112 年財團法人台灣網路資訊中心資通安全維護計畫實施情形稽核作業

實地稽核發現事項 - 改善報告（2023/12/21）

項次	內容分類	對應稽核項次	稽核組別	稽核發現內容	改善措施	（預計）完成日期
1	待改善事項	1.1	A	依資通安全責任等級分級辦法第 11 條規定，機關應完成資通系統分級。 1、查機關雖有制作「財團法人台灣網路資訊中心資通系統防護需求分級清冊」惟未依分級原則進行分級，亦無相關評估紀錄，應改善之。 2、查除核心資通系統為高級外，其他資通系統全數為普級，因部份資通系統含有個資，建議全面檢視其妥適性。	本中心資訊系統分級原則及分級程序符合資安法『附表 九、資通系統防護需求分級原則』及『附表十、資通系統防護基準』針對『資通系統分級清冊』規定。 本中心定期於管審會議檢視資訊系統分級妥適性。 有關發現事項第2點本中心已於11月29日由各組重新檢視資訊系統分級妥適性。 （附件：項次01_附件）	已完成
2	法遵符合情形	1.3	A	已依資通安全責任等級分級辦法應辦事項規定，機關取得資訊安全管理系統公正第三方驗證，亦取得個資管理系統公正第三方驗證，值得肯定。	謝謝肯定	已完成
3	建議事項	2.1	A	依資通安全管理法施行細則第 6 條規定，資通安全維護計畫應包含資通安全政策及目標。查機關「資通安全維護計畫」之「I-01-001 資訊安全政策」目標名稱，與「資訊安全	已參考『I-01-001 資訊安全政策』定量化政策目標名稱， 並調整目標名稱與『資訊安全管理指標量測方式說明與結果』一致。	已完成

項次	內容分類	對應稽核項次	稽核組別	稽核發現內容	改善措施	（預計）完成日期
				管理指標量測方式說明與結果」之目標名稱不一致，建議修正之。		
4	法遵符合情形	2.3	A	已依資通安全管理施行細則第 6 條規定，機關已成立資通安全推動組織，並由董事長兼執行長親自主持 111 年及 112 年之 ISMS 管理審查會議，顯示管理階層對於 ISMS 之承諾及支持，值得肯定。	謝謝肯定	已完成
5	建議事項	2.4	A	依資通安全管理法施行細則第 6 條規定，機關應成立資通安全推動組織。查「品質與資安組織之職掌與劃分程序書」5.1.3「資訊安全小組架構圖」組織表僅限核心系統成員，惟 ISMS 管理審查會議之出席人員亦包含非核心資通系統成員，建議修正之。	將額外邀請非核心資通系統成員出席 ISMS 管理審查會議。 依資安法規定僅核心系統須通過ISMS第三方驗證，本中心目前經費編列額度無法將全中心納入ISMS第三方驗證，因此短期內ISMS不會納入全中心範圍，也不會修改程序書。	已完成

項次	內容分類	對應稽核項次	稽核組別	稽核發現內容	改善措施	（預計）完成日期
6	待改善事項	4.1	B	依資通安全管理法施行細則第 6 條規定，機關應盤點資訊及資通系統，並標示核心資通系統及相關資產。查「資訊資產清冊」未標示核心資通系統，應改善之。	本中心將於『資通系統分級清冊』中，加入用於識別核心資通系統之資訊，並適切識別之。	已完成
7	建議事項	4.1	B	依資通安全管理法施行細則第 6 條規定，機關應盤點資訊及資通系統， 並標示核心資通系統及相關資產。查「資訊資產清冊」未註明資產之使用者，建議改善之。	本中心將於「資訊資產清冊」中，加入用於識別資產使用者之欄位資訊，並適切識別之。	已完成
8	建議事項	4.5	B	依資通安全責任等級分級辦法資通系統防護基準規定，機關應訂定系統備份之 RPO 值及備援 RTO 值。查「資訊備份作業說明書」，雖以 Oracle golden gate 加密傳輸方式進行資料同步，惟未明確規定同步之時間，無法滿足「台灣網路資訊中心資通系統防護需求分級清冊」之核心資通系統RPO 值為 1 小時之規定，建議改善之。	Oracle golden gate 之資料同步為即時作業，已符合 RPO 值為 1 小時之規定。後續可依據建議事項考量調整相關程序規範以避免模糊空間。	已完成
9	待改善事項	5.2	B	依資通安全管理法第 9 條規定，應於徵求建議書文件(RFP)相關採購文件中明確規範防護基準需求。查機關未將防護基準需求納入RFP中，應改善之。	已修改相關程序書，將防護基準納入。 Q-02-020 委外安全管理程序書_v1.2， 5.2.1.1於委外作業前，須進行專案風險評估	已完成

項次	內容分類	對應稽核項次	稽核組別	稽核發現內容	改善措施	（預計）完成日期
					時，應視實際評估結果選列為合約條款要求事項。如屬資通系統之建置、維運或資通服務，須於徵求建議書(RFP)文件明確規範資通安全管理法規範之防護基準需求。	
10	待改善事項	5.11	B	依資通安全管理法施行細則第 6 條規定，資通安全維護計畫應包括資通系統或服務委外辦理之管理措施。查機關之契約書雖訂有保密之約定，惟未要求簽訂個人保密契約書，應改善之。	將根據個別採購活動之特性，評估既有組織對組織之保密約定是否已足夠保障中心權益，若仍有不足，在進一步考量簽訂個人保密約定之時機與作法。 本中心與資安顧問及法律顧問討論皆認為資安法並無明文規定委外案一定要同時簽訂單位及個人保密契約書，依本中心ISMS規定保密契約可為單位或個人，若同時要單位及個人都要簽保密契約實務上會有困難，例如當年行政院委託技服中心對本中心進行技術檢測，技服中心人員就不願簽個人保密契約。	已完成
11	待改善事項	5.15	B	依行政院秘書長 109 年 12 月 18 日院臺護長字第 1090201804A 號函規定，委外廠商不得為大陸廠商、陸籍身分或使用大陸廠牌資通訊產品之使用情形。查機關未於契約中明訂前	行政院函規定之法理基礎為「行政一體」，本中心屬特定非公務機關並不適用「行政一體」法理基礎。本中心可配合相關建議以優於法規要求辦理與執行。	已完成

項次	內容分類	對應稽核項次	稽核組別	稽核發現內容	改善措施	（預計）完成日期
				述規定，應改善之。	Q-02-020 委外安全管理程序書_v1.2， 5.2.1.2 委外廠商不得為大陸廠商、陸籍身分或使用大陸廠牌資通訊產品提供之產品或服務，須考量產品之生產地區(例如:記憶體、硬碟等)、勞務提供地區(例如:程式開發、資料處理等)，以降低資訊資產之潛在風險。	
12	建議事項	6.1	B	依資通安全管理法第 10 條規定，機關應訂定、修正及實施資通安全維護計畫。查「財團法人台灣網路資訊中心資通安全維護計畫」之章節與資通安全署所提供維護計畫範本之章節不一致；另亦無目錄及相關法 規、程序及表單之清單，建議修正之。	本中心所提之維護計畫為依主管機關所提供之範本，主管機關亦已備查本中心所提之計畫相關法規，本中心僅需在主管機關通知之期限內呈報維護計畫，無主動呈報之要求。若主管機關更新範本，本中心將於期限內提報修訂版本。	已完成
13	建議事項	6.2	B	依資通安全責任等級分級辦法應辦事項規定，A 級特定非公務機關每年應辦理內部資通安全稽核 2 次。 1、查「112 年度資訊安全落實度檢查報告」(4/11 至 4/13)，其名稱與「ISMS 內部稽核計畫」不一致。	1. 未來將依據相關建議調整。 2. 將釐清稽核相關規定，以調整留下稽核過程紀錄與簽署之作法。 3. ISO 27001 控制措施包括法律遵循相關領域（A.18），故已包括本中心應遵循之資通安全管理法相關規定之查核， 惟本中心	已完成

項次	內容分類	對應稽核項次	稽核組別	稽核發現內容	改善措施	（預計）完成日期
				2、查該報告僅有查核結果，未留存稽核過程之相關紀錄及簽署。 3、查稽核報告之稽核項目雖以 ISMS 之控制措施為主，惟未將資通安全管理法資安責任分級辦法之應辦事項及防護基準納入稽核項目。 4. 建議改善之。	將進一步評估相關作法以提升稽核項目表達之適切性。 本中心內部稽核為委外辦理，明年度報價單中已包含兩次全中心稽核 （附件：項次13_附件_報價）。	
14	待改善事項	7.4	C	依資通安全責任等級分級辦法應辦事項規定，機關應辦理安全性檢測及資通安全健診。查機關雖已完成安全性檢測及資通安全健診，並移除發現的惡意程式，惟欠缺相關修補作業與驗證程序之佐證文件，應改善之。	未來本中心將針對所有資安事件依 ISMS 進行相關程序， 包括通報及矯正預防措施。 I-02-025 資通安全緊急應變作業程序書_v1.0 5.2.3.2. 外力入侵事件： 1. 病毒感染事件 病毒入侵後，隨時掌握電腦病毒感染最新動態，隔離病毒避免疫情擴散；同時儘速取得所需病毒清除程式，並按病毒修護程序，完成病毒清除及修護復原工作。 2. 駭客攻擊（或非法入侵）事件 (1) 發現（或）被入侵時，立即隔離受入侵系統及拒絕入侵者任何存取動作，如切斷入侵	已完成

項次	內容分類	對應稽核項次	稽核組別	稽核發現內容	改善措施	（預計）完成日期
					者之實體連線或調整防火牆設定等，以阻絕駭客進一步入侵，並迅速啟動備援系統或程序。 (2) 如入侵者已被嚴密監控暨不危害內部（含ＤＭＺ非軍事區）網路安全時，可考慮讓入侵者作有條件的連接，適度允許其繼續動作，並請求技服中心協助追查入侵者 IP 位置；並利用稽核檔案或系統指令、聯合ＩＳＰ公司等方式，追蹤入侵者行蹤。惟一旦入侵者危害到內部（含ＤＭＺ非軍事區）網路安全，則應立即切斷入侵者之實體連線。 (3) 全面檢討網路安全措施、修補安全漏洞或修正防火牆之設定等具體改善補救措施，以防止類似入侵或攻擊情事再度發生。 (4) 正式記錄入侵情形、被駭統計分析及損失評估等資料，以供防護與預警之參考，並向主管機關或檢警單位反應。 5.2.4. 緊急處理措施結束後，需依照「I-02-024 資安事件及事故作業程序書」之後續程序進行。	

項次	內容分類	對應稽核項次	稽核組別	稽核發現內容	改善措施	（預計）完成日期
					5.3. 事後復原 5.3.1. 於緊急處理資安事故後，執行系統復原，保留緊急應變處置過程及復原過程相關紀錄，並應整合組織的業務永續經營計畫（BCP）。 5.3.2. 執行災後復原重建工作，首先應檢驗資通安全環境及硬體設備是否可以正常運作，並執行環境重建、系統復原及掃描作業，其步驟包含軟硬體設備重新取得建置、重置作業系統及應用系統，執行運轉測試等；並俟系統正常運作後即進行安全備份、資料復原等相關事宜。 5.3.3. 在完成復原重建工作後，應將災害應變處置復原過程相關完整紀錄（如資安事件原因分析及檢討改善方案、防止類似事件再次發生之具體方案、稽核軌跡及蒐集分析相關證據等資料），予以建檔管制（如建立資安事件資料庫或列入更新解決方案資料庫等），供爾後查考使用。 5.3.4. 全面檢討檢討確認防護系統之漏	

項次	內容分類	對應稽核項次	稽核組別	稽核發現內容	改善措施	（預計）完成日期
					洞、尋求補強保護方法、修補安全弱點、修正防火牆設定等具體改善措施，以防止類似入侵或攻擊情事再度發生。	
15	待改善事項	7.6	C	依資通安全責任等級分級辦法應辦事項規定，機關應針對電子郵件進行過濾。查機關雖已進行過濾，惟欠缺定期檢討及更新郵件過濾規則相關佐證資料，應改善之。	將郵件過濾規則檢視作業列為定期辦理項目。 將調整程序書及表單，以針過濾規則，進行定期檢視。	2024/02/28
16	建議事項	7.8	C	依資通安全責任等級分級辦法防護基準規定，機關應建立網路服務安全控制措施。查機關雖使用開放原始碼 snort 系統建置入侵偵測系統並採用商用規則，惟欠缺針對 snort 的漏洞追蹤與規則調教佐證資料。若工作負荷過重可考慮引入信譽良好的商業系統，以加強系統漏洞追蹤與規則調教，建議改善之。	評估採購商業系統之可行性，並持續強化 snort 漏洞追蹤與規則調教之落實度。 本中心SOC業務委由中華電信，其中一項工作是針對本中心所使用軟、硬體之安全漏洞追蹤，不論是否採購商業系統(商業系統也會有安全漏洞)，中華SOC之安全通告如下，目前中心在採購商業系統前已先請SOC協助進行漏洞追蹤。 （附件：項次16_附件）	已完成

項次	內容分類	對應稽核項次	稽核組別	稽核發現內容	改善措施	（預計）完成日期
17	待改善事項	7.9	C	依資通安全責任等級分級辦法應辦事項規定，資通安全防護應具有網路防火牆。查機關建置之防火牆數量龐大，雖已針對不同性質網路(動態) 設定不同的防火牆規則，惟欠缺相關定期檢討與有效掌握的佐證文件，應改善之。	本中心將強化定期辦理之防火牆規則檢視作業之成效。	已完成
18	法遵符合情	7.27	C	已針對核心 DNS 服務進行資安防護，除採取相關 DDoS 防護措施(如CDN、TCP 流量清洗) 等標準作法，且已展示其有效性(年度 NS 解析服務可用率達 100%，優於內部政策規範 99.99%) 外，更於公共解析服務上，提供 DNS over TLS 及 DNS over https 等加強隱私的查詢協定，提供更高的安全解析服務，值得讚許。	將持續投入足夠資源以維持管控水準。	已完成
19	待改善事項	8.1, 8.8	C	依資通安全責任等級分級辦法資通系統防護基準規定，系統與服務獲得之控制措施內容應包括系統發展生命週期委外階段，應將安全需求納入委外契約。查機關「ISP 年鑑網站」與「國關組活動網站」之契約書，未依規定將安全需求納入契約，應改善之。	修改相關文件，將安全需求納入。 Q-02-020 委外安全管理程序書_v1.2： 5.2.1.1於委外作業前，須進行專案風險評估時，應視實際評估結果選列為合約條款要求事項。如屬資通系統之建置、維運或資通服	已完成

項次	內容分類	對應稽核項次	稽核組別	稽核發現內容	改善措施	（預計）完成日期
					務，須於徵求建議書(RFP)文件明確規範資通安全管理法規範之防護基準需求。 並同時視案件性質於合約加上「如屬資通系統之建置、維運或資通服務須達成資通安全管理法規範之防護基準需求」條文。 第一條 標的 甲方委託乙方辦理「XXXXXXXXXX」(以下簡稱本專案)。專案內容依甲方審查通過之「委辦『XXXXXXXXXX』整體規劃服務建議書」如附件一專案計畫書(以下稱「計畫書」)，如屬資通系統之建置、維運或資通服務須達成資通安全管理法規範之防護基準需求如附件二。本合約之附件視為合約之一部份，但附件與本合約規定不同時，以本合約為準。	
20	待改善事項	8.2	C	依資通安全責任等級分級辦法資通系統防護基準規定，資通系統開發過程應於安全系統發展生命週期各階段納入資安要求。查機關未依規定訂定相關規範並執行，應改善之。	經檢視系統開發及維護作業程序書，評估已訂定考量資安要求之相關規範。 『I-02-018 系統開發及維護作業程序書』已針	已完成

項次	內容分類	對應稽核項次	稽核組別	稽核發現內容	改善措施	（預計）完成日期
					對資安法進行多次調整並符合相關規範，如下更新紀錄。 v1.8 2019/12/05 PWC/資訊安全小組 依據資安法與程序書差異分析後修訂。6.2.7.4、6.3.1.4 、 6.3.1.5 、 6.3.2 、 6.5.4 、 6.5.5 、 6.6.1.8、6.6.3.2 v1.9 2020/12/25 PWC/資訊安全小組 因應109外稽建議，對應資安法修改普中高描述。 v1.10 2021/11/18 PWC/資訊安全小組 依110年8月23日資安法修正發佈，進行修改。修訂6.2.7.4。	
21	建議事項	8.6	C	依資通安全責任等級分級辦法資通系統防護基準規定，系統發展生命週期測試階段應針對資安等級「普」之資通系統，進行弱點掃描安全檢 測。查機關僅針對部分「普」級之資通系統，於測試階段進行檢測，建議改善之。	將依據相關規範改善之。 T-03-022 弱點管理程序書_v1.1 5.1.1.1. 系統管理者應於系統及程式上線前或依照「政府機關（構）資通安全責任等級分級作業規定」所規定每年資安健檢、弱點掃描及滲透測試之次數進行自行掃描及滲透測試或委由第三方專業服務單位在簽署保密文件後，針對網頁應用程式、主機系統及其他	已完成

項次	內容分類	對應稽核項次	稽核組別	稽核發現內容	改善措施	（預計）完成日期
					內部資訊設備進行資安健檢、弱點掃描及滲透測試，並於掃描後提出弱點掃描及滲透測試報告。 T-03-011 系統開發作業說明書_v1.6 5.2.1 系統安全性測試 5.2.7.1系統上線前由技術組同仁針對系統，委由可信賴之資安廠商，進行程式碼掃描、系統弱點掃描以及滲透測試。	
22	待改善事項	8.10	C	依規定，系統源碼應集中管理於「軟體開發生命週期管理系統」。查機關未建置「軟體開發生命週期管理系統」，卻透過 Gitlab 進行源碼安全管理，且未將所有源碼集中管理，應改善之。	Gitlab 通過持續方法論辦理持續整合、持續交付、以及持續部署，本中心已使用 Gitlab 持續管理之功能落實軟體開發生命週期管理之安全管理，未來將考量擴大 Gitlab 適用範圍，以提升本中心之軟體開發安全。 本中心與顧問公司等討論皆認為gitlab就是一套「軟體開發生命週期管理系統」，網路上搜尋亦可查到一些單位就是使用gitlab作為軟體開發生命週期管理，本中心將持續使用gitlab管理中心所有自行開發之源碼。	已完成

項次	內容分類	對應稽核項次	稽核組別	稽核發現內容	改善措施	（預計）完成日期
23	待改善事項	9.1	C	依資通安全事件通報及應變辦法第 14 條規定，特定非公務機關知悉第3 級或第 4 級資通安全事件後，應召開會議研商相關事宜。查機關「資安事件及事故作業程序書」無制定相關流程，應改善之。	本中心以於 I-02-019 資通安全緊急通報作業程序之 6.1 章節中規範『其中針對 3 與 4 級之資安事故應召開中心內部之事件應變會議(應討論資通安全事故概況、受影響範圍等情事)，並以電話或其他適當方式通報上級機關』。本中心將依相關規定落實之。 I-02-019 資通安全緊急通報作業程序_v1.7 6.1 通報上級機關 當知悉資安事故之發生時，應立即依照「I-02-024資安事件及事故作業程序書」進行資安事故處理，當資通安全處理小組確認最終之資安事故等級後，依照「資通安全管理法」、「資通安全管理法施行細則」與「資通安全事件通報及應變辦法」之規定，「緊急通報窗口」應於知悉資安事故後之一小時內（各系統管理人員於接獲或發現資安事件或事故之時間一小時內），將1~4級之資安事故通報上級機關，其中針對3與4級之資安事故應召開中心內部之事件應變會議(應討論資	已完成

項次	內容分類	對應稽核項次	稽核組別	稽核發現內容	改善措施	（預計）完成日期
					通安全事故概況、受影響範圍等情事)，並以電話或其他適當方式通報上級機關，並填寫「I-04-002資通安全事件通報單」。通報內容至少應包括： 6.1.1 發生事故之機構名稱。 6.1.2 發生或知悉事故的時間。 6.1.3 事故狀況之描述。 6.1.4 事故等級之評估。 6.1.5 因應事故所採取之措施。 6.1.6 外部支援需求評估。 另針對3與4級之資安事故，應定時向事件指揮官、資通安全處理小組成員、上級機關回報控制措施成效。若涉及個人資料外洩，應評估通知當事人之適當方式，依個人資料保護法第十二條規定辦理。	
24	待改善事項	9.2	C	依資通安全事件通報及應變辦法第 15 條規定，機關制訂通報作業規範應包含資通安全事件通報窗口及聯繫方式。查機關「資安事件及事故作業程序書」無明確指定資安事件通報窗口及聯繫方式，應改善之。	本中心將於 ISMS 入口網站明訂資安事件通報窗口及聯繫方式。	已完成

項次	內容分類	對應稽核項次	稽核組別	稽核發現內容	改善措施	（預計）完成日期
						
25	待改善事項	9.14	C	依資通安全情資分享辦法第 6 條規定，應就所接受之情資，辯識其來源之可靠性及時效性，及時進行威脅與弱點分析及研判潛在風險，並採取對應之預防或應變措施。查機關「資通安全威脅情資管理作業程序書」雖有相關規範，惟處理過程無保留相關佐證資料，應改善之。	本中心將依據相關規定留下佐證資料。 請參考附件。 （附件：項次25_附件）	已完成

註:以上改善措施，如需時間才能完成，則填報預估之完成時間。