113年資通安全稽核
財團法人台灣網路資訊中心
實地稽核報告

數位發展部

中華民國113年11月7日

壹、基本資訊

一、稽核日期：113年10月28日

二、稽核地點：財團法人台灣網路資訊中心(臺北市松山區八德路四段123號3樓)

三、稽核範圍：全機關

四、稽核準則

(一)資通安全管理法(以下簡稱資安法)及其子法

(二)國家資通安全發展方案(110年至113年)

(三)資訊安全管理系統國家標準 CNS 27001:2014或國際資訊安全管理標準 ISO 27001:2013

(四)國際資訊服務管理標準 ISO 20000：2018

(五)受稽機關之資通安全維護計畫

五、稽核小組

(一)稽核領隊：數位發展部資源管理司牛信仁司長

(二)稽核委員：

策略面：王復中委員、羅金賢委員
管理面：何昇龍委員、林炫佑委員
技術面：曾　龍委員、林家樑委員
工作人員：吳紫禎、邱淑芳、黃瑟靖、沈培恩、曾子怡、陳美香

貳、稽核發現

本報告分別從策略面、管理面及技術面3個構面，提出法遵符合情形、待改善事項與建議事項。

一、策略面

(一)法遵符合情形(優於法遵事項)

1、稽核項次：1.3

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。

2、稽核項次：2.3

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。

(二)待改善事項

1、稽核項次：1.4

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。

2、稽核項次：1.7

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。

(三)建議事項

1、稽核項次：1.1

(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。

2、稽核項次：1.6

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。

3、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。

4、稽核項次：2.2

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，建議改善之。

5、稽核項次：2.4

(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。

6、稽核項次：2.5

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。

7、稽核項次：3.4

(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。

二、管理面

(一) 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)明確列入 RFP 中，應改善之。

2、稽核項次：5.8

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。

3、稽核項次：5.12

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。

(二)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，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。

2、稽核項次：5.3

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。

3、稽核項次：5.15

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。

三、技術面

(一) 待改善事項

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。

(二)建議事項

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，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。

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，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。

3、稽核項次：7.8

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，建議改善之。

4、稽核項次：7.16

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。

5、稽核項次：7.23

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。

6、稽核項次：8.1

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。

7、稽核項次：9.8

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。

參、後續管考作業

數位發展部將於稽核作業辦理完成後一個月內，函送資安稽核報告予受稽機關，請受稽機關就報告中待改善事項研議因應作為與辦理時程等相關內容，於文到後一個月內函報待改善事項辦理情形表至本部審查，本部將於次年度一月底前彙整稽核結果報告，並提交主管機關本部資通安全署備查；嗣後由本部核定追蹤結果。

肆、實地稽核發現事項紀錄(如附件)

113 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：113.10.28

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	建議事項	1.1	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。	A
2	優於法遵事項	1.3	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。	A
3	待改善事項	1.4	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。	A
4	建議事項	1.6	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。	A
5	待改善事項	1.7	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。	A
6	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。	A
7	建議事項	2.2	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，建議改善之。	A

項次	內容分類	對應稽核項次	稽核發現內容	稽核組別
8	優於法遵事項	2.3	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。	A
9	建議事項	2.4	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。	A
10	建議事項	2.5	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。	A
11	建議事項	3.4	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。	A
12	建議事項	4.1	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。	B
13	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)明確列入RFP中，應改善之。	B
14	建議事項	5.3	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。	B
15	待改善事項	5.8	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。	B
16	待改善事項	5.12	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。	B
17	建議事項	5.15	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。	B
18	建議事項	7.4	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	C

項次	內容分類	對應稽核項次	稽核發現內容	稽核組別
			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。	
19	建議事項	7.6	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。	C
20	建議事項	7.8	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，建議改善之。	C
21	建議事項	7.16	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。	C
22	建議事項	7.23	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。	C
23	建議事項	8.1	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。	C
24	待改善事項	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。	C
25	建議事項	9.8	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。	C

稽核團隊代表：[illegible]　　受稽機關代表：[illegible]

稽核委員：[illegible]

稽　核　日　期：113　年　10　月　28　日