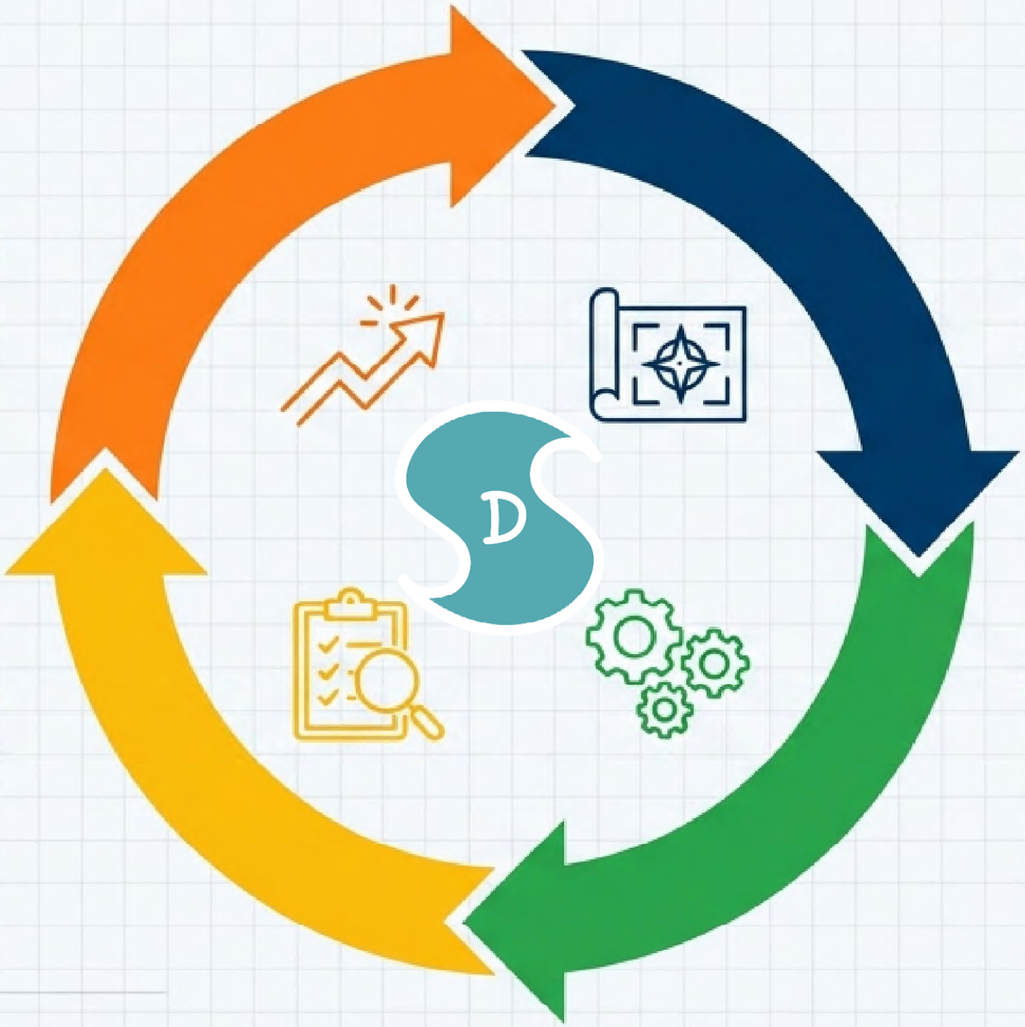
擘劃隱私保護藍圖：您的 ISO 27701 個資管理制度 (PIMS) 實施指南

一份從策略規劃到持續卓越的行動手冊

策略數位服務有限公司
Strategy Digital Service Ltd

我們的旅程：一個持續進化的策略循環

本指南將引導您走過建立世界級 PIMS 的四個關鍵階段。此方法論基於全球公認的 PDCA (規劃-執行-檢查-行動) 管理循環，確保您的隱私保護制度不僅健全，更能持續進化。



規劃 PLAN
- 奠定基礎

執行 DO
- 建立系統

檢查 CHECK
- 監督審查

行動 ACT
- 持續優化

建立信任的基石：什麼是 PIMS？

定義 (Definition)

隱私資訊管理系統 (PIMS) 是一套系統性的方法，用於管理與保護個人資料。它整合了政策、流程、控制措施與技術，以系統化方式降低隱私風險。

標準與框架 (Standards & Frameworks)

我們的導入程序與國際及本地標準完全對齊，確保符合性與最佳實踐。

- ISO 27701
- ISO 27001 / ISO 27002
- ISO 29151
- TPIPAS (台灣個人資料保護與管理制度)
- BS 10012

第一階段：奠定基礎 (PLAN)

擘劃您的隱私保護策略藍圖

策略定錨：確立方向與範疇

高層承諾 (Top Management Commitment)

取得最高管理階層的明確支持，並確保提供專案成功所需的資源（人力、預算、時間）。這是所有工作的起點。

政策制定 (Policy Formulation)

制定組織層級的總體隱私保護政策。此政策應闡明組織對保護個人資料的承諾、目標與指導原則。

符合性評估 (Compliance Assessment)

深入了解並評估組織需遵守的所有相關法規，例如 GDPR、台灣個資法等，鑑別法律與合約要求。

深度剖析：盤點資料與評估風險

現況分析與個資盤點 (Current State Analysis & PII Inventory)

全面辨識組織內所有個人資料的種類、來源、儲存位置、處理流程與流向，建立完整的資料清冊 (Data Inventory)。

風險評鑑作業 (Risk Assessment Operation)

根據盤點結果，識別與個人資料相關的潛在隱私風險與威脅（例如：未經同意蒐集、資料外洩、不當中介傳輸）。

建立職責 (Assigning Responsibilities)

指派專責人員或資料保護官 (DPO)，明確定義其在 PIMS 中的角色、責任與權限。

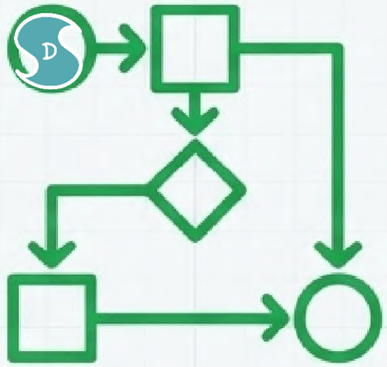
第二階段：建立系統 (DO)

將藍圖化為具體組織行動

構築防線：部署控制措施與作業流程

建立控制措施 (Establish Controls)

依據 ISO 27701 指引與風險評估結結果，設計並導入具體的技術與組織措施，如存取控制、加密、個資最小化、營運持續管理等。



個人資料處理流程 (Define PII Processing Procedures)

針對個資的收集、使用、儲存、揭露至刪除的完整生命週期，建立標準化、合規的處理程序。

四階文件撰寫及建立 (Level-4 Documentation)

建立支持 PIMS 運作的完整文件體系，包括政策、程序書、作業指導書與表單紀錄，確保作業一致性。

全員賦能：深化隱私保護意識

主題：資安教育訓練與宣導 (Security Education, Training, and Awareness)

核心目標 (Core Objective)

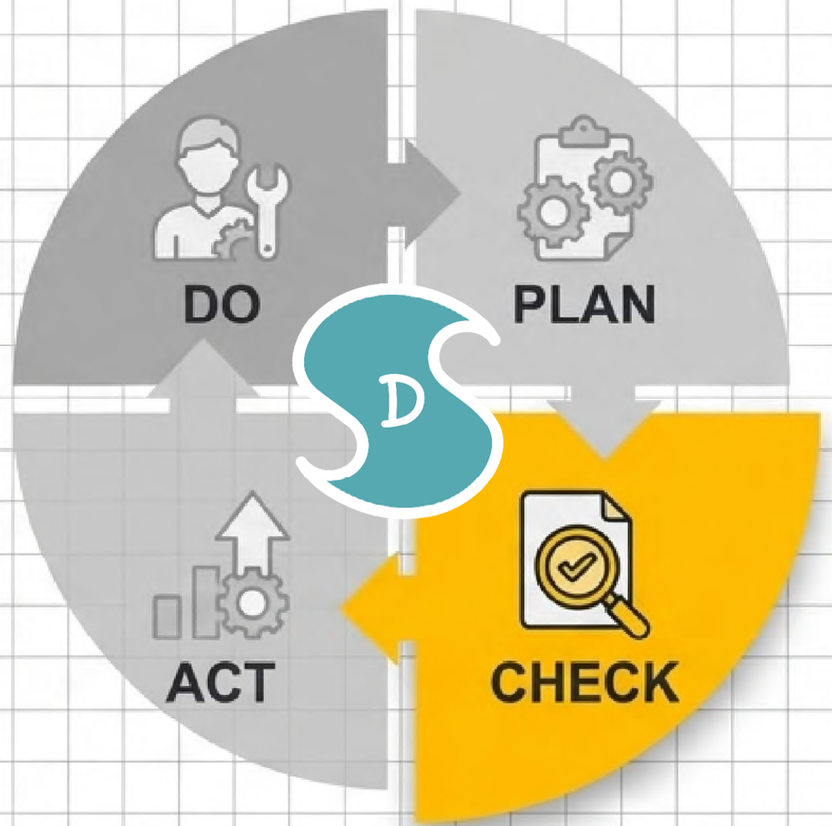
確保組織內所有相關人員，特別是接觸個資的員工，都了解隱私政策、其崗位職責以及不遵循規範的後果。

執行重點 (Key Actions)

- 針對不同角色設計客製化訓練內容。
- 定期舉辦意識提升活動。
- 驗證訓練成效。

第三階段：監督審查 (CHECK)

衡量成效與鑑別改善機會



驗證有效性：內部檢視與管理層審查

內部稽核作業 (Internal Audit Operation)

目的 (Purpose)

定期且獨立地檢查 PIMS 的實施情況是否符合政策、標準與法規要求。

產出 (Output)

稽核報告，詳述符合事項、不符合事項與改善建議。

管理審查作業 (Management Review Operation)

目的 (Purpose)

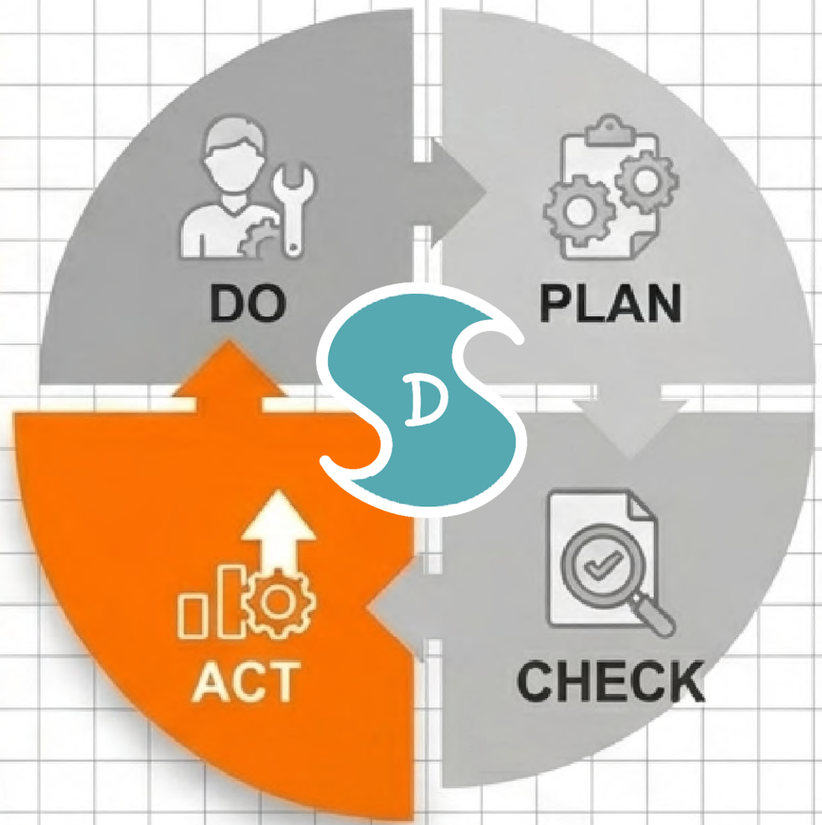
由最高管理階層定期審視 PIMS 的整體績效，包括稽核結果、風險狀態、資源適當性等。

產出 (Output)

決定 PIMS 未來的方向、資源投入與改進目標。

第四階段：持續優化 (ACT)

邁向卓越並取得外部認證



採取行動：從改善到認證

持續改進 (Continuous Improvement)

根據內部稽核、管理審查與事件經驗，採取矯正與預防措施，不斷優化 PIMS 的流程與控制措施。

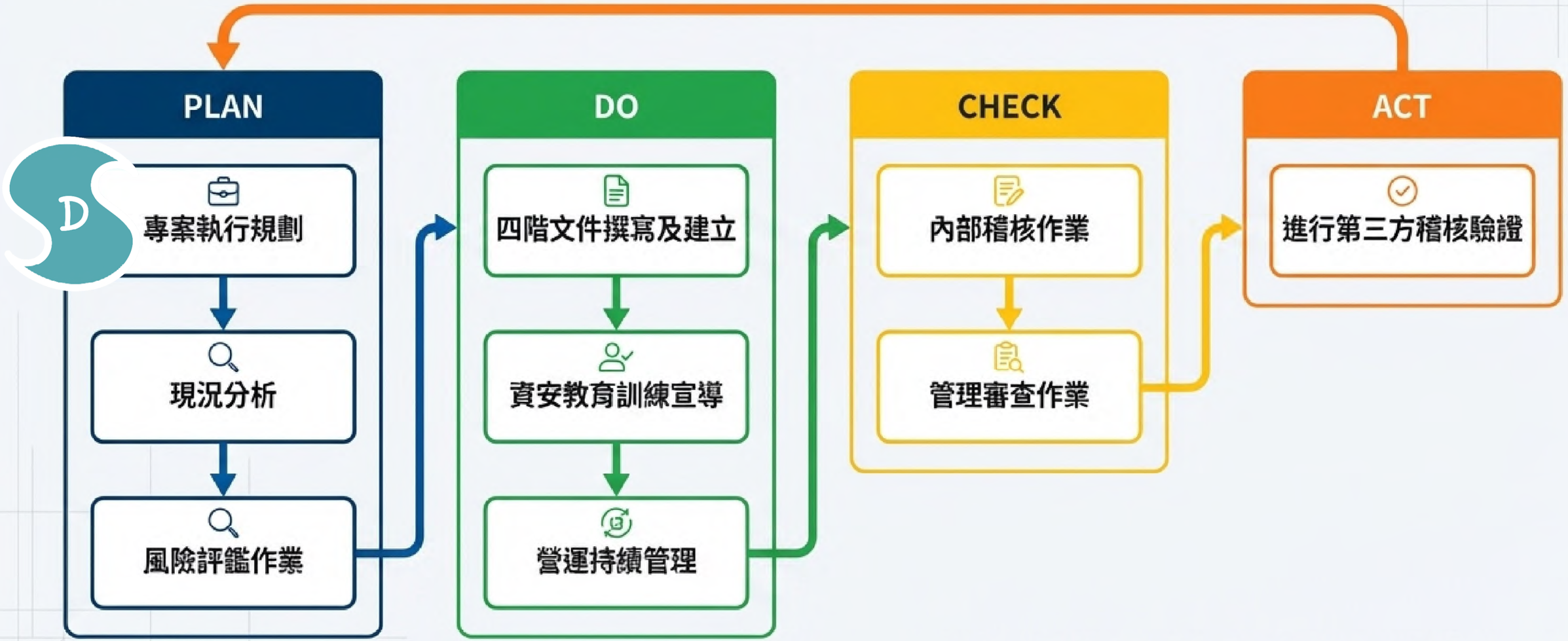
事故應變計畫 (Incident Response Plan)

建立並演練個資外洩等安全事件的應變與個資外洩等安全事件的應變與通報程序，確保能快速、有效地應對危機，降低損害。

進行第三方稽核驗證 (Third-Party Audit & Certification)

接受如 TPIPAS 或 ISO 27701 的外部獨立稽核，以取得正式認證，向客戶與合作夥伴證明您的隱私承諾。

PIMS 導入程序總覽：一個整合性的行動藍圖



PIMS 不只是一項專案，它是對信任的持續承諾。

一個健全的隱私資訊管理系統，是您在數位時代中建立客戶信任、確保業務韌性、並創造永續競爭優勢的關鍵。