教育部 114 年度對所屬公務機關及所管特定非公務機關資通安全稽核計畫

114 年 2 月

壹、依據

一、資通安全管理法第 13 條第 1 項及第 17 條第 3 項。

二、教育部所管特定非公務機關資通安全管理作業辦法第 5 條第 1 項。

貳、目的

依資通安全管理法第 10 條及第 17 條第 1 項規定，公務機關及關鍵基礎設施（Critical Infrastructure，以下簡稱 CI）提供者以外之特定非公務機關應訂定、修正及實施資通安全維護計畫。

另依資通安全管理法第 13 條第 1 項規定，公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形，另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 CI 提供者以外之特定非公務機關資通安全維護計畫實施情形。

教育部（以下簡稱本部）為落實前述法令規定，規劃每年度自所屬公務機關及所管特定非公務機關擇定受稽核對象，查核其資通安全管理法法遵事項符合情形與資通安全維護計畫實施情形，以協助機關改善並強化資通安全防護工作之完整性及有效性，持續精進機關資安防護水準。

受稽機關之資通安全維護計畫實施有缺失或待改善者，應依資通安全管理法第 13 條第 2 項及教育部所管特定非公務機關資通安全管理作業辦法第 10 條規定提出改善報告，以確保資通安全維護計畫實施之合宜性、適切性及有效性。

參、對象及期間

一、本部所屬公務機關

(一)範圍為國民及學前教育署(以下簡稱國教署)、青年署、部屬機構(11間)及國立大專校院(47間)。

(二)實地查核頻率為2年(24個月內)1次，並由本部考量資源、風險程度及前次稽核情形，每年擇定**10至15間稽核對象辦理技術檢測**。

(三)符合下列遴選原則之一者，優先納入技術檢測對象：

1、資通安全責任等級：屬A、B級者。

2、近3年未曾接受行政院或本部技術檢測者。

二、本部所管特定非公務機關

(一)範圍為本部各單位轄管之財團法人(共9間)。

(二)實地稽核每年至少擇定3間。

(三)遴選原則

1、資通安全責任等級：屬A、B級者。

2、本年或近2年曾發生2級以上資通安全事件者。

3、近3年未曾接受行政院或本部實地稽核，或其稽核結果建議持續關注協助者。

4、其他未完成資安應辦事項者(資通安全防護/安全性檢測/資通安全健診等)。

三、專案實地稽核

考量近期國內、外資通安全事件頻繁發生，造成機關之機敏資料外洩、資料遺失、系統服務中斷等重大衝擊，為協助機關重要業務相關資通系統或服務發掘潛在資安風險，得視情況另籌組稽核團隊辦理專案實地稽核。

四、書面查核

除已實地查核者，得另辦理機關資通安全維護計畫實施情形之書面查核，頻率為 2 年 1 次。

肆、作業階段及時程

本計畫之資安稽核作業，分為準備作業、前置作業、實施作業及檢討作業等 3 階段，各階段作業時程及重點工作，詳見表 1。

表 1、稽核作業時程規劃

項次	階段(時程)	重點工作
1	前置作業 (114 年 1~3 月)	(1)研擬稽核計畫、受稽機關及稽核項目等。 (2)確認稽核計畫並進行整備。 (3)確認受稽機關與時程。 (4)確認稽核委員與觀察員名單。 (5)辦理稽核委員共識會議、觀察員作業研討會等相關會議。
2	實施作業 (114 年 3 月 ~114 年 12 月)	進行技術檢測及實地稽核。 第 1 梯次：114 年 3 月~114 年 6 月 第 2 梯次：114 年 7 月~114 年 9 月 第 3 梯次：114 年 10 月~114 年 12 月 註：得視疫情或資源配置情形調整時程。
3	檢討作業 (115 年 1 月~2 月)	(1)每年度結束後，提出稽核結果及共同發現事項。 (2)建議表揚優良機關。

伍、稽核團隊

資安稽核團隊組成原則如下：

一、領隊：

(一)由本部資安與個資管理會召集人、副召集人、執行秘書或各工作分組組長、本部資安或資訊業務人員及主管、教育機構資安驗證中心(ISCB)資安主導稽核員或經本部同意之人員擔任。

(二)原定領隊因故無法參加，得由策略面委員代理。

二、稽核委員（稽核小組成員）：

(一)由本部或委託辦理稽核之單位（教育機構資安驗證中心(ISCB)），考量稽核之需求，邀請具備資通安全政策、管理、技術、法律或實務專業之公務機關代表或專家學者擔任稽核小組成員。

(二)依受稽機關資通作業環境之規模與性質，分配 3 至 7 名委員進行實地查核作業，分別為策略面 1 至 2 名、管理面 1 至 2 名及技術面 1 至 3 名，得視實際稽核範圍，調整委員數量。

(三)如有涉及教育部所管特定非公務機關資通安全管理作業辦法第 8 條第 3 項各款之情形，應提早通知本部並主動迴避。

(四)稽核委員之調派，得由本部委託辦理稽核之單位（教育機構資安驗證中心(ISCB)）辦理。如受稽機關為教育機構資安驗證中心(ISCB)之主辦學校，由本部主導稽核委員之調派。

三、觀察員：

(一)自教育體系相關單位（包含本部、部屬機關(構)、公法人、公私立大專校院、臺灣學術網路(TANet)區域網路中心、縣市教育網路中心、本部捐助之財團法人等）人員遴選，每場次至多 2 名。

(二)本部所屬公務機關（包含本部、部屬機關(構)及國立大專校院）及臺灣學術網路(TANet)區域網路中心，須至少指派 1 名人員參與觀察員之遴選、見習或實習作業。

四、技術檢測團隊：由教育體系資安檢測技術服務中心(TACCST)中具備資安健診、系統滲透測試及網路檢測等資安檢測能力及經驗之技術人員擔任，每場次 5 至 7 名。如受稽機關為教育體系資安檢測技術服務中心(TACCST)之主辦學校，由本部另行召集技術檢測團隊。

五、稽核團隊組成及員額配置如表 2。

表 2、稽核團隊員額配置

項目	稽核團隊組成	人員配置	總計
技術檢測	檢測團隊 ▪領隊[註 1] ▪主導檢測員 ▪檢測員 ▪觀察員	 1 名 1 名 5~7 名 0~2 名	8~13 名
	工作人員	1 至 2 名	
實地稽核	領隊	1 名	5~13 名
	稽核委員 ▪策略面 ▪管理面 ▪技術面	共 3 至 7 名[註 2] ▪ 1 至 2 名 ▪ 1 至 2 名 ▪ 1 至 3 名	
	觀察員	0~2 名	
	工作人員	1 至 3 名	

註 1：得由該場次主導檢測員代理。

註 2：屬本部所屬公務機關之重點稽核對象者，人員配置至少 6 名。

陸、稽核準則

一、資通安全管理法及其子法。

二、CNS 27001 或 ISO 27001 等資訊安全管理系統標準。

三、受稽機關之資通安全維護計畫。

四、個人資料保護法及其子法。

五、臺灣學術網路管理規範。

六、其他適用之行政院或本部資通安全政策或規範。

柒、稽核範圍

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

捌、稽核方式、項目及配分

一、稽核方式

稽核實施項目如下：採技術檢測及實地稽核方式進行。

二、稽核項目及配分

(一)第 1 階段：技術檢測（僅針對部分單位實施）

1、技術檢測分為 8 大檢測項目，各檢測項目之執行內容及配分說明如表 3。（技術檢測評分表，請參閱附件 3）

表 3、技術檢測項目及配分

項次	檢測項目	檢測子項	配分
1	使用者電腦安全檢測	使用者電腦弱點掃描	5
		使用者電腦安全防護檢測	10
2	網路惡意活動檢測	中繼站連線阻擋檢測	5
3	核心資通系統安全檢測	核心資通系統內網滲透測試	15
		核心資通系統防護基準檢測	10
4	網路架構檢測	網路架構檢測	10
5	目錄伺服器安全檢測	目錄伺服器安全防護檢測	10
6	物聯網設備安全檢測	物聯網設備安全檢測	15
7	組態設定安全檢測	組態設定安全檢測	10
8	資料庫安全檢測	資料庫安全檢測	10
9	其他發現事項	其他發現事項	採倒扣，至多扣減 10 分
10	準備作業配合度	應備文件及相關紀錄完整性	採倒扣，至多扣減 10 分
		合計	100

2、若受稽機關無對應之檢測項目，則將技術檢測分數依比例調整。例如：如受稽機關無目錄伺服器，則不進行「目錄伺服器安全檢測」，技術檢測計分方式調整為：技術檢測分數÷90×100。

3、國立大專校院之技術檢測範圍，包含學校各行政單位（例如：電算中心、教務處、學務處、總務處等）及教學單位（例如：各系所辦公室），且相關行政人員之使用者電腦亦包含在內。

(二)第 2 階段：實地查核

1、實地稽核分策略面、管理面及技術面 3 個構面，實地稽核項目檢核表分為公務機關及特定非公務機關 2 式，各構面之稽核項目及配分說明如表 4，總分合計 100 分。（實地稽核評分表，請參閱附件 4）

表 4、實地稽核項目及配分

構面	稽核項目	配分
策略面	一、核心業務及其重要性	10
	二、資通安全政策及推動組織	10
	三、專責人力及經費配置	10
管理面	四、資訊及資通系統盤點及風險評估	10
	五、資通系統或服務委外辦理之管理措施	10
	六、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	10
技術面	七、資通安全防護及控制措施	20
	八、資通系統發展及維護安全	10
	九、資通安全事件通報應變及情資評估因應	10
其他	準備作業配合度	採倒扣，至多扣減 5 分
	合計	100

3、國立大專校院之實地查核範圍，包含學校各行政單位（例如：電算中心、教務處、學務處、總務處等）及教學單位（例如：各系所辦公室）。如機關之資通安全維護計畫實施範圍未完整，相關稽核項目將予以扣分。

(三)評分方式

1、受技術檢測單位：整體總成績 = 技術檢測得分 ×20% + 實地稽核得分 ×80%。

2、未受技術檢測單位：整體總成績 = 實地稽核得分 ×100%。

玖、作業說明

一、機關自評

(一)受稽機關填寫「資通安全實地稽核項目檢核表」(附件 1)及「受稽機關現況調查表」(附件 2)。受技術檢測單位須另於技術檢測前填復「技術檢測基本資料調查表」及「核心資通系統調查表」，文件由教育體系資安檢測技術服務中心提供。

(二)建議受稽機關先行辦理資安健診作業，俾利預先了解資安現況，並進行改善作為（資安健診服務已納入共同供應契約）。

二、技術檢測

受技術檢測單位於辦理實地稽核前，將先進行 2 至 3 天之技術檢測，檢視受稽機關之安全防護情形，並於最後 1 天由技術檢測團隊提交技術檢測摘要報告，除據以進行技術檢測評分外，並提供實地稽核參考。技術檢測重點說明如下：

(一) 使用者電腦安全檢測

針對受稽機關檢測範圍進行全網段弱點掃描。依照弱點掃描結果之風險程度排序，挑選 5~10 臺高風險之使用者電腦進行深度檢測，

其檢測項目包含防毒軟體、安全性修補程式更新、應用程式更新及惡意程式檢測等安全防護措施檢測。

(二) 網路惡意活動檢測

依照國家資通安全研究院每週公布之中繼站名單，抽選機關不同網段（包含使用者及伺服器網段等）進行檢測。

(三) 核心資通系統安全檢測

1. 針對核心資通系統進行內網滲透測試，包括檢測資通系統之權限存取、應用程式及系統弱點、系統通訊保護等項目，若資通系統使用單一簽入進行權限管控，則亦納入檢測範圍。
2. 依資通系統防護需求等級(普、中、高)，針對核心資通系統之存取控制、識別及鑑別、系統及服務獲得、系統與資訊完整性及系統與通訊保護等控制措施進行檢測，並檢視源碼掃描、弱點掃描及滲透測試等檢測報告及修補紀錄，以及安全需求檢核結果。

(四) 網路架構檢測

透過訪談及實際檢視方式，驗證網路及系統之管理控制措施、網路及系統之安全控制措施、網路及系統架構之備援機制、防火牆規則及存取控制，並確認資通系統管理及防護情形。

(五) 目錄伺服器安全檢測

透過實際檢視方式，針對機關之目錄伺服器進行防毒措施、安全性修補程式更新及惡意程式檢測，並確認身分鑑別與授權管理情形。

(六) 物聯網設備安全檢測

針對網路印表機、網路攝影機、無線網路基地台(AP)/無線路由器、門禁設備、環控系統、網通設備及其他物聯網設備之身分鑑別與授權、軟體與韌體之安全性更新、通訊安全等基準項目，透過訪談及實際檢測方式確認是否符合安全基準。

(七) 組態設定安全檢測

針對已公告之政府組態基準(GCB)項目進行抽測。

(八) 資料庫安全檢測

透過訪談及實際檢視方式，抽測 10 項資料庫安全檢測項目，包含特權帳號管理、資料加密、備份保護、弱點管理、存取授權、稽核紀錄及委外管理等安全機制，確認資料庫安全管理與防護狀況。

三、實地稽核

(一)由領隊帶領稽核團隊至受稽機關進行實地稽核（實地稽核時程規劃如表 5）。實地稽核項目依據資通安全管理法及各子法法遵事項，分為三大構面、九大稽核項目，詳參附件「資通安全實地稽核項目檢核表」。

(二)受稽機關如為本部捐助之財團法人，將請其業務主管單位派員出席（例如：「財團法人大學入學考試中心基金會」由高等教育司派員參加稽核）。

(三)實地稽核時間將依機關業務複雜度、機關辦公場域數量、重要資通系統數量等因素，彈性調整稽核時程。稽核啟始/結束會議之受稽機關代表建議由機關資通安全長出席，以帶領機關之資安管理及追蹤改善。

表 5、實地稽核時程

時間	工作項目	參與人員
9:00~9:30	啟始會議 ➢ 受稽機關代表致詞、介紹出席人員 (5 分鐘) ➢ 稽核團隊領隊致詞、介紹稽核團隊 (5 分鐘) ➢資安稽核作業說明 (5 分鐘) ➢受稽機關資安推動情形(15 分鐘)	▪稽核團隊 ▪受稽機關 ▪業務主管單位
9:30~9:45	稽核團隊稽核前意見交換	稽核團隊
9:45~12:00	實地稽核	▪稽核團隊 ▪受稽機關 ▪業務主管單位
12:00~13:00	午餐[註]及彙整稽核發現	稽核團隊
13:00~16:30	實地稽核	▪稽核團隊 ▪受稽機關 ▪業務主管單位
16:30~17:00	稽核團隊意見彙整	稽核團隊
17:00~17:30	結束會議 ➢稽核結果報告 ➢意見交流	▪稽核團隊 ▪受稽機關 ▪業務主管單位

註：午餐委請受稽機關代訂，由稽核團隊支付費用。

壹拾、獎勵及改善作業

各年度資安稽核作業結束後，成績表現優良者，本部將函請受稽機關行政獎勵，相關獎勵原則如表 6。

一、行政獎勵

依各受稽機關成績，擇取排序後前五分之一（未達整數以四捨五入計）受稽機關評為績優機關，本部將函請績優機關，針對有功人員予以敘獎（嘉獎或記功）。

表6 獎勵說明

項目	行政獎勵
受獎對象	各機關依權責分別對參與人員敘獎
獎勵方式	嘉獎或記功
獎勵範圍	前五分之一名 （未達整數以四捨五入計）

限制條件：

(一)績優機關技術檢測及實地稽核個別成績，皆須達 75 分(含)以上；未達標準者，依序由後序名次符合條件者遞補。

(二)受稽機關未達獎勵標準時，名額從缺。

二、改善作業

(一)本部將於每梯次稽核結束後函送資安稽核報告予受稽機關，並請機關就報告中待改善或建議事項研議因應作為及辦理時程，於期限內填報並回復本部，後續本部將通知受稽機關定期回復。

(二)受技術檢測之受稽機關，請於技術檢測總結會議簡報後 1 週內，依簡報內容所提有關核心資通系統滲透測試檢測結果具高風險弱點者、物聯網設備安全檢測具高風險弱點者及其它涉及敏感資訊可能外洩部分（如個資外洩等），至教育體系技術檢測平台(https://tas.moe.edu.tw/account/login/)提交處理措施及相關佐證資料。

(三)技術檢測總報告提供後 1 個月內，請受稽機關提交改善報告及相關佐證資料，其改善規劃時程以 3 個月內為限，若無法於時程內完成，請函文至本部說明並提出暫時性矯正措施，需由本部同意即可列入後續追蹤(相關函文範本請至教育體系資安檢測技術服務中心網站下載)

(四)公務機關所屬人員未遵守資通安全管理法規定者，應依資通安全管理法第 19 條規定辦理之；本部所管特定非公務機關之稽核結果，如有資通安全管理法第 20 條及第 21 條所述情形，本部將依法辦理之。

(五)各年度資安稽核作業結束後，本部將彙整所有受稽機關之稽核結果，並提出資安稽核共同發現事項及建議，供本部所屬公務機關及所管特定非公務機關參考改進。

壹拾壹、機關配合事項

一、本部於稽核前 1 個月通知受稽機關，另將個別通知受稽機關稽核期程。請受稽機關於文到後 2 週內填復「資通安全實地稽核項目檢核表」、「受稽機關現況調查表」，需技術檢測之學校須另填復「技術檢測基本資料調查表」及「核心資通系統調查表」等資料，文件由教育體系資安檢測技術服務中心提供，俾利稽核團隊辦理作業。

二、前述「資通安全實地稽核項目檢核表」得由本部依最新法令要求、重大資安政策等進行內容滾動修正，如有更新情形，本部將於適用該檢核表之受稽核梯次前 1 個月公告周知。

三、請受稽機關於實地檢核前提供機關最新版之資通安全維護計畫、資通系統清冊，及最近一次管理審查會議紀錄**及「資通安全實地稽核項目檢核表」之佐證資料**，俾利稽核團隊初步瞭解機關資通安全維護計畫實施情形。

四、本部將辦理資安稽核說明會、稽核委員共識會議及觀察員作業說明會，其辦理時程、地點及相關事項將另行通知，前述會議得採線上或其他適當方式辦理。

五、本部轄下其他機關稽核作業

各上級/監督/中央目的事業主管機關，應依法要求所屬/所監督/所管機關提報資通安全維護計畫，並由各上級/監督/中央目的事業主管機關制定及實施資安稽核，分層督導方式如下：

(一)醫院以外之大學附設機構：由上級機關（所屬大學）制定及實施資安稽核，原則每 2 年至少辦理 1 次。

(二)大學附設醫院：各醫院之分院應由上級機關（總院）制定及實施資安稽核，原則每 2 年至少辦理 1 次。

(三)國立高級中等以下學校及國教署轄管之財團法人（包含財團法人台灣省中小學校教職員福利文教基金會、財團法人中華幼兒教育發展基金會，共 2 間）：由國教署統籌規劃辦理、制定及實施資安稽核。

壹拾貳、附件

附件	附件名稱	說明
1	資通安全實地稽核項目檢核表	機關之資通安全維護計畫實施情形，資料將提供實地稽核之稽核委員參考
2	受稽機關現況調查表	受稽機關現況說明，包括單位組織、辦公地點、核心資通系統儲放地點、AD 放置地點等
3	技術檢測評分表	技術檢測項目配分說明
4	實地稽核評分表	實地稽核項目配分說明