料計算明細表。

●檢視個資相關管理文件 4 份，除個案 B 個人資料保護管理要點撰寫內容完整不供建議事項外，另三份管理文件建議事項，詳見表 56：

– 個案 B 個人資料保護管理要點。

– 個案 B 資訊業務處理規範。

– 個資事故通報暨處理作業程序(草案)。

– 個案 B 委託辦理資料處理資訊安全約定事項。

本案於導入完成後，邀請個案 B 全體參與人員，針對參考指引之內容與導入方法，提供導入意見並進行彙整，於結案會議中說明，結案簡報詳見附件 25_個案 B 導入結案會議簡報。

5. 改善建議

延續前章發現，個案 A 與個案 B 對於「個人資料保護參考指引」的使用上，提出改善的需求，而導入顧問在協助導入過程中也蒐集了此指引在實作中所面臨的問題。因此，在本章將彙集整體改善建議，做為指引之修訂方向參考。

5.1.個案 A 改善建議

5.1.1. 修正安全控制措施基準表

●風險等級宜與機敏等級相匹配

安全控制措施基準表 48 項係針對風險等級「普」，與控制措施說明「機敏等級為高之系統使用者身分認證是否已採二元識別」不匹配，因機敏等級「高」之系統風險等級不宜為「普」。

●安全控制措施基準表適用角色

安全控制措施基準表中，雖已區分紙本與電子檔案所需安全控制措施，惟部分控制措施係屬伺服器系統工程師範疇，一般應用系統負責人對該等控制措施無法充分了解，宜予區分。

5.1.2. 修正稽核查核表

稽核查核表第 32、36 及 37 項內容「參照 ISMS 相關要求辦理」，建議修正為「參照 ISMS 相關要求或行政院主計總處資通安全外部稽核表辦理」，俾利未通過 ISMS 管理機制之機關有參酌依據。

5.2.個案 B 改善建議

●啟動與結案會議應為管理會議，管理會議以每月為原則。

●隱私衝擊分析檢核表建議更名為法律遵循性檢核表。

●作業流程之方塊應編號並有對應說明。

●個資相關人員可分為治理/行政/管理/業務/技術等類或層次。

●可將蒐集/利用(較偏人工作業)歸為一類，處理：輸入/處理/輸出/儲存/傳輸(較偏電腦作業)另歸一類。

●含有個資類別之風險評估基準值為「普」內容，應刪除未具有任何個資之說明內容。

●可提供參考指引導入摺頁，提綱挈領有助瞭解。

●個資保護制度或程序，應融入各單位標準作業程序。

●建立個資保護參考指引導入所需成本估計模式。

5.3.導入顧問改善建議

5.3.1. 建議刪除無再使用資料，以降低風險

A1 系統風險等級「高」，主要原因為資料量太大，其中結案資料於結案後已無運用需求，若將該等資料刪除，則可大量降低系統資料量，亦可降低風險等級。該系統負責人於導入期間即依導入顧問建議刪除該系統已結案資料，刪除比率高達 91%，詳見表 58。

表58 A1 系統結案資料比較表

年度	資料量	刪除結案後資料量	刪除量	刪除率
97 年	156,362	19,206	137,156	87.72%
98 年	168,436	18,070	150,366	89.27%
99 年	195,107	17,614	177,493	90.97%
100 年	225,426	18,310	207,116	91.88%
101 年	231,027	16,033	214,994	93.06%
合計	976,358	89,233	887,125	90.86%

資料來源：本計畫整理

5.3.2. 建議以資料流程圖(DFD)，盤點個資檔案

個資盤點建議採先畫出資訊系統作業流程圖，再依系統作業流程圖繪製資料流程圖(DFD)，即可找出所有檔案資料，再依其是否含有個資，盤點出含個資之檔案。

本專案係採以作業流程分析方式盤點個資項目，導入時先由系統負責人自行依作業流程盤點出個資項目(詳見表 22)，經導入顧問以訪談方式瞭解作業流程後，以先繪製系統作業流程圖(詳見圖 13~圖 14)，再據以繪製資料流程圖(DFD) (詳見圖 15~圖 17)，找出所有檔案資料(詳見表 23)，再依其是否含有個資，盤點出含個資項目，差異詳見表 59。

表59 個資項目差異表

個人資料檔案名稱	作業流程分析導出	資料流程圖導出
欠費資料檔		V
平信催繳檔	V	V
平信催繳單	V	V
結案資料檔		V
未繳資料檔		V
掛號催繳檔		V
掛號催繳單		V

資料來源：本計畫整理

另公務機關人員常有異動,難免會將前一職務所處理資料帶到新職務場所，個資項目盤點時，僅以目前作業流程分析檢討個資項目，而遺漏前一職務之資料,建議機關於盤點個資項目時,可考量輔以使用市售個資盤點工具。

5.3.3. 檢討保留所需欄位

A1 系統結案檔建議僅保留未來查詢所需之車號、停車日期及結案日期等欄位，此等欄位不具個資，即可排除為個資檔案，且在資訊系統風險評鑑中亦可降低其風險等級。

5.3.4. 安全控制措施

安全控制措施宜強化個資等級分類與標示。

5.3.5. 個資管理相關程序

●訂定個資蒐集與利用作業程序。

●增列個資盤點與風險評估方式，於現行作業規範或程序中。

●訂定個資內部查核資格。

●增加個資委外業務之要求。

●加強個資管理教育訓練。

6. 結論

個案 A 於本專案執行期間計 13 個單位 20 人全程參與，且參與人員於導入期間皆依各階段就其所負責系統完成各項表單，並提供建議，顯見該機關對個資之重視。

個案 B 於本專案執行期間計 13 個單位 23 人參與，主要參與人員為 BA 單位與 BB 單位負責 B1 業務人員，於導入期間依各階段完成各項表單，並提供建議，顯見該機關對個資之重視。

本次試行作業，個案 A 與 B 均認為具有高度的可操作性，除可與現有 ISMS 管理機制相結合外，更可藉由衝繫分析的作業，瞭解機關個資法遵循性的符合情形。對機關的個人資料保護，提供有效的執行方法，同時也強化機關人員對個人資料保護的整體認知。個案 B 更建議未來可考量製作參考指引導入摺頁，協助機關提綱挈領，加速導入執行效率。

其他有關本次試行專案建議事項，綜整如后：

6.1.參考指引修訂

個案 A 與個案 B 於導入期間對參考指引內容所作建議，宜納入後續個人資料保護參考指引修訂參考。

6.2.建立個資管理程序

個人資料保護法已於 101 年 10 月 1 日正式實施，各機關皆已陸續發展相關作業要點與作業程序，其中除作業要點外，應優先完成下列作業程序，俾利相關機關相關單位遵循。

- 個人資料之蒐集、處理、利用及傳輸標準作業程序。
- 個人資料之應變處理程序。

●個人資料之內部檢查、稽核規定。

●個人資料委外監督管理程序。

●個人資料內部人員教育訓練規定。

6.3.個資項目盤點方法

個資項目盤點如業務承辦人對業務熟稔可採作業流程分析方法外，建議可採繪製資料流程圖方式辦理，惟業務單位對資料流程圖繪製不熟，資訊單位宜採訪談方式瞭解作業流程後，協助繪製資料流程圖。另機關亦可輔以市售個資盤點工具清查個資項目，俾利個資盤點更趨完整。

6.4.清除不再使用欄位或資料

系統負責人於資料建立時應檢討作業所需資料，避免過度蒐集。資料運用完成後應檢討刪除不再使用之資料或欄位，以降低資料遺漏時所可能造成之損害。

7. 參考文獻

[1] 行政院研考會，資訊系統風險評鑑參考指引 V2.0 版。

[2] 行政院國家資通安全會報，資訊系統分類分級與鑑別機制參考手冊，99 年 7 月版。

[3] 行政院研考會，個人資料保護參考指引，100 年版。

[4] 行政院國家資通安全會報，個資保護規劃與實作建議報告，100 年。

[5] 中華民國個人資料保護法，99 年。

[6] 中華民國個人資料保護法施行細則，101 年。

[7] 行政院國家資通安全會報，公務機密資料防護研究期末報告，98 年

[8] Organization for Economic Cooperation and Development (OECD), OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980-09-23.

[9] Asia-Pacific Economic Cooperation (APEC), APEC Privacy Framework, 2005.

[10] BSi, BS 10012:2009, Data protection – Specification for a personal information management system, May 2009.

[11] ISO 22307 Financial services – Privacy impact assessment, 2008-05-01.

[12] Information Commissioner's Office (ico.), Privacy Impact Assessment handbook version 2, June 2009.

[13] National Institute of Standards and Technology (NIST), Special Publication 800-122, Guide to Protecting the Confidentiality of Personal Identifiable Information (PII), April 2010.

[14] National Institute of Standards and Technology (NIST), Special Publication 800-53, Recommended Security Controls for Federal Information Systems (Revision 2), December 2007.

[15] http://www.tecsols.com/index.php/promotional-activities/webcasts/326-protection-of-personal-datanov.

8. 附件

8.1.附件 1_個資項目個資衝擊分析檢核表

8.2.附件 2_個資項目衝擊分析表

8.3.附件 3_個資項目技術安全控制措施基準值評估表

8.4.附件 4_個案 A 保密切結書

8.5.附件 5_個案 A 導入啟動會議簡報

8.6.附件 6_個案 A 導入工作計畫書

8.7.附件 7_個案 A 紙本安全控制措施

8.8.附件 8_個案 A 電子檔安全控制措施

8.9.附件 9_個案 A 個人資料保護管理要點

8.10.附件 10_個人資料之蒐集、處理、利用及傳輸標準作業程序

8.11.附件 11_個人資料之盤點、公開作業程序

8.12.附件 12_資安事故通報與紀錄表範例

8.13.附件 13_稽核計畫範例

8.14.附件 14_稽核查核表範例

8.15.附件 15_稽核紀錄範例

8.16.附件 16_個案 A 導入結案會議簡報

8.17.附件 17_個案 B 保密切結書

8.18.附件 18_個案 B 導入啟動會議簡報

8.19.附件 **19_個案 B 導入工作計畫書**

8.20.附件 **20_BA 單位－個資項目技術安全控制措施基準值評估表(紙本)**

8.21.附件 **21_BA 單位－個資項目技術安全控制措施基準值評估表(電子檔)**

8.22.附件 **22_BB 單位－個資項目技術安全控制措施基準值評估表(紙本)**

8.23.附件 **23_BB 單位－個資項目技術安全控制措施基準值評估表(電子檔)**

8.24.附件 **24_個案 B 個人資料保護管理要點**

8.25.附件 **25_個案 B 導入結案會議簡報**