



NLSC-109-50

109 年度測繪成果圖冊管理系統 資料庫移轉採購案

Database Conversion of Surveying and
Mapping Results Management System in 2020

工作總報告書

主辦機關：內政部國土測繪中心

執行單位：恆隆科技股份有限公司

中 華 民 國 109 年 12 月 1 日

摘要

內政部國土測繪中心於地籍資料庫存管大量測繪成果資料及歷史性地籍圖冊，為確保圖籍資料保存完整性及提升管理服務效能，研訂自動化管理作業方式，於 99 年起委外開發「測繪成果圖冊管理系統」，導入無線射頻識別技術以強化地籍資料庫管理作業效率，並於 101 年及 102 年辦理功能擴充及系統維護；後續為整合「地籍測量資料管理系統」及相關功能，嗣於 103 年開發本系統更版，以改善整體籍點效率及圖籍借閱機制，達成圖庫管理自動化目標。

本系統現行系統係基於前述 103 年開發結果與 106 年及 107 年功能擴充後之架構，為配合政府資訊安全相關規定，並因應原作業環境中作業系統更新至 Windows Server 2019 及資料庫搬遷移轉至 Microsoft SQL Server 2019 等因素，故規劃將本系統及資料庫移轉至新設環境，除資料移轉外，另外亦配合新環境、資安規定將系統於原架構適度改寫調整與套用政府組態基準及檢驗資訊安全防護項目等工作。

本案相關工作完成後，將可確保圖冊管理作業持續順利執行，並使系統穩定安全無虞，除可達成政府資安政策外，亦可有效降低系統環境維運成本。

Abstract

The Land Surveying and Mapping Center of the Ministry of the Interior (NLSC) manages a large number of surveying and mapping results and historical cadastral data in the Cadastral Map Storage. In order to ensure the integrity and preservation of aforementioned data and improve the efficiency of management services, NLSC has developed an automated management operation method. Since 2010, NLSC has outsourced the development of "Survey and Mapping Results Management System", and introduced radio frequency identification technology to enhance the efficiency of Cadastral Map Storage management. Additionally, implemented the function expansion and the system maintenance in 2012 and 2013.

The current system is a newly version which had developed in 2014 and updated functions in 2017 and 2018, this project based on aforementioned system structure aim to transfer system to the new operating environment of NLSC, and migrate Oracle 10g database to MS SQL 2019 database. In addition, in accordance with the aforementioned environment parameters and security regulations, the system is appropriately rewritten and adjusted, and also to apply the Government Configuration Baseline (GCB) and checked the system security protection regulations.

After the completion of this project, it will ensure the continuous execution of the management and make the system stable and secure. In addition, to reduce the cost of system environmental maintenance effectively.

目錄

目錄.....	IV
圖目錄.....	V
表目錄.....	VI
壹、 專案概述	1
一、前言	1
二、現況描述	1
貳、 工作項目及內容	7
一、工作項目	7
二、工作方法及內容	8
參、 資料庫移轉及系統調校結果說明	18
一、本案工作項目結果	18
二、各階段成果繳交情形	30
肆、 本案相關建議事項及未來執行建議	35
伍、 附錄	37
一、資料庫移轉報告	37
二、套用 GCB 項目及測試結果	43
三、資安防護基準作業報告	67
四、作業計畫書審查意見	79
五、作業計畫書審查意見修正對照表	81
六、期中報告書審查意見	86
七、期中報告書審查意見修正對照表	88

圖目錄

圖 1 本系統硬體及網路架構	2
圖 2 本案軟體架構.....	3
圖 3 功能及選單架構	4
圖 4 資料轉換測試流程圖	10
圖 5 應用系統及 APP 修改調整	14
圖 6 應用系統 SSL 套用流程	15
圖 7 作業流程圖.....	17
圖 8 各項工作規劃執行進度	17
圖 9 原 Big-5 文字編碼與轉換後 UTF-8 編碼修正範例	20
圖 10 資料表移轉操作畫面	21
圖 11 資料表移轉完成記錄表	22
圖 12 資料表移轉後資料表型態	23
圖 13 轉換後 MSSQL 資料表架構	24
圖 14 新環境應用系統運行情形	25
圖 15 手持式 RFID 讀取器 APP 更新版次	26
圖 16 新版 APP 登入畫面	27
圖 17 新系統盤點紀錄	27
圖 18 套用 SSL 憑證之系統畫面	28
圖 19 新增應用系統登入驗證碼功能	29
圖 20 各項工作執行情形	32
圖 21 平板式 RFID 讀取器	36

表目錄

表 1 新舊環境一覽表	5
表 2 系統所存各類圖冊數量略表	6
表 3 移轉資料表清單	8
表 4 系統功能清單.....	10
表 5 套用 GCB 版次對照表	16
表 6 本案實際移轉資料表清單	18
表 7 本案排除未移轉清單	19
表 8 資料表轉換結果一覽表	24
表 9 套用 GCB 設定結果統計表	29
表 10 成果繳交情形一覽表	33
表 11 作業計畫書審查意見修正對照表	81
表 12 期中報告書審查意見修正對照表	88

壹、專案概述

一、前言

內政部國土測繪中心（以下簡稱機關）針對大量測繪成果圖冊資料，現以無線射頻識別技術(Radio Frequency Identification，RFID)進行管理，並建置「測繪成果圖冊管理系統」用於圖冊供應、統計及盤點管理等作業，前於 103 年整合各項圖冊資料庫，建立圖冊管理基本資料進行系統更版，續於 106 年及 107 年持續精進管理效能及擴充索引查詢功能。

本（109）年度為配合機關係統資安維護作業及資通系統向上集中政策，並因應 Windows Server 2008 作業系統已於本年 1 月 14 日終止支援等因素，規劃將本系統移轉至 Windows Server 2019 作業系統及 Microsoft SQL Server 2019 資料庫，並將系統功能（含手持式 RFID 讀取器 APP）依移轉後環境予以調整；期持續維運系統穩定作業，亦有效降低系統維護成本。

二、現況描述

機關存管各項測繪圖冊資料目前以本系統進行資料管理及借閱等工作，本案系統說明如下：

(一)系統架構：

本系統主要功能為資料管理、法院囑託鑑測資料、報表管理及系統設定等 4 大項目，系統使用者分為一般使用者及系統管理員 2 種身分別，依不同身分別具有圖冊查詢借調、資料管理及系統維護等不同操作權限。

(二)作業移轉後環境：

本系統主要使用 ASP.NET 3.5 及 ASP.NET AJAX 進行網頁應用程式開發，依三層式架構設計，即客戶端應用程式 (Client Application)、應用程式伺服器 (Server) 及資料庫伺服器 (RDBMS, Relational Database Management System) 等三個層次。目前系統可相容使用於 Microsoft Explorer 8.0 及 Chrome 85.x(含)以上瀏覽器，本系統硬體及網路架構如圖 1，軟體架構如圖 2，功能及選單架構如圖 3。

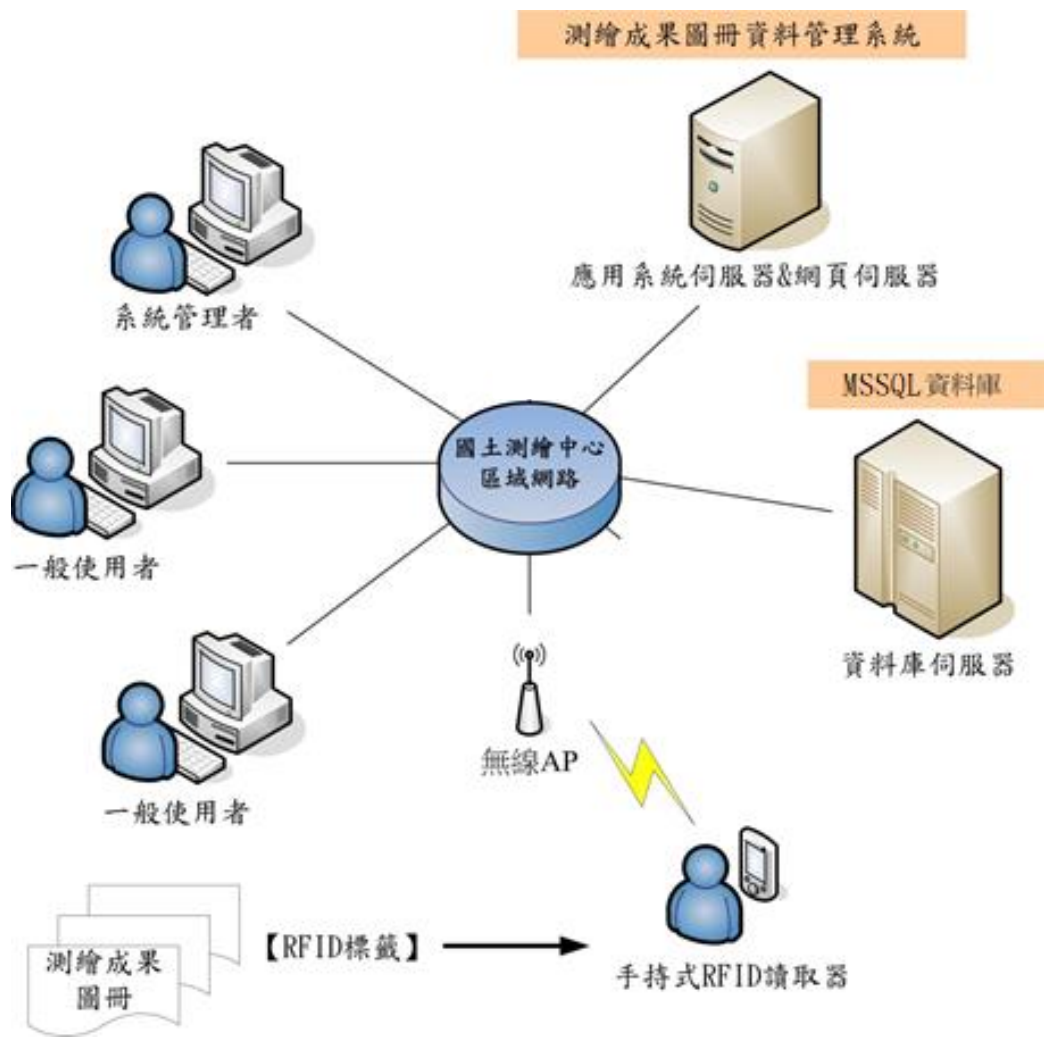


圖 1 本系統硬體及網路架構

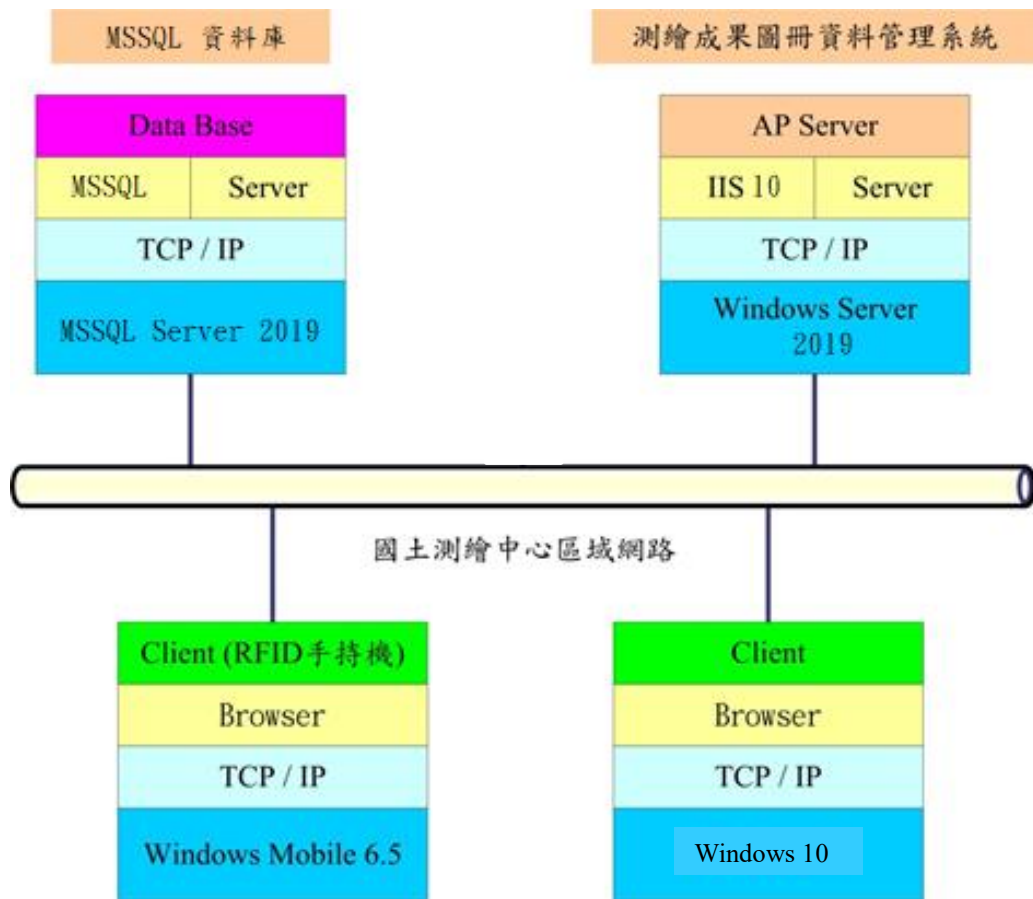


圖 2 本案軟體架構

測繪成果圖冊資料管理系統

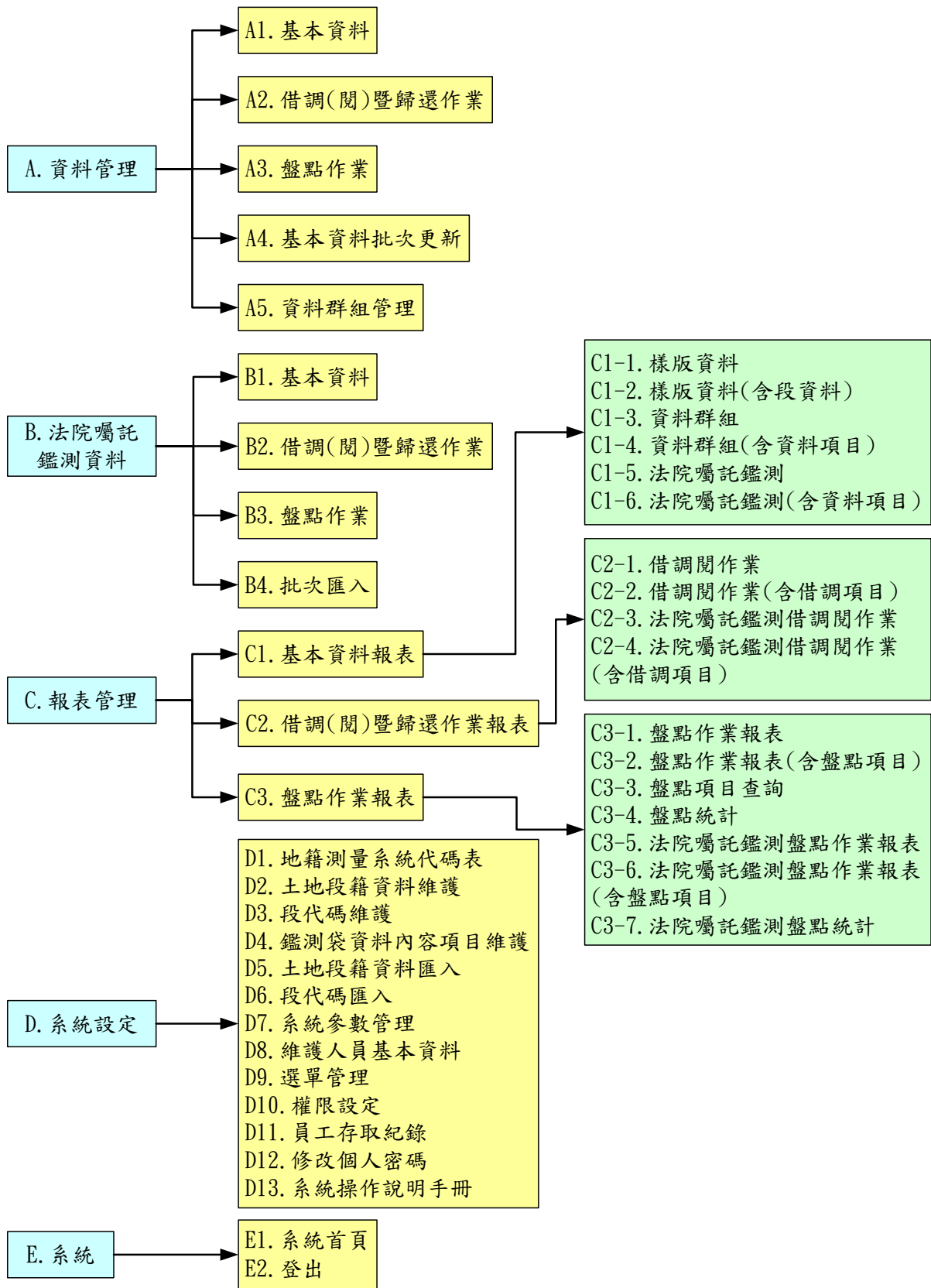


圖 3 功能及選單架構

本案應用系統及資料庫將由原環境移轉至機關新設環境，移轉期間將就新環境進行系統應用程式及手持式 RFID 讀取器 APP 改寫並辦理資料庫轉換，新舊環境如表 1 所示，本系統主要用以儲存及管理各類地籍相關圖冊資料，目前所存圖冊種類及數量略如表 2 所示。

表 1 新舊環境一覽表

項目	原系統環境	移轉後環境	備註
作業系統	Microsoft Windows Server 2008	Microsoft Windows Server 2019 Datacenter	
網頁及應用系統服務	IIS7	IIS10	
資料庫	Oracle 10g RAC	Microsoft SQL Server 2019	
手持式 RFID 讀取器 APP	Windows Mobile 6.5	Windows Mobile 6.5	未異動
項目	原應用系統環境	移轉後應用系統環境	備註
CPU	Intel Xeon E5506 (2 cores)	Intel Xeon E5506 (2 cores)	
RAM	4GB	8GB	
硬碟	100GB	200GB	

表 2 系統所存各類圖冊數量略表

項次	資料種類別	單位	數量
1	地籍原圖	幅	246,651
2	土地面積計算表	冊	5,760
3	地籍藍晒底圖	幅	135,119
4	控制點成果資料	冊	5,010
5	都市計畫椿清理補建與聯測資料	冊	4,926
6	法院囑託鑑測資料	袋	約 7,066
7	地籍清冊	冊	1,226
8	地籍調查卡	冊	646
9	160 磅地籍藍晒圖	幅	49,958
10	基本資料檔案清冊	冊	17,194
11	典藏舊地籍圖	幅	16,626
12	官有林野圖	幅	2,219

貳、工作項目及內容

一、工作項目

本案主要工作項目包含「系統資料庫移轉」及「系統調整」等2項作業，契約所定工作項目如下：

(一) 系統資料庫移轉

1. 全面盤點本系統現行Oracle 資料庫需移轉項目及提出作業方法，上開規劃內容應納入作業計畫。
2. 依機關同意執行之作業計畫，移轉原系統資料庫至機關提供之MS SQL Server 2019 資料庫；並應確保移轉後系統正常運作。

(二) 系統調校

1. 全面盤點本系統相關功能，依機關提供之新版 Windows Server2019 及本案移轉後之MS SQL Server 2019 資料庫提出系統功能調校工作項目及辦理期程，相關規劃應納入作業計畫。
2. 依機關同意執行之作業計畫更新系統，確保系統功能及手持式RFID 讀取器APP 可於更新環境正常運作及正常讀寫本案移轉後MS SQL Server 2019 資料庫。
3. 調整本案網站全面採用SSL 加密傳遞作業方式。
4. 系統需配合導入行政院國家資通安全會報技術服務中心政府組態基準 (Government Configuration Baseline, GCB) 設定相關作業，且需符合資通系統防護基準安全等級(中級)各項規定。
5. 依據「資通安全管理法」子法「資通安全責任等級分級辦法」第11條規定及相關資通系統防護基準(含7大類別)執行相關控制措施，需配合進行修正調整並產出「資安防護基準作業報告」。

二、工作方法及內容

本案系統及資料庫依機關所提供之軟硬體環境改寫移轉，系統功能架構未予變更，僅依環境作必要之語法改寫；資料庫則由原有 Oracle 資料庫移轉至機關提供之 Microsoft SQL 2019 資料庫；依契約所列工作項目已依需求訪談結果，規劃工作方法及執行進度並依契約規定，提列於作業計畫經機關審核通過後，由本公司據以辦理相關工作，工作方法及進度如下：

(一) 工作方法

1. 系統資料移轉

(1) 全面盤點本系統現行 Oracle 資料庫需移轉項目及提出作業方法，上開規劃內容應納入作業計畫；規劃作業方式如下：

- I. 以機關資料相關程序申請遠端登入應用系統主機及資料庫，由機關原有資料庫中匯出系統所有資料表清單。
- II. 檢視系統所需資料表及確認資料表性質及數量後，將盤點結果及規劃移轉方法於作業計畫提列審查；本項資料表盤點結果略如表 3 所示。

表 3 移轉資料表清單

	table_name		table_name		table_name		table_name
1	CHECKED	21	IMPORT_ORGDATA	41	INFODATA_02_H	61	LOG_SQL
2	CHECKED_ITEM	22	IMFO_SCNO	42	INFODATA_02_I	62	MENU_COLLECTION
3	CODE	23	INFODATA	43	INFODATA_02_L	63	MENU_FUNCTION
4	CODE_TYEP	24	INFODATA_01_B	44	INFODATA_02_P	64	MENU_FUNCTION_CONTROL
5	DAT_OLSEC	25	INFODATA_01_C	45	INFODATA_02_R	65	MENU_FUNCTION_FREQUENT
6	DATCODE	26	INFODATA_01_D	46	INFODATA_02_S	66	MENU_SUBSYSTEM
7	DATDATA	27	INFODATA_01_F	47	INFODATA_02_X	67	ORG_SNCO
8	DATDATAM	28	INFODATA_01_G	48	LAWCOURT	68	ORGDATA
9	DATLRESULT	29	INFODATA_01_H	49	LAWCOURT_CHECKED	69	PARAMETER_SHEET
10	DATSEC	30	INFODATA_01_I	50	LAWCOURT_CHECKED_ITEM	70	RESOURCE_PIC
11	DATSECC	31	INFODATA_01_L	51	LAWCOURT_ITEM	71	RESOURCE_TEXT
12	DATSECC_TEMP	32	INFODATA_01_P	52	LAWCOURT_LIST	72	SN_COUNTER
13	EMPLOYEE	33	INFODATA_01_R	53	LAWCOURT_LOAN		
14	EMPLOYEE_LOG	34	INFODATA_01_S	54	LAWCOURT_LOAN_ITEM		
15	IMG_INDEX	35	INFODATA_01_X	55	LIMIT_FUNCTION		

16	IM_INDEX_E	36	INFODATA_02_B	56	LIMIT_FUNCTION_CONTROL		
17	IMPORT_DATSEC	37	INFODATA_02_C	57	LIMIT_GROUP		
18	IMPORT_DATSECC	38	INFODATA_02_D	58	LIMIT_MENU		
19	IMPORT_INFO	39	INFODATA_02_F	59	LOAN		
20	IMPORT_LAWCOURT	40	INFODATA_02_G	60	LOAN_ITEM		

(2) 依機關同意執行之作業計畫，移轉原系統資料庫至機關提供之 MS SQL Server 2019 資料庫，並應確保移轉後系統正常運作；規劃作業方式如下：

- I. 本案因應機關初期新設環境尚未完整建置，考量作業進度需先進行移轉測試，即規劃先由本公司建置之環境辦理相關測試。
- II. 為避免影響原系統執行效能，本公司於系統運作離峰時段，以遠端登入本系統 Oracle 資料庫，將盤點結果之系統所需資料表，以測試作業所需最小數量，傳送至本公司測試環境（具人員及資料進出管制機制）。
- III. 經評估各項轉換模式及工具後，於作業計畫中提出以微軟公司之 SSMA 工具（Microsoft SQL Server Migration Assistant for Oracle v8.8.0）進行資料庫移轉，再由本公司作業人員檢視 SSMA 產出之結果報告，進行異常情形處置。
- IV. 本應用系統資料表文字編碼原為 Big-5 編碼，經工作會議與機關工作小組討論，為解決罕字字無法正確顯示情形，故本案移轉後資料庫中，將資料本之文字編碼變更為 UTF-8 編碼並測試。
- V. 移轉異常情形處置確認後，將於正試移轉後，以本公司自行開發工具比對移轉前後資料表格式、內容、架構及數量一致，測試作業流程如圖 4 所示。

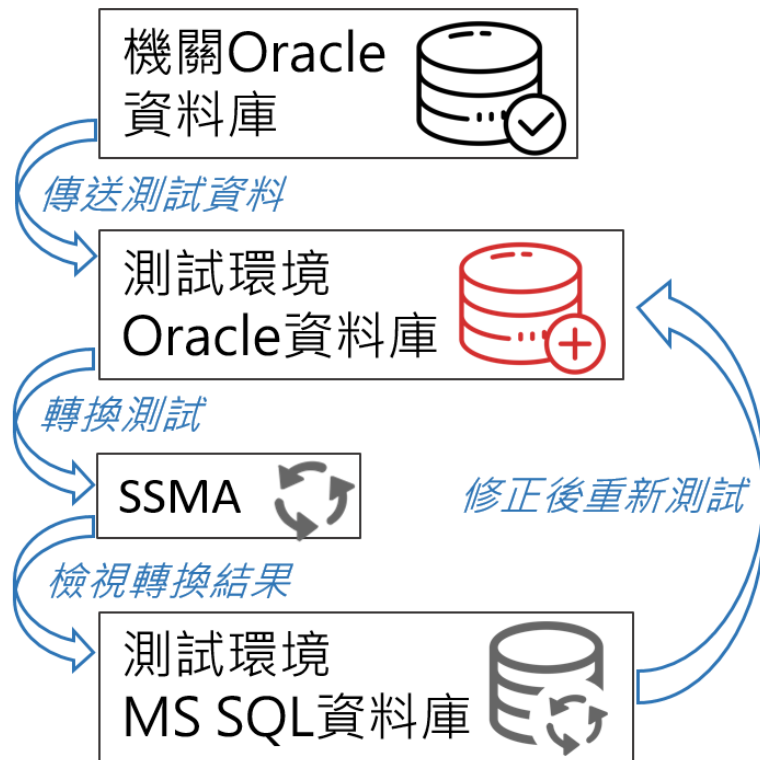


圖 4 資料轉換測試流程圖

2. 系統調校

(1) 全面盤點本系統相關功能，依機關提供之新版 Windows Server2019 及本案移轉後之 MS SQL Server 2019 資料庫提出系統功能調校工作項目及辦理期程，相關規劃應納入作業計畫：

- I. 以機關資料相關程序申請遠端登入應用系統主機及資料庫，並參考本案程式規格相關資料後，盤點系統功能及程式。
- II. 將盤點結果及規劃時程於作業計畫提列審查；本項系統功能及需調校之盤點結果略如表 4 所示

表 4 系統功能清單

系統項目名稱及描述
登入作業
資料管理-基本資料-新增

資料管理-基本資料-查詢
資料管理-基本資料-修改
資料管理-基本資料-刪除
資料管理-借(調)閱暨歸還作業-新增
資料管理-借(調)閱暨歸還作業-查詢
資料管理-借(調)閱暨歸還作業-修改
資料管理-借(調)閱暨歸還作業-刪除
資料管理-盤點作業-新增
資料管理-盤點作業-查詢
資料管理-盤點作業-修改
資料管理-盤點作業-刪除
資料管理-基本資料批次更新-新增
資料管理-基本資料批次更新-查詢
資料管理-基本資料批次更新-檢視
資料管理-基本資料批次更新-刪除
資料管理-資料群組管理-新增
資料管理-資料群組管理-查詢
資料管理-資料群組管理-修改
資料管理-資料群組管理-刪除
資料管理-資料群組批次更新-新增
資料管理-資料群組批次更新-查詢
資料管理-資料群組批次更新-修改
資料管理-資料群組批次更新-刪除
法院囑託鑑測資料-基本資料-新增
法院囑託鑑測資料-基本資料-查詢
法院囑託鑑測資料-基本資料-修改
法院囑託鑑測資料-基本資料-刪除
法院囑託鑑測資料-借(調)閱暨歸還作業-新增
法院囑託鑑測資料-借(調)閱暨歸還作業-查詢
法院囑託鑑測資料-借(調)閱暨歸還作業-修改
法院囑託鑑測資料-借(調)閱暨歸還作業-刪除
法院囑託鑑測資料-盤點作業-新增
法院囑託鑑測資料-盤點作業-查詢
法院囑託鑑測資料-盤點作業-修改
法院囑託鑑測資料-盤點作業-刪除
法院囑託鑑測資料-批次匯入-新增
法院囑託鑑測資料-批次匯入-查詢
法院囑託鑑測資料-批次匯入-檢視
法院囑託鑑測資料-批次匯入-刪除

報表管理-基本資料報表-樣板資料統計
報表管理-基本資料報表-樣板資料統計(含段資料)
報表管理-基本資料報表-資料群組統計
報表管理-基本資料報表-資料群組統計(含資料項目)
報表管理-基本資料報表-法院囑託鑑測資料統計
報表管理-基本資料報表-法院囑託鑑測資料統計(含資料項目)
報表管理-借調暨歸還作業報表-借調閱作業
報表管理-借調暨歸還作業報表-借調閱作業(含借調項目)
報表管理-借調暨歸還作業報表-法院囑託借調閱作業
報表管理-借調暨歸還作業報表-法院囑託借調閱作業(含借調項目)
報表管理-盤點作業-盤點作業報表
報表管理-盤點作業-盤點作業報表(含盤點項目)
報表管理-盤點作業-盤點項目查詢
報表管理-盤點作業-盤點統計
報表管理-盤點作業-法院囑託盤點作業報表
報表管理-盤點作業-法院囑託盤點作業報表(含盤點項目)
報表管理-盤點作業-法院囑託鑑測盤點統計
報表管理-盤點作業-地籍圖清查/抽查表
報表管理-盤點作業-圖冊數量統計
系統設定-地籍測量系統代碼表-新增
系統設定-地籍測量系統代碼表-查詢
系統設定-地籍測量系統代碼表-修改
系統設定-地籍測量系統代碼表-刪除
系統設定-土地段籍資料維護-新增
系統設定-土地段籍資料維護-查詢
系統設定-土地段籍資料維護-修改
系統設定-土地段籍資料維護-刪除
系統設定-段代碼維護-新增
系統設定-段代碼維護-查詢
系統設定-段代碼維護-修改
系統設定-段代碼維護-刪除
系統設定-土地段籍資料匯入-新增
系統設定-土地段籍資料匯入-查詢
系統設定-土地段籍資料匯入-修改
系統設定-土地段籍資料匯入-刪除
系統設定-段代碼匯入-新增
系統設定-段代碼匯入-查詢
系統設定-段代碼匯入-修改
系統設定-段代碼匯入-刪除

系統設定-鑑測袋資料內容項目維護-新增
系統設定-鑑測袋資料內容項目維護-查詢
系統設定-鑑測袋資料內容項目維護-修改
系統設定-鑑測袋資料內容項目維護-刪除
系統設定-代碼表-新增
系統設定-代碼表-查詢
系統設定-代碼表-修改
系統設定-代碼表-刪除
系統設定-系統參數管理-新增
系統設定-系統參數管理-查詢
系統設定-系統參數管理-修改
系統設定-系統參數管理-刪除
系統設定-維護人員基本資料-新增
系統設定-維護人員基本資料-查詢
系統設定-維護人員基本資料-修改
系統設定-維護人員基本資料-刪除
系統設定-選單管理-新增
系統設定-選單管理-查詢
系統設定-選單管理-修改
系統設定-選單管理-刪除
系統設定-權限設定-新增
系統設定-權限設定-查詢
系統設定-權限設定-修改
系統設定-權限設定-刪除
系統設定-員工存取記錄
系統設定-修改個人密碼
系統設定-系統操作說明手冊
系統-系統首頁
系統-登出

(2) 依機關同意執行之作業計畫更新系統，確保系統功能及手持式 RFID 讀取器 APP 可於更新環境正常運作及正常讀寫本案移轉後 MS SQL Server 2019 資料庫：

- I. 依作業計畫盤點結果更新本應用系統各項功能，針對程式碼中涉及作業環境及資料庫語法異動部分，進行調整改寫及測試。

II. 依移轉後應用系統及資料庫，修改手持式 RFID 讀取器之 APP 程式碼調整改寫及測試。

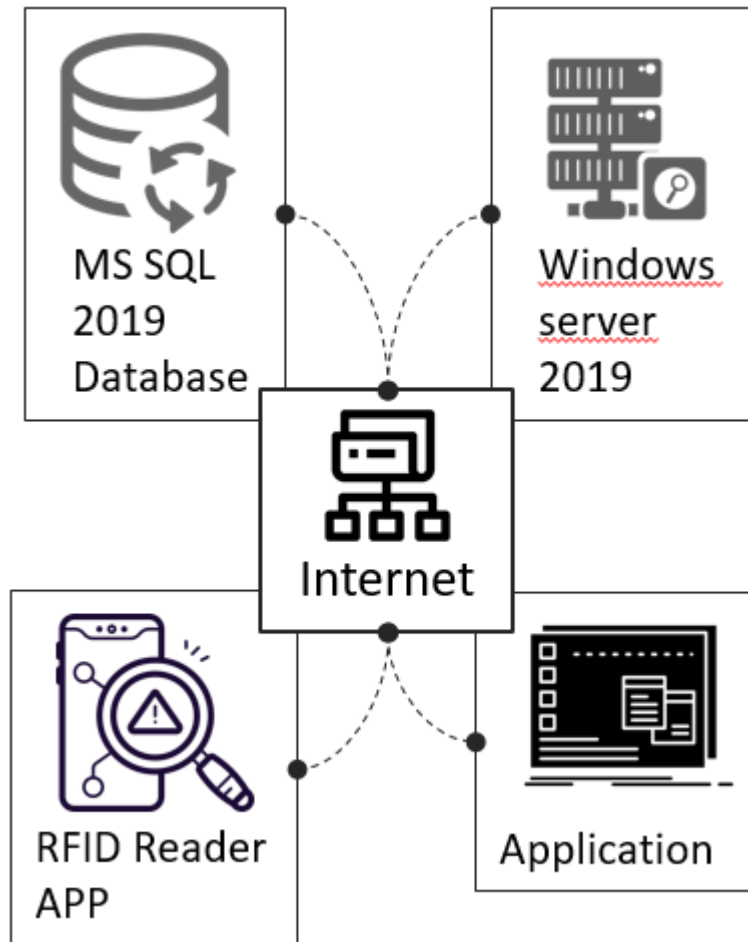


圖 5 應用系統及 APP 修改調整

(3) 調整本案網站全面採用 SSL 加密傳遞作業方式：

- I. 修改調校本應用系統中有關 SSL 之程式碼及相關功能。
- II. 依機關 ISMS 流程申請 SSL 憑證檔。
- III. 於機關建置之測試環境中安裝調校後應用系統及 SSL 憑證，並進行相關設定。
- IV. 測試系統套用 SSL 憑證後各項功能運行是否正常，本項工作流程如圖 6 所示。

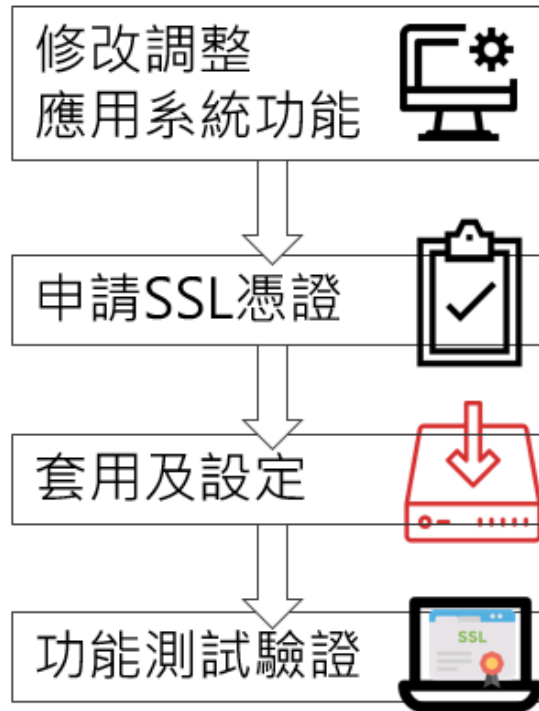


圖 6 應用系統 SSL 套用流程

(4) 系統需配合導入行政院國家資通安全會報技術服務中心政府組態基準 (Government Configuration Baseline, GCB) 設定相關作業，且需符合資通系統防護基準安全等級 (中級) 各項規定：

- I. 機關建置應用系統環境中作業系統等相關軟體，目前尚無可套用之政府組態基準 (GCB) 版次，故本案規劃先以「行政院國家資通安全會報技術服務中心」所發布最新版次 GCB 進行套用測試。
- II. 本案套用 GCB 種類及版次如表 5 所示。

表 5 套用 GCB 版次對照表

項目	機關新設環境	套用測試 GCB 版本
作業系統	Microsoft Windows Server 2019 Datacenter	Windows Server 2016
應用程式	Microsoft IIS10	Microsoft IIS 8.5
瀏覽器	Internet Explorer 11	Internet Explorer 11
	Google Chrome85.X	Google Chrome

(5) 依據「資通安全管理法」子法「資通安全責任等級分級辦法」第 11 條規定及相關資通系統防護基準(含 7 大類別)執行相關控制措施，需配合進行修正調整並產出「資安防護基準作業報告」：

- I. 依據機關所定本系統資安等級之系統防護基準項目，檢視本應用系統相關功能是否符合並進行修正。
- II. 依機關所定格式製作本應用系統之「資通系統防護基準表(中級)」。

(二) 工作進度規劃

本案工作辦理方式規劃於本案作業計畫及系統開發計畫，專案作業流程如圖 7 所示；各項工作規劃執行如圖 8 所示

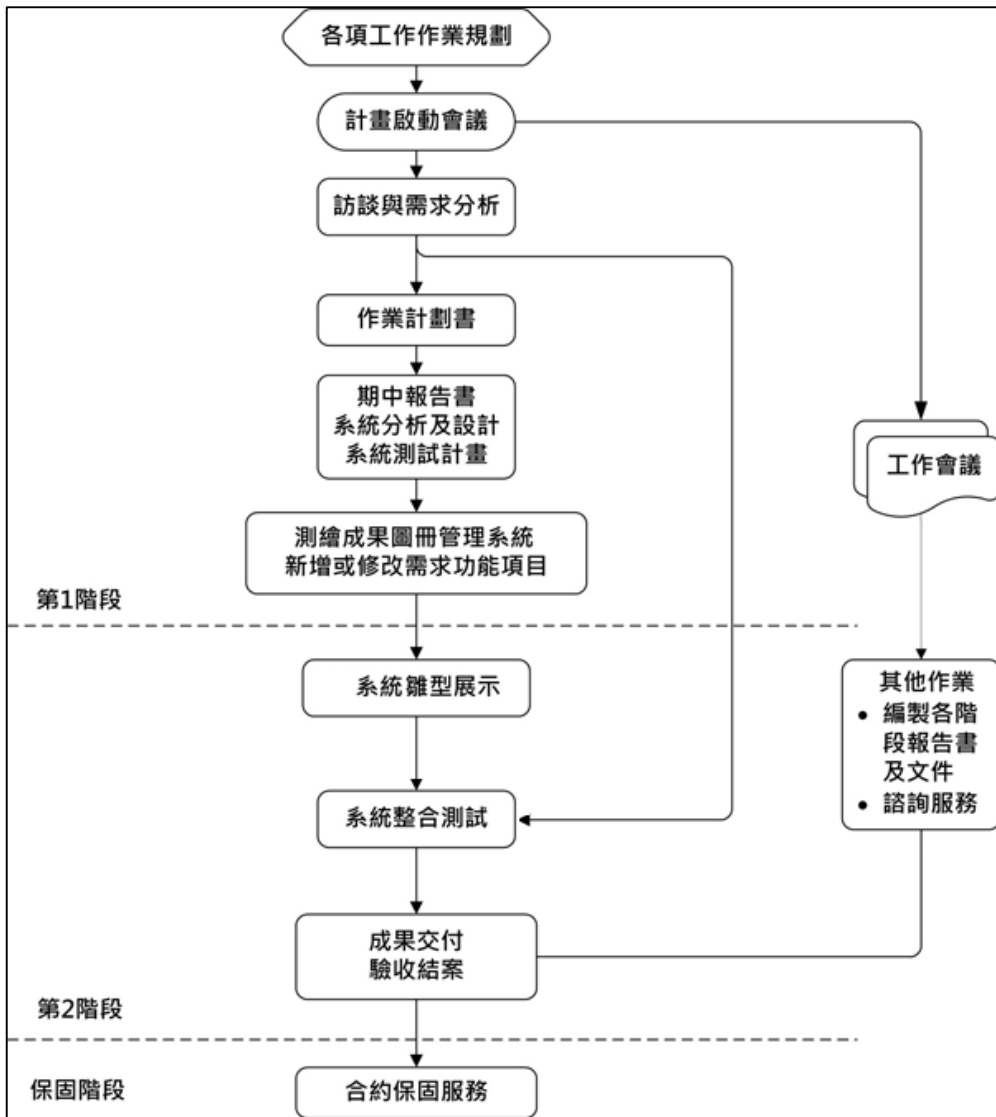


圖 7 作業流程圖

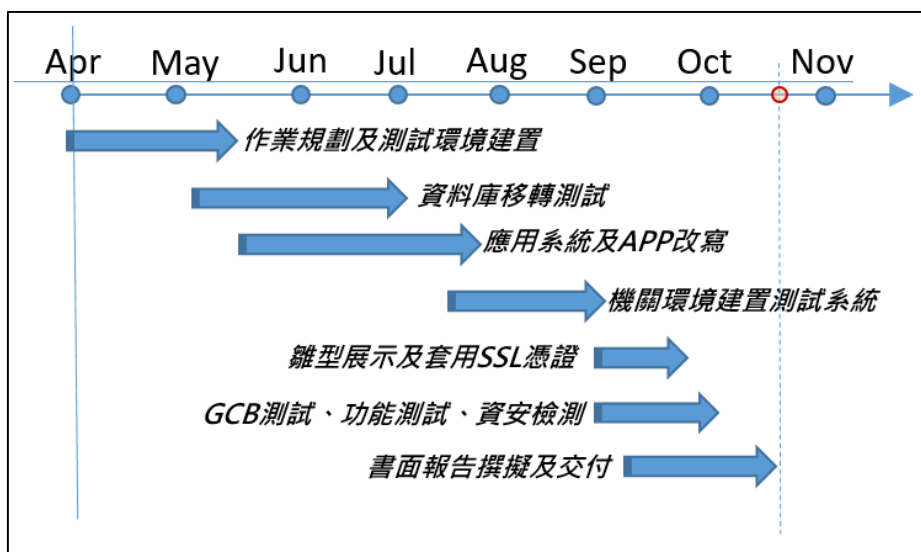


圖 8 各項工作規劃執行進度

參、資料庫移轉及系統調校結果說明

一、本案工作項目結果

本案主要工作項目為「系統資料庫移轉」及「系統調校」等 2 項，皆依作業計畫執行，並依契約所訂期程繳交各項成果，有關各項工作辦理結果說如如下：

一、系統資料庫移轉

1. 全面盤點本系統現行 Oracle 資料庫需移轉項目及提出作業方法，上開規劃內容應納入作業計畫：

- (1) 已依契約將本應用系統資料庫盤點結果，列於作業計劃並經機關審查通過。
- (2) 經比對各資料表內容及應用系統程式碼，發現部分資料表為系統開發初期作為測試、備份之用，於應用系統實際運行並無作用，為增加資料庫效能及有效利用資料表，故本案僅移轉本應用系統必要之資料表共 40 項（如表 6 所示），非必要之資料表共 32 項（如表 7 所示）則不予移轉。

表 6 本案實際移轉資料表清單

1	CHECKED	21	LAWCOURT_LIST
2	CHECKED_ITEM	22	LAWCOURT_LOAN
3	CODE	23	LAWCOURT_LOAN_ITEM
4	CODE_TYEP	24	LIMIT_FUNCTION
5	DATCODE	25	LIMIT_FUNCTION_CONTROL
6	DATSEC	26	LIMIT_GROUP
7	DATSECC	27	LIMIT_MENU
8	EMPLOYEE	28	LOAN
9	EMPLOYEE_LOG	29	LOAN_ITEM
10	IMPORT_DATSEC	30	LOG_SQL
11	IMPORT_DATSECC	31	MENU_COLLECTION
12	IMPORT_INFO	32	MENU_FUNCTION
13	IMPORT_LAWCOURT	33	MENU_FUNCTION_CONTROL
14	IMPORT_ORGDATA	34	MENU_FUNCTION_FREQUENT

15	IMFO_SCNO	35	MENU_SUBSYSTEM
16	INFODATA	36	ORG_SNCO
17	LAWCOURT	37	ORGDATA
18	LAWCOURT_CHECKED	38	PARAMETER_SHEET
19	LAWCOURT_CHECKED_ITEM	39	RESOURCE_TEXT
20	LAWCOURT_ITEM	40	SN_COUNTER

表 7 本案排除未移轉清單

1	DAT_OLSEC	17	INFODATA_01_R
2	DATDATA	18	INFODATA_01_S
3	DATDATAM	19	INFODATA_01_X
4	DATLRESULT	20	INFODATA_02_B
5	DATSECC_TEMP	21	INFODATA_02_C
6	IMG_INDEX	22	INFODATA_02_D
7	IM_INDEX_E	23	INFODATA_02_F
8	INFODATA_01_B	24	INFODATA_02_G
9	INFODATA_01_C	25	INFODATA_02_H
10	INFODATA_01_D	26	INFODATA_02_I
11	INFODATA_01_F	27	INFODATA_02_L
12	INFODATA_01_G	28	INFODATA_02_P
13	INFODATA_01_H	29	INFODATA_02_R
14	INFODATA_01_I	30	INFODATA_02_S
15	INFODATA_01_L	31	INFODATA_02_X
16	INFODATA_01_P	32	RESOURCE_PIC

- (3) 依機關要求將移轉後各資料表之文字編碼由 Big-5 編碼變更為 UTF-8 編碼，以解決罕用字顯示異常之問題；目前轉換完成後之 UTF-8 文字編碼資料表已可正常運作，惟原有罕用字因編碼無法轉換對照，故目前仍為亂碼狀態，需由機關工作人員確認正確文字後予以重新輸入修正即可（範例如圖 9 所示）。

<input type="checkbox"/>	段名	段代碼	段延伸碼	延伸碼說明
<input type="checkbox"/>	下	0034	4	89年鐵塔用地複丈圖

<input type="checkbox"/>	段名	段代碼	段延伸碼	延伸碼說明
<input type="checkbox"/>	廊下	0034	4	89年鐵塔用地複丈圖

圖 9 原 Big-5 文字編碼與轉換後 UTF-8 編碼修正範例

2. 依機關同意執行之作業計畫，移轉原系統資料庫至機關提供之 MS SQL Server 2019 資料庫，並應確保移轉後系統正常運作：
 - (1) 依機關核准之作業計劃所訂方式，以 SSMA 工具將本應用系統必要之 40 項資料表，由原有之 Oracle 10g 資料庫移轉至機關新建之 MS SQL Server 2019 資料庫。本項辦理方式及結果說明如下：
 - I. 使用 SSMA 進行資料庫轉移工具產出之報表，資料庫轉移採步驟簡述如下：
 - i. 於 MSSQL 建立新資料庫
 - ii. 同步資料表 Schema
 - iii. 同步資料表資料內容(如圖 10)
 - iv. 產生轉移報表(如圖 11)
 - II. 比對轉換資料表項目及數量

比對轉換前資料表與轉換後資料表資料型態及數量是否符合(如圖 12)。

III. 轉換後資料遺失疑慮處理:

依產出報表統計(Total Rows、Success Rate)判斷是否有資料遺失問題，再以人工方式進行修正。

IV. 轉換前後資料比對

原計劃使用自行開發應用程式檢驗轉換前後資料正確性，在 SSMA 轉換後產出的結果報表顯示比對後差異統計，因 SSMA 轉換後報表無異常情形，且經測試系統讀取及寫入資料庫比無誤，故無必要再使用應用程式工具進行驗證。

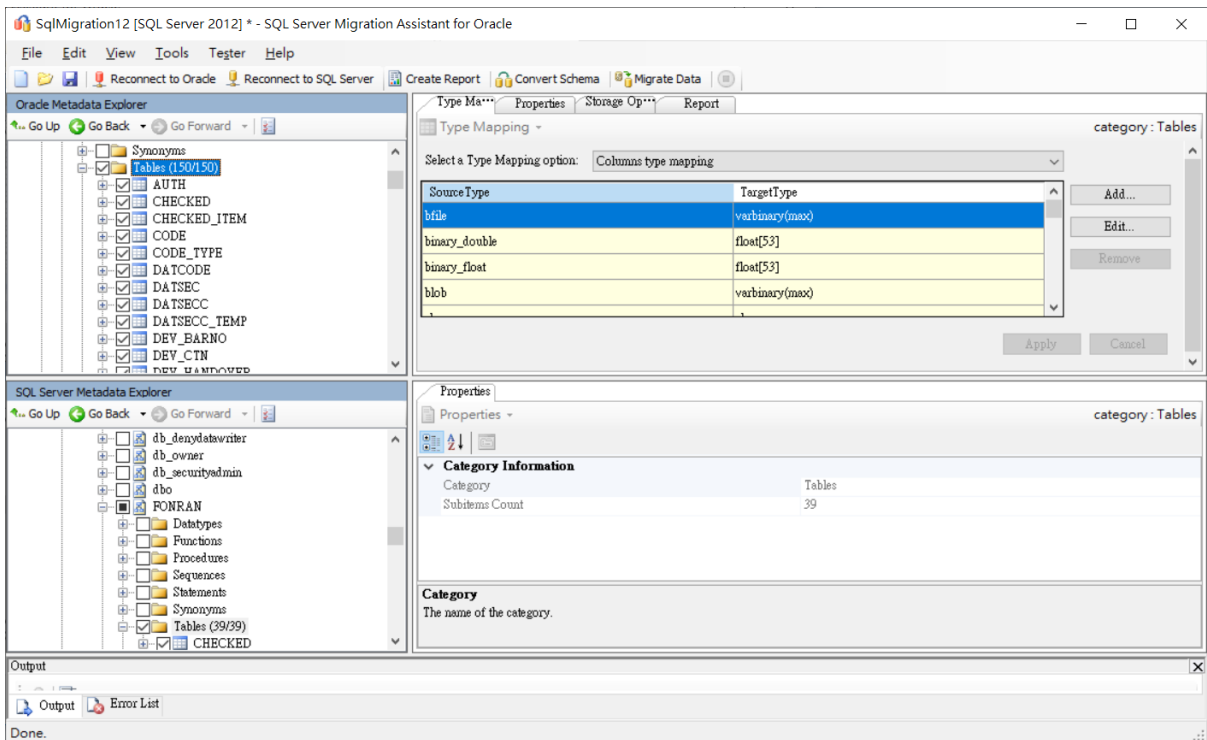


圖 10 資料表移轉操作畫面

Data Migration Report

Status	From	To	Total Rows	Migrated Rows	Success Rate	Duration (DD:HH:MM:SS.M)
📌	"FONRAN"."IMPORT_ORGDATA"	[[sb2020_20201124].[FONRAN].[IMPO	427	427	100.00%	00:00:01:14:608
📌	"FONRAN"."INFODATA"	[[sb2020_20201124].[FONRAN].[INFO	491741	491741	100.00%	00:00:00:02:231
📌	"FONRAN"."INFO_SCNO"	[[sb2020_20201124].[FONRAN].[INFO	463923	463923	100.00%	00:00:00:34:515
📌	"FONRAN"."IMPORT_LAWCOURT"	[[sb2020_20201124].[FONRAN].[IMPO	4	4	100.00%	00:00:01:15:766
📌	"FONRAN"."IMPORT_INFO"	[[sb2020_20201124].[FONRAN].[IMPO	43	43	100.00%	00:00:01:15:771
📌	"FONRAN"."IMPORT_DATSECC"	[[sb2020_20201124].[FONRAN].[IMPO	78	78	100.00%	00:00:01:15:746
📌	"FONRAN"."IMPORT_DATSEC"	[[sb2020_20201124].[FONRAN].[IMPO	5	5	100.00%	00:00:01:14:728
📌	"FONRAN"."EMPLOYEE_LOG"	[[sb2020_20201124].[FONRAN].[EMPL	73657	73657	100.00%	00:00:00:58:445
📌	"FONRAN"."EMPLOYEE"	[[sb2020_20201124].[FONRAN].[EMPL	23	23	100.00%	00:00:01:14:457
📌	"FONRAN"."DATSECC"	[[sb2020_20201124].[FONRAN].[DATS	17930	17930	100.00%	00:00:01:08:075
📌	"FONRAN"."DATSEC"	[[sb2020_20201124].[FONRAN].[DATS	26225	26225	100.00%	00:00:01:04:325
📌	"FONRAN"."DATCODE"	[[sb2020_20201124].[FONRAN].[DATC	1290	1290	100.00%	00:00:01:13:330
📌	"FONRAN"."CODE_TYPE"	[[sb2020_20201124].[FONRAN].[CODE	4	4	100.00%	00:00:01:13:351
📌	"FONRAN"."CODE"	[[sb2020_20201124].[FONRAN].[CODE	6	6	100.00%	00:00:01:13:348
📌	"FONRAN"."CHECKED_ITEM"	[[sb2020_20201124].[FONRAN].[CHEC	370908	370908	100.00%	00:00:00:34:638
📌	"FONRAN"."CHECKED"	[[sb2020_20201124].[FONRAN].[CHEC	12066	12066	100.00%	00:00:01:07:373
📌	"FONRAN"."SN_COUNTER"	[[sb2020_20201124].[FONRAN].[SN_C	1596	1596	100.00%	00:00:01:14:735
📌	"FONRAN"."RESOURCE_TEXT"	[[sb2020_20201124].[FONRAN].[RESC	2	2	100.00%	00:00:01:15:711
📌	"FONRAN"."PARAMETER_SHEET"	[[sb2020_20201124].[FONRAN].[PARA	8	8	100.00%	00:00:01:15:398
📌	"FONRAN"."ORG_SCNO"	[[sb2020_20201124].[FONRAN].[ORG	24755	24755	100.00%	00:00:01:11:758
📌	"FONRAN"."MENU_SUBSYSTEM"	[[sb2020_20201124].[FONRAN].[MENU	5	5	100.00%	00:00:01:15:768
📌	"FONRAN"."MENU_FUNCTION_FF"	[[sb2020_20201124].[FONRAN].[MENU	495	495	100.00%	00:00:01:15:745
📌	"FONRAN"."LAWCOURT_CHECKE"	[[sb2020_20201124].[FONRAN].[LAWC	1	1	100.00%	00:00:01:15:588
📌	"FONRAN"."LAWCOURT"	[[sb2020_20201124].[FONRAN].[LAWC	7135	7135	100.00%	00:00:01:10:838
📌	"FONRAN"."MENU_FUNCTION_C"	[[sb2020_20201124].[FONRAN].[MENU	0	0	100.00%	00:00:01:15:676
📌	"FONRAN"."MENU_FUNCTION"	[[sb2020_20201124].[FONRAN].[MENU	52	52	100.00%	00:00:01:15:318
📌	"FONRAN"."MENU_COLLECTION"	[[sb2020_20201124].[FONRAN].[MENU	33	33	100.00%	00:00:01:15:298
📌	"FONRAN"."LOG_SQL"	[[sb2020_20201124].[FONRAN].[LOG_	0	0	100.00%	00:00:01:15:821
📌	"FONRAN"."LOAN_ITEM"	[[sb2020_20201124].[FONRAN].[LOAN	3098	3098	100.00%	00:00:01:13:613
📌	"FONRAN"."LOAN"	[[sb2020_20201124].[FONRAN].[LOAN	1877	1877	100.00%	00:00:01:15:125
📌	"FONRAN"."LIMIT_MENU"	[[sb2020_20201124].[FONRAN].[LIMIT	179	179	100.00%	00:00:01:15:747
📌	"FONRAN"."LIMIT_GROUP"	[[sb2020_20201124].[FONRAN].[LIMIT	2	2	100.00%	00:00:01:15:625
📌	"FONRAN"."LIMIT_FUNCTION_C"	[[sb2020_20201124].[FONRAN].[LIMIT	0	0	100.00%	00:00:01:15:993
📌	"FONRAN"."LIMIT_FUNCTION"	[[sb2020_20201124].[FONRAN].[LIMIT	204	204	100.00%	00:00:01:15:435
📌	"FONRAN"."LAWCOURT_LOAN_I"	[[sb2020_20201124].[FONRAN].[LAWC	79	79	100.00%	00:00:01:15:817
📌	"FONRAN"."LAWCOURT_LOAN"	[[sb2020_20201124].[FONRAN].[LAWC	495	495	100.00%	00:00:01:14:106
📌	"FONRAN"."LAWCOURT_LIST"	[[sb2020_20201124].[FONRAN].[LAWC	21	21	100.00%	00:00:01:15:741
📌	"FONRAN"."LAWCOURT_ITEM"	[[sb2020_20201124].[FONRAN].[LAWC	3834	3834	100.00%	00:00:01:12:331
📌	"FONRAN"."LAWCOURT_CHECKE"	[[sb2020_20201124].[FONRAN].[LAWC	0	0	100.00%	00:00:01:15:928

Details Save Report Close

圖 11 資料表移轉完成記錄表

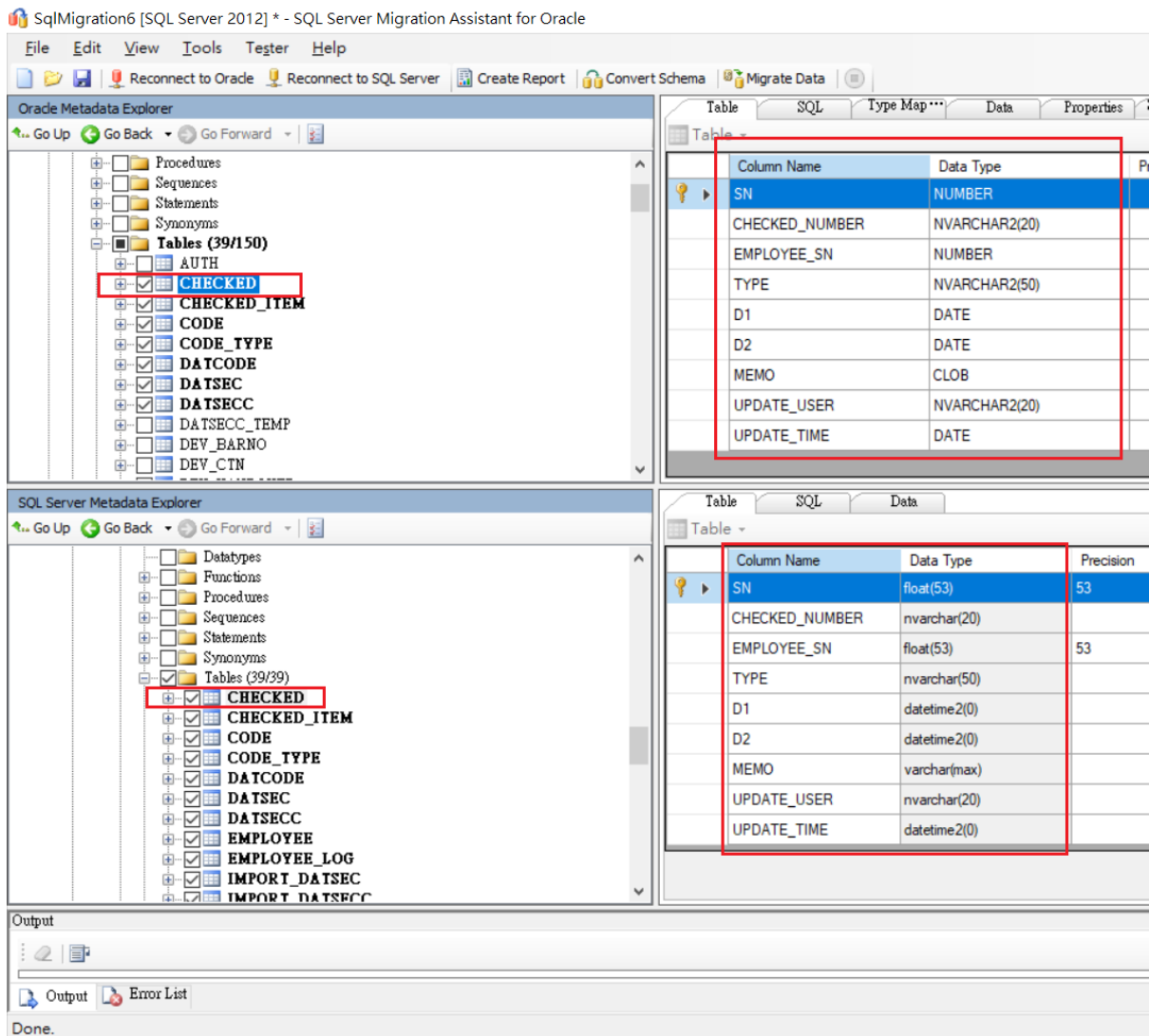


圖 12 資料表移轉後資料表型態

- (2) 資料表移轉後，經本公司檢視 SSMA 移轉報告確認無異常或失敗情形，再實際測試應用系統運行及讀寫資料數據正確無誤，故已無需再以工具進行細部比對。
- (3) 移轉後資料表架構如圖 13 所示，資料表轉換結果統計表如表 8 所示，轉換工具執行結果報告錄於本報告附錄。

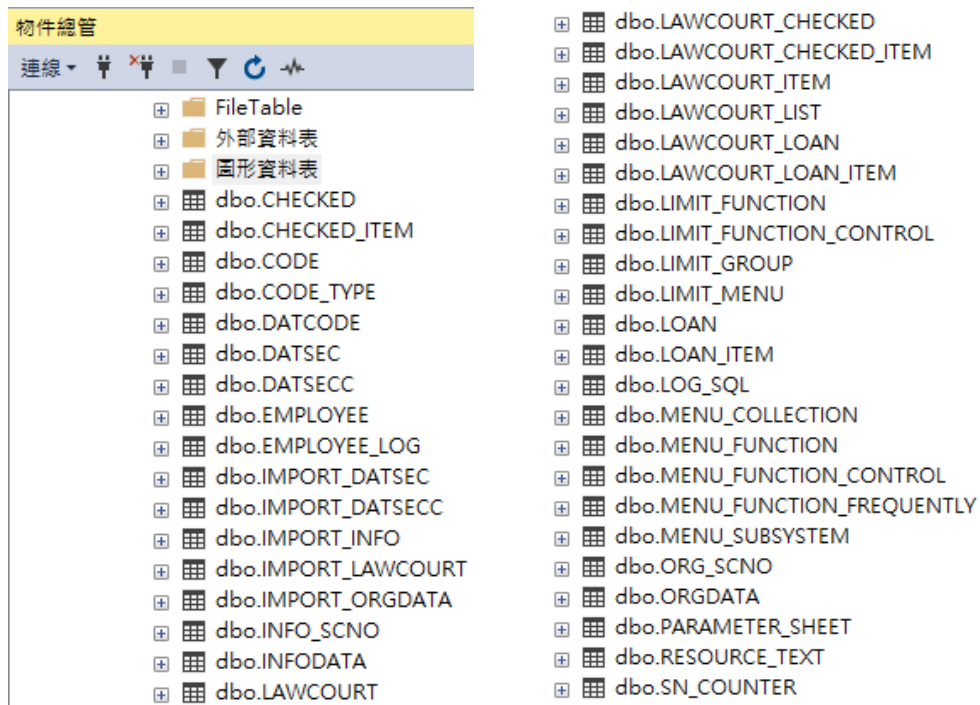


圖 13 轉換後 MSSQL 資料表架構

表 8 資料表轉換結果一覽表

	資料表	轉換前 資料量	轉換後 資料量		資料表	轉換前 資料量	轉換後 資料量
1	CHECKED	12066	12066	21	LAWCOURT_LIST	21	21
2	CHECKED_ITEM	370908	370908	22	LAWCOURT_LOAN	495	495
3	CODE	6	6	23	LAWCOURT_LOAN_ITEM	79	79
4	CODE_TYEP	4	4	24	LIMIT_FUNCTION	204	204
5	DATCODE	1209	1209	25	LIMIT_FUNCTION_CONTROL	0	0
6	DATSEC	26225	26225	26	LIMIT_GROUP	2	2
7	DATSECC	17930	17930	27	LIMIT_MENU	179	179
8	EMPLOYEE	23	23	28	LOAN	1877	1877
9	EMPLOYEE_LOG	73657	73657	29	LOAN_ITEM	3098	3098
10	IMPORT_DATSEC	5	5	30	LOG_SQL	0	0
11	IMPORT_DATSECC	78	78	31	MENU_COLLECTION	33	33
12	IMPORT_INFO	43	43	32	MENU_FUNCTION	52	52
13	IMPORT_LAWCOURT	4	4	33	MENU_FUNCTION_CONTROL	0	0
14	IMPORT_ORGDATA	427	427	34	MENU_FUNCTION_FREQUENT	495	495
15	IMFO_SCNO	463923	463923	35	MENU_SUBSYSTEM	5	5
16	INFODATA	491741	491741	36	ORG_SNCO	24755	24755
17	LAWCOURT	7135	7135	37	ORGDATA		
18	LAWCOURT_CHECKED	1	1	38	PARAMETER_SHEET	8	8
19	LAWCOURT_CHECKED_ITEM	0	0	39	RESOURCE_TEXT	2	2
20	LAWCOURT_ITEM	3834	3834	40	SN_COUNTER	1596	1596

二、系統調整

1. 全面盤點本系統相關功能，依機關提供之新版 Windows Server 2019 及本案移轉後之 MS SQL Server 2019 資料庫提出系統功能調校工作項目及辦理期程，相關規劃應納入作業計畫：

- (1) 已依契約將本應用系統各項功能盤點結果，列於作業計畫並經機關審查通過。
- (2) 本案應用系統依機關審核通過之作業計畫及功能盤點結果，進行系統移轉，未進行系統架構及功能之增修，僅配合機關提供之新設環境及資料庫種類，檢視應用系統程式碼及相關語法予以適度改寫。

2. 依機關同意執行之作業計畫更新系統，確保系統功能及手持式 RFID 讀取器 APP 可於更新環境正常運作及正常讀寫本案移轉後 MS SQL Server 2019 資料庫。

- (1) 將改寫並初步測試無誤之應用系統，於機關提供之測試環境完成建置及設定，經持續測試及修正後，現俟機關驗收無誤後即正式切換上線，並停用原有系統；新環境應用系統運行畫面截圖如圖 14 所示。

資料類別	資料類別	縣市	資料詳述	RFID	地稅	信託	存儲位置	比例尺	修改人員	修改日期	修改
地籍(測繪原)區(鎮區片-S00磅)	修正測繪原	臺中市 北區 中正	000001 0028	016666050303480000010028	乾清子-0303	在庫	1樓-1排-1層-4格	600	陸	2020/9/14 下午 03:40:14	修改
地籍(測繪原)區(鎮區片-S00磅)	修正測繪原	臺中市 北區 中正	000001 0029	016666050303480000010029	乾清子-0303	在庫	1樓-1排-1層-4格	600			修改
地籍(測繪原)區(鎮區片-S00磅)	修正測繪原	臺中市 北區 中正	000001 0030	016666050303480000010030	乾清子-0303	在庫	1樓-1排-1層-4格	600			修改
地籍(測繪原)區(鎮區片-S00磅)	修正測繪原	臺中市 北區 中正	000001 0031	016666050303480000010031	乾清子-0303	在庫	1樓-1排-1層-4格	600			修改
地籍(測繪原)區(鎮區片-S00磅)	修正測繪原	臺中市 北區 中正	000001 0032	016666050303480000010032	乾清子-0303	在庫	1樓-1排-1層-4格	600			修改
地籍(測繪原)區(鎮區片-S00磅)	修正測繪原	臺中市 北區 中正	000001 0033	016666050303480000010033	乾清子-0303	在庫	1樓-1排-1層-4格	600			修改
地籍(測繪原)區(鎮區片-S00磅)	修正測繪原	臺中市 北區 中正	000001 0036	016666050303480000010036	乾清子-0303	在庫	1樓-1排-1層-4格	600			修改
地籍(測繪原)區(鎮區片-S00磅)	修正測繪原	臺中市 北區 中正	000001 0037	016666050303480000010037	乾清子-0303	在庫	1樓-1排-1層-4格	600			修改
地籍(測繪原)區(鎮區片-S00磅)	修正測繪原	臺中市 北區 中正	000001 0038	016666050303480000010038	乾清子-0303	在庫	1樓-1排-1層-4格	600			修改
地籍(測繪原)區(鎮區片-S00磅)	修正測繪原	臺中市 北區 中正	000001 0039	016666050303480000010039	乾清子-0303	在庫	1樓-1排-1層-4格	600			修改
地籍(測繪原)區(鎮區片-S00磅)	修正測繪原	臺中市 北區 中正	000001 0040	016666050303480000010040	乾清子-0303	在庫	1樓-1排-1層-4格	600			修改
地籍(測繪原)區(鎮區片-S00磅)	修正測繪原	臺中市 北區 中正	000001 0041	016666050303480000010041	乾清子-0303	在庫	1樓-1排-1層-4格	600			修改
地籍(測繪原)區(鎮區片-S00磅)	修正測繪原	臺中市 北區 中正	000001 0042	016666050303480000010042	乾清子-0303	在庫	1樓-1排-1層-4格	600			修改
地籍(測繪原)區(鎮區片-S00磅)	修正測繪原	臺中市 北區 中正	000001 0006	016666050303480000010006	乾清子-0303	在庫	1樓-1排-1層-4格	600			修改
地籍(測繪原)區(鎮區片-S00磅)	修正測繪原	臺中市 北區 中正	000001 0007	016666050303480000010007	乾清子-0303	在庫	1樓-1排-1層-4格	600			修改
地籍(測繪原)區(鎮區片-S00磅)	修正測繪原	臺中市 北區 中正	000001 0008	016666050303480000010008	乾清子-0303	在庫	1樓-1排-1層-4格	600			修改
地籍(測繪原)區(鎮區片-S00磅)	修正測繪原	臺中市 北區 中正	000001 0009	016666050303480000010009	乾清子-0303	在庫	1樓-1排-1層-4格	600			修改
地籍(測繪原)區(鎮區片-S00磅)	修正測繪原	臺中市 北區 中正	000001 0010	016666050303480000010010	乾清子-0303	在庫	1樓-1排-1層-4格	600			修改
地籍(測繪原)區(鎮區片-S00磅)	修正測繪原	臺中市 北區 中正	000001 0011	016666050303480000010011	乾清子-0303	在庫	1樓-1排-1層-4格	600			修改
地籍(測繪原)區(鎮區片-S00磅)	修正測繪原	臺中市 北區 中正	000001 0017	016666050303480000010017	乾清子-0303	在庫	1樓-1排-1層-4格	600			修改
地籍(測繪原)區(鎮區片-S00磅)	修正測繪原	臺中市 北區 中正	000001 0018	016666050303480000010018	乾清子-0303	在庫	1樓-1排-1層-4格	600			修改

圖 14 新環境應用系統運行情形

- (2) 手持式 RFID 讀取器 APP 已完成更新版本 (AT880 V1.5 版, 如圖 15) 安裝, 並請機關進行測試作業, 登圖畫面如圖 16, 經測試已可正常執行運作, 並將盤點紀錄傳至應用系統及資料庫 (如圖 17)。



圖 15 手持式 RFID 讀取器 APP 更新版次



圖 16 新版 APP 登入畫面



圖 17 新系統盤點紀錄

3. 調整本案網站全面採用 SSL 加密傳遞作業方式。

- (1) 經申請機關 SSL 憑證並於機關新設環境進行套用設定，暫以本應用系統虛擬主機名稱為域名，經套用 SSL 憑證後之應用系統網址暫為：https://atlases.nlsc.gov.tw。
- (2) 本應用系統套用 SSL 憑證後，經本公司及機關進行測試無誤，系統首頁畫面如圖 18 所示。

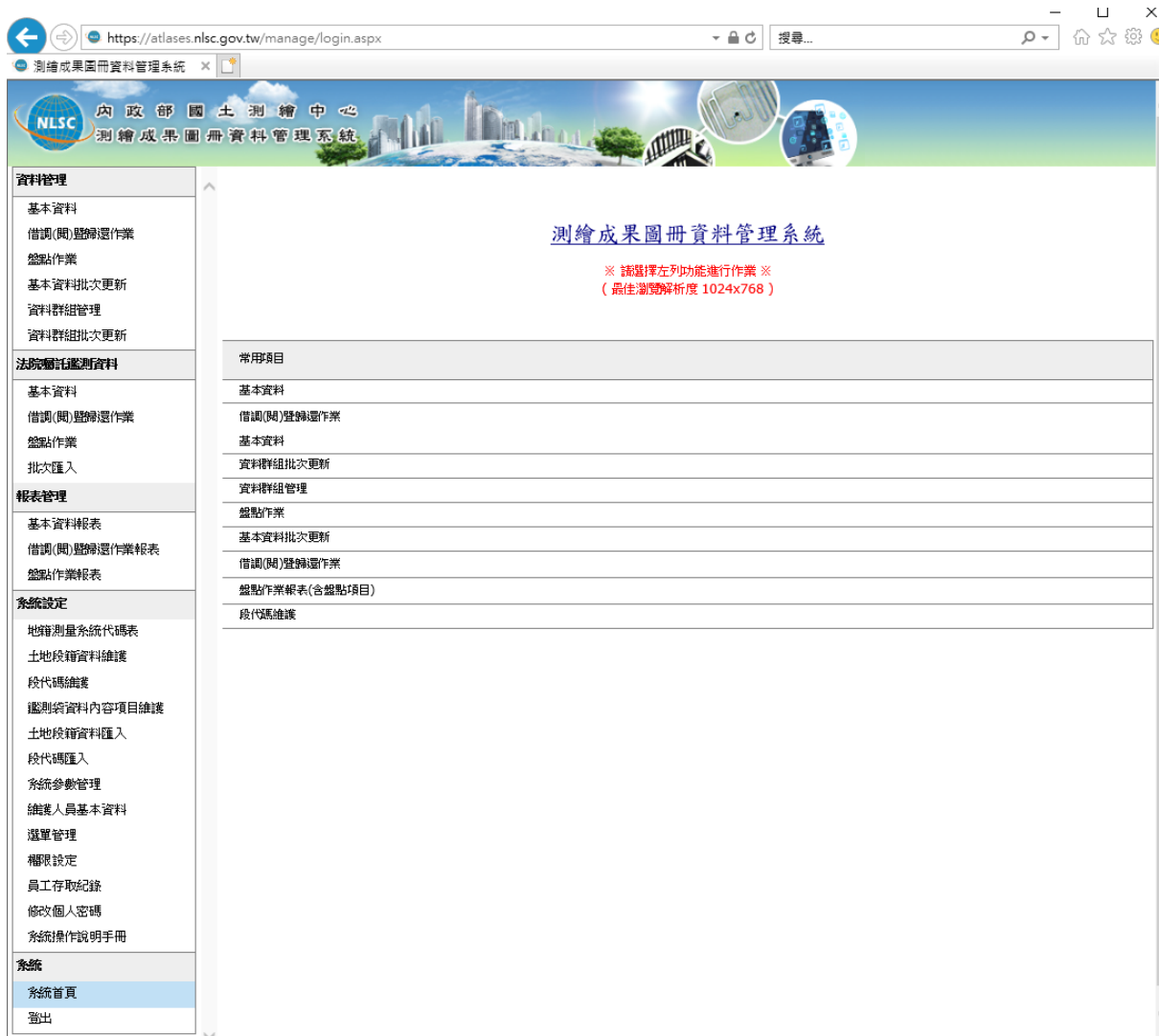


圖 18 套用 SSL 憑證之系統畫面

4. 系統需配合導入行政院國家資通安全會報技術服務中心政府組態基準 (Government Configuration Baseline, GCB) 設定相關作業，且需符合資通系統防護基準安全等級 (中級) 各項規定：
 - (1) 依據機關資安相關規定及防護基準所訂要項，檢視系統是否符合，並進行必要修正，如新增應用系統登入雙重驗證機制 (驗證碼，如圖 19)。



圖 19 新增應用系統登入驗證碼功能

- (2) 依機關審核通過之作業計畫，以現行最新版本 GCB 進行套用，套用結果經本公司實際測試應用系統運行狀態，各項功能皆可正常運作無誤，套用項目錄於本報告之附錄，套用情形略表如表 9 所示。

表 9 套用 GCB 設定結果統計表

項目	機關新設環境	套用測試版本	應套用項目數量	套用結果正常數量	應排除項目數量
作業系統	Microsoft Windows Server 2019 Datacenter	Windows Server 2016 (基本項目)	299	299	0
應用程式	Microsoft IIS10	Microsoft IIS 8.5	53	53	0

瀏覽器	Internet Explorer 11	Internet Explorer 11	154	154	0
	Google Chrome85.X	Google Chrome	33	29	4

5. 依據「資通安全管理法」子法「資通安全責任等級分級辦法」第 11 條規定及相關資通系統防護基準（含 7 大類別）執行相關控制措施，需配合進行修正調整並產出「資安防護基準作業報告」：

- (1) 已依機關資安相關規定檢視並修政本應用系統相關功能及設定。
- (2) 依契約規定產出「資安防護基準作業報告」並錄於本報告附錄及成果光碟。

二、各階段成果繳交情形

本案工作期程自決標次日起 180 個日曆天，相關工作依契約分 2 階段辦理，各階段成果亦分為 2 批次繳交；本專案係於 109 年 4 月 20 日決標，工作期程至 109 年 10 月 17 日止；各項成果辦理進度及繳交情形如圖 17 及表 10 所示，說明如下：

(一) 第 1 階段：

1. 第 1 批成果：應於決標次日起至 30 個日曆天(5 月 20 日)內辦竣需求訪談作業，並依據本案工作項目內容及功能需求訪談紀錄，撰擬本案作業計畫，並交付作業計畫 6 份及電子檔 1 份，作業計畫內容至少應包含：

- 作業目標與範圍
- 資料庫移轉之方法與技術（含資料庫盤點結果）
- 系統相關調整項目（含系統盤點結果）
- 工作時程規劃
- 品質管制
- 對於本案執行之加強及需協助事項。

本公司業於 4 月 27 日至機關辦理需求訪談，並於 5 月 20

日函送本案作業計畫，經機關審核後，續於6月30日函送修正後作業計畫，於7月17日機關函知本公司本批成果審查通過。

2. 第2批成果：應於決標次日起100個日曆天（7月29日）內，須依據機關資訊安全管理系統「資訊系統開發管理程序」及「資訊系統上線管理程序」，交付資訊系統開發計畫、資訊系統需求規格、資訊系統設計規格及系統測試計畫6份及電子檔1份送交機關審查。本批成果業於7月28日函送，經機關審查後，於9月9日函送修正後成果，並於9月29日機關通知審查通過，本階段成果驗收合格。

（二）第2階段：

1. 第1批成果：應於決標次日起至150個日曆天（9月17日）內，於機關指定地點辦理系統展示。本公司已於9月17日至機關辦竣系統雛型展示，並於9月25日函送雛型展示相關文件。
2. 第2批成果：應於決標次日起180個日曆天（10月17日，因例假日，延至10月19日）內完成本案系統資料庫移轉及系統調整作業（含手持式RFID讀取器APP）並交付下列成果：

（1）完成本案工作總報告初稿6份及電子檔1份送交機關辦理期末審查作業，內容至少須包含：

- 專案概述
- 工作項目及內容
- 資料庫移轉及系統調校結果說明
- 本案工作之相關建議事項及未來執行建議
- 其他相關資料及附件（含資料庫移轉報告、套用GCB測試結果及資安防護基準作業報告）

（2）依機關資訊安全管理系統「資訊系統開發管理程序」及「資訊系統上線管理程序」繳交本案系統測試報告、資訊安全檢測報告、程式規格（含程式清冊、程式清單、檔案清冊、資料庫格式）、資訊系統使用手冊6份及電子檔1份送交機關審查。

(3) 繳交本案相關系統之系統完整原始程式碼檔案
 (含編譯所需函式庫)、執行檔、系統自動安裝光
 碟電子檔 1 份送交機關審查。

本公司業於 10 月 19 日繳交本批成果，經機關審查後
 提供修正意見，本公司則據以修正相關成果報告。

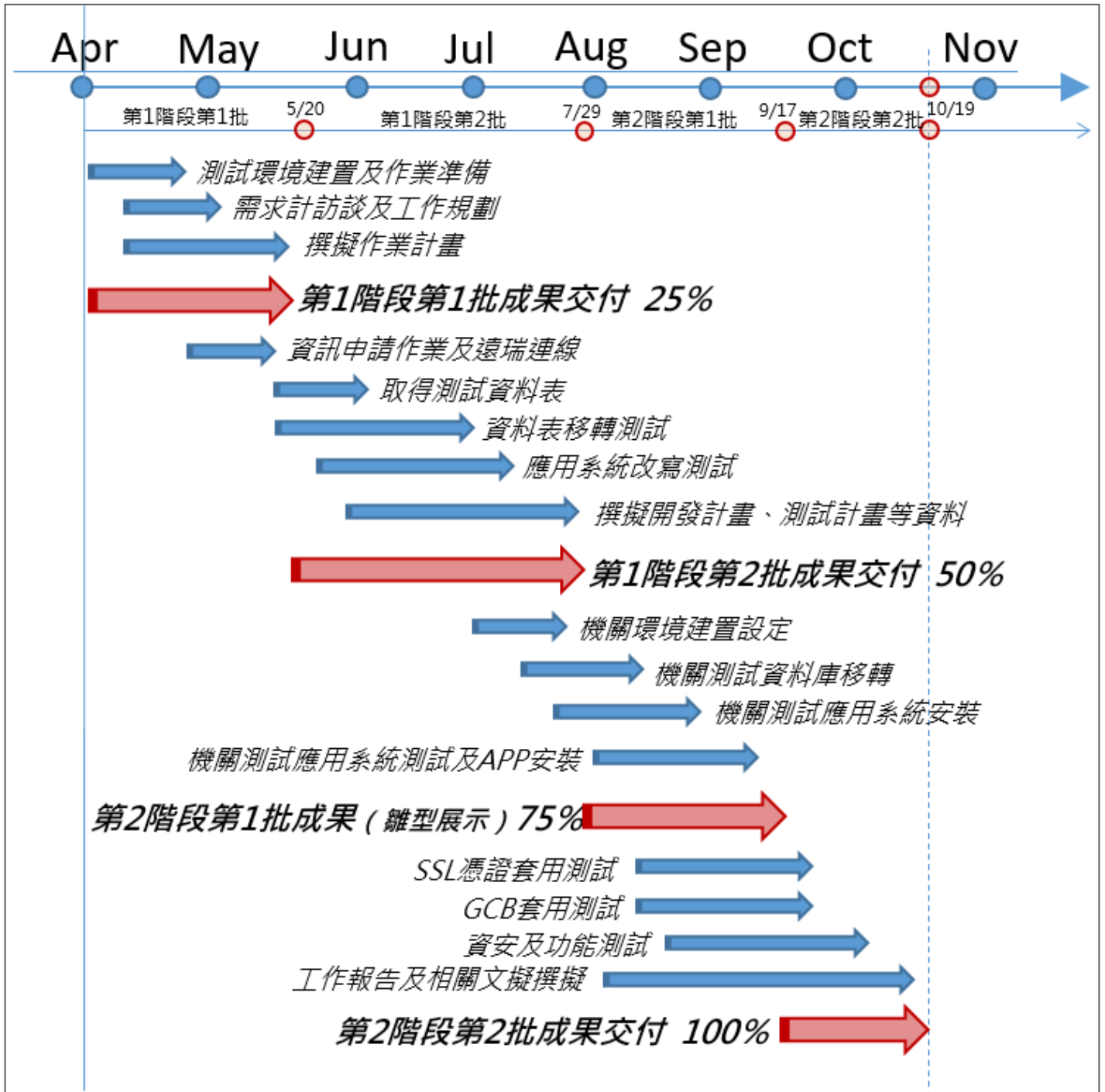


圖 20 各項工作執行情形

表 10 成果繳交情形一覽表

階段	批次	成果繳交項目	繳交數量	成果繳交期限	實際繳交日期	備註
第 1 階段	1	◎本案作業計畫 (含需求訪談紀錄)	書面資料 1 份 電子檔 1 份	於決標次日起 30 個日曆天 (5/20) 內繳交。	◎4/29 辦理需求訪談。 ◎5/20 函送成果。 ◎6/30 函送修正後成果。 ◎7/17 本批成果審查通過。	完成
	2	◎資訊系統開發計畫 ◎資訊系統需求規格 ◎資訊系統設計規格 ◎系統測試計畫	書面資料 1 份 電子檔 1 份	於決標次日起 100 個日曆天 (7/29) 內繳交。	◎7/28 函送本批成果。 ◎9/9 函送修正後成果。 ◎9/29 本批成果審查通過，第 1 階段成果驗收合格。	完成
第 2 階段	1	◎測繪成果圖冊管理系統展示	實地辦理系統展示 展示結果書面資料 1 份	於決標次日起 150 個日曆天 (9/17) 內辦竣系統擴充離型展示，並於辦竣次日起 10 日內函送證明文件 (簽到簿及其他紀錄)。	◎9/17 辦理系統離型展示。 ◎9/25 函送離型展示辦理相關文件。	完成
	2	◎本案完整原始程式碼檔案 (含編譯所需函式庫) ◎執行檔、系統自動安裝光碟	電子檔 2 份	於決標次日起 180 個日曆天 (10/17, 因例假日, 展延至 10/19) 內繳交。	◎10/19 繳交。	審核中
		◎系統測試報告 ◎資訊安全檢測報告 ◎程式規格 ◎資訊系統使用手冊	書面資料 6 份 電子檔 1 份			
		◎工作總報告初稿 (含資料庫移轉報告)	書面資料 6 份 電子檔 1 份			

-	◎修正後工作 總報告	書面資料 5 份 電子檔 1 份	於審查通過後，機關 通知期限內繳交。	
---	---------------	---------------------	-----------------------	--

肆、本案相關建議事項及未來執行建議

- 一、本案資料庫移轉作業，亦將文字編碼由原有之 BIG 5 轉換為 UTF 8，故原有歷史資料倘有字碼無法對應或缺漏字情形，請機關比對確認後自行修正即可。
- 二、硬體部份：機關目前使用手持式 RFID 讀取器規格較為陳舊，其硬體效能較低，螢幕較小且解析度不高，故造成作業人員辨視資訊不易；另其作業系統為 Windows CE，目前已原廠已停止更新支援，新功能開發受限；故建議機關未來工作案，可將手持式讀取器之軟體轉換為 Android 系統（如圖 21），以提升效能。
- 三、資料庫部份：本案資料庫由 Oracle 10g 資料庫移轉至 MS SQL Server 2019（以下稱 MS SQL），雖 MS SQL 已內建資料庫維護精靈等工具可進行資料庫完整性檢查、資料庫壓縮、重整、統計、清理及備份等工作，可由資料庫管理人員以該工具進行簡易的相關維護及排程自動執行，但如長期營運通常容易造成資料庫趨於索碎及複雜，除降低效能外亦有造成潛在錯誤。故建議機關可委請資料庫維護專業團隊，長期維持資料庫穩定性及安全性。

UHF RFID Tablet PDA (Industrial Tablet UHF Reader)

HLT- H860



Feature

- Support EPC Class1 Gen2 protocol
- Android 4.4 Operation system, quad core 1.2 GHz CPU; RAM 2G
- 7 inch LCD screen, 1280x800 IPS capacitive touch screen
- WIFI, Bluetooth, 4G, GPS wireless communication
- 1D/2D barcode optional
- IP67 rating, drop resistance from 1.2m

Parameter

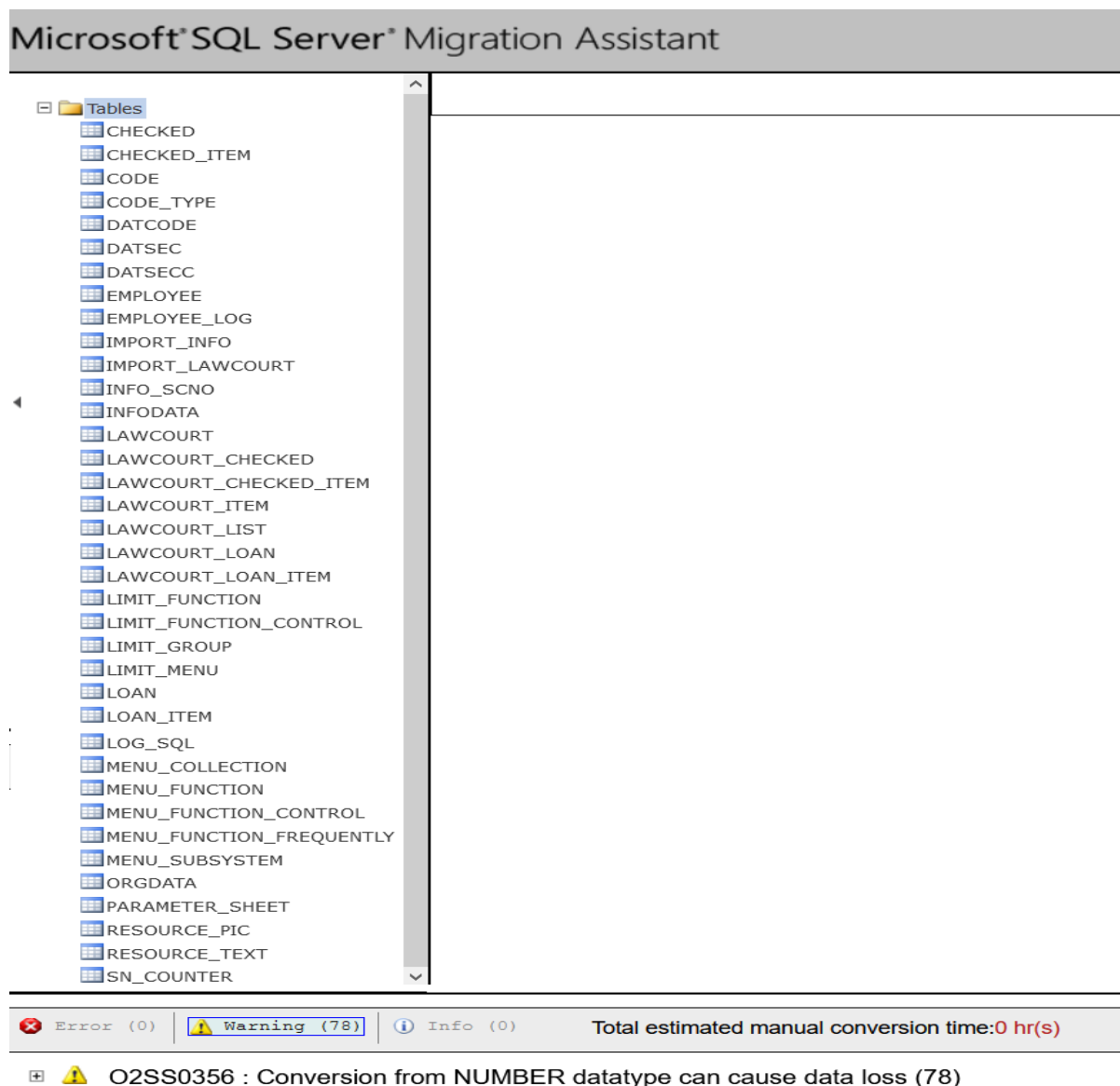
General parameter	
Operation System	Android 4.4
CPU	MSM8916, A53, 4 core CPU, 1.2GHz
Wireless communication	WIFI, Bluetooth , GPS Module, 4G
Communication Interfaces	5 pin Micro USB; support OTG (U-disk/Mouse/Keyboard/USB Ethernet cable)
Screen	7 inch LCD screen, 1280x800 IPS capacitive touch screen
Scanner	1D/2D barcode
Memory	RAM: 2G FLASH: 16G Extended: Micro SD, Maximum 32G

圖 21 平板式 RFID 讀取器

伍、 附錄

一、 資料庫移轉報告

移轉資料表架構



02SS00356:Conversion from number datatype can cause data loss (78)

說明：Oracle 資料類型與 Microsoft SQL Server 資料類型並非一律完全相符，在進行資料轉換時，Oracle 資料表時自動選取相符的資料類型或系統提供手動修改切換資料類型設定。如果單一資料類型對應不清楚，

系統將提供替代的資料類型對應。系統顯示 Warning 件數是提醒在進行數字轉換時需注意 number 資料型類長度()包含小數點位數是否有被截斷的風險，為避免此一情況發生，在轉換時會手動設定比原資料型態較大的轉換類型，防止資料被截斷的錯誤。

下表顯示了將資料從「Oracle 發行者」移至「SQL Server 散發者」時，資料類型在 Oracle 與 SQL Server 之間的預設對應方式。

Oracle 資料類型	SQL Server 資料類型
BFILE	VARBINARY(MAX)
BLOB	VARBINARY(MAX)
CHAR([1-2000])	CHAR([1-2000])
CLOB	VARCHAR(MAX)
日期	DATETIME
FLOAT	FLOAT
FLOAT([1-53])	FLOAT([1-53])
FLOAT([54-126])	FLOAT
INT	NUMERIC(38)
INTERVAL	DATETIME
LONG	VARCHAR(MAX)
LONG RAW	IMAGE
NCHAR([1-1000])	NCHAR([1-1000])
NCLOB	NVARCHAR(MAX)
NUMBER	FLOAT
NUMBER([1-38])	NUMERIC([1-38])
NUMBER([0-38],[1-38])	NUMERIC([0-38],[1-38])
NVARCHAR2([1-2000])	NVARCHAR([1-2000])
RAW([1-2000])	VARBINARY([1-2000])
real	FLOAT

Oracle 資料類型	SQL Server 資料類型
ROWID	CHAR(18)
timestamp	DATETIME
TIMESTAMP(0-7)	DATETIME
TIMESTAMP(8-9)	DATETIME
TIMESTAMP(0-7) WITH TIME ZONE	VARCHAR(37)
TIMESTAMP(8-9) WITH TIME ZONE	VARCHAR(37)
TIMESTAMP(0-7) WITH LOCAL TIME ZONE	VARCHAR(37)
TIMESTAMP(8-9) WITH LOCAL TIME ZONE	VARCHAR(37)
UROWID	CHAR(18)
VARCHAR2([1-4000])	VARCHAR([1-4000])

移轉資料內容

Status	From	To	Total Rows	Migrated Rows	Success Rate	Duration (DD:HH:MM:SS:MS)
	"FONRAN"."INFODATA"	[[sb_2020_20200814].[FONRAN]	491741	491741	100.00%	00:00:00:26:681
	"FONRAN"."INFO_SCNO"	[[sb_2020_20200814].[FONRAN]	463923	463923	100.00%	00:00:00:03:782
	"FONRAN"."IMPORT_LAWCOURT"	[[sb_2020_20200814].[FONRAN]	4	4	100.00%	00:00:00:34:272
	"FONRAN"."IMPORT_INFO"	[[sb_2020_20200814].[FONRAN]	43	43	100.00%	00:00:00:34:262
	"FONRAN"."EMPLOYEE_LOG"	[[sb_2020_20200814].[FONRAN]	73655	73655	100.00%	00:00:00:22:032
	"FONRAN"."EMPLOYEE"	[[sb_2020_20200814].[FONRAN]	23	23	100.00%	00:00:00:33:582
	"FONRAN"."DATSECC"	[[sb_2020_20200814].[FONRAN]	17930	17930	100.00%	00:00:00:31:778
	"FONRAN"."DATSEC"	[[sb_2020_20200814].[FONRAN]	26225	26225	100.00%	00:00:00:24:225
	"FONRAN"."DATCODE"	[[sb_2020_20200814].[FONRAN]	1290	1290	100.00%	00:00:00:33:798
	"FONRAN"."CODE_TYPE"	[[sb_2020_20200814].[FONRAN]	4	4	100.00%	00:00:00:34:198
	"FONRAN"."CODE"	[[sb_2020_20200814].[FONRAN]	6	6	100.00%	00:00:00:34:162
	"FONRAN"."CHECKED_ITEM"	[[sb_2020_20200814].[FONRAN]	370908	370908	100.00%	00:00:00:04:262
	"FONRAN"."CHECKED"	[[sb_2020_20200814].[FONRAN]	12061	12061	100.00%	00:00:00:27:062
	"FONRAN"."SN_COUNTER"	[[sb_2020_20200814].[FONRAN]	1596	1596	100.00%	00:00:00:33:805
	"FONRAN"."RESOURCE_TEXT"	[[sb_2020_20200814].[FONRAN]	2	2	100.00%	00:00:00:34:285
	"FONRAN"."RESOURCE_PIC"	[[sb_2020_20200814].[FONRAN]	0	0	100.00%	00:00:00:34:572
	"FONRAN"."PARAMETER_SHEET"	[[sb_2020_20200814].[FONRAN]	8	8	100.00%	00:00:00:34:452
	"FONRAN"."ORGDATA"	[[sb_2020_20200814].[FONRAN]	23404	23404	100.00%	00:00:00:22:975
	"FONRAN"."MENU_SUBSYSTEM"	[[sb_2020_20200814].[FONRAN]	5	5	100.00%	00:00:00:34:455
	"FONRAN"."MENU_FUNCTION_FREQU"	[[sb_2020_20200814].[FONRAN]	495	495	100.00%	00:00:00:34:355
	"FONRAN"."LAWCOURT_CHECKED"	[[sb_2020_20200814].[FONRAN]	1	1	100.00%	00:00:00:34:368
	"FONRAN"."LAWCOURT"	[[sb_2020_20200814].[FONRAN]	7135	7135	100.00%	00:00:00:29:008
	"FONRAN"."MENU_FUNCTION_CONTR"	[[sb_2020_20200814].[FONRAN]	0	0	100.00%	00:00:00:34:628
	"FONRAN"."MENU_FUNCTION"	[[sb_2020_20200814].[FONRAN]	52	52	100.00%	00:00:00:34:285
	"FONRAN"."MENU_COLLECTION"	[[sb_2020_20200814].[FONRAN]	33	33	100.00%	00:00:00:29:162
	"FONRAN"."LOG_SQL"	[[sb_2020_20200814].[FONRAN]	0	0	100.00%	00:00:00:29:192
	"FONRAN"."LOAN_ITEM"	[[sb_2020_20200814].[FONRAN]	3098	3098	100.00%	00:00:00:28:325
	"FONRAN"."LOAN"	[[sb_2020_20200814].[FONRAN]	1877	1877	100.00%	00:00:00:28:202
	"FONRAN"."LIMIT_MENU"	[[sb_2020_20200814].[FONRAN]	179	179	100.00%	00:00:00:28:332
	"FONRAN"."LIMIT_GROUP"	[[sb_2020_20200814].[FONRAN]	2	2	100.00%	00:00:00:28:248
	"FONRAN"."LIMIT_FUNCTION_CONTR"	[[sb_2020_20200814].[FONRAN]	0	0	100.00%	00:00:00:28:548
	"FONRAN"."LIMIT_FUNCTION"	[[sb_2020_20200814].[FONRAN]	204	204	100.00%	00:00:00:28:248
	"FONRAN"."LAWCOURT_LOAN_ITEM"	[[sb_2020_20200814].[FONRAN]	79	79	100.00%	00:00:00:28:128
	"FONRAN"."LAWCOURT_LOAN"	[[sb_2020_20200814].[FONRAN]	495	495	100.00%	00:00:00:28:115

Details

Save Report

Close

SSMA 結果報表

Status	Source table	Target table	Total rows	Migrated rows	Success rate	Duration (DD:HH:MM:SS:MS)	Error messages
Completed	"FONRAN"."IMPORT_ORGDATA"	[Isb2020_20201124].[FONRAN].[IMPORT_ORGDATA]	427	427	100.00%	00:00:01:14:608	
Completed	"FONRAN"."INFODATA"	[Isb2020_20201124].[FONRAN].[INFODATA]	491741	491741	100.00%	00:00:00:02:231	
Completed	"FONRAN"."INFO_SCNO"	[Isb2020_20201124].[FONRAN].[INFO_SCNO]	463923	463923	100.00%	00:00:00:00:34:515	
Completed	"FONRAN"."IMPORT_LAWCOURT"	[Isb2020_20201124].[FONRAN].[IMPORT_LAWCOURT]	4	4	100.00%	00:00:00:01:15:766	
Completed	"FONRAN"."IMPORT_INFO"	[Isb2020_20201124].[FONRAN].[IMPORT_INFO]	43	43	100.00%	00:00:01:15:771	
Completed	"FONRAN"."IMPORT_DATSECC"	[Isb2020_20201124].[FONRAN].[IMPORT_DATSECC]	78	78	100.00%	00:00:01:15:746	
Completed	"FONRAN"."IMPORT_DATSEC"	[Isb2020_20201124].[FONRAN].[IMPORT_DATSEC]	5	5	100.00%	00:00:01:14:728	
Completed	"FONRAN"."EMPLOYEE_LOG"	[Isb2020_20201124].[FONRAN].[EMPLOYEE_LOG]	73657	73657	100.00%	00:00:00:58:445	
Completed	"FONRAN"."EMPLOYEE"	[Isb2020_20201124].[FONRAN].[EMPLOYEE]	23	23	100.00%	00:00:01:14:457	
Completed	"FONRAN"."DATSECC"	[Isb2020_20201124].[FONRAN].[DATSECC]	17930	17930	100.00%	00:00:01:08:075	
Completed	"FONRAN"."DATSEC"	[Isb2020_20201124].[FONRAN].[DATSEC]	26225	26225	100.00%	00:00:01:04:325	
Completed	"FONRAN"."DATCODE"	[Isb2020_20201124].[FONRAN].[DATCODE]	1290	1290	100.00%	00:00:01:13:330	
Completed	"FONRAN"."CODE_TYPE"	[Isb2020_20201124].[FONRAN].[CODE_TYPE]	4	4	100.00%	00:00:01:13:351	
Completed	"FONRAN"."CODE"	[Isb2020_20201124].[FONRAN].[CODE]	6	6	100.00%	00:00:01:13:348	
Completed	"FONRAN"."CHECKED_ITEM"	[Isb2020_20201124].[FONRAN].[CHECKED_ITEM]	370908	370908	100.00%	00:00:00:34:638	
Completed	"FONRAN"."CHECKED"	[Isb2020_20201124].[FONRAN].[CHECKED]	12066	12066	100.00%	00:00:01:07:373	
Completed	"FONRAN"."SN_COUNTER"	[Isb2020_20201124].[FONRAN].[SN_COUNTER]	1596	1596	100.00%	00:00:01:14:735	
Completed	"FONRAN"."RESOURCE_TEXT"	[Isb2020_20201124].[FONRAN].[RESOURCE_TEXT]	2	2	100.00%	00:00:00:01:15:711	
Completed	"FONRAN"."PARAMETER_SHEET"	[Isb2020_20201124].[FONRAN].[PARAMETER_SHEET]	8	8	100.00%	00:00:01:15:398	
Completed	"FONRAN"."ORG_SCNO"	[Isb2020_20201124].[FONRAN].[ORG_SCNO]	24755	24755	100.00%	00:00:01:11:758	

Completed	"FONRAN"; "MENU_SUBSYSTEM"	[lsb2020_20201124],[FONRAN],[MENU_SUBSYSTEM]	5	5	100.00%	00:00:01:15:768	
Completed	"FONRAN"; "MENU_FUNCTION_FREQUENTLY"	[lsb2020_20201124],[FONRAN],[MENU_FUNCTION_FREQUENTLY]	495	495	100.00%	00:00:01:15:745	
Completed	"FONRAN"; "LAWCOURT_CHECKED"	[lsb2020_20201124],[FONRAN],[LAWCOURT_CHECKED]	1	1	100.00%	00:00:01:15:588	
Completed	"FONRAN"; "LAWCOURT"	[lsb2020_20201124],[FONRAN],[LAWCOURT]	7135	7135	100.00%	00:00:01:10:838	
Completed	"FONRAN"; "MENU_FUNCTION_CONTROL"	[lsb2020_20201124],[FONRAN],[MENU_FUNCTION_CONTROL]	0	0	100.00%	00:00:01:15:676	
Completed	"FONRAN"; "MENU_FUNCTION"	[lsb2020_20201124],[FONRAN],[MENU_FUNCTION]	52	52	100.00%	00:00:01:15:318	
Completed	"FONRAN"; "MENU_COLLECTION"	[lsb2020_20201124],[FONRAN],[MENU_COLLECTION]	33	33	100.00%	00:00:01:15:298	
Completed	"FONRAN"; "LOG_SQL"	[lsb2020_20201124],[FONRAN],[LOG_SQL]	0	0	100.00%	00:00:01:15:821	
Completed	"FONRAN"; "LOAN_ITEM"	[lsb2020_20201124],[FONRAN],[LOAN_ITEM]	3098	3098	100.00%	00:00:01:13:613	
Completed	"FONRAN"; "LOAN"	[lsb2020_20201124],[FONRAN],[LOAN]	1877	1877	100.00%	00:00:01:15:125	
Completed	"FONRAN"; "LIMIT_MENU"	[lsb2020_20201124],[FONRAN],[LIMIT_MENU]	179	179	100.00%	00:00:01:15:747	
Completed	"FONRAN"; "LIMIT_GROUP"	[lsb2020_20201124],[FONRAN],[LIMIT_GROUP]	2	2	100.00%	00:00:01:15:625	
Completed	"FONRAN"; "LIMIT_FUNCTION_CONTROL"	[lsb2020_20201124],[FONRAN],[LIMIT_FUNCTION_CONTROL]	0	0	100.00%	00:00:01:15:993	
Completed	"FONRAN"; "LIMIT_FUNCTION"	[lsb2020_20201124],[FONRAN],[LIMIT_FUNCTION]	204	204	100.00%	00:00:01:15:435	
Completed	"FONRAN"; "LAWCOURT_LOAN_ITEM"	[lsb2020_20201124],[FONRAN],[LAWCOURT_LOAN_ITEM]	79	79	100.00%	00:00:01:15:817	
Completed	"FONRAN"; "LAWCOURT_LOAN"	[lsb2020_20201124],[FONRAN],[LAWCOURT_LOAN]	495	495	100.00%	00:00:01:14:106	
Completed	"FONRAN"; "LAWCOURT_LIST"	[lsb2020_20201124],[FONRAN],[LAWCOURT_LIST]	21	21	100.00%	00:00:01:15:741	
Completed	"FONRAN"; "LAWCOURT_ITEM"	[lsb2020_20201124],[FONRAN],[LAWCOURT_ITEM]	3834	3834	100.00%	00:00:01:12:331	
Completed	"FONRAN"; "LAWCOURT_CHECKED_ITEM"	[lsb2020_20201124],[FONRAN],[LAWCOURT_CHECKED_ITEM]	0	0	100.00%	00:00:01:15:928	

二、 套用 GCB 項目及測試結果

(一) IIS 政府組態基準列表

項次	TWGCB-ID	類別	原則設定名稱	設定位置	GCB設定值	是否套用	測試結果	備註
1	TWGCB-04-002-0001	基本設定	網站內容存放位置	站台	存放在非系統磁區	✓	✓	
2	TWGCB-04-002-0002	基本設定	主機名稱	站台	每個站台都必須設定主機名稱	✓	✓	
3	TWGCB-04-002-0003	基本設定	瀏覽目錄	伺服器	停用	✓	✓	
4	TWGCB-04-002-0004	基本設定	應用程式集區識別	應用程式集區	ApplicationPoolIdentity	✓	✓	
5	TWGCB-04-002-0005	基本設定	應用程式集區	應用程式集區	每個站台皆設定唯一的應用程式集區	✓	✓	
6	TWGCB-04-002-0006	基本設定	匿名使用者識別	伺服器	應用程式集區識別	✓	✓	
7	TWGCB-04-002-0007	設定驗證與授權	表單驗證需要SSL	伺服器	需要SSL	✓	✓	
8	TWGCB-04-002-0008	設定驗證與授權	表單驗證Cookie模式	伺服器	使用Cookie	✓	✓	
9	TWGCB-04-002-0009	設定驗證與授權	表單驗證Cookie保護模式	伺服器	加密及驗證	✓	✓	
10	TWGCB-04-002-0010	設定驗證與授權	基本驗證需要SSL	站台	需要SSL	✓	✓	
11	TWGCB-04-002-0011	設定驗證與授權	credentials元素	站台	移除<credentials>元素段落	✓	✓	
12	TWGCB-04-002-0012	ASP.NET設定建議	以retail模式部署Web應用程式	系統檔案	TRUE	✓	✓	
13	TWGCB-04-002-0013	ASP.NET設定建議	偵錯功能	伺服器	FALSE	✓	✓	
14	TWGCB-04-002-0014	ASP.NET設定建議	自訂錯誤訊息顯示模式	伺服器	開啟或僅限遠端	✓	✓	
15	TWGCB-04-002-0015	ASP.NET設定建議	HTTP詳細錯誤訊息顯示模式	站台	本機要求的詳細錯誤及遠端要求的自訂錯誤網頁或自訂錯誤網頁	✓	✓	
16	TWGCB-04-002-0016	ASP.NET設定建議	ASP.NET堆疊追蹤	伺服器	自設定檔與ASP.NET網頁中，移除所有Trace="true"或trace enabled="true"內容	✓	✓	
17	TWGCB-04-002-0017	ASP.NET設定建議	工作階段狀態Cookie模式	伺服器	使用Cookie	✓	✓	
18	TWGCB-04-002-0018	ASP.NET設定建議	httpOnlyCookies	站台	TRUE	✓	✓	
19	TWGCB-04-002-0019	ASP.NET設定建議	電腦金鑰驗證方法(ASP.Net 3.5)	伺服器	SHA1或AES	✓	✓	
20	TWGCB-04-002-0020	ASP.NET設定建議	電腦金鑰(ASP.Net 4.5)	伺服器	HMACSHA256、HMACSHA384或HMACSHA512	✓	✓	
21	TWGCB-04-002-0021	ASP.NET設定建議	.NET信任層級	伺服器	Medium (web_mediumtrust.config)、Low (web_lowtrust.config)或Minimal	✓	✓	
22	TWGCB-04-002-0022	ASP.NET設定建議	加密提供者	CMD	自iisWasKey中移除IIS IUSRS的存取權限	✓	✓	
23	TWGCB-04-002-0023	要求篩選與其他限制模組	允許的內容長度上限	伺服器	30000000	✓	✓	
24	TWGCB-04-002-0024	要求篩選與其他限制模組	URL長度上限	伺服器	4096	✓	✓	
25	TWGCB-04-002-0025	要求篩選與其他限制模組	查詢字串上限	伺服器	2048	✓	✓	
26	TWGCB-04-002-0026	要求篩選與其他限制模組	允許高位元字元	伺服器	不允許	✓	✓	
27	TWGCB-04-002-0027	要求篩選與其他限制模組	允許雙重逸出	伺服器	不允許	✓	✓	
28	TWGCB-04-002-0028	要求篩選與其他限制模組	HTTP TRACE方法	伺服器	拒絕	✓	✓	

項次	TWGCB-ID	類別	原則設定名稱	設定位置	GCB設定值	是否套用	測試結果	備註
29	TWGCB-04-002-0029	要求篩選與其他限制模組	允許未列出的副檔名	伺服器	不允許	✓	✓	
30	TWGCB-04-002-0030	要求篩選與其他限制模組	處理常式權限	伺服器	不能同時擁有執行/指令碼與寫入權限	✓	✓	
31	TWGCB-04-002-0031	要求篩選與其他限制模組	允許未指定的ISAPI模組	伺服器	不允許	✓	✓	
32	TWGCB-04-002-0032	要求篩選與其他限制模組	允許未指定的CGI模組	伺服器	不允許	✓	✓	
33	TWGCB-04-002-0033	要求篩選與其他限制模組	動態IP限制	伺服器	啟用動態IP限制功能，並依需求設定「根據同時要求的數目拒絕IP位址」與「根據超過一段時間之要求數目拒絕IP位址」參數	✓	✓	
34	TWGCB-04-002-0034	IIS記錄	IIS記錄檔位置	伺服器	記錄檔存放至受管制的非系統磁碟區	✓	✓	
35	TWGCB-04-002-0035	IIS記錄	Advanced Logging	伺服器	啟用	✓	✓	
36	TWGCB-04-002-0036	IIS記錄	記錄檔格式	伺服器	W3C	✓	✓	
37	TWGCB-04-002-0037	IIS記錄	記錄事件目的地	伺服器	記錄檔和ETW事件二者	✓	✓	
38	TWGCB-04-002-0038	FTP要求	FTP SSL設定	伺服器	需要SSL連線	✓	✓	
39	TWGCB-04-002-0039	FTP要求	FTP登入嘗試限制	伺服器	啟用	✓	✓	
40	TWGCB-04-002-0040	傳輸加密	HTTP回應標頭	伺服器	名稱：Strict-Transport-Security	✓	✓	
41	TWGCB-04-002-0041	傳輸加密	SSLv2	regedit	停用	✓	✓	
42	TWGCB-04-002-0042	傳輸加密	SSLv3	regedit	停用	✓	✓	
43	TWGCB-04-002-0043	傳輸加密	TLS 1.0	regedit	停用	✓	✓	
44	TWGCB-04-002-0044	傳輸加密	TLS 1.1	regedit	啟用	✓	✓	
45	TWGCB-04-002-0045	傳輸加密	TLS 1.2	regedit	啟用	✓	✓	
46	TWGCB-04-002-0046	傳輸加密	NULL Cipher	regedit	停用	✓	✓	
47	TWGCB-04-002-0047	傳輸加密	DES	regedit	停用	✓	✓	
48	TWGCB-04-002-0048	傳輸加密	RC2	regedit	停用	✓	✓	
49	TWGCB-04-002-0049	傳輸加密	RC4加密套件	regedit	停用	✓	✓	
50	TWGCB-04-002-0050	傳輸加密	Triple DES加密套件	regedit	啟用	✓	✓	
51	TWGCB-04-002-0051	傳輸加密	AES 128/128加密套件	regedit	啟用	✓	✓	
52	TWGCB-04-002-0052	傳輸加密	AES 256/256加密套件	regedit	啟用	✓	✓	
					TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 P384	✓	✓	
					TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 P256	✓	✓	
					TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 P	✓	✓	
					TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 P	✓	✓	
					TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA P256	✓	✓	

項次	TWGCB-ID	類別	原則設定名稱	設定位置	GCB設定值	是否套用	測試結果	備註
53	TWGCB-04-002-0053	傳輸加密	TLS加密套件順序	regedit	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256	✓	✓	
					TLS_RSA_WITH_AES_256_GCM_SHA384	✓	✓	
					TLS_RSA_WITH_AES_128_GCM_SHA256	✓	✓	
					TLS_RSA_WITH_AES_256_CBC_SHA256	✓	✓	
					TLS_RSA_WITH_AES_128_CBC_SHA256	✓	✓	
					TLS_RSA_WITH_AES_256_CBC_SHA	✓	✓	
					TLS_RSA_WITH_AES_128_CBC_SHA	✓	✓	
					TLS_RSA_WITH_3DES_EDE_CBC_SHA	✓	✓	

(二) Google Chrome 政府組態基準列表

項次	GPO	TWGCB-ID	版本	類別	原則設定名稱	是否套用	測試結果	備註
1	Google Chrome Computer Settings	TWGCB-02-003-0001	Google Chrome	Google Chrome	一律執行需要授權的外掛程式(已淘汰)	×	-	適用Chrome65以前版本
2	Google Chrome Computer Settings	TWGCB-02-003-0002	Google Chrome	Google Chrome	不論線上OCSP/CRL檢查是否執行	√	√	
3	Google Chrome Computer Settings	TWGCB-02-003-0003	Google Chrome	Google Chrome	允許執行過舊的外掛程式	√	√	
4	Google Chrome Computer Settings	TWGCB-02-003-0004	Google Chrome	Google Chrome	允許調用檔案選項對話方塊	√	√	
5	Google Chrome Computer Settings	TWGCB-02-003-0005	Google Chrome	Google Chrome	在Google Chrome關閉時持續執行背景應用程式	√	√	
6	Google Chrome Computer Settings	TWGCB-02-003-0006	Google Chrome	Google Chrome	封鎖第三方Cookie	√	√	
7	Google Chrome Computer Settings	TWGCB-02-003-0007	Google Chrome	Google Chrome	指定是否該停用外掛程式尋找工具(已淘汰)	×	-	適用Chrome65以前版本
8	Google Chrome Computer Settings	TWGCB-02-003-0008	Google Chrome	Google Chrome	停用Google資料同步處理	√	√	
9	Google Chrome Computer Settings	TWGCB-02-003-0009	Google Chrome	Google Chrome	停用略過安全瀏覽警告網頁繼續進行	√	√	
10	Google Chrome Computer Settings	TWGCB-02-003-0010	Google Chrome	Google Chrome	停用儲存瀏覽紀錄功能	√	√	
11	Google Chrome Computer Settings	TWGCB-02-003-0011	Google Chrome	Google Chrome	啟用「Google Cloud print」文件提交功能	√	√	
12	Google Chrome Computer Settings	TWGCB-02-003-0012	Google Chrome	Google Chrome	啟用Google Cloud Print Proxy	√	√	
13	Google Chrome Computer Settings	TWGCB-02-003-0013	Google Chrome	Google Chrome	啟用安全瀏覽	√	√	
14	Google Chrome Computer Settings	TWGCB-02-003-0014	Google Chrome	Google Chrome	啟用自動填入	×	-	適用Chrome70以前版本
15	Google Chrome Computer Settings	TWGCB-02-003-0015	Google Chrome	Google Chrome	啟用使用量和當機相關資料的報告功能	√	√	
16	Google Chrome Computer Settings	TWGCB-02-003-0016	Google Chrome	Google Chrome	啟用替代的錯誤網頁	√	√	
17	Google Chrome Computer Settings	TWGCB-02-003-0017	Google Chrome	Google Chrome	第一執行時從預設瀏覽器匯入已儲存的密碼	√	√	
18	Google Chrome Computer Settings	TWGCB-02-003-0018	Google Chrome	Google Chrome	無痕模式適用性	√	√	
19	Google Chrome Computer Settings	TWGCB-02-003-0019	Google Chrome	HTTP驗證政策	支援的驗證機制	√	√	
20	Google Chrome Computer Settings	TWGCB-02-003-0020	Google Chrome	內容設定	預設Cookie設定	√	√	
21	Google Chrome Computer Settings	TWGCB-02-003-0021	Google Chrome	內容設定	Flash預設設定	√	√	
22	Google Chrome Computer Settings	TWGCB-02-003-0022	Google Chrome	內容設定	預設地理位置設定	√	√	
23	Google Chrome Computer Settings	TWGCB-02-003-0023	Google Chrome	內容設定	預設通知設定	√	√	
24	Google Chrome Computer Settings	TWGCB-02-003-0024	Google Chrome	內容設定	預設彈出式視窗設定	√	√	
25	Google Chrome Computer Settings	TWGCB-02-003-0025	Google Chrome	密碼管理員	允許將密碼儲存到密碼管理員	√	√	
26	Google Chrome Computer Settings	TWGCB-02-003-0026	Google Chrome	設定遠端存取	允許遠端存取主機穿越防火牆	√	√	
27	Google Chrome Computer Settings	TWGCB-02-003-0027	Google Chrome	設定遠端存取	針對遠端存取主機啟用或停用無PIN碼驗證機制	√	√	
28	Google Chrome Computer Settings	TWGCB-02-003-0028	Google Chrome	設定遠端存取	啟用遠端存取主機遮幕	√	√	
29	Google Chrome Computer Settings	TWGCB-02-003-0029	Google Chrome	設定遠端存取	設定遠端存取主機所需的網域名稱	×	-	適用Chrome59(含)以前版本
30	Google Chrome Computer Settings	TWGCB-02-003-0030	Google Chrome	擴充功能	設定擴充功能安裝黑名單	√	√	

項次	GPO	TWGCB-ID	版本	類別	原則設定名稱	是否套用	測試結果	備註
31	Google Chrome Computer Settings	TWGCB-02-003-0031	Google Chrome	設定遠端存取	Configure the required domain names for remote access hosts	√	√	適用 Chrome60(含)以後版本
32	Google Chrome Computer Settings	TWGCB-02-003-0032	Google Chrome	Google Chrome	啟用地址的自動填入功能	√	√	適用 Chrome70(含)以後版本
33	Google Chrome Computer Settings	TWGCB-02-003-0033	Google Chrome	Google Chrome	啟用信用卡的自動填入功能	√	√	適用 Chrome70(含)以後版本

(三) Internet Explorer 11 政府組態基準列表

項次	GPO	TWGCB-ID	類別	原則設定名稱	是否套用	測試結果	備註
1	Internet Explorer 11 Computer Settings	TWGCB-02-002-0001	Internet Explorer	包含來自Microsoft的更新網站清單	√	√	
2	Internet Explorer 11 Computer Settings	TWGCB-02-002-0002	Internet Explorer	停用變更自動設定之設定	√	√	
3	Internet Explorer 11 Computer Settings	TWGCB-02-002-0003	Internet Explorer	防止執行「首次執行」精靈	√	√	
4	Internet Explorer 11 Computer Settings	TWGCB-02-002-0004	Internet Explorer	不允許使用者啟用或停用附加元件	√	√	
5	Internet Explorer 11 Computer Settings	TWGCB-02-002-0005	Internet Explorer	關閉當機偵測	√	√	
6	Internet Explorer 11 Computer Settings	TWGCB-02-002-0006	Internet Explorer	關閉安全性設定檢查功能	√	√	
7	Internet Explorer 11 Computer Settings	TWGCB-02-002-0007	Internet Explorer	防止參與客戶經驗改進計畫	√	√	
8	Internet Explorer 11 Computer Settings	TWGCB-02-002-0008	Internet Explorer	為每台電腦建立Proxy設定-而不是每個使用者	√	√	
9	Internet Explorer 11 Computer Settings	TWGCB-02-002-0009	Internet Explorer	安全性區域：不允許使用者新增/移除網站	√	√	
10	Internet Explorer 11 Computer Settings	TWGCB-02-002-0010	Internet Explorer	安全性區域：不允許使用者變更原則	√	√	
11	Internet Explorer 11 Computer Settings	TWGCB-02-002-0011	Internet Explorer	安全性區域：只使用電腦設定	√	√	
12	Internet Explorer 11 Computer Settings	TWGCB-02-002-0012	Internet Explorer	關閉ActiveX選擇加入提示	√	√	
13	Internet Explorer 11 Computer Settings	TWGCB-02-002-0013	Internet Explorer	防止每一使用者安裝ActiveX控制項	√	√	
14	Internet Explorer 11 Computer Settings	TWGCB-02-002-0014	Internet Explorer	防止略過SmartScreen篩選工具警告	√	√	
15	Internet Explorer 11 Computer Settings	TWGCB-02-002-0015	Internet Explorer	防止略過不是經常從網際網路下載檔案的相關SmartScreen篩選工具警告	√	√	
16	Internet Explorer 11 Computer Settings	TWGCB-02-002-0016	Internet Explorer	防止「修復設定」功能	√	√	
17	Internet Explorer 11 Computer Settings	TWGCB-02-002-0017	Internet Explorer	自動安裝新版Internet Explorer	√	√	
18	Internet Explorer 11 Computer Settings	TWGCB-02-002-0018	Internet Explorer	關閉瀏覽器地理位置	√	√	
19	Internet Explorer 11 Computer Settings	TWGCB-02-002-0019	Internet Explorer	指定在安裝ActiveX控制項時使用ActiveX安裝程式服務	√	√	
20	Internet Explorer 11 Computer Settings	TWGCB-02-002-0020	Internet Explorer	防止變更Proxy設定	√	√	
21	Internet Explorer 11 Computer Settings	TWGCB-02-002-0021	Internet Explorer	開啟ActiveX篩選	√	√	
22	Internet Explorer 11 Computer Settings	TWGCB-02-002-0022	安全性功能	Internet Explorer程序(Mime探查安全功能)	√	√	
23	Internet Explorer 11 Computer Settings	TWGCB-02-002-0023	安全性功能	Internet Explorer程序(MK通訊協定安全性限制)	√	√	
24	Internet Explorer 11 Computer Settings	TWGCB-02-002-0024	安全性功能	Internet Explorer程序(一致的MIME處理)	√	√	

項次	GPO	TWGCB-ID	類別	原則設定名稱	是否套用	測試結果	備註
25	Internet Explorer 11 Computer Settings	TWGCB-02-002-0025	安全性功能	Internet Explorer程序(已撰寫指令碼的Windows安全性限制)	√	√	
26	Internet Explorer 11 Computer Settings	TWGCB-02-002-0026	安全性功能	Internet Explorer程序(來自區域高度的保護)	√	√	
27	Internet Explorer 11 Computer Settings	TWGCB-02-002-0027	安全性功能	Internet Explorer程序(限制ActiveX安裝)	√	√	
28	Internet Explorer 11 Computer Settings	TWGCB-02-002-0028	安全性功能	Internet Explorer程序(限制檔案下載)	√	√	
29	Internet Explorer 11 Computer Settings	TWGCB-02-002-0029	安全性功能	Internet Explorer程序(通知列)	√	√	
30	Internet Explorer 11 Computer Settings	TWGCB-02-002-0030	刪除瀏覽歷程記錄	防止刪除使用者曾經造訪的網站	√	√	
31	Internet Explorer 11 Computer Settings	TWGCB-02-002-0031	刪除瀏覽歷程記錄	允許結束時刪除瀏覽歷程記錄	√	√	
32	Internet Explorer 11 Computer Settings	TWGCB-02-002-0032	刪除瀏覽歷程記錄	防止存取「刪除瀏覽歷程記錄」	√	√	
33	Internet Explorer 11 Computer Settings	TWGCB-02-002-0033	刪除瀏覽歷程記錄	停用「設定紀錄」	√	√	
34	Internet Explorer 11 Computer Settings	TWGCB-02-002-0034	網際網路控制台	防止略過憑證錯誤	√	√	
35	Internet Explorer 11 Computer Settings	TWGCB-02-002-0035	網際網路控制台\安全性畫	開啟憑證位址不符警告	√	√	
36	Internet Explorer 11 Computer Settings	TWGCB-02-002-0036	網際網路控制台\安全性畫	內部網路網站：包含所有網路路徑(UNC)	√	√	
37	Internet Explorer 11 Computer Settings	TWGCB-02-002-0037	網際網路控制台\安全性畫面\內部網路	不要對ActiveX控制項執行反惡意程式碼程式(內部網路區域)	√	√	
38	Internet Explorer 11 Computer Settings	TWGCB-02-002-0038	網際網路控制台\安全性畫面\內部網路	Java權限(內部網路區域)	√	√	
39	Internet Explorer 11 Computer Settings	TWGCB-02-002-0039	網際網路控制台\安全性畫面\內部網路	起始不標示為安全的ActiveX控制項(內部網路區域)	√	√	
40	Internet Explorer 11 Computer Settings	TWGCB-02-002-0040	網際網路控制台\安全性畫面\本機電腦	不要對ActiveX控制項執行反惡意程式碼程式(本機電腦區域)	√	√	
41	Internet Explorer 11 Computer Settings	TWGCB-02-002-0041	網際網路控制台\安全性畫面\本機電腦	Java權限(本機電腦區域)	√	√	
42	Internet Explorer 11 Computer Settings	TWGCB-02-002-0042	網際網路控制台\安全性畫面\本機電腦	開啟SmartScreen篩選工具掃描(本機電腦區域)	√	√	
43	Internet Explorer 11 Computer Settings	TWGCB-02-002-0043	網際網路控制台\安全性畫面\受限制的網站區域	存取跨網域的資料來源(受限制的網站區域)	√	√	
44	Internet Explorer 11 Computer Settings	TWGCB-02-002-0044	網際網路控制台\安全性畫面\受限制的網站區域	允許使用中的指令碼處理	√	√	

項次	GPO	TWGCB-ID	類別	原則設定名稱	是否套用	測試結果	備註
45	Internet Explorer 11 Computer Settings	TWGCB-02-002-0045	網際網路控制台\安全性畫面\受限制的網站區域	允許META REFRESH	√	√	
46	Internet Explorer 11 Computer Settings	TWGCB-02-002-0046	網際網路控制台\安全性畫面\受限制的網站區域	允許透過指令碼執行剪貼簿的剪下、複製或貼上作業(受限制的網站區域)	√	√	
47	Internet Explorer 11 Computer Settings	TWGCB-02-002-0047	網際網路控制台\安全性畫面\受限制的網站區域	不要對ActiveX控制項執行反惡意程式碼程式(受限制的網站區域)	√	√	
48	Internet Explorer 11 Computer Settings	TWGCB-02-002-0048	網際網路控制台\安全性畫面\受限制的網站區域	允許二進位和指令碼行為	√	√	
49	Internet Explorer 11 Computer Settings	TWGCB-02-002-0049	網際網路控制台\安全性畫面\受限制的網站區域	使用快顯封鎖程式(受限制的網站區域)	√	√	
50	Internet Explorer 11 Computer Settings	TWGCB-02-002-0050	網際網路控制台\安全性畫面\受限制的網站區域	下載已簽署的ActiveX控制項(受限制的網站區域)	√	√	
51	Internet Explorer 11 Computer Settings	TWGCB-02-002-0051	網際網路控制台\安全性畫面\受限制的網站區域	下載未簽署的ActiveX控制項(受限制的網站區域)	√	√	
52	Internet Explorer 11 Computer Settings	TWGCB-02-002-0052	網際網路控制台\安全性畫面\受限制的網站區域	啟用跨視窗拖曳不同網域的內容(受限制的網站區域)	√	√	
53	Internet Explorer 11 Computer Settings	TWGCB-02-002-0053	網際網路控制台\安全性畫面\受限制的網站區域	啟用在視窗內拖曳不同網域的內容(受限制的網站區域)	√	√	
54	Internet Explorer 11 Computer Settings	TWGCB-02-002-0054	網際網路控制台\安全性畫面\受限制的網站區域	允許拖放或複製及貼上檔案(受限制的網站區域)	√	√	
55	Internet Explorer 11 Computer Settings	TWGCB-02-002-0055	網際網路控制台\安全性畫面\受限制的網站區域	允許檔案下載	√	√	
56	Internet Explorer 11 Computer Settings	TWGCB-02-002-0056	網際網路控制台\安全性畫面\受限制的網站區域	允許字型下載(受限制的網站區域)	√	√	

項次	GPO	TWGCB-ID	類別	原則設定名稱	是否套用	測試結果	備註
57	Internet Explorer 11 Computer Settings	TWGCB-02-002-0057	網際網路控制台\安全性畫面\受限制的網站區域	允許安裝桌面項目(受限制的網站區域)	√	√	
58	Internet Explorer 11 Computer Settings	TWGCB-02-002-0058	網際網路控制台\安全性畫面\受限制的網站區域	Java 權限(受限制的網站區域)	√	√	
59	Internet Explorer 11 Computer Settings	TWGCB-02-002-0059	網際網路控制台\安全性畫面\受限制的網站區域	啟動在IFRAME中的應用程式及檔案(受限制的網站區域)	√	√	
60	Internet Explorer 11 Computer Settings	TWGCB-02-002-0060	網際網路控制台\安全性畫面\受限制的網站區域	登入選項(受限制的網站區域)	√	√	
61	Internet Explorer 11 Computer Settings	TWGCB-02-002-0061	網際網路控制台\安全性畫面\受限制的網站區域	啟用MIME探查(受限制的網站區域)	√	√	
62	Internet Explorer 11 Computer Settings	TWGCB-02-002-0062	網際網路控制台\安全性畫面\受限制的網站區域	查閱不同網域內的視窗和框架(受限制的網站區域)	√	√	
63	Internet Explorer 11 Computer Settings	TWGCB-02-002-0063	網際網路控制台\安全性畫面\受限制的網站區域	自動提示檔案下載(受限制的網站區域)	√	√	
64	Internet Explorer 11 Computer Settings	TWGCB-02-002-0064	網際網路控制台\安全性畫面\受限制的網站區域	僅允許批准的網域使用ActiveX控制項而不提示(受限制的網站區域)	√	√	
65	Internet Explorer 11 Computer Settings	TWGCB-02-002-0065	網際網路控制台\安全性畫面\受限制的網站區域	執行ActiveX控制項及外掛程式	√	√	
66	Internet Explorer 11 Computer Settings	TWGCB-02-002-0066	網際網路控制台\安全性畫面\受限制的網站區域	標示為安全的ActiveX控制項(受限制的網站區域)	√	√	
67	Internet Explorer 11 Computer Settings	TWGCB-02-002-0067	網際網路控制台\安全性畫面\受限制的網站區域	起始不標示為安全的ActiveX控制項(受限制的網站區域)	√	√	
68	Internet Explorer 11 Computer Settings	TWGCB-02-002-0068	網際網路控制台\安全性畫面\受限制的網站區域	以指令碼執行Java Applet(受限制的網站區域)	√	√	

項次	GPO	TWGCB-ID	類別	原則設定名稱	是否套用	測試結果	備註
69	Internet Explorer 11 Computer Settings	TWGCB-02-002-0069	網際網路控制台\安全性畫面\受限制的網站區域	執行使用Authenticode簽署的.NET Framework相依元件(受限制的網站區域)	√	√	
70	Internet Explorer 11 Computer Settings	TWGCB-02-002-0070	網際網路控制台\安全性畫面\受限制的網站區域	軟體頻道權限(受限制的網站區域)	√	√	
71	Internet Explorer 11 Computer Settings	TWGCB-02-002-0071	網際網路控制台\安全性畫面\受限制的網站區域	開啟跨網站指令碼篩選(受限制的網站區域)	√	√	
72	Internet Explorer 11 Computer Settings	TWGCB-02-002-0072	網際網路控制台\安全性畫面\受限制的網站區域	執行沒有使用Authenticode簽署的.NET Framework相依元件(受限制的網站區域)	√	√	
73	Internet Explorer 11 Computer Settings	TWGCB-02-002-0073	網際網路控制台\安全性畫面\受限制的網站區域	保留使用者資料(受限制的網站區域)	√	√	
74	Internet Explorer 11 Computer Settings	TWGCB-02-002-0074	網際網路控制台\安全性畫面\受限制的網站區域	允許由指令碼起始沒有大小或位置限制的視窗(受限制的網站區域)	√	√	
75	Internet Explorer 11 Computer Settings	TWGCB-02-002-0075	網際網路控制台\安全性畫面\受限制的網站區域	在較少特殊權限的網頁內容區域中的網站可以瀏覽到這個區域(受限制的網站區域)	√	√	
76	Internet Explorer 11 Computer Settings	TWGCB-02-002-0076	網際網路控制台\安全性畫面\受限制的網站區域	允許程式碼片段(受限制的網站區域)	√	√	
77	Internet Explorer 11 Computer Settings	TWGCB-02-002-0077	網際網路控制台\安全性畫面\受限制的網站區域	關閉第一次執行提示(受限制的網站區域)	√	√	
78	Internet Explorer 11 Computer Settings	TWGCB-02-002-0078	網際網路控制台\安全性畫面\受限制的網站區域	使用者將檔案上傳到伺服器時包含本機路徑(受限制的網站區域)	√	√	
79	Internet Explorer 11 Computer Settings	TWGCB-02-002-0079	網際網路控制台\安全性畫面\受限制的網站區域	開啟SmartScreen篩選工具掃描(受限制的網站區域)	√	√	
80	Internet Explorer 11 Computer Settings	TWGCB-02-002-0080	網際網路控制台\安全性畫面\受限制的網站區域	允許透過指令碼更新狀態列(受限制的網站區域)	√	√	

項次	GPO	TWGCB-ID	類別	原則設定名稱	是否套用	測試結果	備註
81	Internet Explorer 11 Computer Settings	TWGCB-02-002-0081	網際網路控制台\安全性畫面\受限制的網站區域	開啟受保護模式(受限制的網站區域)	√	√	
82	Internet Explorer 11 Computer Settings	TWGCB-02-002-0082	網際網路控制台\安全性畫面\受限制的網站區域	顯示可能不安全檔案的安全性警告(受限制的網站區域)	√	√	
83	Internet Explorer 11 Computer Settings	TWGCB-02-002-0083	網際網路控制台\安全性畫面\受限制的網站區域	允許Internet Explorer WebBrowser控制項的指令碼(受限制的網站區域)	√	√	
84	Internet Explorer 11 Computer Settings	TWGCB-02-002-0084	網際網路控制台\安全性畫面\受限制的網站區域	允許載入XAML檔案(受限制的網站區域)	√	√	
85	Internet Explorer 11 Computer Settings	TWGCB-02-002-0085	網際網路控制台\安全性畫面\信任的網站區域	不要對ActiveX控制項執行反惡意程式碼程式(信任的網站區域)	√	√	
86	Internet Explorer 11 Computer Settings	TWGCB-02-002-0086	網際網路控制台\安全性畫面\信任的網站區域	Java權限(信任的網站區域)	√	√	
87	Internet Explorer 11 Computer Settings	TWGCB-02-002-0087	網際網路控制台\安全性畫面\信任的網站區域	起始不標示為安全的ActiveX控制項(信任的網站區域)	√	√	
88	Internet Explorer 11 Computer Settings	TWGCB-02-002-0088	網際網路控制台\安全性畫面\網際網路	存取跨網域的資料來源(網際網路區域)	√	√	
89	Internet Explorer 11 Computer Settings	TWGCB-02-002-0089	網際網路控制台\安全性畫面\網際網路	允許透過指令碼執行剪貼簿的剪下、複製或貼上作業(網際網路區域)	√	√	
90	Internet Explorer 11 Computer Settings	TWGCB-02-002-0090	網際網路控制台\安全性畫面\網際網路	不要對ActiveX控制項執行反惡意程式碼程式(網際網路區域)	√	√	
91	Internet Explorer 11 Computer Settings	TWGCB-02-002-0091	網際網路控制台\安全性畫面\網際網路	使用快顯封鎖程式(網際網路區域)	√	√	
92	Internet Explorer 11 Computer Settings	TWGCB-02-002-0092	網際網路控制台\安全性畫面\網際網路	下載已簽署的ActiveX控制項(網際網路區域)	√	√	
93	Internet Explorer 11 Computer Settings	TWGCB-02-002-0093	網際網路控制台\安全性畫面\網際網路	下載未簽署的ActiveX控制項(網際網路區域)	√	√	
94	Internet Explorer 11 Computer Settings	TWGCB-02-002-0094	網際網路控制台\安全性畫面\網際網路	啟用跨視窗拖曳不同網域的內容(網際網路區域)	√	√	

項次	GPO	TWGCB-ID	類別	原則設定名稱	是否套用	測試結果	備註
95	Internet Explorer 11 Computer Settings	TWGCB-02-002-0095	網際網路控制台\安全性畫面\網際網路	啟用視窗內拖曳不同網域的內容(網際網路區域)	√	√	
96	Internet Explorer 11 Computer Settings	TWGCB-02-002-0096	網際網路控制台\安全性畫面\網際網路	允許拖放或複製及貼上檔案(網際網路區域)	√	√	
97	Internet Explorer 11 Computer Settings	TWGCB-02-002-0097	網際網路控制台\安全性畫面\網際網路	允許字型下載(網際網路區域)	√	√	
98	Internet Explorer 11 Computer Settings	TWGCB-02-002-0098	網際網路控制台\安全性畫面\網際網路	允許安裝桌面項目(網際網路區域)	√	√	
99	Internet Explorer 11 Computer Settings	TWGCB-02-002-0099	網際網路控制台\安全性畫面\網際網路	Java 權限(網際網路區域)	√	√	
100	Internet Explorer 11 Computer Settings	TWGCB-02-002-0100	網際網路控制台\安全性畫面\網際網路	啟動在 IFRAME 中的應用程式及檔案(網際網路區域)	√	√	
101	Internet Explorer 11 Computer Settings	TWGCB-02-002-0101	網際網路控制台\安全性畫面\網際網路	登入選項(網際網路區域)	√	√	
102	Internet Explorer 11 Computer Settings	TWGCB-02-002-0102	網際網路控制台\安全性畫面\網際網路	啟用 MIME 探查(網際網路區域)	√	√	
103	Internet Explorer 11 Computer Settings	TWGCB-02-002-0103	網際網路控制台\安全性畫面\網際網路	查閱不同網域內的視窗和框架(網際網路區域)	√	√	
104	Internet Explorer 11 Computer Settings	TWGCB-02-002-0104	網際網路控制台\安全性畫面\網際網路	自動提示檔案下載(網際網路區域)	√	√	
105	Internet Explorer 11 Computer Settings	TWGCB-02-002-0105	網際網路控制台\安全性畫面\網際網路	僅允許批准的網域使用 ActiveX 控制項而且不提示(網際網路區域)	√	√	
106	Internet Explorer 11 Computer Settings	TWGCB-02-002-0106	網際網路控制台\安全性畫面\網際網路	起始不標示為安全的 ActiveX 控制項(網際網路區域)	√	√	
107	Internet Explorer 11 Computer Settings	TWGCB-02-002-0107	網際網路控制台\安全性畫面\網際網路	執行使用 Authenticode 簽署的 .NET Framework 相依元件(網際網路區域)	√	√	
108	Internet Explorer 11 Computer Settings	TWGCB-02-002-0108	網際網路控制台\安全性畫面\網際網路	軟體頻道權限(網際網路區域)	√	√	
109	Internet Explorer 11 Computer Settings	TWGCB-02-002-0109	網際網路控制台\安全性畫面\網際網路	開啟跨網站指令碼篩選(網際網路區域)	√	√	
110	Internet Explorer 11 Computer Settings	TWGCB-02-002-0110	網際網路控制台\安全性畫面\網際網路	執行沒有使用 Authenticode 簽署的 .NET Framework 相依元件(網際網路區域)	√	√	
111	Internet Explorer 11 Computer Settings	TWGCB-02-002-0111	網際網路控制台\安全性畫面\網際網路	保留使用者資料(網際網路區域)	√	√	

項次	GPO	TWGCB-ID	類別	原則設定名稱	是否套用	測試結果	備註
112	Internet Explorer 11 Computer Settings	TWGCB-02-002-0112	網際網路控制台\安全性畫面\網際網路	允許由指令碼起始沒有大小或位置限制的視窗(網際網路區域)	√	√	
113	Internet Explorer 11 Computer Settings	TWGCB-02-002-0113	網際網路控制台\安全性畫面\網際網路	在較少特殊權限的網頁內容區域中的網站可以瀏覽到這個區域(網際網路區域)	√	√	
114	Internet Explorer 11 Computer Settings	TWGCB-02-002-0114	網際網路控制台\安全性畫面\網際網路	允許程式碼片段(網際網路區域)	√	√	
115	Internet Explorer 11 Computer Settings	TWGCB-02-002-0115	網際網路控制台\安全性畫面\網際網路	關閉第一次執行提示(網際網路區域)	√	√	
116	Internet Explorer 11 Computer Settings	TWGCB-02-002-0116	網際網路控制台\安全性畫面\網際網路	使用者將檔案上傳到伺服器時包含本機路徑(網際網路區域)	√	√	
117	Internet Explorer 11 Computer Settings	TWGCB-02-002-0117	網際網路控制台\安全性畫面\網際網路	允許透過指令碼更新狀態列(網際網路區域)	√	√	
118	Internet Explorer 11 Computer Settings	TWGCB-02-002-0118	網際網路控制台\安全性畫面\網際網路	開啟受保護模式(網際網路區域)	√	√	
119	Internet Explorer 11 Computer Settings	TWGCB-02-002-0119	網際網路控制台\安全性畫面\網際網路	顯示可能不安全檔案的安全性警告(網際網路區域)	√	√	
120	Internet Explorer 11 Computer Settings	TWGCB-02-002-0120	網際網路控制台\安全性畫面\網際網路	允許Internet Explorer WebBrowser控制項的指令碼(網際網路區域)	√	√	
121	Internet Explorer 11 Computer Settings	TWGCB-02-002-0121	網際網路控制台\安全性畫面\網際網路	允許載入XAML檔案(網際網路區域)	√	√	
122	Internet Explorer 11 Computer Settings	TWGCB-02-002-0122	網際網路控制台\安全性畫面\鎖定的內部網路區域	Java權限(鎖定的內部網路區域)	√	√	
123	Internet Explorer 11 Computer Settings	TWGCB-02-002-0123	網際網路控制台\安全性畫面\鎖定的內部網路區域	開啟SmartScreen篩選工具掃描(鎖定的內部網路區域)	√	√	
124	Internet Explorer 11 Computer Settings	TWGCB-02-002-0124	網際網路控制台\安全性畫面\鎖定的本機電腦區域	Java權限(鎖定的本機電腦區域)	√	√	
125	Internet Explorer 11 Computer Settings	TWGCB-02-002-0125	網際網路控制台\安全性畫面\鎖定的本機電腦區域	開啟SmartScreen篩選工具掃描(鎖定的本機電腦區域)	√	√	
126	Internet Explorer 11 Computer Settings	TWGCB-02-002-0126	網際網路控制台\安全性畫面\鎖定的受限制的網站區域	Java權限(鎖定的受限制的網站區域)	√	√	

項次	GPO	TWGCB-ID	類別	原則設定名稱	是否套用	測試結果	備註
127	Internet Explorer 11 Computer Settings	TWGCB-02-002-0127	網際網路控制台\安全性畫面\鎖定的受限制的網站區域	僅允許批准的網域使用ActiveX控制項而且不提示(鎖定的受限制的網站區域)	√	√	
128	Internet Explorer 11 Computer Settings	TWGCB-02-002-0128	網際網路控制台\安全性畫面\鎖定的受限制的網站區域	開啟SmartScreen篩選工具掃描(鎖定的受限制的網站區域)	√	√	
129	Internet Explorer 11 Computer Settings	TWGCB-02-002-0129	網際網路控制台\安全性畫面\鎖定的信任的網站區域	Java權限(鎖定的信任的網站區域)	√	√	
130	Internet Explorer 11 Computer Settings	TWGCB-02-002-0130	網際網路控制台\安全性畫面\鎖定的信任的網站區域	開啟SmartScreen篩選工具掃描(鎖定的信任的網站區域)	√	√	
131	Internet Explorer 11 Computer Settings	TWGCB-02-002-0131	網際網路控制台\安全性畫面\鎖定的網際網路區域	下載已簽署的ActiveX控制項(鎖定的網際網路區域)	√	√	
132	Internet Explorer 11 Computer Settings	TWGCB-02-002-0132	網際網路控制台\安全性畫面\鎖定的網際網路區域	Java權限(鎖定的網際網路區域)	√	√	
133	Internet Explorer 11 Computer Settings	TWGCB-02-002-0133	網際網路控制台\安全性畫面\鎖定的網際網路區域	僅允許批准的網域使用ActiveX控制項而且不提示(鎖定的網際網路區域)	√	√	
134	Internet Explorer 11 Computer Settings	TWGCB-02-002-0134	網際網路控制台\安全性畫面\鎖定的網際網路區域	開啟SmartScreen篩選工具掃描(鎖定的網際網路區域)	√	√	
135	Internet Explorer 11 Computer Settings	TWGCB-02-002-0135	網際網路控制台\進階畫面	允許在使用者電腦上執行CD的主動式內容	√	√	
136	Internet Explorer 11 Computer Settings	TWGCB-02-002-0136	網際網路控制台\進階畫面	檢查伺服器憑證撤銷	√	√	
137	Internet Explorer 11 Computer Settings	TWGCB-02-002-0137	網際網路控制台\進階畫面	啟用加強的受保護模式時，不允許在受保護模式下執行ActiveX控制項	√	√	
138	Internet Explorer 11 Computer Settings	TWGCB-02-002-0138	網際網路控制台\進階畫面	檢查所下載程式上的簽章	√	√	
139	Internet Explorer 11 Computer Settings	TWGCB-02-002-0139	網際網路控制台\進階畫面	允許其他廠商瀏覽器延伸	√	√	
140	Internet Explorer 11 Computer Settings	TWGCB-02-002-0140	網際網路控制台\進階畫面	開啟加強的受保護模式	√	√	
141	Internet Explorer 11 Computer Settings	TWGCB-02-002-0141	網際網路控制台\進階畫面	在64位元版本的Windows上執行加強的受保護模式時，開啟64位元索引標籤處理程序	√	√	
142	Internet Explorer 11 Computer Settings	TWGCB-02-002-0142	網際網路控制台\進階畫面	自動檢查Internet Explorer更新	√	√	

項次	GPO	TWGCB-ID	類別	原則設定名稱	是否套用	測試結果	備註
143	Internet Explorer 11 Computer Settings	TWGCB-02-002-0143	網際網路控制台\進階畫面	即使簽章無效也允許執行或安裝軟體	√	√	
144	Internet Explorer 11 Computer Settings	TWGCB-02-002-0144	網際網路控制台\進階畫面	關閉加密支援	√	√	
145	Internet Explorer 11 Computer Settings	TWGCB-02-002-0145	網際網路設定\元件更新\定期檢查Internet Explorer和網際網路工具更	防止設定更新檢查間隔(天)	√	√	
146	Internet Explorer 11 Computer Settings	TWGCB-02-002-0146	網際網路設定\元件更新\定期檢查Internet Explorer和網際網路工具更	防止變更檢查Internet Explorer及網際網路工具更新時所顯示的URL	√	√	
147	Internet Explorer 11 Computer Settings	TWGCB-02-002-0147	隱私權	關閉「InPrivate瀏覽」	√	√	
148	Internet Explorer 11 Computer Settings	TWGCB-02-002-0148	Windows元件\RSS摘要	防止下載隨函附件	√	√	
149	Internet Explorer 11 User Settings	TWGCB-02-002-0149	Internet Explorer	停用Internet Explorer外部自訂	√	√	
150	Internet Explorer 11 User Settings	TWGCB-02-002-0150	Internet Explorer	停用變更憑證設定	√	√	
151	Internet Explorer 11 User Settings	TWGCB-02-002-0151	Internet Explorer	停用表單自動完成功能	√	√	
152	Internet Explorer 11 User Settings	TWGCB-02-002-0152	Internet Explorer	開啟表單上使用者名稱和密碼的自動完成功能	√	√	
153	Internet Explorer 11 User Settings	TWGCB-02-002-0153	網際網路設定\進階設定\網際網路連線精靈設定	自動啟動「網際網路連線精靈」	√	√	
154	Internet Explorer 11 User Settings	TWGCB-02-002-0154	網際網路設定\進階設定\瀏	關閉畫面轉換	√	√	

(四) Win 基本項目政府組態基準列表

項次	GPO	TWGCB-ID	類別	原則設定名稱	GCB設定值	是否套用	測試結果	備註
1	Windows Server 2016 Account Settings	TWGCB-01-007-0001	密碼原則	密碼最短使用期限	1天	√	√	
2	Windows Server 2016 Account Settings	TWGCB-01-007-0002	密碼原則	密碼最長使用期限	90天以下	√	√	
3	Windows Server 2016 Account Settings	TWGCB-01-007-0003	密碼原則	最小密碼長度	12個字元	√	√	
4	Windows Server 2016 Account Settings	TWGCB-01-007-0004	密碼原則	密碼必須符合複雜性需求	已啟用	√	√	
5	Windows Server 2016 Account Settings	TWGCB-01-007-0005	密碼原則	強制執行密碼歷程記錄	3個以上記憶的密碼	√	√	
6	Windows Server 2016 Account Settings	TWGCB-01-007-0006	密碼原則	使用可還原的加密來存放密碼	已停用	√	√	
7	Windows Server 2016 Account Settings	TWGCB-01-007-0007	帳戶鎖定原則	帳戶鎖定閾值	5次不正確的登入嘗試	√	√	
8	Windows Server 2016 Account Settings	TWGCB-01-007-0008	帳戶鎖定原則	重設帳戶鎖定計數器的時間間隔	15分鐘	√	√	
9	Windows Server 2016 Account Settings	TWGCB-01-007-0009	帳戶鎖定原則	帳戶鎖定時間	15分鐘	√	√	
10	Windows Server 2016 Common Settings	TWGCB-01-007-0010	安全性選項 Microsoft網路用戶端	Microsoft網路用戶端：傳送未加密的密碼到其他廠商的SMB伺服器	已停用	√	√	
11	Windows Server 2016 Common Settings	TWGCB-01-007-0011	安全性選項 Microsoft網路用戶端	Microsoft網路用戶端：數位簽章用戶端的通訊(如果伺服器同意)	已啟用	√	√	
12	Windows Server 2016 Common Settings	TWGCB-01-007-0012	安全性選項 Microsoft網路用戶端	Microsoft網路用戶端：數位簽章用戶端的通訊(自動)	已啟用	√	√	
13	Windows Server 2016 Common Settings	TWGCB-01-007-0013	安全性選項 Microsoft網路伺服器	Microsoft網路伺服器：伺服器SPN目標名稱驗證層級	關閉	√	√	
14	Windows Server 2016 Common Settings	TWGCB-01-007-0014	安全性選項 Microsoft網路伺服器	Microsoft網路伺服器：數位簽章伺服器的通訊(自動)	已啟用	√	√	
15	Windows Server 2016 Common Settings	TWGCB-01-007-0015	安全性選項 Microsoft網路伺服器	Microsoft網路伺服器：數位簽章伺服器的通訊(如果用戶端同意)	已啟用	√	√	
16	Windows Server 2016 Common Settings	TWGCB-01-007-0016	安全性選項 Microsoft網路伺服器	Microsoft網路伺服器：暫停工作階段前，要求的閒置時間	15分鐘	√	√	
17	Windows Server 2016 Common Settings	TWGCB-01-007-0017	安全性選項 Microsoft網路伺服器	Microsoft網路伺服器：當登入時數到期時，中斷用戶端連線	已啟用	√	√	
18	Windows Server 2016 Common Settings	TWGCB-01-007-0018	安全性選項\MSS	MSS：(NoDefaultExempt)Configure IPsec exemptions for various types of network traffic	Multicast, broadcast, and ISAKMP are exempt(Best for Windows XP)	√	√	
19	Windows Server 2016 Common Settings	TWGCB-01-007-0019	安全性選項\MSS	MSS：(KeepAliveTime)How often keep-alive packets are sent in milliseconds	300000 or 5 minutes(recommended)	√	√	
20	Windows Server 2016 Common Settings	TWGCB-01-007-0020	安全性選項\MSS	MSS：(TcpMaxDataRetransmissions)How many times unacknowledged data is retransmitted(3 recommended, 5 is default)	3	√	√	
21	Windows Server 2016 Common Settings	TWGCB-01-007-0021	安全性選項\MSS	MSS：(EnableCMPRedirect)Allow ICMP redirects to override OSPF generated routes	已啟用	√	√	
22	Windows Server 2016 Common Settings	TWGCB-01-007-0022	安全性選項\MSS	MSS：(Hidden)Hide Computer From the Browse List(not recommended except for highly secure environments)	已啟用	√	√	
23	Windows Server 2016 Common Settings	TWGCB-01-007-0023	安全性選項\MSS	MSS：(DisableIPSourceRouting)IP source routing protection level(protects against packet spoofing)	Highest protection, source routing is completely disabled	√	√	
24	Windows Server 2016 Common Settings	TWGCB-01-007-0024	安全性選項\MSS	MSS：(DisableIPSourceRouting IPv6)IP source routing protection level(protects against packet spoofing)	Highest protection, source routing is completely disabled	√	√	
25	Windows Server 2016 Common Settings	TWGCB-01-007-0025	安全性選項\MSS	MSS：(NoNameReleaseOnDemand)Allow the computer to ignore NetBIOS name release requests except from WINS servers	已啟用	√	√	
26	Windows Server 2016 Common Settings	TWGCB-01-007-0026	安全性選項\MSS	MSS：(TcpMaxDataRetransmissions IPv6)How many times unacknowledged data is retransmitted(3 recommended, 5 is default)	3	√	√	
27	Windows Server 2016 Common Settings	TWGCB-01-007-0027	安全性選項\MSS	MSS：(PerformRouterDiscovery)Allow IRDP to detect and configure Default Gateway addresses(could lead to DoS)	已啟用	√	√	
28	Windows Server 2016 Common Settings	TWGCB-01-007-0028	安全性選項\MSS	MSS：(AutoReboot)Allow Windows to automatically restart after a system crash(recommended except for highly secure environments)	已啟用	√	√	
29	Windows Server 2016 Common Settings	TWGCB-01-007-0029	安全性選項\MSS	MSS：(WarningLevel)Percentage threshold for the security event log at which the system will generate a warning	90%	√	√	

項次	GPO	TWGCB-ID	類別	原則設定名稱	GCB設定值	是否套用	測試結果	備註
30	Windows Server 2016 Common Settings	TWGCB-01-007-0030	安全性選項\MSS	MSS : (SafeDllSearchMode)Enable Safe DLL search mode(recommended)	已啟用	√	√	
31	Windows Server 2016 Common Settings	TWGCB-01-007-0031	安全性選項\MSS	MSS : (AutoAdminLogon)Enable Automatic Logon(not recommended)	已停用	√	√	
32	Windows Server 2016 Common Settings	TWGCB-01-007-0032	安全性選項\MSS	MSS : (AutoShareServer)Enable Administrative Shares(recommended except for highly secure environments)	已啟用	√	√	
33	Windows Server 2016 Common Settings	TWGCB-01-007-0033	安全性選項\MSS	MSS : (ScreenSaverGracePeriod)The time in seconds before the screen saver grace period expires(0 recommended)	0	√	√	
34	Windows Server 2016 Common Settings	TWGCB-01-007-0034	安全性選項\互動式登入	互動式登入：在密碼到期前提示使用者變更密碼	14天	√	√	
35	Windows Server 2016 Common Settings	TWGCB-01-007-0035	安全性選項\互動式登入	互動式登入：要求網域控制站驗證以解除鎖定工作站	已啟用	√	√	
36	Windows Server 2016 Common Settings	TWGCB-01-007-0036	安全性選項\互動式登入	互動式登入：網域控制站無法使用時，要快取的先前登入次數	4次	√	√	
37	Windows Server 2016 Common Settings	TWGCB-01-007-0037	安全性選項\互動式登入	互動式登入：智慧卡移除操作	鎖定工作站	√	√	
38	Windows Server 2016 Common Settings	TWGCB-01-007-0038	安全性選項\互動式登入	互動式登入：須有智慧卡	已停用	√	√	
39	Windows Server 2016 Common Settings	TWGCB-01-007-0039	安全性選項\互動式登入	互動式登入：不要按CTRL+ALT+DEL鍵	已停用	√	√	
40	Windows Server 2016 Common Settings	TWGCB-01-007-0040	安全性選項\互動式登入	互動式登入：不要顯示上次登入的使用者名稱	已啟用	√	√	
41	Windows Server 2016 Common Settings	TWGCB-01-007-0041	安全性選項\互動式登入	互動式登入：電腦未使用時間限制	900秒	√	√	
42	Windows Server 2016 Common Settings	TWGCB-01-007-0042	安全性選項\系統加密編譯	系統密碼編譯：對使用者儲存在電腦上的金鑰強制使用增強式金鑰保護	當新金鑰被儲存及使用時，不要求使用者的輸入	√	√	
43	Windows Server 2016 Common Settings	TWGCB-01-007-0043	安全性選項\系統加密編譯	系統密碼編譯：使用 FIPS 相容演算法於加密、雜湊，以及簽章	已啟用	√	√	
44	Windows Server 2016 Common Settings	TWGCB-01-007-0044	安全性選項\系統物件	系統物件：加強內部系統物件的預設權限(例如：符號連結)	已啟用	√	√	
45	Windows Server 2016 Common Settings	TWGCB-01-007-0045	安全性選項\系統物件	系統物件：要求不區分大小寫用於非 Windows 系統	已啟用	√	√	
46	Windows Server 2016 Common Settings	TWGCB-01-007-0046	安全性選項\系統設定	系統設定：選擇性的子系統	Posix	√	√	
47	Windows Server 2016 Common Settings	TWGCB-01-007-0047	安全性選項\系統設定	系統設定：於軟體限制原則對 Windows 可執行檔使用憑證規則	已啟用	√	√	
48	Windows Server 2016 Common Settings	TWGCB-01-007-0048	安全性選項\使用者帳戶控制	使用者帳戶控制：提示提升權限時切換到安全桌面	已啟用	√	√	
49	Windows Server 2016 Common Settings	TWGCB-01-007-0049	安全性選項\使用者帳戶控制	使用者帳戶控制：允許 UIAccess 應用程式不使用安全桌面來提升權限	已停用	√	√	
50	Windows Server 2016 Common Settings	TWGCB-01-007-0050	安全性選項\使用者帳戶控制	使用者帳戶控制：在管理員核准模式，系統管理員之提升權限提示的行為	提示要求同意非 Windows 二進位檔案	√	√	
51	Windows Server 2016 Common Settings	TWGCB-01-007-0051	安全性選項\使用者帳戶控制	使用者帳戶控制：僅針對已簽署與驗證過的可執行檔，提高其權限	已停用	√	√	
52	Windows Server 2016 Common Settings	TWGCB-01-007-0052	安全性選項\使用者帳戶控制	使用者帳戶控制：所有系統管理員均以管理員核准模式執行	已啟用	√	√	
53	Windows Server 2016 Common Settings	TWGCB-01-007-0053	安全性選項\使用者帳戶控制	使用者帳戶控制：偵測應用程式安裝，並提示提升權限	已啟用	√	√	
54	Windows Server 2016 Common Settings	TWGCB-01-007-0054	安全性選項\使用者帳戶控制	使用者帳戶控制：內建的 Administrator 帳戶的管理員核准模式	已啟用	√	√	
55	Windows Server 2016 Common Settings	TWGCB-01-007-0055	安全性選項\使用者帳戶控制	使用者帳戶控制：標準使用者之提高權限提示的行為	提示輸入認證	√	√	
56	Windows Server 2016 Common Settings	TWGCB-01-007-0056	安全性選項\使用者帳戶控制	使用者帳戶控制：僅針對在安全位置安裝的 UIAccess 應用程式，提高其權限	已啟用	√	√	
57	Windows Server 2016 Common Settings	TWGCB-01-007-0057	安全性選項\使用者帳戶控制	使用者帳戶控制：將檔案及登錄寫入失敗虛擬化並儲存至每一使用者位置	已啟用	√	√	
58	Windows Server 2016 Common Settings	TWGCB-01-007-0058	安全性選項\修復主控台	修復主控台：允許軟體複製以及存取所有磁碟和所有資料夾	已停用	√	√	
59	Windows Server 2016 Common Settings	TWGCB-01-007-0059	安全性選項\修復主控台	修復主控台：允許自動系統管理登入	已停用	√	√	
60	Windows Server 2016 Common Settings	TWGCB-01-007-0060	安全性選項\帳戶	帳戶：限制使用空白密碼的本機帳戶僅能登入到主控台	已啟用	√	√	
61	Windows Server 2016 Common Settings	TWGCB-01-007-0061	安全性選項\帳戶	帳戶：重新命名來賓帳戶名稱	Renamed_Guest	√	√	
62	Windows Server 2016 Common Settings	TWGCB-01-007-0062	安全性選項\帳戶	帳戶：重新命名系統管理員帳戶	Renamed_Admin	√	√	
63	Windows Server 2016 Common Settings	TWGCB-01-007-0063	安全性選項\帳戶	帳戶：Administrator 帳戶狀態	已停用	√	√	
64	Windows Server 2016 Common Settings	TWGCB-01-007-0064	安全性選項\帳戶	帳戶：Guest 帳戶狀態	已停用	√	√	
65	Windows Server 2016 Common Settings	TWGCB-01-007-0065	安全性選項\裝置	裝置：防止使用者安裝桌機驅動程式	已啟用	√	√	
66	Windows Server 2016 Common Settings	TWGCB-01-007-0066	安全性選項\裝置	裝置：允許卸除而不須登入	已停用	√	√	

項次	GPO	TWGCB-ID	類別	原則設定名稱	GCB設定值	是否套用	測試結果	備註
67	Windows Server 2016 Common Settings	TWGCB-01-007-0067	安全性選項\裝置	裝置：允許格式化以及退出抽取式媒體	Administrators	✓	✓	
68	Windows Server 2016 Common Settings	TWGCB-01-007-0068	安全性選項\裝置	裝置：CD-ROM存取只限於登入本機的使用者	已停用	✓	✓	
69	Windows Server 2016 Common Settings	TWGCB-01-007-0069	安全性選項\裝置	裝置：軟碟機存取只限於登入本機的使用者	已停用	✓	✓	
70	Windows Server 2016 Common Settings	TWGCB-01-007-0070	安全性選項\網域成員	網域成員：停用電腦帳戶密碼變更	已停用	✓	✓	
71	Windows Server 2016 Common Settings	TWGCB-01-007-0071	安全性選項\網域成員	網域成員：最長電腦帳戶密碼有效期	30天	✓	✓	
72	Windows Server 2016 Common Settings	TWGCB-01-007-0072	安全性選項\網域成員	網域成員：安全通道資料加以數位加密或簽章(自動)	已啟用	✓	✓	
73	Windows Server 2016 Common Settings	TWGCB-01-007-0073	安全性選項\網域成員	網域成員：安全通道資料加以數位簽章(自動)	已啟用	✓	✓	
74	Windows Server 2016 Common Settings	TWGCB-01-007-0074	安全性選項\網域成員	網域成員：要求增強式(Windows 2000或更新)工作階段金鑰	已啟用	✓	✓	
75	Windows Server 2016 Common Settings	TWGCB-01-007-0075	安全性選項\網域成員	網域成員：安全通道資料加以數位加密(可能的話)	已啟用	✓	✓	
76	Windows Server 2016 Common Settings	TWGCB-01-007-0076	安全性選項\網路存取	網路存取：讓Everyone權限套用到匿名使用者	已停用	✓	✓	
77	Windows Server 2016 Common Settings	TWGCB-01-007-0077	安全性選項\網路存取	網路存取：共用和安全性模式用於本機帳戶	傳統-本機使用者以自身身分驗證	✓	✓	
78	Windows Server 2016 Common Settings	TWGCB-01-007-0078	安全性選項\網路存取	網路存取：不允許SAM帳戶的匿名列舉	已啟用	✓	✓	
79	Windows Server 2016 Common Settings	TWGCB-01-007-0079	安全性選項\網路存取	網路存取：限制匿名存取具名管道和共用	已啟用	✓	✓	
80	Windows Server 2016 Common Settings	TWGCB-01-007-0080	安全性選項\網路存取	網路存取：可遠端存取的登錄路徑及子路徑	System\CurrentControlSet\Control\Print\Printers	✓	✓	
					System\CurrentControlSet\Services\Eventlog	✓	✓	
					Software\Microsoft\OLAP Server	✓	✓	
					Software\Microsoft\Windows NT\CurrentVersion\Print	✓	✓	
					Software\Microsoft\Windows	✓	✓	
					System\CurrentControlSet\Control\ContentIndex	✓	✓	
					System\CurrentControlSet\Control\Terminal Server	✓	✓	
					System\CurrentControlSet\Control\Terminal	✓	✓	
					System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration	✓	✓	
					Software\Microsoft\Windows	✓	✓	
System\CurrentControlSet\Services\SysmonLog	✓	✓						
81	Windows Server 2016 Common Settings	TWGCB-01-007-0081	安全性選項\網路存取	網路存取：允許匿名SID/名稱轉譯	已停用	✓	✓	
82	Windows Server 2016 Common Settings	TWGCB-01-007-0082	安全性選項\網路存取	網路存取：可以匿名存取的共用	無	✓	✓	
83	Windows Server 2016 Common Settings	TWGCB-01-007-0083	安全性選項\網路存取	網路存取：可以匿名存取的具名管道	無	✓	✓	
84	Windows Server 2016 Common Settings	TWGCB-01-007-0084	安全性選項\網路存取	網路存取：可遠端存取的登錄路徑	System\CurrentControlSet\Control\ProductOptions	✓	✓	
					System\CurrentControlSet\Control\Server Applications	✓	✓	
					Software\Microsoft\Windows NT\CurrentVersion	✓	✓	
85	Windows Server 2016 Common Settings	TWGCB-01-007-0085	安全性選項\網路存取	網路存取：不允許存放網路驗證的密碼與認證	已停用	✓	✓	
86	Windows Server 2016 Common Settings	TWGCB-01-007-0086	安全性選項\網路存取	網路存取：不允許SAM帳戶和共用的匿名列舉	已啟用	✓	✓	
87	Windows Server 2016 Common Settings	TWGCB-01-007-0087	安全性選項\網路安全性	網路安全性：下次密碼變更時不儲存LAN Manager雜湊數值	已啟用	✓	✓	
88	Windows Server 2016 Common Settings	TWGCB-01-007-0088	安全性選項\網路安全性	網路安全性：允許Local System對NTLM使用電腦身分識別	已啟用	✓	✓	
89	Windows Server 2016 Common Settings	TWGCB-01-007-0089	安全性選項\網路安全性	網路安全性：LAN Manager驗證等級	只傳送NTLMv2回應\拒絕LM和NTLM	✓	✓	
90	Windows Server 2016 Common Settings	TWGCB-01-007-0090	安全性選項\網路安全性	網路安全性：允許對此電腦的PKU2U驗證要求使用線上身分識別	已停用	✓	✓	
91	Windows Server 2016 Common Settings	TWGCB-01-007-0091	安全性選項\網路安全性	網路安全性：NTLM SSP為主的(包含安全)的機器是工作階段的安全性	要求NTLMv2工作階段安全性	✓	✓	

項次	GPO	TWGCB-ID	類別	原則設定名稱	GCB設定值	是否套用	測試結果	備註
	Common Settings	007-0092	安全性	全RPC伺服器端的最小工作階段安全性	要求128位元加密	✓	✓	
92	Windows Server 2016 Common Settings	TWGCB-01-007-0092	安全性選項\網路安全性	網路安全性：允許LocalSystem NULL工作階段回復	已停用	✓	✓	
93	Windows Server 2016 Common Settings	TWGCB-01-007-0093	安全性選項\網路安全性	網路安全性：NTLM SSP為主的(包含安全RPC)用戶端的最小工作階段安全性	要求NTLMv2工作階段安全性	✓	✓	
94	Windows Server 2016 Common Settings	TWGCB-01-007-0094	安全性選項\網路安全性	網路安全性：設定Kerberos允許的加密類型	RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, 未來的加密類型	✓	✓	
95	Windows Server 2016 Common Settings	TWGCB-01-007-0095	安全性選項\網路安全性	網路安全性：LDAP用戶端簽章要求	交涉簽章	✓	✓	
96	Windows Server 2016 Common Settings	TWGCB-01-007-0096	安全性選項\網路安全性	網路安全性：強制限制登入時數	已停用	✓	✓	
97	Windows Server 2016 Common Settings	TWGCB-01-007-0097	安全性選項\稽核	稽核：當無法記錄安全性稽核時，系統立即關機	已停用	✓	✓	
98	Windows Server 2016 Common Settings	TWGCB-01-007-0098	安全性選項\稽核	稽核：稽核通用系統物件的存取	已停用	✓	✓	
99	Windows Server 2016 Common Settings	TWGCB-01-007-0099	安全性選項\稽核	稽核：稽核備份與還原權限的使用	已停用	✓	✓	
100	Windows Server 2016 Common Settings	TWGCB-01-007-0100	安全性選項\稽核	稽核：強制執行稽核原則子類別設定(Windows Vista或更新版本)以覆寫稽核原則類別設定	已啟用	✓	✓	
101	Windows Server 2016 Common Settings	TWGCB-01-007-0101	安全性選項\關機	關機：允許不登入就將系統關機	已停用	✓	✓	
102	Windows Server 2016 Common Settings	TWGCB-01-007-0102	安全性選項\關機	關機：清除虛擬記憶體分頁檔	已停用	✓	✓	
103	Windows Server 2016 Common Settings	TWGCB-01-007-0103	使用者權限指派	鎖定記憶體中的分頁	No One	✓	✓	
104	Windows Server 2016 Common Settings	TWGCB-01-007-0104	使用者權限指派	增加處理程序工作組	Administrators, Local Service	✓	✓	
105	Windows Server 2016 Common Settings	TWGCB-01-007-0105	使用者權限指派	關閉系統	Administrators	✓	✓	
106	Windows Server 2016 Common Settings	TWGCB-01-007-0106	使用者權限指派	調整處理程序的記憶體配額	Administrators, Local Service, Network Service	✓	✓	
107	Windows Server 2016 Common Settings	TWGCB-01-007-0107	使用者權限指派	取代處理程序等級權杖	Local Service, Network Service	✓	✓	
108	Windows Server 2016 Common Settings	TWGCB-01-007-0108	使用者權限指派	取得檔案或其他物件的擁有權	Administrators	✓	✓	
109	Windows Server 2016 Common Settings	TWGCB-01-007-0109	使用者權限指派	拒絕透過遠端桌面服務登入	Guests, 本機帳戶	✓	✓	
110	Windows Server 2016 Common Settings	TWGCB-01-007-0110	使用者權限指派	拒絕從網路存取這台電腦	Guests, 本機帳戶與 Administrators群組的成員	✓	✓	
111	Windows Server 2016 Common Settings	TWGCB-01-007-0111	使用者權限指派	載入及解除載入裝置驅動程式	Administrators	✓	✓	
112	Windows Server 2016 Common Settings	TWGCB-01-007-0112	使用者權限指派	拒絕以服務方式登入	Guests	✓	✓	
113	Windows Server 2016 Common Settings	TWGCB-01-007-0113	使用者權限指派	讓電腦及使用者帳戶受信賴，以進行委派	No One	✓	✓	
114	Windows Server 2016 Common Settings	TWGCB-01-007-0114	使用者權限指派	備份檔案及目錄	Administrators	✓	✓	
115	Windows Server 2016 Common Settings	TWGCB-01-007-0115	使用者權限指派	修改物件標籤	No One	✓	✓	
116	Windows Server 2016 Common Settings	TWGCB-01-007-0116	使用者權限指派	當成作業系統的一部分	No One	✓	✓	
117	Windows Server 2016 Common Settings	TWGCB-01-007-0117	使用者權限指派	變更系統時間	LOCAL SERVICE, Administrators	✓	✓	
118	Windows Server 2016 Common Settings	TWGCB-01-007-0118	使用者權限指派	允許透過遠端桌面服務登入	Administrators	✓	✓	
119	Windows Server 2016 Common Settings	TWGCB-01-007-0119	使用者權限指派	修改軟體環境值	Administrators	✓	✓	
120	Windows Server 2016 Common Settings	TWGCB-01-007-0120	使用者權限指派	建立通用物件	Administrators, SERVICE, LOCAL SERVICE, NETWORK SERVICE	✓	✓	
121	Windows Server 2016 Common Settings	TWGCB-01-007-0121	使用者權限指派	監視系統效能	Administrators, NT SERVICE\WdiServiceHost	✓	✓	
122	Windows Server 2016 Common Settings	TWGCB-01-007-0122	使用者權限指派	產生安全性稽核	Local Service, Network Service	✓	✓	
123	Windows Server 2016 Common Settings	TWGCB-01-007-0123	使用者權限指派	以服務方式登入	No One	✓	✓	
124	Windows Server 2016 Common Settings	TWGCB-01-007-0124	使用者權限指派	存取認證管理員做為信任的呼叫者	No One	✓	✓	
125	Windows Server 2016 Common Settings	TWGCB-01-007-0125	使用者權限指派	變更時區	LOCAL SERVICE, Administrators	✓	✓	
126	Windows Server 2016 Common Settings	TWGCB-01-007-0126	使用者權限指派	執行磁碟區維護工作	Administrators	✓	✓	

項次	GPO	TWGCB-ID	類別	原則設定名稱	GCB設定值	是否套用	測試結果	備註
127	Windows Server 2016 Common Settings	TWGCB-01-007-0127	使用者權限指派	建立權杖物件	No One	✓	✓	
128	Windows Server 2016 Common Settings	TWGCB-01-007-0128	使用者權限指派	強制從遠端系統進行關閉	Administrators	✓	✓	
129	Windows Server 2016 Common Settings	TWGCB-01-007-0129	使用者權限指派	建立符號連結	Administrators	✓	✓	
130	Windows Server 2016 Common Settings	TWGCB-01-007-0130	使用者權限指派	從擴充座移除電腦	Administrators	✓	✓	
131	Windows Server 2016 Common Settings	TWGCB-01-007-0131	使用者權限指派	略過週週檢查	Administrators, Authenticated Users, Local Service, Network Service	✓	✓	
132	Windows Server 2016 Common Settings	TWGCB-01-007-0132	使用者權限指派	建立分頁檔	Administrators	✓	✓	
133	Windows Server 2016 Common Settings	TWGCB-01-007-0133	使用者權限指派	增加排程優先順序	Administrators	✓	✓	
134	Windows Server 2016 Common Settings	TWGCB-01-007-0134	使用者權限指派	管理稽核及安全性記錄檔	Administrators	✓	✓	
135	Windows Server 2016 Common Settings	TWGCB-01-007-0135	使用者權限指派	拒絕以批次工作登入	Guests	✓	✓	
136	Windows Server 2016 Common Settings	TWGCB-01-007-0136	使用者權限指派	拒絕本機登入	Guests	✓	✓	
137	Windows Server 2016 Common Settings	TWGCB-01-007-0137	使用者權限指派	偵錯程式	Administrators	✓	✓	
138	Windows Server 2016 Common Settings	TWGCB-01-007-0138	使用者權限指派	建立永久共用物件	No One	✓	✓	
139	Windows Server 2016 Common Settings	TWGCB-01-007-0139	使用者權限指派	還原檔案及目錄	Administrators	✓	✓	
140	Windows Server 2016 Common Settings	TWGCB-01-007-0140	使用者權限指派	監視單一處理程序	Administrators	✓	✓	
141	Windows Server 2016 Common Settings	TWGCB-01-007-0141	使用者權限指派	以批次工作登入	Administrators	✓	✓	
142	Windows Server 2016 Common Settings	TWGCB-01-007-0142	使用者權限指派	在驗證後模擬用戶端	Administrators, SERVICE, Local Service, Network	✓	✓	
143	Windows Server 2016 Common Settings	TWGCB-01-007-0143	使用者權限指派	從網路存取這台電腦	Administrators, Authenticated Users	✓	✓	
144	Windows Server 2016 Common Settings	TWGCB-01-007-0144	使用者權限指派	允許本機登入	Administrators	✓	✓	
145	Windows Server 2016 Common Settings	TWGCB-01-007-0145	系統管理範本/Windows Installer	永遠以較高的特殊權限安裝	已停用	✓	✓	
146	Windows Server 2016 Common Settings	TWGCB-01-007-0146	系統管理範本/Windows Installer	允許使用者控制安裝	已停用	✓	✓	
147	Windows Server 2016 Common Settings	TWGCB-01-007-0147	系統管理範本/Windows Installer	防止出現Windows Installer指令碼的Internet Explorer安全性提示	已停用	✓	✓	
148	Windows Server 2016 Common Settings	TWGCB-01-007-0148	系統管理範本/自動播放原則	關閉自動播放	已啟用；所有磁碟機	✓	✓	
149	Windows Server 2016 Common Settings	TWGCB-01-007-0149	系統管理範本/自動播放原則	不允許非磁碟區裝置的自動播放	已啟用	✓	✓	
150	Windows Server 2016 Common Settings	TWGCB-01-007-0150	系統管理範本/自動播放原則	設定AutoRun的預設行為	已啟用；不執行任何Autorun命令	✓	✓	
151	Windows Server 2016 Common Settings	TWGCB-01-007-0151	系統管理範本/遠端桌面服務	設定用戶端連線加密層級	已啟用；高等級	✓	✓	
152	Windows Server 2016 Common Settings	TWGCB-01-007-0152	系統管理範本/遠端桌面服務	連線時永遠提示密碼	已啟用	✓	✓	
153	Windows Server 2016 Common Settings	TWGCB-01-007-0153	系統管理範本/遠端桌面服務	需要安全的RPC通訊	已啟用	✓	✓	
154	Windows Server 2016 Common Settings	TWGCB-01-007-0154	系統管理範本/遠端桌面服務	不允許磁碟重新導向	已啟用	✓	✓	
155	Windows Server 2016 Common Settings	TWGCB-01-007-0155	系統管理範本/遠端桌面服務	不要使用每一工作階段的暫存資料夾	已停用	✓	✓	
156	Windows Server 2016 Common Settings	TWGCB-01-007-0156	系統管理範本/遠端桌面服務	結束後不刪除暫存資料夾	已停用	✓	✓	
157	Windows Server 2016 Common Settings	TWGCB-01-007-0157	系統管理範本/遠端桌面服務	不允許儲存密碼	已啟用	✓	✓	
158	Windows Server 2016 Common Settings	TWGCB-01-007-0158	事件記錄服務/安全性	指定記錄檔大小上限(KB)	已啟用；196608KB	✓	✓	
159	Windows Server 2016 Common Settings	TWGCB-01-007-0159	事件記錄服務/安全性	控制記錄檔達到其大小上限時的事件記錄檔行為	已停用	✓	✓	
160	Windows Server 2016 Common Settings	TWGCB-01-007-0160	事件記錄服務/系統	指定記錄檔大小上限(KB)	已啟用；32768KB	✓	✓	
161	Windows Server 2016 Common Settings	TWGCB-01-007-0161	事件記錄服務/系統	控制記錄檔達到其大小上限時的事件記錄檔行為	已停用	✓	✓	
162	Windows Server 2016 Common Settings	TWGCB-01-007-0162	事件記錄服務/應用程式	指定記錄檔大小上限(KB)	已啟用；32768KB	✓	✓	
163	Windows Server 2016 Common Settings	TWGCB-01-007-0163	事件記錄服務/應用程式	控制記錄檔達到其大小上限時的事件記錄檔行為	已停用	✓	✓	

項次	GPO	TWGCB-ID	類別	原則設定名稱	GCB設定值	是否套用	測試結果	備註
164	Windows Server 2016 Common Settings	TWGCB-01-007-0164	Windows元件 \\OneDrive	防止使用OneDrive儲存檔案	已啟用	√	√	
165	Windows Server 2016 Common Settings	TWGCB-01-007-0165	系統管理範本 \\Windows遠端殼	允許遠端殼層存取	已停用	√	√	
166	Windows Server 2016 Common Settings	TWGCB-01-007-0166	系統管理範本 \\Windows登入選	系統起始的重新啟動之後自動登入最後一個互動式使用者	已停用	√	√	
167	Windows Server 2016 Common Settings	TWGCB-01-007-0167	系統管理範本/市集	關閉市集應用程式	已啟用	√	√	
168	Windows Server 2016 Common Settings	TWGCB-01-007-0168	系統管理範本/市集	關閉自動下載和安裝更新	已啟用	√	√	
169	Windows Server 2016 Common Settings	TWGCB-01-007-0169	系統管理範本/市集	關閉更新至最新版Windows的服務	已啟用	√	√	
170	Windows Server 2016 Common Settings	TWGCB-01-007-0170	系統管理範本/登入	不要顯示網路選取UI	已啟用	√	√	
171	Windows Server 2016 Common Settings	TWGCB-01-007-0171	系統管理範本/登入	列舉加入網域電腦上的本機使用者	已停用	√	√	
172	Windows Server 2016 Common Settings	TWGCB-01-007-0172	系統管理範本/登入	關閉鎖定畫面上的應用程式通知	已啟用	√	√	
173	Windows Server 2016 Common Settings	TWGCB-01-007-0173	系統管理範本/稽核建立處理程序	在建立處理程序事件中包含命令列	已停用	√	√	
174	Windows Server 2016 Common Settings	TWGCB-01-007-0174	系統管理範本/搜尋	允許加密檔案索引	已停用	√	√	
175	Windows Server 2016 Common Settings	TWGCB-01-007-0175	系統管理範本/搜尋	設定「搜尋」中可以分享的資訊	已啟用：匿名資訊	√	√	
176	Windows Server 2016 Common Settings	TWGCB-01-007-0176	系統管理範本/應用程式執行階段	允許選用Microsoft帳戶	已啟用	√	√	
177	Windows Server 2016 Common Settings	TWGCB-01-007-0177	系統管理範本/網路通訊管理	關閉Windows Messenger客戶經驗改進計畫	已啟用	√	√	
178	Windows Server 2016 Common Settings	TWGCB-01-007-0178	系統管理範本/網路通訊管理	關閉搜尋小幫手內容檔更新	已啟用	√	√	
179	Windows Server 2016 Common Settings	TWGCB-01-007-0179	系統管理範本/網路通訊管理	關閉檔案和資料夾的「發佈到網站」工作	已啟用	√	√	
180	Windows Server 2016 Common Settings	TWGCB-01-007-0180	系統管理範本/網路通訊管理	關閉HTTP上的列印	已啟用	√	√	
181	Windows Server 2016 Common Settings	TWGCB-01-007-0181	系統管理範本/網路通訊管理	關閉Windows客戶經驗改進計畫	已啟用	√	√	
182	Windows Server 2016 Common Settings	TWGCB-01-007-0182	系統管理範本/網路通訊管理	關閉手寫辨識錯誤報告	已啟用	√	√	
183	Windows Server 2016 Common Settings	TWGCB-01-007-0183	系統管理範本/網路通訊管理	關閉市集的存取權	已啟用	√	√	
184	Windows Server 2016 Common Settings	TWGCB-01-007-0184	系統管理範本/網路通訊管理	關閉透過HTTP下載印表機驅動程式	已啟用	√	√	
185	Windows Server 2016 Common Settings	TWGCB-01-007-0185	系統管理範本/個人化	防止啟用鎖定畫面投影片放映	已啟用	√	√	
186	Windows Server 2016 Common Settings	TWGCB-01-007-0186	系統管理範本/個人化	防止啟用鎖定畫面相機	已啟用	√	√	
187	Windows Server 2016 Common Settings	TWGCB-01-007-0187	系統管理範本/個人化	以密碼保護螢幕保護裝置	已啟用	√	√	
188	Windows Server 2016 Common Settings	TWGCB-01-007-0188	系統管理範本/個人化	啟用螢幕保護裝置	已啟用	√	√	
189	Windows Server 2016 Common Settings	TWGCB-01-007-0189	系統管理範本/個人化	強制特定螢幕保護裝置	已啟用；並指定特定螢幕保護裝置(如scmsave.scr)	√	√	
190	Windows Server 2016 Common Settings	TWGCB-01-007-0190	系統管理範本\\MS Security Guide	Configure SMB v1 client driver	啟用；停用驅動程式	√	√	
191	Windows Server 2016 Common Settings	TWGCB-01-007-0191	系統管理範本\\MS Security Guide	Configure SMB v1 server	已停用	√	√	
192	Windows Server 2016 Common Settings	TWGCB-01-007-0192	系統管理範本/緩和選項	封鎖未受信任的字型	已啟用；封鎖未受信任的字型並記錄事件	√	√	
193	Windows Server 2016 Common Settings	TWGCB-01-007-0193	系統管理範本/Lanman工作站	啟用不安全的來賓登入	已停用	√	√	
194	Windows Server 2016 Common Settings	TWGCB-01-007-0194	進階稽核原則\\DS存取	稽核詳細目錄服務複寫	沒有稽核	√	√	
195	Windows Server 2016 Common Settings	TWGCB-01-007-0195	進階稽核原則\\DS存取	稽核目錄服務複寫	沒有稽核	√	√	
196	Windows Server 2016 Common Settings	TWGCB-01-007-0196	進階稽核原則\\系統	稽核系統完整性	成功與失敗	√	√	
197	Windows Server 2016 Common Settings	TWGCB-01-007-0197	進階稽核原則\\系統	稽核IPsec驅動程式	成功與失敗	√	√	
198	Windows Server 2016 Common Settings	TWGCB-01-007-0198	進階稽核原則\\系統	稽核安全性系統延伸	成功與失敗	√	√	
199	Windows Server 2016 Common Settings	TWGCB-01-007-0199	進階稽核原則\\系統	稽核其他系統事件	沒有稽核	√	√	
200	Windows Server 2016 Common Settings	TWGCB-01-007-0200	進階稽核原則\\系統	稽核安全性狀態變更	成功與失敗	√	√	
201	Windows Server 2016 Common Settings	TWGCB-01-007-0201	進階稽核原則\\物件存取	稽核其他物件存取事件	沒有稽核	√	√	

項次	GPO	TWGCB-ID	類別	原則設定名稱	GCB設定值	是否套用	測試結果	備註
202	Windows Server 2016 Common Settings	TWGCB-01-007-0202	進階稽核原則\物件存取	稽核控制代碼操作	沒有稽核	√	√	
203	Windows Server 2016 Common Settings	TWGCB-01-007-0203	進階稽核原則\物件存取	稽核檔案共用	沒有稽核	√	√	
204	Windows Server 2016 Common Settings	TWGCB-01-007-0204	進階稽核原則\物件存取	稽核篩選平台連線	沒有稽核	√	√	
205	Windows Server 2016 Common Settings	TWGCB-01-007-0205	進階稽核原則\物件存取	稽核憑證服務	沒有稽核	√	√	
206	Windows Server 2016 Common Settings	TWGCB-01-007-0206	進階稽核原則\物件存取	稽核檔案系統	沒有稽核	√	√	
207	Windows Server 2016 Common Settings	TWGCB-01-007-0207	進階稽核原則\物件存取	稽核SAM	沒有稽核	√	√	
208	Windows Server 2016 Common Settings	TWGCB-01-007-0208	進階稽核原則\物件存取	稽核篩選平台封包丟棄	沒有稽核	√	√	
209	Windows Server 2016 Common Settings	TWGCB-01-007-0209	進階稽核原則\物件存取	稽核產生的應用程式	沒有稽核	√	√	
210	Windows Server 2016 Common Settings	TWGCB-01-007-0210	進階稽核原則\物件存取	稽核登錄	沒有稽核	√	√	
211	Windows Server 2016 Common Settings	TWGCB-01-007-0211	進階稽核原則\物件存取	稽核詳細的檔案共用	沒有稽核	√	√	
212	Windows Server 2016 Common Settings	TWGCB-01-007-0212	進階稽核原則\物件存取	稽核核心物件	沒有稽核	√	√	
213	Windows Server 2016 Common Settings	TWGCB-01-007-0213	進階稽核原則\原則變更	稽核篩選平台原則變更	沒有稽核	√	√	
214	Windows Server 2016 Common Settings	TWGCB-01-007-0214	進階稽核原則\原則變更	稽核驗證原則變更	成功	√	√	
215	Windows Server 2016 Common Settings	TWGCB-01-007-0215	進階稽核原則\原則變更	稽核授權原則變更	沒有稽核	√	√	
216	Windows Server 2016 Common Settings	TWGCB-01-007-0216	進階稽核原則\原則變更	稽核「稽核原則變更」	成功與失敗	√	√	
217	Windows Server 2016 Common Settings	TWGCB-01-007-0217	進階稽核原則\原則變更	稽核MPSSVC規則層級原則變更	沒有稽核	√	√	
218	Windows Server 2016 Common Settings	TWGCB-01-007-0218	進階稽核原則\原則變更	稽核其他原則變更事件	沒有稽核	√	√	
219	Windows Server 2016 Common Settings	TWGCB-01-007-0219	進階稽核原則\特殊權限使用	稽核機密特殊權限使用	成功與失敗	√	√	
220	Windows Server 2016 Common Settings	TWGCB-01-007-0220	進階稽核原則\特殊權限使用	稽核非機密特殊權限使用	沒有稽核	√	√	
221	Windows Server 2016 Common Settings	TWGCB-01-007-0221	進階稽核原則\特殊權限使用	稽核其他特殊權限使用事件	沒有稽核	√	√	
222	Windows Server 2016 Common Settings	TWGCB-01-007-0222	進階稽核原則\帳戶登入	稽核Kerberos驗證服務	沒有稽核	√	√	
223	Windows Server 2016 Common Settings	TWGCB-01-007-0223	進階稽核原則\帳戶登入	稽核認證驗證	成功與失敗	√	√	
224	Windows Server 2016 Common Settings	TWGCB-01-007-0224	進階稽核原則\帳戶登入	稽核Kerberos服務票證操作	沒有稽核	√	√	
225	Windows Server 2016 Common Settings	TWGCB-01-007-0225	進階稽核原則\帳戶登入	稽核其他帳戶登入事件	沒有稽核	√	√	
226	Windows Server 2016 Common Settings	TWGCB-01-007-0226	進階稽核原則\帳戶管理	稽核應用程式群組管理	沒有稽核	√	√	
227	Windows Server 2016 Common Settings	TWGCB-01-007-0227	進階稽核原則\帳戶管理	稽核電腦帳戶管理	成功	√	√	
228	Windows Server 2016 Common Settings	TWGCB-01-007-0228	進階稽核原則\帳戶管理	稽核其他帳戶管理事件	成功與失敗	√	√	
229	Windows Server 2016 Common Settings	TWGCB-01-007-0229	進階稽核原則\帳戶管理	稽核安全性群組管理	成功與失敗	√	√	
230	Windows Server 2016 Common Settings	TWGCB-01-007-0230	進階稽核原則\帳戶管理	稽核發佈群組管理	沒有稽核	√	√	
231	Windows Server 2016 Common Settings	TWGCB-01-007-0231	進階稽核原則\帳戶管理	稽核使用者帳戶管理	成功與失敗	√	√	
232	Windows Server 2016 Common Settings	TWGCB-01-007-0232	進階稽核原則\登入/登出	稽核帳戶鎖定	沒有稽核	√	√	
233	Windows Server 2016 Common Settings	TWGCB-01-007-0233	進階稽核原則\登入/登出	稽核IPsec延伸模式	沒有稽核	√	√	
234	Windows Server 2016 Common Settings	TWGCB-01-007-0234	進階稽核原則\登入/登出	稽核網路原則伺服器	成功	√	√	
235	Windows Server 2016 Common Settings	TWGCB-01-007-0235	進階稽核原則\登入/登出	稽核IPsec主要模式	沒有稽核	√	√	
236	Windows Server 2016 Common Settings	TWGCB-01-007-0236	進階稽核原則\登入/登出	稽核其他登入/登出事件	沒有稽核	√	√	
237	Windows Server 2016 Common Settings	TWGCB-01-007-0237	進階稽核原則\登入/登出	稽核登出	成功	√	√	
238	Windows Server 2016 Common Settings	TWGCB-01-007-0238	進階稽核原則\登入/登出	稽核登入	成功與失敗	√	√	

項次	GPO	TWGCB-ID	類別	原則設定名稱	GCB設定值	是否套用	測試結果	備註
239	Windows Server 2016 Common Settings	TWGCB-01-007-0239	進階稽核原則\登入/登出	稽核IPsec快速模式	沒有稽核	√	√	
240	Windows Server 2016 Common Settings	TWGCB-01-007-0240	進階稽核原則\登入/登出	稽核特殊登入	成功	√	√	
241	Windows Server 2016 Common Settings	TWGCB-01-007-0241	進階稽核原則\詳細追蹤	稽核RPC事件	沒有稽核	√	√	
242	Windows Server 2016 Common Settings	TWGCB-01-007-0242	進階稽核原則\詳細追蹤	稽核DPAPI活動	沒有稽核	√	√	
243	Windows Server 2016 Common Settings	TWGCB-01-007-0243	進階稽核原則\詳細追蹤	稽核建立處理程序	成功	√	√	
244	Windows Server 2016 Common Settings	TWGCB-01-007-0244	進階稽核原則\詳細追蹤	稽核終止處理程序	沒有稽核	√	√	
245	Windows Server 2016 Common Settings	TWGCB-01-007-0245	Windows防火牆/網域設定檔	Windows防火牆：網域設定檔：輸出連線	允許(預設)	√	√	
246	Windows Server 2016 Common Settings	TWGCB-01-007-0246	Windows防火牆/網域設定檔	Windows防火牆：網域設定檔：防火牆狀態	開啟(建議選項)	√	√	
247	Windows Server 2016 Common Settings	TWGCB-01-007-0247	Windows防火牆/網域設定檔	Windows防火牆：網域設定檔：輸入連線	封鎖(預設)	√	√	
248	Windows Server 2016 Common Settings	TWGCB-01-007-0248	Windows防火牆/網域設定檔	Windows防火牆：網域設定檔：套用本機防火牆規則	是(預設)	√	√	
249	Windows Server 2016 Common Settings	TWGCB-01-007-0249	Windows防火牆/網域設定檔	Windows防火牆：網域設定檔：顯示通知	是	√	√	
250	Windows Server 2016 Common Settings	TWGCB-01-007-0250	Windows防火牆/網域設定檔	Windows防火牆：網域設定檔：套用本機連線安全性規則	是(預設)	√	√	
251	Windows Server 2016 Common Settings	TWGCB-01-007-0251	Windows防火牆/網域設定檔	Windows防火牆：網域設定檔：允許單點傳播回應	否	√	√	
252	Windows Server 2016 Common Settings	TWGCB-01-007-0252	Windows防火牆/私人設定檔	Windows防火牆：私人設定檔：防火牆狀態	開啟(建議選項)	√	√	
253	Windows Server 2016 Common Settings	TWGCB-01-007-0253	Windows防火牆/私人設定檔	Windows防火牆：私人設定檔：輸入連線	封鎖(預設)	√	√	
254	Windows Server 2016 Common Settings	TWGCB-01-007-0254	Windows防火牆/私人設定檔	Windows防火牆：私人設定檔：套用本機防火牆規則	是(預設)	√	√	
255	Windows Server 2016 Common Settings	TWGCB-01-007-0255	Windows防火牆/私人設定檔	Windows防火牆：私人設定檔：顯示通知	是	√	√	
256	Windows Server 2016 Common Settings	TWGCB-01-007-0256	Windows防火牆/私人設定檔	Windows防火牆：私人設定檔：允許單點傳播回應	否	√	√	
257	Windows Server 2016 Common Settings	TWGCB-01-007-0257	Windows防火牆/私人設定檔	Windows防火牆：私人設定檔：套用本機連線安全性規則	是(預設)	√	√	
258	Windows Server 2016 Common Settings	TWGCB-01-007-0258	Windows防火牆/私人設定檔	Windows防火牆：私人設定檔：輸出連線	允許(預設)	√	√	
259	Windows Server 2016 Common Settings	TWGCB-01-007-0259	Windows防火牆/公用設定檔	Windows防火牆：公用設定檔：允許單點傳播回應	否	√	√	
260	Windows Server 2016 Common Settings	TWGCB-01-007-0260	Windows防火牆/公用設定檔	Windows防火牆：公用設定檔：顯示通知	是	√	√	
261	Windows Server 2016 Common Settings	TWGCB-01-007-0261	Windows防火牆/公用設定檔	Windows防火牆：公用設定檔：套用本機連線安全性規則	是(預設)	√	√	
262	Windows Server 2016 Common Settings	TWGCB-01-007-0262	Windows防火牆/公用設定檔	Windows防火牆：公用設定檔：輸入連線	封鎖(預設)	√	√	
263	Windows Server 2016 Common Settings	TWGCB-01-007-0263	Windows防火牆/公用設定檔	Windows防火牆：公用設定檔：套用本機防火牆規則	是(預設)	√	√	
264	Windows Server 2016 Common Settings	TWGCB-01-007-0264	Windows防火牆/公用設定檔	Windows防火牆：公用設定檔：輸出連線	允許(預設)	√	√	
265	Windows Server 2016 Common Settings	TWGCB-01-007-0265	Windows防火牆/公用設定檔	Windows防火牆：公用設定檔：防火牆狀態	開啟(建議選項)	√	√	
266	Windows Server 2016 Common Settings	TWGCB-01-007-0266	系統管理範本/RSS摘要	防止下載隨函附件	已啟用	√	√	
267	Windows Server 2016 Common Settings	TWGCB-01-007-0267	系統管理範本/Windows	加入Microsoft地圖	已停用	√	√	
268	Windows Server 2016 Common Settings	TWGCB-01-007-0268	系統管理範本/Windows遠端管理(WinRM)	不允許摘要式驗證	已啟用	√	√	
269	Windows Server 2016 Common Settings	TWGCB-01-007-0269	系統管理範本/Windows遠端管理(WinRM)	允許未加密的流量	已停用	√	√	
270	Windows Server 2016 Common Settings	TWGCB-01-007-0270	系統管理範本/Windows遠端管理(WinRM)	允許基本驗證	已停用	√	√	
271	Windows Server 2016 Common Settings	TWGCB-01-007-0271	系統管理範本/Windows遠端管理(WinRM)	不允許WinRM儲存RunAs認證	已啟用	√	√	
272	Windows Server 2016 Common Settings	TWGCB-01-007-0272	系統管理範本/Windows遠端管理(WinRM)	允許未加密的流量	已停用	√	√	

項次	GPO	TWGCB-ID	類別	原則設定名稱	GCB設定值	是否套用	測試結果	備註
273	Windows Server 2016 Common Settings	TWGCB-01-007-0273	系統管理範本/ Windows遠端管理(WinRM)	允許基本驗證	已停用	√	√	
274	Windows Server 2016 Common Settings	TWGCB-01-007-0274	系統管理範本/定 位和感應器	關閉定位	已啟用	√	√	
275	Windows Server 2016 Common Settings	TWGCB-01-007-0275	系統管理範本/認 證使用者介面	不要顯示密碼顯示按鈕	已啟用	√	√	
276	Windows Server 2016 Common Settings	TWGCB-01-007-0276	系統管理範本/認 證使用者介面	提升權限時列舉系統管理員帳戶	已停用	√	√	
277	Windows Server 2016 Common Settings	TWGCB-01-007-0277	系統管理範本/檔 案總管	設定Windows SmartScreen篩選工具	已啟用	√	√	
278	Windows Server 2016 Common Settings	TWGCB-01-007-0278	系統管理範本/檔 案總管	損毀時關閉終止堆棧	已停用	√	√	
279	Windows Server 2016 Common Settings	TWGCB-01-007-0279	系統管理範本/檔 案總管	關閉殼層通訊協定受保護模式	已停用	√	√	
280	Windows Server 2016 Common Settings	TWGCB-01-007-0280	系統管理範本/檔 案總管	關閉檔案總管的資料執行防止	已停用	√	√	
281	Windows Server 2016 Common Settings	TWGCB-01-007-0281	系統管理範本/開 機初期啟動的反 惡意程式碼	開機啟動驅動程式初始化原則	已啟用：良好和不明	√	√	
282	Windows Server 2016 Common Settings	TWGCB-01-007-0282	系統管理範本/睡 眠設定	喚醒電腦時必須使用密碼(一般電源)	已啟用	√	√	
283	Windows Server 2016 Common Settings	TWGCB-01-007-0283	系統管理範本/睡 眠設定	喚醒電腦時必須使用密碼(使用電池)	已啟用	√	√	
284	Windows Server 2016 Common Settings	TWGCB-01-007-0284	系統管理範本/疑 難排解與診斷	Microsoft支援服務診斷工具：開啟MSDT與支援提供者的互動式通訊	已停用	√	√	
285	Windows Server 2016 Common Settings	TWGCB-01-007-0285	系統管理範本/疑 難排解與診斷	啟用/停用PerfTrack	已停用	√	√	
286	Windows Server 2016 Common Settings	TWGCB-01-007-0286	系統管理範本/遠 端協助	設定提供遠端協助	已停用	√	√	
287	Windows Server 2016 Common Settings	TWGCB-01-007-0287	系統管理範本/遠 端協助	設定請求遠端協助	已停用	√	√	
288	Windows Server 2016 Common Settings	TWGCB-01-007-0288	系統管理範本 /Microsoft對等網 路服務	關閉Microsoft對等網路服務	已啟用	√	√	
289	Windows Server 2016 Common Settings	TWGCB-01-007-0289	系統管理範本 /Windows Connect Now	使用Windows Connect Now進行無線設定	已停用	√	√	
290	Windows Server 2016 Common Settings	TWGCB-01-007-0290	系統管理範本 /Windows Connect Now	禁止存取Windows Connect Now精靈	已啟用	√	√	
291	Windows Server 2016 Common Settings	TWGCB-01-007-0291	系統管理範本/連 結階層拓撲搜索	開啟Mapper I/O(LLTDIO)驅動程式	已停用	√	√	
292	Windows Server 2016 Common Settings	TWGCB-01-007-0292	系統管理範本/連 結階層拓撲搜索	開啟Responder(RSPNDR)驅動程式	已停用	√	√	
293	Windows Server 2016 Common Settings	TWGCB-01-007-0293	系統管理範本/網 路連線	要求網域使用者在設定網路的位置時必須提升權限	已啟用	√	√	
294	Windows Server 2016 Common Settings	TWGCB-01-007-0294	系統管理範本/網 路連線	禁止在您的DNS網域網路上安裝、設定及使用網路橋接	已啟用	√	√	
295	Windows Server 2016 Common Settings	TWGCB-01-007-0295	系統管理範本/通 知	在鎖定畫面上關閉快顯通知	已啟用	√	√	
296	Windows Server 2016 Common Settings	TWGCB-01-007-0296	系統管理範本 /Windows Media Player	防止轉碼器下載	已啟用	√	√	
297	Windows Server 2016 Common Settings	TWGCB-01-007-0297	系統管理範本/附 件管理員	不要保留檔案附件的區域資訊	已停用	√	√	
298	Windows Server 2016 Common Settings	TWGCB-01-007-0298	系統管理範本/附 件管理員	開啟附件時通知防毒程式	已啟用	√	√	
299	Windows Server 2016 Common Settings	TWGCB-01-007-0299	系統管理範本/網 路共用	防止使用者共用其設定檔內的檔案	已啟用	√	√	

三、資安防護基準作業報告

資通系統名稱：測繪成果圖冊管理系統		機密等級：普通版次：VI.00 表單編號：ISMS-01170108		業務單位名稱：		審核日期： 年 月 日		預計改善作為		完成日期		備註	
項次	控制領域	控制措施	說明	符合性		符合性或不適用情況說明	符合性情況說明：	不適用情況說明：	符合性情況說明：	不適用情況說明：	符合性情況說明：	不適用情況說明：	備註
				符合	未完全符合								
1	存取控制	帳號管理	控制方式(詳細內容詳參圖冊管理系統) 資通安全責任等級分級辦法(附表十)	<p>普通系統之帳號應透過正式之帳號申請程序所建立，完成開通審核程序始能使用，因此系統應具備帳號管理機制，可對系統帳號進行申請、開通、停用或刪除之行為。</p> <p>建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序。</p>	V	<p>符合性情況說明：</p> <input type="checkbox"/> 已建立帳號管理程序 <input type="checkbox"/> 文件名稱： <input type="checkbox"/> 已建立帳號申請/開通/停用之審核流程 <input type="checkbox"/> 離職表單會辦審核單位 <input checked="" type="checkbox"/> 定期辦理帳號清查作業(每月1個月) <input type="checkbox"/> 採用自動化機制來支援普通系統帳號管理 <input type="checkbox"/> 其他： 不適用情況說明：	<p>符合性情況說明：</p> <input type="checkbox"/> 人工選擇刪除或停用臨時和緊急帳號 <input type="checkbox"/> 普通系統會自動選擇刪除或停用臨時和緊急帳號 <input type="checkbox"/> 其他： 不適用情況說明：本系統無提供臨時或緊急帳號功能。	<p>符合性情況說明：</p> <input type="checkbox"/> 人工審核帳號之建立、修改、啟用、禁用、和刪除動作，並通知機關所屬之花之授權人員 <input type="checkbox"/> 普通系統會自動審核帳號之建立、修改、禁用、禁用、和刪除動作，並通知機關所屬之花之授權人員 <input type="checkbox"/> 其他： 不適用情況說明：	系統管理員備 註管理權限， 並依據不適用內部 相關業務人員備 註部份權限，人 員職權即予以停 用或刪除。				
2			已逾期之臨時或緊急帳號應即刪除或禁用。	V	<p>符合性情況說明：</p> <input type="checkbox"/> 人工選擇刪除或停用臨時和緊急帳號 <input type="checkbox"/> 普通系統會自動選擇刪除或停用臨時和緊急帳號 <input type="checkbox"/> 其他： 不適用情況說明：本系統無提供臨時或緊急帳號功能。	<p>符合性情況說明：</p> <input type="checkbox"/> 人工審核帳號之建立、修改、啟用、禁用、和刪除動作，並通知機關所屬之花之授權人員 <input type="checkbox"/> 普通系統會自動審核帳號之建立、修改、禁用、禁用、和刪除動作，並通知機關所屬之花之授權人員 <input type="checkbox"/> 其他： 不適用情況說明：							
3			登記帳號應最後登入時間，可透過工作稽核，檢查是否有待候一超時間(如半年等)未登入系統之帳號，並實作自動停用該帳號之功能。	V	<p>符合性情況說明：</p> <input type="checkbox"/> 人工審核帳號之建立、修改、啟用、禁用、和刪除動作，並通知機關所屬之花之授權人員 <input type="checkbox"/> 普通系統會自動審核帳號之建立、修改、禁用、禁用、和刪除動作，並通知機關所屬之花之授權人員 <input type="checkbox"/> 其他： 不適用情況說明：	<p>符合性情況說明：</p> <input type="checkbox"/> 人工選擇刪除或停用臨時和緊急帳號 <input type="checkbox"/> 普通系統會自動選擇刪除或停用臨時和緊急帳號 <input type="checkbox"/> 其他： 不適用情況說明：本系統無提供臨時或緊急帳號功能。	<p>符合性情況說明：</p> <input type="checkbox"/> 人工審核帳號之建立、修改、啟用、禁用、和刪除動作，並通知機關所屬之花之授權人員 <input type="checkbox"/> 普通系統會自動審核帳號之建立、修改、禁用、禁用、和刪除動作，並通知機關所屬之花之授權人員 <input type="checkbox"/> 其他： 不適用情況說明：						
4			定期審核普通系統帳號之建立、修改、啟用及刪除。	V	<p>符合性情況說明：</p> <input type="checkbox"/> 人工選擇刪除或停用臨時和緊急帳號 <input type="checkbox"/> 普通系統會自動選擇刪除或停用臨時和緊急帳號 <input type="checkbox"/> 其他： 不適用情況說明：本系統無提供臨時或緊急帳號功能。	<p>符合性情況說明：</p> <input type="checkbox"/> 人工審核帳號之建立、修改、啟用、禁用、和刪除動作，並通知機關所屬之花之授權人員 <input type="checkbox"/> 普通系統會自動審核帳號之建立、修改、禁用、禁用、和刪除動作，並通知機關所屬之花之授權人員 <input type="checkbox"/> 其他： 不適用情況說明：	<p>符合性情況說明：</p> <input type="checkbox"/> 人工選擇刪除或停用臨時和緊急帳號 <input type="checkbox"/> 普通系統會自動選擇刪除或停用臨時和緊急帳號 <input type="checkbox"/> 其他： 不適用情況說明：本系統無提供臨時或緊急帳號功能。	<p>符合性情況說明：</p> <input type="checkbox"/> 人工審核帳號之建立、修改、啟用、禁用、和刪除動作，並通知機關所屬之花之授權人員 <input type="checkbox"/> 普通系統會自動審核帳號之建立、修改、禁用、禁用、和刪除動作，並通知機關所屬之花之授權人員 <input type="checkbox"/> 其他： 不適用情況說明：	定期由系統管理 員審核。				

資通系統防護基準控制措施檢查表

資通系統名稱：測繪成果圖冊管理系統

機密等級：普通 版本：VI.00 表單編號：ISMS-01170108

業務單位名稱： 實施日期： 年 月 日

實施系統安全等級： 高 中 低

項次	控制措施	控制方式(詳細內容請參閱資通安全責任管理分級辦法(附表十))	說明	符合性		符合性或不適用情況說明	預計改善作為	完成日期	備註
				符合	未完全符合				
5	最小權限	權限最小權限原則，僅允許使用者(或代表使用者)執行其必要之任務及業務功能，完成指派任務所需之權限存取。	使用者(或代表使用者)應以完成其工作所需之最小權限存取系統功能，避免過度授權而增加系統資源被不當存取之風險。因此在進行權限決定時，應考慮該使用者(或代表使用者)所能存取之系統功能及資料範圍，限制其所能存取之系統功能及資料。	V		符合性情況說明： <input type="checkbox"/> 已根據使用者之業務性質與範圍，明確核定其所能存取之系統功能及資料。 <input type="checkbox"/> 限制權限應基於機關規定之權限原則使用。 <input checked="" type="checkbox"/> 定期審查使用者角色及權限，並確認是否必要此權限。 <input type="checkbox"/> 其他： 不適用情況說明： <input type="checkbox"/> 其他： 符合性情況說明： <input checked="" type="checkbox"/> 已建立遠端存取申請表單之審核流程。 <input type="checkbox"/> 權限變更作業於伺服器端完成。 <input type="checkbox"/> 其他： 不適用情況說明： <input type="checkbox"/> 其他： 符合性情況說明： <input type="checkbox"/> 已建立遠端存取申請表單之審核流程。 <input type="checkbox"/> 權限變更作業於伺服器端完成。 <input type="checkbox"/> 其他： 不適用情況說明： <input type="checkbox"/> 其他：			由系統管理員依據相關人員性質，設定系統使用權限及功能。
6	遠端存取	對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制，如應需求，連線需求及文件化，使用者之權限應基於其業務需求於伺服器端完成。	機關應明確訂定資通系統之存取限制，如應需求、連線需求，並將這些資訊及評化，以限制遠端存取。應於伺服器端實施權限存取限制，並預設禁止任何未經過審核之存取行為，以避免被使用者繞過。	V		符合性情況說明： <input type="checkbox"/> 已建立遠端存取申請表單之審核流程。 <input type="checkbox"/> 權限變更作業於伺服器端完成。 <input type="checkbox"/> 其他： 不適用情況說明： <input type="checkbox"/> 其他： 符合性情況說明： <input type="checkbox"/> 已建立遠端存取申請表單之審核流程。 <input type="checkbox"/> 權限變更作業於伺服器端完成。 <input type="checkbox"/> 其他： 不適用情況說明： <input type="checkbox"/> 其他：			遠端存取應經核准後，由本中心機房管理。
7		應監控資通系統遠端連線。	資通系統所允許之遠端連線活動，應使用監控設備或其他可偵測未經授權使用的設備，本發現異常連線或存取行為時應提出警告，以防立資通系統被不當使用。	V		符合性情況說明： <input type="checkbox"/> 已監控資通系統遠端連線。 <input type="checkbox"/> 其他： 不適用情況說明： <input type="checkbox"/> 其他：			遠端存取應經核准後，由本中心機房管理。
8		資通系統應採用加密機制。	遠端存取資通系統時，應以加密機制保護機密資料傳輸之機密性。常見作法如採用HTTPS加密傳輸等，並選擇高強度之加密演算法。	V		符合性情況說明： <input type="checkbox"/> 已使用HTTPS加密。 <input type="checkbox"/> 已使用SSH加密。 <input type="checkbox"/> 已使用VPN加密。 <input type="checkbox"/> 已使用遠端桌面通訊協定(RDP)加密。 <input type="checkbox"/> 其他： 不適用情況說明： <input type="checkbox"/> 其他： 符合性情況說明： <input type="checkbox"/> 允許SSL協議。 <input type="checkbox"/> TLS1.0。 <input type="checkbox"/> 使用RC4、DES或3DES。 <input type="checkbox"/> 使用MD5或SHA-1。 於109年12月31日前加入SSL。			應開發儲存設備需採生外置之密碼、來源、IP位址、網卡位址，並限定存取點。
9		資通系統遠端存取之來源應為機關已預先定義及管理之存取控制點。	遠端存取行為應經過適當審核後方可放行，若有必要應先外部遠端存取之系統功能，應限制資通系統遠端存取之來源(如機器、網路位址等)，預先定義合法來源並進行管理，避免全面性開放存取。	V		符合性情況說明： <input checked="" type="checkbox"/> 遠端存取已預先定義合法來源並進行管理。 <input type="checkbox"/> 其他： 不適用情況說明： <input type="checkbox"/> 其他：			應開發儲存設備需採生外置之密碼、來源、IP位址、網卡位址，並限定存取點。

資通系統防護基準控制措施查檢表

資通系統名稱：測繪成果圖冊管理系統

資通系統安全等級：□高 ■中 □低

機密等級：普通 版本：VI.00 表單編號：ISMS-01170108

業務單位名稱：

實施日期： 年 月 日

項次	控制措施	控制方式(詳細內容請參閱資通安全責任管理辦法(附表十))	說明	符合性		符合性或不適用情況說明	預計改善作為	完成日期	備註
				符合	未完全符合				
10	稽核與稽核事件	依規定時間週期及紀錄留存政策，保留稽核紀錄。	應依機關規定之時間週期及紀錄留存政策，保留系統稽核紀錄(Audit Logs)，目的包含稽核除錯、行為調查、稽核取證及法規遵从等。	V		符合性情況說明： <input type="checkbox"/> 已建立系統稽核紀錄管理程序，文件名稱： <input type="checkbox"/> 系統稽核紀錄已依規定留存 一個月 <input type="checkbox"/> 其他：於系統中留存系統稽核紀錄。 不適用情況說明：			
11		確保資通系統所有稽核材料之功能，並決定應稽核之特定資源或系統事件。	資通系統應實作稽核材料之功能，如身分驗證存取、存取資源使用、重要行為、重要事件異動、功能錯誤及管理員行為等。	V		符合性情況說明： <input type="checkbox"/> 稽核身分驗證事件 <input type="checkbox"/> 稽核資源存取事件 <input type="checkbox"/> 稽核系統功能錯誤事件 <input type="checkbox"/> 其他：資料異動 不適用情況說明：			
12		應稽核資通系統其他管理者應能執行之各項功能。	系統管理者為資通系統內具有最高權限之帳號，對系統應具有足夠影響力，記錄所有管理者能執行之各項功能，有助於從新稽核系統行為及異常事件追查。	V		符合性情況說明： <input type="checkbox"/> 資通系統已留存特定事件之LOG(如：更改密碼、登入失敗等) <input type="checkbox"/> 其他： 不適用情況說明：			
13		應定期審查稽核事件。	機關應訂定稽核事件審查程序，由負責人員檢視稽核紀錄內容，以確認是否在預定期內發生重要之異常事件，如異常的行政行為、重大的系統錯誤等。	V		符合性情況說明： <input type="checkbox"/> 已定期審查稽核事件 <input type="checkbox"/> 其他： 不適用情況說明：			
14	稽核紀錄內容	資通系統產生之稽核紀錄應包含事件類別、發生時間、發生位置及任何與事件相關之使用者身分識別資訊，並採用單一日志紀錄機制，確保輸出格式之一致性。	稽核紀錄應詳細描述所觸發的事件，包含：人、事、時、地、物等稽核資訊，宜包含：使用者帳號(避免用實名)、時間、執行之功能或存取之資源名稱、事件類型或發生等級、執行系統或事件描述、事件發生當下相關物件資訊、網路來源與目的地址，以及稽核代碼等。應可能採用單一日志機制，如同一句限稽核應產出相同格式之稽核紀錄等，以便於事件比對與追查。	V		符合性情況說明： <input type="checkbox"/> 事件類型 <input type="checkbox"/> 發生時間 <input type="checkbox"/> 發生位置 <input type="checkbox"/> 使用者身分識別 <input type="checkbox"/> 採用單一日志紀錄機制 <input type="checkbox"/> 其他： 不適用情況說明：			

資通系統防護基準控制措施查檢表

資通系統名稱：測繪成果圖冊管理系統
 機密等級：普通 版本：VI.00 表單編號：ISMS-01170108

項次	控制領域	控制措施	控制方式(詳細內容請參閱資通安全責任管理分級辦法(附表十))	說明	符合性		符合性或不適用情況說明	預計改善作為	完成日期	備註
					符合	未完全符合				
15			資通系統產生之稽核紀錄，應依需求納入其他相關資訊。	稽核紀錄應依法規政策或業務使用需求，納入其他相關資訊，如憑證資訊、稽核紀錄層級、會經識別碼等。	V		符合性情況說明： <input checked="" type="checkbox"/> 稽核紀錄已納入所有資訊 <input type="checkbox"/> 其他： 不適用情況說明：			
16		稽核儲存容量	依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量。	資通系統應配置稽核紀錄所需之儲存容量(如磁碟或資料應空間等)，避免因儲存容量不足造成稽核處理失敗。	V		符合性情況說明： <input checked="" type="checkbox"/> 稽核紀錄儲存需求，資料庫 <input type="checkbox"/> 儲存位置可用容量符合強行二月的要求 <input checked="" type="checkbox"/> 其他：由本中心機房配置併常備儲存容量。 不適用情況說明：			
17		稽核處理失敗之因應	資通系統應在稽核處理失敗時，應採取適當之行動。	稽核處理失敗時，應訂定稽核處理的處理措施(如提高警報的精確紀錄、停止產生稽核紀錄或對特定人員提出警告等)，避免警報系統可用性，或是當資安事件發生時無稽核紀錄可比對異常之情況。	V		符合性情況說明： <input type="checkbox"/> 稽核紀錄容量已隨時採置有最舊紀錄方式因應 <input type="checkbox"/> 稽核紀錄容量已隨時採停止紀錄方式因應 <input type="checkbox"/> 稽核紀錄容量已隨時採停止管理系統故障排除之方式因應 <input checked="" type="checkbox"/> 其他： 不適用情況說明：			
18		時戳及校時	資通系統應採用系統內部時鐘產生稽核紀錄所需時戳，並可以對應到世界協同時間(UTC)或格林威治標準時間(GMT)。	使用系統內部時鐘產生稽核紀錄所需時戳，採用系統一致的時間標準，有助於確保資安事件所發生的各種事件時間點，進而分析資安事件可能發生的原因。	V		符合性情況說明： <input checked="" type="checkbox"/> 與外部標準時間自動校時 <input type="checkbox"/> 與外部標準時間手動校時 <input type="checkbox"/> 其他： 不適用情況說明：			
19			系統內部時鐘應依機關規定之時間週期與基準時間源進行同步。	稽核紀錄必須於使用前預留的時間，以初事件追蹤及稽核狀態運用後，實務上，可使用網路時間協定(Network Time Protocol, NTP)，讓機關內各個系統能與網路設備與校時伺服器進行同步，如國家標準時間伺服器(Time.sttime.gov.tw)或按月與國自建之伺服器。	V		符合性情況說明： <input checked="" type="checkbox"/> 已依規定之時間週期與基準時間源進行同步 <input type="checkbox"/> 其他： 不適用情況說明：			

資通系統名稱：測繪成果圖冊管理系統		業務單位名稱：		審核日期： 年 月 日		本實施或未完實施之預計改善方式	
資通系統安全等級：□ 高 ■ 中 □ 低		符合性		符合性或不適用情況說明		預計改善作為	
項次	控制措施	符合	未完全符合	不符合			備註
20	稽核資訊之保護	V			符合性情況說明： <input type="checkbox"/> 已指定主管、知密 <input type="checkbox"/> 已指定非系統管理人員 <input checked="" type="checkbox"/> 其他：指定系統管理人員 不適用情況說明：		
21	稽核資訊之存取管理，僅限於有權限之使用者。	V			符合性情況說明： <input type="checkbox"/> 已提供稽核資訊之副本 <input checked="" type="checkbox"/> 其他：於109年12月31前 不適用情況說明：	於109年12月31前 理	
22	訂定系統可容忍資料損失之時間要求	V			符合性情況說明： <input type="checkbox"/> 已從災備團可容忍資料損失之時間： 二小時 <input checked="" type="checkbox"/> 其他：依本中心機房統一辦理系統備 份相關規定。 不適用情況說明：		
23	執行系統源碼資料備份。	V			符合性情況說明： <input type="checkbox"/> 已執行系統源碼資料備份 <input checked="" type="checkbox"/> 其他：由本中心機房統一備份管理 不適用情況說明：		
24	應定期測試備份資訊，以驗證備份媒體之可讀性及資料之完整性。	V			符合性情況說明： <input type="checkbox"/> 系統房均碼及資料均已備份；定期每 隔二小時 <input checked="" type="checkbox"/> 其他：由本中心機房統一備份管理 不適用情況說明：		
25	系統備援	V			符合性情況說明： <input checked="" type="checkbox"/> 已訂定資通系統之可容忍時間要求 <input type="checkbox"/> 其他： 不適用情況說明：		

資通系統防衛基準控制措施檢查表

機密等級：普通 版本：VI.00 表單編號：ISMS-01170108

實施系統名稱：測繪成果圖冊管理系統

實施系統安全等級：□高 ■中 □低

業務單位名稱： 審核日期： 年 月 日

項次	控制措施	控制方式(詳細內容請參閱實施安全責任管理辦法(附表十))	說明	符合性		符合性或不適用情況說明	預計改善作為	完成日期	備註
				符合	未完全符合				
26		常服務中斷時，亦可容忍時間內，由備援設備代理提供服務。	機關應準備適當及足夠的備援設備，以確保發生災害時，可於所訂定之容忍時間內恢復回復正常運作。		V	符合性情況說明： <input type="checkbox"/> 已由備援設備代理提供服務 <input type="checkbox"/> 其他： 不適用情況說明：	納入本中心備援規劃，依實際需要，擬納入招標文件工作事項	111.12.31	
27	內部使用者之使用者之識別與鑑別	實施系統應具備唯一識別及鑑別機關使用者之功能，如雙重認證(Active Directory)並多人共用同一個帳號登入系統，則難以收稽核紀錄識別個別使用者身分。		V		符合性情況說明： <input checked="" type="checkbox"/> 均有個別帳號，未者共用帳號 <input type="checkbox"/> 其他： 不適用情況說明：			
28	身分驗證管理	使用預設密碼登入系統時，應於登入後要求立即變更密碼。	使用者註冊時應由營運系統或人工配發預設密碼者，於使用者首次登入時，應強制其變更預設密碼。		V	符合性情況說明： <input type="checkbox"/> 首次登入均要求立即更換預設密碼 <input type="checkbox"/> 其他： 不適用情況說明：無預設密碼功能，帳號及密碼隨本中心AD管理資料異動或變更。			網頁認證防範，帳號及密碼隨本中心AD管理資料異動或變更。
29		身分驗證相關資訊不以明文傳輸。	系統傳輸身分驗證相關資訊(如帳號密碼等)時，採內加密傳輸可防止機敏資訊外洩之風險。		V	符合性情況說明： <input type="checkbox"/> 已使用HTTPS或SSH加密 <input type="checkbox"/> 已將身分驗證資訊加密或編碼後傳輸 <input type="checkbox"/> 其他： 不適用情況說明：	於109年工作案加入SSLv3	109年12月31前	<input type="checkbox"/> 允許SSLv3或TLSv1.0 <input type="checkbox"/> 使用RC4、DES或3DES <input type="checkbox"/> 使用MD5或SHA-1
30		具備用戶鎖定機制，帳號登入連續三次失敗後，至少十五分鐘內不允許該帳號繼續嘗試登入或使月機關自建之失敗驗證機制。	系統應實作帳戶鎖定機制，並建議以電子郵件通知使用者，於鎖定期間禁止該帳號所有登入嘗試，超過鎖定時間重新計次。		V	符合性情況說明： <input type="checkbox"/> 已設定帳號登入失敗達三次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使月機關自建之失敗驗證機制 <input type="checkbox"/> 其他： 不適用情況說明：	於109年工作案加入本局帳號及鎖死機制	109年12月31前	本系統尚未採行聯署登入員使用，無外部人員登入情形。

資通系統防護基準控制措施查檢表

機密等級：普通 版次：VI.00 表單編號：ISMS-01170108

實施系統名稱：測繪成果圖冊管理系統		實施系統安全等級： <input type="checkbox"/> 高 <input checked="" type="checkbox"/> 中 <input type="checkbox"/> 低		業務單位名稱：		實施日期： 年 月 日		本實施或未完符合之預計改善方式	
項次	控制措施	控制方式(詳細內容請參閱實施安全責任管理辦法(附表十))	說明	符合性		符合性或不適用情況說明	預計改善作為	完成日期	備註
				符合	未完全符合				
31		應強制最低密碼複雜度，包含密碼長度限制及組成字元種類，目的在避免因使用安全性不足之密碼而被人輕易破解。強制密碼最短限制，而於短期內頻繁更換密碼後又改用原密碼。強制密碼，實務上，可參考政府認證使用同一組密碼。實務上，可參考政府認證基準(Government Configuration Baseline, GCB)之建議值，設定密碼複雜度及密碼使用效期限制。	應強制最低密碼複雜度，包含密碼長度限制及組成字元種類，目的在避免因使用安全性不足之密碼而被人輕易破解。強制密碼最短限制，而於短期內頻繁更換密碼後又改用原密碼。強制密碼，實務上，可參考政府認證使用同一組密碼。實務上，可參考政府認證基準(Government Configuration Baseline, GCB)之建議值，設定密碼複雜度及密碼使用效期限制。			符合性情況說明： <input type="checkbox"/> 已強制密碼最短效期____天 <input type="checkbox"/> 已強制密碼最長效期____天 <input type="checkbox"/> 其他： 不適用情況說明：密碼及複雜度等規則隨本中心AD管理資料庫異動而變更。			密碼及複雜度等規則隨本中心AD管理資料庫異動而變更。
32		使用者更換密碼時，至少不可以與前三次使用過之密碼相同。(非內部使用者，可依機關自行規範辦理)	使用者更換密碼時(以傳統傳統式)，於設定新密碼時，比對新密碼與舊密碼之複雜度，若新密碼與舊密碼比對密碼一致。			符合性情況說明： <input type="checkbox"/> 已設定更換密碼時，至少不可以與前三次使用過之密碼相同 <input type="checkbox"/> 其他： 不適用情況說明：密碼及複雜度等規則隨本中心AD管理資料庫異動而變更。			密碼及複雜度等規則隨本中心AD管理資料庫異動而變更。
33		身分驗證機制應防範自動化程式之登入或密碼更換嘗試。	系統於使用帳號密碼進行身分驗證，非僅可避免受到自動化程式以暴力破解方式嘗試登入。如運用驗證碼(CAPTCHA)為常見之防範方式，透過驗證碼以圖形方式呈現於畫面上，並要求使用者辨別圖形中文字之方式，或以其他足以辨別人為動作之方式(如勾選「我非機器」等)，防堵自動化程式之嘗試行為。		V	符合性情況說明： <input type="checkbox"/> 已使用CAPTCHA機制 <input type="checkbox"/> 其他： 不適用情況說明：	將於109年度工作案加入圖形驗證或驗證碼機制	109年12月31前	

資通系統防範基準控制措施查檢表

資通系統名稱：測繪成果圖冊管理系統

機密等級：普通 版本：VI.00 表單編號：ISMS-01170108

實施單位名稱： 實施日期： 年 月 日

實施安全等級：□普 ■中 □高

項次	控制措施	控制方式(詳細內容請參閱資通安全責任等級分級辦法(附表十))	說明	符合性		符合性或不適用情況說明	預計改善作為	完成日期	備註
				符合	未完全符合				
34		密碼重設機制對使用者重新身分確認後，發送一次性及具有可效性符記。	密碼重設機制設計不良可能造成安全問題。常見弱點是系統自行產生隨機密碼後以電子郵件寄送給使用者，此問題在於無法確保密碼通過網路加密保護，脫離高資安風險。使用者忘記密碼或密碼遺失時，應以郵件或手機號碼等，先要求使用者輸入該密碼，此問題在於密碼無效後，發送一次性及具有可效性符記(如資訊驗證碼、電子郵件驗證碼等)。使用者按此符記能即時進行輸入密碼驗證。系統檢查回傳符記之有效性後，才允許使用者進行資訊密碼操作。	符合	未完全符合	符合性情況說明： <input type="checkbox"/> 密碼EMAIL驗證連結 <input type="checkbox"/> 發送驗證碼 <input type="checkbox"/> 其他： 不適用情況說明：密碼重設由本中心ID管理資料庫自動變更。			密碼重設由本中心AD管理資料庫自動變更。
35	個別資訊回饋	資通系統應透過軟體別過報中之資訊。	資通系統身分識別頁面中，資料輸入欄位(如密碼等)應以明文顯示方式，如以*取代真實輸入字元，以避免他人窺視而竊取密碼。	符合	未完全符合	符合性情況說明： <input type="checkbox"/> 使用者輸入之密碼採隱碼方式保護 <input checked="" type="checkbox"/> 使用者輸入之密碼採隱碼方式保護 <input type="checkbox"/> 其他： 不適用情況說明：			
36	加密與解碼	資通系統如以密碼進行儲存時，該密碼應加密或加密處理後儲存。	密碼不可以明文方式儲存，應經過加密或加密處理，使資訊管理系統或惡意入侵者攻擊者皆無法輕易取得使用者密碼，以確保密碼外洩風險。實務上，當使用者設定密碼時，應針對管理系統產生一個亂數值(Salt)，將密碼結合亂數值，再以雜湊函式進行雜湊及生成密碼值。應針對不同欄位儲存亂數值及密碼值。後續使用者輸入密碼時，以輸入值添加當初設定密碼時產生的亂數，再次以雜湊函式處理，若產生與當初設定密碼相同的雜湊值，則表示輸入密碼正確。	符合	未完全符合	符合性情況說明： <input type="checkbox"/> 已使用密碼加密儲存 <input checked="" type="checkbox"/> 已使用密碼加密儲存 <input type="checkbox"/> 其他： 不適用情況說明：			
37	非內部使用者之識別與鑑別	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之單件)。	資通系統應開放給外部使用者(含其他機關、委外開發與維護廠商、服務人員及一般民眾等)存取使用，應具備識別及鑑別之能力，如利用帳號、密碼或來源IP位址等方式，識別與鑑別使用者。	符合	未完全符合	符合性情況說明： <input type="checkbox"/> 已具備身分驗證機制 <input type="checkbox"/> 其他： 不適用情況說明：無開放外部使用者			

資通系統防護基準控制措施查檢表

資通系統名稱：測繪成果圖冊管理系統

機密等級：普通 版次：VI.00 表單編號：ISMS-01170108

實施單位名稱： 實施日期： 年 月 日

項次	控制措施	控制方式(詳細內容請參閱實施辦法(附表十))	說明	符合性		符合性或不適用情況說明	預計改善作為	完成日期	備註
				符合	未完全符合				
38	系統與服務獲得	系統發展生命週期需求階段	針對系統安全需求(含機密性、可用性、完整性)，以繼續表方式進行確認。	V		符合性情況說明： <input type="checkbox"/> 系統發展需求階段已識別系統安全需求 <input checked="" type="checkbox"/> 已通過檢核表方式進行確認 <input type="checkbox"/> 其他： 不適用情況說明：			系統開發與測試 包括信息安全檢閱 報告等成果
39	系統發展生命週期設計階段	根據系統功能與要求，識別可能影響系統之威脅，進行風險分析與評估。	可依照下列平面向進行分析與評估：「安全設計原則」，進行系統設計時應參考使用之設計原則；「執行政策面分析」，進行政策面的定義、識別與對照方式，包含如何進行政策面的衡量與評估，並進行管理；「執行風險的衡量與評估」，根據設計過程中，如何透過使用威脅建模與結構化風險分析，進行系統發展與威脅的分析，並使用相同性的部分設計原則與控制措施，提供軟體安全風險分析與控制；「安全設計審查」，在進行一連串安全軟體設計的實施活動之後，應確保安全設計符合需求所提出的相關安全需求及安全設計，以符合軟體安全的基本準則。	V		符合性情況說明： <input checked="" type="checkbox"/> 已根據系統功能與要求，進行風險分析與評估。 <input type="checkbox"/> 其他： 不適用情況說明：			系統開發時所針對 常見風險與 發掘之評估表
40		將風險評估結果回饋需求階段的檢核項目，並提出安全需求修正。	系統發展生命週期需求階段發展之安全需求與檢核項目，可能未能充分符合系統之所有安全需求，故應從風險評估結果進行修正。	V		符合性情況說明： <input type="checkbox"/> 已將風險評估結果，提出安全需求修正。 <input type="checkbox"/> 其他： 不適用情況說明：			
41	系統發展生命週期開發階段	應針對安全需求與實作必要控制措施。	應於系統開發階段，針對安全需求實作必要之控制措施，輔以檢核表方式進行確認，可減少遺漏之可能。	V		符合性情況說明： <input type="checkbox"/> 已依安全需求表進行必要控制措施 <input checked="" type="checkbox"/> 已透過工具避免軟體開發錯誤 <input type="checkbox"/> 其他： 不適用情況說明：			
42		應注意避免軟體常見漏洞及實作必要控制措施。	軟體開發時應參考常見漏洞，如OWASP TOP 10或CVE/SANS TOP 25等，這些漏洞容易疏忽攻擊者利用，造成系統破壞、資訊洩漏或軟體無法運作，故實作必要控制措施，以零低資安風險。	V		符合性情況說明： <input type="checkbox"/> 已從漏洞軟體常見漏洞 <input checked="" type="checkbox"/> 已從漏洞進行必要控制措施 <input type="checkbox"/> 其他： 不適用情況說明：			

資通系統防護基準控制措施查檢表

資通系統名稱：測繪成果圖冊管理系統

機密等級：普通 版本：VI.00 表單編號：ISMS-01170108

實施單位名稱： 實施日期： 年 月 日

實施系統安全等級： 高 中 低

項次	控制措施	控制方式(詳細內容請參閱「實施安全責任管理分級辦法」附表十)	說明	符合性		符合性或不適用情況說明	預計改善作為	完成日期	備註
				符合	未完全符合				
43		發生錯誤時，使用者頁面上應顯示錯誤錯誤訊息及代碼，不包含詳細之錯誤訊息。	系統為設計錯誤處理機制，當系統發生錯誤時，應可能採取錯誤代碼或錯誤訊息呈現，避免將詳細或敏感資訊顯示於使用者頁面，或根據錯誤訊息推測出系統可能之弱點。確保系統所有功能的程式碼，在程式的拋入點之後，儘可能從用程式碼的try-catch陳述，捕捉可能發生的錯誤與例外狀況。另外，採用程式碼的finally陳述，確保該段功能程式碼所使用的資源正確釋放。	V		<p>符合性情況說明：</p> <input checked="" type="checkbox"/> 已設定頁面僅顯示簡短錯誤訊息及代碼 <input type="checkbox"/> 已設定頁面不顯示詳細之錯誤訊息 <input type="checkbox"/> 其他： <p>不適用情況說明：</p>			
44	系統發展生命週期測試階段	執行「弱點掃描」安全檢測。	弱點掃描係利用自動化工具，對受測目標進行安全性掃描，以找出系統潛在弱點。	V		<p>符合性情況說明：</p> <input type="checkbox"/> 定期每月執行普通系統弱點掃描 <input checked="" type="checkbox"/> 其他：弱點掃描同時進行弱點掃描 <p>不適用情況說明：</p>			
45	系統發展生命週期部署與維護階段	於部署階段應針對相關管理安全威脅，進行更新與修補，並關閉不必要服務及埠口。	操作系統或平台之安全更新，定期評估、測試與更新。系統上所有操作系統或平台皆須定期更新服務埠口(Services)進行安全評估，正面列出需要關閉服務埠口之理由，並關閉不必要之項目。	V		<p>符合性情況說明：</p> <input checked="" type="checkbox"/> 弱點掃描結果高風險已進行修補 <input type="checkbox"/> 系統重大修補已更新 <input type="checkbox"/> 其他： <p>不適用情況說明：</p>			
46		普通系統相關軟體，不使用預設密碼。	系統相關軟體元件或組態設定若使用預設密碼，應於系統正式上線前變更完畢。	V		<p>符合性情況說明：</p> <input checked="" type="checkbox"/> 已無使用預設密碼 <input type="checkbox"/> 其他： <p>不適用情況說明：</p>			
47		於系統發展生命週期之維護階段，須注意版本控制與變更管理。	在維護階段可能因需求變更、系統除錯、功能構建等原因而需要變更系統狀態，而版本控制之目的，即在記錄系統狀態在某段時間內之變更行為，使得使用者在需要時可取回特定的版本。維護的版本控制與變更管理可強化系統的安全性與可用性。	V		<p>符合性情況說明：</p> <input checked="" type="checkbox"/> 已設定變更管理並進行版本控制 <input type="checkbox"/> 其他： <p>不適用情況說明：</p>		109年工作案號加入版本控制功能	109年12月31前

資通系統防護基準控制措施查檢表

資通系統名稱：測繪成果圖冊管理系統

機密等級：普通 版本：VI.00 表單編號：ISMS-01170108

實施單位名稱： 實施日期： 年 月 日

實施系統安全等級： 高 中 低

項次	控制措施	控制方式(詳細內容請參閱實施安全責任管理辦法(附表十))	說明	符合性		符合性或不適用情況說明	預計改善作為	完成日期	備註
				符合	未完全符合				
48	系統發展生命週期至外階段	系統發展生命週期至外階段，應將系統發展生命週期各階段依等級安全需求(含機密性、可用性、完整性)納入安全策略。	機關委外開發普通系統時，可參考本文件之內容，並在標不同之安全等級(高、中、低)制定適用之安全需求，明確納入委外契約以做為驗收時之依據。	V		符合性情況說明： <input type="checkbox"/> 已將系統安全需求之檢驗項目納入委外契約 <input type="checkbox"/> 其他： 不適用情況說明：	100年工作案已將本文件檢視及製作列為工作項目。	100年12月31前	
49	操作程序	開發、測試以及正式作業環境應為區隔。	開發環境、測試環境與正式作業環境可區隔或不同的位階及網段，應於可能存取的使用程式及資料庫，以保護正式作業環境系統及資料。實務上，開發人員常以本機電腦為開發環境，並透過使用本機端之資料進行測試與測試主機，係開發人員將測試用程式部署人員進行測試使用。應測試完畢，再將測試用程式部署至正式環境，並建議至正式資料庫提供上線服務。	V		符合性情況說明： <input checked="" type="checkbox"/> 已將開發、測試以及正式作業環境進行區隔 <input type="checkbox"/> 其他： 不適用情況說明：			
50	系統文件	應儲存與管理系統發展生命週期之相關文件。	系統發展生命週期之相關文件如系統需求書、系統規格書、系統發展計畫、系統測試計畫及測試報告等，應書面或電子化形成並行文件保存，並歸納入管理程序。	V		符合性情況說明： <input checked="" type="checkbox"/> 已留存系統發展生命週期之相關文件 <input checked="" type="checkbox"/> 已留存系統設計與開發階段之文件 <input checked="" type="checkbox"/> 已留存系統測試與開發階段之文件 <input checked="" type="checkbox"/> 已留存系統部署與維護階段之文件 <input type="checkbox"/> 其他： 不適用情況說明：			
51	系統恢復性	系統之漏洩修復應測試其有效性及潛在影響，並定期更新。	針對系統所使用的外部元件軟體進行表列，包含其版本管理，定期關注元件版本更新訊息及安全公告漏洞通告，若有相關之安全漏洞評估系統元件更新之必要性，並於系統測試環境進行更新測試無虞後，才於正式環境進行更新。	V		符合性情況說明： <input checked="" type="checkbox"/> 定期在一個月內執行系統漏洩修復 <input type="checkbox"/> 其他： 不適用情況說明：			本中心已辦理漏洩修復，並將漏洩修復通知系統管理員，請廠商修復。
52		定期確認資訊系統相關漏洩修復之狀態。	注意相關之安全漏洩訊息(透過CIE 相關訊息網站、簡訊安全通告等)，若發現使用之軟體或元件存在安全漏洞，應以修復漏洩並定期確認修復後之狀態。	V		符合性情況說明： <input checked="" type="checkbox"/> 已定期確認系統漏洩修復之狀態 <input type="checkbox"/> 其他： 不適用情況說明：			

資通系統名稱：測繪成果圖冊管理系統		業務單位名稱：		審核日期： 年 月 日		本實施或未完符合之預計改善方式		
項次	控制措施	控制方式(詳細內容請參閱資通安全責任管理辦法(附表十))	說明	符合性		符合性或不符合情況說明	預計改善作為	備註
				符合	不符合			
53	普通系統監控	發現普通系統有被入侵跡象時，應通報相關部門人員處理。	機房運送人員應處理普通系統被入侵跡象，並向系統管理人員提出警告。	V		符合性情況說明： <input type="checkbox"/> 已建立通報與應變管理程序，文件名： <input type="checkbox"/> 已建立受理通報處理流程 <input type="checkbox"/> 已留存通報之相關紀錄 <input type="checkbox"/> 其他： 不適用情況說明：		
54		監控普通系統，以偵測攻擊與未授權之連線，並識別普通系統之未授權使用。	機關應具備監控普通系統之能力，如指派專業人員或使用監控設備，用以偵測普通系統連線行為，當發現未授權之連線或存取行為應向系統管理人員提出警告。	V		符合性情況說明： <input type="checkbox"/> 已使用監控系統 <input type="checkbox"/> 其他： 不適用情況說明：		
55	軟體及資訊完整性	使用完整性驗證工具，以偵測未經授權變更軟體及資訊。	提供完整性驗證工具以偵測軟體或資訊在儲存或傳輸過程中未經人員惡意更改，如網站可產生之檔案值，並說明使用的辦法與演算法為何，以使用者取用資料後進行計算排異進行比較。另外，為確保系統程式之完整性，可對系統程式進行驗證，並進行完整性比對，以偵測未經授權之惡意變更。	V		符合性情況說明： <input type="checkbox"/> 已使用完整性驗證工具 <input checked="" type="checkbox"/> 其他：系統主機裝於ID7已導入ID7防護機制 不適用情況說明：		
56		使用者輸入資料合法性檢查應置放於應用系統伺服器端。	對於使用者輸入資料位元資料位元是否合預期之邏輯規則，實務上，以此表示式 (Regular Expression) 驗證內容之合法性，檢查機制若於客戶端實作，容易被使用者端偽造資料，故應於應用系統伺服器端實作處理為有效。	V		符合性情況說明： <input checked="" type="checkbox"/> 已檢查資料合法性 <input type="checkbox"/> 已實作於系統伺服器端 <input type="checkbox"/> 其他： 不適用情況說明：		可指定內容欄位應用以下程式選擇輸入，若欄位位元不符合輸入台法性，則系統不予儲存。
57		發現違反完整性時，普通系統應實施機關指定之安全保護措施。	機關應訂定相關安全保護措施，在發現普通系統完整性違反時應採取適當之行動。如需發現資料完整性違反時，應通知系統管理人員進行緊急應變處理，並依規定之通報流程進行安全事件通報作業。	V		符合性情況說明： <input checked="" type="checkbox"/> 已訂定相關安全保護措施 <input type="checkbox"/> 其他： 不適用情況說明：		欄位應以下列式選擇

四、作業計畫書審查意見

「109 年度測繪成果圖冊管理系統資料庫移轉採購案」 第 1 階段第 1 批成果（作業計畫） 審查意見

一、作業計畫書格式修正及文字誤繕：

1. 封面請依契約所定格式製作：
 - (1) 本成果為「作業計畫」非「作業計劃報告」。
 - (2) 計畫名稱請依規定英譯（建議：Database Conversion of Surveying and Mapping Results Management System in 2019）。
 - (3) 內封面作業名稱錯誤。
2. 目錄：
 - (1) 目錄與內文之頁碼請分別編定。
 - (2) 目錄之字體請統一；章節順序之標示請檢視是否有誤；部份章節名稱為「表」或「清單」者建議列於圖、表目錄。
3. 內文格式修正及文字誤植：
 - (1) P3~P4「二、現況描述」項下之階層亦以一、二…表示，請修正為（一）、（二）…。
 - (2) P10 請修正（五）2. …測試「腳」本。
 - (3) P15 請修正「（一）各階段繳交…如表 4 所示：」及「表 4 專案時程規劃表」之文字格式。
 - (4) 內文附圖說明文字與附圖編定序號不一致「P17. 肆一…開發計劃圖如圖 17 所示」，「P19. …開放程序（如圖 18 所示）…」，「P21. …離型策略（如圖 19 所示）…」。
 - (5) P23. 肆、「1. …Unicode 編號。」，「3. …登入（雙重認證）」，「5. …需標示醒目文字…」，「6. …列在作業計劃文件…結果列在工作總報告書文件內。」。
4. 電子檔之檔名（作業名稱錯誤），且遺漏 odt 格式文件。

二、作業計畫書修正意見：

1. 已於前言將本中心簡稱為「機關」，後續各章節敘述即以「機關」作為代稱即可；而本計畫應以承辦廠商之角色語氣撰寫。
2. P8 所提資料庫移轉作業方式，將資料庫傳送至外部環境，是否僅為測試用途，而未來將於何環境進行移轉作業，請說明。
3. P8 所提資料庫移轉後，將以人工處理異常情形，並以程式比對移轉前後資料庫，請說明以何程式比對，比對結果是否有報表佐證資料庫差異情形，請說明。
4. P8 系統上線方式，是否為原系統測試期間仍正常營運供使用者登載資料；原系統及原資料庫切換至新系統及新資料庫需花費多少時間，是否有需暫停系統使用情形，請說明。
5. P9 二、系統調校（一）1. 所列為本中心目前暫定之環境配置。
6. P9 本中心現有 2 部手持式 RFID 讀取器，其 APP 更新方式為何，需費時多久？是否有暫停作業之需要？
7. P9 本系配合導入 GCB 之作業，倘有無法套用之項目，請於期末成果表列之並加註說明或建議。
8. P10 以資安自動化測試工具 Vega 產生之報告是否可對應並轉換至本中心「資安防護基準作業報告」之項目及格式。
9. P12 請略述資料庫盤點之各資料表型態、欄位、用途說明等項目。
10. P12 請依契約工作項目二（一）提出系統功能盤結果。
11. P14 專案時程規劃甘特圖請配合本案各階段時程標示較明確作業期程；需求訪談及作業計畫應同為第 1 階段成果。
12. P17 專案時程規劃 1 節，應不需再敘本中心驗收方式。
13. P22 系統加強建議中，請先就本案目前作業內容提出建議，至於有關手持 RFID 讀取器升級及擴大管理財產等，可至期末報告再列於未來執行建議一節。
14. P22 需協助事項（一），MS Office Excel 是否為必要安裝之軟體，若是，是否有限定版本？
15. 請補充本案執行所配置之人力及分工架構。

五、 作業計畫書審查意見修正對照表

表 11 作業計畫書審查意見修正對照表

項次	格式修正及文字誤繕	處理修正情形
1	資料庫移轉作業方式，將資料庫傳送至外部環境，是否僅為測試用途，而未來將於何環境進行移轉作業，請補充說明。另請就資料傳送至外部測試環境後，資料存放保全及後續銷毀規劃辦理情形說明之。	已修正，補充說明作業方法、流程及資料管制銷毀措施。(P5、P6)
2	資料庫移轉後，將以人工處理異常情形，並以程式比對移轉前後資料庫，請說明以何程式比對，比對結果是否有報表佐證資料庫差異情形。	已修正。(P6)
3	請補充說明系統上線方式，是否為原系統測試期間仍可正常營運供使用者登載資料；原系統及原資料庫切換至新系統及新資料庫需花費多少時間，是否有需暫停系統使用情形。	已修正。(P6)
4	二、系統調校(一)1.所列為本中心目前暫定之環境配置。另請針對本系統調校列出規畫辦理之方式(如作業系統變動，程式碼需配合轉換；資料庫移轉，系統相關語法	已修正，概述本案系統配合辦理方式。(P7)

	需改寫等)。	
5	本中心現有 2 部手持式 RFID 讀取器，請說明其 APP 更新方式為何，需費時多久？是否有暫停作業之需要？	已修正。(P7)
6	本系統配合導入 GCB 之作業，倘有無法套用之項目，應表列說明或建議，另請說明套用 GCB 規劃情形。	已修正，補充說明 GCB 套用種類及方式。(P8、P9)
7	P10 請說明以資安自動化測試工具 Vega 產生之報告是否可對應並轉換至本中心「資安防護基準作業報告」之項目及格式。	已修正。(P9 ~ P11)
8	P12 請增列資料庫盤點之各資料表型態、欄位、用途說明等項目。另亦請依契約工作項目二(一)增列系統功能盤結果。	已修正。(P12、P13)

9	<p>P14 專案時程規劃甘特圖請配合本案各階段時程標示較明確作業期程及增列系統調校及資料庫移轉相關工作期程（皆標示規劃期程及實際辦理時程）；需求訪談及作業計畫應同為第1階段成果。另請於適當章節補充本案執行所配置之人力及分工架構。</p>	<p>已修正。 重新製作甘特圖及更新相關說明(P21、P22)。 補充專案執行人力說明及分工架構圖(P27、P28)</p>
10	<p>P22 系統加強建議1節，於有關手持RFID讀取器升級及擴大管理財產等，可至工作總報告再列於未來執行建議一節。需協助事項（一），請說明MS Office Excel是否為必要安裝之軟體？用途為何？是否有限定版本？</p>	<p>已修正。(P29)</p>
項次	修正意見	處理修正情形
1	<p>封面請依契約所定格式製作： (1) 請將封面之「作業計畫」修正為「作業計劃報告」。 (2) 計畫名稱請依契約規定予以英譯(建議:Database Conversion of Surveying and Mapping Results Management System in 2020)。 (3) 內封面作業名稱錯誤，請修正。</p>	<p>已修正。</p>

2	<p>目錄：</p> <p>(1) 目錄與內文之頁碼請分別編定（目錄編定羅馬數字 I、II……，內文編定阿拉伯數字 1、2……）。</p> <p>(2) 目錄之字體請統一；部份章節順序標示有誤，且章節名稱不宜包含「表」或「清單」。</p>	已修正
3	<p>內文格式修正及文字誤植：</p> <p>(1) 已於前言將本中心簡稱為「機關」，後續各章節敘述即以「機關」作為代稱即可；而本計畫應以執行單位之角色語氣撰寫。</p> <p>(2) P3~P4「二、現況描述」項下之項目階層編號請修正為（一）、（二）……。</p> <p>(3) P10 請修正(五)2. ……測試「腳」本。</p> <p>(4) P15「(一) 各階段繳交……如表 4 所示：」及「表 4 專案時程規劃表」之文字格式請修正與內文一致。</p> <p>(5) P17 專案時程規劃 1 節，履約功目核算及驗收為本中心權責，執行單位不需再述。</p> <p>(6) 內文附圖說明文字與附圖編定序號不一致「P17. 肆一……開發計畫圖如圖 <u>17</u> 所示」，「P19. ……開放程序（如圖 <u>18</u> 所示）……」，「P21. ……雛型策略（如圖 <u>19</u> 所示）……」。</p> <p>(7) P23. 需求訪談會議紀錄以下文</p>	已修正。

字誤植，請修正：

- 作業名稱應修正為「109 年度測繪成果圖冊管理系統資料庫移轉採購案」。
- 壹、時間 ……10:000 ~ 11:30
- 參、出席單位及人員：國土測繪中心：……李「佩」勳，請修正為李「佩」勳。
- 肆、「1. ……Unicode 編號。」，「3. ……登入（雙重證證）。」，「5. ……需標示警目文字……」，「6. ……列在作業計劃文件……」，「7. 工作總報告書加入系統……」。

(8) 本作業計畫電子檔之檔名錯誤（作業名稱錯誤）。

六、 期中報告書審查意見

內政部國土測繪中心

「109 年度擴充測繪成果圖冊管理系統採購」期中報告書

(含系統分析與系統設計文件、系統測試計畫)

審查意見

「109 年度測繪成果圖冊管理系統資料庫移轉採購案」

第 1 階段第 2 批成果審查意見

壹、修正意見

一、資訊系統開發計畫

1. 章節及內容請依本中心 ISMS 所訂項目 (ISMS-01170101) 調整修正，另「二、專案開發人力配置計畫」一節增述本案相關工作規劃辦理時程及說明，並將本節更名為「專案管理計畫」。
2. P1「一、文件目的」請補充說明本文件大綱及適用範圍。
3. P1「二、現況描述」請依現況補充說明系統功能相關描述。
4. P6「一、開發平臺環境」請補充說明伺服器開發語言 VB、網頁開發使用之 ASP.NET 及 JQuery 程式庫之版本為何？，另系統及盤點程式為相同開發工具 (Microsoft Visual Studio) 版本不同，請補說明原因為？

二、資訊系統需求規格

1. 章節及內容請依本中心 ISMS 所訂項目 (ISMS-01170102) 調整修正。
2. P3「表 1 系統軟硬體規格一覽表」內容請確認規格項目為原環境或新設環境。
3. P7「圖 4 系統架構與細部功能圖」與 P13「圖 5 系統項目介面設計」之功能項目有部份不同，請檢視修正；另請將「圖 4 系統架構與細部功能圖」請參照 P8「表 3 系統子功能清單」標示編號以利對照。
4. P13「參、系統項目介面設計」請補充說明文字。

三、資訊系統設計規格

1. 章節及內容請依本中心 ISMS 所訂項目 (ISMS-01170104) 調整修正。
2. P2「1.4 作業環境說明」之「(3) 字戶端瀏覽器」請補充

Google Chrome 版本要求。

3. P5「表 3 測繪成果圖冊資料管理系統軟體單元清單」請依上層功能架構將表格內之單元名稱區分排列。
4. P190「第 8 章」軟體項目介面設計」請補充文字說明及相關介面圖說。

四、系統測試計畫

1. 章節及內容請依本中心 ISMS 所訂項目 (ISMS-01170103) 調整修正。
2. P4「圖 3 本專案功能架構圖」中「C. 報表管理」—「C1. 基本資料表報」項下之「圖冊數量統計」，應列於「C3. 盤點作業報表」項下。「C. 盤點作業報表」項下應與系統實際項目相符。
3. P16 廠商測試環境中作業系統及資料庫版本與本中心環境不同，請確認是否為誤植及說明測試結果是否適用於本中心環境。
4. P17 所述測試方式為「單元測試」及「系統測試」，而計畫所附紀錄表單為「單元測試紀錄表」及「整合測試紀錄表」，請確認測試方試及表單之一致性。

貳、格式及文字修正

一、資訊系統開發計畫

1. P6「(二) 盤點程式 (手持機) ……以進行圖冊盤點 (抽查/清查) 作業」。請修正為「……盤點 (抽查/清查/清點) ……」。
2. P6「二、軟體發展方法……並經國土機關人員確認無誤後」; 文字請修正為「……並經機關確認無誤後」。

二、資訊系統需求規格

1. 目錄標示項目請檢視修正與內容章節名稱一致。
2. 圖目錄所列圖號與內文不符，請修正。
3. P5「五、參考文件」之最後一段文字及 P12 表格下方文字應為誤植，請修正。

4. P6 「一、系統概觀說明」內文與各圖表標示不同，請修正。

三、資訊系統設計規格

1. 內封面文件名稱下方不需再加註「(含程式清單……)」文字。

2. P7 「表 3 測繪成果圖冊資料管理系統軟體單元清單」文字應置於該表上方。

四、系統測試計畫

1. P18 「六、測試步驟」內文之粗體字，請確認有無表示特殊涵意。

2. P21 表 9 之專案名稱錯誤，請修正。

七、期中報告書審查意見修正對照表

表 12 期中報告書審查意見修正對照表

「測試計畫」內容修正對照		
項次	審查意見	處理修正情形
1	章節及內容請依本中心 ISMS 所訂項目 (ISMS-01170103) 調整修正。	已依貴中心 ISMS 所列章節調整，各章節對照如下： 文件目的 (P1)，名詞解釋 (P1)，參考文件資料 (P2)，需求確認 (P2)，功能設計驗證 (P3)，測試類別 (P3)，測試機制 (P3)，測試準則 (P4)，測試工作時程 (P5)，測試應交付文件 (P5)。
2	P4 「圖 3 本專案功能架構圖」中「C. 報表管理」—「C1. 基本資料表報」項下之「圖冊數量統計」，應列	依前項意見調整及修改相關章節，故該圖無使用必要已刪除；功能架構圖修正後亦可參閱本案「資訊系統需求規格」及「資訊系統設計規格」。

	於「C3. 盤點作業報表」項下。「C. 盤點作業報表」項下應與系統實際項目相符。	
3	P16 廠商測試環境中作業系統及資料庫版本與本中心環境不同，請確認是否為誤植及說明測試結果是否適用於本中心環境。	前為誤植，已修正(P3)
4	P17 所述測試方式為「單元測試」及「系統測試」，而計畫所附紀錄表單為「單元測試紀錄表」及「整合測試紀錄表」，請確認測試方試及表單之一致性。	已於 P6 及 P7 補充測試方及所用表單說明文字。
「測試計畫」格式及文字修正		
項次	格式修正及文字誤繕	處理修正情形
1	P18 「六、測試步驟」內文之粗體字，請確認有無表示特殊涵意。	並無特殊意涵，已修正。
2	P21 表 9 之專案名稱錯誤，請修正。	已修正。

「資訊系統設計規格」內容修正對照

項次	審查意見	處理修正情形
1	章節及內容請依本中心 ISMS 所訂項目 (ISMS-01170104) 調整修正。	已依貴中心 ISMS 所列章節調整，各章節對照如下： 文件目的 (P1)，名詞解釋及參考文件 (P2)，設計方法與工具 (P5)，軟體組織架構 (P3)，系統流程 (P10)，軟體元件設計 (P219)，使用者介面設計 (P196)，資料結構設計 (P94)，資料庫設計 (P202)，例外處理 (P231)，規格追溯表 (P231)。
2	P2「1.4 作業環境說明」之「(3) 字戶端瀏覽器」請補充 Google Chrome 版本要求。	已補充(P2)
3	P5「表 3 測繪成果圖冊資料管理系統軟體單元清單」請依上層功能架構將表格內之單元名稱區分排列。	已將圖 2-2 (p4) 配合表 3 所列項目及編號予以補充及對照。
4	P190「第 8 章」軟體項目介面設計」請補充文字說明及相關介面圖說。	已修正，於本章及相關附圖佐以文字說明。
「資訊系統設計規格」格式及文字修正		
項次	格式修正及文字誤繕	處理修正情形
1	內封面文件名稱下方不需再加註「(含程式清	已修正

	單……)」文字。	
2	P7「表3測繪成果圖冊資料管理系統軟體單元清單」文字應置於該表上方。	已修正

「資訊系統開發計畫」內容修正對照		
項次	格式修正及文字誤繕	處理修正情形
1	章節及內容請依本中心 ISMS 所訂項目 (ISMS-01170101) 調整修正, 另「二、專案開發人力配置計畫」一節增述本案相關工作規劃辦理時程及說明, 並將本節更名為「專案管理計畫」。	已依貴中心 ISMS 所列章節調整, 各章節對照如下: 文件目的 (P1), 現有系統 (P1), 現有系統限制 (P5), 名詞解釋 (P5), 參考文件資料 (P5), 開發平臺環境 (P6), 軟體發展方法 (P6), 專案管理計畫 (P9), 品質保證計畫 (P10), 型態管理計畫 (P11)。
2	P1「一、文件目的」請補充說明本文件大綱及適用範圍。	已修正 (P1)。
3	P1「二、現況描述」請依現況補充說明系統功能相關描述。	已修正 (P1)。
4	P6「一、開發平臺環境」請補充說明伺服器開發語言 VB、網頁開發使用之 ASP.NET 及 JQuery 程式庫	已修正(P6)

	之版本為何？另系統及盤點程式為相同開發工具（Microsoft Visual Studio）版本不同，請補充說明原因。	
「資訊系統開發計畫」格式及文字修正		
項次	格式修正及文字誤繕	處理修正情形
1	P6「(二) 盤點程式(手持機)……以進行圖冊盤點(抽查/清查)作業」。請修正為「……盤點(抽查/清查/清點)……」。	已修正(P6)
2	P6「二、軟體發展方法……並經國土機關人員確認無誤後」；文字請修正為「……並經機關確認無誤後」。	已修正(P6)

「資訊系統需求規格」內容修正對照		
項次	審查意見	處理修正情形
1	章節及內容請依本中心 ISMS 所訂項目 (ISMS-01170102) 調整修正。	已依貴中心 ISMS 所列章節調整，各章節對照如下： 文件目的 (P1)，現有系統 (P1)，現有系統限制 (P5)，名詞解釋 (P5)，參考文仔 (P5)，整體系統概述 (P6)，系統操作環境平臺 (P13)，使用者作

		業活動 (P13), 遵循及參考標準 (P14), 驗收前應準備之文件(P14), 功能需求 (P16), 介面需求 (P17), 非功能性需求 (P17), 雛形系統摘述 (P18), 需求追溯表 (P19)。
2	P3「表 1 系統軟硬體規格一覽表」內容請確認規格項目為原環境或新設環境。	該表係為原有環境, 部份規格誤植, 已修改(P3)
3	P7「圖 4 系統架構與細部功能圖」與 P13「圖 5 系統項目介面設計」之功能項目有部份不同, 請檢視修正; 另請將「圖 4 系統架構與細部功能圖」請參照 P8「表 3 系統子功能清單」標示編號以利對照	已修與, 經比對後, 已將「系統項目介面設計」(現為圖 6, p18) 修正一致。另將圖 4 (p7) 對照表 3 項目標示編號。
4	P13「參、系統項目介面設計」請補充說明文字	已修正 (P18)。
「資訊系統需求規格」格式及文字修正		
項次	格式修正及文字誤繕	處理修正情形
1	目錄標示項目請檢視修正與內容章節名稱一致。	已修正。
2	圖目錄所列圖號與內文不符, 請修正。	已全部檢視並修正。
3	P5「五、參考文件」之最後一段文字及 P12 表格下	已修正。

	方文字應為誤植，請修正。	
4	P6「一、系統概觀說明」內文與各圖表標示不同，請修正。	已修正。

恆隆科技股份有限公司
EPC Solutions Taiwan Inc.

<http://www.epcsolutionsinc.com.tw>

30076 新竹科學園區工業東二路 13 號 2 樓

TEL: 03-5786361

FAX: 03-5771491