NLSC-107-3

107年及108年度資訊安全服務及管理系統維運採購案

107年度報告

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 107年 12 月 19日

目　錄

壹、報告查核期間

107 年 1 月 1 日至 107 年 12 月 10 日

貳、本專案各事項辦理情形

項次	工作項目	交付文件	預定交付時程	實際執行日期
1	年度專案工作計畫書	年度專案工作計畫書	每年 2 月 10 日前。	1 月 22 日發文交付
2	工作報告書	月報告	自 107 年 2 月起每月 10 日前（12 月份應於 12 月 20 日前交付）。	1 月-2 月 9 日交付 2 月-3 月 9 日交付 3 月-4 月 9 日交付 4 月-5 月 9 日交付 5 月-6 月 8 日交付 6 月-7 月 9 日交付 7 月-8 月 8 日交付 8 月-9 月 7 日交付 9 月-10 月 9 日交付 10 月-11 月 9 日交付 11 月-12 月 7 日交付 12 月-12 月 19 日交付
		季報告	每季結束後 10 日內，除第 4 季外（每年 12 月 20 日前）。	第一季-4 月 9 日交付 第二季-7 月 9 日交付 第三季-10 月 9 日交付 第四季-12 月 19 日交付
		年度報告書	每年 12 月 20 日前。	12 月 19 日交付
3	ISMS 維運輔導	現況分析與前次稽核後續追蹤之改善建議	每年交付第 1 次月報前。	1 月 22 日交付
		資訊系統安全等級評估表	每年 6 月 30 日前。	5 月 1 日交付
		資訊資產清冊	每年 6 月 30 日前（上半年）及每年 12 月 20 日前（下半年）。	3 月 28 日交付 8 月 1 日交付
		風險評鑑報告與風險處理計畫書	每年 6 月 30 日前（上半年）及每年 12 月 20 日前（下半年）。	3 月 29 日交付 8 月 2 日交付

項次	工作項目	交付文件	預定交付時程	實際執行日期
		資訊安全管理文件	每年 12 月 20 日前。	5 月 24 日修改 2 份三階文件、1 份四階文件 8 月 31 日修改 1 份二階文件、1 份三階文件、4 份四階文件，刪除 1 份四階文件 11 月 27 日修改 1 份二階文件、5 件四階文件
		營運衝擊分析報告	每年 6 月 30 日前。	4 月 18 日交付
		營運持續演練計畫書	每年 6 月 30 日前。	4 月 24 日完成並交付-國土測繪 e 商城 5 月 28 日完成並交付-國土測繪圖資服務雲
		營運持續演練報告（實際演練）	實際演練後 30 天內。	6 月 22 日執行國土測繪圖資服務雲營運持續演練-6 月 22 日交付演練報告 7 月 11 日執行國土測繪 e 商城營運持續演練-7 月 18 日交付演練報告
		營運持續演練報告（沙盤推演）	每年 6 月 30 日前。	5 月 18 日交付 5 項資訊系統沙盤推演營運持續演練報告
		內部稽核計畫	每年 6 月 30 日前。	6 月 14 日交付
		稽核查檢表（併同內部稽核計畫裝訂）		6 月 14 日交付
		內部稽核報告	內部稽核結束後 10 天內。	8 月 15 日完成內部稽核，8 月 22 日交付
		啟始會議及結束會議簽到表（併同內部稽核報告裝訂）		
		不符合事項改善之追蹤與成效確認表	內部稽核結束後 45 天內。	8 月 31 日交付 9 月 6 日 8 月工作會議討論
		ISMS 工作小組會議資料	依本機關實際開會前 20 天。	第一季：3 月 2 日提供，3 月 22 日開會

項次	工作項目	交付文件	預定交付時程	實際執行日期
				第二季：6 月 1 日提供，6 月 20 日開會 第三季：8 月 29 日提供，9 月 20 日開會 第四季：11 月 20 提供，12 月 14 日開會
		ISMS 工作小組會議及資訊安全推行小組簽到表	依本機關實際開會後 10 天內。	3 月 30 日開會 6 月 29 日開會 9 月 25 日開會 預計 12 月 27 日開會
		每季之資訊安全監測項目清單及計畫表	每年 3 月、6 月、9 月及 12 月。	第一季：3 月 6 日交付 第二季：6 月 6 日交付 第三季：9 月 3 日交付 第四季：12 月 3 日交付
4	第三方驗證	會議簡報及主席講稿	先期檢驗前 7 天內。	10 月 31 日辦理先期檢驗，10 月 12 日交付
		稽核結果報告（第三方驗證機構）及驗證通過證明文件	稽核後 30 天內。	11 月 20 日交付
5	資安治理成熟度評估服務	資安治理成熟度評估報告書	每年 12 月 20 日前。	8 月 1 日交付
6	資安監控服務	監控環境整備報告書	決標後次日起 30 天內。	1 月 22 日發文交付
		資安事件監控管理服務報告書（併同月報裝訂）	自 107 年 2 月起每月 10 日前（12 月份應於 12 月 20 日前交付）。	1 月-2 月 9 日交付 2 月-3 月 9 日交付 3 月-4 月 9 日交付 4 月-5 月 9 日交付 5 月-6 月 8 日交付 6 月-7 月 9 日交付 7 月-8 月 8 日交付 8 月-9 月 7 日交付 9 月-10 月 9 日交付 10 月- 11 月 9 日交付 11 月- 12 月 7 日交付 12 月-12 月 19 日交付

項次	工作項目	交付文件	預定交付時程	實際執行日期
7	資訊安全教育訓練	教育訓練課程配當表（含課程、時數及講師）、講義教材及簽到表	每年 4 月 30 日前。	3 月 29 日交付
		教育訓練成果及滿意度調查表	依實際辦理時程後 10 天內。	1. 5 月 16 日辦理危機處理（3HR）及資安防護（3HR），並於 5 月 17 日交付教育訓練成果及滿意度調查表 2. 5 月 22 日辦理資安防護研討會（6HR），並於 5 月 29 日交付教育訓練成果及滿意度調查表
		國際資安專業證照課程上課證明	每年 9 月 30 日前。	5 月 29 日交付
8	資安健診服務	資安健診計畫書	資安健診前。	3 月 5 日交付
		資安健診結果報告書	執行結束後 30 天內。	執行時間：3 月 19 日至 4 月 18 日，5 月 11 日交付資安健診結果報告
9	滲透測試服務	滲透測試計畫書（初測及複測）	滲透測試前。	3 月 21 日交付
		滲透測試結果報告書（初測及複測）	執行結束後 30 天內。	初測時間：4月9日至4月20日， 5月15日交付滲透測試報告 複測時間：7月16日至7月27日，8月2日交付滲透測試報告，並持續進行弱點矯正追蹤與成效確認

一、ISMS 維運及驗證

(一) 現況分析與前次稽核後續追蹤

依契約要求，執行現況分析與前次稽核後續追蹤之改善建議，並於一月工作報告前提出，並持續追蹤至第一季均已處理完竣。

(二) 資訊系統安全等級評估作業

資訊系統分級

依據行政院「資訊系統分級與資安防護基準作業規定」，自行或委外開發之資訊系統需要進行分級，各項資訊系統均須依循程序填寫「安全等級評估表」，並本公司彙整成「資訊系統清冊」。

資訊系統名稱	業務屬性	資訊系統安全等級	共同性系統	承辦單位
e-GNSS 即時動態定位系統入口網站	業務類	高	N	控制測量課
國土測繪圖資 e 商城	業務類	高	N	測繪資訊課
測量儀器校正實驗室	業務類	中	N	企劃課
基本地形圖資料庫分組入口網站	業務類	中	N	地形及海洋測量課
臺灣通用電子地圖服務網	業務類	中	N	地形及海洋測量課
經費核銷整合系統	行政類	中	N	會計室
差假及派車管理系統	行政類	中	N	人事室
全國衛星追蹤站暨基本控制點查詢系統	業務類	中	N	控制測量課
薪資整合管理系統	行政類	中	N	秘書室
全國土地段籍總檢核系統	業務類	中	N	測繪資訊課
測量成果圖冊資料管理系統	業務類	中	N	測繪資訊課
圖冊數立詮釋資料管理系統	業務類	中	N	測繪資訊課
員工教育訓練系統	行政類	普	N	企劃課
全球資訊網	業務類	普	N	測繪資訊課

資訊系統名稱	業務屬性	資訊系統安全等級	共同性系統	承辦單位
個人工作儀表板（LDAP）	行政類	普	N	測繪資訊課
行政支援系統	行政類	普	N	測繪資訊課
公文系統	業務類	非系統開發機關	Y	秘書室
測量助理及工友人事管理資訊系統	行政類	中	N	秘書室
國土利用監測查報系統	業務類	中	N	地形及海洋測量課
測繪知識網（KM）	業務	普	N	企劃課
鑑測資料庫查詢及管理系統	業務	普	N	地籍測量課
重測便民服務查詢系統	業務	普	N	地籍圖重測課

(三) 資訊資產盤點作業

依據契約當年度至少辦理 2 次（需間隔 3 個月以上）盤點本機關相關資訊資產，並建立與確保資訊資產清冊之完整性及正確性，第 1 次資產盤點作業時間為 3 月 27 日，第 2 次資產點作業時間為 8 月 1 日，間隔達 4 個月。

1. 上半年資產盤點作業

本次資產清查以 107 年 3 月 27 日當天之資產為準，包括至善樓機房、地籍資料庫機房(包含應用軟體系統)以及機房共通資產，並於 107 年 3 月 28 日完成資產價值評估。總計機房以及辦公室(以 ISMS 相關工作人員及其所使用之設備為範圍)內所含之各類資別出各類資產共有 437 項，較 106 年度增加 14 項，在保管人事異動及功能說明的部份，已進行更新事宜。

本次資產清查結果總計機房以及辦公室(以 ISMS 相關工作人員及其所使用之設備為範圍)內所含之各類資別出各類資產共有 437 項，屬「實體類」資產者計 232 項屬「軟體類」資產者計 118 項；屬「資訊類」資產者計 35 項；屬「人員類」資產者計 9 項；屬「服務類」資產者計 43 項。

2. 下半年資產盤點作業

本次資產清查以 107 年 8 月 1 日當天之資產為準，包括至善樓機房、地籍資料庫機房(包含應用軟體系統)以及機房共通資產，並於 107 年 8 月 1 日完成資產價值評估。總計機房以及辦公室（以 ISMS 相關工作人員及其所使用之設備為範圍）內所含之各類資別出各類資產共有 450 項，在保管人事異動及功能說明的部份，已進行更新事宜。

其中，實體類資產更動計 17 項，新增 8 項、異動 5 項、停用 4 項；軟體類資產更動計 8 項，新增 7 項、移除 1 項；服務類資產更動計 4 項，新增 3 項、移除 1 項；至於資訊類、人員類資產則無變更。。

本次資產清查結果，屬「實體類」資產者計 240 項屬「軟體類」資產者計 123 項；屬「資訊類」資產者計 33 項；屬「人員類」資產者計 9 項；屬「服務類」資產者計 45 項。

(四) 風險評鑑與處理

依契約規定上半年及下半年需各執行 1 次風險評鑑，並識別威脅來源及脆弱點，本團隊依據貴機關風險管理作業原則，完成驗證範圍內風險評鑑，並提出妥適之風險處理計畫。

風險評鑑過程中，考量各項業務維運需求並參照 ISO 27002 國際標準資訊安全管理作業規範，以及 ISO 13335、ISO 31000、ISO 27005 資訊安全風險管理指導綱要之建議作法，針對重要之資產及應用系統納入風險評鑑範圍，依據風險分析與評估所計算出之風險值換算成風險等級。

1. 上半年風險評鑑報告

以 107 年 3 月 27 日當天之資產為準，包括至善樓機房、地籍資料庫機房（包含應用軟體系統）以及機房共通資產，並於 107 年 3 月 27 日完成資產價值評估。總計機房以及辦公室（以 ISMS 相關工作人員及其所使用之設備為範圍）內所含之各類資別出各類資產共有 437 項。

接受評鑑之重要資產共計 278 項（資產價值等級 3（含）以上者），與 106 年度一樣。經進行資產群聚歸納整理後，共計 21 大項資產，依據資產特性及分類識別其風險及威脅弱點，總計識別出可能的威脅與弱點共計 333 項，其中風險等級為 1（微）者，共計 293 項，風險等級為 2（低）者，共計 40 項，並未發現有高於風險等級 3（中）以上者。

2. 下半年風險評鑑報告

以 107 年 8 月 1 日當天之資產為準，包括至善樓機房、地籍資料庫機房（包含應用軟體系統）以及機房共通資產，並於 107 年 8 月 1 日完成資

產價值評估。總計機房以及辦公室（以 ISMS 相關工作人員及其所使用之設備為範圍）內所含之各類資別出各類資產共有 450 項，在保管人事異動及功能說明的部份，已進行更新事宜；實體類資產更動計 17 項，新增 8 項、異動 5 項、停用 4 項；軟體類資產更動計 8 項，新增 7 項、移除 1 項；服務類資產更動計 4 項，新增 3 項、移除 1 項；至於資訊類、人員類資產則無變更。

本次針對異動重要資產風險評鑑統計結果，接受評鑑之重要資產共計 13 項，經進行資產群聚歸納整理後，共計 4 大項資產，依據資產特性及分類識別其風險及威脅弱點，總計識別出可能的威脅與弱點共計 94 項，其中風險等級為 1（微）者，共計 87 項，風險等級為 2 （低）者，共計 7 項，並未發現有高於風險等級 3（中）以上者。

3. 上下半年風險評鑑趨勢

風險等級	1（微）	2（低）	3（中）	4（高）	5（極	總計
上半年統計數量	293	40	0	0	0	333
下半年統計數量	87	7	0	0	0	94

4. 風險處理計畫

本次風險評鑑結果，並未發現有超過可接受風險等級 4(高)含以上者，亦無風險等級 3（中）者。

（1） 實體類資產方面

實體類資產中，以伺服器主機設備群資產具有較高之資產價值等級（屬第 3 級）。

風險評鑑發現，「電力供應喪失」之威脅，具有「對電壓變化的敏感性」的脆弱點。另外「不當維護」之威脅，具有「缺乏有效的變更控制」的脆弱點，系統或設備變更相關事宜時須遵照資訊安全管理系統之相關規定並評估影響範圍及風險並做成紀錄，防止此狀況之發生。

（2） 軟體類資產方面

軟體類資產中，以應用軟體暨資料庫系統群資產具有較高之資產價值等級（屬第 4 級），因應用軟體暨資料庫系統群為提供本中心資訊服務之必要資產。

風險評鑑發現，「惡意的軟體」之威脅，具有「已知的軟體瑕疵」的脆弱點，在本中心持續且密集的實施弱點掃描與外部偵測後，其發生機率已有效降低，可偵測性亦已有效提升。另外的「偽造權限」之威脅中，尚有「缺乏如使用者授權的識別與授權機制」所造成的弱點部份，應落實定期執行帳號清查及權限控管之審核，以預防此狀況之發生。

(五) ISMS 文件修訂

依據貴機關實際執行 ISMS 流程、內部稽核建議以及法令法規遵循，檢視並修訂 ISMS 文件， 本年度檢視現有資訊安全管理系統全部文件及相關流程。

ISMS 文件檢視狀態列表：

文件階層	編號	名稱	版次	狀態
一階文件	ISMS-01000000	政策文件	V2.6	未修改
一階文件	ISMS-02000000	適用性聲明	V2.4	未修改
二階文件	ISMS-01010000	文件與紀錄管理程序	V1.5	未修改
二階文件	ISMS-01020000	稽核程序	V1.4	修改
二階文件	ISMS-01030000	風險評鑑與管理程序	V1.6	未修改
二階文件	ISMS-01040000	網路安全管理程序	V1.3	未修改
二階文件	ISMS-01050000	資料備份與回復管理程序	V1.2	未修改
二階文件	ISMS-01060000	組織管理程序	V1.2	未修改
二階文件	ISMS-01070000	資產管理程序	V1.5	未修改
二階文件	ISMS-01080000	人員安全管理程序	V1.5	未修改
二階文件	ISMS-01090000	實體與環境安全管理程序	V1.6	未修改
二階文件	ISMS-01100000	通訊與操作管理程序	V1.5	未修改
二階文件	ISMS-01110000	存取控制管理程序	V1.8	未修改
二階文件	ISMS-01120000	資訊系統上線管理程序	V1.3	未修改
二階文件	ISMS-01130000	事件管理程序	V2.0	修改
二階文件	ISMS-01140000	資訊業務營運持續管理程序	V1.4	未修改
二階文件	ISMS-01150000	法規適用性管理程序	V1.3	未修改
二階文件	ISMS-01160000	供應商管理程序	V1.3	未修改
二階文件	ISMS-01170000	資訊系統開發管理程序	V1.1	未修改
三階文件	ISMS-01040100	網路弱點管理作業	V1.4	未修改
三階文件	ISMS-01040200	電腦病毒防治作業	V1.1	未修改
三階文件	ISMS-01040300	電腦機房管理作業	V1.5	修改
三階文件	ISMS-01140100	資訊業務營運持續計畫	V3.3	修改
三階文件	ISMS-01140200	電腦機房緊急應變計畫	V2.3	未修改

文件階層	編號	名稱	版次	狀態
三階文件	ISMS-01170100	軟體開發文件規劃	V1.0	未修改
四階文件	ISMS-01000001	組織全景	V1.2	未修改
四階文件	ISMS-01010001	文件、表單清冊	V1.0	未修改
四階文件	ISMS-01010002	紀錄清冊	V1.0	未修改
四階文件	ISMS-01010003	文件/紀錄調閱申請單	V1.0	未修改
四階文件	ISMS-01020001	資訊安全矯正與預防措施處理表	V1.1	修改
四階文件	ISMS-01020002	資訊安全矯正及預防措施報告	-	刪除
四階文件	ISMS-01030001	風險評鑑表	V1.0	未修改
四階文件	ISMS-01030002	ISMS 風險處理計畫表	V1.0	未修改
四階文件	ISMS-01030003	資訊安全監測項目清單及計畫表	V2.6	修改
四階文件	ISMS-01040001	防火牆異動申請單	V1.0	未修改
四階文件	ISMS-01040002	安全防護工具變更申請單	V1.0	未修改
四階文件	ISMS-01040101	弱點通知處理單	V1.3	修改
四階文件	ISMS-01040102	異常事件通知處理單	V2.1	修改
四階文件	ISMS-01050001	備份媒體管理清單	V1.0	未修改
四階文件	ISMS-01050002	媒體資料調閱申請表	V1.0	未修改
四階文件	ISMS-01050003	媒體銷毀作業處理表	V1.0	未修改
四階文件	ISMS-01050004	測試及回復作業紀錄表	V1.0	未修改
四階文件	ISMS-01070001	資產明細表	V1.1	未修改
四階文件	ISMS-01070002	資產清冊	V1.0	未修改
四階文件	ISMS-01080001	駐點服務人員報到單	V1.0	未修改
四階文件	ISMS-01080002	駐點服務人員撤駐單	V1.0	未修改
四階文件	ISMS-01080003	資訊安全保密切結書（個人）	V1.0	未修改
四階文件	ISMS-01080004	資訊安全保密切結書（廠商）	V1.0	未修改
四階文件	ISMS-01090001	電腦機房人員進出登記簿	V1.0	未修改
四階文件	ISMS-01110001	帳號管理表單	V1.1	修改
四階文件	ISMS-01110002	遠端登入使用申請表	V1.0	未修改
四階文件	ISMS-01110003	電腦機房工作日誌	V1.0	未修改
四階文件	ISMS-01110004	遠端登入作業記錄表	V1.0	未修改
四階文件	ISMS-01120001	資訊服務申請表	V1.0	未修改
四階文件	ISMS-01120002	資訊系統上線作業紀錄表	V1.0	未修改

文件階層	編號	名稱	版次	狀態
四階文件	ISMS-01120003	重大安全更新確認表	V1.1	修改
四階文件	ISMS-01130001	資通安全事件通報單	V1.1	修改
四階文件	ISMS-01140001	損壞資產清冊	V1.0	未修改
四階文件	ISMS-01140002	災害預防與減災措施表	V1.0	未修改
四階文件	ISMS-01140003	災害緊急應變任務分工名單	V1.1	修改
四階文件	ISMS-01140004	資源檢核表	V1.0	未修改
四階文件	ISMS-01140101	營運持續計畫測試/演練結果報告單	V1.0	未修改
四階文件	ISMS-01150001	資訊安全法規總覽表	V1.0	未修改
四階文件	ISMS-01170101	資訊系統開發計畫書	V1.0	未修改
四階文件	ISMS-01170102	資訊系統需求規格書	V1.0	未修改
四階文件	ISMS-01170103	資訊系統測試計畫書	V1.0	未修改
四階文件	ISMS-01170104	資訊系統設計規格書	V1.0	未修改
四階文件	ISMS-01170105	資訊系統使用手冊	V1.0	未修改
四階文件	ISMS-01170106	資訊系統測試報告	V1.0	未修改
四階文件	ISMS-01130002	資通安全事件處理單	V1.0	新增

(六) 營運持續計畫之規劃與演練

1. 營運衝擊分析

契約規定須於 107 年 6 月 30 日前交付營運衝擊分析報告，已於 4 月 20 日完成並於工作會議中提出討論及審核。

依據本（107）年度上半年風險評鑑結果（107 年 3 月 29 日），提供本中心資訊服務之應用系統共計 22 項，並依據重要資訊服務應用系統之**復原時間需求**，以及**營運中斷衝擊**分析評估結果，彙整如下表：營運衝擊分析結果所示。

序位	系統名稱	最大可容許中斷時間	資料回復時間目標	衝擊分析分數	合計
1	e-GNSS 即時動態定位系統	5	4	22	31
2	國土測繪圖資 e 商城	5	4	22	31
3	全球資訊網	5	4	19	28
4	國土測繪圖資服務雲	4	4	19	27
5	臺灣通用電子地圖服務網	4	2	19	25
6	全國衛星追蹤站暨基本控制點查詢系統	5	2	17	24
7	重測便民服務查詢系統	4	4	15	23
8	國土利用監測整合通報查報系統	3	4	15	22
9	國土利用調查成果資訊網	3	3	15	21
10	測量儀器校正實驗室服務網	3	3	15	21
11	基本地形圖資料庫分組入口網站	3	3	14	20
12	差假管理與派車申請	3	2	14	19
13	薪資整合管理系統	3	2	14	19
14	經費核銷整合系統	3	2	14	19
15	行政支援系統	4	3	12	19
16	法院鑑測案件管理系統	3	3	12	18
17	測量助理及工友人事管理資訊系統	2	2	13	17
18	測繪知識網（KM）	2	2	13	17
19	測繪成果圖冊資料管理系統	2	4	11	17
20	全國土地段籍總檢核系統	3	2	12	17
21	圖冊數位詮釋資料管理系統	3	2	12	17
22	公文系統	2	1	12	15

經由本次營運衝擊分析辦理結果中發現,「e-GNSS 即時動態定位系統」及「國土測繪圖資 e 商城」為本中心所提供眾多資訊服務中，其重要程度為最高者，因其提供全國大眾之收費服務，一但發生資安事故時其影響範圍較大，嚴重影響本中心良好聲譽，故本系統應於事故發生而導致服務中斷時，於最短時間內完成復原，以利持續接收衛星觀測資料，並避免超過 4 小時停

機造成該日營運之損失。資訊系統已每兩年度辦理一次營運持續演練作業，但仍建議持續辦理本系統之營運持續演練相關作業，以提昇資訊服務之可用性程度等級，作為服務契約制訂及系統改善強化規劃方向之參考。此外，建議規劃建置系統同步備援機制以及資料庫同步異動機制，以提升系統之持續運作能力。

至於「全球資訊網」部分，屬機關對外主要網站入口，且介接國土測繪資訊服務，當服務中斷時容易造成使用者找不到相關圖資服務連結，雖其他介接之圖資系統服務正常，但仍會造成使用者操作系統之不便，萬一發生中斷事故，仍需在短時間內恢復運作，唯因備份週期之故，對於資料流失問題應謀求解決之道，建議在可能的情況下，建立相關同步備份機制。

2. 營運持續演練

依據契約需根據資訊系統分級評估結果選擇至少 2 個重要系統執行實際演練，廠商須參與及執行營運持續計畫，並產出演練結果報告，並依演練結果修正計畫

(1) 營運持續演練計畫

依據 ISMS 工作小組會議審核通過，確認本年度要執行營運持續演練之系統為「國土測繪圖資 e 商城」及「國土測繪圖資服務雲」兩個系統，依契約規定須協助訂定營運持續計畫。

國土測繪圖資 e 商城

國土測繪中心位於至善樓機房提供外界圖資供應服務之「國土測繪圖資 e 商城」發生狀況，民眾來電反應國土測繪中心「國土測繪圖資 e 商城」出現網頁無法瀏覽情形，造成民眾與各售圖站人員無法查詢瀏覽網站功能，導致圖資查詢停擺。另經「國土測繪圖資 e 商城」網站管理人員(以下簡稱網站管理人員)嘗試以內網及外網方式瀏覽該網站檢查民眾反應問題，均無法正常瀏覽，緊急通報異常事件。

國土測繪圖資服務雲

國土測繪中心「圖資服務雲」建置於國家高速網路與計算機中心(以下簡稱國網中心)提供外界服務，民眾來電反應圖資服務雲出現網頁無法瀏覽情形，同時民眾與介接軟體均無法正常使用網站功能。經圖資服務雲網站管理人員(以下簡稱網站管理人員)嘗試瀏覽該網站檢查民眾反應問題，發現確實無法正常瀏覽，亦無法遠端登入伺服器主機，遂緊急通報異常事件。

(2) 營運持續演練報告(實際演練)

國土測繪圖資 e 商城

依據「國土測繪圖資 e 商城_營運持續演練計畫」，於 7 月 11 日執行相關演練，並於 7 月 18 日整理演練相關紀錄產製營運持續演練報告交付，符合執行 30 日內交付。

本次演練，圖資 e 商城資訊系統啟動備份還原步驟符合原先計畫要求，應用系統管理人員先通報維護廠商人員檢視網站伺服器，發現 IIS 服務異常，經重新安裝並啟動 IIS 服務失效後，立即啟用備份還原機制，使用近日的備份檔案在 VM 上還原圖資 e 商城網站伺服器，測試其功能正常，記錄於營運持續演練報告，使國土測繪中心相關人員與維護廠商人員熟悉圖資 e 商城資訊系統網站備份還原步驟及通報流程。

經本次演練測試結果，確認應用系統管理人員與維護廠商人員及技術支術人員充份配合且對系統熟悉度之純熟，才可以於最短時間內完成備份復原作業，並將測試結果留存為作業程序，中斷時間亦低於規劃中斷時間 5 小時。

貴機關已於 8 月完成圖資 e 商城異地備援機制，並測試確認應用系統發生異常時，可順利於 30 分鐘內手動切換至異地備援應用系統。

國土測繪圖資服務雲

依據「國土測繪圖資服務雲_營運持續演練計畫」，於 6 月 22 日執行相關演練，並於 6 月 22 日整理演練相關紀錄產製營運持續演練報告交付，符合執行 30 日內交付。

本次演練，圖資服務雲資訊系統備援機制切換步驟符合原先計畫要求，系統負責人員先聯繫國網中心將位於「臺中機房」圖資服務雲

資訊系統服務手動中斷，在使用手動設定切換至「新竹機房」備援設備後，測試其登入功能正常，記錄於營運持續演練報告，使國土測繪中心相關人員與維護廠商熟悉圖資服務雲資訊系統切換步驟及通報流程。

經本次演練測試結果，確認圖資服務雲資訊系統負責人員與相關雲端提供廠商及維護廠商人員充份配合且對系統熟悉度之純熟，才可以於最短時間內完成切換及復原作業，並將測試結果留存為作業程序，中斷時間亦低於規劃中斷時間 4 小時。

(3) 營運持續演練報告(沙盤演練)

依據契約需辦理至少 5 個資訊系統沙盤推演，並交付沙盤推演報告，參考貴機關相關環境，擬定沙盤推演項目。

項次	資訊系統名稱	推演情境
1	臺灣通用電子地圖服務網	臺灣通用電子地圖服務網網頁目錄檔案遭受加密軟體攻擊，無法正常作業。
2	公文系統(內政部)	內政部公文系統(以下簡稱公文系統)不明原因，無法正常作業。
3	差假管理系統	差假管理系統網頁目錄檔案遭受加密軟體攻擊，無法正常作業。
4	測量儀器校正實驗室服務網	測量儀器校正實驗室服務網網頁目錄檔案遭受加密軟體攻擊，無法正常作業。
5	地籍圖重測便民服務系統	地籍圖重測便民服務系統網頁目錄檔案遭受加密軟體攻擊，無法正常作業。

(七) 執行內部稽核

依契約規定需配合貴機關執行內部稽核作業，並在內部稽核日次日起 20 天內交付內部稽核報告。

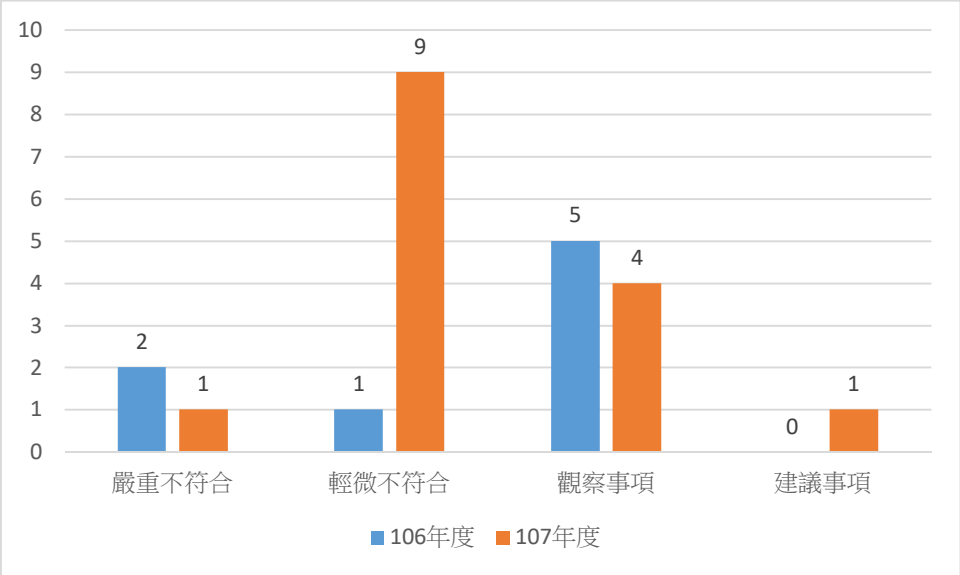
1. 內部稽核作業

本年度於 8 月 13 日-8 月 15 日協助貴機關執行內部稽核作業。

2. 內部稽核報告

本次稽核項目計 355 項，其中適用性聲明排除列為不適用者計 3 項、稽核發現符合者計 338 項；稽核發現嚴重不符合者計 1 項；稽核發現輕微不符合者計 9 項；稽核發現列為觀察事項者計 4 項;並提列建議事項 1 項。

已於 8 月 22 日完成並交付內部稽核報告，符合內部稽核日次日起 20 天內之契約要求。



3. 缺失矯正預防

依據 8 月 13 日-15 日執行內部稽核，8 月 22 日交付內部稽核報告，於 8 月 31 日針對不符合事項進行改善之追蹤，並交付「不符合事項改善之追蹤與成效確認表」，共開立 18 件矯正措施單，持續追蹤至 10 月 18 日均已處理完畢並結案。

紀錄編號	發現事項	處理情形	結案日期
1070815001	未確保制定及更新文件化資訊時，識別及描述適切。違反本文 7.5.2 規定(檢核表項次 0.61)： 1、備份及回復管理程序規定，完成備份之媒體，應製作「備份媒體管理清單」，並由網路管理人員放置於安全處所妥善保存。經分別調閱至善樓機房及地籍資料庫機房「備份媒體管理清單」，至善樓機房部分，紀錄編號 107070301(至善樓機房)，核章欄多主管欄，無表單編號及版次，所用表單與四階文件不符，另發現文件中，存有 107 年各月光碟片備份內容清單(非 ISMS 四階文件) ，光碟片屬於媒體，應予納管，上開文件屬備份媒體管理清單附件性質，發現事實與上開規定不符。 2、調閱「測試及回復作業紀錄表」，紀錄編號 107020501 及 107080701(至善樓機房)，所用表單與四階文件不符。 3、有關文件管理，政策文件資料夾內，文件編號 ISMS-01040300，存有 1.4 版(106/09/30)及 1.5 版(107/07/10)，舊版本文件未剔除。	1.已補送 ISMS 小組進行核章審查作業。 2.已修改表單，並更正後續執行作業之表單。 3.已將舊版本文件剔除。	9/12 結案
1070815002	未確保制定及更新文件化資訊時，識別及描述適切。違反本文 7.5.2 規定(檢核表項次 0.61)： 1、備份及回復管理程序規定，完成備份之媒體，應製作「備份媒體管理清單」，並由網路管理人員放置於安全處所妥善保存。經分別調閱至善樓機房及地籍資料庫機房「備份媒體管理清單」，地籍資料庫機房部分，無相關「備份媒體管理清單」紀錄，僅有 107 年各月光碟片備份內容清單(非 ISMS 四階文件)。 2、紀錄編號 107021201 及 107080801 (地籍資料庫機房)，陳核程序未完成，ISMS 工作小組審查意見未核章。	1.已補送 ISMS 小組進行核章審查作業，如附件 1。 2.已依 ISMS 規定及稽核意見增列輩分媒體管理清單，如附件 2(已由 106/12 起補正)。	8/20 結案
1070815003	未留有詳細的管理者與操作員之作業日誌。違反標準 A.12.4.3 規定(檢核表項次 12.28)： 1. 調閱「電腦機房工作日誌」紀錄編號 107033101、107051601、107052201、107061201 及 107061301(至善樓機房)，駐點工程師陳賢原於 107/3/31、5/16、5/22、6/12 及 6/13 皆有請假紀錄，惟上開紀錄之值班人員仍為陳賢原，顯與實際不符。 2. 至善樓機房資訊服務申請表紀錄編號 107053001 有關 Fortinet ADC-200F 上線，已依「資訊安全管理系統資訊	1.已修改相關機房工作日誌 2.已附上修補後之無風險之弱掃報告	9/12 結案

紀錄編號	發現事項	處理情形	結案日期
	系統上線管理程序」規定，填寫「資訊系統上線作業紀錄表」，其中安全性檢測附件尚存有弱點（含有 1 個高風險），申請單位雖辦理修補，惟未將處理結果及情形作成紀錄記載於任何可供查閱之文件中。		
1070815004	未留有詳細的管理者與操作員之作業日誌。違反標準 A.12.4.3 規定(檢核表項次 12.28)： 1.調閱「電腦機房工作日誌」紀錄編號 107051601 及 107052201 (地籍資料庫機房)，駐點工程師陳弘彬於 107/5/16 及 5/22 等皆有請假紀錄，惟上開紀錄之值班人員仍為陳弘彬，顯與實際不符。	已更正本年 5/16、5/22 及 6/8 電腦機房工作日誌值班人員，如附件。	8/20 結案
1070815005	未決定監督、量測、分析及評估之適用方法。違反本文 9.1(b)規定(檢核表項次 0.73)： 調閱「資訊安全監測項目清單及計畫表」各季紀錄，表單紀錄監測人員為委託廠商人員，惟表單頁尾核章欄，監測人員為安全預防分組人員核章，顯與事實不符。另各項目之監測週期，僅於表末欄列有分季、半年、年之監測週期，惟第一大項(目標)未列有監測週期欄位。有關監督量測應考量決定適用方法。	修改「資訊安全監測項目清單及計畫表」，增加 ISMS 目標監測週期欄位，並由委外廠商監測人員於下方簽名	10/9 結案
1070815006	未識別所有資產，並製作與維持重要資產的清冊，定期進行盤點、更新。違反標準 A.8.1.1 規定(檢核表項次 8.1)： 資產管理程序規定，有關資訊資產分級管制之措施，屬密等級者，須標示「紅色」或「密」。查資產清冊機密性等級（C）列為「2 密等級」者，查識別編號 SO-4 亦未貼標示，與上開規定不符。	已依照 ISMS 規範，貼上紅色標示	10/16 結案
1070815007	使用者存取權限未定期複檢(建議每 6 個月一次)或在權限變更後立即複檢。違反標準 A.9.2.5 規定(檢核表項次 9.28)： A.9.2.5 使用者存取權限之審查係指資產擁有者應定期審查使用者之存取權限，另本中心存取控制管理程序規定，使用者權限定期審查部分，網路管理人員應定期（至少每 6 個月 1 次）檢視伺服器所設定之帳號權限是否與註冊申請資料相符，應用系統管理人員應定期（至少每 6 個月 1 次）檢視伺服器所設定之帳號權限是否適當。查無國土測繪圖資 e 商城應用系統管理人員辦理之紀錄，與上開規定不符。	修正表單內容，新增帳號權限是否適當及應用系統管理人員核章的欄位。	10/9 結案
1070815008	對於資訊財產攜出辦公處所，未依攜出管理規則(含安全查核)。違反標準 A.11.2.5 規定(檢核表項次 11.26)： 實體環境安全管理程序規定，重要物品攜出、入機房時，應填寫「資訊服務申請表」說明原因，並經核可後始得放行，經調閱「電腦機房工作日誌」紀錄編號 107050301，更換地籍資料庫機房之 NetAPP 儲存設備 HD，未有核可之相關紀錄，與上開規定不符。	已補申請 5/23 硬碟攜入之資訊服務申請表，如附件。	8/20 結案
1070815009	未建立資訊處理設施使用的監視程序，並定期審查監視活動的結果。違反標準 A.12.4.1 規定(檢核表項次 12.25)： 調閱至善樓機房 107/6/20-27 攝影紀錄時，只發現該日期資料夾並無備份內容，因此無活動紀錄。	已使用 host monitor 機制，確認錄影主機已利異	9/12 結案

紀錄編號	發現事項	處理情形	結案日期
		常情形時可立即發現及處理。	
1070815010	作業系統軟體更新未知會應用系統管理人員。違反標準 A.12.5.1 規定(檢核表項次 12.30)： 資訊系統上線管理程序規定，作業系統在升級進行修補程式或軟體進行修改之前，網路管理人員須先以「重大安全更新確認表」知會相關應用系統管理人員，以評估其對應用系統之影響。經調閱「電腦機房工作日誌」紀錄編號 107040901，其附件僅「WSUS 主機更新狀態清單」(非 ISMS 四階文件)，該日更新 whgis.nlsc.gov.tw, Windows Server 2008 R2 Enterprise Edition，查無「重大安全更新確認表」，與上開規定不符。	已依 ISMS 規定於重大更新作業時填寫「重大更新確認表」。	9/12 結案
1070815011	機關員工及外部使用者未知悉資安事件通報及處理程序並依規定辦理。違反標準 A.16.1.1 規定(檢核表項次 16.4)： 事件管理程序規定，電腦機房發生異常徵兆時....，填寫「異常事件通知處理單」並分析判斷是否為資安事件或非資安事件。經調閱地籍資料庫機房「電腦機房工作日誌」紀錄編號 107042001、107042301、107042401 及 107042501，均記載環控異常，查無「異常事件通知處理單」，與上開規定不符。	已依 ISMS 規定填寫異常事件通知處理單，如附件	8/20 結案
1070815012	稽核後未產生稽核報告並追踪改善情形。違反本文 18.2.2 規定(檢核表項次 18.12)： 稽核程序規定，「單位主管應指派適當人員，按月將未完成改善之事項填寫於「資訊安全矯正及預防措施報告」中，並檢附「資訊安全矯正與預防措施處理表」，送交 ISMS 工作小組稽核分組進行追蹤查核。經查 106 年度外部稽核發現事項所開立「資訊安全矯正與預防措施處理表」，紀錄編號 10611160001 及 10611160004 尚未完成矯正預防作業，查無「資訊安全矯正及預防措施報告」紀錄，與上開規定不符。	依現況修正「ISMS-01020000-資訊安全管理系統稽核程序」，調整矯正及預防措施處理表追蹤流程，刪除無使用之「資訊安全矯正及預防措施報告」。	10/9 結案
1070815013	重要實體區域的進出權利未定期審查並更新。違反標準 A.11.1.2 規定(檢核表項次 11.3)： 「電腦工作日誌」，紀錄編號 107031401(至善樓機房及地籍資料庫機房)，門禁系統於 107/3/14 更換(採指紋及卡片兩種)，現行為採指紋及卡片並行使用，查 107 年門禁授權情形僅有 6 月份門禁卡領用清冊，無其他資料可稽。另該份清冊都是卡片授權，其地籍資料庫機房從 4/17 已有採指紋進出機房，至稽核日(8/13)尚未完成最新之人員門禁授權資料。	已完成 8/20 更新門禁權限領用清冊，新增指紋識別說明	9/12 結案
1070815014	重要實體區域的進出權利未定期審查並更新。違反標準 A.11.1.2 規定(檢核表項次 11.3)： 「電腦工作日誌」，紀錄編號 107031401(至善樓機房及地籍資料庫機房)，門禁系統於 107/3/14 更換(採指紋及卡片兩種)，現行為採指紋及卡片並行使用，查 107 年門禁授權情形僅有 6 月份門禁卡領用清冊，無其他資料可稽。	已完成 8/20 更新門禁權限領用清冊，新增指紋識別說明	8/20 結案

紀錄編號	發現事項	處理情形	結案日期
	另該份清冊都是卡片授權，其地籍資料庫機房從 4/17 已有採指紋進出機房，至稽核日(8/13)尚未完成最新之人員門禁授權資料。		
1070815015	各項安全設備定期檢查但未依設備適切處理。違反標準 A.11.2.1 規定(檢核表項次 11.15)： 至善樓機房使用之滅火器因由海龍型式更換為二氧化碳型式，其檢查記錄表未依滅火器使用說明調整。	已依照 CO2 滅火器檢測方式調整檢測表。	9/12 結案
1070815016	依規定定期弱點掃描，弱點掃描後，未持續追蹤漏洞修補情形。違反標準 A.12.6.1 規定(檢核表項次 12.33)： 「弱點處理單」多筆已超過 3 個月期限，未回復弱點處理結果。	由機房工作會議進行後續追蹤。	9/12 結案
1070815017	對於無法修補之系統，未評估其風險，並採取適當之控制措施。違反標準 A.12.6.1 規定(檢核表項次 12.35)： 「弱點處理單」（107041101、107030506、107022602、107022601）有殘餘風險未修正完成，亦未經過安全預防防分組組長同意其『接受風險』之簽署確認。	未符合程序之弱點處理單已處理中，並辦理簽核作業。	9/25 結案
1070815018	依「資訊安全管理系統電腦機房管理作業」規定，網路管理人員應依據「電腦機房工作日誌」中載列之查檢項目，每日巡察相關設備，並將檢視結果記錄於「電腦機房工作日誌」內；經查目前實務上，網路管理人員及委外廠商駐點工程師僅依據相關監控設備辦理檢視作業，並未每日實際進入機房檢視設備及相關環境。次查 107/7/11 於地籍資料庫機房發現天花板及地板均有嚴重積水情形，惟相關監控設備卻未偵測到，網路管理人員及委外廠商駐點工程師亦均未發現，還是由測繪資訊課人員通報後才作緊急處理，故僅由監控設備辦理每日機房檢視，似乎尚有不妥，建議重新討論並完善相關規定。	考量冷氣漏水等現象為長時間污垢累積，已規劃每年主動清潔及排水管改良作業，另立行機房巡檢仍規畫以自動化設備為主(如：攝影機、各項監測/感測器)，異常事件發生時，再以人工介入處理，並視網管人員/駐點工程師等人力情況增加巡檢頻率。	8/20 結案

(八) 有效性量測

依契約規定每年 3 月、6 月、9 月、12 月 10 日前，完成 ISMS 有效性量測，填載資訊安全監測項目清單及計畫表。本年度分別於 107 年 3 月 6 日、107 年 6 月 6 日、107 年 9 月 3 日及 107 年 12 月 3 日協助執行貴機關執行有效

性量測作業，並於每季 ISMS 工作小組會議中進行審視完畢，貴機關針對各控制項目皆有效且於時限內完成。

ISMS 目標部分

ISMS 目標	監測方式	監測人員	監測結果	監測週期
通過並維持 ISO27001/CNS27001 驗證	是否通過 ISO27001/CNS27001 驗證及追蹤審查。	德欣寰宇_林世和	追查稽核業於 107 年 11 月 16 日辦理完竣，審查結果通過並維持，符合。	○
確保本中心電腦機房之網路、電力及空調服務，於正常上班時間內因意外或操作錯誤造成無法使用持續達 4 小時以上之次數，每年不得高於 2 次。	統計電腦機房因意外或操作錯誤造成網路、電力及空調服務，無法完全使用之次數。	德欣寰宇_林世和	經檢查相關紀錄，未有因意外或操作錯誤造成網路無法完全使用事件，符合。	○
確保本中心電腦機房因資訊安全事件造成機密等級以上資料外洩事件，每年不得有 1 件。	統計電腦機房因資訊安全事件造成機密等級以上資料外洩次數。	德欣寰宇_林世和	經檢查相關紀錄，未有因資訊安全事件造成機密等級以上資料外洩事件，符合。	○
確保核心資訊系統之可用性，於正常上班時間內因意外或操作錯誤造成無法使用持續達 4 小時以上之次數，每年不得高於 4 次。	統計「資通安全事件通報單」因意外或操作錯誤造成核心資訊系統，無法使用之次數。	德欣寰宇_林世和	經檢查相關紀錄，核心資訊系統於上班時間未有因意外或操作錯誤造成無法使用情形，符合。	○

二、控制措施有效性部分

控制目標	控制措施群組	控制措施	監測方式	監測人員	監測結果	監測日期	監測週期
資訊安全政策	資訊安全之管理指導方針	資訊安全政策文件 資訊安全政策之審查	檢查是否審查 ISMS 政策性文件至少 1 次	德欣寰宇_林世和	於 107 年資訊安全推行小組第 1 次會議審查修正通過 ISMS 政策文件，並依程序發佈實施，未違反。	1071203	○

控制目標	控制措施群組	控 制 措 施	監測方式	監測人員	監測結果	監測日期	監測週期
資訊安全的組織	內部組織	資訊安全之角色及職責	檢查資通安全管理審查會議召開次數： 1. 資訊安全推行小組會議每季至少召開 1 次。 2. ISMS 工作小組會議每季至少召開 1 次。	德欣寰宇_林世和	1.ISMS 工作小組會議，預計第 1 次將於 3 月 19 日召開。 2.資訊安全推行小組會議，預計第 1 次將於 3 月 30 日前召開。	1070306	⊕
					1.ISMS 工作小組會議，預計第 2 次將於 6 月 20 日召開。 2.資訊安全推行小組會議，預計第 2 次將於 6 月 29 日召開。	1070606	
					1.ISMS 工作小組會議，預計第 2 次將於 6 月 20 日召開。 2.資訊安全推行小組會議，預計第 2 次將於 6 月 29 日召開。	1070903	
		職務區隔 與權責機關之聯繫 與特殊關注方之聯繫			1. ISMS 工作小組會議，第 3 次已於 9 月 20 日召開，未違反。 2. 資訊安全推行小組會議，第 3 次已於 9 月 25 日召開，未違反。	1071203	
		專案管理之資訊安全	每年抽查 1 次本中心資訊安全管理系統範圍內各項計畫內容是否有資訊安全相關管理內容，不得有 1 件違反。	德欣寰宇_林世和	抽查 107 年度國土測繪圖資 e 商城資訊系統營運持續演練計畫內容，操作時間與計畫相符，未違反。	1071203	○
	行動裝置及遠距工作	行動設備的政策	檢查使用行動設備均有進行申請，不得有 1 件違反。	德欣寰宇_林世和	目前未開放行動設備使用內部網路上網，未違反。 抽查發現資訊服務申請表 1070517004 申請	1070606	⊘

控制目標	控制措施群組	控 制 措 施	監測方式	監測人員	監測結果	監測日期	監測週期
					作業期間 107 年 5 月 18 日至 108 年 12 月 31 日止，呈豐科技股份有限公司以遠端辦理維護測繪知識網 (含保固期限)並附安全防護變更申請單、遠端登入使用申請表及防火牆異動申請單，未違反。		
					近半年並未有行動設備使用申請，無違反。經查無發現非授權人員非法存取，另抽查遠端登入使用申請表 107010504（遠端使用起訖時間為 107 年 1 月 5 日至 107 年 12 月 31 日），依規定辦理，未違反。	1071203	
		遠距工作	檢查是否有非授權人員進行遠距工作，不得有 1 件違反。	德欣寰宇_林世和			
人力資源安全	聘僱前	篩選	檢查因人為疏失或錯誤操作導致設備故障之次數，不得有 2 次違反	德欣寰宇_林世和	抽查「異常事件通知處理單」紀錄編號：107107051502 未發現因人為疏失或錯誤操作導致設備故障。	1070606	⊘
		聘用條款及條件			抽查「主機異常通知單」未發現因人為疏失或錯誤操作導致設備故障，未違反。	1071203	
	聘用期間	管理階層責任	檢查各級人員資訊安全相關上課時數： 1. 每年資安人員（資訊人員）至少１人次須接受 12 小時以上資安專業課程訓練或資安職能訓練。	德欣寰宇_林世和	檢視資安教育訓練統計資料 1. 資安人員(資訊人員)12 小時以上教育訓練，已於 5 月 16 日及 5 月 22 日完成資安專業教育訓練。	1070606	⊘

控制目標	控制措施群組	控 制 措 施	監測方式	監測人員	監測結果	監測日期	監測週期
			2. 每年一般使用者與主管至少須接受 3 小時資安宣導課程並通過程評量。		2. 3 小時資安宣導課程寄 539 人，截至 6 月 6 日寄 537 人完成，並通過評量		
		資訊安全認知、教育及訓練			檢視資安教育訓練統計資料 1. 資安人員(資訊人員)12 小時以上教育訓練，已於 5 月完成資安專業教育訓練。 2. 一般人員 3 小時課程，於 9 月底前辦理完成。	1071203	
		懲處過程					
	聘用之終止及變更	聘用責任之終止或變更	抽查離退人員，帳號是否確實刪除或停用，不得有 1 件違反。	德欣寰宇_林世和	抽查 AD 伺服器使用者帳號 54104，離職人員顏于玲已停用，無違反。	1070606	⊘
					抽查離職人員余建賦，使用者帳號為 15039 已停用，無違反。	1071203	
資產管理	資產責任	資產清冊	抽查資產清冊，內容是否涵蓋新購資產(包含服務類)，不得有 1 件違反。	德欣寰宇_林世和	抽查資產清冊至善樓機房與地籍資料庫機房新購資產已列入，無違反。	1070606	⊘
		資產之擁有權			抽查資產清冊至善樓機房與地籍資料庫機房新購資產均已列入，未違反。	1071203	
		資產之可被接受的使用					
		資產之歸還					
	資訊分級	資訊之分級	抽查機敏性資產是否依機密等級標示，不得有 2 件以上違反。	德欣寰宇_林世和	檢視 107 年度風險評鑑報告(107 年 8 月 1 日)包含設備與資產清冊機密等級為密，檢視弱點掃描處理通知單機密等級為密，未違反。	1071203	○
		資訊之標示					
		資產之處置					

控制目標	控制措施群組	控 制 措 施	監測方式	監測人員	監測結果	監測日期	監測週期
	媒體處置	可移除式媒體之管理 媒體之汰除 實體媒體傳送	檢查儲存媒體汰除，均依規定進行消磁或破壞至無法使用，並記錄於「媒體銷毀作業處理表」不得有 1 件違反。	德欣寰宇_林世和	檢視「媒體銷毀作業處理表」本年度 1 月 8 日有銷毀紀錄，計 101 件電腦硬碟銷毀。	1070606	⊘
					檢視「媒體銷毀作業處理表」，於 107 年 11 月 14 日進行伺服器硬碟計 19 顆消磁作業，均依規定辦理，未違反。	1071203	
存取控制	存取控制之營運要求事項	存取控制政策 對網路及網路服務之存取	抽查重要設備（如：防火牆）之存取權限是否定期審查，不得有 1 件違反。	德欣寰宇_林世和	至善樓機房與地籍資料庫機房之重要設備之存取權限審查作業均於 107 年 3 月 7 日完成，未違反	1070606	⊘
					至善樓機房與地籍資料庫機房之重要設備之存取權限審查作業均於 107 年 10 月 5 日前完成，未違反	1071203	
	使用者存取管理	使用者註冊及註銷 使用者存取權限之配置 具特殊存取權限之管理 使用者之秘密鑑別資訊的管理 使用者存取權限之審查 存取權限之移除或調整	檢查系統特權帳號是否均已申請，不得有 1 件違反。	德欣寰宇_林世和	抽查至善樓機房伺服器主機，確認使用者授權清冊，均已申請，未違反。	1070606	⊘
					抽查至善樓機房伺服器主機使用者授權清冊 WWW-2014 (192.168.10.66)帳號 NLSC\ban 全球資訊網系統服務帳號，未違反。	1071203	
	使用者責任	秘密鑑別資訊之使用	抽查是否設定螢幕鎖定並以密碼保護，不得有 1 件違反。	德欣寰宇_林世和	抽查電腦 (192 .168.150.21)，以 AD 登入並套用 GCB，設定螢幕鎖定	1070606	⊘

控制目標	控制措施群組	控 制 措 施	監測方式	監測人員	監測結果	監測日期	監測週期
					並以密碼保護，未違反。		
					抽查電腦(192 .168.220. 4)，需使用 AD 登入（密碼保護），並已套用 GCB 設定(螢幕鎖定)，未違反。	1071203	
	系統及應用存取控制	資訊存取限制	檢查發生非授權人員非法存取網路成功件數，不得有 1 件成功。	德欣寰宇_林世和	抽查防火牆 Log，107 年 6 月 6 日 08:58~09:15 00(192.168.10.9)，已有遠端服務申請，經查無發現非授權人員非法存取網路成功事件，未違反。	1070606	⊘
		保全登入程序			經查無發現非授權人員非法存取網路成功事件，另抽查防火牆 Log，107 年 11 月 5 日紀錄(192.168.10.34)，已有遠端服務申請，未違反。	1071203	
		通行碼管理系統					
		具特殊權限公用程式之使用					
		對程式源碼之存取控制					
實體及環境安全	保全區域	實體安全周界	抽查「電腦機房(操作室)人員進出登記簿」是否確實填寫，不得有 1 件以上違反。	德欣寰宇_林世和	抽查至善樓機房之 107 年 2 月份「電腦機房人員進出登記簿」，發現「資訊服務申請表」(107020701)冷氣維護，由本中心人員陪同廠商進入機房，且該廠商人員有登錄在登記簿上，未違反。	1070306	⊕
					抽查至善樓機房之 107 年 5 月份「電腦機房人員進出登記簿」，發現「資訊服務申請表」	1070606	

控制目標	控制措施群組	控 制 措 施	監測方式	監測人員	監測結果	監測日期	監測週期
					(107053001)展昇裝機，由本中心人員陪同廠商進入機房，且該廠商人員有登錄在登記簿上，未違反。		
					抽查至善樓機房之 107 年 8 月份「電腦機房人員進出登記簿」，發現「資訊服務申請表」(107081602)隆業興環控檢修，由本中心人員陪同廠商進入機房，且該廠商人員有登錄在登記簿上，未違反。	1070903	
					抽查至善樓機房之 107 年 11 月份「電腦機房人員進出登記簿」，發現「資訊服務申請表」(107110501)冷氣維護，由本中心人員陪同廠商進入機房，且該廠商人員有登錄在登記簿上，未違反。	1071203	
		實體進入控制措施					
		保全之辦公室、房間及設施					
		防範外部及環境威脅					
		於保全區域內工作					
	設備	設備安置及保護	檢查以下項目： 1. 機房設備須安置於機架上，不得有 1 件違反。 2. 資訊設備汰除是否依規定清除儲存設備資料，不得有 1 件違反。	德欣寰宇_林世和	1. 經查機房設備均固定於機架上。 2. 經查汰除之設備，均依規定清除儲存設備資料，未違反。	1071203	○
		支援的公用服務事業					
		佈纜安全					
		設備維護					
		資產之攜出					
		設備汰除或再使用之保全..					
		桌面淨空與螢幕淨空政策					
		文件化運作程序				1071203	○

控制目標	控制措施群組	控 制 措 施	監測方式	監測人員	監測結果	監測日期	監測週期
運作安全	運作程序及責任	變更管理 容量管理 開發、測試及運作環境之區隔 .	抽查重要設備是否實施容量監控，不得有 1 部設備未納入。	德欣寰宇_林世和	抽查至善樓機房及地籍資料庫機房之 107 年 11 月份「機房工作日誌」，已實施容量監控，未違反。		
	防範惡意軟體	防範惡意軟體之控制措施	檢查發生中毒或遭植入木馬程式，造成內部網路無法正常運作之事件數，不得有 3 件以上。	德欣寰宇_林世和	OfficeScan 防毒軟體伺服器本機雲端病毒碼版本 14.295.00，抽查控制測量課(吳峻宇電腦)本機雲端病毒碼版本 14.295.00 相符，抽查電腦主機 (192.168.0.23) 本機雲端病毒碼版本 14.295.00 相符，尚無發現中毒或遭植入木馬程式，造成內部網路無法正常運作之事件，未違反。	1070606	⦸
					OfficeScan 防毒軟體伺服器本機雲端病毒碼版本 14.649.00，抽查委外人員辦公室(陳 o 原電腦)本機雲端病毒碼版本 14.649.00 相符，抽查電腦主機 (192.168.10.7)e-map2 主機雲端病毒碼版本 14.649.00 相符，未發現中毒或遭植入木馬程式，造成內部網路無法正常運作之事件，未違反。	1071203	
	備份	資訊備份	抽查使用備份媒體執行回復資料作業是否	德欣寰宇	107 年 2 月執行主機備份資料還原作業，成功	1070606	⦸

控制目標	控制措施群組	控 制 措 施	監測方式	監測人員	監測結果	監測日期	監測週期
			正常，無法正常執行作業件數不得多於 1 件。	_林世和	還原相關資料。未違反。		
					107 年 8 月執行 Cris、Whgis 等 2 部主機之備份資料進行備份回存還原作業，成功還原相關資料。未違反。	1071203	
	存錄及監視	事件存錄	每季抽查 1 次側錄系統 LOG 是否進行備份並提報會議審查，不得有 1 件違反。	德欣寰宇_林世和	側錄系統 DB 為 MS-SQL 每日備份，經抽查皆有成功備份，並於每月工作報告中提出審查，無違反。	1070306	⊕
					側錄系統 DB 為 MS-SQL 每日備份，經抽查皆有成功備份，並於每月工作報告中提出審查，無違反。	1070606	
					側錄系統 DB 為 MS-SQL 每日備份，經抽查皆有成功備份，並於每月工作報告中提出審查，無違反。	1070903	
					側錄系統 DB 為 MS-SQL 每日備份，經抽查皆有成功備份，並於每月工作報告中提出審查，無違反。	1071203	
		日誌資訊之保護 管理者及操作者日誌 鐘訊同步	抽查重要設備的時間是否均已同步，不得有 1 件違反。	德欣寰宇_林世和	抽查內部行政伺服器，時間已與本中心 NTP 伺服器同步，無違反。	1071203	○
	運作中軟體之控制	對運作中系統之軟體安裝	抽查運作中系統是否有變更的文件化紀錄，不得有 1 件違反。	德欣寰宇_林世和	抽查國土測繪差假管理與派車申請系統，擴充功能安裝主機，有資訊服務申請表、上線作業	1070606	⊘

控制目標	控制措施群組	控 制 措 施	監測方式	監測人員	監測結果	監測日期	監測週期
					紀錄表等文件化紀錄，無違反。		
					抽查防毒伺服主機進行更版轉移作業，有資訊服務申請表、上線作業紀錄表等文件化紀錄，無違反。	1071203	
	技術脆弱性管理	技術脆弱性管理	抽查每季是否執行弱點掃描，不得有 1 季未執行。	德欣寰宇_林世和	第 1 季於 107 年 2 月 27 日確實執行弱點掃描，未有違反。	1070306	⊕
					第 2 季於 107 年 6 月 22 日確實執行弱點掃描。	1070606	
		對軟體安裝之限制			第 3 季於 107 年 8 月 31 日確實執行弱點掃描。	1070903	
					第 4 季於 107 年 10 月 31 日確實執行弱點掃描。	1071203	
	資訊系統稽核考量	資訊系統稽核控制措施	檢查執行弱點掃描或滲透測試是否事先取得書面的同意，不得有 1 件違反。	德欣寰宇_林世和	於 107 年 10 月 1 日至 107 年 10 月 19 日進行網站弱點掃描作業，已於 9 月份於工作會議提出，未違反。	1071203	○
通訊安全	網路安全管理	網路控制措施	檢查是否每月分析網路異常使用，不得有 1 個月未執行。	德欣寰宇_林世和	檢查「主機系統暨個人電腦等軟硬體設備委外服務案」107 年 2 月報資料，報告中確實針對中毒電腦及網路流量進行異常分析，未違反。	1070306	⊕
					檢查「主機系統暨個人電腦等軟硬體設備委外服務案」107 年 5 月報資料，報告中確實針對	1070606	

控制目標	控制措施群組	控 制 措 施	監測方式	監測人員	監測結果	監測日期	監測週期
					中毒電腦及網路流量進行異常分析，未違反。		
					檢查「主機系統暨個人電腦等軟硬體設備委外服務案」107 年 7 月報資料，報告中確實針對中毒電腦及網路流量進行異常分析，未違反。	1070903	
		網路服務之安全			檢查「主機系統暨個人電腦等軟硬體設備委外服務案」107 年 10 月報資料，報告中確實針對中毒電腦及網路流量進行異常分析，未違反。	1071203	
		網路之區隔					
	資訊傳送	資訊傳送政策及程序	抽查是否有未經授權之資料交換情形，不得有 1 件違反。	德欣寰宇_林世和	經查未發現有未經授權之資料交換情形，未違反。	1071203	○
		資訊傳送協議					
		電子傳訊					
		機密性或保密協議					
系統獲取、開發及維護	資訊系統之安全要求事項	資訊安全要求事項分析及規格	抽查資訊系統招標資料，是否明訂資訊安全要求與規格，不得有 1 件違反。	德欣寰宇_林世和	抽查『107 年度測繪資料智慧雲端加值服務擴充採購案』，已於徵求建議書內明列【保密責任】履約期間所知悉之機關機敏資料或任何不公開之文書、圖畫、消息、物品或其他資訊，均應保密，不得洩漏，並應提交「資訊安全、個人資料保護及保密切結書（廠商）」及參與專案成員之「資訊安全、個人資料保護及保	1071203	○
		保全公共網路之應用服務					
		保護應服務交易	抽查線上交易服務系統，是否有未經授權之變更，不得有一件違反。				

控制目標	控制措施群組	控 制 措 施	監測方式	監測人員	監測結果	監測日期	監測週期
					密切結書（個人）」，未違反。		
	於開發及支援過程中之安全	系統變更控制程序 運作平台變更後，應用之技術審查 軟體套件變更之限制 系統驗收測試	抽查軟硬體異動是否事先提出申請（資訊服務申請表）核可後始可變更，不得有 1 件以上違反。	德欣寰宇_林世和	抽查資訊服務申請表 107051601 NLSCEMAP0 (192.168.10.40)，符合作業程序要求，無發現不符合事項，未違反。	1070606	⃠
					抽查資訊服務申請表 107082101 QNAP (192.168.0.100)，符合作業程序要求，無發現不符合事項，未違反。	1071203	
		保全系統工程原則 保全開發環境 委外開發 系統安全測試	抽查核心資訊系統開發維運紀錄，是否遵循資訊安全要求與規格，不得有 1 件違反。	德欣寰宇_林世和	經檢查相關紀錄，開發維運記錄皆遵循資訊安全要求，未違反。	1071203	○
	測試資料	測試資料之保護	抽查作業系統變更上線時，測試資料是否予以保護，不得有 1 件違反。	德欣寰宇_林世和	107 年 1 月至 6 月未有系統變更上線作業。	1070606	⃠
					107 年 7 月至 12 月未有系統變更上線作業。	1071203	
供應者關係	供應者關係中之資訊安全	供應者關係之資訊安全政策 於供應者協議中闡明安全性 資訊及通訊技術供應鏈	抽查委外契約，有否確實簽署保密協議，契約中有否註明資訊保密條款，不得有 1 件違反。	德欣寰宇_林世和	抽查「107 年及 108 年度資訊安全服務及管理系統維運採購案」已確實簽署保密協議，契約中亦註明資訊保密條款，未有違反。	1071203	○
	供應者服務交付管理	供應者服務之監視及審查 管理供應者服務之變更					

控制目標	控制措施群組	控 制 措 施	監測方式	監測人員	監測結果	監測日期	監測週期
資訊安全事故管理	資訊安全事故及改善之管理	責任及程序 通報資訊安全事件	抽查發生資安事件未依規定通報之件數，不得有 1 件未通報。	德欣寰宇_林世和	經查 107 年度未發生資安事件，未違反。	1071203	○
		通報資訊安全弱點 對資訊安全事件之評鑑及決策 資訊安全事故之回應 由資訊安全事故中學習 證據之收集	檢查資通安全事件通報單，是否重複發生相同資安事故件數，須少於 1 件。	德欣寰宇_林世和	經查 107 年度未發生資安事件，未違反。	1071203	○
營運持續管理之資訊安全層面	資訊安全持續	規劃資訊安全持續 實作資訊安全持續 查證、審查並評估資訊安全持續	檢查： 1.每年是否執行營運持續計畫演練 1 次以上。 2.每年是否執行風險評鑑 1 次以上。	德欣寰宇_林世和	1. 107 年 6 月 22 日執行國土測繪圖資服務雲及 107 年 7 月 11 日執行國土測繪圖資 e 商城營運持續演練，未違反。 2. 107 年 3 月 27 日及 107 年 8 月 1 日完成風險評鑑共 2 次，符合要求，未違反。	1071203	○
	多重備援	資訊處理設施之可用性	檢查是否辦理回復測試	德欣寰宇_林世和	107 年 2 月 5 日選擇 DNS、GBA、TEMIS 等 3 部虛擬主機之備份資料來進行虛擬主機還原驗證，成功還原相關資料，未違反。	1070606	⊘
					107 年 11 月 8 日辦理國土測繪 e 商城資訊系統異地備援切換測試作業，未違反。	1071203	
遵循性	對法律及契約要求事	適用之法規及契約的要求事項之識別	檢查是否至少 1 次更新「資訊安全法規總覽表」。	德欣寰宇	於 ISMS 工作小組第 3 次會議紀錄討論更新	1071203	○

控制目標	控制措施群組	控 制 措 施	監測方式	監測人員	監測結果	監測日期	監測週期
	項之遵循	智慧財產權		_林世和	「資訊安全法規總覽表」，未違反。		
		紀錄之保護					
		個人可識別資訊之隱私及保護					
		密碼式控制措施之監管					
	資訊安全審查	資訊安全之獨立審查	檢查是否有因違背資訊安全政策導致機敏資料外洩等情事，不得有 1 件違反。	德欣寰宇_林世和	經檢查相關紀錄，未有機敏資料外洩事件，未違反。	1071203	○
		安全政策及標準之遵循性					
		技術遵循性審查					

(九) 第三方驗證

1. 會議簡報及主席講稿

依據契約確認驗證日期(11 月 16 日)後，需於驗證日期前配合本機關辦理外部稽核先期檢驗(10 月 31 日)，並於先期檢驗前 7 天(10 月 23 日)交付啟始會議簡報及主席講稿，已於 10 月 12 日製作並交付。

2. 先期檢驗作業

依據契約確認驗證日期(11 月 16 日)後，需於驗證日期前配合本機關辦理外部稽核先期檢驗，配合貴機關(10 月 31 日)辦理外部稽核先期檢驗，並於結束後辦理矯正作業。

於先期檢驗當日發現有部分表單遺漏，已由機房駐點人員及機房管理人員協助進行矯正作業。

3. 稽核結果報告（第三方驗證機構）及驗證通過證明文件

依據契約應於第三方驗證日(11 月 16 日)次日起 30 天內，交付稽核結果報告（第三方驗證機構）及驗證通過證明文件，稽核結果

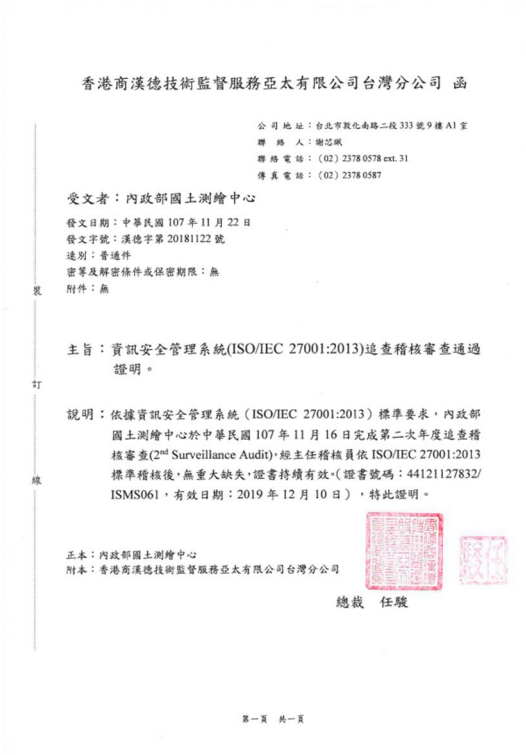
Audit Report (Stage 2) 2018

Organisation National Land Surveying and Mapping Center, Ministry of Interior 內政部國土測繪中心

Audits (ZA): IT-118

TÜV NORD Certification

Master Data of Organisation		
Name of Organisation	National Land Surveying and Mapping Center, Ministry of Interior 內政部國土測繪中心	
Name of corporate group (in case of group certification)	NA	
Street	HO) 4F, No. 497, Liming Rd., Sec.2, 黎明路二段 497 號 4 樓 Server Room 1) 5F, No. 497, Liming Rd., Sec.2, 黎明路二段 497 號 5 樓 Server Room 2) 4F, No.51 , Lane 80, Boai St., 博愛街 80 巷 51 號 4 樓	
Postcode / Town / Country	HO) Taichung City 408, Taiwan (R.O.C.) 台灣 408 台中市南屯區 Server Room 1) Taichung City 408, Taiwan (R.O.C.) 台灣 408 台中市南屯區 Server Room 2) Taichung City 408, Taiwan (R.O.C.) 台灣 408 台中市南屯區	
Contact	Mr. Chen, Jian-Nan 陳建男先生	
E-Mail	54100@mail.nlsc.gov.tw	
Phone/Fax	886-4-22522966 ext 311	N/A
Language	Mandarin 中文	
Scope Description	The information security management of computer center operation in National Land Surveying and Mapping Center, Ministry of the Interior, R.O.C. is applied to network facilities (coreswitches, routers, switches, optical fiber distribution panel), network infrastructure (firewalls, DNS Servers, Anti-Virus gate servers, PCs Anti-Virus servers), environment control equipment, room space, foundation materiality facilities (UPSs, cabinets, air conditioner, firefighting equipment.), and the core systemsdevelopment and maintenance and database's daily maintenance and change requests operation. Statement of Applicability ISMS-02000000, version 2.4 dated 20.07.2017 機房營運之安全管理，本中心機房營運之安全管理，適用於「電腦機房」之網路設備(如核心交換器、路由器、交換器及光纖配接盒)、網路基礎設施(如防火牆、DNS 伺服器、防毒閘道伺服器及個人電腦防毒伺服器)、環境控制設備、機房空間及實體基礎設施(如 UPS、機櫃、空調系統、消防設備等)及核心系統開發及維護作業及資料庫之日常維運與變更申請作	



香港商漢德技術監督服務亞太有限公司台灣分公司 函

公司地址：台北市敦化南路二段 333 號 9 樓 A1 室
聯 絡 人：謝芯帆
聯絡電話：（02）2378 0578 ext. 31
傳真電話：（02）2378 0587

受文者：內政部國土測繪中心

發文日期：中華民國 107 年 11 月 22 日
發文字號：漢德字第 20181122 號
速別：普通件
密等及解密條件或保密期限：無
附件：無

主旨：資訊安全管理系統(ISO/IEC 27001:2013)追查稽核審查通過證明。

說明：依據資訊安全管理系統（ISO/IEC 27001:2013）標準要求，內政部國土測繪中心於中華民國 107 年 11 月 16 日完成第二次年度追查稽核審查(2nd Surveillance Audit)，經主任稽核員依 ISO/IEC 27001:2013 標準稽核後，無重大缺失，證書持續有效（證書號碼：44121127832/ISMS061，有效日期：2019 年 12 月 10 日），特此證明。

正本：內政部國土測繪中心
副本：香港商漢德技術監督服務亞太有限公司台灣分公司

總裁 任駿

第一頁 共一頁

僅提出 6 個建議事項，並未有任何不符合事項，代表貴機關於資訊安全之管理事項皆持續且有效運作，稽核當日即宣布貴機關證書持續有效。

4. 依契約要求，應於第三方驗證日次日起 30 個日曆天完成，11 月 16 日完成第三方驗證並提出共 6 個建議事項，於 11 月 20 日完成因應措施，並於 11 月工作會議（12/6）中提出討論。

二、 資安治理成熟度評估服務

依據契約廠商需於年度專案工作計畫書中，提出規劃建議及預計辦理時程，資安治理成熟度評估作業辦理完竣後，應於 30 天內交付「資安治理成熟度評估報告書」。

本年度依照「105 年國家資通安全防護整合服務計畫」之規則整理評估針對 4 大面向，共 19 個流程構面、83 個檢核項目進行評估，結果為 Level 2 成熟度皆達成能力度 1，成熟度滿足 Level 1，如下表。

流程構面分級原則	流程構面成熟度等級	流程構面	流程構面能力度	機關整體成熟度
Extended Process Set	Level 5	M.1 創新管理	3	Level 2 成熟度皆達成能力度 1，故成熟度滿足 **Level 1**。
	Level 4	P.3 資安風險監控	5	
		M.5 績效與成果監督	5	
	Level 3	P.1 治理架構與政策	3	
		P.2 資安資源確保與監控	3	
		P.4 利害關係人溝通	3	
	Level 2	M.2 目標與計畫管理	3	
		M.3 預算與成本管理	3	
		M.6 資安事故管理與緊急應變	3	
		M.8 供應商管理	1	
		O.1 資訊資產識別與管理	4	
		O.2 存取控制	2	
		O.4 系統獲取、開發及維護	2	
Basic Process Set	Level 1	E.1 角色與權責	3	
		E.2 認知與訓練	4	
		P.5 第三方驗證與內稽	2	
		M.4 風險及安全性評鑑與管理	4	
		M.7 營運持續管理	2	
		O.3 作業與通訊安全管理	2	

三、 資安監控

依據契約提供本專案為 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。

(一) 監控設備：

項次	設備名稱	數量	類別
1	iMPERVA X2010	1	WAF
2	Juniper SRX240	1	防火牆
3	Fortigate 1200D	1	
4	Fortigate 200B	1	
5	Fortigate 310B	1	
6	Dell R320	1	日誌收集器
7	Fortianalyzer 300D	1	
8	PaloAlto 3020	1	APT+IPS
9	Fortigate 200B	1	高雄 IDC 防火牆
10	網路設備+重要系統 Server	21	

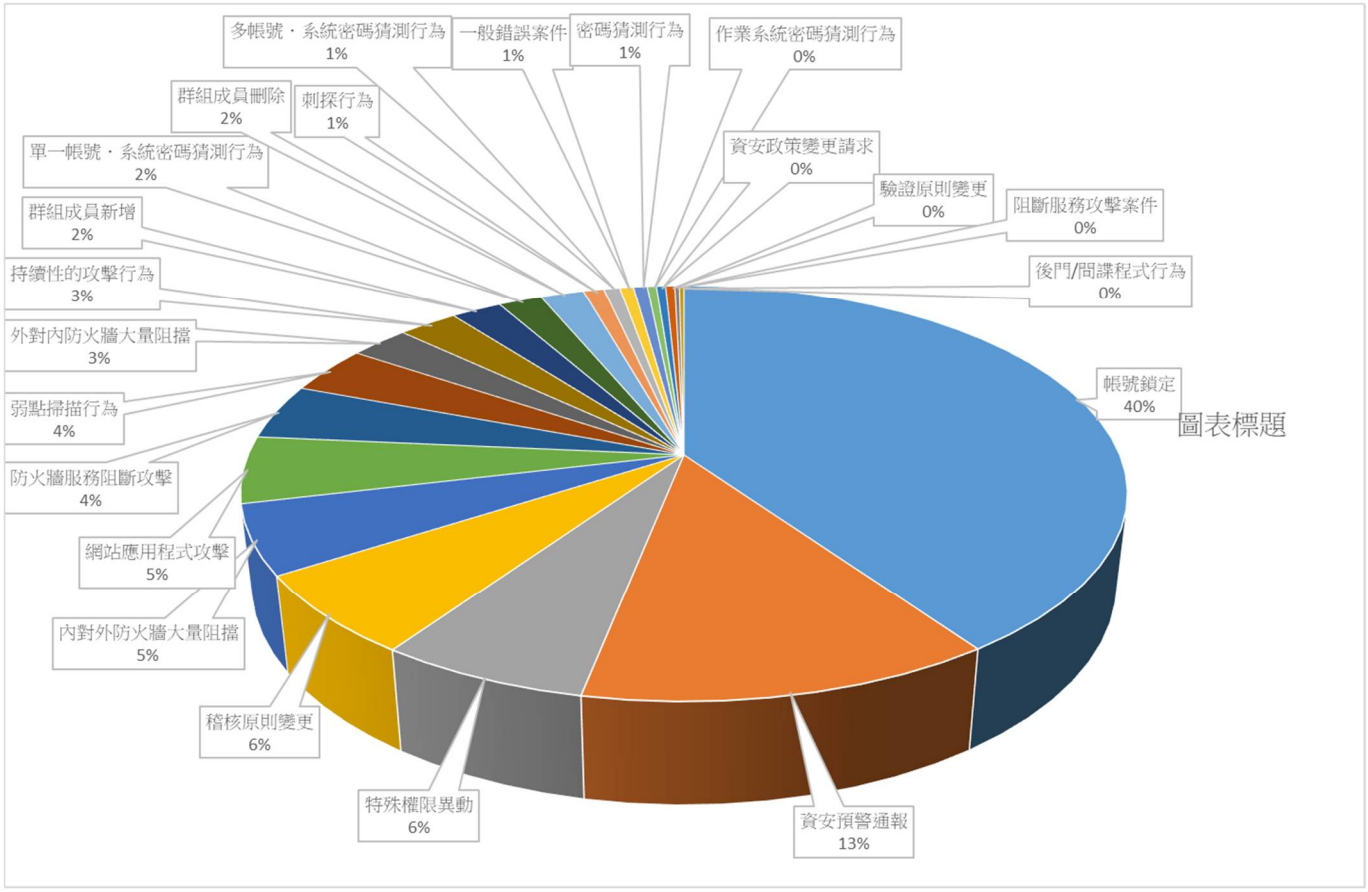
項次	類別	設備名稱	數量
1	WAF	iMPERVA X2010	1
2	Firewall	Juniper SRX240	1
3	Firewall	Fortigate 1200D	1
4	Firewall	Fortigate 200B	1
5	Firewall	Fortigate 310B	1
6	U-Agent	Dell R320	1
7	Firewall reporter	Fortianalyzer 300D	1
8	APT	PaloAlto 3020	1
9	Firewall	Fortigate 200B	1
10	mail	Centos 5.8	1
11	Lucky102	Windows 2012 STD	1
12	Nlsc-dc03	Windows 2012 STD	1
13	Nlsc-dc04	Windows 2012 STD	1

項次	類別	設備名稱	數量
14	orarac1	Oracle linux 5.9	1
15	money	Windows 2008 R2 STD	1
16	SQLCLU1	Windows 2008 R2 ENT	1
17	MDSERVER	CentOS 7.5	1
18	MEMBER	Windows 2012 Standard	1
19	dns	Windows 2012 Standard	1
20	emap3	Windows 2012 Standard	1
21	eservice	Windows 2008 R2 STD	1
22	ngis	Windows 2008 ENT	1
23	SICL	Windows 2008 R2 STD	1
24	WHGIS	Windows 2008 R2 ENT	1
25	www-2014	Windows 2012 Standard	1
26	switch	Cisco C2960S	1
27	Post	Ubuntu	1
28	PIVOT	Windows 2008 R2 STD	1
29	WEB	Windows 2008 STD	1
30	W08sp1-1	Windows 2008 STD	1

(二) 監控時間：1 月 1 日至 12 月 10 日

(三) 事件單發生時間趨勢分析

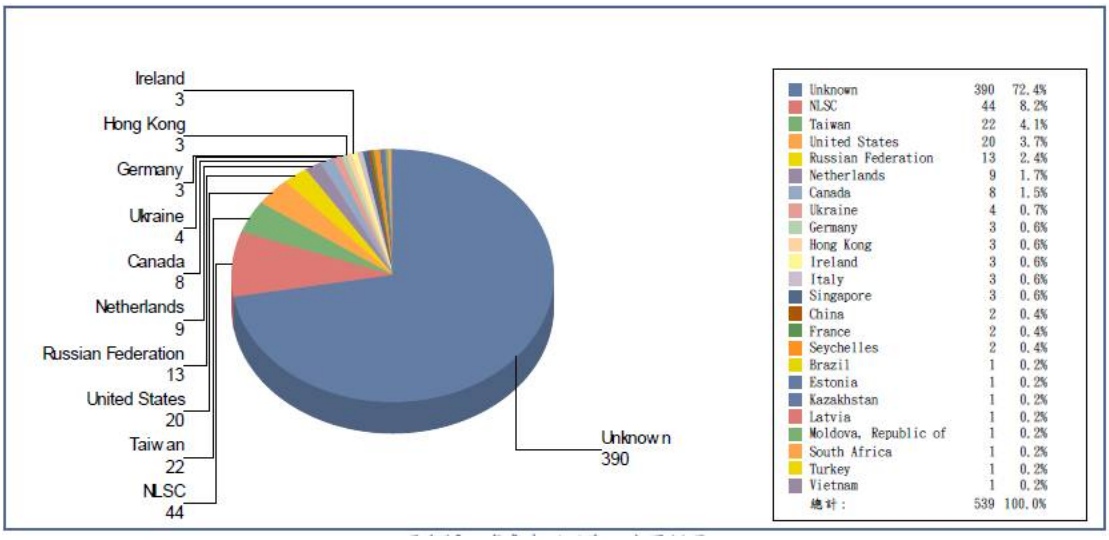
本年共新增 539 則資安通報案件，69 則系統通報案件（預警通報），通報單以「帳號鎖定」為主。



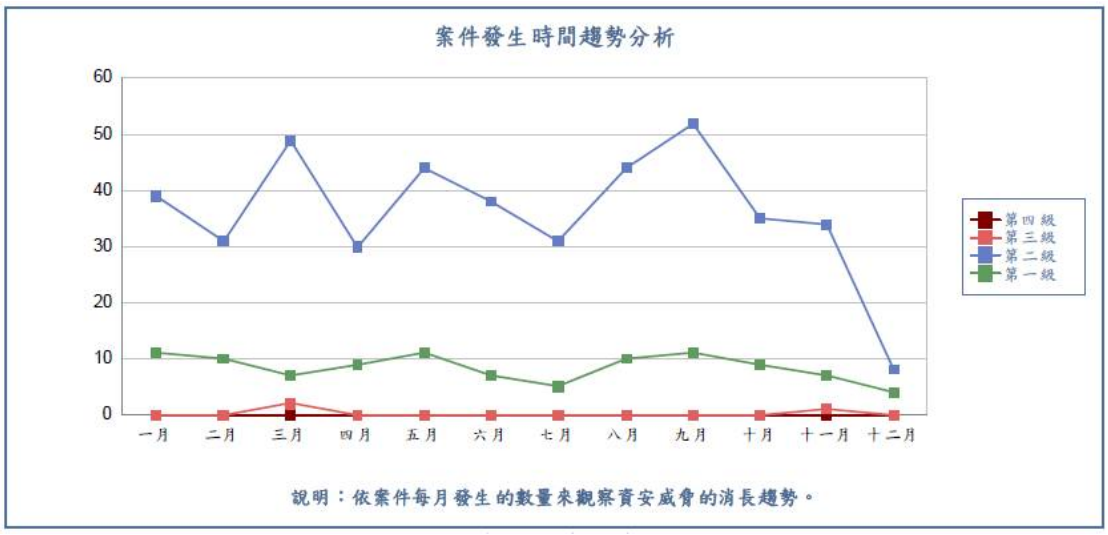
(四) 威脅來源統計

從案件來源統計中可以得知威脅來源的比率。

根據威脅來源比率較大的區域為未來防禦系統部署優先考慮的區域。



(五) 案件趨勢分析



四、 教育訓練

(一) 資安職能研習會

依據契約廠商於各項研習會辦理完竣後 10 天內，提送教育訓練成果及滿意度調查表。

已於本年度 5 月 16 日辦理危機處理、資安防護並於 5 月 17 日交付教育訓練成果及滿意度調查表；5 月 22 日辦理資安防護相關研討會並於 5 月 29 日交付教育訓練成果及滿意度調查表，均於 10 天內交付符合契約要求。

日期	時間	課程名稱	講師	公司名稱
107.05.16 （三）	09:00~12:00 （3 小時）	資訊安全研習會	邱俊傑	德欣寰宇

受訓人員 24 名，其中得 100 分者 16 名，80 分者 8 名。

滿意度調查整體來說有非常滿意有 20 名，滿意有 4 名。

訓練內容	5: 非常滿意	4:滿意	空白

日期	時間	課程名稱	講師	公司名稱

一.講座方面			
教學方式	20	4	
教學內容	20	4	
二.環境方面			
教學環境及設備	13	11	
三.教學活動方面			
1.教材提供	14	10	
2.課程時數安排	15	9	
四.工作相關性			
1.本次講習內容與我的實際工作相關	18	6	
2.本次講習對於我的工作頗有助益	17	7	
五.整體方面	100-90	90-80	
1.我對本次講習整體給予之評分	20	4	
2.我的其他建議: 無			

107.05.16 (三)	14:00~17:00 (3 小時)	資安危機處理研習會	邱俊傑	德欣寰宇

受訓人員 24 名，其中得 100 分者 22 名，80 分者 2 名。

滿意度調查整體來說有非常滿意有 19 名，滿意有 5 名。

訓練內容	5: 非常滿意	4:滿意	空白
一.講座方面			
教學方式	18	3	3
教學內容	17	3	4
二.環境方面			

日期	時間	課程名稱	講師	公司名稱

教學環境及設備	14	10	
三.教學活動方面			
1.教材提供	15	9	
2.課程時數安排	17	7	
四.工作相關性			
1.本次講習內容與我的實際工作相關	18	6	
2.本次講習對於我的工作頗有助益	19	5	
五.整體方面	100-90	90-80	
1.我對本次講習整體給予之評分	19	5	
2.我的其他建議: 無			

107.05.22 (二)	09:00~12:00 (3 小時)	資安防護研習會(一)	陳宏昌	數聯資安

受訓人員 20 名,其中得 100 分者 20 名。

107.05.22 (二)	14:00-17:00 (3 小時)	資安防護研習會(二)	陳宏昌	數聯資安

受訓人員 20 名,其中得 100 分者 20 名。

滿意度調查整體來說有非常滿意有 15 名，滿意有 5 名。

訓練內容	5: 非常滿意	4:滿意	空白
一.講座方面			
教學方式	14	5	1
教學內容	14	5	1
二.環境方面			

日期	時間	課程名稱	講師	公司名稱
教學環境及設備		12	8	
三.教學活動方面				
1.教材提供		13	7	
2.課程時數安排		12	8	
四.工作相關性				
1.本次講習內容與我的實際工作相關		14	6	
2.本次講習對於我的工作頗有助益		14	6	
五.整體方面		100-90	90-80	
1.我對本次講習整體給予之評分		15	5	
2.我的其他建議: 無				

(二) 國際資安專業證照課程

依據契約當年度廠商應視本機關資訊安全人力情形，建議國際資安專業證照課程及參訓人數，並提供總時數 80 小時以上國際資安專業證照課程（含認證考試費用），並於每年 9 月 30 日前交付國際資安專業證照課程上課證明。

已於 04/23-04/27 辦理 SSCP 課程，5/9-11, 5/14-15 辦理 ISO29100 課程，檢附上課證明。

SSCP 課程

ISO29100 課程

五、 資安健診服務

依據契約 107 年需辦理 1 次，提供各項資訊安全項目的檢視服務，其中至少 65 臺個人電腦及至少 20 臺伺服器主機，以提升網路與資訊系統安全防護能力，健診完畢後，應於 30 天內交付「資安健診結果報告書」，提出具體可行之改善建議，以提供後續架構調整及系統強化作業之參考。

已於執行期間 3 月 19 日至 4 月 18 日完成，並於 5 月 11 日交付「資安健診結果報告書」，符合健診完畢後 30 天內交付要求，並持續追查貴機關修正情形，貴機關已於 6 月完成相關更新作業，並於 10 月份機房工作會議討論防火牆白名單設定規則，確認完成後也於 11 月份設定防火牆白名單作業。

項目	內容說明	單位	檢測數量	檢測結果摘要
網路架構檢視	針對網路架構圖進行安全性弱點檢視，檢視之項目包含設計邏輯是否合宜、主機網路位置是否適當及現有防護程度是否足夠	網路架構	1 式	**『至善樓』機房部分** 1 『行政相關系統區域』、『測繪相關系統區域』及『衛星追蹤站暨控制點系統區域』三個區域間是採用 Cisco 6509 核心交換器以 VLAN 方式作區隔，若於此三個網路區域內有提供重要之相關系統服務，建議應再以防火牆設備作介接防護。 2 DMZ 區域內的 WEB 服務有經由 AP 防火牆(WAF)作網頁系統應用層之連線存取的防護，WAF 目前配置於防火牆 DMZ 端與 DMZ 內部交換器間，使所有出入 DMZ 之網路流量皆會經由 WAF 主機，建議可將 WAF 系統主機部署於所需防護之應用系統主機群之前端，以防範 WAF 系統主機發生問題時可能造成其他應用系統服務中斷或影響到 DMZ 主機其他的應用系統服務網路流量之效率。 **『地籍資料庫』機房部分** 1 於 DMZ 區域內包含 WEB 服務系統，建議評估配置 AP 防火牆

項目		內容說明	單位	檢測數量	檢測結果摘要
					(WAF)作網頁系統應用層之連線存取的防護。 2 防火牆 Juniper SRX 240 以單台方式運作，建議配置第二台作線上或非線上備援使用。
有線網路惡意活動檢視	封包監聽與分析	針對有線網路適當位置架設側錄設備，觀察內部電腦或設備是否有對外之異常連線或 DNS 查詢，並比對是否連線已知惡意 IP、中繼站(Command and Control，C&C)或有符合惡意網路行為的特徵 發現異常連線之電腦或設備需確認使用狀況與用途 封包側錄至少以 6 小時為原則，以觀察是否有異常連線	側錄設備	2 台	**『至善樓』機房部分** 部分連線中也有發現有部分之 DNS 查詢及 IP 連線與具有潛在信譽問題之 IP 及 DNS URL 之內容，這些 IP/DNS URL 皆是在 VirusTotal 網站上於最近三個月內尚有信譽問題之分析結果記錄登記存在 **『地籍資料庫』機房部分** 部分連線中也有發現有部分之 DNS 查詢及 IP 連線與具有潛在信譽問題之 IP 及 DNS URL 之內容，這些 IP/DNS URL 皆是在 VirusTotal 網站上於最近三個月內尚有信譽問題之分析結果記錄登記存在
	網路設備紀錄檔分析	檢視網路與資安設備(如防火牆、入侵偵測/防護系統等)紀錄檔，分析過濾內部電腦或設備是否有對外之異常連線紀錄 發現異常連線之電腦或設備需確認使用狀況與用途 網路設備紀錄檔分析以 1 個月或 100 Mbyte 內的紀錄為原則	網路設備	3 台	**IP:192.168.10.250 (Cisco 網路交換器)** 檢視記錄共計 856,607 筆，沒有發現對外之異常連線紀錄，未發現其他資安相關事件記錄。 **IP:192.168.26.252 (Fortigate 200B 防火牆)** 檢視記錄共計 553,177 筆，沒有發現對外之異常連線及其他相關事件紀錄。 **IP:192.168.99.102 (Cisco 網路交換器)** 檢視記錄共計 202,717 筆， 沒有發現對外之異常連線及其他相關事件紀錄。

項目		內容說明	單位	檢測數量	檢測結果摘要
使用者端電腦檢視	使用者端電腦惡意程式或檔案檢視	針對個人電腦進行是否存在惡意程式或檔案檢視，檢視項目包含活動中與潛藏惡意程式、駭客工具程式及異常帳號與群組	使用者電腦	65台	經分析其紀錄，並無發現 Comodo 全球資料庫中已確認的異常活動中與潛藏惡意程式、駭客工具程式，及異常帳號與群組。
	使用者電腦更新檢視	作業系統、Office 應用程式、防毒軟體、Adobe Acrobat、 Adobe flash player 及 Java 應用程式更新檢視			**作業系統：**全部皆已升級至最新版本 **Office 應用程式：**2 台 Client 未更新至最新版本 **Adobe Acrobat：**有 10 台 Client 未更新至最新版本 **Adobe flash player：**有 4 台 Client 未更新至最新版本
	使用者電腦組態設定檢視	針對使用者個人電腦進行電腦組態設定檢測，依行政院國家資通安全會報技術服務中心，官方網站「政府組態基準」專區所公布安全性檢視之內容為主，以確認機關對於組態設定之落實情形。參考網址為 http://www.nccst.nat.gov.tw/GCB。			1 檢測之使用者個人電腦作業系統分別為 Windows 7: 44 台、Windows 8: 1 台及 Windows 10: 20 台共計 65 台。 2 本次採用之 GCB 版本為 Windows 設定對照表 V1.3，發行日期為 107 年 1 月 29 日之最新版本。
伺服器主機檢視	伺服器主機惡意程式或檔案檢視	針對伺服器主機進行是否存在惡意程式或檔案檢視，檢視項目包含活動中與潛藏惡意程式、駭客工具程式及異常帳號與群組	伺服器主機	20台	經分析其紀錄，並無發現 Comodo 全球資料庫中已確認的異常活動中與潛藏惡意程式、駭客工具程式，及異常帳號與群組。
	伺服器主機更新檢視	作業系統、Office 應用程式、防毒軟體、Adobe Acrobat 、Adobe flash player 及 Java 應用程式更新檢視			**作業系統安全性更新：**已升級至最新版本 **Office 應用程式：**未安裝 **防毒軟體：**有 18 台安裝並已更新到最新版本，有 2 台未安裝防毒軟體 1 台未更新到最新版本。 **Adobe Acobat：**有 1 台未更新 **Adobe flash player：**有 4 台未更新

項目		內容說明	單位	檢測數量	檢測結果摘要
安全設定檢視	目錄伺服器(如 MS AD)中群組的密碼設定與帳號鎖定原則	檢視目錄伺服器中，針對 AD 伺服器組態設定，依行政院國家資通安全會報技術服務中心，官方網站「政府組態基準」專區所公布安全性檢視之內容為主，以確認機關對於組態設定之落實情形。參考網址為 http://www.nccst.nat.gov.tw/GCB。 若無 AD 伺服器，可以其他目錄伺服器(如 LDAP)或以個別使用者端電腦檢視方式完成「密碼設定原則」與「帳號鎖定原則」安全設定檢視(使用者端電腦以項次 3 的電腦為範圍)	目錄伺服器	1 台	檢視結果發現伺服器作業系統之設定合規比率為 18.2%及 Internet Explorer 瀏覽器設定的合規比率為 0.60%，請參考政府組態基準(GCB)於伺服器 2012 作業系統與網域控制站與 Internet Explorer 瀏覽器設定 於版本 V1.3 內之相關建議規範設定。
	防火牆連線設定	檢視防火牆的連線設定規則(如外網對內網、內網對外網、內網對內網)是否有安全性弱點，確認來源與目的 IP 與通訊埠連通的適當性(包含設置「Permit All/Any」與「Deny All/Any」等 2 項防火牆檢測規則確認) 。	防火牆設備	7 台	檢視防火牆連線設定 **Fortigate 1200D 防火牆**一台、**Fortigate 1200D-HA 防火牆**一台、**Fortigate 200B 防火牆**一台、**PaloAlto 2020 防火牆一台**、**PaloAlto 3020 防火牆一台**、**地籍資料庫防火牆一台及地籍資料庫備援防火牆一台，共七台**防火牆之連線規則。

本次資安健診服務，未發現立即明顯的資安威脅。請貴中心參考本公司資安健診服務結果建議事項，針對各項可能產生資訊安全威脅評估可能的改善方式，以降低任何可能發生資訊安全問題的衝擊。

六、 滲透測試服務

依契約於 107 年辦理一次，由貴機關指定 5 個對外服務網站為對象，以檢測受測目標在遭遇外部攻擊者攻擊活動時之資安防護能力與執行成效，於執行結束後 30 天內交付結果報告。

初測：

依據 1 月份工作報告紀錄，選定五個資訊系統進行滲透測，並於 4 月 9 日至 4 月 20 日執行滲透測試初測，5 月 15 日交付滲透測試結果報告(初測)。

複測：

於 7 月 16 日-27 日執行複測作業，8 月 2 日交付滲透測試複測報告，內容包含初測弱點矯正追蹤與成效確認，符合執行後 30 天內交付測試結果報告，符合契約規定。

序號	目標		弱點數量			安全風險
			高風險	中風險	低風險	
1	https://www.nlsc.gov.tw (全球資訊網)	初測	0	0	30	低度風險
		複測	0	0	2	低度風險
2	https://maps.nlsc.gov.tw (國土測繪圖資服務雲)	初測	0	1	5	中度風險
		複測	0	1	0	中度風險
3	https://www.egnss.nlsc.gov.tw(e-GNSS 即時動態定位系統入口網)	初測	0	0	3	低度風險
		複測	0	0	0	低度風險
4	https://whgis.nlsc.gov.tw (國土測繪圖資 e 商城)	初測	0	116	5	中度風險
		複測	0	0	2	低度風險
5	https://emap.nlsc.gov.tw (臺灣通用電子地圖服務網)	初測	0	11	1	中度風險
		複測	0	10	1	中度風險

複測報告交付後，於每月工作報告持續追蹤貴機關修補情形，已於 9 月 12 日，各系統管理人員皆已回覆修補完竣。

七、 委外供應商資訊安全實地稽核

依據契約優規每年提供一次委外供應商資訊安全實地稽核，於 11 月 29 日與貴機關簡任技正及承辦人員到「呈豐科技有限公司」進行實地稽核，並於 11 月 30 日交付稽核結果報告。

稽核目的

內政部國土測繪中心(以下簡稱本中心) 依據「107 年制年度核心資訊系統委外供應商稽核計畫」執行 e-GNSS 即時動態定位系統入口網站委外廠商之稽核。

稽核人員安排與分工

一、稽核人員

1. 國土測繪中心 2 名：林簡任技正志清、吳技士峻宇

2. 德欣寰宇：邱顧問立德

二、稽核工作排程

本次稽核工作於 107 年 11 月 29 日執行，實際稽核工作執行內容如下：

查核時間	稽核人員	作業內容	參加人員
10:00～10:10	林簡任技正志清 吳技士峻宇 邱顧問立德	稽核作業說明 (由稽核小組說明)	1.稽核小組成員。 2.受稽核委外廠商專責人員及其主管。
10:10～11:50	林簡任技正志清 吳技士峻宇 邱顧問立德	進行書面及實地稽核	
11:50～12:00	林簡任技正志清 吳技士峻宇 邱顧問立德	稽核發現事項說明 (由稽核小組說明)	

本次稽核結果

一、不符合事項(Non Conformity)

本次稽核無發現不符合事項。

二、建議改善事項(OFI)

建議受稽核公司於平時內部員工宣導資安教育以及個資保護教育時，可以留下相關宣導佐證資料， 例如課程講義，簽到表等。

項次	稽核項目	稽核方式	稽核紀錄	對應標準條款
1. 共同條款				
1.1	供應商須遵循本契約、本中心資訊安全管理制度相關之規定。無規定者，依其他相關法律辦理。	檢視有無違反之情事發生。	玖、資安保密責任、契約中之附加責任等。	ISO 27001 A.15.1.2 供應者協議中之安全的說明
1.2	供應商提供參與專案員工之名單。	檢視專案成員名單。	專案成員吳 O 廷、張 O 傑	ISO 27001 A.15.2.1 供應者服務之監視與審查
1.3	供應商履行契約提供及使用之軟體，均需為合法軟體，不得違反智慧財產權、著作權、及專利法之規定，如有違反致發生事件，承包廠商須承擔所有法律責任。	檢視委外契約條款。由需求單位提供佐證	本案為自行開發，提供及使用之軟體，均需為合法軟體。	ISO 27001 A.15.1.2 供應者協議中之安全的說明
1.4	供應商若需轉包承接之案件，須經本中心書面同意。	檢視委外契約條款。由需求單位提供佐證	本案無轉包。	ISO 27001 A.15.1.3 資訊與通訊技術供應鏈
1.5	供應商所交付之標的物如侵害第三人合法權益時，應由供應商負責處理並承擔一切法律責任。	檢視交付標的物是否有侵害第三人合法權益。	本案為自行開發無侵害第三人合法權益。	ISO 27001 A.15.1.1 供應者安全之資訊安全政策

項次	稽核項目	稽核方式	稽核紀錄	對應標準條款
1.6	供應商如因其員工，或分包供應商執行職務之過失，造成本中心損害，供應廠商需負連帶損害賠償責任。	檢視是否有損害本中心之情事發生。	本案契約書。	ISO 27001 A.15.1.3 資訊與通訊技術供應鏈
1.7	若本中心有相當之事實發現供應商之人員可能涉及違反本契約或其他相關法令規定之行為時，供應商應配合協助本中心調查，並提供所有需要之資料。	檢視是否有違反契約或其他相關法令規定事項之情事發生。	本案契約書。	ISO 27001 A.15.1.3 資訊與通訊技術供應鏈
1.8	接觸公務機密資料之供應商委外人員須參加本中心辦理之資訊安全講習或由供應商提供原單位安全管理教育訓練證明。	檢視訓練簽到表或訓練證明	專案成員吳 O 廷先生、張 O 傑先生到職宣導	ISO 27001 A.7.1.2 聘僱條款與條件
2. 資訊安全管理條款				
2.1	供應商專案成員因遵循本中心 ISMS 管理程序填寫相關切結書資料並確實遵守保密之協定。	檢視保密協議 由採購單位提供佐證	專案成員吳 O 廷先生、張 O 傑先生員工保密切結	ISO 27001 A.7.1.2 聘僱條款與條件
2.2	供應商更換專案人員應提供資歷供本中心審查，並經本中心書面同意後，始得更換。	檢視專案成員異動紀錄及異動同意書。 由需求或採購單位提供佐證	本案專案人員仍在職，如更換專案人員依契約書辦理。	ISO 27001 A.7.3.1 聘僱責任之終止或變更
2.3	供應商（含分包供應商）對所提供之資通訊技術服務及產品供應鏈負有安全責任，並應評估其資安風險，不得造成資訊安全事件之發生。	檢視供應商與其合作之分包供應商之資訊安全與個資保護控管措施。	交付軟體已經執行弱點掃描(Acunetix)	ISO 27001 A.15.1.3 資訊與通訊技術供應鏈
2.4		根據異常事件通報單，檢視本計畫之	已設立專人，針對資通安全、異常事件，	ISO 27001 A.16.1.1

項次	稽核項目	稽核方式	稽核紀錄	對應標準條款
	因專案導致之資通安全、異常事件，應配合本中心辦理安全事件緊急處理。	廠商於發生資安事件、異常事件時，是否依「安全事件緊急應變程序書」辦理，並留下紀錄。	配合中心辦理安全事件緊急處理。	職責與程序
3. 硬體採購與維護案				
3.1	硬體設備維修或更新，須經過本中心權責單位同意，並由權責單位公告相關受影響單位後，始得進行維修或更新。	檢視硬體設備維修或更新同意紀錄。	本案無硬體採購。	ISO 27001 A.12.1.2 變更管理
3.2	主機作業系統更新，須經過本中心權責單位同意，並由權責單位公告相關受影響單位後，始得進行維修或更新。	檢視主機作業系統變更同意紀錄。	中心現行作業為 Windows2008，若中心通知異常，由廠商相關人員進行維護。	ISO 27001 A.14.2.2 系統變更控制程序
3.3	主機需要移機時，供應商須配合本中心之作業，提出相關文件。	檢視相關文件。	主機目前正規畫由單臺伺服器移機至虛擬主機，先行確認虛擬機環境，例 CPU、RAM、DISK 空間。107/9/28 確認 OK。	ISO 27001 A.12.1.2 變更管理
3.4	供應商應提供本中心主機管理、維護操作說明書或操作教育訓練。	檢視操作說明書或教育訓練紀錄。	抽驗 105 年已交付 e-GNSS 入口網系統操作手冊。	ISO 27001 A.12.1.1 文件化運作程序
3.5	供應商應提供硬碟、陣列式磁碟機等儲存媒體資料清除工具，該工具需以確保當該設備報廢時，儲存之資料皆已安全清除。	檢視媒體資料清除工具規格。	本案範圍無設備報廢處理。	ISO 27001 A.12.4.3 管理者與操作者日誌存取控制
3.6	提供伺服主機及作業系統之架構、操作、管理、維護等完整之教育訓練課程與技術支援。	檢視伺服主機及作業系統教育訓練課程與技術支援紀錄。	抽驗 105 年 e-GNSS 入口網結案報告同時提供教育訓練。	ISO 27001 A.12.1.1 文件化運作程序

項次	稽核項目	稽核方式	稽核紀錄	對應標準條款
3.7	供應商提供或出租本中心資訊設備或事務機器時，應提供之管理介面具有刪除影像檔案功能之機型，以避免資料外洩並確保安全。	檢視資訊設備或事務機器之管理介面	本案範圍無提供或出租資訊設備或事務機器設備。	ISO 27001 A.15.1.2 供應者協議中之安全的說明
4. 系統開發及維護案				
4.1	在執行系統開發及維護契約中是否要求安全相關要求事項(如：遵循中心之政策與法規)	檢視是否有測試過程及獲取過程之紀錄。	本案契約書。	ISO 27001 A.14.1.1 安全要求分析與規格
4.2	供應商對所提供之應用系統應加入檢查措施，以確保資訊的正確性。	檢視應用系統資訊的正確性檢查措施。	於測試機上先行檢查應用系統設定，以確保系統正確性。	ISO 27001 A.14.2.8 系統安全測試
4.3	供應商進行系統程式測試時，應避免使用真實資料。	檢視測試資料。	於呈豐科技測試機測試。	ISO 27001 A.14.3.1 測試資料的保護
4.4	供應商應提供程式文件版本之控管方式，並確保程式與文件版本之一致性。	檢視程式文件版本之控管方式及版本是否一致。	程式版本已納入控管。	ISO 27001 A.14.2.1 安全開發政策
4.5	供應商應配合本中心業務需要對機敏資料進行加密。	檢視機敏資料是否加密。	經檢視目前提供給中心無機敏資料。	ISO 27001 A.14.2.6 開發環境之安全
4.6	供應商發現系統異常時，應立即通知需求單位。	根據異常事件通報單，檢視本計畫之廠商於發生資安事件、異常事件時，是否依「安全事件緊急應變程序書」辦理，並留下紀錄。	依據中心弱掃發現 e-GNSS 入口網俱 *Cross-site scripting,*XSS 弱點需進行修補，廠商完成修補並提供報告。	ISO 27001 A.16.1.1 職責與程序
4.7	供應商需針對交付之系統出具切結書，保證系統內	檢視相關切結書。	提供系統網頁弱掃，	ISO 27001 A.14.2.6

項次	稽核項目	稽核方式	稽核紀錄	對應標準條款
	不含後門程式及隱密通道。		107/9/4 報告，未發現高、中、低風險，3 項 Information。	開發環境之安全
4.8	資訊系統開發或變更上線前，須進行系統安全性檢測並交付合格檢測報告，以確保供應商已完成系統弱點或漏洞修補。	檢查相關檢測及修補報告	提供系統網頁弱掃，107/9/4 報告，未發現高、中、低風險，3 項 Information。	ISO 27001 A.14.1.3 應用服務交易之保護 A.14.2.8 系統安全測試 A.18.2.3 技術遵循性審查
4.9	系統開發或維護，若涉有夾帶個人資料之網路傳輸，必須透過加密機制傳輸。	檢視個人資料傳遞方式(ex.mail、USB、磁帶傳送)及管控機制	本案系統開發或維護交付之程式以網路傳輸，未含個人資料。	ISO 27001 A.13.2.3 電子傳訊 A.13.2.4 機密性或保密協議個資法
5. 其他建議條款				
5.1	供應商應提供符合本中心要求之專職人員於需求時間派駐本中心服務，負責系統維護、聯絡窗口及電話詢答服務，並解決系統相關事宜；非派駐時段需提供異常狀況通報窗口，並依本中心相關程序辦理異常排除及通報事宜。	檢視駐點人員、異常排除及通報	本案已建立專職人員及聯絡窗口與程式上傳中心為謝 O 俊先生。	ISO 27001 A.16.1.2 通報資訊安全事件
5.2	為保障專案各項設備可用性，供應商應規劃各項設備產品與解決方案（例如採取高可用性、負載平衡、硬體備援、叢集、磁碟陣列等技術），以降低系統服務中斷之發生機率與時間。	檢視設備障礙及處理紀錄	本案未提供硬體設備。目前中心將採用 VM 處理 e-GNSS 入口網，已測試。	ISO 27001 A.17.2.1 資訊處理設施之可用性
5.3				ISO 27001

項次	稽核項目	稽核方式	稽核紀錄	對應標準條款
	開放外單位存取資料，應依本中心作業程序申請並經核准。	檢視外單位存取申請紀錄	依據資訊服務申請單申請呈豐IP=122.117.180.188	A.12.4.3 管理者與操作者日誌存取控制
5.4	供應商應留存異常處理紀錄，本中心得視需要查核。	檢視異常處理紀錄	檢視異常處理紀錄符合契約書要求。	ISO 27001 A.12.4.1 事件存錄
5.5	供應商應定期檢視維護系統之紀錄，隨時掌握系統執行狀況，並適時提供異常狀況警訊。	檢視維護系統之紀錄	如有異常由相關專案人員修改程式或軟體設定。	ISO 27001 A.12.4.1 事件存錄
5.6	依照契約規範，修補系統漏洞，如因該漏洞未修補導致之一切損失或費用由供應商負責賠償；但該漏洞修補會導致系統不正常運作時，得經本中心相關負責人以書面同意免予修補。	檢視漏洞修補紀錄	目前呈豐機房主機為Windows2016 已更新修補，中心 e-GNSS 主機依中心修補作業進行。	ISO 27001 A.18.2.3 技術遵循性審查
5.7	依契約規範提供符合契約要求維護時間。	檢視叫修紀錄	抽查相關要求修復及完工資料 叫修 107/8/14 15:41 完成 107/8/15 11:16 叫修 107/8/22 14:46 完成 107/8/22 16:13 符合契約 48 小時完成	ISO 27001 A.15.2.1 供應者服務之監視與審查
5.8	應依契約書規定配合本中心所辦理之資訊安全與個資保護稽核工作，並針對缺失進行相關改善作業。	檢視稽核紀錄及缺失改善紀錄	本次為第一次資訊安全與個資保護稽核工作，無前次缺失進行相關改善作業。	ISO 27001 A.15.1.1 供應者安全之資訊安全政策
5.9	供應商應就契約標的，提供安全管理教育訓練，教育訓練內容應包含帳號密碼管理、稽核設定、日誌分析、漏洞修補安裝、系統安全管理與設定等。	檢視安全管理教育訓練紀錄	交付控制測量課之105 年期末報告，併行實施對單位之教育訓練。	ISO 27001 A.15.1.1 供應者安全之資訊安全政策

項次	稽核項目	稽核方式	稽核紀錄	對應標準條款
6. 履約管理				
6.1	供應商專案人員是否具備該領域之專業證照，以保證履約交付內容之品質。	檢視專案人相關證照	檢視契約書計畫主持人為吳O廷 國立嘉義大學碩士符合契約書要求。	ISO 27001 A.7.1.1 篩選

建議事項：

建議受稽核公司於平時內部員工宣導資安教育以及個資保護教育時，可以留下相關宣導佐證資料， 例如課程講義，簽到表等。

與會稽核人員	受稽廠商代表

參、效益及統計分析

一、ISMS 文件修正數量統計分析

依據 ISO27001:2013 標準及貴機關執行狀況檢視全部文件（共計 70 件），修正 10 件，新增 1 件，刪除 1 件。

文件階層	檢視件數	修改件數	增加件數	刪除
一階文件	2	0	0	0
二階文件	17	2	0	0
三階文件	6	2	0	0
四階文件	45	6	1	1

二、資安監控異常事件

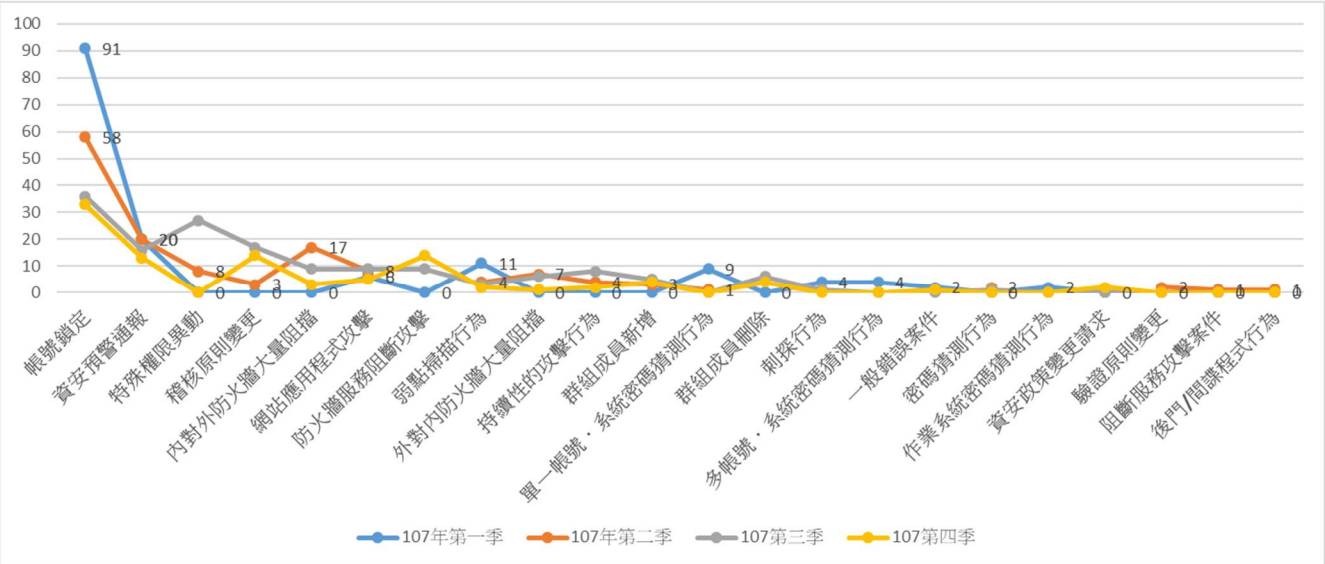
共有 567 件異常事件，均已處理完畢並結案。

異常事件名稱	風險等級		
	第一級	第二級	第三級
帳號鎖定		218	
資安預警通報	69		
特殊權限異動		35	
稽核原則變更		34	
內對外防火牆大量阻擋		29	
網站應用程式攻擊	28		
防火牆服務阻斷攻擊		23	
弱點掃描行為		20	
外對內防火牆大量阻擋		14	
持續性的攻擊行為		14	
群組成員新增		12	
單一帳號．系統密碼猜測行為		10	
群組成員刪除		10	
刺探行為	5		

異常事件名稱	風險等級		
	第一級	第二級	第三級
多帳號．系統密碼猜測行為		4	
一般錯誤案件			3
密碼猜測行為		3	
作業系統密碼猜測行為		2	
資安政策變更請求	2		
驗證原則變更		2	
阻斷服務攻擊案件		1	
後門/間諜程式行為		1	
總計	**104**	**432**	**3**

三、 資安事件統計分析

本年度無發生資安事件，僅提供異常事件統計分析，其中以「帳號鎖定」為多數，由機房駐點人員逐一確認後發現皆為貴機關使用者行為造成；其他外部攻擊等行為亦於貴機關接獲通報當下由網管人員填寫相關表單審核確認後，交由機房駐點人員進行相關資安防護設備調整作業。



肆、改進建議與需求

一、 本年度資訊安全管理系統文件已遵照稽核作業發現事項及平時營運狀態進行調整及修正，並且依據資通安全法子法「資通安全事件通報及應變辦法」修改「資訊安全管理系統事件管理程序」內容，並依據行政院技服中心通報應變流程變動，新增及修改通報表單及流程；明年度將依據資通安全法及相關子法要求事項持續進行相關文件之調整。

二、 本年度資訊資產盤點共執行兩次，發現貴機關機房內部分設備狀態為「關機」，建議可應通知各資產管理人員規劃是否留用，如無需求應進行相關流程，以維持安全管理區域空間之可用性。

三、 本年度營運持續演練標的為核心資訊系統「圖資 e 商城」及非核心資訊系統「圖資服務雲」，皆已順利完成並且符合營運衝擊分析「預計復原時間(RTO)」之目標，建議貴機關須多加宣導各系統管理人員進行系統變更或維護時須遵照相關管理流程，並更新相關文件。

四、 本年度已執行「資訊系統分級與資安防護基準」評估作業，自行建置或委外建置資訊系統產出「資訊系統清冊」共計 22 個系統，其中等級「高」2 個、等級「中」16 個及等級「普」4 個，目前已執行等級「高」之資安防護基準檢視，依據資通安全法子法「資通安全責任等級分級辦法」，本公司將會提供相關表格給貴機關各資訊系統管理人

員，需要請資訊系統等級「中」及「普」之資訊系統管理人員偕同相關維護廠商進行資安防護基準之評估及填寫，以利後續貴機關各資訊系統資安防護之規劃及檢視並達成法規遵循性。

五、 本年度已執行「資安治理成熟度評估」作業，針對 4 大面向，共 19 個流程構面、83 個檢核項目進行評估，評估 Level 2 流程構面「M.8 供應商管理」能力度 1「近兩年機關已有針對資訊系統安全等級為高的資訊供應商進行查核」，已於今年度規劃並完成資訊分級等及「高」之核心資訊系統 e-GNSS 維護廠商查核作業，故能力度等級為 1，建議貴機關可中期規劃逐步提升或短期規劃持續維持流程構面之等級。

六、 本年度 SOC 異常事件通報中等級 3 之通報事件有 3 件，皆為「一般錯誤案件」，數聯資安監控人員於發生當下使用電話及電子郵件方式立即通知貴機關相關承辦人員，貴機關相關承辦人員也於第一時間進行相關處理，並未造成相關資安事件；等級 2 之通報事件以「帳號鎖定」（包含大量帳號鎖定）事件較多，共計 218 件，經貴機關機房駐點人員確認皆屬正常行為，建議貴機關應持續追蹤異常事件發生原因，避免帳號鎖定事件發生。

伍、本專案列管缺失案件辦理情形

無

陸、結語或綜合說明

一、 資訊安全管理系統：遵照 ISO27001:2013 標準及資通安全法等相關資安規定提供貴機關 ISMS 執行及改善等相關建議，協助貴機關執行 ISMS 相關活動（如：風險評鑑、營運衝擊分析、營運持續演練規劃、ISMS 文件修訂、內部稽核、矯正預防及每季 ISMS 有效性量測...等），並協助通過第三方驗證及提出後續矯正預防建議，均已於專案期程內完成。

二、 資安治理熟度評估：依據依照「105 年國家資通安全防護整合服務計畫」之規則評估針對 4 大面向，共 19 個流程構面、83 個檢核項目進行評估，依據評估項目分為 5 個等級，本公司依據貴機關現況評估後能力度為 1，依照時程於評估完畢後繳交相關報告，並提出相關改善建議，由貴機關相關管理人員評估並進行後續改善。

三、 SOC 監控：提供貴機關重要設備及資安設備之 log 監控，於發現異常事件及收到重要資安預警情資時立即通報予貴機關，並於每月工作會議提出相關違反貴機關防火牆規則之檢視及建議，藉以檢討並改善相關內部伺服器設定錯誤及外部可疑威脅來源之排除，逐步發現並排除內外部風險，確保內外部網路之安全性及可用性。

四、 資安健診：依據資安責任等級 B 之應辦事項，每兩年至少執行一次，本年度提供貴機關重要伺服器及網路架構等資通訊服務健康檢

查，並提出相關改善建議，由貴機關相關管理人員評估並進行後續改善。

五、 滲透測試：依據資安責任等級 B 之應辦事項，核心資訊系統每兩年至少執行一次，本年度提供五個 URL 進行滲透測試作業，並提交滲透測試結果報告，由貴機關通知各資訊系統管理人員進行修補作業。

六、 委外供應商資訊安全稽核：依據 ISO27001 部分與系統開發為訊相關控制項目，提出相關稽核查檢表，並擬定計畫提交給貴機關，由貴機關挑選核心資訊系統配合，執行完畢後於當天與受稽廠商確認發現事項，並交付相關稽核報告，均於專案期程內完成。