NLSC-109-4

109 年及 110 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 2020 and 2021

109 年度總報告(修正版)

2020 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 民 國 110 年 1月 5日

目錄

壹、 摘要說明

內政部國土測繪中心（以下簡稱貴機關）「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)協助持續及精進貴機關資訊安全管理系統(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，確保貴機關所提供之資訊服務、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，降低貴機關營運中所產生之資訊安全風險。

貴機關於 108 年 6 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，本採購案也協助貴機關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，共同強化貴機關資訊安全管理作為。

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，供貴機關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 June, year 2019. 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(109)年專案各項辦理工作項目

依合約規定之交付內容(項目)及實際交付時程如下表 1 所示：

項次	交付內容(項目)		交付時程	實際交付時程
1	109 年度專案工作計畫(含監控環境部署報告)		1 月 10 日前	1 月 9 日
2	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 6 日
3	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. 資安健診計畫（109 年度） 4. 滲透測試計畫（109 年度）	3 月 6 日前	3 月 6 日
4	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 5. 資訊安全監測項目清單查檢表	4 月 6 日前	4 月 6 日
5	第 1 季報告		4 月 15 日前	4 月 14 日
6	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. 資產清冊 4. 營運衝擊分析報告	5 月 6 日前	5 月 6 日
7	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. 資通系統防護需求分級評估報告 4. 風險評鑑報告 5. 風險處理計畫 6. 營運持續演練計畫 7. 營運持續演練結果報告（沙盤演練） 8. ISMS 內部稽核計畫	6 月 6 日前	6 月 5 日
8	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	7 月 6 日前	7 月 6 日

項次	交付內容(項目)		交付時程	實際交付時程
		3. 資訊安全監測項目清單查檢表		
9	第 2 季報告		7 月 15 日前	7 月 14 日
10	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. 營運持續演練結果報告（實際演練）	8 月 6 日前	8 月 6 日
11	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. 資安治理成熟度評估報告 6. 資通系統防護基準評估報告 7. 委外廠商資安稽核計畫	9 月 6 日前	9 月 4 日
12	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. 資訊安全監測項目清單查檢表 4. 第三方驗證啟始會議簡報及主席講稿	10 月 6 日前	10 月 6 日
13	第 3 季報告		10 月 15 日前	10 月 15 日
14	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. 委外廠商資安稽核報告 4. 資產清冊	11 月 6 日前	11 月 6 日
15	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. 風險處理計畫 5. 第三方驗證稽核結果報告 6. 第三方驗證稽核不符合事項改善之建議表	12 月 6 日前	12 月 4 日

項次	交付內容(項目)		交付時程	實際交付時程
16	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. 資訊安全監測項目清單查檢表	12 月 20 日前	12 月 18 日
17	第 4 季報告		12 月 25 日前	12 月 25 日
18	109 年度總報告		12 月 25 日前	12 月 25 日
19	資安事件處理報告		發生資安事件時才須辦理，應於資安事件結案後 30 日內交付，	本年度無發生資安事件，故無資安事件處理報告。
20	資安健診服務（109 年辦理）		資安健診結束後 30 日內	資安健診執行期間為 109 年 4 月 15 日至 5 月 6 日，並於 5 月 21 日交付結果報告，符合合約要求。
21	滲透測試結果報告（初測及複測，109 年辦理）		滲透測試（初測及複測）結束後 30 日內	1.初測於 4 月 24 日完成，並於 5 月 21 日交付初測報告。 2.複測於 7 月 24 日完成，並於 8 月 21 日交付複測報告，符合合約要求。

表 1：專案工作項目交付期程表

參、 109 年度專案工作計畫

依據貴機關「109 工作行事曆(ISMS)」規劃期程，就本專案之規劃管理、組織、時程及進度查核等方面撰寫「109 年度專案工作計畫」(含監控環境部署報告)，說明專案需求規劃、專案管理、專案組織、交付項目、時程及進度查核、專案驗收及貴機關配合事項、會議紀錄及執行方式、專案文件編碼原則等，於 1 月 10 日交付。

肆、 資通安全服務

一、資安治理成熟度評估

本採購案專案顧問透過實際與貴機關人員訪談及書面資料檢視方式並依據行政院公布之資安治理成熟度評估方法論，評估貴機關現行資安治理成熟度等級，109 年第 1 次執行結果貴與 108 年評估結果一致為 Level 2，經過專案顧問協助提供相關意見與實作指引，提供貴機關持續精進 ISMS 程序書相關規定，專案顧問於 10 月份執行第 2 次評估作業，製作第 2 次資安治理成熟度評估報告，再次檢次各項流程構面之能力度，評估後異動 2 項查核項目，其餘 39 項無異動，評估結果貴機關資安治理成熟度各流程構面皆已達到能力度 3 或更高(評估結果詳如表 2)，故貴機關成熟度符合 Level 3，

流程構面成熟度等級	流程構面	流程構面能力度			109 年成熟度判定結果					備註
		108 年評估	109 年第一次評估	**109 年第二次評估**	L1	L2	L3	L4	L5	
Level 5	S2 資安治理架構	2	2	2	○	○	×	×	×	
Level 4	S4 資安管理監督	3	3	3	○	○	○	×	×	
Level 3	T4 資通系統開發與維護安全	3	3	3	○	○	○	×	×	
	T3 資安事件通報與處理	3	3	**4**	○	○	○	○	×	提升
	S3 資安資源管理	2	2	**3**	○	○	○	×	×	提升
Level 2	T1 存取控制管理	3	3	3	○	○	○	×	×	
	M2 資訊委外安全管理	3	3	3	○	○	○	×	×	
	M1 資產管理與風險評鑑	4	4	4	○	○	○	○	×	
Level 1	T2 通訊與作業安全管理	3	3	3	○	○	○	×	×	
	M3 資安認知與教育訓練	3	3	3	○	○	○	×	×	
	S1 資安政策與組織健全	4	4	4	○	○	○	○	×	

表 2：資安治理成熟度評估表

二、資通系統防護需求分級

本採購案專案顧問依據「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評估，評估後由貴機關 ISMS 管理師提送第 2 次 ISMS 工作小組及資通安全推行小組討論，討論結果 109 年貴機關資通系統共 17 項，其中資通系統防護需求「高等級」2 項、「中等級」10 項、「普等級」5 項。

三、 資通系統防護基準評估

貴機關 109 年資通系統共 17 項，專案顧問協助測繪資訊課召開資通系統防護基準說明會，邀集各資通系統承辦人及維運廠商參加，並由專案顧問針對防護基準查檢表項目逐項說明，以確保各資通系統落實防護基準控制措施，專案顧問也提供駐點服務，提供各資通系統承辦人及維運廠商執行諮詢服務並針對不符合項目協助研擬改善方案及期程，統整資料後產製資通系統防護基準評估報告，供貴機關執行後續追蹤作業。

四、 委外廠商資安稽核

本採購案專案顧問已於 10 月 5 日協助執行貴機關委外廠商資安稽核作業，稽核過程委外廠商人員均配合本次稽核作業，稽核結果共發現 2 項未符合事項及 1 項建議事項。

伍、 ISMS 維運輔導

一、 現況分析與前次稽核後續追蹤

依據合約要求每年應依據最新版國際資訊安全標準 ISO 27001/CNS27001 進行 ISMS 制度現況業務分析及前次第三方驗證稽核結果進行後續追蹤作業，109 年 ISMS 現況分析及追蹤結果於 2 月 6 日併入 1 月份工作報告一併交付。

二、 資訊資產盤點

本採購案專案顧問依據合約要求協助貴機關辦理 2 次資訊資產盤點作業，分別於 5 月 4 日及 10 月 19 日完成完成資產價值之適切性檢視、保管人事異動調整等事項，調整貴機關資產清冊，確保資產清冊之完整性及正確性與貴機關現況一致。

本年度 2 次資訊資產盤點結果均未發現資訊資產尚未涉及中國大陸廠牌之資訊資產，並將委外廠商納入資產清冊，以利後續針對委外廠商風險評鑑作業。

三、風險評鑑與處理

本採購案專案顧問依據合約辦理 2 次風險評鑑作業，評鑑結果各資產之風險等級皆未達到不可接受風險等級 3(含)，係因貴機關以往已就各項資訊資產實施相應之控制措施，如人員之專業訓練、委外廠商維護合約資安規定、設備定期保養維護、系統資安檢測作業、存取權限控管、資料備份、資安宣導講習等，實際反應在本次風險評鑑之結果，顯見既有之控制措施，已能有效控制與預防本中心資產可能發生的風險，目前並無資產須立即進行後續風險處理事宜。

四、營運衝擊分析

依據採購案合約要求，本次營運衝擊分析作業以系統化的方法進行收集與分析貴機關 ISMS 適用範圍內，提供資訊服務所需之資通系統，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，以利貴機關了解資通系統之重要性排序。

本次評估結果之前三大重要資訊服務資通系統，以「e-GNSS 即時動態定位系統」及「國土測繪圖資 e 商城」之衝擊最高，其次為「國土測繪圖資服務雲」。

五、營運持續演練

（一）實際演練

依據貴機關資通系統分級評估結果，選擇 2 個資通系統執行實際演練，分別於 7 月 9 日及 15 日執行資通系統營運持續演練，演練結果均符合規劃之目標回復時間，並於 7 月份工作報告交付營運持續演練結果報告。

（二）沙盤推演

依據貴機關資通系統評估結果，協助貴機關辦理 5 個資通系統沙盤推演作業，完成後於 5 月份工作報告交付沙盤推演報告。

六、精進 ISMS 文件

協助貴中心精進各項 ISMS 文件，並檢討至少 1 次。貴中心 ISMS 文件共計 73 件，本年度已全數檢視完畢。

七、內部稽核

本採購案規定貴機關辦理 ISMS 內部稽核作業時須至少派 2 人（含）以上具有 ISO27001:2013 主導稽核員資格之內部稽核顧問，協助貴機關執行內部稽核，並產出內部稽核報告。

本次內部稽核項目計 355 項，其中適用性聲明排除列為不適用者計 3 項，提列優良事項計 7 項；稽核發現符合者計 345 項，嚴重不符合者 1 項，輕微不符合者計 5 項，列為觀察事項者計 1 項。

本年執行 ISMS 內部稽核結果，共開立 12 件矯正措施單，針對各項矯正措施單，專案顧問與相關單位討論後提供矯正及預防相關建議，製作 ISMS 內部稽核不符合事項改善之建議表與內部稽核報告併入 8 月份工作報告一併交付。

八、管理階層審查輔導

為持續改善及精進貴機關 ISMS，貴機關每年每季召開 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，本採購案專案顧問均配合貴機關會議時間列席參與會議，並針對會議內容及 ISMS 議題等適時提供建議。

九、ISMS 有效性量測

依據合約規定每年 3 月、6 月、9 月及 12 月辦理 1 次 ISMS 有效性量測，量測結果填載於貴機關 ISMS「資通安全監測項目清單及計畫表」。

本年度執行共 4 次 ISMS 有效性量測作業，貴機關資通安全政策目標及各項資訊安全控制措施衍生之量測指標，無發生違反或異常之情事發生。

陸、 第三方驗證

一、會議簡報及主席講稿

依據合約規定須協助研擬第三方驗證啟始會議簡報及主席講稿供貴機關機關參考，並納入 9 月份工作報告交付。

二、ISMS 追查驗證稽核先期檢驗作業

依據合約要求，本採購案專案顧問已於 10 月 26 日協助辦理貴機關 ISMS 追查驗證稽核先期檢驗作業，檢驗結果共發現 2 項建議事項。

三、第三方驗證稽核結果報告

本次第三方驗證稽核活動於 109 年 11 月 5 日順利完成，經第三方驗證機構之主任稽核員依 ISO/IEC27001:2013 標準稽核後，無重大缺失，證書維持有效，並於 12 月 1 日交付 ISO/IEC 27001:2013 年度通過證明至貴機關。

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 項觀察事項及 1 項建議事項，專案團隊顧問已針對各委員所提出建議事項提出改善之建議，併值持續持行相關改善作業。

柒、 SOC 監控服務

提供貴機關 7X24 小時全天候監控、異常事件通報及相關資安聯防回傳機制，本年度監控設備共 32 台，包含貴機關之資安防禦設備及重要資通系統伺服器等，本公司均於每月提交資安事件監控管理服務報告，藉由監控事件提供資安相關改善建議。

捌、 資安健診服務

資安健診執行期間為 4 月 15 日至 5 月 6 日，執行完畢後於 5 月 21 日交付「資安健診結果報告書」，符合合約規定於檢測完畢後 30 天內交付要求；本採購案之資安技術顧問於貴機關第二次資通安全推行小組提供一次資安健診結果簡報及資詢作業；貴機關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。

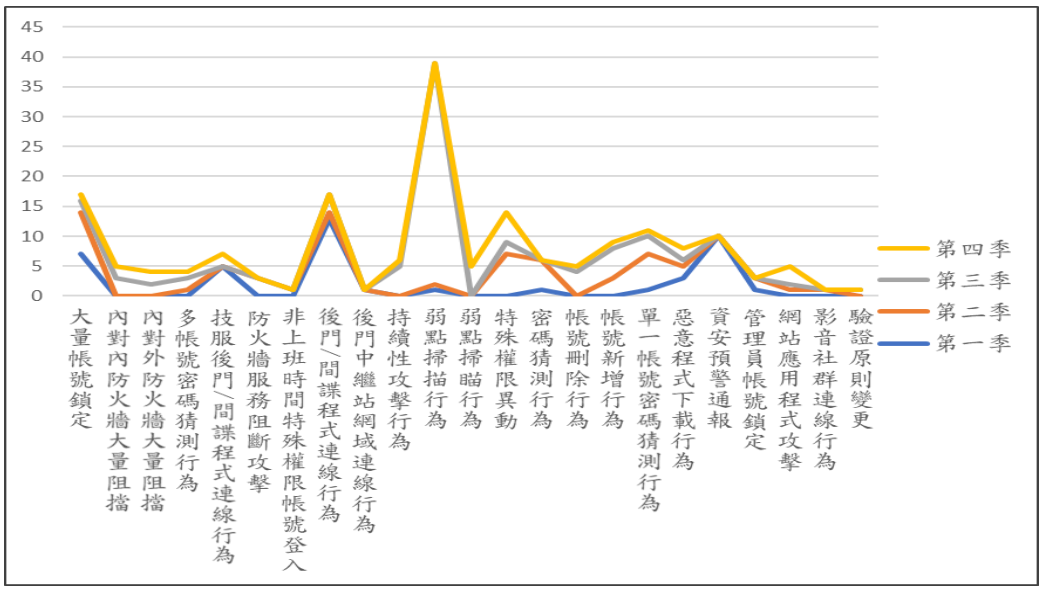
玖、 滲透測試服務

本次針對貴中心所提供之 10 個標的來執行黑箱滲透測試服務(複測)，在此次測試評估結果中發現存在有中、低風險漏洞，本公司建議貴中心盡速針對中度風險弱點進行修補，其餘低風險漏洞建議根據貴中心之安全性考量來進行修補，避免遭受駭客進行有效的攻擊。

壹拾、 效益及統計分析

一、資安監控異常事件

本年度(1 月 1 日至 12 月 31 日)共 182 件異常事件，均已處理完畢並結案。



二、作業人員性別平等資訊統計

本專案一貫嚴守法令規定，落實性別平等之對待，於專案執行過程中，整體人力投入共 33 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	**10**	：	**1**
2	ISMS 維運服務	**10**	：	**1**
3	第三方驗證	**10**	：	**1**
4	SOC 監控服務	**13**	：	**2**
5	資安健診服務	**9**	：	**1**
6	滲透測試服務	**9**	：	**1**

壹拾壹、　改善建議與需求

貴機關 ISMS「組織全景」雖該文件為四階表單，惟考量該文件係為了解組織及其全景、了解關注方之需要及期望等，應屬高位階 ISMS 文件之性質，貴機關可優先於明(110)年與本採購案專案顧問討論文件位階與內容修正事宜。

壹拾貳、　綜合說明

貴機關目前資通安全責任等級為 B 級，已依據「資通安全責任等級分級辦法」附表三資通安全責任等級 B 級之公務機關應辦事項執行各項內容，本(109)年配同貴機關接受內政部所屬機關資通安全稽核作業(以下簡稱內政部資安稽核)，專案顧問也協助貴機關辦理先期檢驗作業及陪同內政部稽核作業，內政部稽核團隊稽核結果無開立缺失事項，另提出 6 項優良事項及 19 項建議事項，專案顧問也持續提供相關改善建議供貴機關執行矯正與預防作業。

配合資通安全管理法要求，貴機關下半年已加強推動資訊服務委外案之安全管理，擬定「委外專案資通安全控制措施要求檢核表」，措施內容包含資通系統防護需求分級所對應防護基準及委外廠商資通安全要求(如：廠商發現疑似資訊安全或個資外洩等異常事件或事故時，應負有即時通報本中心，並提供事件或事故相關資訊之責任)，並擬納入下年度之資通系統維護委外契約要求；另本年除辦理委外廠商之實地資安稽核作業外，新增書面委外資安廠商稽核作業，提升委外廠商對於受託標的之資通安全要求與貴中心之期望。

內政部國土測繪中心
地址：臺中市南屯區黎明路 2 段 497 號 4 樓
網址：www.nlsc.gov.tw
總機：（04）22522966
傳真：（04）22592533