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報告

數位發展部

中華民國 112 年 11 月

目 錄

壹、依據

依《資通安全管理法》第 17 條第 3 項規定，中央目的事業主管機關得稽核所管第一項特定非公務機關之資通安全維護計畫實施情形，發現有缺失或待改善者，應限期要求受稽核之特定非公務機關提出改善報告。

貳、稽核目的

本部為查核特定非公務機關辦理資通安全管理法及其子法相關法遵事項之落實情形，爰依《資通安全管理法》擬訂本（112）年度稽核計畫，經由外部稽核特定非公務機關資通安全維護計畫實施情形，改善並強化資通安全防護工作之完整性及有效性，以持續精進管理特定非公務機關資安風險。

參、受稽機關

財團法人台灣網路資訊中心

肆、稽核範圍

稽核範圍為受稽機構資通安全維護計畫所包括之全機構及核心資通系統之各項資通安全管理政策、程序等。

伍、稽核小組

本次稽核係依資通安全管理法相關規定，由具資通安全管理、技術或實務專業知識之專家學者及公務機關代表擔任稽核委員、本部派員擔任領隊，組成資通安全維護計畫實施情形稽核小組（稽核小組組成詳表 1）。

表 1、稽核小組組成說明彙整表

成員	人數配置	單位	姓名
領隊	1名	數位發展部資源管理司司長	牛信仁
稽核委員	6名	銓敘部資訊處處長	王復中
		國家科學及技術委員會資訊處副處長	何昇龍
		國家通訊傳播委員會前技監	羅金賢
		財團法人電信技術中心副執行長	林炫佑
		崑山科技大學資訊工程系教授	曾龍
		長庚大學資訊管理系教授	許建隆

陸、稽核行程

112 年 11 月 10 日以實地稽核方式辦理

（地點：財團法人台灣網路資訊中心 3 樓大會議室）。

柒、稽核項目及判定基準

稽核項目係採用資通安全署之 112 年資通安全稽核計畫之實地稽核項目，將《資通安全管理法》及其子法法遵事項，整併為三大構面、九大稽核項目（稽核內容詳如表 2），並依《資通安全管理法》及其子法、國際資訊安全管理系統標準 ISO/IEC 27001:2013 或資訊安全管理系統國家標準 CNS 27001:2014、受稽機關之資通安全維護計畫，以及其他相關規定等據以擬定稽核判定標準。

一、 策略面

(一)核心業務及其重要性：確認資通系統分級、資訊安全管理系統（ISMS）之範圍、機關業務持續之營運衝擊分析、核心資通系統持續運作計畫、業務持續運作演練、備份及備援機制、復原測試等。

(二)資通安全政策及推動組織：確認資安政策及目標、受稽機構之資安管理及運作、資安組織推動、利害關係人管理等。

(三)專責人力及經費配置：確認資安經費及資安人力等資源配置之妥適性、資安/資訊經費占經費比率、資安人力配置情形、資安認知及訓練、資安人員專業證照等。

二、 管理面

(一)資訊及資通系統盤點及風險評估：確認資訊資產盤點及相關管理程序、資訊資產處置規範與異動汰除管控作業、風險評估、風險處理及後續追蹤情形及管理與大陸廠牌資通訊產品之管理措施。

(二)資通系統或服務委外辦理之管理措施：確認資訊作業委外安全管理程序、資訊委外資安要求及服務等級協議、委外人員管理、委外供應商之管理、監督及稽核。

(三)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：機關資通安全計畫訂定、修正及實施情形、內部稽核及後續追蹤、上級/監督/中央目的事業主管機關之監督管理辦理情形。

三、 技術面

(一)資通安全防護及控制措施：確認安全性檢測及資通安全健診實施情形、資通安全弱點通報機制／資通安全防護實施情形、電子資料(含防疫個資)安全管理機制、網路規劃及管理、電腦機房及重要區域管理、資料處理、儲存及傳輸安全、電子資料相關設備管理、行動裝置安全、軟體使用安全、網路即時通訊安全及電子郵件安全等。

(二)資通系統發展及維護安全：確認資通系統之防護需求、SSDLC 各個階段之安全檢核，包括系統需求、設計、開發、測試、驗收時應注意之安全措施、資通系統之變更管制程序等。

(三)資通安全事件通報應變及情資評估因應：確認情資分享機制、資通安全威脅偵測管理機制實施情形、資通系統及相關設備監控事件日誌管理、資安事件通報及應變作業規範及落實、資安事件改善措施之有效性、資通安全演練作業實施情形。

表 2、稽核項目與內容

稽核項目	稽核內容
(1)核心業務及其重要性	
1.1	是否界定機關之核心業務，完成資通系統之盤點及分級，且每年至少檢視1次分級之妥適性？
1.2	是否針對重要業務訂定適當之變更管理程序，且落實執行，並定期檢視、審查及更新程序(如業務調整後對外資訊更新等)？
1.3	是否將全部核心資通系統納入資訊安全管理系統(ISMS)適用範圍？
1.4	是否定期執行重要資料之備份作業，且備份資料異地存放？存放處所環境是否符合實體安全防護？
1.5	是否訂定備份資料之復原程序，且定期執行回復測試，以確保備份資料之有效性？復原程序是否定期檢討及修正？
1.6	資通系統等級中/高等級者，是否設置備援機制，當系統服務中斷時，於可容忍時間內由備援設備取代提供服務？
1.7	業務持續運作計畫是否已涵蓋全部核心資通系統，並定期辦理全部核心資通系統之業務持續運作演練，包含人員職責應變、作業程序、資源調配及檢討改善等？ (A 級機關：每年1次；B、C 級機關：每2年1次)
(2)資通安全政策及推動組織	

2.1	是否訂定資通安全政策及目標，由管理階層核定，並定期檢視且有效傳達其重要性？如何確認人員瞭解機關之資通安全政策，以及應負之資安責任？
2.2	是否訂定資通安全之績效評估方式(如績效指標等)，且定期監控、量測、分析及檢視？
2.3	是否有文件或紀錄佐證管理階層(如機關首長、資通安全長等)對於 ISMS 建立、實作、維持及持續改善之承諾及支持？
2.4	是否指派適當層級人員兼任資通安全管理代表，負責推動及督導機關內資通安全相關事務？是否成立資通安全推動組織，負責推動、協調監督及審查資通安全管理事項？推動組織層級之適切性，且業務單位是否積極參與？
2.5	是否建立機關內、外部利害關係人清單，並定期檢討其適宜性？
(3)專責人力及經費配置	
3.1	資安經費占資訊經費比例？資訊經費占機關經費比例？針對法遵要求作業、稽核或事件缺失改善所需經費，是否合理配置？
3.2	資通安全專責人員配置情形？對應機關自身及對所屬資安作業推動，目前之資安人員配置是否進行合理性評估及因應？ (A 級機關：4位資安專責人員；B 級機關：2位資安專責人員)
3.3	是否訂定人員之資通安全作業程序及權責？是否明確告知保密事項，且簽署保密協議？
3.4	各類人員是否依法規要求，接受資通安全教育訓練並完成最低時數？
3.5	資通安全專責人員是否各自持有資通安全專業證照1張以上，且維持證照之有效性？
(4) 資訊及資通系統盤點及風險評估	
4.1	是否確實盤點資訊資產建立清冊(如識別擁有者及使用者等)，且鑑別其資產價值？
4.2	是否訂定資產異動管理程序，定期更新資產清冊，且落實執行？
4.3	是否建立風險準則且執行風險評估作業，並針對重要資訊資產鑑別其可能遭遇之風險，分析其喪失機密性、完整性及可用性之衝擊？
4.4	是否訂定風險處理程序，選擇適合之資通安全控制措施，且相關控制措施經權責人員核可？是否妥善處理剩餘之資通安全風險？
4.5	核心資通系統是否鑑別可能造成營運中斷事件之機率及衝擊影響，且進行營運衝擊分析(BIA)？是否明確訂定核心資通系統之系統復原時間目標(RTO)及資料復原時間點目標(RPO)？
4.6	針對公務用之資通訊產品，包含軟體、硬體及服務等，是否已禁止使用大陸廠牌資通訊產品？其禁止且避免採購或使用之作法為何？
4.7	機關如仍有大陸廠牌資通訊產品，是否列冊管理？另相關控管措施為何?
(5)資通系統或服務委外辦理之管理措施	
5.1	是否針對委外業務項目進行風險評估，包含可能影響資產、流程、作業環境或特殊對機關之威脅等，以強化委外安全管理？
5.2	是否於採購前識別是否為核心資通系統？並依資通系統分級，於徵求建議書文件(相關採購文件中明確規範防護基準需求？
5.3	是否訂定資訊作業委外安全管理程序，包含委外選商及監督相關規定，確保委外廠商執行委外作業時，具備完善之資通安全管理措施或通過第三方驗證？
5.4	機關及委外廠商是否皆已指定專案管理人員，負責推動、協調及督導委外作業之資通安全管理事項？其負責督導的委外作業資通安全管理事項有哪些？
5.5	是否要求委外廠商配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員？其要求標準為？
5.6	委外業務如允許分包，對分包廠商之資通安全維護措施要求為？如何確認其落實辦

	理？
5.7	對於資通系統之委外廠商，是否針對其人員(如能力、背景等)及開發維運環境之資通安全管理進行評估？
5.8	委外客製化資通系統開發者，是否要求委外廠商提供資通系統之安全性檢測證明，並請其針對非自行開發之系統或資源，標示內容與其來源及提供授權證明？若該資通系統屬核心資通系統或委託金額達新臺幣一千萬元以上者，是否自行或另行委託第三方進行安全性檢測之複測？
5.9	是否訂定委外廠商對於機關委外業務之資安事件通報及相關處理規範？委外廠商執行委外業務，違反資通安全相關法令或知悉資通安全事件時，是否立即通知機關並採行補救措施？
5.10	委外關係終止或解除時，是否確認委外廠商返還、移交、刪除或銷毀履行契約而持有之資料？
5.11	是否訂定委外廠商之資通安全責任及保密規定？
5.12	是否對委外廠商執行受託業務之資安作為進行檢視？其時機及做法為何？針對查核發現，是否建立後續追蹤及管理機制？
5.13	委外廠商專案成員進出機關範圍是否被限制？對於委外廠商駐點人員使用之資訊設備(如個人、筆記型、平板電腦、行動電話及智慧卡等)是否建立相關安全管控措施？是否定期檢視並分析資訊作業委外之人員安全、媒體保護管控、使用者識別及鑑別、組態管控等相關紀錄？
5.14	是否訂定委外廠商系統存取程序及授權規定(如限制其可接觸之系統、檔案及資料範圍等)？委外廠商專案人員調整及異動，是否依系統存取授權規定，調整其權限？
5.15	針對涉及資通訊軟體、硬體或服務相關之採購案、具委外營運公眾場域之委外案，契約範圍內是否使用大陸廠牌資通訊產品?委外廠商是否為大陸廠商或所涉及之人員是否有陸籍身分？是否於契約內明訂禁止委外廠商使用大陸廠牌之資通訊產品，包含軟體、硬體及服務等？
(6)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	
6.1	是否訂定、修正及實施機關資通安全維護計畫，且每年向上級或監督/主管機關提出資通安全維護計畫實施情形？
6.2	是否訂定內部資通安全稽核計畫，包含稽核目標、範圍、時間、程序、人員等？是否規劃及執行稽核發事項改善措施，且定期追蹤改善情形？
(7) 資通安全防護及控制措施	
7.1	是否針對全部核心資通系統定期辦理弱點掃描？ (A 級機關：每年 2 次；B 級機關：每年 1 次；C 級機關：每 2 年 1 次)
7.2	是否針對全部核心資通系統定期辦理滲透測試？ (A 級機關：每年 1 次；B、C 級機關：每 2 年 1 次)
7.3	是否定期辦理資通安全健診，包含網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆設定檢視等？ (A 級機關：每年 1 次；B、C 級機關：每 2年 1 次)
7.4	是否針對安全性檢測及資通安全健診結果執行修補作業，且於修補完成後驗證是否完成改善？
7.5	是否完成下列資通安全防護措施？防毒軟體：A 、B 、C 、D 級網路防火牆：A 、B 、C 、D 級電子郵件過濾機制：A 、B 、C 級入侵偵測及防禦機制：A 、B 級應用程式防火牆 具有對外服務之核心資通系統者))：A 、B 級進階持續性威脅攻擊防禦：A 級

7.6	是否針對電子郵件進行過濾，且定期檢討及更新郵件過濾規則？是否針對電子郵件進行分析，主動發現異常行為且進行改善(如針對大量異常電子郵件來源之 IP 位址，於防火牆進行阻擋等)？
7.7	是否建立電子資料(含防疫個資)安全管理機制，包含分級規則(如機密性、敏感性及一般性等)、存取權限、資料安全、人員管理及處理規範等，且落實執行？
7.8	是否建立網路服務安全控制措施，且定期檢討？是否定期檢測網路運作環境之安全漏洞？
7.9	是否已確實設定防火牆並定期檢視防火牆規則，DNS 查詢是否僅限於指定 DNS 伺服器？有效掌握與管理防火牆連線部署？
7.10	針對機關內部同仁及委外廠商進行遠端維護資通系統，是否採「原則禁止、例外允許」方式辦理，並有適當之防護措施？
7.11	網路架構設計是否符合業務需要及資安要求？是否依網路服務需要區隔獨立的邏輯網域(如 DMZ、內部或外部網路等)，且建立適當之防護措施，以管制過濾網域間之資料存取？
7.12	是否針對機關內無線網路服務之存取及應用訂定安全管控程序，且落實執行？
7.13	資通系統重要組態設定檔案及其他具保護需求之資訊是否加密或其他適當方式儲存(如實體隔離、專用電腦作業環境、資料加密等)？是否針對系統與資料傳輸之機密性與完整性建立適當之防護措施？
7.14	使用預設密碼登入資通系統時，是否於登入後要求立即變更密碼，並限制使用弱密碼？是否是最小權限？是否有使用角色型存取控制？有管理者權限之帳號是否有只用於管理活動？
7.15	是否訂定電子郵件之使用規則，且落實執行？是否依郵件內容之機密性、敏感性規範傳送限制？
7.16	是否針對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)等項目建立適當之管理措施，且落實執行？
7.17	是否定期評估及檢查重要資通設備之設置地點可能之危害因素(如火、煙、水、震動、化學效應、電力供應、電磁輻射或人為入侵破壞等)？
7.18	是否針對電腦機房及重要區域之公用服務(如水、電、消防及通訊等)建立適當之備援方案？
7.19	是否針對資訊之交換，建立適當之交換程序及安全保護措施，以確保資訊之完整性及機密性(如採行識別碼通行碼管制、電子資料加密或電子簽章認證等)？是否針對重要資料的交換過程，保存適當之監控紀錄？
7.20	是否訂定資訊處理設備作業程序、變更管理程序及管理責任，且落實執行？
7.21	是否針對電子資料相關設備進行安全管理(如相關儲存媒體、設備是否有安全處理程序及分級標示、報廢程序等)？
7.22	是否訂定資訊設備回收再使用及汰除之安全控制作業程序，以確保任何機密性或敏感性資料已確實刪除？
7.23	是否針對使用者電腦訂定軟體安裝管控規則？是否確認授權軟體及免費軟體之使用情形，且定期檢查？
7.24	是否針對個人行動裝置及可攜式媒體訂定管理程序，且落實執行，並定期審查、監控及稽核？
7.25	是否訂定網路即時通訊使用原則(如機密公務或因處理公務上而涉及之個人隱私資訊，不得使用即時通訊軟體處理及傳送等)？
7.26	是否訂定即時通訊軟體使用規範、安全需求及購置準則？

7.27	機關所維運對外或為民服務網站，是否採取相關 DDOS 防護措施(例如靜態網頁切換、CDN、流量清洗或建置 DDoS 防護設備等)，並確認其有效性?
(8)資通系統發展及維護安全	
8.1	針對自行或委外開發之資通系統是否依資通系統防護需求分級原則完成資通系統分級，且依資通系統防護基準執行控制措施？
8.2	系統開發過程請是否依安全系統發展生命週期(Secure Software Development Life Cycle, SSDLC)納入資安要求？
8.3	資通系統開發前，是否設計安全性要求，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾等，且檢討執行情形？
8.4	資通系統設計階段，是否依系統功能及要求，識別可能影響系統之威脅，進行風險分析及評估？
8.5	資通系統開發階段，是否避免常見漏洞(如 OWASP Top 10等)？且針對防護需求等級高者，執行源碼掃描安全檢測？
8.6	資通系統測試階段，是否執行弱點掃描安全檢測？且針對防護需求等級高者，執行滲透測試安全檢測？
8.7	資通系統上線或更版前，是否執行安全性要求測試，包含邏輯及安全性驗測、機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾測試等，且檢討執行情形？
8.8	資通系統開發如委外辦理，是否將系統發展生命週期各階段依等級將安全需求(含機密性、可用性、完整性)納入委外契約？
8.9	是否將開發、測試及正式作業環境區隔，且針對不同作業環境建立適當之資安保護措施？
8.10	是否儲存及管理資通系統發展相關文件？儲存方式及管理方式為何？
8.11	資通系統測試如使用正式作業環境之測試資料，是否針對測試資料建立保護措施，且留存相關作業紀錄？
8.12	是否針對資通系統所使用之外部元件或軟硬體，注意其安全漏洞通告，且定期評估更新？
(9)資通安全事件通報應變及情資評估因應	
9.1	是否訂定資安事件通報作業規範，包含判定事件等級之流程及權責、事件影響及損害評估、內部通報流程、通知其他受影響機關之方式、通報窗口及聯繫方式等，並規範於知悉資通安全事件後1小時內進行通報，若事件等級變更時應續行通報？相關人員是否熟悉相關程序，且落實執行？
9.2	是否訂定資安事件應變作業規範，包含應變小組組織、事前之演練作業、事中之損害控制機制、事後之復原、鑑識、調查及改善機制、相關紀錄保全等，且落實執行？
9.3	是否每年進行1次資安事件通報及應變演練？是否將新興資安議題、複合式攻擊或災害納入演練情境，以驗證各種資安事件之安全防護及應變程序？
9.4	是否建立資安事件相關證據資料保護措施，以作為問題分析及法律必要依據？
9.5	近3年重大資安事件之通報時間、過程、因應處理及改善措施，是否依程序落實執行？
9.6	是否訂定資安事件處理過程之內部及外部溝通程序？
9.7	針對所有資安事件，是否保留完整紀錄，並與其他相關管理流程連結，且落實執行後續檢討及改善？
9.8	是否建置資通安全威脅偵測管理(SOC)機制？監控範圍應包括「資通安全防護」之辦理內容、目錄服務系統與機關核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄？SOC 是否有委外供應商？SOC 供應商是否依契約規範(包含 SLA 水準)確實履約？

	(A、B 級機關適用)
9.9	是否訂定應記錄之特定資通系統事件(如身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等)、日誌內容、記錄時間週期及留存政策，且保留日誌至少6個月？是否有啟用 DNS 相關紀錄日誌(有記錄到 DNS 行為的日誌)？是否有開啟監測內部網路連線至 DMZ 的日誌？
9.10	是否依日誌儲存需求，配置所需之儲存容量，並於日誌處理失效時採取適當行動及提出告警？
9.11	針對日誌之是否進行存取控管，並有適當之保護控制措施？
9.12	知悉資通安全事件後，是否於規定時間內完成損害控制或復原作業，並持續進行調查及處理，於1個月內送交調查、處理及改善報告，且落實執行？(第一級或第二級事件：72小時內完成損害控制或復原作業；第三級或第四級事件：36小時內完成損害控制或復原作業)
9.13	知悉第三級或第四級資通安全事件後，是否指派適當層級之人員召開會議研商相關事宜？
9.14	是否建立資通安全情資之評估及因應機制，針對所接受之情資，辨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？
9.15	是否適時進行資通安全情資分享？分享哪些資訊？

捌、稽核結果

本次實地稽核計有 14 項待改善事項與 8 項建議事項以及 3 項法遵符合情形，受稽機關應於收受稽核結果報告後一個月內，向本部提出改善報告，並敘明後續矯正措施、辦理時程及辦理情形。稽核結果如下：

一、策略面

(一)稽核項目 1：核心業務及其重要性

1.待改善事項

稽核項次：1.1

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。

2.法遵符合情形

稽核項次：1.3

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。

(二)稽核項目 2：資通安全政策及推動組織

1.建議事項

(1)稽核項次：2.1

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。

(2)稽核項次：2.4

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。

2.法遵符合情形

稽核項次：2.3

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。

二、管理面

(一)稽核項目 4：資訊及資通系統盤點及風險評估

1.待改善事項

稽核項次：4.1

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。

2.建議事項

(1)稽核項次：4.1

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。

(2)稽核項次：4.5

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。

(二)稽核項目 5：資通系統或服務委外辦理之管理措施

1.待改善事項

(1)稽核項次：5.2

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。

(2)稽核項次：5.11

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。

(3)稽核項次：5.15

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述規定，應改善之。

(三)稽核項目 6：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

1.建議事項

(1)稽核項次：6.1

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。

(2)稽核項次：6.2

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。

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。

三、技術面

(一)稽核項目 7：資通安全防護及控制措施

1.待改善事項

(1)稽核項次：7.4

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。

(2)稽核項次：7.6

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。

(3)稽核項次：7.9

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。

2.建議事項

稽核項次：7.8

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。

3.法遵符合情形

稽核項次：7.27

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。

(二)稽核項目 8：資通系統發展及維護安全

1.待改善事項

(1)稽核項次：8.1,8.8

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。

(2)稽核項次：8.2

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。

(3)稽核項次：8.10

依機關「I-02-018 系統開發及維護作業程序書」以及「I-03-011 系統開發作業說明書」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。

2.建議事項

稽核項次：8.6

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。

(三)稽核項目 9：資通安全事件通報應變及情資評估因應

1.待改善事項

(1)稽核項次：9.1

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。

(2)稽核項次：9.2

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。

(3)稽核項次：9.14

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。

玖、附件

「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」實地稽核發現事項紀錄表

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

受稽機關：**台灣網路資訊中心**

稽核日期：112.11.10

稽核發現

項次	內容分類	對應稽核項次	稽核發現內容	稽核組別
1	待改善事項	1.1	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。	A
2	法遵符合情形	1.3	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。	A
3	建議事項	2.1	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。	A
4	法遵符合情形	2.3	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。	A
5	建議事項	2.4	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。	A
6	待改善事項	4.1	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。	B
7	建議事項	4.1	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。	B
8	建議事項	4.5	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。	B
9	待改善事項	5.2	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。	B

項次	內容分類	對應稽核項次	稽核發現內容	稽核組別
10	待改善事項	5.11	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。	B
11	待改善事項	5.15	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述規定，應改善之。	B
12	建議事項	6.1	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。	B
13	建議事項	6.2	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。 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。	B
14	待改善事項	7.4	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。	C
15	待改善事項	7.6	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。	C
16	建議事項	7.8	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。	C
17	待改善事項	7.9	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。	C
18	法遵符合情形	7.27	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。	C
19	待改善事項	8.1, 8.8	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。	C

項次	內容分類	對應稽核項次	稽核發現內容	稽核組別
20	待改善事項	8.2	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。	C
21	建議事項	8.6	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。	C
22	待改善事項	8.10	依機關「I-02-018 系統開發及維護作業程序書」以及「I-03-011 系統開發作業說明書」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。	C
23	待改善事項	9.1	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。	C
24	待改善事項	9.2	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。	C
25	待改善事項	9.14	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。	C

稽核團隊代表：

受稽機關代表：

稽核委員：

稽　核　日　期：112 年 11 月 10 日