本公司輔導導入
資訊安全管理制度 (ISO 27001)
ISMS 簡易程序

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

旅程的終點：為何我們需要資訊安全管理制度 (ISMS)？

ISMS 的核心目標是建立一個系統化的管理架構，以系統性地保護組織的資訊資產。

ISO 27001 不僅是認證，更是組織達成此目標的國際通用語言與最佳實踐藍圖。

我們信賴的地圖：PDCA 持續改善循環

P (Plan) 計畫:
擘劃藍圖，設定方向。

D (Do) 執行:
依循藍圖，穩健前行。

C (Check) 檢查:
校準方位，衡量進度。

A (Act) 行動:
調整步伐，持續精進。

第一階段：計畫 (Plan) - 劃定邊界與擘劃路徑

1. 了解與準備
學習 ISO 27001 標準精神與要求，建立共識。

2. 現況分析 (本公司導入重點)
深入了解您現有的流程與資源，找出差距。

3. 界定範圍
精準確定 ISMS 的保護邊界（例如：特定部門、核心服務）。

4. 建立資安政策與目標
制定總體安全政策，並設定具體、可衡量的目標。

計畫的核心：識別路途中的挑戰與險阻 (風險評鑑)

風險評鑑是 ISMS 的基石，目的是系統性地識別、分析及評估潛在威脅。

關鍵步驟 (Key Steps)

步驟一：識別資訊資產 -
盤點所有需要保護的關鍵資訊。

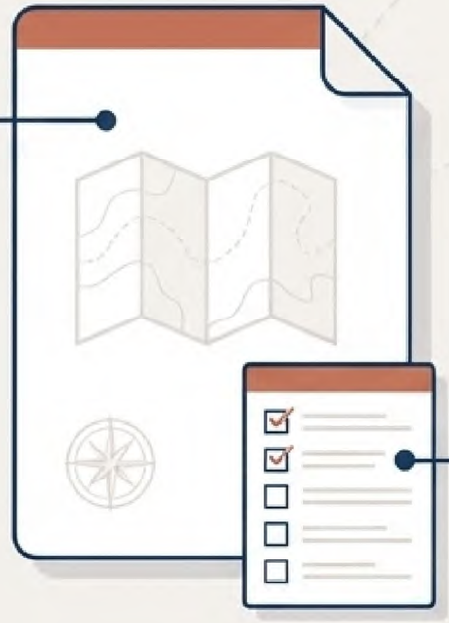
步驟二：分析威脅與弱點 -
找出可能危害資產的內外部威脅與自身弱點。

步驟三：評估風險等級 -
結合衝擊與可能性，量化風險高低。

關鍵產出 (Key Outputs)

風險處理計畫

針對不可接受的風險，決定規避、轉移、降低或接受的策略。



適用性聲明 (SoA)

依據風險評估結果，從 Annex A 中選定合適的控制措施，作為執行的依據。

第二階段：執行 (Do) - 依循藍圖，構築防禦工事

建立並實施 ISMS

根據計畫，導入 Annex A 控制措施與管理程序（如：存取控制、資產管理）。

資源與能力建構

- 確保所需資源到位。
- 進行全員資訊安全意識與技能培訓，讓每個人都成為防線的一份子。

系統化文件管理 本公司導入重點

系統文件導入與資源，請問單、資訊概念、規劃、信件控制、執行管理。

系統化文件管理 本公司導入重點

協助進行**四階文件撰寫**，建立清晰、實用的管理文件與紀錄，確保制度可以落地執行。

執行的深化：建立危機下的營運韌性（營運持續管理）

真正的安全，是在意外發生時仍能持續運作。營運持續管理 (BCM) 是 ISMS 中確保核心業務不中斷的關鍵實踐。

本公司輔導重點

業務衝擊分析 (BIA)

識別關鍵業務流程及其對營運的衝擊。

本公司輔導重點

復原策略擬定

制定在不同災難情境下的應變及復原計畫。

本公司輔導重點

演練與測試

定期演練計畫，確保其有效性與可行性。

價值：將資訊安全從成本中心轉變為支撐組織永續經營的策略性投資。

第三階段：檢查 (Check) - 校準方位，確保航向正確

透過系統性的檢查，驗證 ISMS 是否如預期般有效運行。

1. 監控與量測

持續監控 ISMS 運行狀況，追蹤資安目標的達成率。

2. 內部稽核作業

由受過訓練的內部稽核員定期執行稽核，從客觀角度找出系統與標準準要求的符合性及潛在改善機會。

3. 管理審查作業

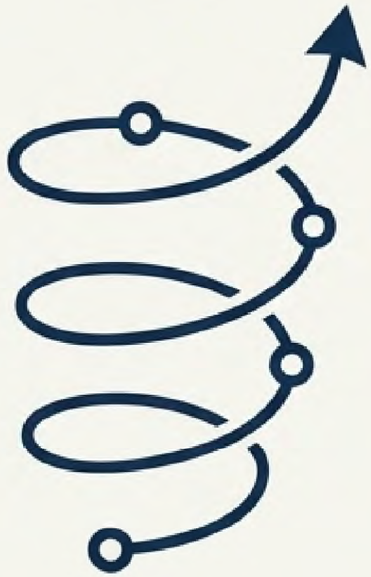
由高階管理者定期審查 ISMS 的整體績效，確保其與組織策略目標保持一致，並做出資源投入的決策。

第四階段：行動 (Act) - 調整步伐，邁向卓越

將檢查階段的發現，轉化為具體的改進動力。

矯正與預防

- 針對稽核發現的缺失或不符合事項，進行根本原因分析並執行有效的**矯正措施**。
- 主動識別潛在問題，採取**預防措施**，防患於未然。



持續改善

- 基於管理審查與稽核結果，不斷優化 ISMS 政策、流程與控制措施。
- 這確保了您的 ISMS 是一個能夠適應變化的「活系統」。

攀登頂峰：第三方驗證與認證流程

本公司將全程陪同，確保流程順暢。

1. 準備就緒

完成內部 ISMS 的建置、文件化，並至少完成一次完整的內部稽核與管理審查。

2. 第一階段稽核 (文件審查)

驗證機構 (CB) 審查您的 ISMS 文件是否符合 ISO 27001 標準要求。

3. 第二階段稽核 (實地審查)

驗證機構派員至現場，確認文件化的制度是否在組織內被確實執行。

4. 改善與發證

針對稽核發現的缺失完成改善後，由驗證機構正式建議發證，取得 ISO 27001 證書。

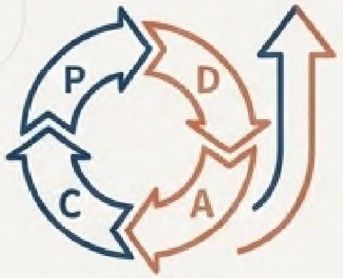
我們的承諾：將標準流程轉化為您的成功實踐

PDCA 標準流程		本公司輔導導入服務
	Plan（計畫）	現況分析 風險評鑑作業建立
	Do（執行）	四階文件撰寫 營運持續管理
	Check（檢查）	內部稽核作業 管理審查作業
	Act（行動）& 認證	進行第三方稽核驗證作業

我們不僅解釋流程，更與您一同走過每一步。

認證不是終點，而是持續守護的開始

在快速變化的數位環境中，資訊安全是一場沒有終點的旅程。
取得 ISO 27001 認證，代表您的組織已經建立了一個穩固的「高海拔基地營」。



持續改善

透過 PDCA 循環，您的 ISMS 將不斷進化，以應對新的威脅與挑戰。

定期再審核

維持認證資格需要定期接受監督稽核，這將成為組織自我檢視的動力。

我們致力於協助您不僅是「通過認證」，更是真正地「內化資訊安全文化」，建立可持續的數位韌性。