111 年資通安全稽核計畫

111 年 4 月

壹、依據

一、資通安全管理法第 7 條第 2 項、第 13 條第 1 項、第 16 條第 4 項及第 17 條第 3 項。

二、特定非公務機關資通安全維護計畫實施情形稽核辦法第 3 條第 1 項。

貳、目的

一、查核公務機關及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。

二、經由外部稽核各機關資通安全維護計畫實施情形，改善並強化機關資通安全防護工作之完整性及有效性，以持續精進管理政府整體資安風險。

參、作業階段及時程

本(111)年資安稽核作業，分為準備作業、前置作業、實施作業及檢討作業等 4 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
一	準備作業(2-3 月)	研擬年度稽核整體規劃、受稽機關、稽核委員建議名單及調修稽核項目等
二	前置作業(4 月)	(一)擬定稽核計畫並進行整備 (二)確認受稽機關與協調時程 (三)確認稽核委員與觀察員名單並辦理通知作業
三	實施作業(5 月-12 月)	(一)辦理稽核委員與觀察員稽核前訓練 (二)辦理受稽機關技術檢測及實地稽核

項次	階段(時程)	重點工作
四	檢討作業 (12 月~112 年 1 月)	提出稽核結果及共同發現事項、建議表揚成績優良機關、撰擬送交立法院之年度稽核概況報告

肆、稽核團隊

行政院(以下簡稱本院)資安稽核團隊組成原則如下：

一、領隊：本院國家資通安全會報副召集人或協同副召集人，得由策略面委員代理。

二、稽核委員：

(一)每個受稽機關原則配置 7 名委員進行資安實地稽核作業，分配為策略面 2 人、管理面 2 人及技術面 3 人[註]。

(二)由本院考量稽核實際需求，邀請具備資通安全政策、管理、技術、法律專業或具實務經驗之公務機關代表或產、學、研等專家學者擔任小組成員，其中公務機關代表不少於全體成員人數之四分之一。

(三)如有涉及特定非公務機關資通安全維護計畫實施情形稽核辦法第 6 條第 4 項各款之情形，應提早通知本院並主動迴避擔任該場次稽核委員。

(四)如於本年已受其他上級或中央目的事業主管機關邀約擔任同一受稽機關稽核委員，亦請提早通知本院並請迴避擔任該場次稽核委員。

三、觀察員：自總統府與中央一級機關含直屬機關、直轄市政府及所屬一級機關之公務人員遴選，每場次至多 2 名觀察員。

四、技術檢測團隊：由本院國家資通安全會報技術服務中心(以下簡稱技服中心)中具備惡意程式檢測、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，每場技術人員至多 10 名。

稽核團隊組成及員額配置，詳見表 2。本院並得視實際情況及受稽機關之屬性、規模、查檢場域及系統等因素進行有關調整。

表2　稽核團隊組成及員額配置

項目	稽核團隊組成	人員配置	總計
實地稽核	領隊	1 名	1 名
	稽核委員 ▪策略面 ▪管理面 ▪技術面	 2 名 2 名 3 名	7 名
	觀察員	2 名	2 名
	工作人員	6 名	6 名
技術檢測	技服中心檢測人員	10 名	10 名

伍、受稽機關

資通安全管理法已於 108 年 1 月 1 日施行，該法授權本院稽核所屬公務機關及特定非公務機關

一、公務機關：

(一)本院所屬二級及獨立機關受稽核頻率為 2 年 1 次，爰本年受稽機關原則為 109 年受稽核之本院所屬二級及獨立機關，惟本院將另依 109、110 年稽核結果等整體考量分配調整。

(二)原定於 110 年辦理稽核之受稽機關，受 COVID-19 疫情影響延期至本年辦理者。

(三)實質保有大量政府重要資料者。

二、特定非公務機關

(一)關鍵基礎設施提供者、公營事業及政府捐助之財團法人。

(二)符合下列遴選原則之一者

1、 資通安全責任等級 A、B 級者，且本年以關鍵基礎設施提供者優先。

2、 提供共用(通)性資通系統服務者及近期已執行重大系統改版者。

3、 本年或近 2 年曾發生資安事件者。

4、 近 3 年未曾受稽核或稽核結果建議持續關注協助者。

5、 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)。

陸、稽核準則

依據資通安全管理法及其子法、國家資通安全發展方案(110 年至 113 年)、資訊安全管理系統國家標準 CNS 27001:2014 或資訊安全管理系統國際標準 ISO 27001:2013、服務管理系統國際標準 ISO 20000-1:2018 及受稽機關之資通安全維護計畫等，據以規劃稽核項目。

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通安全管理政策、程序等。

捌、稽核方式、項目及配分

本院年度稽核方式含資安實地稽核、工業控制系統(Industrial Control Systems,ICS，以下簡稱工控系統)資安稽核試行作業及第二方資安稽核輔導，說明如下：

一、資安實地稽核

本年經整體考量受稽機關屬性及為有效運用稽核能量，採將受稽機關依資通安全責任等級進行分組(如表 3)，各分組資安稽核方式如表 4：

表3　受稽機關分組(註)

稽核分組	一	二	三	四
共通屬性	(一)公務機關 (二)資通安全責任等級 A 級	(一)公務機關 (二)資通安全責任等級 B 級	(一)公務機關 (二)資通安全責任等級 C 級	特定非公務機關
家數	6	5	6	6

表4　各分組資安稽核方式

稽核分組		一	二	三	四
稽核方式	技術檢測	V			
	實地稽核	V	V	V	V

(一)第 1 階段：技術檢測(僅針對第一分組實施)

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 5。(技術檢測評分表，請參閱附件 8)

表5　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	10
		使用者電腦安全防護檢測	10
2	物聯網設備檢測		10
3	網域主機安全防護檢測	防毒軟體檢測	5
		安全性更新檢測	
		惡意程式檢測	
4	資料庫安全檢測		10
5	核心資通系統安全檢測	核心資通系統內網滲透測試	20
		核心資通系統防護基準檢測	5
6	網路架構檢測		10
7	組態設定安全檢測	作業系統組態檢測	15
		瀏覽器組態檢測	
		網通設備組態檢測	
		應用程式組態檢測	
8	網路惡意活動檢視	惡意中繼站連線阻擋檢測	5
		APT 網路流量檢測	試行不計分(註)

註：「APT 網路流量檢測」係本年新增檢測項目，爰先試行俟 112 年評估納入正式檢測計分項目。

2、 如受稽機關無網域主機，則不進行「網域主機安全防護檢測」，技術檢測計分方式調整為：技術檢測分數÷95x100。

3、 如受稽機關無核心資料庫，則不進行「資料庫安全檢測」，技術檢測計分方式調整為：技術檢測分數÷90x100。

4、 如受稽機關無網域主機與核心資料庫，則不進行「網域主機安全防護檢測」與「資料庫安全檢測」，技術檢測計分方式調整為：技術檢測分數÷85x100。

(二)第 2 階段：實地稽核(所有分組均會實施)

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 6，總分合計 100 分。 (實地稽核評分表，請參閱附件 9)。

表6　各構面稽核項目及配分

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
	合計：	100

(三)評分方式

1、 第一分組

整體總成績=技術檢測得分 × 30% ＋ 實地稽核得分 × 70%。

2、 第二、三、四分組：

整體總成績=實地稽核得分 × 100%。

二、工控系統資安稽核試行作業(相關作業說明將另函發試行機關)

針對受稽核之特定非公務機關屬關鍵基礎設施提供者，本院將視其所屬關鍵基礎設施領域，評估併同實地稽核作業，同日試行工控系統資安稽核，試行之稽核結果不列入年度資安實地稽核成績，作業說明如下：

(一)書面審查

1、 查核工控系統資安稽核試行機關自評內容之妥適性。

2、 查核試行機關資通安全維護計畫之完整性。

(二)實地稽核

1、 就擇定之核心工控系統等，依據十大稽核項目(分管理面及技術面 2 大構面)、該領域中央目的事業主管機關就特定類型資通系統，自行擬訂並經核定之防護基準，進行資安防護稽核。

2、 就工控系統資安防護提出稽核結果及精進建議。

(三)後續作業

透過實地稽核，對試行機關工控系統資安防護提出強化建議；並據以檢視調修本院工控系統資安稽核相關共通性項目等。

三、第二方資安稽核輔導(相關作業說明將另函發受輔導機關)

為落實法令分層監督管理原則，本年本院並辦理第二方資安稽核輔導作業，確認及協助上級/監督/中央目的事業主管機關依法對所屬/所監督/所管機關之監督管理作為，輔導方式說明如下：

(一)書面審查

1、 上級/監督/中央目的事業主管機關所提稽核計畫。

2、 受稽核之所屬/所監督/所管機關之資通安全維護計畫。

(二)實地驗證

1、 規劃由 2 位專家觀察機關辦理實地稽核整體流程。

2、 對於整體稽核規劃內容及執行程序彙整提出精進建議。

(三)作業成效

本院透過協助輔導各上級/監督/中央目的事業主管機關第二方稽核所屬/所監督/所管機關稽核整體流程，檢視法令落實度、稽核作法及成效。

四、資安稽核除對本院所屬公務機關、特定非公務機關辦公場域外，並延伸至重要系統所在之外部專案辦公室或機房；另併實施第二方稽核輔導，配合上級/監督/中央目的事業主管機關對所屬/所監督/所管機關稽核時程，擴展為多場域稽核模式，依實際需要動態調整稽核天數，不以 1 日為限。

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) 、「受稽機關現況調查表」(附件 2)、「技術檢測基本資料調查表」(附件 3)、「核心資通系統評選表」(附件 4)、「核心資通系統安全防護評量表」(附件 5)及「組態設定現況調查表」(附件 6)。上述表單回復日期請參考表 10「受稽機關配合事項」。

(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

稽核分組中第一分組於辦理實地稽核前，將先進行 3 天之技術檢測，檢視受稽機關之安全防護情形，並於技術檢測最後 1 天由檢測團隊說明技術檢測結果，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

針對受稽機關進行全機關網段連接埠掃描(Port scan)，藉由掃描結果挑選可能存在風險之 50 台使用者電腦進行弱點掃描。依照弱點掃描結果之風險程度排序，挑選 5 台不同作業系統版本之高風險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 4 項安全防護措施檢測。

(二) 物聯網設備檢測

針對網路印表機、門禁設備、網路攝影機、無線網路基地台/無線路由器、環控系統及網路儲存裝置(NAS)等物聯網設備之身分鑑別、資料安全、系統安全及通訊安全等基準項目，透過訪談與實際檢測方式確認是否符合安全基準。

(三) 網域主機安全防護檢測

透過實際檢視方式，針對機關之網域主機進行防毒軟體、安全性修補程式更新及惡意程式檢測。

(四) 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。

(五) 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、 依據系統等級(普、中、高)，針對核心資通系統之存取控制、識別與鑑別、系統與服務獲得、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。

(六) 網路架構檢測

透過訪談及實際檢視方式，驗證網路與系統之管理控制措施、網路與系統之安全控制措施、網路與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。

(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) 網路惡意活動檢視

1、 依照技服中心每日公布之惡意中繼站名單，分別針對機關使用者網段與資通系統管理者網段進行檢測。

2、 機關協助提供即時側錄之完整流量，透過部署技服中心自行研發之 APT 流量偵測規則，針對機關內對外與外對內完整流量進行 APT 活動檢測。

三、實地稽核

由領隊帶領稽核團隊至受稽機關進行實地稽核，如受稽機關為特定非公務機關，請通知上級/監督/中央目的事業主管機關派員出席(實地稽核時程規劃如表 7)。實地稽核項目依據資通安全管理法及各子法法遵事項，整併為三大構面、九大稽核項目，重點說明如下：

(一) 策略面

1、 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、復原測試及資安治理成熟度評估等。

2、 資通安全政策及推動組織：確認資安政策及目標、受稽機關之資安管理及運作、資安組織推動、所屬人員對於資通安全維護之考核機制及獎懲基準、利害關係人管理等。

3、 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、資安人員專業證照及職能訓練等。

(二) 管理面

1、 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、管理與限制使用大陸廠牌資通訊產品。

2、 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。

3、 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、對於所屬/所監督/所管之機關稽核作業、對於所屬/所監督/所管之機關資安事件之審核、對於所屬/所監督/所管之機關資通安全演練之實施。

(三) 技術面

1、 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、政府組態基準／資通安全弱點通報機制／端點偵測及應變機制／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。

2、 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。

3、 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7　實地稽核時程(註 1)

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 ▪ 上級/監督/中央目的事業主管機關
9:30~09:45	稽核團隊稽核前意見交換	稽核團隊
9:45~12:30	實地稽核	▪ 稽核團隊 ▪ 受稽機關
12:30~13:30	午餐(註 2)及彙整稽核發現	稽核團隊
13:30~16:30	實地稽核	▪ 稽核團隊 ▪ 受稽機關
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 ▪ 上級/監督/中央目的事業主管機關

註 1：實地稽核時間將依機關業務複雜度、機關公務場域數量、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資安長出席，以帶領機關之資安管理及追蹤改善。

註 2：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

本院資安稽核作業結束後，依前述稽核分組(共 4 組)，就分組成績表現優良者，本院將函請受稽機關行政獎勵及頒發獎座，相關獎勵說明如表 8。

一、行政獎勵及頒發獎座

依據稽核分組各受稽機關成績，擇取各分組第 1 名之受稽機關評為績優機關，本院將函請績優機關，針對有功人員予以敘獎(嘉獎或記功)，並於本院國家資通安全會報委員會議或相關會議中頒發績優獎座。

表8　獎勵說明

獎勵分式	行政獎勵	頒發獎座
受獎對象	各機關依權責分別對有功人員敘獎	受稽機關
獎勵方式	嘉獎或記功	獎座
各稽核分組	第 1 名	第 1 名

限制條件：

(一) 稽核分組第一組績優機關之技術檢測及實地稽核個別成績，皆須達 75 分(含)以上；稽核分組第二、第三及第四組績優機關之實地稽核成績，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) 各稽核分組之受稽機關稽核成績均未達獎勵標準時，名額從缺。

二、改善作業

(一) 本院將於每季稽核結束後函送資安稽核報告予受稽機關，並請機關就報告中建議及待改善事項研議因應作為及辦理時程，於期限內至本院國家資通安全會報資通安全作業管考系統(https://spm.nat.gov.tw)填報，後續本院將以電子郵件通知受稽機關定期填報。

(二) 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；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 條所述之情形，中央目的事業主管機關應依法辦理之。

(三) 本年資安稽核作業結束後，本院將彙整所有受稽機關之稽核結果，並提出本年資安稽核共同發現事項及建議，供中央機關及地方政府參考改進。

壹拾壹、政府機關配合事項

一、本院於稽核前 1 個月通知受稽機關，並個別通知受稽機關稽核期程，請受稽機關於文到後 3 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」，另稽核分組第一組併需填復「技術檢測基本資料調查表」、「核心資通系統評選表」、「核心資通系統安全防護評量表」及「組態設定現況調查表」，俾利稽核團隊(技術檢測團隊及實地稽核團隊)辦理作業。

二、本年資安實地稽核項目係依資通安全管理法及其子法之相關法遵事項為主，並為因應 COVID-19(武漢肺炎)疫情，故以提供稽核作業說明文件方式取代資安稽核說明會。各上級/監督/中央目的事業主管機關於收到本院今年稽核計畫後，應轉知所屬/所監督/所管機關相關資安稽核事宜，依法要求所屬/所監督/所管機關提報資通安全維護計畫及實施情形，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。

三、本年第二方稽核輔導部分，本院另將於稽核前 1 個月通知受輔導機關及受稽機關，請受輔導機關整備第二方稽核規劃資料等，辦理報院審查等相關事宜，並通知本院派遣專家觀察實際稽核作業。

四、有關受稽機關應填復之文件及配合事項分如表 9、表 10。

表9　附件填復說明

附件	附件名稱	說明	稽核分組第一組受稽機關填寫	稽核分組第二、三、四組受稽機關填寫	稽核團隊填寫
1	資通安全實地稽核項目檢核表	機關資安防護現況，資料將供實地稽核之稽核委員參考	V	V	
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、核心系統儲放地點、AD 放置地點等	V	V	
3	技術檢測基本資料調查表	技術檢測所需相關基本資訊，如內部作業系統分布及升級、安全性更新派送及網路架構等資訊	V		
4	核心資通系統評選表	核心資通系統及資料庫架構及設定資訊 (1) 自行擇選提報 3 個具資料庫之核心資通系統 (2) 以近 2 年新建置之重要系統為優先，原則 2 年內已提報過之系統不重複提報 (3) 由本院裁定檢測標的	V		
5	核心資通系統安全防護評量表	核心資通系統依防護基準配置資訊	V		
6	組態設定現況調查表	組態設定及例外管理狀況	V		
7	技術檢測評分表	技術檢測項目配分說明			V
8	實地稽核評分表	實地稽核項目配分說明			V

表10 受稽機關配合事項

對象	稽核期間	通知日期及方式	協調稽核日期	填寫文件	文件回復日期
受稽機關	第 2 季 5-6 月 第 3 季 7-9 月 第 4 季 10-12 月	稽核前 1 個月函文通知	發通知函文前	全分組： 1.資通安全實地稽核項目檢核表 2.受稽機關現況調查表 第一分組併加填： 1.技術檢測基本資料調查表 2.核心資通系統評選表 3.核心資通系統安全防護評量表 4.組態設定現況調查表	依通知函文所訂期限內

壹拾貳、附件

附件 1　資通安全實地稽核項目檢核表 (分公務機關及特定非公務機關 2 式)

附件 2　受稽機關現況調查表

附件 3　技術檢測基本資料調查表

附件 4　核心資通系統評選表

附件 5　核心資通系統安全防護評量表

附件 6　組態設定現況調查表

附件 7　技術檢測評分表

附件 8　實地稽核評分表