（受稽機關：財團法人台灣網路資訊中心）

提報113年10月28日資通安全稽核報告所列各項待改善事項辦理情形彙整表

構面	項次	待改善事項	對應稽核項目代碼 註	改善措施	（預計）完成日期
策略面	1	1.依資通安全管理法施行細則第6條規定，機關應盤點資通系統及資訊，並標示核心資通系統及相關資產。查機關資通安全維護計畫之核心業務及重要性表單欄位名稱，未呈現核心業務及核心資通系統；另2024年4月1日之資通系統分級清冊，未記載填表時間及填表人員，建議改善之。 2.依資通安全責任等級分級辦法第11條規定，機關應依資通系統防護需求分級原則完成資通系統分級。查資通系統分級清冊雖已盤點共26個資通系統，惟無證據顯示對各資通系統執行分級評估分析並留存紀錄，建議改善之。	P6(1.1建議事項)	1. 財團法人台灣網路資訊中心『資通安全維護計畫』，項目 "3.1 核心業務及重要性" 項目名稱說明其為核心業務，且於表內也載明此為 "核心業務名稱" 請參考『附件01-資通安全維護計畫_V1.7)』 另2024年4月1日之資通系統分級清冊，已於第三頁之 "本文件歷次變更紀錄" 表格內記載修訂日期及修訂者。請參考『附件02-資通系統分級清冊』 具體彙整填寫人及簽核相關資訊，可參考"簽核文件簡簽47849"『附件03-資通系統分級清冊-簡簽』 2. 重新根據資安法附表九資通系統防護需求分級原則，進行資通系統分級清冊全部26個資通系統之資通系統分級評估，並將填寫相關文件紀錄。如附件『附件04-資通系統分級評估表』。	113年12月31日

	2	依資通安全責任等級分級辦法應辦事項規定，全部核心系統應導入及通過第三方 ISMS 驗證。查機關 ISMS 驗證範圍包括全部核心資通系統及資料託管服務，優於法規。	P6(1.3 優於法遵事項)	謝謝肯定	已完成
	3	依資通安全責任等級分級辦法資通系統防護基準規定，營運持續計畫應包括系統備份，並訂定系統可容忍資料損失之時間要求(RPO)，以及執行系統源碼與資料備份。查機關資通系統分級清冊之 DNS 註冊管理服務及網域管理註冊服務，兩者之 RPO 均為1小時，惟資訊備份作業說明書每天備份3次：上午8點、下午1點及下午8點，不符合 RPO 之規定，應改善之。	C0301(1.4 待改善事項)	修改對應程序書，以符合現況及要求。 程序書 "T-03-008 資訊備份作業說明書_v1.6" 之 "5.2.1 TWNIC 的資料庫" 關於備份作業之內容，將修改如下： 備份時間需參考中心 "系統可容忍資料損失之時間要求(RPO)" 之相關要求進行備份。請參考『附件05-T-03-008 資訊備份作業說明書_v1.7』。	113年12月31日
	4	依資通安全責任等級分級辦法資通系統防護基準規定，營運持續計畫應包括屬中/高等級之系統備援。查資通安全維護計畫2個核心資通系統之 MTPD 為4小時，與資通系統分級清冊2個核心系統之 RTO 為4小時，兩者之時間相同，宜檢視其妥適性，建議改善之。	C0301(1.6 建議事項)	經重新檢視其妥適性，本中心辦理系統回復時，是以回復為正常服務水準(100%)為目標，故 RTO 亦以回復正常服務水準(100%)為設定基礎，故呈現出 RTO 等於 MTPD 之情形。請參考『附件19-BCP2024_EPP-DNS_測試報告』	已完成

	5	依資通安全責任等級分級辦法應辦事項規定，A級機關每年應辦理1次全部核心資通系統BCP演練。查機關業務永續經營計畫測試報告(BCP)未標示2個核心資通系統名稱，亦未先擬定營運持續計畫，應改善之。	P9(1.7待改善事項)	已修改 " I-04-026 業務永續經營計畫測試報告" 表單，已於新表單要求擬定營運持續計畫並明確標示所測試之資通系統名稱標的。請參考『附件06-I-04-026 業務永續經營計畫測試報告_v1.1』	113年12月31日
	6	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安政策及目標。查機關「資通安全維護計畫」將資安政策及目標另訂於「資訊安全政策」，執行結果呈現於「資訊安全管理指標量測方式說明與結果」，惟兩份文件部分內容名稱、測量期間不一致，且缺乏定性目標說明與結果，建議修正之。	P2(2.1建議事項)	根據「資訊安全政策」內容調整「資訊安全管理指標量測方式說明與結果」，使其內容名稱、與測量期間一致，並添加項目11至14說明定性目標之量測方式與結果。調整後文件請詳『附件07-資訊安全管理指標量測方式說明與結果』。	已完成
	7	依資通安全管理法施行細則第6條規定，應辦理資通安全維護計畫與實施情形之持續精進及績效管理機制；另依ISO/IEC 27001之9.1監督、量測、分析及評估之規定，應指派監督及量測、分析及評估之人員及執行時間。查機關資訊安全管理指標量測方式與結果，僅填報監督及量測單位，未依ISO/IEC 27001之指派規定辦理，建議改	P13(2.2建議事項)	經參考 ISO/IEC 27001:2022 9.1監督、量測、分析及評估組織應決定下列事項： (a) 需要監督及量測之事項，包括資訊安全過程及控制措施。 (b) 監督、量測、分析及評估之適用方法，以確保有效的結果。所選擇之方法宜產生	已完成

		善之。		適於比較及可重製視為有效的結果。 (c) 應執行監督及量測之時間。 (d) 應執行監督及量測之人員。 (e) 監督及量測結果應分析及評估之時間。 (f) 應執行分析及評估此等結果之人員。 應具備文件化資訊，作為結果之證據。 組織應評估資訊安全績效及資訊安全管理系統之有效性。 重新檢視 "資訊安全管理指標量測方式說明與結果"，於文件新增監督及量測時間、分析及評估之人員及執行時間，相關調整內容如附件『附件07-資訊安全管理指標量測方式說明與結果』。	
	8	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。查機關113年 ISMS 管理審查委員會均由資安長親自主持，一級主管全部出席，顯示管理階層對於 ISMS 建立、實作、維持及持續改善之承諾及支持。	N10200 (2.3 優於法遵事項)	謝謝肯定	已完成

	9	1.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。查機關「資通安全維護計畫」將資通安全專責人員名單及職掌另訂於「品質與資安組織之職掌與劃分程序書」，查該程序書未說明專責人員名單及職掌，管理代表亦未說明產生方式，建議修正之。 2.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，未明訂管理審查委員會之委員組成，建議改善之。	P3(2.4建議事項)	1. 根據稽核建議，已於新增表單文件定訂資通安全專責人員名單及職掌，請參考『附件08-I-04-001 人員職掌分工表(資安人員)』。 2. 根據稽核建議，增訂5.1.4 管理代表產生方式為由資安長指派，增訂 5.2.2.11 管理審查會議之成員為全中心各組組長。請參考『附件09-Q-02-001 品質與資安組織之職掌與劃分程序書_v2.5』	113年12月31日
	10	依資通安全事件通報及應變辦法第15條規定，機關應建立資通安全事件通報窗口及聯繫方式。查機關雖訂有關鍵系統作業最小資源需求與相關聯絡電話表，惟未完整納入各資通系統之軟硬體廠商及上級機關之聯絡清單，建議改善之。	P9(2.5建議事項)	經討論及檢視，已添加軟硬體廠商及上級機關之聯絡清單，請參考附件『附件10-I-04-024_關鍵系統作業最小資源需求與相關聯絡電話表』	已完成
	11	1.依資通安全責任等級分級辦法應辦事項規定，一般使用者及主管之資通安全教育訓練每年接受3小時以上。查機關人員安全管理與教育訓練程序書雖已明訂新進人員應接受教育	N30103(3.4建議事項)	1. 已於民國113年11月4日，完成進行新進人員資訊安全教育訓練3H。新進人員之相關教育訓練紀錄如附件『附件11-教育訓練簽到表_新進人員』。	已完成

		訓練，惟未留存新進人員之相關教育訓練紀錄，建議改善之。 2.依資通安全責任等級 A 級之特定非公務機關應辦事項，機關應辦理資通安全教育訓練。查機關「資訊安全管理指標量測方式說明與結果」針對教育訓練量測方式為每年資訊安全教育訓練計畫及紀錄，未有計畫相關佐證資料，建議改善之。		2. 相關資安教育訓練紀錄稽核委員已確認，中心均符合資安法相關規定。重新檢視並調整「資訊安全管理指標量測方式說明與結果」文件關於 "6. 應依其職務、責任適當授與全體員工資訊安全相關訓練(每年至少執行一次）。" 之量測方式陳述移除 "計劃" 兩字，減少歧意使其符合現況。相關內容如附件『附件07-資訊安全管理指標量測方式說明與結果』。	
管理面	12	依資通安全管理法施行細則第6條規定，應完成資訊資產盤點。查機關門禁系統及 IPcam 未納入盤點，建議改善之。	P6(4.1 建議事項)	根據稽核建議，已於風險評估與控管表及資訊資產清單第六頁新增監控攝影機與門禁設施。請參考『附件12-風險評估與控管表及資訊資產清單』。	已完成
	13	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。查機關已將相關規定納入「委外安全管理程序書」，惟「IP 推廣資訊系統(IP Apply)」委外案，尚未將防護基準等級(普級)明確	P11(5.2待改善事項)	將調整採購相關 RFP 規範，並列入防護基準等級相關要求。	114年6月30日

		列入 RFP 中，應改善之。			
	14	依資通安全管理法施行細則第4條規定，應訂定資訊作業委外安全管理程序。查機關雖已訂定「委外安全管理程序書」，惟適用範圍未包含委外 IDC、資安檢測等委外作業，建議依業務實際範圍修訂程序書。	P11(5.3建議事項)	根據稽核建議，已於「2.1適用範圍」加入網路「及數據中心(IDC)或雲端服務」及「各項資訊安全檢測服務」請參考『附件 13-Q-02-020 委外安全管理程序書』。	113年12月31日
	15	依資通安全管理法施行細則第4條規定，委外開發系統應請委外廠商提供該系統之安全檢測證明。查「網路治理交流論壇」委外案，RFP 未有相關要求，應改善之。	P11(5.8待改善事項)	將調整採購相關範本，並列入防護基準等級相關要求。	114年6月30日
	16	依資通安全管理法施行細則第4條規定，對委外廠商受託業務之資安作為進行檢視。查未有辦理相關作業之紀錄，應改善之。	P11(5.12待改善事項)	1. 每年度之 ISMS 內部與外部稽核，皆會選定 IDC 機房辦理查核作業。 2. 本中心 PIMS 亦要求須針對各項作業活動委外廠商辦理資料安全保護檢視作業，亦留有檢視「C-04-008 個人資料委外作業查檢表」。請參考『附件 14-C-04-008 個人資料委外作業查檢表』。	已完成
	17	依數位發展部於112年7月6日以電子郵件轉知督導政府捐助財團法人參考資通	P11(5.15建議事	將調整相關契約範本納入資安法相關要求。	114年6月

		訊產品使用原則，公務資通訊產品(含軟體、硬體及服務)不得使用大陸廠牌，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。查機關雖已於「委外安全管理程序書」訂定，惟「2024年度伺服器採購案」未於契約中明訂前述規定，建議於契約範本新增之。	項)		30日
技術面	18	依資通安全責任等級分級辦法應辦事項規定，應辦理安全性檢測。查機關雖已完成核心資通系統部分並擴大至部分非核心資通系統，惟行政部門的部分系統未經技術組確認，仍呈現TLS1.0/1.1弱點，宜統一管理，建議改善之。	N20101(7.4建議事項)	將於近期業務會報決議全中心所有系統之安全性檢測交由技術組負責。	113年12月31日
	19	依資通安全責任等級分級辦法應辦事項規定，應辦理資通安全防護之電子郵件過濾。查機關雖已針對電子郵件進行過濾，並已定期檢討及更新郵件過濾規則，惟欠缺分析文件，建議改善之。	N20703(7.6建議事項)	後續將定期檢討郵件過濾規則時將納入分析資訊。	已完成
	20	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安全防護及控制措施。查機關欠缺定期檢測網路運作環境(防火牆、入侵偵測系統)之安全漏洞相關紀錄，建	N20704(7.8建議事項)	新增表單『T-04-035 定期檢核表』，參考NICS、SOC、CVE 漏洞及資安訊息警訊，針對實體防火牆及入侵偵測系統之網路運作環境定期進行檢測及	113年12月31日

		議改善之。		判斷處置。請參考『附件15-T-04-035 定期檢核表』。	
	21	查電腦機房及重要區域之安全控制、人員進出管控、環境維護(如溫溼度控制)等項目，雖已建立適當之管理措施，惟欠缺監控錄影，建議改善之。	P8(7.16建議事項)	經討論並重新檢視，預計採購攝影機，補強機房管控措施。請參考『附件17-機房攝影機請購單』。	已完成
	22	查使用者電腦訂定軟體安裝管控規則，雖已確認授權軟體及免費軟體之使用情形，並具備定期檢查之紀錄文件，惟可安裝軟體清單部分軟體已過時，建議改善之。	P8(7.23建議事項)	已重新檢視 "中心軟體列表" 軟體使用情形，將未使用之過時軟體移除。並於113年11月11日完成更新。已移除 netscape、icq...，請參考『附件18-software-list』。	已完成
	23	查機關「資通系統分級清冊-全中心」之資通系統名稱編號1為「網域註冊管理服務」，未列出其核心系統與相關支援系統，例如：網域註冊管理系統後台，建議改善之。	P6(8.1建議事項)	經重新討論及檢視「資通系統分級清冊-全中心」文件之「網域註冊管理服務」為多個項目所構建而成，其中「網域註冊管理系統後台」只是其中一個項目，其無法獨立存在，故需整合在「網域註冊管理服務」之下。 「網域註冊管理服務」內的多個項目均有列入『風險評估與控管表及資訊資產清單』進行風險評估及管	已完成

				理，每年內外稽均有透過其進行檢視。請參考附件『附件12-風險評估與控管表及資訊資產清單』	
	24	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-系統發展生命週期測試階段，應執行源碼掃描安全檢測，以及滲透測試安全檢測(資通系統高等級者)。查機關「網域註冊管理服務」之核心系統未見源碼掃描安全檢測結果，應改善之。	N20101(8.6待改善事項)	該系統於十餘年前開發，當時已有進行源碼掃瞄，但目前詢問多家廠商已無提供該程式語言之源碼掃描服務，已建置開源掃瞄系統供內部使用，檢測報告如『附件16-源碼掃描安全檢測報告』。	已完成
	25	依資通安全責任等級分級辦法應辦事項規定，應辦理 SOC 監控機制。查機關監控範圍雖已涵蓋多數資通系統，惟「網域註冊管理服務」之網域名稱查詢與註冊之 XML 格式紀錄未納入 SOC 監控範圍，建議改善之。	N20300(9.8建議事項)	經與 SOC 廠商討論，確認目前已傳送之 LOG 應已足夠。	已完成

請將待改善事項對應所附「參考資料-稽核項目對應代碼表」，查填該欄正確稽核項目代碼。

參考資料-稽核項目對應代碼表

稽核項目	稽核代碼	驗證項目細項
資通安全維	P1	核心業務及其重要性
	P2	資通安全政策及目標之訂定
	P3	設置資通安全推動組織
	P4	專責人力及經費之配置

護計畫實施情形	P5	資通安全長之配置		
	P6	資訊及資通系統之盤點及核心資通系統、相關資產之標示		
	P7	資通安全風險評估		
	P8	資通安全防護及控制措施		
	P9	事通安全事件通報、應變及演練相關機制		
	P10	資通安全情資之評估及因應機制		
	P11	資通系統或服務委外辦理之管理		
	P12	公務機關所屬人員辦理業務涉及資通安全事項之考核機制		
	P13	資通安全維護計畫及實施情形之持續精進及績效管理機制		
資通安全責任等級應辦事項	N10100	管理面	系統分級及防護基準	
	N10200		ISMS 導入及驗證	
	N10300		資安專責人員	
	N10400		內部資安稽核	
	N10500		核心資通系統業務持續運作演練	
	N10600		資安治理成熟度評估	
	N20101	技術面	安全性檢測	弱點掃描
	N20102			滲透測試
	N20201		資通安全健檢	網路架構檢視
	N20202			網路惡意活動檢視
	N20203			使用者端電腦惡意活動檢視
	N20204			伺服器主機惡意活動檢視
	N20205			目錄伺服器設定及防火牆連線設定檢視
	N20300		資通安全威脅偵測管理機制	
	N20400		政府組態基準	
	N20500		資通安全弱點通報機制	
	N20600		端點偵測及應變機制	
	N20701		資通安全防護	防毒軟體
	N20702			網路防火牆
	N20703			具有郵件伺服器者，應備電子郵件過濾機制
	N20704			入侵偵測及防禦機制

	N20705			具有對外服務之核心資通系統者，應備應用程式防火牆
	N20706			進階持續性威脅攻擊防禦措施
	N30101	認知與訓練	資通安全教育訓練	教育訓練-資通安全專職人員
	N30102			教育訓練-資通安全專職人員以外之資訊人員
	N30103			教育訓練-一般使用者及主管
	N30200			資通安全專業證照及職能訓練證書
資通系統防護基準	C0101	存取控制	帳號管理	
	C0102		最小權限	
	C0103		遠端存取	
	C0201	事件日誌與可歸責性	記錄事件	
	C0202		日誌紀錄內容	
	C0203		日誌儲存容量	
	C0204		日誌處理失效之回應	
	C0205		時戳及校時	
	C0206		日誌資訊之保護	
	C0301	營運持續計畫	系統備份	
	C0302		系統備援	
	C0401	識別與鑑別	內部使用者之識別與鑑別	
	C0402		身分驗證管理	
	C0403		鑑別資訊回饋	
	C0404		加密模組鑑別	
	C0405		非內部使用者之識別與鑑別	
	C0501	系統與服務獲得	系統發展生命週期需求階段	
	C0502		系統發展生命週期設計階段	
	C0503		系統發展生命週期開發階段	
	C0504		系統發展生命週期測試階段	
	C0505		系統發展生命週期部署與維運階段	
	C0506		系統發展生命週期委外階段	
	C0507		獲得程序	
	C0508		系統文件	
	C0601	系統與通訊保護	傳輸之機密性與完整性	
	C0602		資料儲存之安全	

	C0701	系統與資訊完整性	漏洞修復
	C0702		資通系統監控
	C0703		軟體及資訊完整性
其他	O01	其他-規範	
	O02	其他-防護	