NLSC-113-15

113 年及 114 年資通安全服務及資訊安全管理系統維運採購案

Information Security Services and the Information Security Management System maintenance procurement project in 2024 and 2025

113 年度總報告(修正版)

2024 Annual Report(Revised Edition)

主辦機關：內政部國土測繪中心

執行單位：德欣寰宇科技股份有限公司

中華資安國際股份有限公司

中 華 民 國 114 年 1 月 6 日

目錄

壹、 摘要說明

內政部國土測繪中心（以下簡稱貴中心）「資通安全服務及資訊安全管理系統維運採購案」（以下簡稱本採購案)，由得標廠商德欣寰宇科技股份有限公司(以下簡稱本公司)協助持續及精進貴中心資訊安全管理系統(Information Security Management. System，ISMS)(以下簡稱 ISMS)各項控制措施之有效性並定期通過公正第三方機構驗證，確保貴中心所提供之資訊服務、內部員工電腦、內部網路環境、資訊設備等需要執行保護之資訊資產皆已受到適當管控，降低貴中心營運中所產生之資訊安全風險。

貴中心於 112 年 8 月經行政院核定為資通安全責任等級 B 級公務機關，須辦理資通安全責任等級分級辦法規定之 B 級公務機關應辦事項，本採購案也協助貴中心完成資通系統分級防護基準檢視、資安治理成熟度評估、系統滲透測試、資通安全健診、資通安全威脅偵測管理機制及 ISMS 等相關維運輔導作業，每月召開工作會議，檢討本專案各項專案成果及資安監控報告，共同強化貴中心資訊安全管理作為。

本次報告會含有本採購案各工作項目執行結果、效益及統計分析、改進建議與需求及綜合說明，供貴中心確認本採購案工作項目內容之完整性及思考未來持續精進之方向。

關鍵字：資訊安全管理系統、資通安全管理法、資通安全責任等級 B 級之公務機關應辦事項、ISMS

Summary

The National Land Surveying and Mapping Center of the Ministry of the Interior (hereinafter referred to as the NLSC) "Information Security Services and the Information Security Management System maintenance procurement project" (hereinafter referred to as the ISMS Procurement Project), the winning bidder by TSC Technologies , Inc. (hereinafter referred to as the TSC company) To assist in the continuous and refinement of the effectiveness of the various control measures of the Information Security Management System (ISMS) (hereinafter referred to as the ISMS) of NLSC and regularly pass the certificated by an impartial third-party organization to ensure that the NLSC Internal employee computers, internal network environment, information equipment, and other information assets that require to be implemented and protected have been properly controlled to reduce information security risks in NLSC's operations.

NLSC was approved by the Executive Yuan as Level-B of the cyber security responsibility levels of the government agency in August, year 2023. It must handle the matters required by the cyber security responsibility Level-B as specified in the Measures for the Classification of Information Security Responsibility. This procurement project also assists NLSC in completing the defense standards of information and communication system review, Cyber security governance maturity assessment, Testing of system penetration, Cyber security health diagnosis, Inspection of cyber security management mechanism, ISMS and other related maintenance and tutoring services, monthly review meetings are held to review the project results and information security monitoring reports in order to reinforce together the Cyber Security management Act of NLSC.

This report contains the implementation results, benefits and statistical analysis, improvement suggestions and requirements and comprehensive description. for NLSC to confirm the completeness of the work items of this procurement project and thinking about the direction of continuous improvement in the future.

Keywords: Information Security Management System, Cyber Security Management Act , Matters to be conducted by the government agency of cyber security responsibility Level-B, ISMS, SOC

貳、 本(113)年專案各項辦理工作項目

本專案團隊依據契約之各項要求與期程辦理各項工作，並定期交付月工作報告、季工作報告及年報告至貴中心與召開各月工作會議，說明各階段工作項目成果辦理情形，並依貴中心研議之會議紀錄配合辦理相關事項(詳如附件一)，各月份成果交付以電子檔案郵寄方式進行交付，並提供紙本文件交付單由貴中心人員與本專案團隊成員簽署(詳如附件二)，確認已完成當月應辦理事項之成果交付，滲透測試結果報告(初、複測)、資安事件處理報告、季工作報告及年報告以公文方式進行交付。

本專案契約規定之交付內容(項目)及實際交付時程如下表所示。

項次	交付內容(項目)		交付時程	
			契約規定	實際完成
1	113 年度專案工作計畫(含監控環境部署報告)		1 月 15 日前	1 月 12 日
2 3 4	1 月份 工作報告	1.1 月份工作報告 2.監控事件管理服務報告 3.ISMS 現況分析與前次稽核後續追蹤	2 月 6 日前	2 月 5 日
5	2 月份 工作報告	1.2 月份工作報告 2.監控事件管理服務報告 3.資通安全維護計畫實施情形彙整 4.滲透測試計畫 5.資安件診計畫(113 年度)	3 月 6 日前	3 月 6 日
6	3 月份 工作報告	1.3 月份工作報告 2.監控事件管理服務報告 3.資通安全監測項目清單查檢表	4 月 6 日前	4 月 8 日 (遇假日)
7	第 1 季季報告		4 月 15 日前	4 月 15 日
8	4 月份 工作報告	1.4 月份工作報告 2.監控事件管理服務報告 3.資通訊資產清冊 4.營運衝擊分析報告 5.營運持續演練計畫	5 月 6 日前	5 月 6 日
9	5 月份 工作報告	1.5 月份工作報告 2.監控事件管理服務報告 3.資通系統防護需求等級檢視報告 4.風險評鑑報告 5.ISMS 內部稽核計畫 6.供應商資通安全稽核計畫(實地及書面) 7.資安教育訓練報告(113 年)	6 月 6 日前	6 月 5 日
10	6 月份 工作報告	1.6 月份工作報告 2.監控事件管理服務報告 3.資通安全監測項目清單查檢表 4.資安教育訓練結訓證書(113 年)	7 月 6 日前	7 月 5 日
11	第 2 季季報告		7 月 15 日前	7 月 15 日

項次	交付內容(項目)		交付時程	
			契約規定	實際完成
12	7 月份 工作報告	1.7 月份工作報告 2.監控事件管理服務報告 3.營運持續演練報告(7 月)	8 月 6 日前	8 月 6 日
13	8 月份 工作報告	1.8 月份工作報告 2.監控事件管理服務報告 3.ISMS 內部稽核報告 4.ISMS 內部稽核不符合事項改善之建議表 5.資通系統防護基準檢視報告 6.供應商資通安全書面稽核報告 7.營運持續演練報告(8 月)	9 月 6 日前	9 月 6 日
14	9 月份 工作報告	1.9 月份工作報告 2.監控事件管理服務報告 3.資安治理成熟度評估報告 4.資通安全監測項目清單查檢表 5.第三方驗證啟始會議簡報及主席講稿	10 月 6 日前	10 月 7 日 (遇假日)
15	第 3 季季報告		10 月 15 日前	10 月 15 日
16	10 月份 工作報告	1.10 月份工作報告 2.監控事件管理服務報告 3.供應商資通安全實地稽核報告 4.資通訊資產清冊	11 月 6 日前	11 月 6 日
17	11 月份 工作報告	1.11 月份工作報告 2.監控事件管理服務報告 3.風險評鑑報告 4.第三方驗證稽核報告 5.第三方驗證稽核不符合事項改善之建議表 6.資通安全維護計畫妥適性檢視	12 月 6 日前	12 月 5 日
18	12 月份 工作報告	1.12 月份工作報告 2.監控事件管理服務報告 3.資通安全監測項目清單查檢表	12 月 20 日前	12 月 19 日
19	第 4 季季報告		12 月 25 日前	12 月 25 日
20	113 年度總報告		12 月 25 日前	12 月 25 日
21	滲透測試結果報告(初測)		檢測結束後 30 日內交付。	6 月 5 日
22	滲透測試結果報告(複測)			9 月 4 日
23	資安健診報告		資安健診結束後 30 日內	5 月 24 日

項次	交付內容(項目)	交付時程	
		契約規定	實際完成
24	資安事件處理報告	於機關通報資安事件（以國家通報應變網站通報時間為主）之次日起 20 日內交付。	113 年未發生資安事件。

參、 113 年度專案工作計畫(含監控環境部署報告)

本專案團隊依據契約各工作項目內容與辦理期程撰寫「113 年度專案工作計畫(含監控環境部署報告)」，計畫內容包含專案概要說明、專案團隊、工作執行規劃、專案管理、配合事項、工作時程規劃及監控環境部署報告，使貴中心了解本專案內容與提升執行之順暢度，計畫撰寫完成後於 1 月 12 日進行交付作業。

肆、 資通安全服務

一、資通安全維護計畫實施情形彙整

本專案團隊依據契約要求辦理貴中心 112 年資通安全維護計畫實施情形進行彙整作業，彙整內容項目依「數位發展部資通安全署資通安全作業管考系統」進行，完成後併入 2 月份工作報告進行交付作業。

二、資通安全維護計畫妥適性檢視

依據合約規定辦理貴中心資通安全維護計畫妥適性檢視作業，本專案團隊資安顧問於本次資通安全維護計畫妥適性檢視結果尚未有發現違反資通安全管理法及相關子法之內容，惟有部分章節內容可持續精進，詳細說明如檢視報告，此作業完成後併入 11 月份工作報告進行交付作業。

三、資安治理成熟度評估

本次評估報告協助配合數位發展部資通安全署要求辦理年度資安治理成熟度評估作業，評估內容針對 3 大面向，共 11 個流程構面、46 個檢核項目進行貴中心資安治理成熟度評估作業，完成後併入 9 月份工作報告進行交付作業。

四、資通系統防護需求等級檢視

依據資通安全責任等級分級辦法之應辦事項規定，資通安全責任等級 B 級之公務機關，每年至少檢視一次資通系統分級妥適性，本團隊資安顧問依據「資通安全責任等級分級辦法」之附表九資通系統防護需求分級原則協助資通系統業管人員進行資通系統安全等級妥適性評估作業，此作業完成後併入 5 月份工作報告進行交付作業

五、 資通系統防護基準檢視

依據合約規定每年 8 月份辦理資通系統防護基準評估報告，本團隊資安顧問於 8 月份提供各資通系統管理人員防護基準之內容確認與諮詢作業，後續由各資通系統管理人員提供資通系統防護基準控制措施評估表交由本團隊資安顧問確認與彙整作業，確認各項未完全符合或未實施之防護基準控制措施是否均已規劃改善作業，並計算各資通系統防護基準控制措施之符合率與提供評估結果建議，此作業完成後併入 8 月份工作報告進行交付作業，。

伍、 ISMS 維運輔導

一、 現況分析與前次稽核後續追蹤

本專案團隊依據貴中心現行 ISMS 管理機制執行情況與最新版資訊安全管理系統標準進行分析，並檢視前次第三方驗證稽核結果進行後續追蹤作業，提出後續具體後續調整或補強之建議，以作為貴中心後續資訊安全管理制度及文件調整之參考，提升業務管理流程之效能與效率，此作業辦理完成後提送「ISMS 現況分析與前次稽核後續追蹤」，完成後併入 1 月份工作報告進行交付作業。

二、 資通訊資產盤點

本專案團隊依據契約要求協助貴中心辦理 1 年 2 次資訊資產盤點作業，分別於 4 月及 10 月執行資產價值之適切性檢視、保管人事異動調整等事項，因應 113 年修訂「ISMS-01070000-資訊安全管理系統資產管理程序」文件，調整資通訊資產盤點方式及範圍，並辦理 1 場次說明會與提供盤點資料範例，盤點項目包含全機關之網路設備、網路基礎設施、環境控制設備、機房環境與實體基礎設施，並將所有資通系統納入盤點範圍內，由各資通訊業務承辦盤點完後協助確認其資料完整性，確認後併入 4 月份及 10 月份工作報告進行交付作業。

三、 風險評鑑與處理

本專案團隊依據契約要求協助貴中心辦理 1 年 2 次風險評鑑作業，識別與分析電腦機房內各項資通訊資產及資通系統可能遭受之風險，方便於日後維運能清楚識別將面對之處境及需要加強之控制，使貴中心電腦機房之資產遭受弱點、威脅的傷害及機率降低，完成後併入 5 月份及 11 月份工作報告進行交付作業。

本年度風險評鑑結果並未發現有高於風險等級 3(中)以上者，故無須辦理後續風險處理作業，其中風險識別內容已因應貴中心資安事件鑑別相關風險議題，例如：資通訊設備老舊、未妥善執行資通訊設備巡檢和監控不足而導致服務標的的效能受到影響或中斷的風險，上傳檔案檔案頁面為限制檔案類型、使用者帳號及密碼強度不足遭惡意入侵等風險。

資產管理者應持續遵守貴中心的 ISMS 規範和資通訊服務委外合約，並觀察資通訊服務的運作情況。如果資通訊服務出現異常或中斷，應按照貴中心的「ISMS-01130000-資訊安全管理系統事件管理程序」進行事件通報、應變和處理工作。同時，在執行事件根因分析後，應識別相關的風險威脅和脆弱性，檢視現有的控制措施是否能夠降低或避免資通安全事件的發生。

四、營運衝擊分析

本專案團隊依據契約要求協助貴中心辦理營運衝擊分析作業，此營運衝擊分析作業以系統化的方法進行收集貴中心 ISMS 適用範圍內，提供資訊服務所需之資通系統進行業務分析，透過與各系統負責人員討論及意見交流，深入瞭解、搜集實質有效資訊，以作為營運衝擊分析之依據，並計算出營運衝擊分結結果總分，以利貴中心了解資通系統之重要性排序，完成後併入 4 月份工作報告進行交付作業。

五、營運持續演練

本專案團隊依據合約需求辦理營運持續演練作業，演練標的選擇根據貴中心資通系統分級評估結果選擇至少 4 個資通訊服務執行實際演練，本專案團隊協助營運持續演練計畫撰寫，並於演練過程中彙整演練紀錄後，製作營運持續演練結果報告，並視演練結果檢視是否需修正演練計畫或執行矯正作業，計畫及報告完成後分別併入 4 月份及 7 月與 8 月份工作報告進行交付作業。

本次演練共 4 項資通訊服務，皆於 7 月及 8 月辦理完竣，演練作業有部分後續需關注或改善事項，建議貴中心仍持續參考各演練結果檢討內容，精進營運持續能量。

六、精進 ISMS 文件

本專案團隊資安顧問為符合資通安全要求，於專案期間內持續檢視內部或外部議題、主管機關要求、相關法規命令，遵循 ISO 27001/CNS 27001 標準，持續檢視貴中心 ISMS 文件，執行相關文件增修作業，並將調整結果提報每月工作會議進行討論，本年度已協助貴中心由 ISO 27001 2013 版本改版至 ISO 27001 2022 版本，並持續視執行現況進行調整作業。

七、內部稽核

本專案團隊依據合約需求辦理 ISMS 內部稽核作業，協助內容包含 ISMS 內部稽核計畫與稽核查檢表之研擬作業，完成後併入 5 月份工作報告進行交付作業，並於稽核過程指派 2 人具有 ISO 27001:2013 主導稽核員資格之內部稽核顧問協助稽核活動，並於稽核活動後產出 ISMS 內部稽核報告，併入 8 月份工作報告進行交付作業。

本次 ISMS 內部稽核活動於 8 月 19 日 9 時 30 分召開啟始會議，並於是日 10 時至 8 月 21 日 12 時執行 ISMS 符合性稽核。8 月 21 日 14 時召開結束會議，本次稽核項目計 123 項，其中適用性聲明排除列為不適用者計 1 項、稽核發現符合者計 118 項；輕微不符合者 1 項；列為觀察事項 3 項；列為建議事項 3 項，依 ISMS 內部稽核結果，共開立 7 件矯正措施單，針對各項矯正措施單，本專案團隊資安顧問與貴中心相關單位討論後提供矯正及預防相關建議，提供 ISMS 內部稽核不符合事項改善之建議表，供貴中心持續精進 ISMS 之參考。

八、管理階層審查輔導

為持續改善及精進貴中心 ISMS，貴中心每年每季召開 ISMS 工作小組會議及資通安全推行小組會議，討論 ISMS 相關事宜，本專案團隊資安顧問均配合貴中心會議時間派員列席參與會議，並針對會議內容及 ISMS 議題等適時提供建議，各會議時間及參與之本專案團隊資安顧問如下表所示。

項次	會議名稱	會議時間	資安顧問
1	第 1 次 ISMS 工作小組會議	3 月 19 日	李 O 甫
2	第 1 次資通安全推行小組會議	3 月 29 日	吳 O 仁、李 O 甫
3	第 2 次 ISMS 工作小組會議	6 月 18 日	林 O 和
4	第 2 次資通安全推行小組會議	6 月 28 日	林 O 和
5	第 3 次 ISMS 工作小組會議	9 月 16 日	吳 O 仁
6	第 3 次資通安全推行小組會議	9 月 30 日	吳 O 仁
7	第 4 次 ISMS 工作小組會議	12 月 18 日	蕭 O 余
8	第 4 次資通安全推行小組會議	12 月 27 日	吳 O 仁

九、ISMS 有效性量測

本專案團隊依據契約要求辦理於每年 3 月、6 月、9 月及 12 月配合貴中心辦理 1 次 ISMS 有效性量測作業，量測結果將填寫貴中心 ISMS「資通安全監測項目清單查檢表」，辦理過程由貴中心 ISMS 安全預防分組成員及 ISMS 管理師一同執行此作業，針對貴中心資通安全政策目標及各項資訊安全控制措施項目進行有效性量測作業，以確保控制目標或控制措施之有效性仍持續維持，完成後併入當月份工作報告進行交付作業。

本年度執一行共 4 次 ISMS 有效性量測作業，過程中得知貴中心人員已確實遵守 ISMS 各項規定辦理資安維運作業並納入日常習慣，故作業執行結果均無發生違反或異常之情事發生。

陸、 第三方驗證

一、啟始會議簡報及主席講稿

本專案團隊依據契約要求須協助貴中心研擬第三方驗證啟始會議簡報及主席講稿供貴中心參考，簡報及主席講稿內容包含組織概況、資通安全業務概況、資通安全業務推動情況(含 ISMS 維運及資通安全管理法遵循與精進)、未來工作重點、貴中心資通安全相關工作人員介紹，使第三方驗證稽核委員於第三方驗證稽核啟始會議時更能了解貴中心資安執行概況，使稽核過程更順暢，此作業完成後併入 9 月份工作報告進行交付作業。

簡報部分節錄如下圖所示：

二、第三方驗證稽核先期檢驗作業

本專案團隊依據契約要求須於第三方驗證稽核前協助辦理第三方驗證稽核先期檢驗作業，本專案團隊成員已於 10 月 28 日完成第三方驗證稽核先期檢驗作業，檢驗結果共發現 4 項建議事項，現已完成相關改善作業。

三、第三方驗證稽核報告及通過證書

本次第三方驗證稽核活動於 11 月 8 日順利完成，本次經第三方驗證機構依 ISO/IEC 27001:2022 標準稽核後，無重大缺失，證書維持有效，第三方驗證稽核報告已併入 11 月份工作報告進行交付作業，並以郵寄方式提供第三方驗證稽核通過證書至貴中心。

四、第三方驗證稽核不符合事項改善之建議表

本次第三方驗證稽核結果共 4 項觀察事項，本專案團隊依據契約要求配合第三方驗證團隊委員所提出建議事項提出貴中心改善之建議，完成第三方驗證稽核稽核不符合事項改善之建議表併入 11 月份工作報告進行交付作業。

柒、 供應商資通安全稽核（實地及書面）

本專案團隊依據契約要求辦理供應商稽核作業，執行內容包含稽核計畫(含稽核項目)之研擬與執行稽核作業，計畫完成後併入 5 月份工作報告進行交付作業。

本作業協助貴中心執行 7 個供應商稽核作業，其中書面稽核配合貴中心 8 月份 ISMS 內部稽核作業期間一併辦理，書面稽核報告已於 8 月份工作報告進行交付作業，實地稽核報告於 10 月份工作報告進行交付作業；稽核發現結果事項若需由供應商進行改善，則由貴中心函送各資通系統供應商進行後續改善追蹤作業。

捌、 SOC 監控服務

本專案團隊依據契約要求提供貴中心全天候(365 日*24 小時)SOC 監控服務，並每月產出 SOC 監控服務月報告進行交付作業，分析當月 SOC 監控事件情形，提供相關資安技術防禦改善建議。本專案截至 12 月 15 日，監控範圍已包含貴中心資安防禦設備、重要設備主機日誌及核心資通系統應用程式日誌，共 17 項資通訊服務已納入監控範圍。

玖、 滲透測試服務

本專案團隊依據契約要求提供 5 個資通系統滲透測試服務作業，測試標的由貴中心進行挑選，並由本專案團隊撰寫滲透測試計畫，完成測試作業後彙整發現之相關弱點撰寫滲透測試報告撰寫(初測&複測)交付至貴中心，並請貴中心針對具有風險之相關弱點進行評估，必要時請委外廠商修正後自行透過報告中提供驗證成功的指令或方式予以確認發現弱點之修補有效性。

壹拾、 資安健診服務

本專案團隊已依據第 1 次工作會議之資安健診討論撰寫資安健診計畫並於 3 月 6 日併入 2 月份工作報告一併交付至貴中心，健診標的由貴中心進行挑選，並由本專案團隊撰寫資安健診計畫，透過整合各項資通安全項目的檢視服務作業，提供貴中心資安改善建議，藉以落實技術面與管理面相關控制措施，以提升網路與資訊系統安全防護能力，貴中心可以據本次執行結果考量現有資源之配置，提升相關軟硬體設備之管控作業，降低資通安全事件發生之可能性並同時降低資通安全事件發生所造成之危害。

本次資安健診執行期間於 4 月 22 至 4 月 26 日完成相關作業，完成於 5 月 24 日交付資安健診服務報告。

壹拾壹、 效益及統計分析

一、資安監控事件分級統計

本專案 113 年 1 月 1 日至 12 月 31 日共發送 726 件資安監控事件通知，其中包含低風險 432 件、中風險 291 件及高風險 3 件。

二、資安監控事件分類統計

本年度案件種類分析中，本年度排除資安預警通報及資安情資分享後，監控事件之「內主機執行掃描探測攻擊」、「非上班時間特權帳號登入成功」及「外部主機執行掃描探測攻擊」事件較多，已委請機房管理單位執行相關確認與處理作業。

三、作業人員性別平等資訊統計

本專案團隊一貫嚴守法令規定，落實性別平等之對待，於專案執行過程中，整體人力投入共 21 人，男女工作分配比例如下表所示。

項次	作業項目	男：女
1	資通安全服務	5：1
2	ISMS 維運輔導	6：2
3	第三方驗證	5：1
4	供應商資通安全稽核	8：2
5	資安監控服務	4：0
6	資安教育訓練	2：0
7	資安健診服務	5：0
8	滲透測試服務	3：1

壹拾貳、 改善建議與需求

貴中心已完成國際標準 ISO 27001:2022 改版作業，透過定期內部稽核、有效性量測、資安檢測及管理審查等資安維運作業維持其有效性，並持續通過公正第三方驗證作業，請貴中心持續依照新版標準內容及程序內容進行資安維運作業，例如：威脅情資、雲端服務使用的資安、資通訊技術營運持續整備、實體安全監控、組態管理、資訊刪除、資料遮罩、資料外洩防護、網站過濾等要求，並持續安排人員參與稽核員證照及轉版課程，強化貴中心人員對於新版標準之認知。

另建議貴中心除策略面與管裡面之資安作為外，可考量於現有 ISMS 管理措施，例如：資料加密、設備上鎖或妥善存放的基礎上，進一步評估並導入技術性控制機制，例如資料加密、多因素驗證及 DLP（資料外洩防護），以提升可攜式媒體、電子郵件及網路傳輸等面向的資料洩露預防管理能力。

壹拾參、 綜合說明

本年度專案各項作業皆已順利完成，貴中心同仁仍需持續執行 ISMS 各項規定，落實資安管理作業於日常業務中，維持資通訊服務之機密性、完整性、可用性及法律遵循性，本專案團隊也將持續協助與配合內外部關注方之回饋與議題變更，持續協助貴中心強化 ISMS 程序規定與執行 SOC 監控作業，共同維護安全的資通訊環境。

壹拾肆、 附件

一、會議記錄(含簽到表)

二、各月份成果交付單