服務建議書

AI輔助處分案系統之擴充

經濟部國際貿易署

AI 輔助處分案系統服務擴充



8.1 廠商自評表

評選項目	評選標準	廠商具優勢、獨特、差異之內容說明	服務建議書章節及項次	備註
一、廠商履約能力與實績	廠商規模及營運狀況。			
	過去參與相關系統承作案件實績或與本案相關之資訊系統開發經驗。			
	廠商對本專案支援能力及人力。			
二、專案需求及建議	對本案之系統架構、維護項目及增修需求能完全掌握並提出可行方法。			
	對於本案提出之改進建議（含採行工具及技術）之適切性。			
三、專案組織及管理方式	專案管理方法及所使用之工具。			
	專案組織架構及人力規劃與其運作方式。			
	專案組織成員之學經歷、專長及與本專案相關實績經驗等。			
	對大型資訊專案之策略規劃、專業顧問諮詢能力。			
	交付產品與時程建議（含重要查核點）			
	品質保證（含監控與查核暨如何進行變更管理與版控）			
四、資安作為	對本案資安管理需求應遵循資安規範之有效作法			

	廠商內部資安政策、資安人力配置、獲得資安認證等。			
	資安作為自評情形。			
五、**價格合理性**	對本專案之經費預估(含資安經費)、人力配置及成本分析之完整性及合理性。			

目次

表目錄.....iv

圖目錄.....vii

壹、專案概述.....1

1.1 專案名稱與背景.....1

1.2 專案目標與成功準則.....2

1.3 專案範圍與責任邊界.....5

1.4 專案時程與交付策略.....9

貳、廠商簡介與能力.....12

2.1 廠商能力與專業資格.....12

2.2 公司實績與相關經驗.....12

2.3 計畫主持人與履約團隊.....12

2.4 人員資格、證照與證明文件.....12

參、需求建議.....13

3.1 現況架構與整體設計原則.....13

3.1.1 分層架構與信任邊界.....13

3.1.2 非功能需求與可觀測性.....15

3.1.3 部署拓撲、容量與相容性驗證.....16

3.2 影像辨識與結構化資料擷取.....17

3.2.1 輸入、辨識與欄位映射.....18

3.2.2 品質樣本與驗證策略.....20

3.2.3 資料模型、校驗規則與營運回饋.....21

3.3 地端 TAIDE 解析與人工覆核.....23
3.3.1 地端推論管線與輸出約束.....23
3.3.2 模型風險、測試與營運治理.....25
3.3.3 提示治理、成效分析與安全降級.....27
3.4 案件流程擴增與定型稿管理.....28
3.4.1 共用流程與差異配置.....29
3.4.2 定型稿生命週期與內容正確性.....31
3.4.3 資料轉換、分批上線與案件回歸.....32
3.5 外部系統介接、權限與追蹤報表.....34
3.5.1 安全介接與交易一致性.....34
3.5.2 追蹤報表與操作軌跡.....36
3.5.3 介接契約測試、對帳與報表治理.....38
3.6 維護增修、工具與技術改進.....39
3.6.1 維護事件、問題與增修需求.....40
3.6.2 工具鏈改進與技術債治理.....42
3.6.3 保固運作與改進驗證.....43
肆、管理建議.....44
4.1 管理方法、監控機制與協作工具.....44
4.2 專案組織、人力規劃與運作方式.....48
4.3 策略規劃、專業顧問與需求治理.....52
4.4 工作時程、交付產品與重要查核點.....56
4.5 品質保證、測試與驗收管理.....73

4.6 變更管理、版本控制與移轉交接.....79
伍、訓練建議.....84
5.1 訓練目標、對象與成效指標.....84
5.2 課程內容、教材與實作演練.....87
5.3 技術移轉與知識管理.....91
5.4 執行、查核與持續改善.....94
陸、安全需求.....98
6.1 資安治理、法遵與風險管理.....98
6.2 資料保護、身分識別與存取控制.....102
6.3 安全開發、組件治理與環境管理.....107
6.4 弱點檢測、修補與事件應變.....112
6.5 備援演練、稽核與持續營運.....117
6.6 資安責任、人力與自我評估銜接.....121
柒、價格分析.....128
7.1 總包價估算基礎與價格結構.....128
7.2 工作項目、數量、單價與複價明細.....132
7.3 成本效益、合理性與付款連動.....139
捌、結論.....144
8.1 綜合結論.....144
參考文獻.....145
附件一、附錄.....146

表目錄

表 1 專案背景與基線盤點 2

表 2 專案目標與成功準則 4

表 3 專案工作範圍與主要交付 6

表 4 機關與廠商責任邊界 7

表 5 分期里程碑、進入條件與交付證據 10

表 6 整體架構決策與驗證方式 14

表 7 非功能需求、觀測指標與驗收證據 16

表 8 影像解析狀態與控制 19

表 9 影像與欄位解析驗證矩陣 21

表 10 地端 TAIDE 推論閘門與失敗處置 25

表 11 TAIDE 模型風險與治理證據 26

表 12 案件類型擴增需求追溯矩陣 30

表 13 定型稿生命週期與控制證據 32

表 14 介接交易狀態與復原策略 36

表 15 追蹤報表與稽核軌跡驗收矩陣 37

表 16 維護事件處理與服務證據 41

表 17 專案治理節奏與管理輸出 45

表 18 專案控制線、監控資料與決策證據 47

表 19 關鍵工作之人力持續性與交接證據 51

表 20 重大需求與技術方案決策紀錄 54

表 21 工作時程、交付產品與相依關係 57

表 22 重要查核點與進退場條件 58

表 23 測試層級、範圍與放行證據 75

表 24 驗收面向與完整性判定 77

表 25 變更類型、核准與驗證要求 80

表 26 工作移轉與退場查核清單 82

表 27 訓練對象、任務與成效證據 85

表 28 四小時訓練課程模組與查核方式 88

表 29 訓練情境與例外演練案例 89

表 30 技術移轉資產與接手驗證 92

表 31 訓練執行、查核與改善閉環 95

表 32 資安風險、控制與查核證據 99

表 33 委外資安監督與法遵查核矩陣 101

表 34 資料生命週期、保護控制與證據 103

表 35 身分、權限與稽核控制矩陣 105

表 36 安全開發生命週期與發布閘門 108

表 37 軟體組件、開源與環境治理清單 110

表 38 資安檢測、修補與複測矩陣 113

表 39 資安事件應變、通報與結案證據 115

表 40 備份、復原與替代流程驗證矩陣 118

表 41 備援演練、稽核與改善追蹤 119

表 42 資安責任、資格與自評證據索引 122

表 43 資安管理作業自我評估表 126

表 44 總包價估算基礎與交付關聯 129

表 45 全案價格結構、占比與用途 130

表 46 AI 輔助處分案系統擴充案詳細價格明細 134

表 47 成本投入、效益與驗證證據 141

表 48 資安經費與三期付款驗證 142

圖目錄

圖 1 AI 輔助處分案件系統擴充之任務脈絡 1

圖 2 專案目標、控制方法與驗收證據鏈 3

圖 3 三期擴充交付與保固服務銜接 10

圖 4 地端 AI 案件處理目標架構與信任邊界 14

圖 5 影像辨識、欄位擷取與品質檢核流程 19

圖 6 地端 TAIDE 解析、引用依據與人工覆核閉環 24

圖 7 案件類型擴增、共用流程與定型稿治理 30

圖 8 跨系統介接交易、權限與狀態追蹤架構 35

圖 9 維護、增修與技術改進的證據閉環 41

圖 10 治理層級、管理節奏與協作證據 45

圖 11 專案角色、最低配置與責任協作關係 49

圖 12 需求治理與重大決策的分級閘門 54

圖 13 履約工作甘特圖（系統擴充及保固）（一）：第 1 至 9 週 60

圖 14 履約工作甘特圖（系統擴充及保固）（二）：第 10 至 18 週 61

圖 15 履約工作甘特圖（系統擴充及保固）（三）：第 19 至 27 週 62

圖 16 履約工作甘特圖（系統擴充及保固）（四）：第 28 至 36 週 63

圖 17 履約工作甘特圖（系統擴充及保固）（五）：第 37 至 45 週 64

圖 18 履約工作甘特圖（系統擴充及保固）（六）：第 46 至 54 週 65

圖 19 履約工作甘特圖（系統擴充及保固）（七）：第 55 至 63 週 66

圖 20 履約工作甘特圖（系統擴充及保固）（八）：第 64 至 72 週 67

圖 21 履約工作甘特圖（系統擴充及保固）（九）：第 73 至 81 週 68

圖 22 履約工作甘特圖（系統擴充及保固）（十）：第 82 至 90 週 69

圖 23 履約工作甘特圖（系統擴充及保固）（十一）：第 91 至 98 週 70

圖 24 需求、設計、測試與驗收證據 V 模型 75

圖 25 變更、版本、發布與移轉的可追溯鏈 80

圖 26 角色導向訓練路徑與成效證據 85

圖 27 技術移轉資產、實作驗證與知識更新循環 92

圖 28 中級資通系統之資安治理與風險證據架構 99

圖 29 安全軟體開發、組件治理與環境隔離流程 108

圖 30 弱點與資安事件之分級、修補及驗證閉環 113

圖 31 成本投入、交付證據與分期付款連動 140

壹、專案概述

1.1 專案名稱與背景

本專案正式名稱為「AI 輔助處分案系統擴充案」。其核心任務是延續既有處分案件系統，將來文影像解析、地端語言模型輔助、案件內容製作、跨系統介接與追蹤報表整合為可治理、可查核的作業鏈。現行場域已有 Windows Server 2019、SQL Server 2019、Ubuntu 22.04.5、Docker 與 Spring Boot 內嵌 Tomcat 等環境，擴充設計須在既有基礎上控制相容性、資安及移轉風險。

業務痛點來自多格式來文需人工摘錄、不同案件類型存在欄位與定型稿差異，且處理狀態散落於多個環節。建議以機關內網作為信任邊界，讓影像辨識與 TAIDE 只產生結構化候選內容，承辦人仍負責核對、編輯與核准；核准結果再進入公文、郵局、罰鍰、登記及商工等介接與追蹤流程。這項安排同時回應效率、正確性、責任歸屬與可稽核性，並以測試紀錄、操作軌跡、交付文件及月報作為驗收證據，如圖 1 所示。

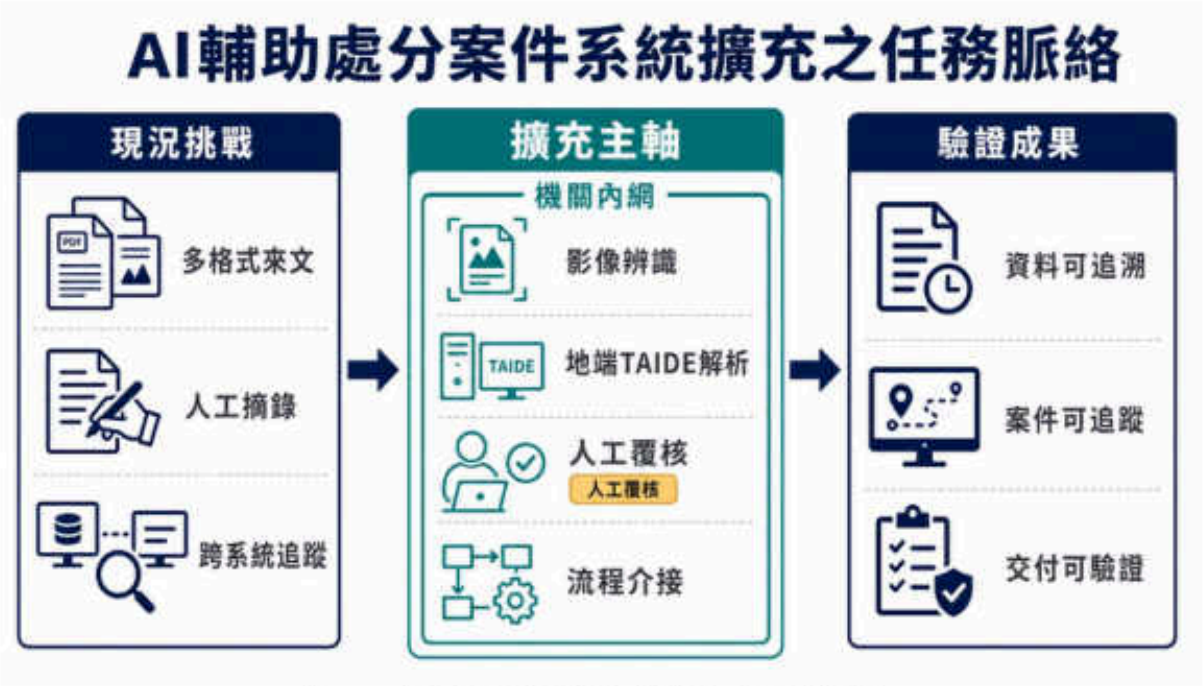

圖 1 AI 輔助處分案件系統擴充之任務脈絡

專案背景與技術環境必須在啟動期轉化為可驗證基線，而不是僅列出設備與版本。盤點結果需標明現況、擴充影響、控制方式與輸出證據；例如既有作業系統與資料庫涉及相容性，地端推論硬體涉及容量與模型版本，外部介接涉及身分、權限與交易復原。如此可把環境限制連到設計、測試與移轉清冊，並讓後續變更有一致比較基礎，如表 1 所示。

表 1 專案背景與基線盤點

基線面向	已知條件	擴充重點	控制與驗收證據
應用環境	Windows Server 2019、Spring Boot 內嵌 Tomcat	既有服務相容與增修	環境盤點、建置與運轉測試紀錄
資料環境	SQL Server 2019	欄位、案件狀態與日誌一致性	資料字典、轉換檢核、備份復原紀錄
AI 環境	Ubuntu 22.04.5、Docker、地端 TAIDE 推論硬體	影像與文字解析均在內網執行	模型與映像版本、容量測試、操作紀錄
業務流程	來文、案件製作、介接、追蹤	16 類案件擴增與定型稿管理	需求追溯、情境測試、使用者確認紀錄
維運服務	上線諮詢、保固與工作移轉	事件處理與知識接續	工單、月報、教材、移轉清冊

1.2 專案目標與成功準則

本節以業務可用、技術可控、資安合規及維運可持續四個面向定義成功。第一項目標是把影像與文件內容轉為可編輯的結構化候選資料，降低重複輸入，同時保留原始影像、辨識結果及人工修訂差異。第二項目標是以地端 TAIDE 輔助內容解析，但不把模型輸出直接視為行政決定；所有重要欄位與函稿仍經規則檢核及承辦覆核。第三

項目標是讓案件狀態、介接交易與操作行為可追溯，失敗可辨識、可重送、可稽核。第四項目標是以文件、程式碼、測試、教材及保固月報形成可接手的維運資產。

依行政院《行政院及所屬機關（構）使用生成式 AI 參考指引》，機關使用生成式 AI 應重視資料治理、風險評估與人工覆核；本案以地端執行、資料最小化、輸出標示及權責分離落實這些原則。（行政院，2023）系統成功不以單一模型指標決定，而是以端到端情境能否完成、人工是否能辨認與修正、介接是否留下完整狀態、錯誤是否未揭露內部細節及交付證據是否可重現共同判定。

四類目標均須在需求階段建立查核方法，並沿需求、設計、測試、交付與保固持續累積證據。解析可用性著重欄位與例外；流程可追蹤性著重狀態與日誌；介接可靠性著重權限、資料交換與復原；維運持續性著重監控、文件及接手實作。各目標若只完成畫面而未留下測試或稽核軌跡，即不得視為完整達成，如圖 2 所示。



圖 2 專案目標、控制方法與驗收證據鏈

成功準則採「需求可追溯、控制可執行、證據可重現、責任可辨識」四項共通原則。需求可追溯表示每一功能均能連回核定需求與案件情境；控制可執行表示權限、

檢核與例外處理可由測試重現；證據可重現表示報告、日誌、版次及資料可支持審查；責任可辨識表示機關與廠商、系統與人工之決策邊界明確。其衡量方式與驗收輸出需一併列管，如表 2 所示。

表 2 專案目標與成功準則

目標面向	成功準則	驗證方法	主要證據
解析可用	影像與文字可轉為可編輯候選欄位，例外可辨識	標準、邊界及異常樣本測試	測試資料、欄位差異、人工覆核紀錄
流程可追蹤	案件狀態、操作與失敗原因可查詢	端到端案件情境與權限測試	狀態紀錄、操作軌跡、報表
介接可靠	身分、交換、錯誤與重送行為符合規格	API、SSO、重送與復原測試	介接規格、交易識別、整合測試結果
資安可控	地端執行、最小權限、檢測與改善形成閉環	設定檢查、弱點與滲透測試、稽核	組態、檢測報告、修補與複測證明
維運可持續	人員能依文件完成操作、監控、部署與回復	接手實作、演練與保固服務查核	手冊、程式碼、教材、移轉清冊、月報

成功準則在需求確認階段由業務情境、現況基線及交付條件共同建立。每一準則均記錄適用案件、資料時點、測試環境、責任角色及證據來源，並區分必須達成的契約符合性與用於持續改善的觀察指標。未有可靠基線的效率或準確數值不先作承諾，而以代表性樣本建立初始資料，再由機關依業務風險核定驗收情境；如此可以避免不同文件品質、案件類型或模型版本被混為同一比較母體。

準則的維護隨需求、資料、介接或版本變更同步進行。變更申請須說明原準則是否仍適用、哪些案例需重跑、數據是否可比較及殘餘風險如何處理；通過變更後保留

舊口徑及生效時間，使驗收、月報與保固分析能回到正確版本。若功能可用但操作負擔偏高，或模型結果可讀但人工修訂集中於重要欄位，管理上應拆解原因並安排介面、規則、資料或訓練改善，不以整體平均掩蓋高影響例外。

驗收時由需求追溯矩陣逐項核對準則、案例、實際結果與缺失。通過代表核定範圍及版本具備所需功能與控制，不代表系統永遠不會發生例外；後續仍由監控、工單、弱點、人工覆核差異及月報持續觀察。這項治理可讓專案目標在設計、交付與保固之間保持相同語意，並為任何偏差提供可查證的改善入口。

1.3 專案範圍與責任邊界

專案範圍涵蓋影像解析、TAIDE 文字解析、案件追蹤報表、既有系統維護、16 類案件擴增、定型稿管理及外部系統介接。工作並非單純新增模型服務，而是把輸入、資料、流程、介接、報表、資安、測試、文件與保固一併納入。所有功能均在機關內網執行，不使用外部雲端模型或運算環境；對外資料交換則經核定介接與安全 API，並以最小資料集、身分驗證、權限檢核與交易紀錄控制。

功能範圍分為七個工作包。影像解析負責輸入品質、辨識及欄位映射；地端 TAIDE 負責在核准資料範圍內產生結構化候選內容；案件擴增負責 16 類流程、可編輯欄位與建議函稿；定型稿管理負責版次、生效與歷程；介接負責公文、郵局、罰鍰、登記及商工等資料交換；追蹤報表負責案件狀態、操作軌跡及下載；維運與資安負責監控、事件、檢測、備援、稽核及移轉。每一工作包都有輸入、輸出與驗收證據，避免交付邊界落在模糊的「功能已完成」，如表 3 所示。

表 3 專案工作範圍與主要交付

工作包	核心內容	邊界控制	主要交付 / 驗收證據
影像解析	輸入檢查、辨識、欄位映射、例外佇列	原始影像保留，低品質轉人工	欄位規格、測試資料、差異紀錄
地端 TAIDE	內容解析、候選欄位、建議內容	內網推論、人工覆核、不直接核定	模型與提示版本、情境測試、覆核紀錄
案件與定型稿	16 類案件、可編輯欄位、函稿及版次	共用流程與差異規則分離	需求追溯、定型稿清冊、回歸測試
介接與報表	SSO、安全 API、交易狀態、追蹤下載	最小權限、錯誤不洩漏內部細節	介接規格、整合測試、報表樣本、日誌
維運與資安	監控、事件、弱點、備援、稽核、保固	變更須核准及可回復	工單、檢測報告、演練、月報、改善證明
文件與移轉	設計、程式碼、操作維護、教材	版次一致、清冊點交、接手實作	電子檔、USB 審定版、移轉與簽認紀錄

責任邊界採機關核定、廠商執行、共同查核三層。機關負責業務規則、帳號授權、外部系統協調、需求與變更核定、驗收及正式上線決策；廠商負責分析設計、開發測試、資安控制、文件及保固服務；雙方共同負責需求澄清、測試情境、缺失分級、重大風險處理與移轉演練。AI 輸出僅是輔助候選內容，正式業務判斷始終由具權限人員依程序完成。

資料與環境亦有明確邊界。機關提供合法且經授權的測試資料、帳號與介接窗口，廠商只在核准環境及用途內處理；開發、測試與正式環境分離，測試資料須去識別或

採專用資料集。設備交付含掃描器，但其型號、數量、安裝位置及驗收條件依核定規格與清冊執行。任何超出核定範圍的新介接、資料用途或業務規則，均經影響分析與變更程序，不由技術人員逕行擴張，如表 4 所示。

表 4 機關與廠商責任邊界

活動	機關責任	廠商責任	共同查核點
需求與規則	提供業務依據、核定需求與優先序	訪談、分析、追溯與可行性評估	需求基線與例外清單
資料處理	確認用途、授權、測試資料與存取	最小化處理、保護、留痕與銷毀 / 返還	資料清冊與權限檢查
系統介接	協調外部窗口、核發必要帳號	設計安全 API、錯誤與重送機制	規格、整合測試與交易紀錄
上線變更	核定窗口、時段與風險接受	建置、測試、部署與回復準備	上線檢核與回復演練
資安事件	依機關程序指揮與對外通報	發現、控制、蒐證、修復與報告	事件紀錄、根因及改善追蹤
驗收移轉	審查、測試、驗收及指定接手人員	提交成果、缺失改善、訓練與移轉	清冊、版次、接手實作與簽認

範圍管理先將七個工作包分解為可驗收能力，再定義工作包之間的介面。影像解析輸出候選欄位與來源定位，地端 TAIDE 輸出受結構約束的候選內容，案件服務接收經人工核准的資料，定型稿服務依生效版本產生文件，介接服務只傳送核准最小欄位，追蹤服務彙整案件及交易狀態。每個介面都有資料所有者、輸入條件、錯誤責任、版次及測試方式，避免上游以「已送出」認定完成而下游無法使用。

啟動盤點建立範圍內資產及相依清冊，包括應用服務、資料表、批次、報表、端點、帳號、憑證、掃描設備、模型、容器、備份與文件。清冊標示由本案修改、僅介

接、僅查閱或不在範圍，並記錄可進入環境、維護窗口與限制。對無法在前期取得的外部介接條件，以未決事項管理其決策人、取得日與對測試的影響，仍先完成可獨立驗證的資料契約及模擬案例。

範圍外事項不等於不管理風險。外部公文或登記系統的內部功能不由本案修改，但其可用性、欄位與錯誤會影響本案；機房基礎設施若由機關管理，本案仍需說明地端 AI 對電力、網路、儲存與監控的必要條件。這些依賴以責任介面與前置條件呈現，不將外部延誤自動轉為功能刪減，也不以廠商無權修改為由忽略替代、對帳與復原設計。

驗收範圍由經機關審定的需求、系統版本、環境、資料與交付清冊共同界定。操作介面、應用服務、資料庫、AI 模型、介接、報表、權限、日誌、文件與操作訓練須相互一致；外部正式端點尚無法配合時，先在核准測試環境完成契約與錯誤情境，再依保存的查核步驟辦理正式接通。設備則依審定規格、數量、序號、安裝、操作及保固清冊驗收。

任何新增案件類型、資料用途、外部介接、模型任務或法規控制，都先判斷是否屬原核定範圍及是否影響成本、時程、資安與交付。屬範圍內的澄清仍更新需求與測試，超出基線者依變更程序核准後才執行。這能保護總包價責任的完整，也避免未經評估的需求透過會議紀錄直接進入正式版本。 範圍基線另需建立「不處理但須監控」清單，例如外部系統內部功能、機房基礎服務及非本案資料治理事項，列出所有者、相依、替代及觸發。清單在每月檢討與重大變更時複核，若外部條件轉為本案阻礙，即升級議題並更新驗收計畫；若確實無影響，保留判斷依據而非刪除。如此可使責任邊界既不無限擴張，也不留下未被管理的灰色地帶。

1.4 專案時程與交付策略

履約時程以決標次日啟動，決標次日起 10 個工作天內提交團隊成員名冊、專案工作計畫書及保密文件；115 年 3 月 31 日前交付需求確認報告書，115 年 6 月 30 日前交付系統運轉測試報告、程式原始碼及目的碼與資安檢測報告，115 年 9 月 30 日前完成結案報告、設計規格、安裝維護與使用操作手冊、資安檢測報告及程式碼。保固至 116 年 12 月 31 日，最後一期月維護報告於 117 年 1 月 5 日前提出。

交付策略採「期前定義、期中檢核、期末審定」三步。期前將文件章節、資料格式、測試範圍與查核人明列於工作計畫；期中以需求追溯、版本清冊與缺失單掌握完成度；期末先做內部複核，再依機關意見修正並提交審定版。文件使用 Microsoft Office 或 LibreOffice 製作，各期先交電子檔，審定後以 USB 點交，且程式、文件、測試與資安報告的版次必須一致。

三期交付並非彼此獨立。第一期需求基線決定設計與測試範圍；第二期以運轉測試、程式碼及資安檢測證明主要功能達到可部署狀態；第三期將上線修正、完整規格、手冊、資安結果及移轉資產收斂為結案基線；保固月報再延續事件、變更、風險與改善紀錄。日期節點與證據依賴須一併管理，避免只追截止日而忽略前置審查，如圖 3 所示。



圖 3 三期擴充交付與保固服務銜接

各里程碑應設置進入條件與完成條件。需求報告進入條件是訪談、現況與介接盤點完成，完成條件是範圍、欄位、流程、權限及驗收方式可追溯；第二期進入條件是設計與主要開發完成，完成條件是測試、程式碼與資安報告可重現；第三期進入條件是上線修正與訓練完成，完成條件是結案資產齊全、缺失關閉及移轉可接手。保固則以月維護報告持續證明服務、事件與版本狀態，如表 5 所示。

表 5 分期里程碑、進入條件與交付證據

里程碑	截止 / 期間	進入條件	完成條件與交付證據
啟動	決標次日起 10 個工作天內	契約啟動、窗口建立	名冊、工作計畫、保密文件齊備
第 1 期	115 年 3 月 31 日前	現況、訪談、資料與介接盤點	需求確認報告可追溯且經審查
第 2 期	115 年 6 月 30 日前	設計與主要功能完成	運轉測試、程式碼、資安檢測報告

里程碑	截止 / 期間	進入條件	完成條件與交付證據
第 3 期	115 年 9 月 30 日前	上線修正、訓練與移轉準備完成	結案、規格、手冊、資安報告及程式碼審定
保固	至 116 年 12 月 31 日	結案基線移交	事件處理、變更、風險與月維護報告持續留存
保固末報	117 年 1 月 5 日前	保固資料收斂	最後一期月維護報告及未結事項狀態完整

時程基線分開管理固定截止、相對週次、工作相依與審查週期，進度依可查核成果而非投入時間判定。偏差發生時分析原因、剩餘工作、關鍵路徑及品質資安風險，再採重排、增援、縮小批次或替代環境；趕工不省略人工覆核、資安檢測、回歸、備份與回復。交付前由技術、測試、資安及文件角色核對內容、版本、敏感分級與意見處置，審定成果納入下一階段基線。

貳、廠商簡介與能力

2.1 廠商能力與專業資格

2.2 公司實績與相關經驗

2.3 計畫主持人與履約團隊

2.4 人員資格、證照與證明文件

參、需求建議

3.1 現況架構與整體設計原則

現況環境同時包含 Windows 應用服務、SQL Server 資料庫、Ubuntu 與 Docker 容器化推論環境，且既有系統已承載案件處理作業。擴充設計先以啟動盤點建立實體、虛擬、網路、服務、資料庫、介接帳號、憑證、排程及備份清冊，再以服務依賴圖辨認單點、版本衝突與容量瓶頸。任何架構調整均需說明不調整的風險、調整影響、測試方式與回復方法，避免以全面重建增加轉換風險。

3.1.1 分層架構與信任邊界

目標架構分為使用、應用、AI 服務、整合及資料維運五層。使用層接收掃描影像與承辦操作；應用層處理案件、定型稿與追蹤報表；AI 服務層執行影像辨識、地端 TAIDE 與欄位規則；整合層提供 SSO、安全 API 及跨系統交換；資料維運層保存業務資料、日誌、備份與監控。安全控制以身分、權限、輸入驗證、加密傳輸、稽核與組態基線貫穿各層，不在單一閘道後即假定內部流量可信。

機關內網是模型與業務資料的主要信任邊界。影像、案件文字及模型提示不得送至外部雲端推論；需要對外交換的業務資料，只能經核定介接、資料最小化與交易留痕。人工覆核置於 AI 輸出進入正式案件流程之前，承辦人可查閱來源片段、候選欄位、檢核結果及修訂差異。這個位置確保模型不直接觸發公文、罰鍰或登記行為，也讓錯誤能在責任明確的節點被發現。

五層服務各有可獨立驗證的輸入、輸出與控制，卻透過案件識別碼、交易識別碼及版本資訊維持端到端關聯。既有應用與資料庫以相容性測試保護，AI 服務以容器映像與模型版本控制，整合層以身分、權限與失敗復原控制，資料維運層以備份、日誌

與監控提供證據。架構圖的重點在於界定資料何時進入 AI、何時回到人工以及何時可對外交換，如圖 4 所示。

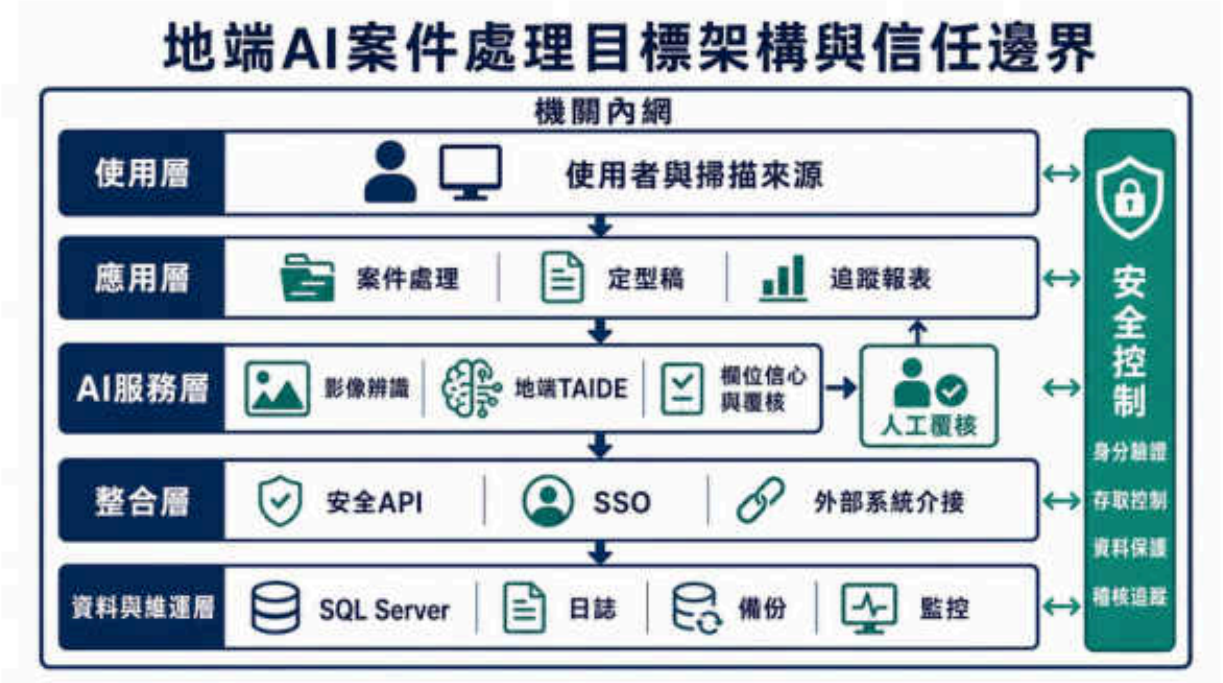

圖 4 地端 AI 案件處理目標架構與信任邊界

架構決策須以約束與驗證共同記錄。地端推論可降低敏感資料外送風險，但增加容量、版本及維運責任；容器化可固定依賴，卻仍需處理映像來源、弱點與資料持久化；安全 API 可隔離介接差異，但必須具備逾時、冪等、重送與稽核；人工覆核能控制模型不確定性，卻需避免畫面資訊不足造成形式化勾選。各項取捨均連結測試與回復證據，如表 6 所示。

表 6 整體架構決策與驗證方式

架構決策	採行理由	主要風險	控制與驗證
延續既有應用與資料庫	降低轉換及停機風險	版本相容、既有技術債	依賴盤點、回歸與運轉測試
地端 TAIDE 推論	資料不送外部雲端，符合內網執行	容量不足、模型或提示漂移	容量測試、版本清冊、覆核紀錄

架構決策	採行理由	主要風險	控制與驗證
AI 服務容器化	固定執行依賴並利於回復	映像弱點、設定或資料遺失	核准映像、掃描、組態與持久化檢查
安全 API 整合	隔離外部差異並集中稽核	逾時、重複交易、敏感錯誤	身分驗證、冪等、重送、遮蔽與日誌測試
人工覆核閘門	保留業務責任與例外判斷	過度信任模型、覆核資訊不足	顯示來源、差異、規則結果及核准人紀錄

3.1.2 非功能需求與可觀測性

非功能設計以安全、可靠、效能、可維護及可移轉為五項主軸。安全要求涵蓋 HTTPS、角色權限、錯誤遮蔽、日誌、弱點修補與檢測；可靠要求涵蓋逾時、重試、交易一致及備份復原；效能要求以機關核定的資料量與併發情境執行容量及壓力測試；可維護要求將組態、版本、監控與事件連至工單；可移轉要求程式、文件、建置方式與接手實作一致。數值門檻若未由來源固定，於需求確認時透過實際基線與業務尖峰情境建立，並納入測試案例。

可觀測性需跨越影像、模型、應用、介接與資料庫。每筆處理至少具備案件識別、請求或交易識別、步驟狀態、開始與完成時間、處理版本、結果類型及錯誤分類；日誌不得寫入不必要的完整影像、敏感內容、密碼或憑證。監控同時關注服務存活、資源使用、佇列積壓、處理失敗、介接逾時、資料庫容量與備份狀態，告警需能連到處置人、工單及結案原因。

非功能驗收不以文件敘述取代實測。安全由設定檢查、權限情境及資安檢測證明；可靠由逾時、重送與復原演練證明；效能由代表性資料與尖峰情境證明；可維護由監

控、事件及發布演練證明；可移轉由指定人員依文件完成接手任務證明。如此能把抽象品質要求轉為可重複的情境、觀察值及證據，如表 7 所示。

表 7 非功能需求、觀測指標與驗收證據

面向	需求情境	觀測重點	驗收證據
安全	未授權存取、輸入異常、敏感錯誤	拒絕結果、稽核事件、遮蔽內容	權限測試、組態檢查、檢測與複測報告
可靠	介接逾時、服務中斷、重複送件	交易狀態、重送次數、資料一致	故障注入、冪等、備份與復原紀錄
效能	批次影像、多人同時操作、報表下載	等候、佇列、資源及完成情形	容量與壓力測試報告
可維護	告警、事件、版本發布與回復	告警到工單、版次、根因及改善	監控截錄、工單、發布與回復紀錄
可移轉	新人依文件建置、操作與排錯	步驟完整、權限適當、缺口數	手冊、移轉清冊、接手實作與修訂紀錄

3.1.3 部署拓撲、容量與相容性驗證

部署設計先盤點現行伺服器、虛擬化或實體資源、作業系統修補、網路區段、DNS、時間同步、儲存、備份、監控與機房進入程序，再建立應用、資料庫與 AI 服務的部署圖。Windows 應用服務與 Ubuntu 推論服務之間只開放必要通訊，服務帳號、連接字串及憑證依環境分離；Docker 容器所需模型與設定由核准來源部署，執行時不以掛載不受控主機目錄或特權模式換取便利。資料持久化、日誌與暫存的所在位置、容量及清理規則在上線前明確。

容量評估以實際案件影像大小、頁數、同時操作、批次量、報表範圍及模型資源需求建構情境。測試同時觀察應用回應、佇列等候、CPU、記憶體、GPU、磁碟、資

料庫連線與外部介接，不只量測模型單次推論。尖峰若超過即時處理能力，採佇列、批次、優先序或受控降級，並向使用者顯示狀態；系統不得因資源不足而遺失案件或重複交易。容量結果保留資料集、環境、版本及限制，作為正式監控門檻與擴充依據。

相容性驗證涵蓋 Windows Server 2019、SQL Server 2019、Ubuntu 22.04.5、Docker、Spring Boot 內嵌 Tomcat 與核准 TAIDE 版本。作業系統、資料庫、框架或映像修補先在測試環境重建，執行建置、資料庫異動、AI 案例、介接、權限、報表及回復測試；正式發布後核對實際版次。若元件支援狀態或弱點要求升級，評估功能、驅動、資料、授權及硬體相容，提出分期與回復方案，不把升級風險延至保固末期。

上線準備另包含組態差異檢查、備份可用、回復步驟、監控告警、操作窗口與冒煙案例。開發、測試與正式環境的差異需逐項說明；無法完全複製的外部介接或資料量，使用模擬與正式接通後補充查核共同控制。部署結果進入環境與發布清冊，使維運人員能由服務異常回查依賴、組態及最近變更，也讓移轉時可在不依賴原開發者的情況下重現核准環境。 架構驗證完成後，需產出可供維運的依賴與故障影響清單。每項服務列上游、下游、健康檢查、告警、必要連接、資料位置與安全責任，並從登入、影像、AI、案件、介接及報表各抽一條端到端路徑演練。若單一元件失敗，清單應能指出受影響能力、可用替代及恢復後的資料檢核；成果同步納入安裝維護手冊與移轉，避免架構圖只在設計審查時使用。 架構文件的每項元件均指定所有者與更新觸發，正式變更、事件或弱點若改變資料流與信任邊界，即同步修訂並重做相應測試，避免設計資料在開發後失去效力。

3.2 影像辨識與結構化資料擷取

來文影像品質、版面與欄位位置具有差異，影像辨識不可只以文字輸出是否存在判斷完成。本節處理影像接收、品質檢查、文字與版面辨識、欄位映射、規則驗證、

人工覆核、例外佇列及證據保存。設計以原始影像不可變、衍生結果可版本化、每次修訂可追溯為原則，讓結構化資料能回指來源頁面與區域。

3.2.1 輸入、辨識與欄位映射

影像接收先檢查檔案類型、大小、頁數、完整性與惡意內容，再檢查方向、清晰度、傾斜、對比及遮擋。未通過技術檢查者不得直接送入後續流程，而是建立可讀的例外原因；可校正項目保留處理前後版本，不可校正項目轉人工處理。掃描器交付需以代表性文件驗證掃描設定、頁面順序與成像品質，並將設定納入操作手冊。

辨識階段分離版面區塊、文字、表格與鍵值對，保留頁碼、座標、識別信心與辨識引擎版本。欄位映射不直接依固定座標，而以文件類型、標籤、相鄰關係及格式規則共同判斷，降低版型微調造成錯置。每個候選欄位均連回來源文字與影像區域，承辦人可快速對照；同一欄位有多個候選時，系統應顯示差異與選擇理由，不以靜默覆蓋處理。

欄位檢核至少包含必填、資料型態、日期、識別碼格式、允許值、跨欄一致性及重複案件。通過規則不表示內容必然正確，而是表示可進入人工覆核；未通過則依缺欄、格式、矛盾、低信心或系統錯誤分類。這條流程把自動化集中在可重複的擷取與檢核，把語意例外與正式判斷保留給人員，並以處理版本及差異紀錄支持查核，如圖 5 所示。



圖 5 影像辨識、欄位擷取與品質檢核流程

處理狀態應能反映資料處於接收、檢查、辨識、映射、待覆核、例外或已確認的哪一階段，且任何失敗都有下一個可執行動作。狀態間轉換由系統事件或具權限人員操作觸發，記錄來源版本、處理版本、操作人及時間。原始影像、衍生影像、候選資料與確認資料分層保存，避免後續重跑辨識改寫已核准內容，如表 8 所示。

表 8 影像解析狀態與控制

狀態	進入條件	系統處理	人工處置	保留證據
已接收	檔案完整且取得案件識別	雜湊、類型與安全檢查	檢視來源是否正確	原始檔、接收時間、來源
品質檢查	通過基本安全檢查	方向、清晰、傾斜、頁序檢測	重掃或接受例外	品質結果、校正前後版本
辨識與映射	影像可處理	文字、版面、欄位候選及規則檢查	無	引擎版次、座標、信心、規則結果
待覆核	候選資料已產生	顯示來源、差異與警示	核對、編輯、核准或退回	修訂前後值、操作人與時間

狀態	進入條件	系統處理	人工處置	保留證據
例外	缺欄、矛盾、低品質或系統失敗	分類、指派、保護技術細節	補件、人工輸入或重處理	例外類型、工單、處理結果
已確認	具權限人員核准	鎖定核准版並送後續流程	依法定程序續辦	核准版、來源關聯、版本與稽核軌跡

3.2.2 品質樣本與驗證策略

測試資料要涵蓋標準、邊界與異常情境，並避免只使用開發期間反覆調整過的樣本。標準情境檢查常見版型與清晰掃描；邊界情境包含多頁、旋轉、表格、手寫註記、低對比及相似欄位；異常情境包含缺頁、重頁、破損、錯誤檔案、惡意內容及無法辨識。資料集須有來源授權、去識別方式、預期結果、使用目的及保存期限，完成後依機關規範返還或處理。

驗證分為技術正確、業務可用與操作可控。技術正確比較文字及欄位候選與標註答案；業務可用檢查重要欄位是否能支持後續案件處理；操作可控檢查承辦人能否辨識來源、修正錯誤與處理例外。數值指標僅是判斷材料，正式驗收還須抽查錯誤類型、重要欄位影響及人工補救成本。每次模型、辨識引擎、版型或規則變更均重跑固定回歸集，並將新增缺失補入案例庫。

缺失管理需區分來源品質、辨識、欄位映射、業務規則、畫面呈現及環境問題，避免把所有失敗歸因於模型。修正完成後使用原案例與相鄰案例複測，確認沒有造成其他版型退步。報告同時列出樣本版本、環境、引擎與規則版次、執行人、預期與實際結果、缺失單及結案依據，才能重現判定。

驗證矩陣將資料類型、處理階段、風險與證據連結。高影響欄位應配置更多異常與人工覆核案例；低品質文件則驗證能否安全轉例外，而非要求系統產出看似完整的內容。每一類案例均明確定義「可接受結果」與「不得發生結果」，例如技術錯誤不得洩漏內部路徑，核准前不得送出外部交易，如表 9 所示。

表 9 影像與欄位解析驗證矩陣

測試類型	代表情境	可接受結果	不得發生	證據
標準版型	清晰、頁序完整、常見欄位	候選欄位可對照來源並進入覆核	無來源定位即自動核准	標註樣本、欄位差異、畫面紀錄
邊界版型	旋轉、多頁、表格、相似欄名	校正或轉例外，頁面關聯正確	欄位跨頁錯置而無警示	前後版本、規則結果、缺失單
低品質	模糊、遮擋、低對比	顯示品質問題並引導重掃或人工	以空白或猜測值覆蓋正式欄位	品質檢測與例外處理紀錄
無效 / 惡意	格式錯誤、破損、異常內容	阻擋、隔離並留下安全事件	執行未授權內容或暴露技術細節	安全日誌、告警及處置工單
回歸	引擎、版型或規則變更	既有重要案例維持可用	修正一類後造成其他類退步	固定案例庫、版次與比較報告

3.2.3 資料模型、校驗規則與營運回饋

結構化資料模型將業務欄位、來源定位、候選值、核准值與處理狀態分開保存。每個欄位定義資料型態、長度、格式、允許值、是否必填、重複性、敏感等級、可編輯角色及介接對應；候選值另保存辨識引擎、版次、頁面區域與規則結果，核准值則

保存操作人、時間與前後差異。如此可支援人工覆核、歷史重現與模型改善，並避免新一輪辨識覆蓋既有核准資料。

校驗規則分為語法、欄位、跨欄、案件及外部參照五層。語法層檢查編碼、日期與數字，欄位層檢查必填及允許值，跨欄層檢查相互一致，案件層檢查狀態與重複，外部參照則只在核准介接可用時查證。規則具有優先序、嚴重度、生效版次及可理解訊息，並區分阻擋、警示與提示；阻擋項在人工補正前不得進正式流程，警示項需具權限人員明確處置，提示則不干擾核心操作。

影像與欄位資料的轉換需具冪等與可回復特性。同一原始檔重送時先辨認雜湊、案件與處理狀態，再決定拒絕、建立新版或重新處理；批次失敗不應留下部分欄位被視為完整。資料庫異動使用交易或受控補償，並將原始、候選與核准版本納入備份。若辨識引擎或版型規則更換，先以影子或測試方式比較，不直接對已核准案件批次重算。

營運回饋分解人工修改原因，包括影像品質、文字辨識、欄位映射、業務規則、來源矛盾、介面理解與案件例外。不同原因對應不同改善責任：掃描設定改善輸入、版面與欄位規則改善映射、模型或提示改善文字候選、介面與訓練改善覆核操作。月度分析標明案件類型、資料時點及版本，修改量增加時先判斷是否源於新案件或新版型，再決定是否調整技術。

正式運轉的抽樣查核以高影響欄位、低品質影像、人工大量修改及例外案件為優先。抽查同時驗證原始影像、候選、規則、核准、後續介接與日誌的關聯，不只比對最終文字。發現系統性錯誤時，先控制受影響案件與版本，建立查詢清單、修正與回歸，再由授權角色決定是否需要補正既有案件。這讓資料品質改善能在保留歷史及責任的前提下進行。 解析服務的可維運性還需處理規則與樣本的變更來源。業務規則、

版型或欄位異動先由需求決策識別，建立新版本及受影響文件類型，測試通過後才生效；緊急修正也保存舊版及回復條件。保固期間每月抽查低信心、例外、人工大量修改及新出現版型，將資料品質、技術缺失與正常業務差異分開，不以提高接受率要求人員忽略問題。

資料輸出到後續案件前，執行完整性與一致性封裝，包含案件識別、來源版本、候選版、核准版、規則版、人工操作與狀態。封裝失敗不得只送出部分欄位，重試前先確認下游是否已接收；成功後保存關聯識別，讓報表、函稿或介接錯誤能回查到當時影像及覆核。這項控制同時支援資料補正、稽核及復原。

3.3 地端 TAIDE 解析與人工覆核

地端 TAIDE 用於正體中文案件內容解析及候選內容生成，執行環境位於機關內網，不使用外部雲端模型或運算環境。TAIDE 官方資訊可作為模型背景，但本案實際採用的模型版本、授權、硬體相容性與容量均以核准環境的測試與清冊為準。（TAIDE 計畫團隊，2024） 模型定位是協助承辦人理解與整理，不代替法定職權、業務規則或人工核准。

3.3.1 地端推論管線與輸出約束

輸入在送入模型前先做用途與欄位最小化，移除不需要的個人或技術資訊，再依案件類型組合核定提示範本。提示內容明列任務、允許資料、輸出結構、禁止推測及缺值處理；模型輸出以 JSON 等結構化格式回傳，通過語法、欄位、型態、允許值與跨欄規則後才呈現在覆核畫面。任何解析失敗、欄位缺漏或內容不一致均轉為清楚的業務警示，技術堆疊與內部路徑只留於受控日誌。

模型、推論映像、提示範本、規則集與輸出結構各自具版號，並以相容矩陣記錄可搭配版本。版本變更先在固定案例庫測試，檢視重要欄位錯誤、過度推論、拒答、

格式失敗與資源需求，再經核准發布。正式案件保留當時使用的模型及提示版本，使日後能說明候選內容的生成條件；但日誌不重複保存不必要的完整敏感輸入。

人工覆核介面同時呈現來源片段、候選欄位、規則結果、模型不確定或缺漏提示及修訂入口。承辦人可接受、修改、清空或退回，每個動作留下前後值與理由類型；系統不得以預設勾選弱化覆核。覆核完成後，核准版與模型候選版分離保存，後續介接只取核准資料。差異可供案例與規則改善，但不直接觸發未經治理的自動回訓，如圖 6 所示。

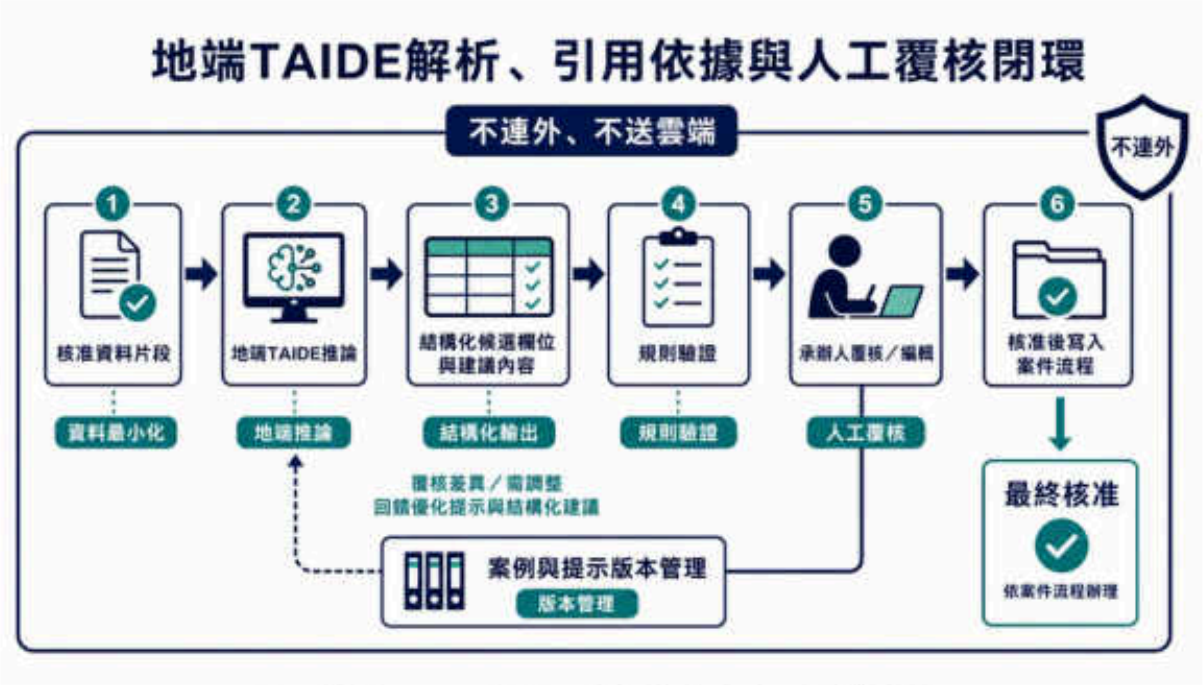

圖 6 地端 TAIDE 解析、引用依據與人工覆核閉環

推論流程的每一閘門都要有明確失敗處置。輸入最小化未通過即不送模型；輸出結構錯誤可在受控次數內重試，仍失敗則轉人工；規則矛盾不得被模型文字掩蓋；人工未核准不得進入正式流程；版本不相容則阻擋發布並回復既有版本。這些控制使效率增益不以責任與資料安全為代價，如表 10 所示。

表 10 地端 TAIDE 推論閘門與失敗處置

閘門	檢查內容	通過後動作	未通過處置	證據
輸入治理	用途、欄位最小化、案件關聯	組合核定提示	阻擋、補正或改人工	輸入欄位清冊、提示版次
地端推論	模型、映像、資源及逾時	產生結構化候選	受控重試、降級或工單	模型版次、資源與執行狀態
結構驗證	JSON、欄位、型態、必填	進入業務規則檢查	標示格式失敗並轉人工	驗證結果、錯誤分類
業務規則	允許值、跨欄一致、來源支持	顯示覆核畫面	缺漏或矛盾警示	規則版次、候選與來源關聯
人工覆核	來源、候選、差異及權限	建立核准版	修改、清空或退回	操作人、前後值、理由與時間
發布與介接	核准狀態、版本相容	送案件流程或介接	阻擋並保留現況	發布清冊、交易與稽核紀錄

3.3.2 模型風險、測試與營運治理

生成式模型可能出現內容無依據、欄位遺漏、格式漂移、對提示敏感或在不同版本產生不一致結果。風險控制依序採限制輸入、限制任務、限制輸出、規則驗證、人工覆核及完整留痕。對法令、金額、日期、身分與處分結果等高影響內容，不以模型自述信心取代來源核對；模型若找不到支持資料，輸出應保持空值或明確標示不足，而非補齊看似合理的文字。

測試資料按案件類型、文件品質、內容長度、欄位重要性與例外情境分層。基準集在版本間固定，挑戰集涵蓋矛盾、缺漏、相似名稱、跨頁資訊、提示注入及不應回答內容，實務抽樣則評估實際業務分布。結果除了欄位一致，也檢查來源可追溯、拒

絕不當指令、敏感資料處理、人工修訂負擔與資源容量。測試報告保留資料集版次與限制，避免不同資料時點的數值被直接比較。

營運監控關注格式失敗、規則不通過、人工修改、退回、逾時、資源不足及案件類型分布。人工修改率上升不必然等同模型退步，可能來自新版型、規則變更或資料品質差異，因此月檢討要分解原因並以同一基準集重測。若發現高影響錯誤、資料外洩風險或版本不相容，先停用受影響功能或回復核准版，再進行根因分析、修正、複測與發布。

模型治理清冊把風險情境連到預防、偵測、處置與驗收證據。每一風險都有責任角色及停止條件，尤其資料外送、無依據高影響內容與未核准版本不得靠使用者自行辨識。治理結果透過月報、版本清冊、測試報告與覆核差異持續更新，形成可稽核而非一次性的 AI 風險說明，如表 11 所示。

表 11 TAIDE 模型風險與治理證據

風險情境	預防控制	偵測方式	處置與停止條件	驗收 / 營運證據
無依據內容	限定任務、來源片段與結構欄位	來源關聯、規則與人工抽查	高影響錯誤即阻擋發布或回復	挑戰集、覆核差異、缺失單
敏感資料外送	地端執行、網路與欄位最小化	網路、日誌與組態檢查	發現外連或不當留存即停用	架構、設定、稽核與檢測紀錄
格式或版本漂移	固定結構、相容矩陣與基準集	格式失敗、回歸差異	不相容版本不得上線	模型、提示、規則與測試版次

風險情境	預防控制	偵測方式	處置與停止條件	驗收 / 營運證據
提示注入	輸入分界、指令限制、輸出驗證	挑戰案例與異常輸出告警	拒絕不當指令並轉人工	安全測試、告警與處置紀錄
資源不足	容量規劃、佇列及逾時控制	CPU、記憶體、GPU、佇列與逾時	降級、排程或暫停新工作	容量測試、監控與工單
過度依賴	強制人工覆核、來源並列	修改、退回與抽查結果	不得自動作成正式業務結果	權限測試、操作軌跡、訓練紀錄

3.3.3 提示治理、成效分析與安全降級

提示範本視為受控系統元件，包含任務目的、允許輸入、角色界線、輸出結構、缺值規則、禁止事項及範例。建立與修改由具業務及技術知識的人員協作，經案例測試與核准後發布；正式使用的系統指令與業務資料採明確分隔，來文中的任何指示均被視為資料，不得覆蓋系統規則。提示範本不包含秘密、正式帳號或不必要個資，且由版本與案件紀錄追溯。

模型評估依欄位重要性與錯誤型態分層，而不只看整體一致。高影響欄位若無來源支持、把否定理解成肯定、混淆當事人或日期，即使其他欄位大多正確，仍應阻擋或轉人工；低影響格式差異則可由規則正規化。報告同時呈現無依據、遺漏、格式失敗、拒答、人工修改與處理時間，並標明基準集、挑戰集與實務抽樣的資料範圍，避免從單一數值推導不適用的結論。

人工覆核品質透過畫面與程序共同保障。來源片段與候選內容並列，重要差異突出但不以顏色作唯一訊息，規則警示說明原因與下一步；承辦人可快速回到原始頁面，核准前系統檢查仍存在的阻擋項。批次核准或大量接受預設值須受限制及稽核，避免

效率功能削弱逐案責任。覆核紀錄保留足夠的前後值與理由，但不要求人員重複輸入系統已能取得的內容。

安全降級在模型服務逾時、資源不足、版本異常、輸出大量失敗或偵測到疑似提示攻擊時啟動。系統可暫停模型、改以影像文字與規則、將案件排入人工佇列或限制特定案件類型，並清楚呈現狀態與影響；降級期間不重複送出、不中斷已核准案件，也不連往未授權外部服務。恢復前以健康檢查、代表案例與版本核對驗證，必要時對降級期間案件重新評估。

成效改善透過經核准的案例與提示版本進行，不把承辦修訂自動用於訓練。若未來需要模型調整或再訓練，須另行確認資料目的、來源、權利、去識別、環境、模型授權、風險及驗證；在未完成治理前，修訂資料只作缺失分析。這項限制保護業務資料，也能避免未經審查的偏差或錯誤被持續放大。 模型營運另建立停止與恢復授權。高影響錯誤、疑似資料外送、版本不明、持續格式失敗或資源異常達到核准條件時，由授權角色暫停全部或特定類型 AI 處理，案件轉人工且保留狀態；恢復須完成原因、修正、代表案例、資安與容量查核。暫停及恢復事件記錄適用範圍、版本、受影響案件與核准，避免功能在無人知悉下反覆開關。

提示與規則的改善需比較同一案例在新舊版本的差異，並檢查原本正確的案件是否退步。若改變輸出欄位或格式，先更新資料契約與介面，再安排相容期；不能用解析器容錯永久承接未治理輸出。人工覆核差異若集中於業務判斷而非模型錯誤，則改善來源呈現與操作說明，不以模型迎合個別人員表述。

3.4 案件流程擴增與定型稿管理

16 類案件擴增牽涉欄位、規則、角色、狀態、函稿與介接差異，若逐類複製程式，後續法規或流程調整會造成多套邏輯不一致。本節建議以共用案件生命週期承載收件、

解析、檢核、簽辦、發文及追蹤，再將案件類型差異收斂為可治理的欄位設定、規則、定型稿及介接條件。個別類型仍可有專屬流程，但其例外必須有需求依據、責任角色與測試案例。

3.4.1 共用流程與差異配置

共用案件主檔至少保存案件識別、來源、類型、目前狀態、承辦角色、處理期限來源、資料版本及稽核資訊。案件明細採結構化欄位及可擴充群組，欄位定義包含名稱、型態、必填、允許值、來源、顯示條件、可編輯角色與敏感等級。流程定義則包含狀態、允許轉換、進入與離開條件、操作角色、失敗處置及通知，避免只在畫面按鈕中隱含業務規則。

案件類型配置需有草稿、審查、生效、停用及封存狀態，修改前先建立影響分析，辨認欄位、定型稿、報表、介接、既有案件及測試的影響。生效時點不得改寫已進行案件的歷史邏輯；若確需套用，應由具權限人員依核定規則執行批次轉換並留下前後值。配置資料與程式版次共同納入發布清冊，使問題可追溯到確切組合。

擴增工作依「盤點共通性、定義差異、建立配置、開發例外、情境驗證」逐類完成，並以同一需求追溯矩陣管理。16 類案件不是 16 個孤立模組，而是共用核心與受控差異的組合；定型稿、欄位與介接條件均連到對應案件情境及回歸案例。這種關係可降低重複開發，亦能在共用元件變更時迅速辨認受影響類型，如圖 7 所示。



圖 7 案件類型擴增、共用流程與定型稿治理

需求追溯應以案件情境而非畫面名稱為核心。每一情境描述觸發、角色、前置狀態、輸入、主要步驟、例外、輸出與證據，並連結欄位設定、規則、定型稿、介接與測試。共用功能變更時可從元件反查案件類型，案件規則變更時則可正向找到需更新的測試、文件與報表，形成雙向影響分析，如表 12 所示。

表 12 案件類型擴增需求追溯矩陣

追溯項目	應記錄內容	變更影響	驗證證據
案件情境	觸發、角色、前置狀態、主要與例外流程	流程、權限、通知	情境腳本、使用者確認、測試結果
欄位設定	型態、必填、來源、編輯權限、敏感等級	畫面、資料庫、報表、介接	資料字典、欄位測試、差異清冊
業務規則	條件、優先序、錯誤訊息、生效時點	既有案件、函稿與測試	規則版次、邊界案例、核定紀錄

追溯項目	應記錄內容	變更影響	驗證證據
定型稿	適用類型、欄位、內容、版本與生效日	文件輸出、簽辦與歷史重現	樣張比對、版次與簽核紀錄
外部介接	對象、欄位、狀態、錯誤及重送	API、帳號、交易一致	規格、整合與復原測試
回歸案例	正常、邊界、例外及權限情境	受影響類型與共用核心	固定案例庫、執行版次、缺失關閉

3.4.2 定型稿生命週期與內容正確性

定型稿管理將內容、資料欄位、格式、適用案件、角色權限與生效條件視為同一版本單位。草稿由授權角色編修，審查時比對前後差異及欄位引用，核准後才可生效；已生效版本不得直接覆寫，停用也不刪除歷史。案件生成文件時保存所用版本、資料快照與生成時間，使日後能重現當時內容，而不是用最新定型稿重新產生舊案。

欄位代入前先驗證資料型態、必填及格式，缺值不得以空白悄然輸出；應顯示可理解的警示並回到補正或覆核。對相似欄名、複數當事人、多筆明細與跨頁內容，使用明確資料路徑與排序規則，不靠自由文字拼接。定型稿預覽同時顯示來源欄位、套用結果及缺漏，正式輸出須與核准預覽一致。

定型稿測試包含樣張比對、欄位代入、條件段落、特殊字元、長文字、缺值、多筆資料、權限及歷史重現。內容審查與技術測試分工：業務人員核對文義、適用條件與格式，技術人員核對欄位、規則、權限及輸出穩定。每次變更建立受影響案件清單與回歸結果，必要時並行保留新舊版本到生效時點。

生命週期的控制點依序為草稿完整、差異可讀、內容與欄位審查通過、測試無阻擋缺失、核准與生效時間清楚、歷史版本可重現及停用後不可新用。相關清冊讓機關

能快速辨認目前生效版本、即將生效版本及仍被歷史案件引用的版本，並以樣張、測試及簽核證明內容正確，如表 13 所示。

表 13 定型稿生命週期與控制證據

狀態	允許活動	必要控制	轉換條件	證據
草稿	編修內容、欄位與條件	編修權限、版次、來源依據	結構與欄位檢查完成	草稿版、差異及編修紀錄
審查	業務與技術平行核對	前後差異、樣張、缺值及權限測試	意見關閉、回歸通過	審查意見、樣張、測試結果
核准	確認適用範圍與生效時點	核准角色、不可直接改寫	核准資料完整	核准人、時間與版本雜湊
生效	供新案件選用與產出	保存案件所用版本與資料快照	到達生效條件	生成紀錄、案件與版本關聯
停用	禁止新案件選用	歷史案件仍可重現	替代版生效或適用原因消失	停用原因、替代關係、影響清冊
封存	唯讀查詢與稽核	不刪除必要歷史	保存期限及程序到達	封存清冊、存取與處理紀錄

3.4.3 資料轉換、分批上線與案件回歸

案件擴增前先盤點既有案件欄位、狀態、定型稿、報表與介接資料，辨認空值、重複、代碼差異及歷史例外。資料轉換規格列來源、目的、型態、對照、預設、例外、驗證與回復，並以唯讀抽樣建立轉換報告；任何無明確規則的欄位不以推測補值，而是列入人工或業務決策。正式轉換前備份並凍結必要寫入，轉換後核對筆數、關鍵欄位、狀態、關聯及抽樣案件。

16 類案件宜按共用性、風險、資料與介接就緒度分批驗證。先以代表類型證明共用生命週期、權限、資料與報表，再納入差異較大的類型；每批均包含正常、邊界、例外、歷史版本及跨系統情境。分批不改變完整交付責任，而是讓缺失在影響範圍較小時被發現，並讓共用元件修正可在下一批前回歸。

上線策略需界定新舊案件如何分流。既有進行中案件可依核定原則維持舊版或受控移轉，新收案件自生效時點使用新版；定型稿及規則的適用版本由案件建立或核准時點決定，避免同一案件處理中途靜默改變。若採並行期，需有資料對帳、功能責任、停止條件及結束準則，不能長期維持兩套無主責流程。

案件回歸案例庫以共用核心、類型差異與歷史缺失三個維度維護。共用核心變更需跑所有受影響類型的最小代表集，類型設定變更需跑該類正常與例外，歷史缺失則永久保留相鄰案例。每次執行記錄資料、環境、程式、設定、定型稿與介接版本，結果若因外部資料時點不同不可直接比較，須標示限制並補充可重現的模擬證據。

上線後觀察案件量、例外、人工修訂、流程停滯、介接失敗及報表差異，依批次與版本分層判讀。若某類案件異常集中，先限制該類或回復設定，不必回退不受影響類型；若共用核心有高影響缺失，則啟動整體控制及回復。所有處置保留案件清單、版本、影響、補正與重新驗證，確保正式資料不因技術回復失去一致性。 案件配置的治理需防止「低程式碼」變成「低控制」。配置編輯、審查、核准、發布與回復權限分離，重大規則及定型稿變更需差異預覽；批次修改先在影子資料檢查受影響案件與文件。正式配置有完整性資訊與相容矩陣，系統啟動時若版本缺漏或不相容即阻擋，而不是用預設值繼續處理。

擴增完成的定義包含需求核定、資料與流程配置、程式、權限、定型稿、介接、報表、回歸、操作文件與移轉，而非單一畫面可操作。每類案件在清冊列完成狀態及

未結事項，跨類共用缺失只建立一個主問題並列受影響類型。驗收抽樣同時涵蓋共用核心與差異最大的案例，以實際證據證明完整範圍。 案件狀態的歷史只能透過合法轉換與補正調整，管理者不得直接改寫以美化報表。必要資料修正建立原因、核准、前後值、受影響報表與外部交易，並以專用程序執行；大量補正先試跑與抽樣，完成後對帳。這使追蹤資料能支援查核與趨勢，不因日常維護失去可信度。

3.5 外部系統介接、權限與追蹤報表

外部系統介接包含公文、郵局、罰鍰、登記及商工等對象，其可用時間、資料格式與錯誤語意可能不同。系統應以安全 API 與交易管理層隔離差異，不讓業務畫面直接耦合外部端點。每筆交換先確認使用者與服務身分、角色權限、案件狀態、資料最小化及輸出格式，再產生唯一交易識別，保存請求摘要、回應狀態與後續處置。

3.5.1 安全介接與交易一致性

介接規格需包含目的、資料欄位、來源與目的系統、觸發方式、身分驗證、加密、逾時、重試、冪等、錯誤碼、對帳、日誌及版本。JSON 等開放格式可降低資料交換耦合，但欄位語意、長度、編碼、必填及允許值仍須明訂。機密憑證不寫入程式或文件明文，分環境管理並限制存取；正式與測試帳號、端點及資料明確分離。

交易處理依序保留待送出、處理中、成功、失敗、待人工及已取消等狀態。逾時時先查詢或對帳，再決定是否重送；重送使用同一業務鍵與冪等識別，防止重複公文、罰鍰或登記。使用者接收可採取行動的業務訊息，技術細節只進受控日誌；需要人工介入時，系統明列責任人、必要資料與重新執行條件。

SSO 負責使用者身分入口，角色權限則依職務、案件狀態及操作類型決定查詢、編輯、核准、重送、下載與管理能力。服務對服務帳號採最小權限及可輪替憑證；高

影響操作需再次確認並完整留痕。權限異動由核准流程驅動，離職、調職或代理到期即調整，不以共用帳號維持便利。

介接架構把外部對象匯入同一身分、交換與狀態控制，但各介接仍保留獨立規格及錯誤映射。操作軌跡與交易日誌以案件及交易識別關聯，讓承辦人看到可理解狀態，維運人員看到診斷資訊，稽核人員則看到誰在何時對何資料執行何動作。失敗重送只能由授權角色依狀態執行，如圖 8 所示。

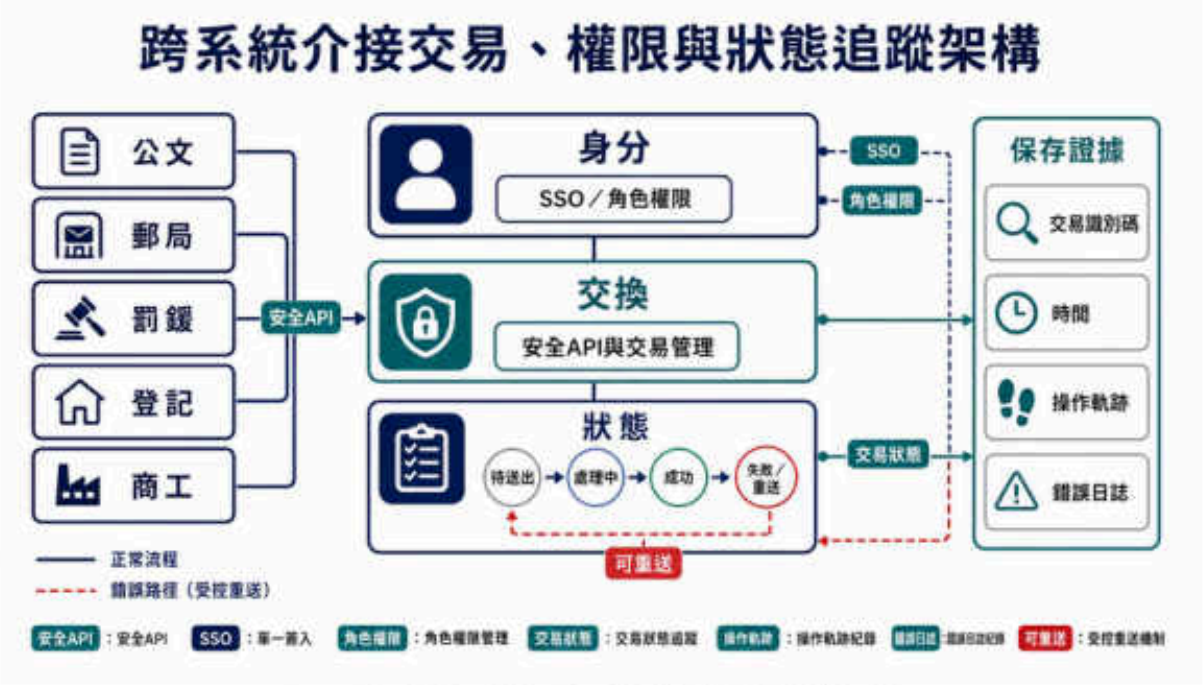

圖 8 跨系統介接交易、權限與狀態追蹤架構

交易控制須同時考慮技術結果與業務結果。HTTP 成功不一定代表業務受理，技術逾時也不等於外部未執行；因此成功需有業務識別或可對帳結果，失敗則依可重試、需補正、需人工或不可重試分類。狀態轉換與對應證據應在介接測試中逐項驗證，如表 14 所示。

表 14 介接交易狀態與復原策略

交易狀態	判定依據	允許動作	復原 / 對帳方式	稽核證據
待送出	權限與資料檢核完成	送出或取消	無外部影響	案件、資料版本、操作人
處理中	已送出但未取得確定業務結果	查詢、等待，不直接重送	以交易識別查詢或對帳	請求摘要、時間、端點版本
成功	取得可核對業務識別或狀態	查詢、後續流程	定期對帳	回應摘要、外部識別、完成時間
可重試失敗	暫時性錯誤且外部未受理	授權重送	同一冪等鍵重送	錯誤分類、重送人與次數
需補正	欄位或業務規則不符	回案件補正後再送	建立新資料版本	外部訊息、前後值、核准紀錄
待人工	結果不確定或對帳不一致	指派、查證、核定處置	人工對帳、取消或補登	工單、查證依據、處置結果

3.5.2 追蹤報表與操作軌跡

案件追蹤以業務可理解的狀態呈現收件、解析、覆核、簽辦、發文、介接及結案，不把底層技術狀態直接暴露給一般使用者。每個狀態顯示進入時間、責任角色、未完成原因與下一步；逾期或停滯的判定依核定規則與資料時點計算。報表可依案件類型、狀態、期間、承辦單位及處理結果篩選並下載，下載資料仍受原資料權限及敏感欄位遮蔽控制。

操作軌跡記錄登入、查詢高敏感資料、建立、編輯、核准、退回、介接、重送、下載、權限與設定變更。紀錄至少包含使用者或服務身分、時間、案件或資源、動作、

結果、來源位置及關聯交易；敏感值採遮蔽或摘要，避免稽核日誌成為另一份高風險資料副本。日誌須防未授權修改，並依用途設定保存與查閱權限。

報表數值需標示資料截止時點、篩選條件與狀態定義。跨月或跨版本比較時，若案件分類、狀態規則或資料完整度已變更，報表應保留口徑版本並揭露限制，不能把不同口徑直接視為趨勢。下載檔建立匯出事件，記錄查詢條件、欄位、筆數、操作人及時間；大量或敏感下載可納入額外授權及告警。

報表與日誌的驗收以角色及情境交叉驗證。一般承辦只能查其權限案件，管理者依授權看彙整，維運人員看技術狀態但不因此取得完整業務內容，稽核角色可依職責查軌跡。資料更新、狀態轉換、介接失敗、重送及下載後，畫面、報表與日誌應在一致時間點反映，如表 15 所示。

表 15 追蹤報表與稽核軌跡驗收矩陣

驗收情境	權限與資料口徑	預期呈現	不得發生	證據
案件查詢	依角色、單位與案件授權	目前狀態、責任與下一步一致	越權看見案件或敏感欄位	角色測試、查詢結果、稽核事件
狀態追蹤	依核定生命週期與截止時點	轉換時間、停滯原因可追溯	畫面與報表狀態不一致	狀態紀錄、報表與資料比對
介接追蹤	以案件及交易識別關聯	成功、失敗、補正、重送可辨識	逾時即顯示成功或重複送出	交易日誌、對帳與工單
報表下載	延續原資料權限及遮蔽	條件、口徑、時點與欄位明確	下載未授權欄位或無事件紀錄	匯出檔、條件、筆數與操作軌跡

驗收情境	權限與資料口徑	預期呈現	不得發生	證據
版本比較	標示狀態與分類口徑版本	可說明差異與限制	將不同口徑直接合併為趨勢	口徑清冊、資料時點與比較說明
稽核查證	依稽核職責與核准範圍	身分、時間、動作、結果完整	日誌可任意修改或含明文秘密	完整性檢查、查閱紀錄與抽查結果

3.5.3 介接契約測試、對帳與報表治理

每個外部介接建立機械可讀與人可審查的資料契約，包含欄位名稱、語意、型態、長度、編碼、必填、枚舉、時間格式、敏感等級及版本相容原則。契約變更先辨認向前與向後相容，並安排雙方測試端點、樣本、錯誤碼及切換時點；未核准的新欄位不直接送正式端點，已停用欄位也需在過渡期保留可辨識處置，避免一方先更新導致交易遺失。

契約測試分為結構、業務、權限、錯誤與容量。結構測試檢查 JSON 及欄位，業務測試檢查案件狀態與允許值，權限測試檢查身分及資料範圍，錯誤測試涵蓋逾時、拒絕、重複、部分成功與不可用，容量測試則使用代表交易量觀察佇列及外部限制。無法在測試端點重現的正式情境，先以模擬證據驗證本案責任，再於接通後依清單補驗。

對帳依交易識別、業務鍵、時間、狀態與結果執行。系統每日或依核定週期辨認本地成功但外部無紀錄、外部成功但本地未完成、重複、長時間處理中及資料差異，產生待處置清單；自動補償只適用規則確定且可回復的情況，其餘由授權人員查證。對帳完成保留前後狀態、依據與處置人，不以直接修改資料庫清除差異。

報表治理建立指標定義、來源欄位、計算邏輯、排除、資料截止、刷新、權限及口徑版次。案件數、處理中、完成、異常與逾期等名稱需有明確狀態集合；報表修改先以同一資料集比對新舊數值，差異說明是規則變更、資料補正或缺失修正。歷史報表保留原口徑或提供轉換說明，避免新版定義重新解讀舊期數據。

下載與大量查詢受資源及資料保護控制。大量資料查詢採受控條件與非同步作業，使用者可查詢進度及資料截止時點；失敗不產生半成品或未受控暫存。下載檔的保存、分享與處理由機關規範約束，系統記錄事件但不在日誌複製完整內容。維運人員以效能及錯誤資訊診斷，不因報表問題取得超出職責的完整案件資料。 介接服務的可觀測性需在不揭露敏感內容下支援查障。每筆請求保存案件、交易、介接、版本、開始完成、狀態、回應分類及重試關聯，資料內容僅保存必要摘要；不同外部系統的錯誤映射到一致業務分類，同時保留原始代碼於受控位置。告警應指出影響範圍與可執行動作，避免只顯示大量無關技術訊息。

SSO 或外部端點變更憑證時，先在測試環境驗證信任鏈、權限、時鐘與失敗情境，再依核准時段輪替；新舊憑證的並行及撤除有明確期限。憑證不可因到期緊急處理而以關閉驗證或共用帳號替代，保固月報持續列效期與責任，避免服務在長期維運中突然中斷。

3.6 維護增修、工具與技術改進

維護範圍包含既有系統問題處理、擴充功能修正、環境與組態管理、介接異常、資料問題、資安弱點、技術諮詢及保固月報。服務通知後 4 小時內回應，8 小時內恢復或提出替代方案；回應是確認影響、責任與下一步，恢復可為正式修復或可控替代，不以關閉工單取代業務可用性。每起事件均保留時間、影響、處置、根因與改善證據。

3.6.1 維護事件、問題與增修需求

單一入口接收事件、服務請求、問題、增修與資安事項，依影響範圍、業務急迫、資料風險、是否有替代方案及法遵影響分級。事件先恢復服務與控制影響，問題管理再尋找根因；增修需求則進入需求澄清、影響分析、核定與排程。不同類型可互相關聯，但不得將事件修復未經評估即轉為永久功能變更。

事件處理依序為受理、確認、分級、控制、診斷、恢復、驗證、結案及問題追蹤。達到 4 小時與 8 小時要求時，證據應是時間戳記、聯繫內容、可用狀態與替代方案，而非事後敘述。替代方案需說明可用範圍、操作步驟、風險、期限與回復正式服務的條件。重大或重複事件於月檢討提出趨勢與改善，不以個案關閉掩蓋系統性風險。

增修優先序考慮法定或契約必要性、業務效益、風險降低、使用範圍、技術依賴、工作量及時程。每項需求均有接受、排程、合併、暫緩或拒絕的決策及理由；核准後連到版本、測試與交付。工具用來支持工單、需求、版本、測試與文件關聯，實際產品可依機關環境選擇，但資料應可匯出、權限可控、歷程可稽核，避免供應商鎖定。

維護閉環以通知時間起算，把回應、恢復或替代、根因、增修、測試、發布及月檢討串成完整證據。4 小時及 8 小時節點只適用於需求所定服務處理，不被擴張為未載明的全年無休可用率承諾；若需跨單位或外部系統協作，仍持續記錄影響控制與責任進展，如圖 9 所示。

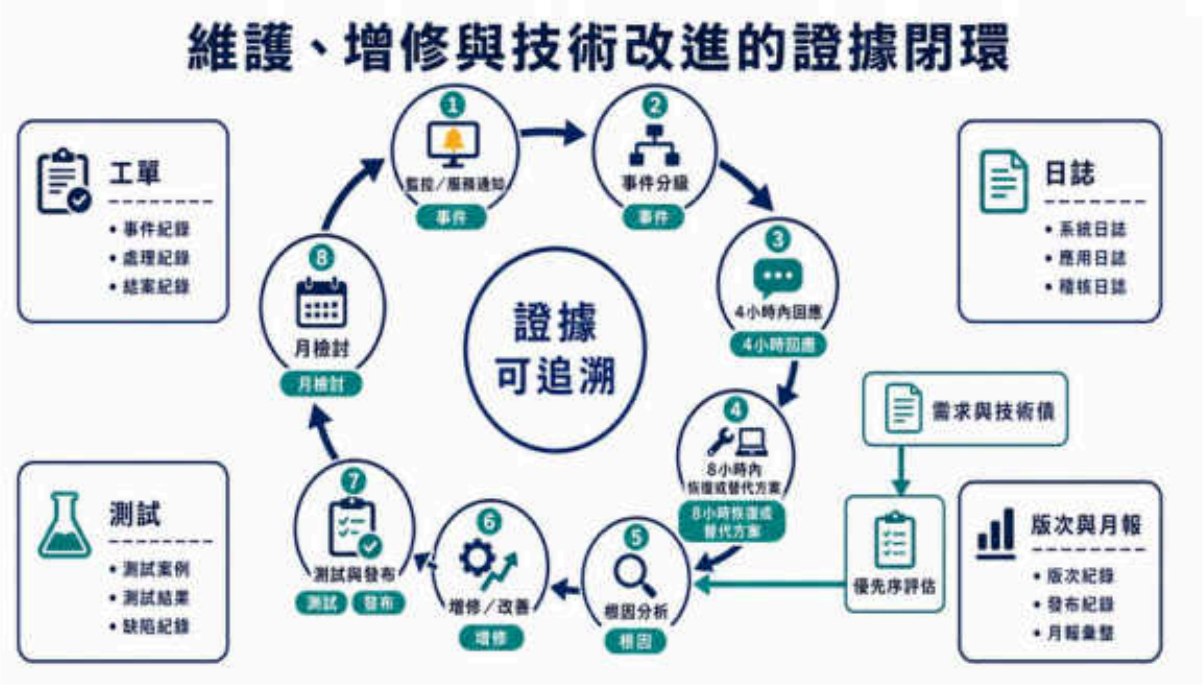

圖 9 維護、增修與技術改進的證據閉環

工單欄位必須支持時效與根因分析。除標題外，至少記錄來源、通知時間、案件或服務、影響、分級、責任人、回應時間、恢復時間、替代方案、根因、變更、測試、發布與結案依據。暫停計時或外部等待不得任意設定，需有狀態、理由及雙方可見紀錄；月報按事件類別、影響與重複根因分析，而不只列總件數，如表 16 所示。

表 16 維護事件處理與服務證據

階段	必要動作	時效 / 判定	主要證據	管理重點
受理與回應	確認影響、窗口、分級與下一步	通知後 4 小時內回應	通知、回應時間、責任人	不以自動回信取代有效確認
控制與恢復	限制影響、修復或提出替代方案	8 小時內恢復或提出替代方案	服務狀態、操作步驟、風險與期限	替代方案須可控且可回復
驗證	由技術與業務情境共同確認	關鍵功能可用、資料一致	測試、監控、使用者查核	避免只看程序或服務存活

階段	必要動作	時效 / 判定	主要證據	管理重點
結案	彙整原因、處置、影響與證據	完成確認且未結風險已列管	工單、版本、缺失與確認紀錄	未完成改善轉問題管理
根因與改善	分析重複、共因與控制缺口	重大或重複事件必辦	根因、改善、責任與期限	月檢討追蹤至複測關閉

3.6.2 工具鏈改進與技術債治理

工具與技術改進不以追求新版本為目的，而以降低手工作業、提高追溯、縮短復原及控制安全風險為準則。建議建立需求與工單關聯、版本與建置可重現、測試結果自動彙整、組件與弱點可追蹤、文件與發布版次一致及監控告警可轉工單等能力。工具導入先以小範圍驗證資料權限、匯出、稽核、備份與移轉，再決定是否納入正式流程。

技術債清冊記錄成因、受影響元件、業務與資安風險、暫行控制、改善選項、估計工作、依賴與最後檢視日。高風險項目可與功能版本一併處理，低風險項目則持續觀察；任何項目被接受延後，都需明列風險接受角色與再檢視條件。清冊與事件、弱點、效能及變更資料交叉分析，辨認重複故障或長期人工補救。

版本升級先盤點生命週期、相容性、弱點、授權、回復及測試成本。作業系統、資料庫、框架、容器映像、模型與套件不得因「最新」即直接升級，而應有影響分析、測試環境驗證、資安掃描、資料備份與回復演練。對停止支援或高風險元件，提出替代路徑與分期計畫；對仍受支援且穩定元件，維持必要修補及監控。

改進項目以效益、風險、成本、依賴與可回復性排序，並以試點結果而非工具宣傳作決策。驗收證據包括導入前基線、試點範圍、權限與稽核、資料可攜、故障處置、

回復及操作文件。試點未達預期時停止導入並保留既有流程，避免工具成為新的單點或資料孤島；達成條件者才進入版本、操作文件與移轉清冊。

3.6.3 保固運作與改進驗證

保固以結案版次、已知問題、服務窗口及月報口徑為基線。工單區分原功能缺失、環境資料、外部介接、操作協助、資安與新增需求，避免責任或時效被錯誤分類；同一事件由主工單整合最早通知與後續處置，關閉前由指定角色驗證業務可用。

月維護報告列服務狀態、回應與恢復或替代、版本、弱點、備份、重複問題、未結風險及下期工作。案件量、監控範圍或分類改變時標示資料時點與可比性；重要結論能回查工單、日誌、測試及版本，不以總件數取代影響分析。

問題管理從重複事件、人工繞路與趨勢辨認共因，區分觸發、根因、立即修復與永久改善。改善可涵蓋程式、組態、容量、監控、文件或訓練，並以原事件及相鄰情境再驗證；高影響技術債優先納入版本，接受延後者記錄控制、責任與再檢視。

工具資料在導入時規劃權限、稽核、匯出與備份，需求、工單、測試、程式及文件以共同識別連結。停止使用前核對資料、附件、關聯與保存再關閉帳號。技術建議同時列短期控制與長期選項，由機關依效益、風險、成本與時程決策。

保固結束前彙整事件、變更、技術債、弱點、文件及未結事項，逐項標示已關閉、已接受或已移交，並完成帳號、工具、資料與知識接續，使後續維運保有清楚責任與證據。

保固工單結案前由提出者或機關指定驗證人核對原情境、修正版本、資料影響與替代措施，不能重現者保留原因與監控方式。跨系統問題由主責工單連結外部處理紀錄，避免各方分別關閉卻仍留下業務中斷。每月再以重複率、逾期未結、回復次數與相鄰功能回歸結果辨識改善是否有效，相關紀錄納入維護報告及最終移轉清冊。

肆、管理建議

4.1 管理方法、監控機制與協作工具

管理方法以需求、時程、品質、風險、資安、變更及交付七條控制線為主，所有控制線使用一致的工作分解、責任、狀態、優先序、版次與證據欄位。決標次日起 10 個工作天內的專案工作計畫書建立範圍與管理基線，此後每月檢討實際進度、下期工作、問題、風險、品質、資安、變更及機關決策，不以報告產出取代問題解決。

日常管理由工作項目、工單、測試與版本狀態驅動，負責人更新完成度、阻礙、預計完成日及證據。週期監控由專案經理彙整里程碑差異、交付成熟度、重要缺失、介接依賴及資源衝突，跨工作包協調。每月檢討聚焦需機關核定的範圍、優先序、重大風險、變更、資安與交付事項，會議前提供狀態資料，會議後形成決議、責任與期限。

例外升級以影響而非職級判斷。涉及法遵或資料外洩、正式服務中斷、關鍵里程碑、不可回復資料、外部介接阻礙或跨單位決策者，立即通知專案經理與機關窗口並啟動相應程序；一般問題依工單及週期管理。所有升級需記錄事實、影響、已採控制、所需決策、選項與建議，避免只傳遞警示而缺乏可行動內容。

協作工具可支援任務、工單、文件、版控、測試及報表，但工具名稱不構成管理能力。權限依角色配置，重大刪除、權限或基線變更留存稽核；資料可匯出並定期備份，避免契約終了無法移轉。機關能以唯讀或核定角色查閱所需狀態，廠商內部管理資料則提供足以證明履約的摘要與證據。

三層節奏把日常事實逐步彙整成月度決策，並將核定事項向下轉回工作與驗證。日常層關注任務、工單、風險與版次，週期層比較進度、品質、測試及阻礙，月度層

處理里程碑、重大風險與變更；每一層都留下清單、紀錄與報告，不依賴口頭訊息，如圖 10 所示。



圖 10 治理層級、管理節奏與協作證據

管理會議的輸入與輸出需固定但不僵化。日常協作輸出可執行工單，週期檢視輸出跨組協調與偏差處置，月檢討輸出機關決議與基線變更；重大例外可跳過正常週期即時升級。會議紀錄連回原始工單、風險或變更，後續以責任、期限及關閉證據追蹤，如表 17 所示。

表 17 專案治理節奏與管理輸出

管理層級	主要輸入	檢視重點	輸出	升級條件
日常執行	任務、工單、測試、告警	責任、阻礙、下一步、證據	狀態更新、處置與新工單	服務、資安、資料或里程碑重大影響
週期監控	工作包進度、缺失、版本、依賴	偏差、資源、跨組衝突	協調方案、預測與議題升級	超出授權、需機關或外部單位決策

管理層級	主要輸入	檢視重點	輸出	升級條件
每月檢討	里程碑、風險、品質、資安、變更	完成度、趨勢、決策與下月計畫	月報、決議、責任與期限	基線、契約、重大風險或驗收影響
即時例外	事件事實、影響、控制與選項	控制擴散、復原、法遵與通報	指揮決策、處置節點、後續報告	依事件或資安程序持續升級

進度不以主觀完成百分比判斷，而以可驗證產出計算。例如需求完成需具追溯與審查，開發完成需具程式、測試與文件，缺失完成需複測關閉，交付完成需審查意見收斂。時程預測同時檢查關鍵依賴、未決事項及剩餘工作，避免大量標示「接近完成」卻無法進入下一閘門。

品質指標包含需求變動、測試通過、缺失分級與重開、文件意見、介接失敗及人工覆核差異；資安指標包含弱點、修補、複測、事件、稽核及演練改善。指標需有分母、資料時點、範圍與口徑版本，不同月份若工具、案例或分類改變，先揭露可比性限制再判讀。單一數值不直接決定獎懲，而是觸發查證及改善。

風險清冊至少記錄原因、事件、影響、可能性與衝擊評估、既有控制、應變、責任人、觸發條件、期限及殘餘風險。機會事項亦可列管，例如共用元件能同時改善多類案件，但需先驗證不造成回歸。重大風險每月檢討，已發生者轉為議題或事件，不在風險清冊中重複等待。

管理控制矩陣將每條控制線連到資料、責任、警戒與決策證據。警戒值可於工作計畫依實際基線核定，正文不臆造門檻；一旦觸發，專案經理提出原因、影響與選項，機關核定涉及範圍或優先序的處置。決策紀錄保存日期、參與者、事實、選項、結論、適用範圍及待辦，如表 18 所示。

表 18 專案控制線、監控資料與決策證據

控制線	監控資料	責任角色	觸發後動作	決策 / 驗收證據
需求	基線、未決、變更、追溯完整	系統分析師、機關窗口	澄清、影響分析、核定	需求書、追溯、決策與版本
時程	工作包、依賴、里程碑與剩餘工作	專案經理、各工作負責人	重排、增援、縮小批次或升級	進度表、差異、核定處置
品質	測試、缺失、重開與文件意見	品質 / 測試責任人	根因、修正、複測、阻擋發布	測試報告、缺失單、複測證據
資安	弱點、事件、稽核與演練	資安專責	控制、修補、通報、複測	檢測、事件、稽核及改善紀錄
變更	申請、影響、核准、版本與回復	專案經理、技術負責人	審查、排程、測試、發布	變更單、核准、版次與發布紀錄
交付	文件、程式、測試、清冊與意見	專案經理、文件負責人	內審、修正、審定與點交	交付清冊、審查、電子檔與 USB 紀錄

工作分解的最小管理單位必須能交付可檢查成果，例如一組核定需求及案例、一個具測試的介接版本或一份完成內審的文件，而非籠統的「持續開發」。各項成果設定零、進行中、可檢視、已核准及已交付等狀態，只有達到對應完成條件才列入進度；進行中工作另外呈現剩餘量、阻礙與預測，防止以投入時間誤認為完成。

里程碑預測從工作依賴、審查意見、缺失、外部介接及資源負荷推導。對固定截止日期，專案經理持續比較剩餘工作與可用時間，辨認最晚決策點；如發現資料、帳

號或外部測試未就緒，先建立可用模擬與替代工作，同時保留正式接通查核，不讓所有工作停等。預測變動需說明新事實、範圍及信心水準，原預測保留以檢討估算偏差。

決策與行動採唯一識別並連到會議、工單或風險。決策記錄適用範圍與生效版本，行動記錄責任、期限、完成證據及逾期處置；若後續事實推翻原決策，新增決策並保留關聯，不直接改寫歷史。月報抽查高影響決策是否已落實到需求、程式、測試、預算或文件，使治理輸出真正改變專案執行。

管理資料品質亦納入複核。無責任人、期限已過、狀態與證據矛盾、同一問題分散多筆或已關閉卻仍造成影響，均視為管理缺失並在週期檢視修正。工具中的狀態不是唯一真相，應與程式版次、測試、日誌與交付清冊交叉核對，讓預測及月檢討建立在可驗證事實上。 管理指標與原始證據之間需保留可追溯查詢，任何人工調整均註明原因、範圍及核准。月檢討後由專案經理抽查決議是否已更新工作、風險與版本，未落實者維持未結，確保會議結論不會脫離實際交付。

4.2 專案組織、人力規劃與運作方式

本案最低配置包含專案經理 1 人、系統分析師 1 人、系統設計師 2 人及資安安全專責 1 人，並應符合來源所定資歷與全職要求。組織設計以職能互補與責任可代理為重點，不以人數表取代工作負荷分析。人力配置需覆蓋需求、架構、影像與 AI、應用與介接、測試、資安、文件、上線、訓練及保固，尖峰期則依工作量調度必要支援。

專案經理對範圍、時程、品質、風險、溝通、變更與交付整體負責，是機關單一管理窗口；系統分析師負責現況、流程、資料、權限、介接與需求追溯；系統設計師負責架構、資料、應用、AI 整合、程式與技術文件；資安專責負責風險、控制、檢測、弱點、事件與佐證。測試與 AI 等工作可由符合工作計畫配置的人員支援，但驗證責任不得由開發者單獨自我核定。

機關專案窗口負責業務協調與核定，業務、資訊及資安角色依議題參與；廠商角色在授權範圍內提出事實、選項與建議，不代替機關作成應由機關負責的決策。跨角色活動採主責、核准、協作及知會的責任分類，例如需求由分析師主責、機關核准、設計與資安協作；發布由技術主責、機關核准、測試與資安提供證據。

代理機制需預先指定而非事件發生後臨時安排。代理人取得必要文件、工具與權限，參與週期檢視並能接續重要任務；正式權限只在代理期間開啟並於結束後撤除。人員異動時完成工作、風險、未決、帳號、設備、文件及知識清單，並由接手人以實作證明可承接，避免只以口頭交接。

角色關係以機關窗口及專案經理為治理主軸，分析、設計及資安職能共同支援需求、實作、測試與交付。最低人數是履約底線，實際排程仍依工作包與尖峰調度；圖中虛線代理與交接關係確保單一人員短暫不可用時，重要決策、資安與交付不失去責任歸屬，如圖 11 所示。



圖 11 專案角色、最低配置與責任協作關係

責任配置須避免同一活動無主責或多人同時核准。需求與優先序由機關決定，專案經理統籌履約，分析與設計角色分別負責情境規格及技術實作，資安角色保有獨立檢視；涉及正式資料、上線、變更或風險接受的決定仍由機關權責角色辦理。人員姓名、學經歷、工具經驗及資格證明依指定欄位與佐證呈現，正文不預設未經證明的能力。

人力計畫以工作包、期間與角色負荷估算，不只列全期人月。啟動與需求期需專案經理及分析師高投入，設計開發期由設計與 AI 相關人力承擔，測試與上線期增加測試、資安與文件整合，保固期維持事件、版本、資安與月報責任。每月比較計畫與實際投入、未完成工作及未來尖峰，若出現負荷集中，提前調整批次、支援或依賴。

關鍵工作至少有可接手角色與最新作業資產。需求有訪談紀錄、決策與追溯；程式有儲存庫、建置、組態與測試；AI 有模型、提示、案例與容量資料；資安有控制、弱點、事件與檢測；維運有監控、工單、備份及回復；文件有清冊、版次與審查狀態。這些資產定期由非原作者演練，才能證明知識不只存在個人記憶。

人員異動需評估對里程碑、權限、利益衝突、保密與持續性的影響。接替人員的資格依來源要求提出佐證，並完成並行、實作、缺口修正與機關溝通；舊帳號、憑證及設備於程序完成後調整。若關鍵角色短暫缺席，代理人依授權執行日常工作，但範圍、基線、正式發布或風險接受等重大決策仍遵循原核准層級。

持續性清單把工作資產、代理準備及異動證據連結。每個關鍵領域都需明確的主責、代理可用條件、最小交接資產與接手驗證；結果於月檢討呈現，不以「已有備援人員」的宣告取代實作。接手人若無法重現建置、測試或處置，缺口回到文件與訓練改善，如表 19 所示。

表 19 關鍵工作之人力持續性與交接證據

關鍵領域	主責職能	代理準備	最小交接資產	接手驗證
需求與流程	系統分析	參與訪談與週期檢視	基線、決策、追溯、未決清單	說明情境並完成影響分析
架構與程式	系統設計	具儲存庫及測試環境授權	架構、程式、建置、組態、測試	由核准版重建並執行回歸
地端 AI	AI 整合 / 系統設計	熟悉模型、提示及案例版本	映像、模型、提示、案例、容量紀錄	重現代表情境與回復版本
資安	資安專責	參與風險、檢測與事件演練	控制、弱點、檢測、事件、通報流程	完成抽查、事件桌上演練與證據彙整
維運保固	專案經理與技術角色	可接工單及監控	工單、監控、備份、回復、月報	模擬告警、處置、驗證與結案
文件交付	專案經理與各文件負責人	熟悉清冊及審查狀態	文件、版次、意見、點交清冊	核對程式、測試與文件一致性

工作計畫將角色所需能力對應到工作包及交付，不以職稱推定。專案經理需能整合需求、時程、風險與契約證據，分析師需能建立流程、資料與追溯，設計人員需能處理既有 Java 環境、資料庫、地端 AI 與介接，資安專責需能把風險轉為控制、檢測與改善。資格文件用來證明基本條件，實際能力再由過往佐證、面談或啟動任務與接手演練確認。

人力負荷按月與工作包檢視，區分計畫、實際及未來需求。若同一人同時承擔多個關鍵角色，需分析是否產生排程衝突或職務分離不足；開發者可以執行單元測試，

但不可單獨核准自身重大變更或安全風險，資安專責可協調修補，但檢測與風險接受仍需適當獨立性及權限。保固期間人力較精簡時，也要保留事件、版本、資安與月報的明確責任及代理。

績效評估以成果品質及責任履行為核心。角色工作連到需求完整、設計審查、程式與測試、缺失重開、資安改善、文件意見、事件時效及移轉缺口，並排除由外部依賴造成但已適當管理的影響。發現能力或負荷不足時，先調整工作、提供同儕複核、訓練或增加支援；涉及關鍵人員替換，依程序提出符合資格的接替資料、影響及交接證據。

會議與溝通亦遵守最小必要參與。業務規則由適當業務代表決定，技術設計由分析、設計及資安共同評估，正式上線與風險接受由具權限角色核定；未參與必要討論的人員透過決策紀錄及工作項目接收結果。這既避免所有人被大量會議占用，也防止關鍵決策只存在少數人口頭記憶。

團隊持續改善從缺失、估算偏差、重複工單、審查意見與移轉演練分析。問題若源於責任模糊，調整矩陣與流程；若源於知識集中，增加配對與接手；若源於工具或環境權限，完成授權與文件。改善結果在後續相同情境驗證，不能只以新增規定宣告完成。

4.3 策略規劃、專業顧問與需求治理

大型資訊專案的顧問能力表現在能否把業務問題、法遵限制、資料狀況、技術選項與履約時程轉為可核定決策，而不是提出無約束的技術清單。本案的策略主軸為地端 AI 可控導入、共用流程與差異配置、跨系統交易可追溯、資安內建及移轉可接手；每項主軸均以現況基線、試點、風險與證據逐步落實。

議題先描述現況、受影響角色、資料、頻率、例外與不處理後果，再確認哪些條件不可變、哪些可透過流程或技術調整。方案至少比較維持現況、最小改良及結構性改善，從效益、風險、成本、資安、時程、維護與移轉評估。資訊不足時可做原型、資料抽樣或介接試驗，但原型結果需標明環境與樣本限制，不直接等同正式容量與品質。

需求依來源、業務目標及驗收證據分類，設定唯一識別、優先序、依賴與責任。澄清結果進入需求基線，任何功能、欄位、規則、報表或介接變更均回到基線評估。對 AI 需求，額外確認輸入資料、允許任務、輸出結構、人工責任及停止條件；對介接需求，確認外部窗口、身分、欄位、狀態及對帳；對資安需求，確認控制、檢測及佐證。

顧問建議應同時呈現推薦方案與保留風險。機關可依政策與業務責任核定，廠商則將核定結果轉為工作、測試與交付；未採方案亦保存理由，避免相同議題重複討論。若新事實出現，透過變更重新比較，不把原決策視為不可調整。

決策閘門將議題依序經過事實限制、方案形成、五面向評估、原型或試驗及機關核定。任何階段未具備足夠證據，可補件、調整或暫緩；核准後納入需求基線，涉及既有承諾者再進變更控制。此流程使顧問判斷能被查核，也保留機關最終決策權，如圖 12 所示。

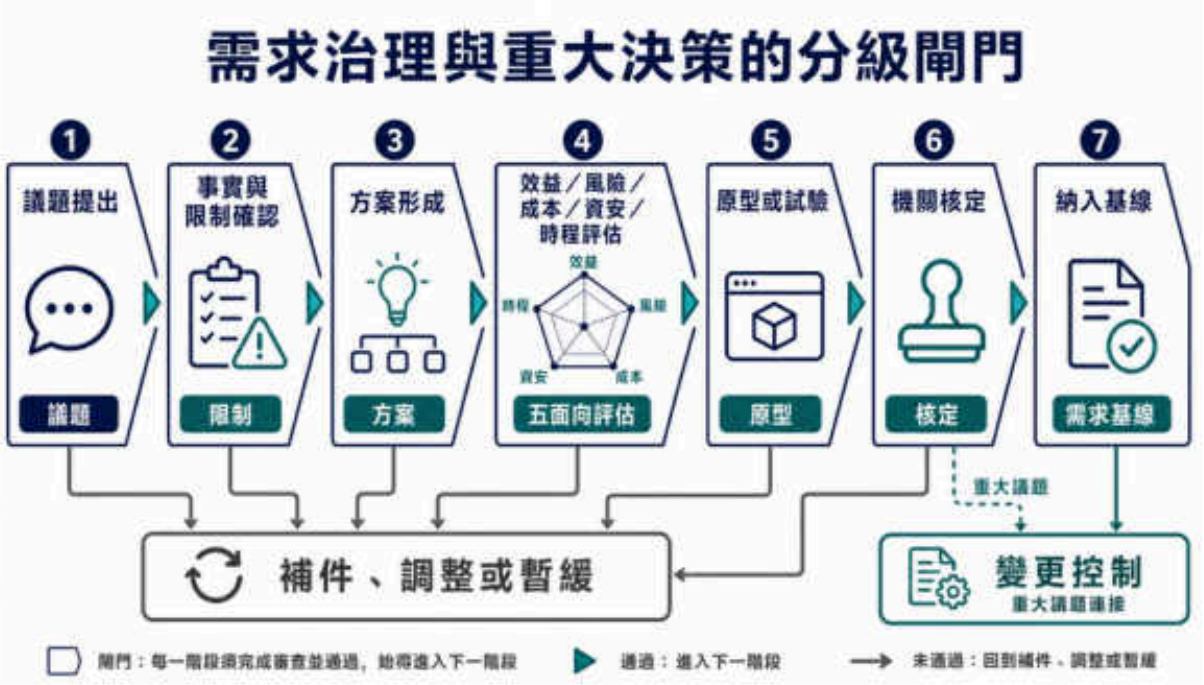

圖 12 需求治理與重大決策的分級閘門

重大決策紀錄至少包含問題、事實、限制、方案、五面向評估、試驗結果、推薦、核定與後續工作。評估不強行量化無可靠資料的因素，而以可查核證據及清楚假設呈現；不同資料時點需說明可比性。決策完成後更新需求、風險、時程、預算、測試與文件，確保建議真正落地，如表 20 所示。

表 20 重大需求與技術方案決策紀錄

決策欄位	應記錄內容	查核重點
問題與事實	現況、受影響角色、資料、頻率、例外	與基線及證據一致，不以假設代替事實
限制與目標	法遵、內網、相容、時程、可移轉與成功條件	不可變條件與可調整條件分離
方案與取捨	現況、最小改良、結構性改善及其他可行方案	效益、風險、成本、資安、時程均有比較
原型 / 試驗	範圍、資料、環境、步驟、結果與限制	不將小樣本直接外推為正式承諾

決策欄位	應記錄內容	查核重點
推薦與殘餘風險	採行理由、未解風險、控制與停止條件	風險接受角色及後續監控清楚
核定與落地	核定內容、適用範圍、責任、期限	需求、時程、測試、預算、風險及文件同步

策略路線以本案固定交付為界，先確保需求、核心功能、資安、上線、移轉與保固，再安排可在範圍內逐步改善的資料品質、案件配置、報表及維運工具。每項策略標明依賴、最小可驗證成果、停止條件及不採行後果；AI 能力不以追求更大模型為方向，而以地端相容、來源可追溯、人工負擔、資料保護與維運可控共同衡量。

顧問分析使用訪談、流程觀察、系統與資料盤點、工單、測試、日誌、樣本及法規等證據。不同資料來源若時間、範圍或口徑不一致，先分層呈現並說明限制；沒有足夠資料的判斷列出假設及驗證方法，不把經驗轉成無證據承諾。對高影響問題，可用原型或技術試驗降低不確定，但試驗須使用核准資料與環境，且有明確退出及清理。

方案評估包含功能符合、業務操作、資安法遵、資料治理、效能可靠、維運移轉、時程與成本。若某方案在單一面向表現較佳但使其他面向不可接受，顧問需提出緩解或替代，不以加權平均掩蓋阻擋風險。例如雲端模型可能帶來不同能力，但本案明定地端且不使用外部雲端推論，故不列為可採路徑；改以模型版本、提示、規則、硬體容量與人工流程的組合最佳化。

需求治理也處理負面需求與邊界情境，例如不得外送資料、不得暴露技術錯誤、未人工核准不得對外交易、權限不足不得查詢、版本不相容不得發布。這些限制轉為可執行測試及監控，不只寫在原則。顧問在每次重要審查核對正向功能與禁止行為是否同時落實，避免效率需求侵蝕控制。

策略建議經機關決策後建立落地追蹤，連到工作、責任、期限、成本影響、測試、風險及交付。若建議以設定或流程即可達成，不為展示技術而新增程式；若需要開發，先確認共用元件與回歸影響；若不採行，保留理由及再檢視觸發。月檢討關注已採行建議的實際結果與新事實，必要時調整路線但保留原決策脈絡。

專業諮詢輸出可包括議題簡報、決策紀錄、風險評估、資料分析、原型結果與實施建議，但每份輸出都需有明確決策用途。遇到資安事件、重大弱點或外部介接政策變動時，先提供事實、影響、立即控制及選項，後續再補完整分析；一般改善則以足夠資料避免頻繁改向。這種分級回應使顧問能力既能支援即時決策，也能保持可稽核與可落地。 顧問服務須能處理相互衝突的目標。例如提高模型輸出量可能增加人工查核負荷，增加日誌有助稽核卻可能擴大敏感資料，強制即時介接可能降低外部中斷時的韌性。分析時明列衝突、不可妥協控制及替代，透過資料最小化、結構驗證、佇列、遮蔽或分批上線取得平衡，不以單一技術指標替機關作決策。

建議的實施順序優先處理信任邊界、資料與需求基線，再完成共用核心、代表案件及介接契約，後續擴增差異類型、報表、移轉與保固。每階段都能交付可驗證成果，且前期決策能透過案例被挑戰；若事實顯示原方案不可行，依決策紀錄回到相應閘門，而非到期末才整體改寫。

4.4 工作時程、交付產品與重要查核點

工作時程以決標次日為第 1 週，將啟動、需求、設計、開發、資安、測試、上線、移交、驗收及保固安排為 98 週控制範圍。115 年 3 月 31 日、6 月 30 日及 9 月 30 日為固定交付截止，實際對應週次由決標日校準；排程中的週次用於工作依賴與資源管理，不改變固定日期義務。保固持續至 116 年 12 月 31 日，最後一期月維護報告於 117 年 1 月 5 日前提出。

時程基線不只列工作起訖，還需標明輸入、責任、前置依賴、輸出、查核人與完成證據。啟動工作計畫定義全案基線；需求確認報告控制設計與測試範圍；第二期以運轉測試、程式碼及資安檢測證明可部署程度；第三期整合結案、規格、手冊、資安報告與程式碼；保固月報持續呈現服務、事件、變更與風險。任何延期預測均先分析關鍵依賴與補救選項，再由相應權限核定。

各期文件在正式提交前先做內容、版次、引用、敏感資訊與清冊複核。程式原始碼及目的碼需能對應建置版次，測試報告需對應需求與執行環境，資安報告需對應掃描標的、版本與修補狀態，手冊需對應實際畫面及操作。這些交叉一致性是交付成熟度的核心，不能由單一文件已完成取代，如表 21 所示。

表 21 工作時程、交付產品與相依關係

階段	主要工作	交付產品	關鍵相依	完成證據
啟動	編組、盤點、工作計畫與管理基線	名冊、工作計畫、保密文件	決標、窗口與環境可進入	核定計畫、權責、清冊與會議紀錄
第 1 期	訪談、流程、資料、介接與驗收分析	需求確認報告	現況及業務規則可追溯	需求基線、未決、追溯與審查意見
第 2 期	設計、開發、整合、資安及運轉測試	運轉測試、程式原始碼及目的碼、資安檢測	需求基線、測試環境與介接條件	測試、缺失、建置版次與修補複測
第 3 期	上線修正、訓練、移轉、結案整編	結案、設計規格、安裝維護與操作手冊、資安報告、程式碼	主要缺失關閉、文件同版	審定版、交付清冊、接手實作與點交

階段	主要工作	交付產品	關鍵相依	完成證據
保固	監控、事件、變更、弱點與諮詢	每月維護報告、月工作報告	結案基線及服務窗口	工單、版本、檢測、風險及月報
保固末期	未結事項收斂與服務狀態移交	最後一期月維護報告	保固資料完整	未結清單、最終狀態與報告交付

查核點使用進入條件、檢查活動、退出條件與證據四欄，並依缺失影響決定通過、附條件通過或不通過。附條件通過只適用不影響下一階段核心工作的事項，須有責任、期限與再查核；涉及資料正確、資安重大風險、無回復能力或交付缺漏者不得以附條件方式掩蓋。查核結果同步更新時程、風險及付款相關資料，如表 22 所示。

表 22 重要查核點與進退場條件

查核點	進入條件	查核活動	退出條件	證據與後續
工作計畫核定	團隊、範圍及環境資訊齊備	檢查工作包、責任、時程、品質、資安與溝通	基線可執行、缺漏已補正	核定版、清冊、議題與期限
需求基線	訪談、現況與介接盤點完成	情境走查、原型、欄位與驗收追溯	需求可測、未決可控	需求報告、追溯、核定與未決清單
測試與資安放行	主要功能、環境及案例就緒	單元、整合、壓力、運轉及資安檢測	阻擋缺失關閉、殘餘風險有核定	報告、缺失、修補複測、版本清冊
上線與回復	核准版、備份及窗口就緒	上線檢核、冒煙測試、監控及回復演練	業務情境可用、監控正常	上線單、測試、監控、回復及核准

查核點	進入條件	查核活動	退出條件	證據與後續
結案與移轉	文件、程式、教材與清冊齊備	版次核對、接手實作、缺失與資產盤點	審定、可接手、未結事項列管	點交、USB、簽認、未結清單
保固結束	月報、工單、變更及風險資料完整	服務狀態、未結事項與最終報告檢查	責任與資產狀態清楚	最後一期報告、清冊與結束紀錄

第 1 至 9 週集中在編組、工作計畫、環境盤點、業務訪談、需求追溯與初步設計，影像與 AI 開發自第 8 週開始銜接。第 2 週的工作計畫與第 7 週的需求報告為早期查核點，前者確立治理基線，後者控制後續設計範圍；若訪談或介接資料延誤，需先以未決清單及不受影響工作維持進度，再把影響納入月檢討，如圖 13 所示。

履約工作甘特圖（系統擴充及保固）

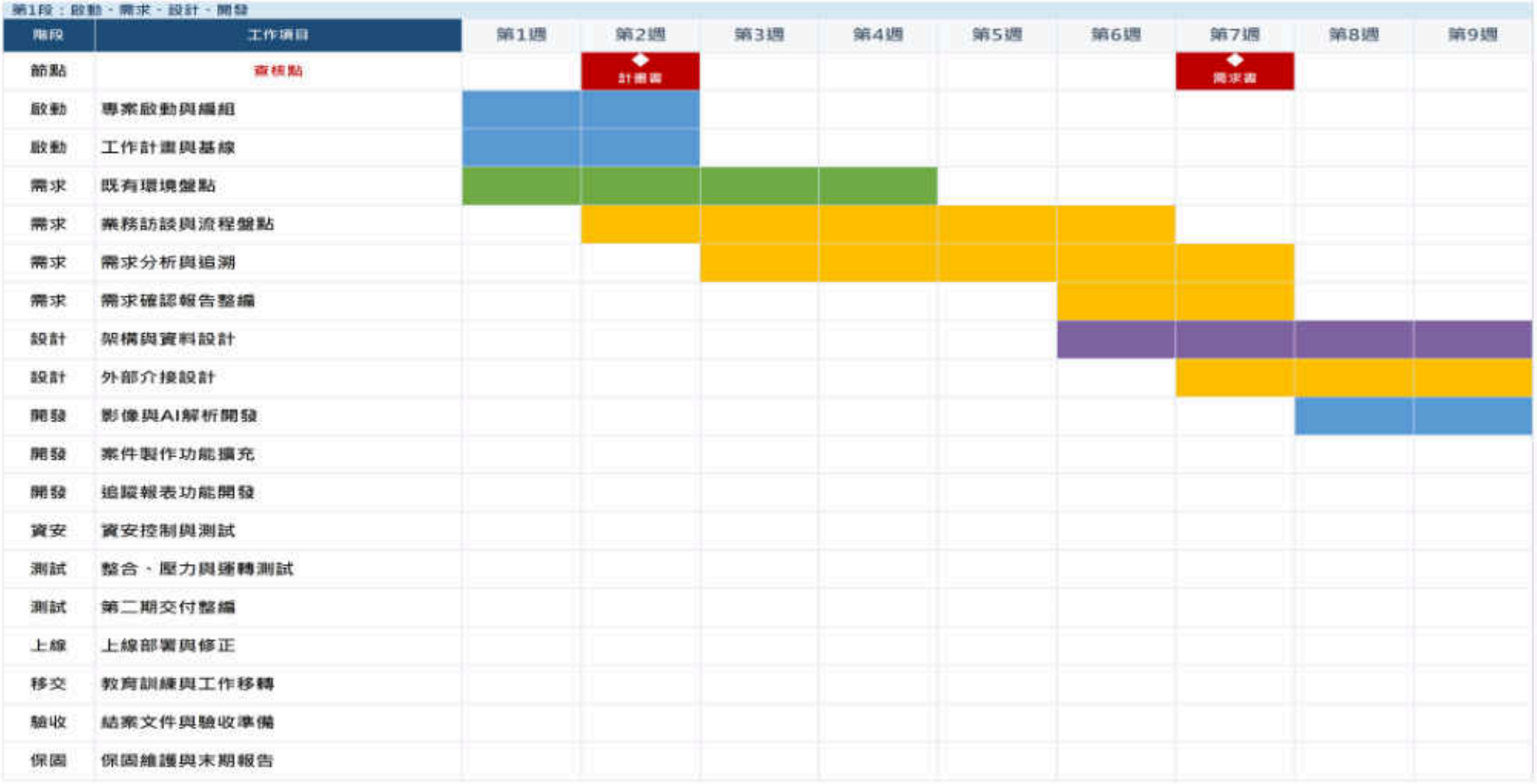

圖 13 履約工作甘特圖（系統擴充及保固）（一）：第 1 至 9 週

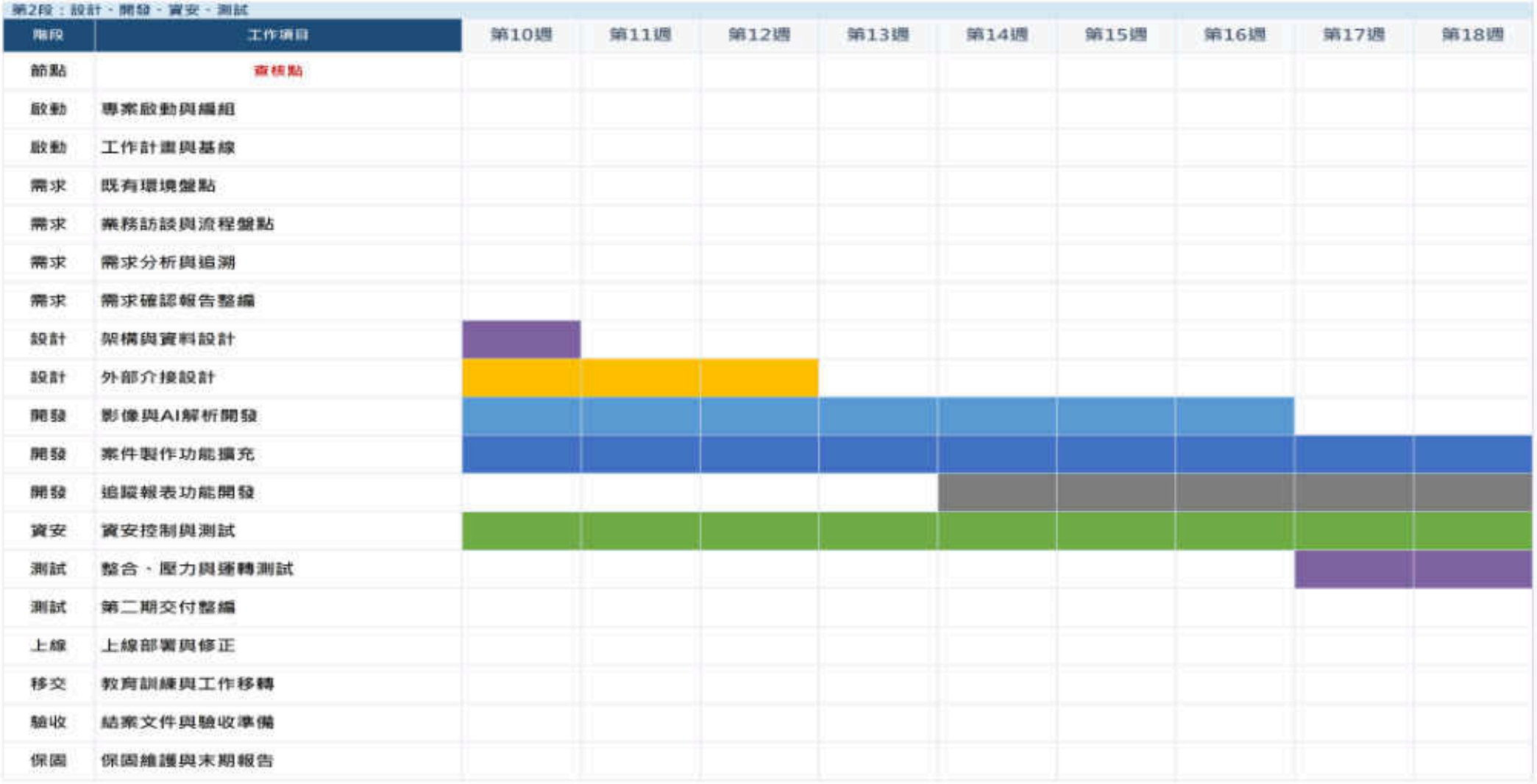

圖 14 履約工作甘特圖（系統擴充及保固）（二）：第 10 至 18 週

履約工作甘特圖（系統擴充及保固）

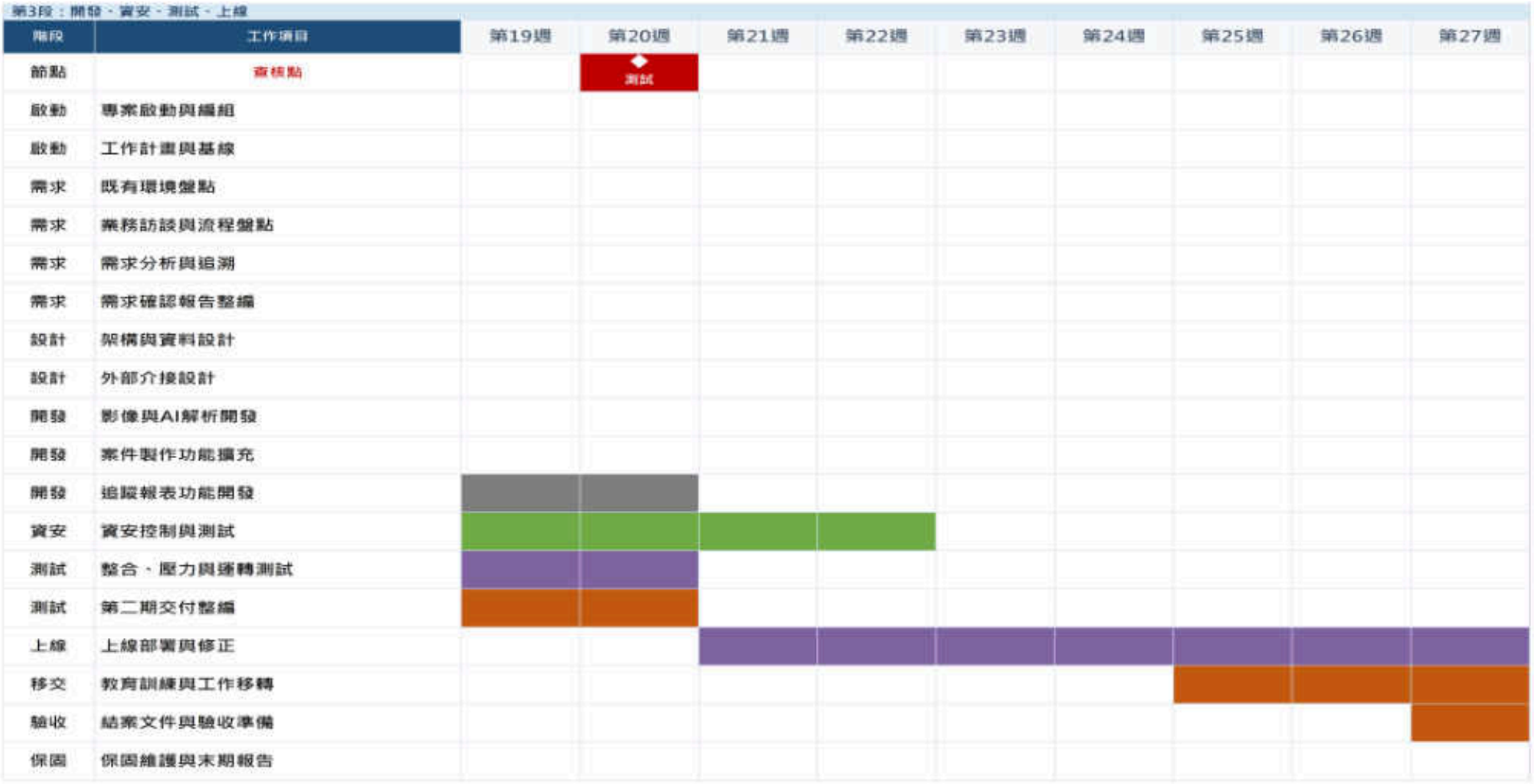

圖 15 履約工作甘特圖（系統擴充及保固）（三）：第 19 至 27 週

履約工作甘特圖（系統擴充及保固）

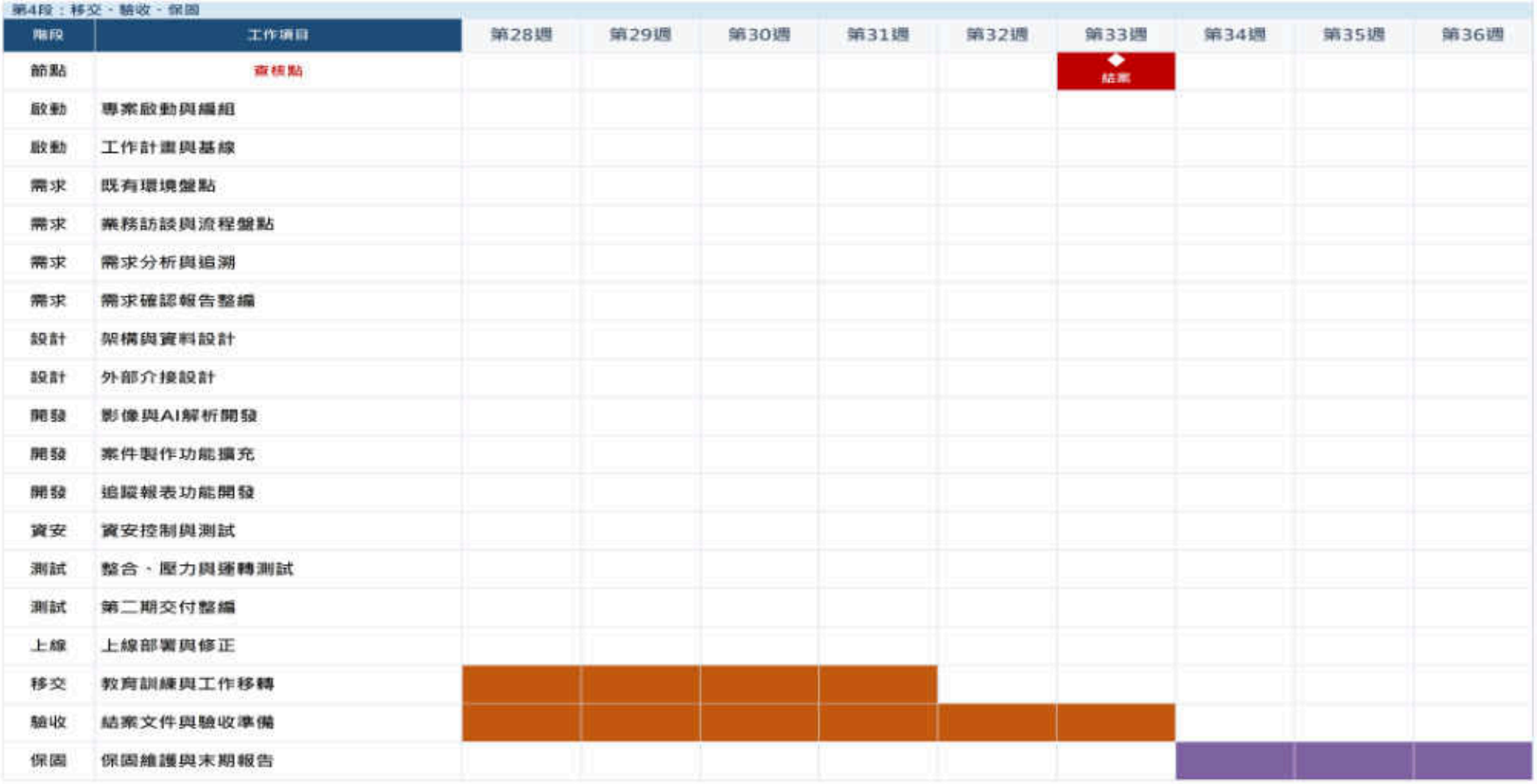

圖 16 履約工作甘特圖（系統擴充及保固）（四）：第 28 至 36 週

第5段：保固

階段	工作項目	第37週	第38週	第39週	第40週	第41週	第42週	第43週	第44週	第45週
節點	查核點									
啟動	專案啟動與編組									
啟動	工作計畫與基線									
需求	既有環境盤點									
需求	業務訪談與流程盤點									
需求	需求分析與追溯									
需求	需求確認報告整編									
設計	架構與資料設計									
設計	外部介接設計									
開發	影像與AI解析開發									
開發	案件製作功能擴充									
開發	追蹤報表功能開發									
資安	資安控制與測試									
測試	整合、壓力與遷轉測試									
測試	第二期交付整編									
上線	上線部署與修正									
移交	教育訓練與工作移轉									
驗收	結案文件與驗收準備									
保固	保固維護與末期報告									

圖 17 履約工作甘特圖（系統擴充及保固）（五）：第 37 至 45 週

履約工作甘特圖（系統擴充及保固）

第6段：保固

階段	工作項目	第46週	第47週	第48週	第49週	第50週	第51週	第52週	第53週	第54週
節點	查核點									
啟動	專案啟動與編組									
啟動	工作計畫與基線									
需求	既有環境盤點									
需求	業務訪談與流程盤點									
需求	需求分析與追溯									
需求	需求確認報告整編									
設計	架構與資料設計									
設計	外部介接設計									
開發	影像與AI解析開發									
開發	案件製作功能擴充									
開發	追蹤報表功能開發									
資安	資安控制與測試									
測試	整合、壓力與遷轉測試									
測試	第二期交付整編									
上線	上線部署與修正									
移交	教育訓練與工作移轉									
驗收	結案文件與驗收準備									
保固	保固維護與末期報告									

圖 18 履約工作甘特圖（系統擴充及保固）（六）：第 46 至 54 週

第7段：保固

階段	工作項目	第55週	第56週	第57週	第58週	第59週	第60週	第61週	第62週	第63週
節點	查核點									
啟動	專案啟動與編組									
啟動	工作計畫與基線									
需求	既有環境盤點									
需求	業務訪談與流程盤點									
需求	需求分析與追溯									
需求	需求確認報告整編									
設計	架構與資料設計									
設計	外部介接設計									
開發	影像與AI解析開發									
開發	案件製作功能擴充									
開發	追蹤報表功能開發									
資安	資安控制與測試									
測試	整合、壓力與遷轉測試									
測試	第二期交付整編									
上線	上線部署與修正									
移交	教育訓練與工作移轉									
驗收	結案文件與驗收準備									
保固	保固維護與末期報告									

圖 19 履約工作甘特圖（系統擴充及保固）（七）：第 55 至 63 週

第8段：保固

階段	工作項目	第64週	第65週	第66週	第67週	第68週	第69週	第70週	第71週	第72週
節點	查核點									
啟動	專案啟動與編組									
啟動	工作計畫與基線									
需求	既有環境盤點									
需求	業務訪談與流程盤點									
需求	需求分析與追溯									
需求	需求確認報告整編									
設計	架構與資料設計									
設計	外部介接設計									
開發	影像與AI解析開發									
開發	案件製作功能擴充									
開發	追蹤報表功能開發									
資安	資安控制與測試									
測試	整合、壓力與遷轉測試									
測試	第二期交付整編									
上線	上線部署與修正									
移交	教育訓練與工作移轉									
驗收	結案文件與驗收準備									
保固	保固維護與末期報告									

圖 20 履約工作甘特圖（系統擴充及保固）（八）：第 64 至 72 週

第9段：保固

階段	工作項目	第73週	第74週	第75週	第76週	第77週	第78週	第79週	第80週	第81週
節點	查核點									
啟動	專案啟動與編組									
啟動	工作計畫與基線									
需求	既有環境盤點									
需求	業務訪談與流程盤點									
需求	需求分析與追溯									
需求	需求確認報告整編									
設計	架構與資料設計									
設計	外部介接設計									
開發	影像與AI解析開發									
開發	案件製作功能擴充									
開發	追蹤報表功能開發									
資安	資安控制與測試									
測試	整合、壓力與遷轉測試									
測試	第二期交付整編									
上線	上線部署與修正									
移交	教育訓練與工作移轉									
驗收	結案文件與驗收準備									
保固	保固維護與末期報告									

圖 21 履約工作甘特圖（系統擴充及保固）（九）：第 73 至 81 週

第10段：保固

階段	工作項目	第82週	第83週	第84週	第85週	第86週	第87週	第88週	第89週	第90週
節點	查核點									
啟動	專案啟動與編組									
啟動	工作計畫與基線									
需求	既有環境盤點									
需求	業務訪談與流程盤點									
需求	需求分析與追溯									
需求	需求確認報告整編									
設計	架構與資料設計									
設計	外部介接設計									
開發	影像與AI解析開發									
開發	案件製作功能擴充									
開發	追蹤報表功能開發									
資安	資安控制與測試									
測試	整合、壓力與遷轉測試									
測試	第二期交付整編									
上線	上線部署與修正									
移交	教育訓練與工作移轉									
驗收	結案文件與驗收準備									
保固	保固維護與末期報告									

圖 22 履約工作甘特圖（系統擴充及保固）（十）：第 82 至 90 週

履約工作甘特圖（系統擴充及保固）

第11段：保固

階段	工作項目	第91週	第92週	第93週	第94週	第95週	第96週	第97週	第98週
節點	審核點								◆ 保固末期
啟動	專案啟動與編組								
啟動	工作計畫與基線								
需求	既有環境盤點								
需求	業務訪談與流程盤點								
需求	需求分析與追溯								
需求	需求確認報告整編								
設計	架構與資料設計								
設計	外部介接設計								
開發	影像與AI解析開發								
開發	案件製作功能擴充								
開發	追蹤報表功能開發								
資安	資安控制與測試								
測試	整合、壓力與還轉測試								
測試	第二期交付整編								
上線	上線部署與修正								
移交	教育訓練與工作移轉								
驗收	結案文件與驗收準備								
保固	保固維護與末期報告								

圖 23 履約工作甘特圖（系統擴充及保固）（十一）：第 91 至 98 週

第 10 至 18 週進入架構、介接、影像 AI、案件功能及資安控制的平行實作期。案件製作自第 10 週展開，追蹤報表於第 14 週加入，資安活動自第 10 週持續到第 22 週，顯示資安並非期末一次檢測；週期查核應特別比較共用資料模型、權限與介接規格是否一致，並以程式版次、測試及風險紀錄支撐整合，如圖 14 所示。

第 19 至 27 週由開發轉入整合、壓力、運轉測試、第二期交付、上線部署與修正。第 20 週對應運轉測試、程式碼及資安檢測成果，之後才能依核准版本進行上線；教育訓練與移轉自第 25 週起步，可把測試及上線發現同步納入教材。這一段的決策重點是阻擋缺失、回復能力及文件版次一致，如圖 15 所示。

第 28 至 36 週承接訓練、工作移轉、結案文件、驗收準備與保固啟動，第 33 週為第三期結案成果節點，第 34 週起保固維護進入長期執行。此段必須完成程式、規格、手冊、資安報告與清冊的同版核對，並由接手人員進行操作或維護實作；若仍有不阻擋驗收的事項，需列明責任、期限、風險與查核方式，不得在移交後失去追蹤，如圖 16 所示。

第 37 至 45 週已進入保固穩定期，工作主軸從大量功能交付轉為事件、監控、問題、弱點、版本與月報。月報應以結案基線比較實際服務狀態，列出通知、回應、恢復或替代、根因及改善，不因開發期結束而降低證據要求；若發生新增需求，須與保固缺失分開分類並進入變更程序，如圖 17 所示。

第 46 至 54 週保固工作持續，應用累積工單與監控資料辨認重複事件、資源趨勢及操作困難。單月無重大事件不代表風險消失，仍需查核備份、帳號、憑證、套件弱點與未結變更；跨月比較須保持相同分類口徑，若監控或案件量改變則標明資料時點與可比性限制。查核結果形成改善與下月追蹤，如圖 18 所示。

第 55 至 63 週仍以保固維護為連續工作包，管理上須避免長期任務只留一條色帶而缺乏月度成果。每月應有事件與服務摘要、版本與變更、資安檢測或修補、備份狀態、風險及下期計畫，並從高影響工單抽查原始證據；若根因改善跨月，保留責任與期限直至複測關閉，使營運資料可支持期末交代，如圖 19 所示。

第 64 至 72 週的保固活動應同時檢視系統版本與環境生命週期，辨認作業系統、資料庫、框架、容器映像、模型及套件的支援與弱點狀態。必要修補先做影響分析、備份、測試與回復準備，再依核准時段發布；因不同版本或掃描基準的檢測結果不可直接相比，月報需列標的、版本、工具基準與複測關聯，如圖 20 所示。

第 73 至 81 週持續維護時，須以代表性情境檢查文件與實際系統是否同步，特別是帳號權限、備份復原、模型提示、介接錯誤與報表口徑。若期間有正式變更，操作與維護手冊、版本清冊、測試及資安證據隨發布更新；接手人可依文件抽查處置，發現缺口立即回補。這使知識移轉不是結案時一次活動，而是保固中的持續控制，如圖 21 所示。

第 82 至 90 週接近保固末期，需開始彙整全期版本、工單、弱點、風險、備份、文件及未結事項，並辨認哪些事項可於保固內關閉、哪些需以明確狀態移交。彙整不是提前結束服務，日常回應與維護仍持續；期末資料須能回溯到原始工單與證據，避免只提供總數而無法判讀影響、根因及改善成效，如圖 22 所示。

第 91 至 98 週完成保固服務收斂，第 98 週對應 116 年 12 月 31 日保固屆期及 117 年 1 月 5 日前最後一期月維護報告。最終報告需區分已關閉、已移交與仍有外部依賴的事項，列明服務狀態、程式與文件最新版、帳號設備處置、風險及證據位置；保固期滿不應造成監控、權限或知識斷點，相關責任依核定清冊完成移交，如圖 23 所示。

排程每次更新均保留核定基線、實際開始完成、剩餘期間、依賴與預測完成，不以覆寫原計畫隱藏偏差。固定交付日與里程碑維持不變，週次映射在決標日確定後校準；工作提前或延後時，先檢查是否改變審查、測試、資安或移轉所需時間。只有具證據的完成項目才能關閉，外部等待與內部阻礙分別呈現。

資源平衡以角色可用量與工作相依為基礎。分析、設計、AI、介接、測試及資安工作在中期重疊，排程需避免同一人同時成為多個關鍵路徑；可透過分批案件、先完成共用元件、提早準備案例及並行文件降低尖峰。若增加人力，仍需預留進入環境、理解基線與同儕複核，不能把人數增加直接等同產能。

交付預警至少檢查需求未決、外部介接、測試環境、阻擋缺失、資安檢測、文件意見、接手實作與審定週期。預警發生時，列出對固定日期、付款與後續階段的影響，提出可並行、不影響品質的補救與需機關決策事項；解決後保留原因與實際成效，供後續估算改善。保固長期工作則以月報與工單為週期成果，避免排程只有一條長工項而無法判斷履行狀態。 甘特圖基線與詳細工作清單使用共同識別，圖中長工項仍由週期成果、月報或查核點證明。每次更新保留原始基線及變更理由，固定日期、週次校準與實際完成分欄呈現，使機關可判斷偏差而非只看到最新圖面。

4.5 品質保證、測試與驗收管理

品質保證從需求可測性開始，貫穿設計檢視、程式檢查、單元與整合測試、壓力與運轉測試、資安檢測、文件審查及驗收。每一階段先定義進入與退出條件，再以獨立證據判斷是否可進下一階段；開發完成但未測試、測試通過但版本不一致、文件齊全但無法重現，都不視為可交付成果。

品質計畫在工作計畫中明列品質目標、角色、檢視活動、測試層級、缺失分級、發布與交付閘門、證據格式及抽查方式。系統分析師確保需求與驗收可追溯，設計人

員確保架構與程式符合基線，測試角色以核准案例驗證，資安專責執行安全檢視，專案經理控制版本與交付完整性。機關依業務情境審查與驗收，不承擔廠商內部品質責任。

單元測試檢查函式、類別、規則與錯誤處理；整合測試檢查資料庫、AI 服務、SSO 與外部介接；系統及運轉測試檢查端到端案件、角色、報表、效能、備份及可維運性；驗收確認則對應核定需求與交付清冊。重大變更在實作前完成雛型展示與確認，正式發布前完成壓力測試，並依其資安影響安排上線前與上線後檢測。

測試環境、資料、版本與預期結果均受控。測試資料涵蓋標準、邊界、異常、權限及復原情境，敏感資料採授權、去識別及最小化；測試失敗建立缺失，記錄重現步驟、預期、實際、影響、環境與證據。修正後由適當角色複測並執行受影響回歸，不由同一提交紀錄直接宣告關閉。

V 模型使需求與驗收、系統設計與系統測試、模組設計與整合 / 單元測試形成對應，需求變更可找到受影響案例，缺失也能回查需求與設計。重大變更的雛型、壓力與安全檢測作為額外閘門，底部的缺失、修正、再測與關閉則保證問題不在層級間遺失，如圖 24 所示。

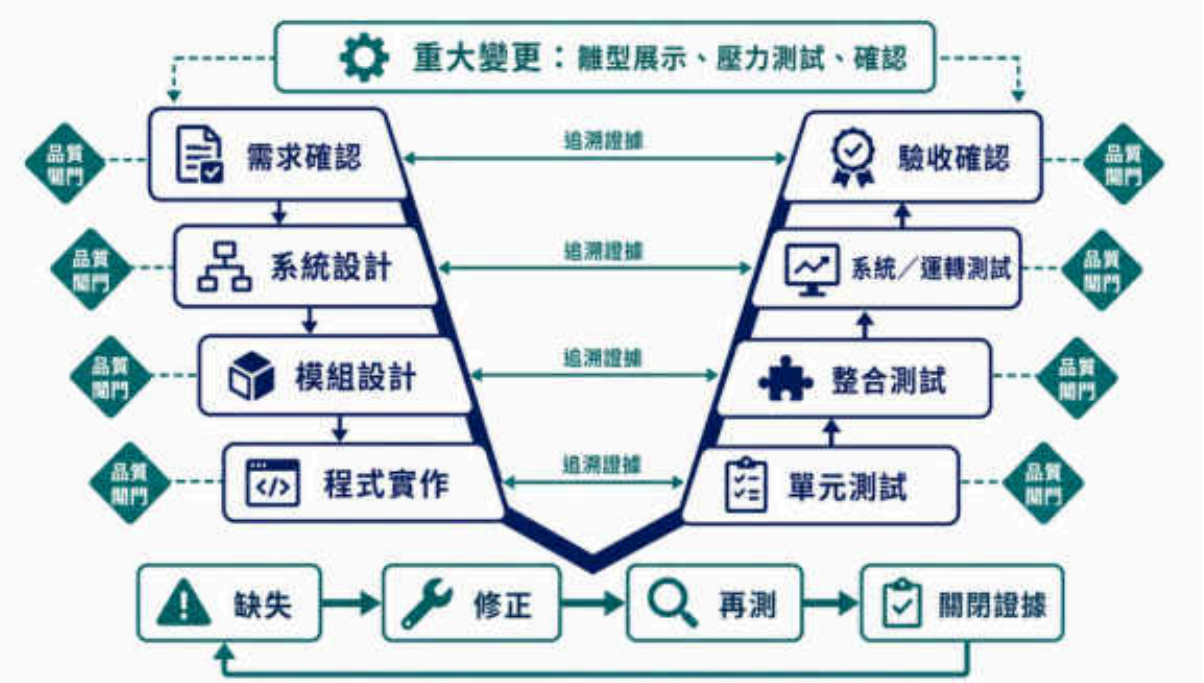

圖 24 需求、設計、測試與驗收證據 V 模型

各測試層級需有明確責任與放行證據。單元通過不足以證明跨服務交易，整合通過不足以證明業務端到端可用，系統測試通過亦不足以取代機關驗收；相反地，驗收中發現的缺失也要回到相應設計、程式及回歸案例，避免只在畫面修補，如表 23 所示。

表 23 測試層級、範圍與放行證據

層級	驗證範圍	主要情境	放行條件	證據
靜態與單元	程式、規則、輸入、錯誤處理	正常、邊界、例外與安全規則	阻擋問題修正，重要邏輯可重現	檢查、案例、結果與版次
整合	資料庫、AI、SSO、API 與介接	交易、逾時、重送、權限、資料一致	介面契約與錯誤復原通過	整合結果、日誌、對帳與缺失
系統／運轉	端到端案件、報表、效能、維運	16 類案件、角色、壓力、備份復原	核心流程可用、重大風險受控	運轉、壓力、復原與資安報告

層級	驗證範圍	主要情境	放行條件	證據
重大變更	高影響功能、架構或資料變動	雛型、壓力、上線前後安全檢測	機關確認、可回復、檢測完成	原型、核定、測試與檢測證據
驗收	核定需求、交付物及接手能力	業務情境、文件、程式與移轉	需求符合、缺失處置及清冊完整	驗收紀錄、交付清冊、簽認與未結事項

缺失依業務、資料、資安、服務及交付影響分級，分級決定處置順序與發布限制。每筆缺失有唯一識別、來源案例、影響範圍、重現步驟、根因、修正版本、複測與關閉依據；無法重現也須保存環境與查證結果，不以「未再發生」直接結案。重開或重複缺失進入根因與品質改善。

文件品質採作者自檢、同儕檢視、跨文件一致性及交付複核。需求、設計、程式、測試、資安、手冊與清冊共享版本及基線關係；使用操作手冊的畫面與欄位須對應核准版本，安裝維護手冊的組態、備份、監控與回復須經實作。文件含敏感設定時，公開操作內容與受控維運內容分級管理。

驗收前建立需求—功能—測試—缺失—交付追溯報告，逐項說明符合、部分符合或不適用及依據。不適用需有核准理由，部分符合需有影響、替代、責任與期限。機關驗收發現的事項進入同一缺失流程，修正後提交差異與複測；所有最終文件與程式重新產生清冊與完整性資訊。

驗收矩陣將功能、資料、介接、資安、效能、維運及文件證據集中比對。核心決策在於證據能否重現核定版本，而非文件數量；若測試標的、程式版次、手冊畫面或資安掃描標的不一致，即使各自存在仍不得視為完整。查核結果需回到缺失、變更與交付清冊直到關閉，如表 24 所示。

表 24 驗收面向與完整性判定

驗收面向	查核內容	完整證據	常見不完整情形	處置
功能與流程	核定情境、角色、例外與狀態	追溯、案例、結果、操作紀錄	只測正常路徑或無需求對應	補案例、修正、回歸與複測
資料與 AI	欄位、來源、版本、覆核與歷史重現	資料字典、候選 / 核准差異、案例	模型輸出無來源或核准軌跡	阻擋正式流程並補控制
介接	身分、交易、錯誤、對帳與重送	規格、交易日誌、整合與復原測試	只以技術成功判斷業務完成	補對帳、冪等及失敗情境
資安	組態、權限、弱點、滲透與修補	標的版次、報告、複測、風險核定	掃描版本與交付版本不同	重新檢測或完成差異評估
效能與維運	尖峰、監控、備份、回復、事件	壓力、監控、演練、工單與月報	無代表資料或只看服務存活	重建情境並驗證業務可用
文件與移轉	文件同版、清冊、接手操作	審定文件、程式、USB、實作與簽認	文件無法重現建置或排錯	修訂並由接手人再次實作

測試資料管理建立資料來源、授權、用途、敏感等級、去識別、預期結果、版本與處理期限。基準集用於版本比較，挑戰集涵蓋異常與攻擊，驗收集則依機關核定情境執行；三者目的不同，開發人員不得反覆針對驗收集調整到失去代表性。資料若因業務或法規無法長期保存，保留產生方法、結構及必要摘要，使後續仍能重現同等情境。

測試環境需記錄應用、資料庫、容器、模型、提示、規則、介接模擬、作業系統及組態。結果若來自不同環境或資料時點，報告明列差異，不能把測試環境的效能或正式環境的單筆觀察直接互相比較。重大測試前凍結候選版，缺失修正後產生新版並重跑受影響案例，避免同一報告混合多個未標示版本。

品質度量以決策用途設計。需求追溯完整度用於辨認無測試需求，缺失重開用於辨認根因或複測不足，人工覆核差異用於辨認資料、模型或介面問題，介接失敗用於辨認對帳與外部依賴，文件意見則用於辨認版次或內容缺口。每項度量有分母、排除、資料時點與口徑版本；數值觸發分析，不單獨取代實際缺失影響。

缺失分級由業務與技術共同判定。資料錯置、越權、重複正式交易、無法回復及高風險弱點，即使發生頻率低仍可能阻擋；排版或低影響提示則可依優先序處理。爭議分級保留雙方事實、替代控制與核定，未解爭議不得以降低等級關閉。缺失的根因分類涵蓋需求、設計、程式、資料、環境、測試、文件與操作，改善應對準確原因。

文件稽核以抽樣步驟驗證內容，而不只校對文字。從安裝手冊抽一組建置與回復，從操作手冊抽一個正常及例外案件，從設計規格抽一個介接或資料欄位，從資安報告抽一項弱點到修補版，從交付清冊抽一個程式與目的碼關聯。無法依文件重現者建立缺失，修訂後由非原作者再做一次實作。

驗收前進行完整性審查，檢查需求、版本、程式、測試、資安、文件、教材、清冊、USB 及未結事項。交付檔案採一致命名、版次與完整性資訊，敏感資料依分級包裝；審查意見逐項完成處置，並由差異及版本紀錄連結更新後的需求、程式、測試或文件，避免只提交新檔而無變更說明。最終審定版進入移轉及保固基線，後續變更延續相同品質與證據規則。 品質保證另建立抽查計畫，依風險選取高影響欄位、特權操作、AI 例外、外部交易、重大變更與復原，不只抽取成功案例。抽查發現證據缺漏時，

先判斷控制是否未執行或只是紀錄不足；前者需立即控制及重做，後者補證仍須能由原始資料重現，不能事後創作紀錄。

4.6 變更管理、版本控制與移轉交接

變更管理適用需求、流程、欄位、定型稿、程式、AI 模型與提示、資料庫、介接、組態、權限、資安控制及文件。任何會改變核定基線、正式資料或服務風險的事項先提出變更申請，記錄原因、範圍、效益、風險、成本、時程、測試、發布與回復；緊急變更可先控制影響，但仍需依程序補齊核准、證據與事後檢討。

變更審查比較不變更後果、替代方案及相依影響，確認是否屬契約範圍、是否影響交付日期、資安、資料、介接及使用者。核准後建立實作任務與版本關聯，未核准變更不得混入正式發布。低風險標準變更可依預先核准程序執行，但其適用條件、測試與回復仍須明確；超出條件即轉一般或重大變更。

版本控制涵蓋程式、資料庫結構、組態範本、容器映像、模型、提示、規則、定型稿與文件。發布清冊列出各元件版本、提交或雜湊、相容關係、建置環境、測試結果、已知限制與回復版；敏感秘密不納入版本庫，而由受控機制注入。資料庫變更需有向前與回復腳本、備份及資料檢核，避免程式回復但資料已不可逆。

發布前核對核准變更、程式審查、測試、資安、文件、備份、監控、窗口與回復條件；發布後執行冒煙與關鍵業務情境，觀察錯誤、資源、介接及資料一致。達到停止條件即控制新交易並依回復計畫處理，不以持續嘗試延長影響。發布結果與實際版本回寫清冊及工單。

端到端追溯鏈把變更申請、影響分析、核准排程、提交建置、測試、發布、部署回復、文件同步及原始碼與目的碼移轉連在一起。每個節點都能回查需求、版次及證

據，避免程式已變更但測試、手冊或資安檢測仍指向舊版；回復並非最後備註，而是上線前可執行的放行條件，如圖 25 所示。



圖 25 變更、版本、發布與移轉的可追溯鏈

變更類型決定核准與驗證深度，但不改變必須留痕的原則。標準變更依預核程序，普通變更依影響分級，重大變更增加原型、壓力與兩階段資安檢測，緊急變更優先控制服務或資安影響並安排事後審查。所有類型最後都要更新基線、文件與未結風險，如表 25 所示。

表 25 變更類型、核准與驗證要求

變更類型	適用條件	核准方式	測試／資安要求	回復與事後管理
標準變更	重複、低風險、步驟及範圍固定	依預先核准程序與授權執行	固定檢核、冒煙與必要回歸	依標準步驟回復，定期抽查適用性
普通變更	對功能、資料、組態或文件有一般影響	影響分析後由相應權限核准	受影響單元、整合、回歸及安全檢查	核准回復計畫，發布後觀察

變更類型	適用條件	核准方式	測試／資安要求	回復與事後管理
重大變更	架構、高影響資料、核心流程或重大資安影響	機關核定並納入重要查核點	雛型展示、壓力、完整回歸及上線前後資安檢測	完整備份、演練、停止條件與回復決策
緊急變更	服務或資安風險需立即控制	依緊急授權先處置並留痕	最小必要測試，復原後補完整測試	事後審查、根因、文件與基線補正

工作移轉從開發期即開始累積，不在契約末期才整理。每次核准發布同步更新架構、建置、資料、介接、監控、備份、回復、權限、AI 版本、已知問題及操作文件；重大知識以導讀、示範、接手實作與問答四步移轉。接手人依文件完成代表性任務，原負責人觀察並記錄缺口，再修訂文件與權限。

移轉資產包含程式原始碼及目的碼、建置與部署方式、組態範本、資料庫物件、介接規格、模型與提示清冊、測試案例與結果、資安報告、操作維護手冊、工單與風險、帳號設備及授權資料。每項資產列所有者、位置、版次、敏感等級、開啟方式與完整性資訊；需交電子檔及審定 USB 者依交付程序辦理。

退場控制處理帳號停用、憑證輪替、設備與資料返還、工作資料保存或處理、工具匯出、未結工單、弱點、變更、保固及第三方依賴。不能移交的秘密不得以明文附檔替代，而由機關指定安全機制重新設定。廠商保留資料僅限法令或契約所需，範圍、權限與期限明確，期滿依程序處理。

移轉清冊的判定重點是「資產存在、版本一致、可開啟、可操作、責任清楚」。程式與目的碼需能對應，文件需能重現建置與維運，帳號需依機關控制接續，未結事

項需有影響與後續責任；任一關鍵資產只存在於個人裝置或記憶，即視為缺口並在移轉演練中改善，如表 26 所示。

表 26 工作移轉與退場查核清單

移轉類別	應交資產	驗證活動	完成證據
程式與建置	原始碼、目的碼、依賴、組態範本、建置部署與回復	由核准版重建、部署、冒煙及回復	版次、雜湊、執行紀錄與清冊
資料與介接	資料字典、資料庫物件、API、帳號申請與對帳	查欄位、執行代表交易與復原	規格、測試、權限與對帳紀錄
AI 與規則	模型、映像、提示、規則、案例與容量	重現代表情境、切換及回復版本	相容矩陣、測試、監控與版本清冊
維運與資安	監控、備份、工單、弱點、事件、檢測與演練	模擬告警、復原、弱點追蹤與事件桌演	工單、報告、演練及改善證據
文件與訓練	設計、安裝維護、使用操作、教材、已知問題	接手人依文件完成實作	審定版、缺口修訂、簽到與簽認
退場與責任	帳號、憑證、設備、資料、工具匯出、未結事項	停用 / 輪替、返還、匯出及責任核對	退場清冊、處理紀錄、未結狀態

組態管理涵蓋程式、資料庫、環境變數、排程、網路、容器、模型、提示、規則、定型稿及監控。每項組態有所有者、核准值、環境與變更來源，正式環境定期比對基線；未授權差異先保存事實、評估影響並依程序復原或補正。

發布候選由核准提交與固定依賴建置，清單核對變更、資料庫、備份、測試、弱點、監控及回復。發布後觀察登入、影像、AI、案件、交易、報表與資源；異常先界定受影響版本及案件，再修正或回復，並同步檢查資料與文件。

移轉完成需同時符合資產可開啟且同版、必要權限由機關接續、接手人完成代表任務、未結風險有責任及廠商帳號資料依程序處理。保固中的每次正式變更都更新清冊與接手材料，最後報告指出最終版、變更、事件及未結狀態。

變更查核以需求識別、核准範圍、程式提交、組態、資料庫異動、測試案例、發布紀錄與回復結果形成單一追溯鏈。審查人不只確認文件齊全，也比較核准內容與實際差異，檢查是否漏列介接、資料轉換、權限、監控、手冊或訓練影響；發現未授權內容時，不得以事後補文件取代影響評估與正式決策。緊急處置先維持服務與證據，事後仍須完成原因、差異、測試、核准及基線更新。

版本回復能力在上線前以代表性情境驗證，涵蓋程式、容器、資料庫、組態、模型或規則的相容關係。資料結構不可逆時，需另備轉換前備份、還原步驟與業務核對方法；回復後重新確認登入、權限、案件、交易、介接、報表及監控，不把服務程序啟動視為成功。演練證據記錄使用版本、開始與完成時點、異常、處置及最終判定，並把發現回饋發布清單。

移轉驗收由機關指定接手角色依文件實際完成建置、監控、查詢、事件或復原等代表任務。遇到缺頁、失效帳號、環境差異或未說明依賴時，立即回到清冊修訂並再次驗證；未結事項則載明影響、暫行控制與責任。最終簽認以資產可用、版本一致、任務可重現、權限已接續及廠商存取已依程序處理為準，使保固與退場不依賴個別人員記憶。

伍、訓練建議

5.1 訓練目標、對象與成效指標

教育訓練總計 4 小時，並於契約期滿前完成教材與技術移轉。訓練目標不是讓學員記住畫面位置，而是能在授權範圍內完成掃描與查詢、解析結果覆核、案件處理、報表使用、帳號與維運、事件回報及必要復原。課前先依機關指定參訓角色及實際上線版本調整案例，課後以情境實作、提問與操作紀錄判斷缺口。

對象分為一般使用、案件承辦、系統維運及管理角色。共同內容說明專案範圍、人工覆核、資料保護與事件通報；角色內容則對應其實際權限，不向一般使用者揭露敏感組態，也不讓維運角色因技術權限而取得超出職責的業務資料。若同一人兼具角色，仍按操作責任分段演練。

成效指標採完成指定情境、辨識例外、使用正確權限、找到必要證據及能提出處置步驟。正式門檻由訓練計畫依機關需求與案例難度明列，不臆造及格分數；未完成者安排補充說明或再次實作，並將反覆問題回饋到畫面、提示、手冊或權限設計。

四類角色先接受共同導入，再分流至掃描查詢、解析覆核、帳號維運或管理報表等任務，最後以情境實作與成果紀錄收斂。總計 4 小時須涵蓋必要共同觀念及角色練習，實際分配依參訓名單與上線功能調整；簽到、教材、案例、提問及成果構成完整證據，如圖 26 所示。



圖 26 角色導向訓練路徑與成效證據

角色矩陣將學習任務與權限、案例及證據對齊。一般使用著重安全查詢，案件承辦著重來源與候選差異，維運著重組態、監控與復原，管理角色著重報表口徑及決策；所有角色都需知道 AI 輸出須經人工覆核、不得外送資料及如何通報異常，如表 27 所示。

表 27 訓練對象、任務與成效證據

對象	核心任務	必要控制	情境實作	成效證據
一般使用者	登入、查詢、掃描 / 上傳與基本操作	個人帳號、最小權限、資料保護	完成核准資料的查詢與輸入	操作結果、提問與簽到
案件承辦	影像與 TAIDE 候選覆核、案件流程、函稿與介接	來源核對、修訂留痕、正式核准	處理正常與例外案件並追蹤狀態	前後值、狀態與操作軌跡

對象	核心任務	必要控制	情境實作	成效證據
系統維運	帳號、組態、監控、備份、發布與事件	權限分離、秘密保護、回復準備	告警查證、備份復原或版本回復	工單、演練、監控與清冊
管理角色	報表、停滯、風險與服務狀態	口徑、時點、權限與匯出稽核	依報表辨識問題並提出處置	查詢條件、判讀與決策紀錄

訓練需求由角色訪談、權限矩陣、操作風險、既有經驗及上線情境彙整。首次使用者需要理解安全登入與基本流程，承辦人需能核對來源及處理例外，維運與資安人員需掌握監控、備份、版本、弱點與通報，管理者則需理解報表口徑與資料時點。課程不要求所有人學習不屬於職責的細節，降低敏感資訊暴露及無效負荷。

成效分為知識、操作及移轉三層。知識層確認責任與禁止行為，操作層確認能在授權下完成情境，移轉層確認能依文件處理告警或變更。每一層使用可觀察證據，不以滿意度取代能力；學員問題集中時，先判斷是教材、介面、規則或權限原因，再選擇補課或系統改善。 訓練計畫也需明列無障礙或操作協助需求，教材與示範採清楚文字、步驟及不只依賴顏色的狀態提示；實際需求由機關參訓名單與環境決定，確保 4 小時能有效參與。 訓練成效另以課前基線與課後任務結果比較，辨識知識已理解但操作仍受阻、個別學員缺口或系統介面造成的共同障礙。承辦窗口彙整出席、任務完成、錯誤類型、提問與後續處理，不公布不必要的個人成績；可由教材或操作指引解決者更新版次，可由介面、規則或權限改善者轉成正式工單。結案時以核准教材、簽到、情境成果、缺口處置與移轉清冊交叉查核，證明訓練內容、對象、時數與實際系統版本一致。

5.2 課程內容、教材與實作演練

課程以實際上線版本與代表性案件情境設計，內容包含系統定位與責任邊界、登入與權限、影像輸入、TAIDE 候選與人工覆核、案件狀態、定型稿、介接、追蹤報表、錯誤與通報、資料保護及常用維運。四小時內優先安排必需操作與高風險例外，不以大量功能逐頁講解稀釋實作。

共同導入說明系統只在機關內網執行、模型輸出屬候選、正式結果由授權人員核准、操作均可能留存軌跡。承辦模組依來文接收、品質檢查、解析、覆核、案件製作、函稿、介接與追蹤完成端到端情境；維運模組處理帳號、監控、工單、備份、版本、弱點與事件；管理模組練習報表口徑、時點與異常判讀。

教材包含簡明講義、角色操作步驟、情境腳本、常見錯誤、例外處置、快速查詢、問題回報及維運附件。畫面截圖、欄位、角色及版本均對應交付系統；含敏感組態或帳號操作的內容分級保存，不放入一般教材。教材首頁標示版本、適用環境、修訂紀錄與聯絡流程，內容變更能回到發布清冊。

課前由講師驗證帳號、環境、樣本、掃描器、介接替代情境及教材，避免現場因外部系統不可用而無法達成目標。需使用正式資料的情境改採核准測試資料或去識別樣本；操作產生的測試案件有明確識別與清理方式，不混入正式統計。

課程模組與證據必須一一對應：導入以責任問答查核，承辦以端到端案件查核，維運以告警或復原演練查核，管理以報表判讀查核。總時數固定為 4 小時，模組內比重依實際角色與已核准功能調整，且保留足夠實作與問答，如表 28 所示。

表 28 四小時訓練課程模組與查核方式

課程模組	適用角色	核心內容	實作 / 查核	教材輸出
系統導入與安全責任	全體	內網、權限、人工覆核、資料保護、通報	角色權限與責任情境問答	導讀、責任與通報速查
影像與 AI 輔助案件	承辦、一般使用	掃描、品質、候選、來源、修訂與核准	正常、低品質及缺欄案例	操作步驟、例外與覆核清單
流程、函稿與介接追蹤	承辦、管理	狀態、定型稿、交易、重送、報表	完成案件並查詢交易與報表	情境腳本、狀態與報表說明
維運與資安	維運、資安	帳號、監控、備份、版本、弱點、事件	告警到工單、復原或回復演練	維運手冊、檢核與事件速查
問答、深化與成果確認	全體分流	易錯點、缺口與後續查詢	指定任務、提問與再次實作	問答、成果、缺口與修訂紀錄

情境演練先提供任務與預期業務結果，不逐步提示所有按鍵，讓學員依教材判斷。標準情境從清晰影像完成候選覆核與案件追蹤；邊界情境處理多頁、缺欄、低品質或格式錯誤；權限情境驗證無權操作會被阻擋並知道正確申請方式；介接情境處理逾時、失敗、補正與對帳；維運情境處理告警、備份、回復與工單。

講師觀察學員是否核對來源、辨識警示、保留稽核、避免重複交易及遵循資料保護，而不只看最終結果。學員若以不安全捷徑完成，例如共用帳號、跳過覆核、下載未必要資料或反覆送出交易，應立即說明風險並重新演練。結果記錄任務、版本、角色、完成情形、問題與後續學習，不記錄不必要的個人敏感資訊。

演練環境與正式環境分離，外部介接可使用核准測試端點或模擬回應，但必須清楚標示，避免誤送正式交易。測試帳號具最小權限並在活動後處理，樣本資料依清冊回收或刪除。任何演練發現的系統缺失建立正式工單，教材問題則修訂版次，操作誤解則納入常見問題。

案例庫按角色、風險及系統階段維護，並在上線變更後抽查。每個案例列前置條件、資料、步驟、預期結果、禁止事項、觀察與證據；這使訓練能重複執行且支援新人移轉。例外案例尤其要驗證學員知道何時停止、何時轉人工及何時通報，如表 29 所示。

表 29 訓練情境與例外演練案例

情境類型	任務	預期行為	禁止事項	證據 / 改善
標準案件	由影像到覆核、函稿與追蹤	核對來源、正確核准、查到狀態	未覆核即送正式流程	操作結果、軌跡、提問
低品質 / 缺欄	處理模糊、缺頁或欄位不足	轉例外、補件或人工輸入並留痕	以猜測值完成欄位	例外紀錄、再次實作與教材修訂
權限不足	嘗試未授權查詢或操作	被阻擋並走正式申請	借用或共用帳號	權限測試、申請流程理解
介接異常	逾時、失敗、補正或對帳不一	查狀態、避免重複、依權限處置	未查證即反覆重送	交易、工單與對帳紀錄

情境類型	任務	預期行為	禁止事項	證據 / 改善
資安事件	發現異常內容、告警或疑似外洩	保存必要證據、控制影響、依程序通報	自行刪除紀錄或對外說明	演練紀錄、通報鏈與改善
維運復原	告警、服務異常、備份或版本回復	依文件診斷、恢復、驗證與結案	無備份或未核准即變更	工單、監控、復原與缺口清單

授課環境在課前依清單驗證網路、瀏覽器、掃描設備、測試帳號、角色、樣本、AI 服務、報表及必要介接模擬。每個案例有重置方式，前一組操作不影響下一組；環境不可用時，只能啟用已演練的替代情境，仍保留角色操作與例外判斷，不能改為純口頭講解後宣告完成。正式環境如被用於展示，採唯讀或核准測試資料並避免產生正式交易。

講師需熟悉業務情境、人工覆核、權限、錯誤、資安與通報，不只熟悉畫面。課前以交付版實際跑過所有案例，記錄預期、常見錯誤、可接受替代及需要升級的問題；助教負責帳號與環境、觀察、問題分類及證據，不在學員遇到困難時直接代做。對外部介接與高風險操作，先在模擬或安全環境演練。

教材與系統版次共同管理。每次畫面、欄位、角色、流程、定型稿、模型提示或錯誤處置改變，發布清單檢查是否需更新講義、操作步驟、案例、快速查詢及常見問題。教材修訂保留差異、生效版本及核准，過期教材移出一般使用區但可供歷史查證。保固期間若工單顯示同一操作問題反覆發生，將實際原因與修正納入新版教材。

課程證據依個資最小化原則管理。簽到及角色資料限於證明參訓，操作截錄避免包含真實敏感案件，個人缺口只供必要學習支援；彙整報告呈現角色、案例、完成情形與系統性問題。教材、案例、成果與提問均列版本，使機關能證明 4 小時訓練實際

對應核准系統及所需工作。 教材驗收抽查連結、截圖、角色與步驟，若正式版本更新後內容失效，即在發布清單阻擋或同步修訂，不能由講師口頭補充取代正式知識資產。

5.3 技術移轉與知識管理

技術移轉涵蓋業務流程、架構、程式、資料、介接、地端 AI、測試、資安、部署、監控、備份、事件與文件。移轉從需求及設計期建立知識資產，在每次核准變更後同步更新，結案前以接手實作驗證完整；保固期間再以實際工單、版本與弱點狀態持續修訂，避免審定文件停留在結案時點。

知識資產依用途及敏感等級分類。一般使用者取得操作與例外處理，承辦角色取得案件與覆核，管理角色取得報表口徑與服務狀態，維運與資安角色在受控範圍取得架構、組態、帳號申請、備份、回復、弱點及事件資料。憑證與秘密不寫入手冊，由機關控制的安全機制產生或輪替。

移轉方法採導讀、示範、共同操作、接手操作及缺口修正。接手人需從核准清冊找到資產，依文件完成建置、代表性案件、介接查證、監控告警或復原等任務，再說明風險與升級方式。若只能在原作者協助下完成，視為知識仍未移轉，需修訂文件、權限或工具。

系統設計、原始碼與目的碼、安裝維護、使用操作、資安檢測及已知問題等資產匯入版本化知識庫，再透過示範、實作與問答回饋修正。移轉清冊與簽認只在資產可開啟、版次一致及接手可完成後成立；保固事件的根因及處置持續回到知識資產，如圖 27 所示。

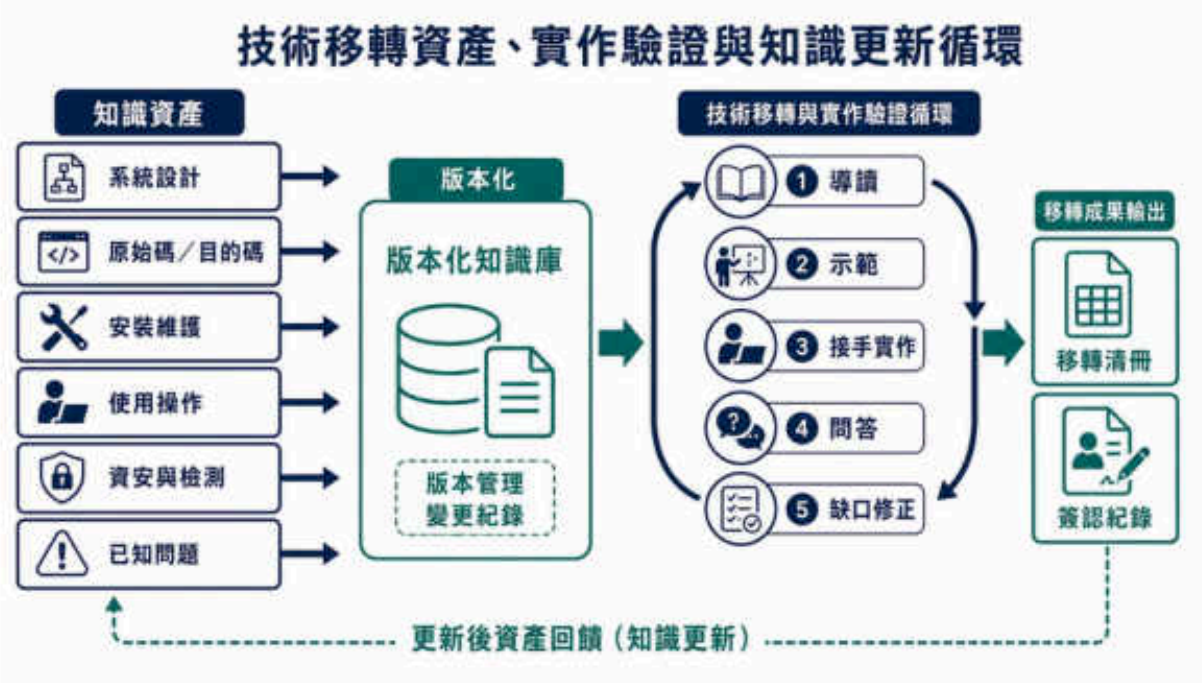

圖 27 技術移轉資產、實作驗證與知識更新循環

移轉矩陣把資產、接手任務與成功證據對齊。文件存在但無法重建、程式可建置但與交付目的碼不一致、資安報告無法對應掃描標的、帳號只掌握在原人員手中，均屬移轉缺口。每項缺口有責任與期限，重新實作後才關閉，如表 30 所示。

表 30 技術移轉資產與接手驗證

資產領域	主要內容	接手任務	成功證據
業務與需求	流程、欄位、規則、角色、追溯、未決	依情境說明規則並評估一項變更	追溯、影響分析與提問紀錄
程式與架構	原始碼、目的碼、依賴、組態、資料庫	由核准版建置、部署、冒煙及回復	版次、雜湊、執行與回復紀錄
AI 與案例	模型、映像、提示、規則、基準與挑戰集	重現候選、覆核及版本回復	相容矩陣、測試與操作紀錄
介接與報表	API、SSO、交易狀態、口徑與對帳	執行代表交易、失敗查證與報表比對	交易、日誌、對帳與口徑清冊

資產領域	主要內容	接手任務	成功證據
維運與資安	監控、備份、弱點、事件、檢測與演練	模擬告警、復原、弱點及事件處置	工單、復原、檢測與改善證據
文件與清冊	設計、安裝、維護、操作、教材、已知問題	從清冊尋找資產並完成指定任務	審定版、差異、缺口修訂與簽認

知識架構依「為何、是什麼、如何做、出錯怎麼辦、誰負責」組織。需求與決策說明原因，架構與資料描述系統，操作及維護手冊提供步驟，工單、已知問題與事件提供排錯，責任及聯絡清單提供升級。文件之間以唯一識別及版次連結，避免同一設定散落多處；快速查詢可引導使用者找到正式文件，但不成為無版本的另一份真相。

知識庫內容具有所有者、審查人、適用版本、敏感等級、最後驗證及下次檢視。程式與組態由版本庫及清冊管理，操作文件由業務與技術共同審查，資安及秘密內容限制查閱。搜尋結果應顯示適用版本，停用文件不作一般建議；重要外部連結保留必要摘要或正式名稱，以免網址變動造成程序中斷。

接手演練按風險逐步增加難度。先由接手人依清冊找到資產並說明架構，再完成標準建置與操作，接著處理低品質影像、介接逾時、弱點或備份復原等例外，最後說明何時停止及升級。原負責人只在必要時提示，觀察到的缺口分為文件、權限、工具、資料及能力，逐項修正後由相鄰案例再驗證。

程式移轉需證明原始碼、目的碼與建置來源一致；AI 移轉需證明映像、模型、提示、規則及案例相容；資料移轉需證明字典、備份、復原與處理責任；介接移轉需證明端點申請、憑證輪替、錯誤與對帳；維運移轉需證明監控、工單、發布、回復與月報。各領域可由不同接手角色執行，但最終清冊由專案經理統整。

知識更新以正式變更與已驗證工單為觸發。尚未證實的排錯猜測只放在工單，不直接寫入正式手冊；根因與處置經驗證後，才更新已知問題及步驟。文件若長期未被演練，不以最後修改日推定有效，而需在發布、月檢討或移轉時抽查。這使知識管理能反映可操作的現況，而非大量過期檔案。 知識資產還需定期做可開啟性與完整性檢查，避免連結失效、格式無法讀取或權限只剩原作者。清冊抽樣驗證檔案、版次、附件與敏感分級，接手人能由索引找到正式來源；發現重複或衝突文件時，指定唯一有效版並保留歷史關聯。這項維護在保固月報及最後移轉前各自留存證據。 接手演練結果由接手人與原負責人共同記錄，但完成判定由指定權責角色依清冊與實作證據確認；提示次數、文件缺口與權限問題均保留，確保簽認反映真實可接手狀態。

5.4 執行、查核與持續改善

訓練執行前完成版本凍結、參訓角色、帳號、場地、環境、樣本、掃描設備、教材及替代方案檢查；講師依實際系統演練，並確認敏感資料與外部介接不被誤用。執行中由講師與助教分工示範、觀察與紀錄，問題可當場解答者立即處理，涉及系統或需求者轉正式工單，避免口頭承諾脫離變更程序。

查核資料包括通知、課程、教材版次、簽到、角色、案例、操作成果、提問、缺口及後續學習。出席不等同具備操作能力，故至少以指定情境或接手任務觀察；個人結果只在必要範圍使用，彙整報告以角色與問題類型為主。訓練成果與 4 小時總時數、教材交付及技術移轉清冊一併納入結案證據。

持續改善從四類訊息找原因：操作錯誤可能是訓練不足，反覆提問可能是教材難找，經常繞路可能是介面不符流程，維運無法重現可能是文件或權限缺口。改善分為教材修訂、追加說明、介面優化、規則調整、權限或監控修正；後三類若改變基線，須進變更與測試程序。

訓練閉環依準備、執行、查核、缺口分類、改善與再驗證進行。每一階段有輸入及輸出，尤其問題不能只留在課堂筆記，而要轉為可追蹤的教材修訂或工單；在保固期間，月報可持續觀察相同問題是否下降，並保持資料口徑與時點清楚，如表 31 所示。

表 31 訓練執行、查核與改善閉環

階段	主要活動	查核資料	不符合處置	完成判定
準備	版本、角色、帳號、環境、樣本、教材檢查	課前清單、教材版次、演練結果	補正或啟用核准替代情境	參訓者可安全進入實作
執行	導入、角色分流、情境實作、問答	時數、簽到、案例、操作與提問	當場再次實作或建立正式工單	核心內容及實作完成
查核	觀察指定任務、例外與權限行為	成果、缺口、角色與版本	追加說明、再次實作	能依授權完成任務並知道升級方式
改善	分析教材、操作、介面、規則與權限原因	問題分類、責任、期限、版次	修訂教材或依變更程序改善系統	改善已發布且證據可追溯
再驗證	以原情境或相鄰情境重測	新舊結果、問題與月報趨勢	未改善則重做原因分析	缺口關閉且知識資產同步更新

訓練問題依對安全、資料、正式交易及操作效率的影響分級。無法辨識 AI 候選責任、可能越權或重複交易、不了解事件通報者，先以指定情境重新說明與實作；一般操作不熟則運用快速查詢或練習。若原因在介面、規則或權限，建立正式工單並依變更及測試程序處理。

上線初期支援不代替承辦核准。使用者先依教材辨認狀態及證據，支援人員再協助查證；問題記錄角色、版本、案件類型、原因與處置，敏感資料只在核准工具處理。重複問題形成教材或系統改善，特殊案件則標示適用邊界。

成效追蹤觀察操作求助、例外轉人工、權限錯誤、重複介接、工單分類、文件搜尋及接手任務，並標示資料時點、案件與版本。數據差異先拆解學習、資料或系統原因，不鼓勵跳過覆核或少報事件。改善後以相同或相鄰情境驗證，未有效者重新分析。

技術移轉與一般使用訓練採不同完成條件。維運人員需依文件重建、監控或復原，一般使用者需在授權範圍完成業務；兩類成果均更新同一知識版本。保固末期點交最終教材、案例、常見問題、成果及未結事項，確認機關能持續查閱、更新與執行。

每次訓練活動結束後，承辦窗口先核對通知、簽到、教材、案例、實作成果與問題紀錄是否同版，再由講師確認學員遇到的困難屬知識、操作、權限、資料或系統原因。可以現場處理者留下再次實作結果，需要系統調整者轉入工單並標示影響角色與替代作法；涉及資安或正式交易的問題在未完成驗證前不得以口頭說明結案。這套判定使學習缺口與產品缺失分流，但仍能在同一追蹤鏈上查核。

課後改善由責任人更新教材、快速查詢、案例或操作步驟，修訂時保留變更原因、適用版本及核准紀錄。若系統版本已改變，舊教材須標示不再適用，並以代表角色試讀或實作確認新內容能完成任務；若問題來自個別操作，後續支援只提供其職責所需資訊。月報彙整問題類型、處理狀態與再次驗證結果，使機關能判斷 4 小時訓練是否真正支援上線及接手，而不僅證明人員曾出席。

結案查核逐一連結課程計畫、實際時數、參訓角色、教材版次、情境成果、問題處置與移轉清冊。缺少任一關鍵證據時先補正紀錄或重新執行必要任務；未結工單則

明列影響、替代作法、責任及期限。經機關確認的教材與成果納入正式文件基線，保固期間因版本或事件修訂時同步更新知識資產，維持後續人員可查、可學、可操作。

陸、安全需求

6.1 資安治理、法遵與風險管理

本系統資安分級為中級，資安治理需同時覆蓋受託者管理、系統生命週期、資料保護、供應鏈、弱點檢測、事件應變、備援演練、稽核與持續改善。專案工作計畫建立資安組織、責任、資產與資料清冊、風險方法、控制基線、檢測節點及證據格式；資安專責負責推動與複核，專案經理確保資安工作納入時程、成本與交付，機關依權責審查與核定。

依《資通安全管理法》、《資通安全管理法施行細則》及《資通安全責任等級分級辦法》，受託資通系統的選任、監督與責任等級控制應建立可查核管理機制；本案以中級要求為基準，並將實際適用控制映射到設計、測試、維運及佐證。（數位發展部，2018；數位發展部，2026；數位發展部，2026） 若處理可識別自然人的影像或案件資料，另依《個人資料保護法》落實特定目的、資料最小化、安全維護與權利影響控制。（法務部，2023）

風險評估先辨認資產、資料、流程、角色、介接與依賴，分析威脅、弱點、既有控制及對機密性、完整性、可用性、可稽核性與個人權益的影響。風險處理可採降低、避免、移轉或接受；接受必須由具權限角色在瞭解殘餘風險、適用期間及監控條件後作成，不由技術人員以無法修正為由直接結案。

控制落實需具設計、操作與成效三層證據。設計證據說明政策、流程、架構與責任；操作證據包含帳號、組態、日誌、工單、備份、檢測及教育訓練；成效證據則由測試、抽查、稽核、演練及事件結果判斷控制是否有效。控制文件存在但未被執行，或日誌存在但無人檢視，都不能視為有效。

治理閉環由盤點、風險評估、控制選定、執行監控、稽核演練及改善追蹤組成，專案執行、資安專責與機關查核形成不同責任線。風險清冊、檢測報告、稽核紀錄及改善證明需能對應相同資產與版本；任何重大變更或事件都重新檢視風險，不只沿用啟動期評估，如圖 28 所示。



圖 28 中級資通系統之資安治理與風險證據架構

風險清冊應把原因、事件與影響分開，並列現行控制、殘餘風險、責任、處理、期限、觸發與查核證據。地端 AI 的風險不只模型內容，還包括映像、硬體、提示、資料與人工過度依賴；介接風險不只傳輸加密，還包括身分、重複交易與錯誤洩漏；保固風險則包含弱點、帳號、生命週期與知識斷點，如表 32 所示。

表 32 資安風險、控制與查核證據

風險面向	代表情境	主要控制	查核證據	再評估觸發
資料與個資	未授權查閱、過度蒐集、測試資料外洩	特定目的、最小化、遮蔽、權限、留痕	資料清冊、授權、存取與處理紀錄	新資料用途、欄位或介接

風險面向	代表情境	主要控制	查核證據	再評估觸發
地端 AI	外連、提示注入、無依據內容、版本漂移	網路限制、輸入分界、輸出驗證、人工覆核	組態、案例、版次、覆核與告警	模型、映像、提示或任務變更
應用與介接	越權、注入、錯誤洩漏、重複交易	SSO、最小權限、輸入驗證、冪等與遮蔽	權限、整合、安全測試與交易日誌	API、角色或外部系統變更
供應鏈	未知來源、弱點套件、秘密進入程式庫	核准來源、組件清冊、掃描、秘密管理	清冊、來源、掃描、修補與發布紀錄	套件、工具、授權或供應者變更
可用與復原	服務、資料庫、硬體或備份失效	監控、容量、備份、復原、替代方案	告警、壓力、備份與演練紀錄	架構、資料量、事故或演練缺失
人員與知識	共用帳號、權限未撤、關鍵知識集中	個人帳號、職務分離、定期複核、代理與移轉	帳號清冊、核准、訓練、接手實作	到離調、代理、組織或角色調整

ISMS 管理採風險導向及 PDCA 概念，將本案納入適用性、資產、風險、控制、績效與改善。ISO/IEC 27001:2022 可作為資訊安全管理系統對照框架，但廠商是否取得有效認證必須以證書、範圍、機構與效期佐證，正文不預設認證事實。（International Organization for Standardization; International Electrotechnical Commission，2022）即使有認證，也不能取代本系統的風險、控制與檢測證據。

委外監督從人員與保密、環境與存取、分包與第三方、開源與組件、事件通報、稽核權、交付與退場等面向設計。廠商人員只取得完成任務所需權限，機關可依程序查核，重大缺失有改善與複測，契約終了完成帳號、憑證、設備、資料及工作檔處理。

任何次受託或第三方服務均先揭露其角色、資料與風險，不因工具方便而引入外部雲端推論。

法規與控制映射表需記錄法規全名、適用內容、內部控制、技術實作、責任、頻率及證據位置。法規或機關規範更新時，先做差異與適用性分析，再更新風險、控制、測試及文件；不同年度或版本的要求不能混用，報告應標明檢視時點。若機關內規較嚴格，依其核定要求執行。

委外監督矩陣把治理要求落到專案節點。啟動檢查人員、保密與工作計畫，開發檢查安全設計、組件及存取，上線檢查檢測與回復，保固檢查事件、修補、稽核與演練，退場檢查帳號資料及移轉；每項監督都有提交、抽查與改善證據，如表 33 所示。

表 33 委外資安監督與法遵查核矩陣

階段	監督主題	廠商應交／應辦	機關查核	改善證據
啟動	人員、保密、責任、風險與計畫	名冊、保密文件、資安計畫、資產資料清冊	文件、權限與責任抽查	補正、核准與追蹤清單
設計開發	安全需求、架構、資料、組件與存取	設計檢視、組件清冊、環境與權限紀錄	里程碑檢視、程式與組態抽查	缺失、修正、複核與版本
測試上線	弱點、滲透、網頁、壓力與回復	測試、資安報告、修補複測、回復計畫	標的版次、重大風險與放行查核	複測、風險核定、上線紀錄

階段	監督主題	廠商應交 / 應辦	機關查核	改善證據
保固	事件、弱點、稽核、備援與月報	通報、工單、修補、演練、稽核與報告	趨勢、抽樣及未結事項查核	根因、改善、複測與月報追蹤
退場	帳號、憑證、設備、資料、工具與知識	停用 / 輪替、返還、處理、匯出與移轉	清冊、接手實作及未結責任	退場紀錄、簽認與最後報告

資安績效以控制是否運作及風險是否受控判斷，包含帳號複核、弱點修補複測、事件時間線、備份復原、稽核缺失、教育演練及供應鏈清冊。各項資料標示期間、資產與版本，避免不同掃描範圍或事件分類直接比較。月檢討由資安專責提出高風險、逾期改善與重大變更，專案經理整合時程成本，機關依權責核定殘餘風險。

治理檢討同時抽查證據品質。缺少標的版次、無法回查原始日誌、改善未複測、風險接受無期限或帳號清冊與實際不同，均列為控制缺口。改善更新政策、程序、技術、訓練與證據索引，並在相同情境再次驗證，使中級資通系統要求落實為持續管理而非交付前一次整備。

6.2 資料保護、身分識別與存取控制

本案處理來文影像、案件欄位、操作軌跡及介接資料，可能包含可識別個人的內容。資料治理先建立資料類別、欄位、來源、特定目的、角色、流向、保存、敏感等級與處理方式，再決定哪些資料可進入影像辨識或地端 TAIDE。資料使用只限核定目的與環境，不因技術可取得即擴張；測試、訓練、日誌與報表各自採最小化及遮蔽。

接收階段確認來源、完整性、授權及案件關聯；處理階段區分原始影像、衍生影像、模型候選、人工核准及外部交換版本；使用階段依角色與案件狀態限制；保存階

段依業務、法令、契約與稽核用途設定；期滿依核定程序封存、返還、刪除或不可逆處理。資料複本、匯出、備份與日誌均納入同一清冊，不只管理主資料庫。

傳輸使用 HTTPS 及核定安全協定，資料靜態保護依敏感與環境配置加密、磁碟、資料庫或檔案權限。金鑰與憑證由受控機制保存、輪替、備份與撤銷，不寫入程式、映像或一般文件。資料庫帳號按應用、維運、備份及查核分離，管理操作需有核准與留痕；直接查正式資料庫只在必要情境依程序執行。

日誌採資料最小化，保存案件與交易識別、事件、結果及必要診斷，不寫入密碼、完整憑證或不必要敏感內容。畫面與報表依角色遮蔽，下載延續原存取權並建立匯出事件；大量或異常存取納入告警。測試資料優先使用專用或去識別資料，若需真實資料則限制範圍、權限、期間及環境，使用後依清冊處理。

資料生命週期的驗收不只檢查能否查詢，也需驗證未授權讀取、匯出、備份、還原、封存與期滿處理。每個階段有控制與證據，原始與核准版本不可被衍生流程覆寫，AI 候選不得直接取代正式資料，外部交換則保留最小欄位與交易紀錄，如表 34 所示。

表 34 資料生命週期、保護控制與證據

階段	主要資料	保護控制	例外處理	查核證據
接收	來文影像、來源及案件識別	完整性、安全檢查、授權與隔離	破損、錯誤或惡意檔阻擋	接收、雜湊、檢查與例外紀錄
解析	衍生影像、文字、候選欄位、提示	地端處理、最小化、版本、來源關聯	低品質、格式或規則失敗轉人工	模型 / 引擎、提示、規則與差異
核准使用	人工核准資料、函稿、狀態	角色、案件狀態、前後值與核准軌跡	越權阻擋、退回或補正	身分、操作、核准與版本

階段	主要資料	保護控制	例外處理	查核證據
介接 / 匯出	最小交換欄位、報表及下載檔	身分、加密、遮蔽、交易與匯出留痕	逾時、補正、重送、異常下載	API、交易、對帳、下載事件
保存 / 備份	正式資料、日誌、備份與文件	分級權限、完整性、備份與復原測試	損毀或復原失敗轉事件	清冊、備份、復原與抽查
封存 / 處理	到期資料、退場工作資料與複本	核准、雙人或系統控制、處理紀錄	法令或爭議保留依程序延長	封存、返還、刪除或不可逆處理紀錄

使用者以機關 SSO 或核定身分機制登入，系統以角色與案件屬性決定功能及資料權限。角色設計遵循最小權限、職務分離、預設拒絕及必要知悉，至少區分一般查詢、案件承辦、核准、管理、維運、資安與稽核；建立、修改與核准高影響設定不由同一角色單獨完成。服務帳號與人員帳號分離，禁止共用人員帳號。

權限生命週期由申請、核准、建立、使用、定期複核、異動、停用及刪除組成。申請列業務理由、角色、範圍、期間與核准人；代理權限有起訖，自動或依程序撤除；特權權限採更嚴格核准、使用紀錄及定期複核。人員到離調、契約角色變更、長期未用與異常登入均觸發檢查。

應用、資料庫、作業系統、容器與介接服務的權限須一致治理，不能只在應用畫面限制。維運人員需要技術管理權，不代表可任意瀏覽完整業務內容；必要查證採特定時段、特定案件及核准範圍。機密憑證與 API 金鑰使用安全儲存及輪替，不在工單或聊天中傳遞；存取失敗與特權操作納入告警。

稽核紀錄可回答誰、何時、從何處、對何案件或資源、執行何動作、結果如何及關聯版本。不同層日誌以時間與識別碼關聯，但依角色分級查閱；日誌完整性受保護，

異常刪除或停記觸發告警。查核以抽樣重現權限申請、登入、操作、下載、特權及停用流程，而非只檢查帳號清單。

權限矩陣將功能與資料範圍分開，並為高影響操作增加核准或職務分離。具體角色名稱可於需求基線配合機關組織調整，但不得降低最小權限及稽核要求；每次角色或流程變更都重跑正向、負向與跨角色測試，如表 35 所示。

表 35 身分、權限與稽核控制矩陣

控制主題	設計要求	測試情境	監控 / 複核	證據
使用者身分	個人帳號、SSO、適當驗證、失敗保護	正常、失敗、鎖定、逾期或離職帳號	異常登入、長期未用	帳號、登入、告警與停用紀錄
角色與資料	最小權限、預設拒絕、案件與單位範圍	正向、負向、跨角色、跨單位	定期權限與資料範圍複核	申請、核准、角色、測試與複核
高影響操作	核准、職務分離、再次確認	權限設定、重送、發布、匯出、刪除	特權使用及例外抽查	核准、操作、前後值與結果
服務帳號	專用身分、最小權限、秘密輪替	憑證失效、權限不足、輪替後連線	到期、異常來源、非預期使用	帳號用途、憑證、輪替與日誌
維運與資料庫	技術權與業務資料分離、限時核准	查障、直接查詢、備份與復原	特權會話、敏感查詢	工單、核准、命令 / 查詢摘要與結果
稽核紀錄	完整、關聯、分級查閱、防竄改	操作、失敗、下載、權限與設定變更	停記、刪除、容量與完整性	日誌、完整性、查閱與抽查紀錄

資料盤點需辨認哪些影像、欄位、日誌或下載可直接或間接識別個人，並說明蒐集來源、特定目的、使用角色、介接對象與保存理由。新增欄位或 AI 任務若改變處理

目的、資料範圍、自動化程度或個人影響，先做適用性與風險分析，再決定是否調整告知、權限、遮蔽、人工覆核及保存。沒有業務必要的敏感內容不進提示、日誌、測試或報表。

資料品質與個資保護並非衝突。錯誤的身分、日期或案件關聯可能對當事人造成影響，因此原始來源、候選、核准及更正歷程需完整；但為驗證正確性而建立的複本仍要受最小化與權限控制。更正作業記錄來源、原因、影響案件、外部是否已交換及補正結果，不能只改本地欄位而忽略已產出函稿、報表或外部交易。

異常存取偵測關注非預期時段、來源、失敗、跨單位查詢、大量下載、特權操作及服務帳號異常。告警先確認使用者、業務理由、案件與工具狀態，避免將合法尖峰直接視為事件；但在查證期間可限制高風險操作並保存必要證據。確認為誤設權限、帳號濫用或外洩時，依事件程序停用、輪替、控制、通報與追蹤受影響資料。

權限定期複核由資料或業務所有者檢查人員與範圍，系統管理者提供帳號及使用資料但不替所有者核准。未使用、到期、角色不符或代理結束者撤除，特權與服務帳號另核對用途、責任、憑證及來源。複核不是重新匯出同一清單簽名，而是比較組織、人員、實際使用與目前職責的差異，處置後再次確認。

資料外洩或錯誤匯出的應變除技術控制外，還需辨認資料類型、對象、期間、下載或外送範圍、後續使用及可回收性。任何通知與對外說明由機關依程序決定，廠商提供事實、時間線、證據與控制。事件結束後檢視是否需調整欄位、權限、匯出、遮蔽、告警、教材及保存，使相同路徑不再重複。

退場時由資料清冊逐項核對正式資料、測試資料、日誌、備份、匯出、工單附件、模型提示與工作檔。機關接續所需資料按核准格式點交，廠商持有複本依法令與契約

處理，處理紀錄包含範圍、方式、責任與時間。帳號與憑證停用或輪替後，以存取測試及日誌確認無遺留權限，完成資料與身分兩方面的退場閉環。

資料清冊與權限複核的缺失若涉及正式使用，立即控制並評估過往存取；只修正帳號而不查歷史不足以關閉。查證結果及後續改善納入風險與自評證據。

6.3 安全開發、組件治理與環境管理

安全開發把資安活動放入需求、設計、開發、建置、測試、發布及維運，不在上線前才做一次掃描。可參考 NIST SP 800-218 SSDF v1.1 的安全軟體開發實務，將組織準備、軟體保護、安全產出及弱點回應映射至本案流程，但不以引用框架宣稱自動符合。（National Institute of Standards and Technology，2022）

安全需求包含身分、權限、輸入輸出、資料、日誌、加密、介接、AI、錯誤、備份、事件及退場，並連到測試與證據。設計階段檢查信任邊界、資料流、攻擊面、特權、失敗模式與回復；開發階段執行程式審查、輸入驗證、安全錯誤處理與秘密管理；建置階段固定依賴及產出可重現；測試階段執行原始碼、弱點、滲透與網頁檢測；發布階段核對修補、殘餘風險及版本。

程式碼變更需經同儕檢視，檢查需求關聯、安全影響、錯誤處理、日誌敏感內容、測試及文件。建置使用核准依賴與組態，產出記錄來源版次及完整性；開發者不得將密碼、金鑰、憑證或正式資料提交儲存庫。自動化檢查可提高一致性，但誤報、規則版本與未涵蓋語言仍需人工判讀。

發布閘門依變更風險配置檢視深度。一般變更需受影響測試與安全檢查，重大變更增加威脅檢視、原型、壓力、完整回歸及兩階段資安檢測；緊急修補在控制影響後補齊完整證據。任何高風險弱點、無回復能力、版本不一致或未授權組件均可阻擋發布。

SSDLC 管線由安全需求、設計檢視、程式與秘密管理、原始碼及組件掃描、安全測試、發布核准到維運監控；組件清冊、來源揭露、版本鎖定與弱點追蹤貫穿全程。開發、測試與正式環境分區，發布只由核准產物進行，這使弱點可追到元件與版本，如圖 29 所示。



圖 29 安全軟體開發、組件治理與環境隔離流程

階段閘門需有明確的進入、活動、退出與證據，不以「已做安全檢查」概括。安全設計的輸出進入程式檢視，掃描結果連到缺失及修正提交，安全測試標的連到發布候選版，維運弱點再回饋組件與需求；如此能把資安工作與交付版次鎖定，如表 36 所示。

表 36 安全開發生命週期與發布閘門

階段	安全活動	退出條件	阻擋條件	證據
需求	法遵、資料、身分、介接、AI、日誌與事件需求	需求可測且責任明確	高影響需求無驗收方法	安全需求、追溯、風險與核定

階段	安全活動	退出條件	阻擋條件	證據
設計	資料流、信任邊界、威脅、權限、失敗與回復	控制可實作、殘餘風險列管	敏感資料流或特權無控制	架構、資料流、檢視與風險清冊
開發建置	程式審查、秘密、依賴、靜態與組件檢查	核准提交可重現建置	秘密、未授權組件或高風險問題	審查、掃描、組件與建置版次
安全測試	弱點、網頁、滲透、權限、輸入與重大變更檢測	問題修補複測，風險有核定	標的不明、重大問題未控制	測試標的、報告、缺失、複測
發布	清冊、備份、回復、監控、文件與核准	產物同版且可回復	版本不一致或停止條件無法執行	發布單、清冊、核准、冒煙與監控
維運	弱點情報、事件、組件、變更與改善	風險持續更新並按月查核	已知高風險未有控制	工單、月報、修補、複測與改善

組件清冊涵蓋直接與間接依賴、作業系統套件、框架、容器基底、AI 模型、驅動及工具，記錄名稱、版本、來源、授權、用途、相依、雜湊、弱點、支援狀態與處理決策。開源來源依要求揭露，不以「開源」推定安全或無授權義務；未知來源、無法驗證完整性或不相容授權的組件不得納入發布。

弱點情報與組件清冊比對後，先確認本案是否使用、是否可達、是否有緩解，再決定修補、替換、組態控制或接受。掃描工具結果是線索，不直接等於風險；但無法立即升級時，需列受影響範圍、暫行控制、期限及再檢視。模型與容器映像亦按版次、來源與弱點管理，不將其視為獨立於軟體供應鏈。

環境分為開發、測試與正式，帳號、資料、憑證、端點及權限分離。程式由版本控制及核准建置產生，透過發布程序移動，不從開發環境直接複製未追蹤檔案；正式組態變更有核准與前後值。時間同步、日誌、備份、端點保護、網路規則與監控納入基線及定期檢查。

組件治理的決策需同時考慮功能相容、授權、安全、支援、移轉與回復。清冊不只在結案產生，而是在每次依賴變更及弱點通報時更新；資安檢測報告須指向相同清冊與發布版，讓機關能辨認問題是否已修補、是否只是工具誤報或仍以暫行控制接受，如表 37 所示。

表 37 軟體組件、開源與環境治理清單

治理對象	必要資料	准入／變更控制	弱點與生命週期處置	證據
應用套件	名稱、版本、直接／間接、來源、授權、用途	核准來源、相容與授權檢查	比對弱點、修補／替換／緩解	組件清冊、掃描、決策與複測
容器映像	基底、層、雜湊、來源、建置方式	核准基底、固定版次、可重現建置	重新建置、掃描與退役舊版	映像清冊、建置與發布版次
模型與相關檔	模型、授權、來源、雜湊、硬體與提示相容	地端核准、完整性與容量測試	版本回復、弱點或風險再評估	模型清冊、相容矩陣、測試
作業環境	OS、資料庫、框架、驅動、組態基線	分環境、權限、變更核准	修補、支援期限、替代與回復	盤點、基線、修補、測試與監控

治理對象	必要資料	准入 / 變更控制	弱點與生命週期處置	證據
秘密與憑證	用途、所有者、環境、效期、輪替與撤銷	不入程式庫、最小存取、安全儲存	到期 / 外洩立即輪替或撤銷	清冊、核准、輪替與存取紀錄
開發測試資料	來源、用途、敏感、去識別、期限	核准、最小化、環境限制	期滿返還、刪除或不可逆處理	資料清冊、授權、使用與處理紀錄

威脅建模選取影像接收、地端 AI、人工覆核、外部介接、報表下載、管理設定及發布等高影響資料流，辨認身分冒用、竄改、否認、洩漏、阻斷與權限提升情境。每一威脅連到現行控制、未解假設、測試及監控；設計或重大變更時更新，不要求對低影響元件做形式化文件堆疊。結果用來決定輸入驗證、職務分離、日誌、限流、回復與測試優先序。

秘密管理涵蓋資料庫、API、SSO、憑證、簽章及備份金鑰等，不把模型或容器便利性作為例外。秘密由機關核准機制保存，程式只取得執行所需引用；不同環境、服務與用途分離，效期及輪替有責任。發現秘密出現在程式庫、映像、日誌或文件時，不能只刪檔，還要立即輪替、查閱歷史與使用範圍、評估外洩並清理衍生產物。

可重現建置從核准提交、固定依賴、建置腳本及環境描述產生目的碼、容器或部署包，記錄雜湊及組件清冊。建置機限制權限與網路，避免臨時下載未知依賴；相同來源應能產生可核對產物，若因工具或時間資訊無法完全一致，至少保留差異原因及完整來源鏈。正式發布只接收經掃描、測試及簽核的產物。

環境基線定期檢查修補、服務、連接埠、帳號、檔案權限、時間、日誌、備份、監控與容器設定。掃描發現與實際基線比對後建立修正或風險接受，手工例外設定有

期限及責任；正式環境的緊急修正於事後回寫自動化腳本及文件，防止下次部署覆蓋。這使環境狀態能由版本與清冊重現，而不依賴個別維運者記憶。

6.4 弱點檢測、修補與事件應變

資安檢測涵蓋原始碼、組件、弱點、網頁及滲透測試，測試標的必須指向正式發布候選或明確版本，列出環境、範圍、工具與規則基準、執行時間及限制。OWASP Top 10:2021 可協助分類 Web 應用風險，但交付時仍應依當時適用版本、機關要求及實際架構調整，不以單一清單取代完整測試。（OWASP Foundation，2021）

檢測前確認授權、窗口、時段、資料、流量限制、停止條件、備份與事件處置，避免測試本身影響正式服務或資料。原始碼與組件檢查宜在開發中持續執行，網頁與弱點檢測在整合環境驗證，滲透測試由適當獨立性與能力的人員於核准範圍辦理。重大變更依要求安排上線前及上線後兩階段檢測，兩階段標的與目的分別記錄。

發現項目先去除重複與誤報，確認受影響資產、版本、可達性、資料與業務影響，再依機關基準分級。風險不只看工具分數，還考慮是否可被利用、是否有現行控制及修補影響；高風險項目優先控制暴露與修補，無法立即修補者採限制存取、停用功能或其他暫行控制，並列責任、期限及再檢視。

修補流程建立缺失與變更關聯，於測試環境驗證功能及安全後發布。複測使用原檢測方式確認問題消除，並執行相鄰情境以避免回歸；只更新套件版本而無複測，或工具顯示不再出現但正式標的未更新，都不能結案。報告保留原始發現、分析、修正提交、發布版本、複測及殘餘風險核定。

弱點與事件雙入口共同進入確認分級、控制擴散、修補或處置、複測／復原、結案及根因改善。重大變更的兩階段檢測形成額外閘門，使上線前確認設計與候選版，

上線後確認正式設定與暴露面；所有結果連到工單、報告、版次及改善證據，如圖 30 所示。



圖 30 弱點與資安事件之分級、修補及驗證閉環

檢測矩陣需避免不同工具與年度結果直接比較。每份結果標示資料時點、規則／弱點資料庫版本、範圍與排除，趨勢分析只比較相同口徑或明列差異。機關查核可從高風險、已關閉與接受風險項目抽樣，確認其標的、修補與複測皆對應正式版本，如表 38 所示。

表 38 資安檢測、修補與複測矩陣

檢測類型	主要標的	執行時點	結果判讀	關閉證據
原始碼檢查	自製程式、輸入輸出、秘密與高風險函式	開發中及發布候選	去除誤報，確認路徑與影響	修正提交、單元／回歸與複測
組件／映像掃描	直接間接套件、OS 套件、容器基底	依賴變更、建置及弱點通報	比對使用、可達、授權與支援	清冊、升級／緩解、建置版與複測

檢測類型	主要標的	執行時點	結果判讀	關閉證據
弱點 / 網頁檢測	主機、服務、Web、TLS 與組態	整合、上線及定期	以正式架構與設定確認真實風險	組態 / 程式修正、發布與複測
滲透測試	核准範圍的應用與介接	重要交付及高風險變更	以利用可能與業務影響判斷	測試報告、修補、複測與風險核定
重大變更檢測	變更元件及相關攻擊面	上線前與上線後	前後標的、設定及差異分別記錄	兩階段報告、差異、修補與放行

資安事件來源包含監控告警、使用者通報、異常日誌、弱點被利用、資料外洩跡象、惡意檔案、帳號濫用、模型外連或提示注入。受理後先保存必要時間、來源、資產、案件及狀態，進行確認與分級；不確定是否事件時仍建立觀察紀錄，避免過早刪除證據。技術錯誤訊息對一般使用者保持必要且可行動，不暴露內部路徑、版本與堆疊。

應變依確認、控制、根除、復原、通報、結案及改善進行。控制擴散可包含停用帳號、隔離服務、限制介接、暫停 AI 功能或切換替代流程；任何措施都考量證據保存與業務影響。復原使用乾淨且核准版本，驗證資料完整、權限、關鍵流程、監控及外部介接，再由相應權限決定恢復服務。

通報依機關資安事件程序、適用法令、契約及分級要求執行，廠商不得自行對外發言。初始資訊即使不完整，也應以事實、影響、已採控制、所需支援與下一更新節點呈現，後續以同一事件識別更新。涉及個人資料、安全執法或第三方時，並行評估相應通知、保存與協作責任。

事件結案須有時間線、影響、根因、控制、復原、通知、證據處理、殘餘風險與改善；重大或重複事件安排桌上或實作演練驗證改善。紀錄從發現到結案連續，明確標示推測與已證實事實，並對敏感證據限制存取。事件管理矩陣使技術處置、機關指揮及後續改善各有責任，如表 39 所示。

表 39 資安事件應變、通報與結案證據

階段	廠商主要動作	機關協作 / 決策	必要證據	完成判定
發現確認	保存必要紀錄、確認資產與影響、建立事件識別	提供業務及資產資訊、確認分級程序	告警、日誌、時間、初步事實	事件範圍及下一步明確
控制擴散	隔離、停用、限制、替代與持續監控	核定高影響措施、協調外部單位	指令、操作、影響與狀態變化	擴散受控、重要證據保存
根除修復	移除原因、修補、輪替、重建	審查風險與修復方案	根因、修正、組態、建置與弱點	已知原因及受影響面受控
復原驗證	由乾淨版復原，驗證資料、權限、流程與監控	核定服務恢復	備份、復原、測試、監控與介接結果	業務可用且無異常擴散
通報更新	依程序提供事實、影響、控制及更新	指揮並依法規與程序對外通報	事件編號、通知、版本與收件紀錄	應報事項完成且資訊一致
結案改善	完整時間線、根因、殘餘風險、改善與演練	審查結案、風險接受及改善	報告、工單、複測、演練與月報	改善有責任並查核至關閉

弱點情報來源包括檢測工具、組件供應者、主管機關、專業社群及事件，接收後先比對資產與版本，再判斷可達性及控制。未使用或不可達不代表可直接忽略，仍保存分析依據；使用中且高影響者立即建立工單與控制，相關組件若同時存在多個服務，統一辨認範圍，避免只修掃描到的單一主機。

修補時程依機關規範、風險、暴露與變更影響安排，正文不自訂未有來源的固定日數。若正式修補需要較長測試，先採限制、停用、監控或網路控制並設定到期及再檢視；暫行控制不能讓弱點自動成為已關閉。每次月檢討檢查高風險、逾期、接受與重複弱點，並確認資安經費及人力仍支持處置。

數位證據保存遵守必要性、完整性及權限。事件日誌、檔案、記憶體或網路資料由授權人員在不破壞證據的前提蒐集，記錄時間、工具、來源、雜湊、保管與存取；一般工單不複製大量敏感內容，只保留安全位置及摘要。時間同步及日誌關聯讓應用、AI、介接、系統與身分事件可建立一致時間線。

複測須使用已知原問題的步驟及相鄰攻擊面，標明修正提交、建置、環境與正式發布。若修補只是加入阻擋規則，還需檢查繞過、誤擋及監控；若升級組件，檢查相容、授權與新弱點；若修改權限，檢查正負向角色。複測通過後，確認正式版已部署並更新組件、風險與報告清冊。

事件與弱點的共同根因例如未受控變更、過期元件、權限集中、日誌不足或流程未被執行，應採系統性改善。改善可能涉及需求、設計、工具、訓練或治理，並在下次檢測、演練或稽核查核。若只針對單一事件修補，仍保留共因風險及責任，避免同類問題在其他案件模組或介接再次出現。 資安檢測委外或由不同人員執行時，仍由本案維護標的、版本、範圍及缺失主清冊。報告轉錄不得遺失證據或風險語意，修補工

單與原發現保持關聯；不同報告對同一問題分級不同時，依實際資產與機關基準統一判斷並保留理由。這能避免多家工具或服務造成重複與漏追。

6.5 備援演練、稽核與持續營運

持續營運規劃先辨認案件接收、人工覆核、正式資料、外部介接、追蹤報表、身分服務、地端 AI 與維運監控的相依關係，並評估服務中斷、資料損毀、硬體故障、網路隔離、外部系統不可用及關鍵人員缺席。復原優先序由業務影響與資料一致性決定，不預設未經來源核定的時間或資料復原門檻；具體目標在工作計畫依機關業務需求及可行性建立並測試。

備份範圍包含資料庫、影像與檔案、組態、程式與建置資訊、模型與提示、規則、定型稿、憑證必要中繼資料、日誌及文件。每項資產定義所有者、方式、頻率、保存、位置、加密、權限與復原步驟；備份成功訊息不等於可復原，需依風險抽樣執行還原及業務情境驗證。備份帳號與儲存採隔離及最小權限，防止主環境問題同時破壞備份。

復原先確認事件範圍與乾淨時間點，再依服務、資料庫、檔案、AI 與介接順序執行。技術服務啟動後還要檢查案件狀態、交易對帳、權限、定型稿版本與報表一致；未完成交易不直接重送，先查外部狀態。復原操作、資料差異與人工補正完整留痕。

外部介接或 AI 服務暫時不可用時，系統應能保留案件與狀態，避免資料遺失或重複交易。核准替代流程可採待處理佇列、人工輸入或延後執行，但需明確範圍、權限、資料保護、對帳及回復條件；恢復後由清單逐項比對，不把替代期間資料直接批次送出而無覆核。

備援矩陣將資產、失效情境、復原順序、業務驗證及證據對齊。資料庫復原需與影像及交易狀態一致，AI 版本復原需與提示規則相容，介接恢復需先對帳；演練發現的缺口進入工單、風險與月報直到複測，如表 40 所示。

表 40 備份、復原與替代流程驗證矩陣

資產 / 服務	失效情境	復原 / 替代重點	業務驗證	證據
資料庫與案件資料	損毀、誤改、服務故障	選乾淨備份、還原、交易一致與權限	案件、狀態、欄位、報表一致	備份、還原、差異與驗證紀錄
影像與檔案	檔案遺失、連結或儲存故障	完整性、路徑 / 識別關聯與權限	原始影像可開啟且對應案件	清冊、雜湊、還原與抽查
AI 服務	容器、模型、硬體或組態失效	回復核准映像、模型、提示及規則	代表案例可解析並經人工覆核	版次、部署、案例、監控與回復
外部介接	端點、網路、憑證或對方服務不可用	保留狀態、受控佇列、對帳後重送	無重複、遺失或未授權交易	交易、對帳、重送與工單
身分與權限	SSO 或權限服務異常	依核准替代與最小權限，避免共用帳號	只有授權角色可進行必要操作	啟用、使用、稽核與撤除紀錄
文件與知識	關鍵人員或文件不可用	代理、版本化資產與接手實作	指定人員可依文件完成處置	交接、演練、缺口與修訂

備援演練有範圍、情境、目標、角色、前置、停止條件、觀察及復原，不只做口頭推演。可採桌上演練驗證決策與通報、技術演練驗證備份復原、情境演練驗證 AI 或介接降級；執行前評估對正式服務與資料的影響。演練資料標示為測試，完成後依清冊處理。

稽核包含資安政策與程序、帳號權限、資料處理、組態基線、組件與弱點、事件、備份、訓練、委外監督及退場。抽樣以風險、變更及前次缺失為基礎，確認紀錄與實

際操作一致；年度佐證或定期報告標明涵蓋期間、資產、版本及限制，不將不同年度環境直接比較。機關查核意見進入改善清單。

改善項目記錄來源、事實、影響、根因、立即控制、永久措施、責任、期限與複測。只修文件但實際控制未變、只修設定但程序未更新、或已教育但介面仍持續誘發錯誤，都需再評估。重大缺失在關閉前由適當獨立角色複核，並在後續演練或稽核確認不再發生。

演練與稽核計畫以風險、範圍與證據決定頻率，並將結果納入月檢討與年度佐證。資料時點、環境與抽樣限制清楚，趨勢只在口徑可比較時使用；持續改善不是增加紀錄數，而是使弱點、事件或演練缺口實際降低，如表 41 所示。

表 41 備援演練、稽核與改善追蹤

活動	規劃重點	執行觀察	結果判定	改善與複測
桌上演練	事件、角色、決策、通報與外部依賴	資訊是否足夠、責任與升級是否明確	能在不完整資訊下作成可追蹤處置	修流程、聯絡、表單並再演練
技術復原	備份、環境、權限、順序、停止條件	還原、資料一致、監控與業務情境	復原結果可用且證據完整	修備份、腳本、容量或文件後重測
降級 / 替代	AI、介接或身分服務不可用	佇列、人工、最小權限與恢復對帳	無資料遺失、重複或越權	修降級、對帳與回復流程

活動	規劃重點	執行觀察	結果判定	改善與複測
資安稽核	政策、資產、權限、資料、弱點、事件與委外	設計、操作及成效證據是否一致	缺失分級、影響與責任明確	改善、抽查、複核至關閉
年度／定期佐證	期間、範圍、資產、版本與資料口徑	報告是否可回查原始證據	不同時點限制揭露、證據可重現	納入風險、月報及下期計畫

營運衝擊分析以業務流程而非伺服器清單為起點，辨認收件、覆核、簽辦、介接、報表與查詢在中斷時的影響、替代方式、資料積壓與恢復後補正。每項流程連到應用、資料庫、AI、身分、網路、外部系統、人員及文件相依；若同一基礎服務支援多個流程，其故障優先序依整體影響判斷。具體復原目標由機關依業務與技術實測核定。

替代流程須事前設計表單、責任、權限、資料保存、序號與對帳，不能在中斷時臨時使用個人檔案或未授權通訊工具。人工處理產生的資料在系統恢復後按清單補登，由另一角色或規則檢查重複與錯誤；已對外處理者先對帳再更新本地狀態。替代結束有明確決策及時間，相關暫時帳號與檔案隨即處理。

備份策略需考量勒索或權限濫用等共同失效，至少使部分備份與正式環境在帳號、位置或不可變性上有適當隔離。備份作業與失敗告警由指定角色監看，復原測試抽取不同資產與時間點，不只每次還原最容易的一份資料庫。備份保存期間與資料處理義務一致，逾期備份也納入安全處理，不形成永久複本。

長期保固期間持續檢查容量、憑證效期、作業系統與套件支援、備份成功、復原演練、聯絡窗口及代理。跨年度資料因環境、案件量與版本不同，月報先標示範圍再判斷趨勢；若演練時間變長，可能源於資料量或步驟改變，需拆解原因而非直接認定退步。風險與改善連到實際版本及下次查核。

稽核獨立性依活動風險安排。日常自檢由執行人確認，週期複核由非原執行角色抽查，重大控制或缺失由資安專責、機關或適當獨立人員檢視。稽核樣本涵蓋成功與失敗、一般與特權、當期與歷史缺失，不只挑選完整案例。結果保留事實、範圍、限制、分級與被查核單位回應。

持續營運成果最終應使機關知道何種中斷可採何種替代、資料在哪裡、由誰決策、如何復原與如何證明一致。保固終了前以最新版本再核對計畫、備份、聯絡、代理及未結風險，並將有效步驟納入移轉。這項查核避免第三期驗收後的變更使早期復原文件失效。 備援資源與正式環境同步管理授權與安全修補，避免災難時啟用過期或有高風險弱點的系統。演練前後核對版本、帳號、憑證、時間及監控，備援平時未啟用的服務也需有資產所有者與檢視頻率。復原文件在每次重大變更後抽樣，確保資料庫、模型與介接順序仍正確。

持續營運的外部依賴清單包含身分、網路、公文及其他介接窗口，記錄聯絡、服務限制、替代與對帳。外部異常期間，本案仍保存案件及必要證據並提供可理解狀態；外部恢復後，依交易清單逐筆收斂，避免大量自動重送造成重複或超載。

6.6 資安責任、人力與自我評估銜接

資安責任由公司治理、專案管理、資安專責、設計開發、測試維運及全體專案人員共同承擔。資安專責至少 1 人並符合來源要求，負責風險、控制、檢測、弱點、事件、稽核、演練與佐證協調；專案經理確保資安工作有時程與成本；設計及開發人員落實安全需求；測試人員提供適當獨立驗證；所有人員遵守保密、帳號、資料與通報規定。

內部資安政策應涵蓋組織責任、資產、存取、密碼與憑證、開發、組件、資料、實體與環境、事件、營運持續、供應商、教育訓練、稽核及退場。政策不只提供文件

名稱，還需以適用範圍、版次、核准、宣導、執行紀錄及缺失改善證明在本案有效。人員到職、角色變更及定期訓練依權限與風險辦理，資安事件與重大缺失後安排針對性能力提升。

廠商能力、團隊資格、學經歷、資安證照及 ISO 27001 認證等事項，均以可核對證書或文件呈現，不臆稱已持有。認證證據需檢查主體、標準版本、認證範圍、發證機構與效期；個人證照需檢查姓名、資格、效期及本案角色關聯。證照能支持能力判斷，但不能替代本案控制、檢測與履約證據。

資安管理作業自我評估表與本章控制矩陣使用相同證據來源。管理面連到政策、責任、風險、委外與稽核；技術面連到身分、資料、安全開發、檢測、備援與日誌；認知訓練面連到訓練、演練、通報與改善。原式表單依實際辦理情形填列，證據需能回查本章清冊、紀錄與報告，不能由敘述推定已完成。

控制與自評的銜接清楚區分「制度已設計」、「已執行」、「成效已驗證」三種成熟度。只有文件層設計證據，操作紀錄證明執行，抽查、測試、稽核或演練才支持成效；若證據缺一層，自評應如實反映並列改善。表單附於本章後，可讓評選及履約查核沿同一證據索引檢視，如表 42 所示。

表 42 資安責任、資格與自評證據索引

自評面向	責任角色	設計證據	執行證據	成效 / 資格證據
治理與風險	公司治理、專案經理、資安專責	政策、組織、風險方法、控制基線	清冊、會議、核准、風險處理	稽核、抽查、改善關閉
人員與認知	專案經理、資安專責、全體人員	保密、到離調、教育與通報程序	名冊、權限、簽署、訓練與演練	情境結果、事件反應、證照 / 資格佐證

自評面向	責任角色	設計證據	執行證據	成效 / 資格證據
技術控制	設計開發、維運、資安專責	架構、資料流、權限、安全需求	組態、日誌、組件、備份與變更	測試、檢測、複測、復原演練
委外與供應鏈	專案經理、採購 / 資安相關角色	受託、組件、第三方與退場要求	來源揭露、清冊、存取與監督	查核、弱點處置、退場與移轉紀錄
認證與能力	公司與指定人員	適用範圍及本案角色說明	依證書條件維持的必要紀錄	有效證書、發證機構、範圍與效期核對
自評與改善	資安專責、專案經理、機關查核角色	自評題項與證據索引	實際辦理情形、缺口與責任	複核、改善、再驗證及更新表單

資安人力計畫把治理、設計、檢測、弱點、事件、演練、稽核及文件分配到主責與代理。資安專責統整證據，技術角色修補，機關權責角色判斷業務影響與殘餘風險；高影響事項維持開發、檢測與最終核准的適當分離。人力負荷在檢測、上線及稽核尖峰納入時程。

能力以資格文件與實際成果共同證明。證照核對姓名、資格、效期及本案角色，組織認證核對主體、標準版本、範圍、機構與效期；範圍不含本案者不作過度推論。政策落實則由安全設計、程式檢視、弱點處置、事件演練、權限複核及接手實作等紀錄驗證。

自評前建立題項、控制、期間、資產、版本、責任與證據索引。僅有計畫而未執行者如實呈現，不適用項目提出系統、資料或業務依據；管理、技術及認知訓練面與

本章風險、檢測、月報及資格佐證一致。敏感組態、弱點或個資只列受控位置與必要摘要。

非原填寫角色抽樣回查政策、帳號、組態、日誌、工單、測試、演練或證書。發現日期、版本、範圍或辦理情形不一致時，建立改善並更新自評；重大缺口同步進入風險與交付查核。複核保存抽樣、發現、處置及再驗證，表單因重大變更、事件或年度佐證而更新時保留原因及版次。

資安人員異動須交接通報、檢測帳號、掃描工具、弱點清冊、憑證與稽核資料，接替者以代表弱點、事件及題項完成實作，原權限按程序撤除。退場時再核對帳號憑證、工作資料、設備、檢測報告與未結風險，最後一期報告明列已完成、已移交及持續追蹤狀態。

自評缺口以風險影響、可利用性、資料敏感度及履約階段排序，處置內容明列原因、控制措施、責任、期限、驗證者與殘餘風險。能立即修正的權限、組態或文件差異保留修正前後證據；需版本變更者連到需求、程式、測試與發布；受外部條件限制者建立替代控制及再檢視觸發。關閉條件不是欄位填滿，而是控制已執行、證據時點與範圍相符，且獨立複核能重現結論。

資安會議按專案階段檢視風險、弱點、事件、存取、備份、供應商及自評缺口，決議直接進入工單或風險清冊。重大技術事項由資安、開發、維運與業務共同判讀，避免只以掃描分數決定影響；機關需要接受殘餘風險時，應取得完整事實、替代控制、適用期限及後續觀測資料。月報呈現新增、逾期、關閉與再開啟的變化，並可回查對應證據，不以單一累計數掩蓋高影響未結事項。

交付前的自評複核與其他驗收證據採同一版本基線。題項涉及帳號時抽核名冊、核准、權限與停用，涉及安全開發時抽核程式檢視、組件與測試，涉及事件及持續營

運時抽核通報、演練、復原與改善；若抽樣結果與表單陳述不一致，先更正事實及缺口狀態，再判斷能否完成驗收。最終證據包提供題項索引、受控證據位置、複核紀錄、未結風險與後續責任，既維持可審查性，也避免在建議書或一般報告複製敏感內容；移交清冊另標示機關接手角色與保存期間。

表 43 資安管理作業自我評估表

8.3 資安管理作業自我評估表

日期：　　年　　月　　日

評估項目	辦理情形
1.管理面	
1.1辦理本專案受託業務相關程序及環境之資通安全管理措施或通過第三方驗證	□辦理本專案受託業務之相關程序及環境已(將)通過_____認(驗)證並持續有效，驗證公司為_____ □辦理本專案受託業務之相關程序及環境已具備完善資安管理措施，詳_____文件(如未載明於既有文件內，請於備註欄內說明相關措施) □本專案受託業務之相關程序及環境未導入適當資安管理措施 備註：_____
1.2本專案之資安負責人、資安專責主管或其他資安人員之人力配置規劃	□本專案之資安負責人(專案主管)為_____ □本專案之資安人員為_____ □本專案未指派資安負責人、資安專責主管或其他資安人員 備註：_____
1.3本專案之資安風險評估，包含可能之資通系統機密性、完整性、可用性風險，及採取之對應控制措施	□本專案受託業務相關程序及環境之資安風險評估結果已(將)載明於_____文件，已(將)採取對應之控制措施詳_____文件(如未載明於既有文件內，請於備註欄內說明相關措施) □未就本專案進行資安風險評估 備註：_____
1.4本專案範圍內之資安事件通報應變程序，包含知悉資安事件發生或有發生之虞之相關通報時效規定、通報方式、資安事件調查、處理及改善流程	□本專案受託業務相關程序及環境之資安事件通報應變程序已(將)載明於文件(如未載明於既有文件內，請於備註欄內說明相關措施)，知悉資安事件或發現有事件發生之虞時，應於小時內向機關等相關利害關係人通報，通報對象包含_____ □未就本專案訂定相關資安事件通報及應變程序 備註：_____
1.5由招標公告日起算，過去3年是否發生因管理議題肇因之重大資安事件	□過去3年無發生因管理議題肇因之資安事件 □是，共____次，事件發生主要根因為____ 備註：

2.技術面	
2.1本專案範圍內之資通系統，包含主要履約標的之資通系統及其他執行本專案業務所需使用之業務、行政相關資通系統，辦理安全性檢測	□本專案範圍內之資通系統將規劃執行_____(如源碼掃描、弱點掃描、滲透測試)，檢測項目及本案範圍為：_____ □未就本專案範圍內之資通系統規劃安全性檢測 備註：_____
2.2辦理本專案受託業務環境及設備導入之相關資通安全防護措施	□本專案受託業務之環境及設備已(將)導入(啟用)_____(如防毒軟體、防火牆、電子郵件過濾機制、入侵偵測及防禦機制等)，導入項目及本案範圍為：_____ □本專案受託業務之環境及設備未導入相關資通安全防護措施 備註：_____
2.3本專案範圍內之資通系統及專案資料之存取控制等權限管理機制，如 PM、系統管理員、一般使用者帳號之權限分級原則及控管方式	□本專案範圍內之資通系統帳號或使用者權限分成___種等級，相關存取控制、權限管理機制說明如下：___ □未規劃本專案範圍內之資通系統及專案資料相關存取控制及權限管理機制 備註：_____
3.認知訓練面	
3.1本專案直接履約相關人員之資安教育訓練	□本專案直接履約相關人員之資安教育訓練包含_小時之資安通識教育訓練，對象包含_____；___小時之資安專業教育訓練，對象包含_____ □未規劃相關資安教育訓練 備註：_____
3.2本專案團隊人員取得之資通安全專業證照	□本專案具資安證照之團隊成員有：____位 □本專案團隊人員未具備資通安全專業證照 備註：

柒、價格分析

7.1 總包價估算基礎與價格結構

本案採總包價法，估算以公告預算新臺幣 8,000,000 元為上限，依工作分解、人力投入、資安檢測、整合上線、訓練移轉、保固支援、公司管理及營業稅編列。正式價格為 7,980,000 元，較公告預算低 20,000 元；成本範圍涵蓋系統擴充至保固最後一期報告，不以未列項目於履約後另行拆價。數量與單價均能連回人月、時數或可審查工項。

總價由直接薪資、直接執行費、公司管理費與稅費四個獨立最大項構成，其關係如下。

$$C_{total} = C_{salary} + C_{execution} + C_{management} + C_{tax} \tag{7-1}$$

式中，C_{total}為全案總價，單位為新臺幣元；C_{salary}為直接薪資，單位為新臺幣元；$C_{execution}$為直接執行費，單位為新臺幣元；$C_{management}$為公司管理費，單位為新臺幣元；C_{tax}為稅費，單位為新臺幣元。

估算基礎將需求、角色、數量、單價、複價及交付證據連結。人力以 6 個月擴充期為主要投入基準，測試工程師按 4 人月編列；直接執行費按檢測、演練、上線、4 小時訓練及保固支援等可查核工項計價；管理費承擔契約行政、品質複核、文件版控、保險與履約風險；稅費依稅前小計計算。若工作安排調整，仍以總包價內完成契約範圍為原則，如表 44 所示。

表 44 總包價估算基礎與交付關聯

成本基礎	數量依據	成本動因	對應工作 / 交付	查核證據
專案與技術人力	專案經理、分析、設計、AI、資安及測試人月	需求複雜、地端 AI、介接、16 類案件、資安與測試	需求、設計、開發、測試、上線與結案	工時計畫、工作成果、程式、測試與文件
資安檢測與演練	依檢測與演練各項工式	中級防護、重大變更、弱點與備援	檢測報告、修補複測、演練與稽核佐證	標的、報告、工單、複測與改善
整合、訓練與保固	依上線、4 小時訓練及保固支援工式	環境介接、移轉、事件與月報	上線、教材、技術移轉及月維護報告	上線紀錄、教材、清冊、工單與月報
公司管理	依全案行政、品質、風險與保險工式	多期交付、文件版控、履約與管理責任	核定、品質複核、交付及契約管理	管理紀錄、審查、版次與交付清冊
稅費	稅前小計 7,600,000 元乘營業稅率 5%	法定稅負	全案發票與付款	計價、稅額與發票資料

四大項中直接薪資 5,300,000 元，占總價約 66.42%，顯示主要成本在需求、設計、AI 整合、開發、資安與測試等知識工作；直接執行費 1,200,000 元，占約 15.04%，集中於檢測、演練、上線、訓練及保固；公司管理費 1,100,000 元，占約 13.78%，獨立呈現行政、品質與履約風險；稅費 380,000 元，占約 4.76%。各項加總 7,980,000 元，與正式明細總計一致，如表 45 所示。

表 45 全案價格結構、占比與用途

最大項	金額（元）	占總價	主要用途	主要成本風險
壹 直接薪資	5,300,000	66.42%	專案、分析、設計、AI、資安與測試人力	需求晚定、介接依賴、整合與缺失重工
貳 直接執行費	1,200,000	15.04%	資安檢測、演練、上線、訓練與保固支援	檢測範圍、環境、外部窗口與事件量
參 公司管理費	1,100,000	13.78%	契約行政、品質複核、版控、保險與風險	多期審查、文件一致與履約協調
肆 稅費	380,000	4.76%	營業稅	稅前基礎變動會連動稅額
全案總計	7,980,000	100.00%	完整履約範圍	由總包價、變更控制與交付查核共同管理

主要成本驅動來自 16 類案件差異、影像版型、地端 TAIDE 與既有環境相容、五類外部介接、角色權限、資安中級控制、三期交付及延伸保固。人力估算將需求分析、設計開發、AI 整合、測試、資安及管理分工，不以單一平均人月掩蓋角色差異；直接執行費則將可委託或可獨立查核的檢測、演練、上線、訓練及保固列成工式。

估算假設包括機關按計畫提供核准環境、窗口與必要測試條件，外部系統能依協調時程提供規格或測試方式，既有環境不進行與本案無關的全面重建，功能與交付以需求基線及正式變更為準。假設不是排除履約責任，而是用來辨認成本與時程敏感因素；假設改變時先評估是否可由批次、模擬、資源重排或既有預備費用吸收，再依契約程序處理。

價格風險以管理與技術控制降低。需求晚定透過早期追溯與原型，介接延誤透過資料契約及模擬，AI 品質透過基準集與人工覆核，資安缺失透過開發中掃描及修補，文件重工透過持續版控與內審。若只在期末集中測試與檢測，容易造成高成本重工，因此人力及直接執行費依工作節點提前投入。

單價分析考慮角色責任、期間、專業與成果，不把人月視為單純出勤。專案經理及分析師的產出是核定基線、決策與追溯，設計及 AI 人員產出可建置程式與技術證據，資安與測試人員產出控制、檢測及驗證。工式項則以範圍、方法、報告、複測、教材、上線或月報為驗收，確保金額能對應工作而非抽象名目。

敏感度分析不另行創造價格，而是辨認哪些變動最可能耗用成本：案件版型與規則增加會影響分析回歸，外部端點異動影響整合對帳，重大弱點影響修補檢測，環境容量影響部署調校，保固事件量影響支援。專案以風險清冊、變更、版本及月報監控這些因素，使總包價內的資源能及早調整。

總價治理要求預算明細、工作計畫、交付清冊與付款證據使用相同工作名稱及範圍。內部資源調度若不改變契約總價及交付，仍保留理由與對品質資安的影響；涉及正式價金或範圍者依核准程序，不以月報備註自行生效。發票與請款按審定成果辦理，成本發生不等於可請款，避免投入與驗收脫節。 估算資料在提交前由非原編製人複核，抽查人月、工式、稅額、占比、資安分子與三期金額。複核不只驗算，還確認工作名稱、範圍與本書其他章一致，沒有把公司管理費併入執行費、沒有遺漏保固或把同一檢測重複計列。結果及修正留存版本，正式報價、正文分析與請款基礎維持同一總價。

總包價的合理性也以風險分配檢視。可由廠商透過專業與效率控制的估算、開發、測試及文件風險納入價格；機關或外部系統所掌握的條件則以早期協調、未決與替代降低影響，但不自行創造追加承諾。若正式變更發生，依核准範圍更新成本與交付，

不破壞原四大項及算術一致性。 預算表的比例採四捨五入到小數點後兩位，四大項顯示占比僅供結構判讀；正式金額仍以元及小計為準，避免四捨五入造成比例相加或請款差異。

7.2 工作項目、數量、單價與複價明細

價格明細以可審查工作量為基礎，直接薪資編列專案經理 6 人月 900,000 元、系統分析師 6 人月 810,000 元、兩名系統設計師各 6 人月 720,000 元、AI / TAIDE 工程師 6 人月 840,000 元、資安安全專責 6 人月 870,000 元及測試工程師 4 人月 440,000 元。這些角色覆蓋需求、設計、開發、地端 AI、介接、測試、資安及交付，直接薪資合計 5,300,000 元。

專案經理單價 150,000 元 / 人月，負責工作計畫、月檢討、查核及履約品質，6 人月複價 900,000 元；其投入與三期交付及多條管理控制線相連，並不只是行政窗口。系統分析師單價 135,000 元 / 人月，6 人月複價 810,000 元，承擔 16 類案件、資料、權限、介接與驗收追溯，若需求基線不完整會放大後續重工，因此分析投入集中於前中期並持續支援驗收。

兩名系統設計師各以 120,000 元 / 人月、6 人月編列，合計 1,440,000 元；一名可聚焦影像、案件追蹤及既有系統增修，另一名可聚焦地端 TAIDE、API 與報表，但正式分工仍由工作計畫依能力與依賴安排。雙人配置符合最低系統設計師 2 人要求，也降低應用、AI 與介接在同一時段爭用單一技術責任人的風險。

AI / TAIDE 工程師單價 140,000 元 / 人月，6 人月複價 840,000 元，工作包含模型地端部署、文件解析、結構化輸出、提示與版本、容量及案例驗證。成本動因不是單次安裝模型，而是與影像、規則、人工覆核、硬體及安全控制整合；若模型版本或資料版型變動，需以基準集回歸與相容矩陣控制，不由追加未授權雲端費用處理。

資安安全專責單價 145,000 元 / 人月，6 人月複價 870,000 元，負責安全設計、風險、檢測協調、弱點修補、事件、稽核、演練及佐證；這筆薪資與外部或專項資安檢測服務分工，前者是全期治理與改善，後者是可獨立查核的檢測工作。測試工程師單價 110,000元 / 人月，4人月複價440,000元，集中支援單元整合、壓力、運轉與驗收，並對開發結果提供適當分離的驗證。

直接薪資合計占總價約 66.42%，與本案以系統分析、軟體增修、AI 整合、介接、資安與測試為主的服務性質相符。風險在於需求與外部介接延遲造成設計及測試重疊，因此以需求閘門、分批開發、固定回歸集及跨角色週期檢視控制；所有人力須對應工作成果、版次與交付，不以人月存在本身作為驗收。

直接執行費 1,200,000 元包含資安檢測 600,000 元、備援復原演練與資安稽核佐證 160,000 元、地端環境介接與運轉測試 240,000 元、4 小時教育訓練與技術移轉 100,000 元，以及保固監控與月報支援 100,000 元。資安檢測占總價約 7.52%，其標的、工具基準、缺失、修補與複測必須對應發布版；演練與稽核約占 2.01%，輸出是可重現的復原、查核及改善證據。

地端環境介接、上線及運轉測試 240,000 元支應核准環境的部署、介接、測試、監控與回復準備，成本受既有環境、外部窗口與正式資料條件影響；以工作計畫提前盤點並以整合測試證據驗收。訓練與移轉 100,000 元對應總計 4 小時課程、教材、角色實作與知識清冊，不以出席取代成效。保固支援 100,000 元對應監控、工單與月報交付，仍須符合回應、恢復或替代方案要求。

公司管理費 1,100,000 元獨立於直接執行費，占總價約 13.78%。其用途是契約行政、公司層品質複核、文件版控、保險與履約風險管理，對應核定、審查、跨期清冊

與交付一致性；不得以此項重複計列已在直接薪資中的專案執行工作。管理費的驗收關聯表現在審查、版控及履約成果，而非另行交付一套無用途的內部行政文件。

稅前小計為 7,600,000 元，營業稅以 5%計算 380,000 元，全案總計 7,980,000 元。稅額與稅前成本可由明細直接重算，避免以倒推總價形成無工作基礎的調整項；若依法核准的契約價金變更影響稅前基礎，稅額依適用計價程序連動。正式詳細價格如下，各複價均為數量乘單價並與小計及總計一致，如表 46 所示。

表 46 AI 輔助處分案系統擴充案詳細價格明細

項次	工作項目	單位	數量	單價	複價
壹	直接薪資				
一	專案管理、分析與系統開發人力				
1	計畫主持人／專案經理（專案計畫、月檢討、查核及履約品質控管，6.00 人月）	人月	6.00	150,000	900,000
2	系統分析師（需求確認、流程與介接規格分析，6.00 人月）	人月	6.00	135,000	810,000

項次	工作項目	單位	數量	單價	複價
3	系統設計師一（影像解析、案件追蹤及既有系統增修，6.00 人月）	人月	6.00	120,000	720,000
4	系統設計師二（TAIDE 地端整合、API 及報表功能開發，6.00 人月）	人月	6.00	120,000	720,000
5	AI / TAIDE 工程師（模型部署、文件解析及輸出驗證，6.00 人月）	人月	6.00	140,000	840,000
6	資安安全專責人員（安全設計、弱點修補協調及資安佐證，6.00 人月）	人月	6.00	145,000	870,000

項次	工作項目	單位	數量	單價	複價
7	測試工程師（單元、整合、壓力及驗收測試支援，4.00 人月）	人月	4.00	110,000	440,000
壹小計	直接薪資小計				5,300,000
貳	直接執行費				
一	資安檢測、整合交付與保固支援				
1	資安檢測服務（原始碼、弱點掃描及滲透測試，1 式）	式	1	600,000	600,000
2	備援復原演練及資安稽核佐證整理（1 式）	式	1	160,000	160,000
3	地端環境介接、上線及運轉測試支援（1 式）	式	1	240,000	240,000

項次	工作項目	單位	數量	單價	複價
4	教育訓練教材與技術移轉交付（4 小時，1 式）	式	1	100,000	100,000
5	保固期維護監控及月報交付支援（1 式）	式	1	100,000	100,000
貳小計	直接執行費小計				1,200,000
參	公司管理費				
一	專案行政、品質與風險管理				
1	公司管理費（契約行政、品質複核、文件版控、保險及履約風險管理，1 式）	式	1	1,100,000	1,100,000
參小計	公司管理費小計				1,100,000
肆	稅費				
一	營業稅				

項次	工作項目	單位	數量	單價	複價
1	營業稅（稅前小計 7,600,000 元 ×5%，1 式）	式	1	380,000	380,000
肆小計	稅費小計				380,000
總計	全案總計				7,980,000

明細的控制重點是數量、單價與複價能連到工作及成果。人月項由工作分解、期間與角色成果查核，工式項由範圍、執行、報告或移轉證據查核，稅費由稅前小計重算；壹至肆小計加總即全案總計。這種結構保留公司管理費的獨立性，也讓資安、訓練、保固及上線成本不被人力總額掩蓋。

明細校驗先逐列確認數量乘單價等於複價，再確認各細項加總等於壹、貳、參、肆小計，四項小計加總等於 7,980,000 元。直接薪資 7 個細項合計 5,300,000 元，直接執行費 5 個細項合計 1,200,000 元，公司管理費 1,100,000 元，稅前小計 7,600,000 元；營業稅 380,000 元加入後即為全案總計。任何請款或核准變更都以同樣算式重算，避免人工轉錄差異。

工項邊界避免重複計價。資安專責薪資涵蓋全期治理、設計、協調與佐證，600,000 元資安檢測服務涵蓋原始碼、弱點及滲透等可查核檢測，160,000 元演練稽核涵蓋復原與查核佐證；三者成果不同但可由同一風險與缺失追溯。系統設計與 AI 工程師的開發工作不再於地端上線 240,000 元重複計列，後者著重環境介接、部署及運轉測試支援。

訓練 100,000 元支應 4 小時課程、教材與技術移轉整合，不只計算授課時間，還包含案例、環境、版次、接手與證據；保固支援 100,000 元用於監控及月報交付，不減免

各角色對缺失、弱點或文件的原責任。公司管理費則處理公司層行政、品質、保險與履約風險，與專案經理的日常計畫及協調有清楚區別。

履約追蹤按工作成果而非財務內部分攤驗收。人力細項連到工作包、提交、程式、測試、檢視及文件，檢測與演練連到標的、報告、複測及改善，上線連到部署、監控及回復，訓練移轉連到教材、情境與清冊，保固連到工單與月報。每期交付清冊從這些證據選取契約要求的成果，並保持版次一致。

成本偏差由廠商內部管理時，仍須評估是否影響品質、資安、時程或人力底線。若某角色投入增加、另一工項節省，只要總包價與交付不變，透過資源與風險管理控制；若需要減少檢測、訓練、保固或最低人力才能吸收，即不可視為一般調度。任何正式範圍或價金變動遵循契約及變更程序，價格表與交付同步更新。 人力成果每月由工作包與交付證據核對，避免總人月雖足但關鍵角色投入時點不符。分析與架構需在開發前提供可用基線，資安不能只在檢測前集中，測試需在整合與驗收期具有足夠獨立驗證，專案經理則貫穿三期；若因重工移動投入，月檢討說明原因、後續負荷與品質風險。

工式服務亦設定範圍邊界與完成條件。檢測必須含標的、方法、報告與複測，演練需有情境、執行與改善，上線需有部署、監控與回復，訓練需有教材及成果，保固需有工單與月報。只提供報告封面、出席或服務窗口而無實質執行，不構成相應工項完成。 明細中的角色名稱、工項與本書管理、訓練、資安及交付章交叉核對，確保價格不是與技術方案分離的另一套承諾；任何名稱調整保留對照而不改變範圍。

7.3 成本效益、合理性與付款連動

成本效益以「投入是否形成可驗收能力」判斷，不以未有實測基線的節省工時或投資報酬率作承諾。影像與地端 TAIDE 投入的效益是減少重複摘錄並提高來源可追溯，

案件與定型稿投入的效益是共用流程及版本治理，介接與報表投入的效益是交易可對帳及狀態可追蹤，資安與維運投入的效益則是風險、弱點、事件及復原有證據閉環。

效益驗證需要比較上線前基線與上線後同口徑資料，至少標示案件類型、資料期間、版型、使用人數、系統版本與異常因素。不同年度、模型版本或案件分布的數據不可直接比較；若資料口徑改變，先重建基線或分層呈現。量化結果可作後續改善依據，但付款與驗收仍以契約交付、測試及審定證據為主。

投入—產出關係顯示四大成本項支援需求設計、功能、測試資安、文件移轉及保固，並在三期交付形成審查證據。第 1 期 20%連結需求確認，第 2 期 40%連結運轉測試、程式與資安檢測，第 3 期 40%連結結案、規格、手冊、資安報告、程式及移轉；價格不因付款期別切割而改變整體責任，如圖 31 所示。

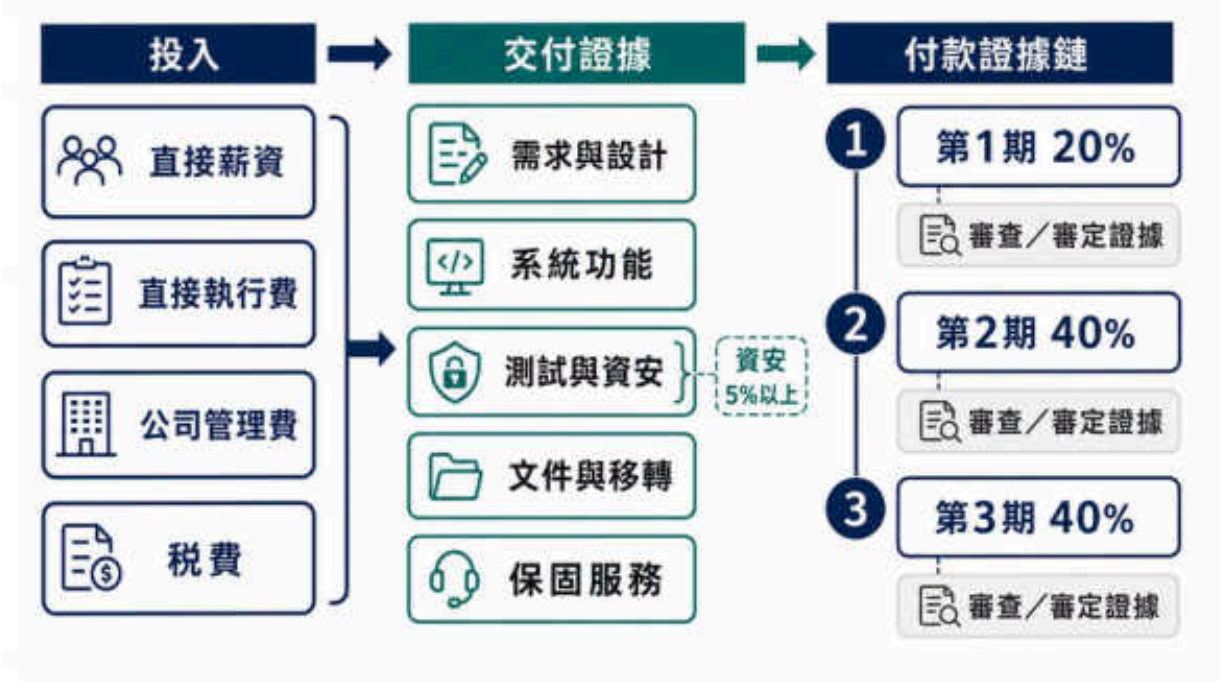

圖 31 成本投入、交付證據與分期付款連動

效益矩陣把每項投資連到可觀察改變、基線與證據。若影像品質、案件分布或外部介接可用性不同，需揭露限制；若效益不足，先查資料、流程、操作、模型或控制

原因，再以改善與回歸驗證，不以增加自動化比例作唯一解法。這能避免為追求數字而跳過人工覆核或資安控制，如表 47 所示。

表 47 成本投入、效益與驗證證據

投入領域	預期效益	基線 / 限制	驗證方式	交付證據
影像與地端 AI	減少重複摘錄、提高來源與候選可追溯	影像品質、版型、案件分布、模型版本	同口徑樣本、人工差異與例外分析	測試、覆核、版本與案例報告
案件與定型稿	共用流程、差異配置、歷史版本可重現	16 類差異、規則與生效時點	情境回歸、樣張、歷史案件重現	追溯、定型稿清冊、測試結果
介接與報表	交易可對帳、狀態與操作可追蹤	外部系統可用、資料口徑與權限	成功、逾時、重送、下載與對帳測試	規格、日誌、報表、工單
資安與品質	弱點、缺失、事件及殘餘風險可控	檢測標的、工具基準、資料時點	檢測、複測、稽核、演練與趨勢	資安報告、缺失、改善與風險核定
訓練移轉與保固	人員可操作、可接手並持續維運	角色、版本、事件量與知識缺口	情境實作、接手、工單與月報查核	教材、清冊、簽認、月維護報告

資安經費以明確細項核算：資安安全專責 870,000 元、資安檢測 600,000 元及備援復原演練與資安稽核 160,000 元，合計 1,630,000 元。以全案總價 7,980,000 元為分母，資安經費占比約 20.43%，高於服務費用 5%以上的最低要求；此算法只納入明確可辨識項目，未把一般設計、測試與管理中兼具資安效益的工時重複計入。

$$C_{sec} = 870000 + 600000 + 160000 \tag{7-2}$$

$$R_{sec} = \frac{C_{sec}}{C_{total}} \times 100\% \tag{7-3}$$

式中，C_{sec}為明確資安經費合計，單位為新臺幣元；R_{sec}為資安經費占全案總價之百分比，單位為百分比；C_{total}為全案總價 7,980,000 元，單位為新臺幣元。

付款以 20%、40%、40%連到三期審定成果，依 7,980,000 元計算分別為 1,596,000 元、3,192,000 元及 3,192,000 元。每期請款前核對交付清冊、版本、審查、缺失與審定狀態；第二期資安檢測若有缺失，需呈現修補及複測，第三期則核對最終資安報告與正式版一致。資安占比與付款均可由同一成本及交付資料重算，如表 48 所示。

表 48 資安經費與三期付款驗證

查核項目	金額 / 比例	核算與用途	付款 / 驗收證據
明確資安經費	1,630,000 元	資安專責 870,000 元 + 檢測 600,000 元 + 演練稽核 160,000 元	人力成果、檢測、修補複測、演練與稽核佐證
資安經費占比	約 20.43%	1,630,000 元除以全案 7,980,000 元，高於 5%	預算明細、交付清冊與資安報告一致
第 1 期付款	20%，1,596,000 元	需求與管理基線	需求確認報告審查 / 審定及未決事項列管
第 2 期付款	40%，3,192,000 元	運轉測試、程式碼與資安檢測	版本、測試、缺失、檢測及複測證據

查核項目	金額 / 比例	核算與用途	付款 / 驗收證據
第 3 期付款	40%，3,192,000 元	結案、規格、手冊、資安、程式及移轉	審定文件、清冊、USB 點交、接手實作與簽認
全案總計	100%，7,980,000 元	三期加總與詳細價格總計一致	計價、發票、審定成果及付款紀錄

效益資料按案件、版本與時點維持同一口徑，差異先拆解資料、模型、流程、介接與訓練原因，再決定改善。三期請款仍以審定交付及版次證據為準；資安經費與全案總價如有依法核准的變動，依同一明細重新核算占比，維持 5%以上要求與工作內容一致。

成本效益追蹤同時觀察人工處理時間、例外比例、介接失敗、重複作業、事件與維護負荷，但各指標須標示基準時點、資料範圍及版本，避免把案件量或流程改變誤判為系統效益。依法核准的範圍或數量變更，應同步更新工作分解、價格明細、交付條件、驗收證據與資安經費核算；未完成變更程序前，不以新增工作主張原總包價外付款。各期付款完成後保留審查意見、補正、核定成果與金流紀錄，使全案總計、獨立報價單及實際請款可相互核對。

捌、結論

8.1 綜合結論

本服務建議以「地端執行、人工覆核、全程追溯、證據驗收」為核心，將影像辨識、TAIDE 解析、16 類案件擴增、定型稿、外部介接、追蹤報表與既有系統維護整合為一條受控作業鏈。技術上延續既有 Windows、SQL Server、Ubuntu、Docker 與 Spring Boot 環境，以分層架構、安全 API、版本化模型與提示、規則驗證及人工核准控制相容性與生成式 AI 風險；管理上由需求基線、三期查核、測試 V 模型、變更與發布清冊、月檢討及保固工單維持範圍、時程、品質與責任一致。

主要風險包括影像品質差異、模型無依據內容、跨系統交易不確定、權限與敏感資料、供應鏈弱點、重大變更及知識集中。對應控制不是單點工具，而是輸入最小化、來源並列、角色分權、交易冪等、原始碼與組件治理、弱點修補複測、備份復原演練及接手實作所形成的閉環。每項控制均連至日誌、測試、工單、清冊、報告或簽認，讓機關能從需求追到正式版本，也能從缺失回查影響及改善。

交付依決標後工作計畫、需求確認、運轉測試與資安檢測、結案文件與程式碼、訓練移轉及保固月報逐期收斂；完成判定重視程式、文件、測試、資安與清冊同版，以及指定人員能依文件操作、維運與復原。價格以 7,980,000 元總包價完整編列直接薪資、直接執行費、公司管理費及稅費，明確資安經費 1,630,000 元，占比約 20.43%，並與三期 20%、40%、40%付款證據連動。整體預期價值在於提升案件資料整理與追蹤的一致性，同時保留業務判斷權、資料控制權與長期維運能力，使效率改善不以法遵、資安或可移轉性為代價。

參考文獻

1. 行政院（2023）。行政院及所屬機關（構）使用生成式 AI 參考指引。 行政院全球資訊網。 https://www.ey.gov.tw/Page/448DE008087A1971/40c1a925-121d-4b6b-8f40-7e9e1a5401f2
2. TAIDE 計畫團隊（2024）。TAIDE—推動臺灣可信任生成式 AI 發展計畫。 TAIDE。 https://www.taide.tw/
3. 數位發展部（2018）。資通安全管理法。 數位發展部主管法規共用系統。 https://law.moda.gov.tw/LawContent.aspx?id=FL088622
4. 數位發展部（2026）。資通安全責任等級分級辦法。 數位發展部主管法規共用系統。 https://law.moda.gov.tw/LawContent.aspx?id=FL089966&media=print
5. 法務部（2023）。個人資料保護法。 全國法規資料庫。 https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=I0050021
6. International Organization for Standardization; International Electrotechnical Commission（2022）。ISO/IEC 27001:2022 — Information security management systems。 ISO。 https://www.iso.org/standard/27001
7. National Institute of Standards and Technology（2022）。SP 800-218: Secure Software Development Framework (SSDF) Version 1.1。 NIST Computer Security Resource Center。 https://csrc.nist.gov/pubs/sp/800/218/final
8. OWASP Foundation（2021）。OWASP Top 10:2021。 OWASP。 https://owasp.org/Top10/2021/

附件一、附錄



版權所有 翻印必究