檔　　號:
保存年限:

教育部 函

地址：100217 臺北市中正區中山南路5號
承辦人：江宜倫
電話：02-7712-9036
電子信箱：yilun74@mail.moe.gov.tw

受文者：國立臺北科技大學

發文日期：中華民國111年5月9日
發文字號：臺教資(四)字第1110042489號
速別：普通件
密等及解密條件或保密期限：
附件：行政院秘書長函、111年資通安全稽核計畫、計畫附件1-1、計畫附件1-2、計畫附件2、計畫附件3、計畫附件4、計畫附件5、計畫附件6、計畫附件7、計畫附件8、111年資通安全稽核作業說明（A09000000E_1110042489_senddoc2_Attach1.PDF、A09000000E_1110042489_senddoc2_Attach2.pdf、A09000000E_1110042489_senddoc2_Attach3.pdf、A09000000E_1110042489_senddoc2_Attach4.pdf、A09000000E_1110042489_senddoc2_Attach5.pdf、A09000000E_1110042489_senddoc2_Attach6.pdf、A09000000E_1110042489_senddoc2_Attach7.pdf、A09000000E_1110042489_senddoc2_Attach8.pdf、A09000000E_1110042489_senddoc2_Attach9.pdf、A09000000E_1110042489_senddoc2_Attach10.pdf、A09000000E_1110042489_senddoc2_Attach11.pdf、A09000000E_1110042489_senddoc2_Attach12.pdf）

主旨：函轉行政院111年資通安全稽核計畫及稽核作業說明簡報，請預為準備，請查照。

說明：依行政院秘書長111年4月25日院臺護長字第1110171844號函辦理。

正本：部屬機關(構)及國家運動訓練中心、各國立大專校院、各國立大學附設醫院及農林場、財團法人大學入學考試中心基金會、財團法人私立學校興學基金會、財團法人台灣省中小學校教職員福利文教基金會、財團法人高等教育國際合作基金會、財團法人社教文化基金會、財團法人臺灣省童軍文教基金會、財團法人吳健雄學術基金會、財團法人教育部接受捐助獎學基金會、財團法人高等教育評鑑中心基金會、財團法人中華幼兒教育發展基金會、財團法人蔣經國國際學術交流基金會

副本：電子公文交換章 2022/05/09 16:35:32

檔　　號:
保存年限:

行政院秘書長 函

地址：10058臺北市忠孝東路1段1號
聯絡人：蘇柏菁 02-33568144
電子信箱：pcsu1@ey.gov.tw

受文者：教育部

發文日期：中華民國111年4月25日
發文字號：院臺護長字第1110171844號
速別：普通件
密等及解密條件或保密期限：
附件：如主旨（1110171844-0-0.zip）

主旨：檢送111年資通安全稽核計畫及稽核作業說明簡報資料各1份，請查照辦理。

說明：請貴機關協助轉知所屬公務機關及特定非公務機關並預做整備，本院將依計畫於每季1個月前通知該季受稽機關，另於辦理第二方稽核實地輔導作業1個月前通知受輔導機關。

正本：各部會行總處署
副本：本院國家資通安全會報技術服務中心(含附件) 電子公文交換章 2022/04/25 15:57:56

1110042489 收文日期:111/04/26

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

資通安全實地稽核項目檢核表(適用公務機關)

機關名稱：_____

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(一) 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	是否將全部核心資通系統納入資訊安全管理系統(ISMS)適用範圍？ (A、B 級機關：全部核心資通系統 2 年內完成 ISMS 導入，3 年內通過公正第三方驗證，第三方核發之驗證證書應有 TAF 認證標誌；C 級機關：全部核心資通系統 2 年內完成 ISMS 導入)						
1.3	是否盤點核心資通系統，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)？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
1.4	是否設置資通系統之備援設備，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？(資通系統等級中/高等級者適用)						
1.5	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？						
1.6	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？						
1.7	是否針對核心資通系統制定業務持續運作計畫，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)						
1.8	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)？						
1.9	是否每年落實辦理資安治理成熟度評估？(A、B 級機關適用)						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(二) 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？						
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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
2.5	是否指派副首長或適當人員兼任資通安全長，負責推動及督導機關內資通安全相關事務？						
2.6	是否訂定機關人員辦理業務涉及資通安全事項之考核機制及獎懲基準？						
2.7	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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(三)、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？資安經費編列是否符合業務需要？						
3.2	資安專職人員配置情形？是否有適切分工？ (A 級機關：4 人；B 級機關：2 人；C 級機關：1 人)						
3.3	是否指定專人或專責單位負責資訊服務請求/事件處理、維運及檢討，且有適切分工？						
3.4	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？						
3.5	人員是否瞭解機關之資通安全政策，以及應負之資安責任？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
3.6	資通安全專職人員是否每年接受 12 小時以上之資通安全專業課程訓練或資通安全職能訓練？(A、B、C 級機關適用)						
3.7	資通安全專職人員以外之資訊人員是否每 2 年接受 3 小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受 3 小時以上之資通安全通識教訓練？(A、B、C 級機關適用)						
3.8	一般使用者及主管是否每年接受 3 小時以上之資通安全通識教育訓練？						
3.9	資通安全專職人員是否分別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？						
3.10	資通安全專職人員是否分別各自持有資通安全職能訓練證書 1 張以上，且維持證書之有效性？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(四) 資訊及資通系統盤點及風險評估							
4.1	是否確實盤點資產建立清冊(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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
4.5	是否訂定資通安全風險處理計畫，且妥善處理剩餘之資通安全風險？						
4.6	是否配合新增業務或組織調整時，適時檢視原風險評估作業，以確保相關控制措施之有效性？						
4.7	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？						
4.8	是否列冊管理大陸廠牌資通訊產品，並已於 110 年底前將該產品自公務環境中移除？如該產品仍有與公務環境介接之情況，是否經行政院核定評估同意？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(五) 資通系統或服務委外辦理之管理措施							
5.1	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？						
5.2	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？						
5.3	委外廠商是否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？						
5.4	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？						
5.5	是否依委外業務項目之性質允許委外廠商就委外業務項目分(轉)包？如允許分(轉)包，是否注意分(轉)包之範圍，以及分(轉)包之廠商是否具備資通安全維護措施？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
5.6	是否依資通系統分級，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？						
5.7	對於核心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，並針對非委外廠商自行開發之系統或資源，標示非自行開發之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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
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，且落實執行？						
5.12	是否定期或於知悉委外廠商發生可能影響委外作業之資通安全事件時，對委外廠商所提供之服務、報告及紀錄等進行管理及安全檢視(如廠商端實地稽核、要求廠商提供異常報告、要求廠商提供相關安全檢測紀錄等)，以利後續追蹤及管理？						
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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
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	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？						
5.16	針對涉及資通訊軟體、硬體或服務相關之採購案，契約範圍內之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？是否允許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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(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							
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	是否落實管理階層(如機關首長、資通安全長等)定期(每年至少 1 次)審查 ISMS，以確保其運作之適切性及有效性？						
6.3	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，且落實執行？ (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)						
6.4	是否規劃及執行稽核發現事項改善措施，且定期追蹤改善情形？						
6.5	是否針對特定非公務機關之資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告提出及其他應遵行事項，訂定相關辦法？【中央目的事業主管機關適用】						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
6.6	是否針對所屬/監督之公務機關及所管之 CI 提供者稽核其資通安全維護計畫實施情形，包含訂定稽核計畫、稽核相關紀錄及提出稽核報告等？且針對實施有缺失或待改善者追蹤其改善情形？						
6.7	是否針對所屬/監督之公務機關及所管之特定非公務機關通報之事件於規定時間內完成審核，且於 1 小時內依指定之方式向上通報？(第一級或第二級事件：8 小時內完成審核；第三級或第四級事件：2 小時內完成審核)						
6.8	是否定期針對所屬/監督之公務機關辦理下列演練，且於演練完成後 1 個月內，送交執行情形及成果報告？ (1)每半年規劃及辦理 1 次社交工程演練？ (2)每年規劃及辦理 1 次資安事件通報及應變演練？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(七) 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)						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
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	是否完成政府組態基準導入作業？(A、B 級機關適用)						
7.6	是否完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定方式提交資訊資產盤點資料？(A、B 級公務機關應於核定後 1 年內完成；C 級公務機關應於核定後 2 年內完成)						

<table>
<tr><th>稽核項目</th><th>資通安全稽核檢核項目</th><th>符合</th><th>部分符合</th><th>不符合</th><th>不適用</th><th>簡述符合、部分符合、不符合或不適用之原因</th><th>紀錄文件</th></tr>
<tr><td>7.7</td><td>是否完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定方式提交偵測資料？(A、B 級公務機關應於核定後 2 年內完成)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>7.8</td><td>是否完成下列資通安全防護措施？
<table>
<tr><th>安全防護項目</th><th>A 級</th><th>B 級</th><th>C 級</th><th>D 級</th></tr>
<tr><td>防毒軟體</td><td>v</td><td>v</td><td>v</td><td>v</td></tr>
<tr><td>網路防火牆</td><td>v</td><td>v</td><td>v</td><td>v</td></tr>
<tr><td>電子郵件過濾機制</td><td>v</td><td>v</td><td>v</td><td></td></tr>
<tr><td>入侵偵測及防禦機制</td><td>v</td><td>v</td><td></td><td></td></tr>
<tr><td>應用程式防火牆(具有對外服務之核心資通系統者)</td><td>v</td><td>v</td><td></td><td></td></tr>
<tr><td>進階持續性威脅攻擊防禦</td><td>v</td><td></td><td></td><td></td></tr>
</table></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
7.9	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)？						
7.10	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？						
7.11	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？						
7.12	是否已確實設定防火牆並定期檢視防火牆規則，有效掌握與管理防火牆連線部署？						
7.13	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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
7.14	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？						
7.15	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？						
7.16	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？						
7.17	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？						
7.18	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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
7.19	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？						
7.20	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)？						
7.21	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？						
7.22	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？						
7.23	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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
7.24	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)？						
7.25	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？						
7.26	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？						
7.27	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？						
(八) 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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
8.2	資通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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
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體，注意其安全漏洞通告，且定期評估更新？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(九) 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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
9.4	機關參與本院資安會報對外資通系統實兵演練，是否就相關系統弱點訂定資安防護改善計畫，並落實執行？						
9.5	是否每半年進行 1 次社交工程演練？是否針對開啟郵件、點閱郵件附件或連結之人員加強資安意識教育訓練？						
9.6	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？						
9.7	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？						
9.8	是否訂定資安事件處理過程之內部及外部溝通程序？						
9.9	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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
9.10	是否建置資通安全威脅偵測管理(SOC)機制？監控範圍是否包括「端點偵測及應變機制」與「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？ (A、B 級機關適用)						
9.11	是否依指定方式提交 SOC 監控管理資料？ (A、B 級機關適用)						
9.12	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？						
9.13	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？						
9.14	針對日誌之是否進行存取控管，並有適當之保護控制措施？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
9.15	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)						
9.16	知悉第三級或第四級資通安全事件後，是否由資通安全長召開會議研商相關事宜，並得請相關機關提供協助？						
9.17	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？						
9.18	是否適時進行資通安全情資分享？分享哪些資訊？						

資通安全實地稽核項目檢核表(適用特定非公務機關)

機關名稱：_____

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(一) 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	是否將全部核心資通系統納入資訊安全管理系統(ISMS)適用範圍？ (A、B 級機關：全部核心資通系統 2 年內完成 ISMS 導入，3 年內通過公正第三方驗證，第三方核發之驗證證書應有 TAF 認證標誌；C 級機關：全部核心資通系統 2 年內完成 ISMS 導入)						
1.3	是否盤點核心資通系統，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)？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
1.4	是否設置資通系統之備援設備，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？(資通系統等級中/高等級者適用)						
1.5	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？						
1.6	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？						
1.7	是否針對核心資通系統制定業務持續運作計畫，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)						
1.8	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)？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(二) 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？						
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？						
2.6	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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(三)、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？資安經費編列是否符合業務需要？						
3.2	資通安全專責人員配置情形？是否有適切分工？ (A 級機關：4 人；B 級機關：2 人；C 級機關：1 人)						
3.3	是否指定專人或專責單位負責資訊服務請求/事件處理、維運及檢討，且有適切分工？						
3.4	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？						
3.5	人員是否瞭解機關之資通安全政策，以及應負之資安責任？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
3.6	資通安全專責人員是否每年接受 12 小時以上之資通安全專業課程訓練或資通安全職能訓練？(A、B、C 級機關適用)						
3.7	資通安全專責人員以外之資訊人員是否每 2 年接受 3 小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受 3 小時以上之資通安全通識教訓練？(A、B、C 級機關適用)						
3.8	一般使用者及主管是否每年接受 3 小時以上之資通安全通識教育訓練？						
3.9	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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(四) 資訊及資通系統盤點及風險評估							
4.1	是否確實盤點資產建立清冊(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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
4.5	是否訂定資通安全風險處理計畫，且妥善處理剩餘之資通安全風險？						
4.6	是否配合新增業務或組織調整時，適時檢視原風險評估作業，以確保相關控制措施之有效性？						
4.7	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？						
4.8	是否列冊管理大陸廠牌資通訊產品，並已於 110 年底前將該產品自公務環境中移除？如該產品仍有與公務環境介接之情況，是否經行政院核定評估同意？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(五) 資通系統或服務委外辦理之管理措施							
5.1	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？						
5.2	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？						
5.3	委外廠商是否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？						
5.4	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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
5.5	是否依委外業務項目之性質允許委外廠商就委外業務項目分(轉)包？如允許分(轉)包，是否注意分(轉)包之範圍，以及分(轉)包之廠商是否具備資通安全維護措施？						
5.6	是否依資通系統分級，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？						
5.7	對於核心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，並針對非委外廠商自行開發之系統或資源，標示非自行開發之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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
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，且落實執行？						
5.12	是否定期或於知悉委外廠商發生可能影響委外作業之資通安全事件時，對委外廠商所提供之服務、報告及紀錄等進行管理及安全檢視(如廠商端實地稽核、要求廠商提供異常報告、要求廠商提供相關安全檢測紀錄等)，以利後續追蹤及管理？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
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？						
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	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？						
5.16	針對涉及資通訊軟體、硬體或服務相關之採購案，契約範圍內之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？是否允許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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(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							
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	是否落實管理階層(如機關首長、資通安全長等)定期(每年至少 1 次)審查 ISMS，以確保其運作之適切性及有效性？						
6.3	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，且落實執行？ (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)						
6.4	是否規劃及執行稽核發現事項改善措施，且定期追蹤改善情形？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(七) 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？						

<table>
<tr><th>稽核項目</th><th>資通安全稽核檢核項目</th><th>符合</th><th>部分符合</th><th>不符合</th><th>不適用</th><th>簡述符合、部分符合、不符合或不適用之原因</th><th>紀錄文件</th></tr>
<tr><td>7.5</td><td>是否完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定方式提交資訊資產盤點資料？(A、B 級關鍵基礎設施提供者應於核定後 1 年內完成；C 級關鍵基礎設施提供者應於核定後 2 年內完成)</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>7.6</td><td>是否完成下列資通安全防護措施？
<table>
<tr><th>安全防護項目</th><th>A 級</th><th>B 級</th><th>C 級</th><th>D 級</th></tr>
<tr><td>防毒軟體</td><td>v</td><td>v</td><td>v</td><td>v</td></tr>
<tr><td>網路防火牆</td><td>v</td><td>v</td><td>v</td><td>v</td></tr>
<tr><td>電子郵件過濾機制</td><td>v</td><td>v</td><td>v</td><td></td></tr>
<tr><td>入侵偵測及防禦機制</td><td>v</td><td>v</td><td></td><td></td></tr>
<tr><td>應用程式防火牆(具有對外服務之核心資通系統者)</td><td>v</td><td>v</td><td></td><td></td></tr>
<tr><td>進階持續性威脅攻擊防禦</td><td>v</td><td></td><td></td><td></td></tr>
</table></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
7.7	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)？						
7.8	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？						
7.9	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？						
7.10	是否已確實設定防火牆並定期檢視防火牆規則，有效掌握與管理防火牆連線部署？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
7.11	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？						
7.12	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？						
7.13	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？						
7.14	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？						
7.15	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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
7.16	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？						
7.17	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？						
7.18	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)？						
7.19	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？						
7.20	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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
7.21	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？						
7.22	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)？						
7.23	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？						
7.24	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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
7.25	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？						
(八) 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	資通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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
8.12	是否針對資通系統所使用之外部元件或軟體，注意其安全漏洞通告，且定期評估更新？						
(九) 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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
9.3	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？						
9.4	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？						
9.5	是否訂定資安事件處理過程之內部及外部溝通程序？						
9.6	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？						
9.7	是否建置資通安全威脅偵測管理(SOC)機制？監控範圍是否包括「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？(A、B 級機關適用)						
9.8	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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
9.9	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						
9.10	針對日誌之是否進行存取控管，並有適當之保護控制措施						
9.11	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)						
9.12	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？						
9.13	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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
9.14	是否適時進行資通安全情資分享？分享哪些資訊？						

受稽機關現況調查表(範例)

受稽機關(構)	辦公地點	辦公單位	使用者電腦數量	核心資通系統名稱	系統管理員存取核心資通系統地點	網域主機放置地點 (若無網域主機則不需填寫)	網域主機管理者存取網域主機地點
○○○委員會(範例 1)	臺北市中正區仁愛路○○號(會本部)	綜合規劃處 平台事業管理處 射頻與資源管理處 法律事務處 秘書室 人事室 政風室 主計室	500	無	無	網域主機與濟南路辦公室相同	網域主機與濟南路辦公室相同
	臺北市濟南路○○號(濟南路辦公室)	基礎設施事務處	300	A 系統	濟南路辦公室	濟南機房	濟南路辦公室
	臺北市中正區○○號(北區)	北區監理處	100	無	無	延平機房	北區監理處
	某機房	無	0	B 系統 E 系統	濟南路辦公室	無	無
	某機房	無	0	C 系統 D 系統	濟南路辦公室	無	無

受稽機關(構)	辦公地點	辦公單位	使用者電腦數量	核心資通系統名稱	系統管理員存取核心資通系統地點	網域主機放置地點 (若無網域主機則不需填寫)	網域主機管理者存取網域主機地點
○○部○○中心 (範例 2)	臺北市信義區忠孝東路四段○○號	綜合規劃組 國稅組 地方稅組 徵課管理組 電子發票推廣小組 支援服務室 政風室 人事室 主計室 秘書室	500	A 系統 B 系統 C 系統 D 系統 E 系統	○○中心	1F 機房	○○中心

註：核心資通系統實體位置及管理者存取核心資通系統地點請參考本年資安稽核計畫中**核心資通系統評選表**；另，網域主機即本年資安稽核計畫中**技術檢測基本資料調查表**中第 4 項**網域主機安全防護檢測**。

附件 3 技術檢測基本資料調查表

1.填表人基本資料			
機關（構）名稱			
填表人姓名			
填表人公務電話		分機	
填表人公務 E-mail			
填表日期	111 年_____月_____日		

2.使用者電腦安全檢測		
2.1.使用者電腦弱點掃描		
2.1.1	使用者電腦作業系統版本(可複選)	□Microsoft Windows XP _____台 □Microsoft Windows 7 _____台 □Microsoft Windows 8 _____台 □Microsoft Windows 8.1 _____台 □Microsoft Windows 10 _____台 □Microsoft Windows 11_____台 □其他：_____
2.1.2	是否定期執行使用者電腦弱點掃描作業?	□是， ■最近一次掃描日期：___年___月___日 ■執行廠商：_____ ■掃描工具：_____ ■掃描方式： □由 1 組固定 IP 進行跨網段弱點掃描 □無法跨網段掃描，改由每個網段設定 1 組 IP 進行弱點掃描 □其他：_____ □否
2.2.使用者電腦安全防護檢測		
2.2.1	使用者電腦是否安裝 Java 軟體?	□是，安裝版本：_____ (如：8.0.2810.9) □否
2.2.2	使用者電腦 Java 軟體是否有更新政策?	□是，

		■政策文件名稱：_____ ■更新頻率： □每月 □每兩週 □每週 □每天 □修補程式發布後就更新 □其他：_____ ■最近更新時間：____年___月___日 ■更新方式： □使用者手動下載更新與安裝 □自動下載更新，使用者決定是否安裝 □中控台集中派送 □其他：_____ ■是否有檢視更新紀錄： □是， ➢每隔_____天檢視一次更新紀錄 ➢最近檢視時間：___年___月___日 □否 □否
2.2.3	使用者電腦是否安裝 Adobe Flash Player 軟體?	□是，安裝版本：_____ (如：32.0.0.465) □否
2.2.4	使用者電腦 Adobe Flash Player 是否有更新政策?	□是， ■政策文件名稱：_____ ■更新頻率： □每月 □每兩週 □每週 □每天 □修補程式發布後就更新 □其他：_____ ■最近更新時間：____年___月___日 ■更新方式： □自動安裝更新 □自動下載更新，使用者決定是否安裝

		□中控台集中派送 □其他：_____ ■是否有檢視更新紀錄： □是， ➢每隔_____天檢視一次更新紀錄 ➢最近檢視時間：___年___月___日 □否 □否
2.2.5	使用者電腦是否安裝 Adobe Reader 軟體?	□是，安裝版本：_____ (如：21.001.20142) □否
2.2.6	使用者電腦 Adobe Reader 是否有更新政策?	□是， ■政策文件名稱：_____ ■更新頻率： □每月 □每兩週 □每週 □每天 □修補程式發布後就更新 □其他：_____ ■最近更新時間：____年___月___日 ■更新方式： □自動安裝更新 □自動下載更新，使用者決定是否安裝 □使用者手動下載更新與安裝 □中控台集中派送 □其他：_____ ■是否有檢視更新紀錄： □是， ➢每隔_____天檢視一次更新紀錄 ➢最近檢視時間：___年___月___日 □否 □否

2.2.7	使用者電腦是否安裝防毒軟體?	□是， ■防毒軟體名稱：_____ ■防毒軟體版本：_____ □否
2.2.8	使用者電腦防毒軟體病毒碼是否有更新政策?	□是， ■政策文件名稱：_____ ■更新方式： □集中管控、派送(如防毒軟體中控台) □使用者手動更新 □其他：_____ ■更新頻率： □每月 □每兩週 □每週 □每天 □其他：_____ ■最近更新時間：___年___月___日 ■是否有檢視更新紀錄： □是， ➢每隔_____天檢視一次更新紀錄 ➢最近檢視時間：___年___月___日 □否 □否
2.2.9	使用者電腦作業系統相關修補程式是否有更新政策?	□是， ■政策文件名稱：_____ ■更新來源： □微軟更新伺服器 □機關內部 WSUS 伺服器 □其他：_____ ■更新方式： □使用者手動下載與更新 □自動下載，使用者決定是否更新 □自動下載，設定排程安裝更新

		□自動下載，自動更新 □其他：_____ ■更新頻率： □每月 □每兩週 □每週 □每天 □其他：_____ ■最近更新時間：___年___月___日 ■是否有檢視更新紀錄： □是， ➢每隔_____天檢視一次更新紀錄 ➢最近檢視時間：___年___月___日 □否 □否
2.2.10	使用者電腦之 Microsoft Office 與其他微軟應用程式是否有更新政策?	□是， ■政策文件名稱：_____ ■更新來源： □微軟更新伺服器 □機關內部 WSUS 伺服器 □其他：_____ ■更新方式： □使用者手動下載與更新 □自動下載，使用者決定是否更新 □自動下載，設定排程安裝更新 □自動下載，自動更新 □其他：_____ ■更新頻率： □每月 □每兩週 □每週 □每天 □其他：_____ ■最近更新時間：___年___月___日 ■是否有檢視更新紀錄：

		□是， ➢每隔_____天檢視一次更新紀錄 ➢最近檢視時間：___年___月___日 □否 □否
2.2.11	是否使用 WSUS 派送使用者電腦安全性更新?	□是， ■派送更新類別(可複選)： □Service Pack □Upgrades □工具 □功能套件 □安全性更新 □更新 □更新彙總套件 □定義更新 □重大更新 □驅動程式 ■目前已選擇更新之產品(可複選)： □Developer Tools, Runtimes, and Redistributables □Office □Silverlight □SQL Server □Windows 作業系統 □其他：_____ ■自動核准之更新規則(可複選)： □Service Pack □Upgrades □工具 □功能套件 □安全性更新 □更新 □更新彙總套件 □定義更新 □重大更新 □驅動程式 □否
3.物聯網設備檢測		

※請填復機關內所有的「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 6 類相關設備，項次不足請自行增加，若無某類型設備時，則不需填復該類型設備

※檢測標的為下列可直接使用 RJ45 進行連線之設備、後端管控平台、控制器及伺服器主機:

- 網路印表機：提供紙張輸出功能 (範例:印表機、多功能事務機、影印機等)
- 門禁設備：提供門禁開關或設定功能 (範例:指紋機、指掌靜脈機、門禁卡機等、門禁管理伺服器等)
- 網路攝影機：提供影像錄製或影像顯示/儲存功能 (範例:攝影機與網路影像錄影機(NVR)等)
- 無線網路基地台/無線路由器：提供無線網路分享或控制功能 (範例:無線網路基地台、無線路由器、無線區域網路控制器等)
- 環控系統：提供監控機房溫度或濕度功能 (範例:溫度計、溼度計、機房溫度監控伺服器等)
- 網路儲存裝置(NAS)：提供電子檔案儲存與讀取功能。

3.1.網路印表機 ※項次不足請自行增加

無此類別設備	項次	設備名稱	網址（內部 IP）	廠牌型號/作業系統	放置位置	僅能進入機房連線
□	範例 1	HP 網路印表機	192.168.5.101	HP LaserJet 4300	資訊處 5 樓辦公室	□
	範例 2	HP 網路印表機	192.168.5.102	HP LaserJet 4400	資訊處 6 樓辦公室	□
	範例 3	HP 網路印表機	192.168.5.103	HP LaserJet 4500	資訊處 7 樓辦公室	□
□	1					□
	2					□
	3					□

3.2.門禁設備 ※項次不足請自行增加

□	範例 1	怡群科技門禁卡機	192.168.20.11	怡群科技 Bic-301	人事室 1 樓辦公室	□

	範例 2	門禁管理伺服器	192.168.20.2	Windows 7	資訊處 1 樓機房	■
□	1					□
	2					□
	3					□
3.3.網路攝影機 ※項次不足請自行增加						
□	範例 1	AXIS 網路攝影機	192.168.10.11	AXIS P1354	資訊處 6 樓機房	□
	範例 2	AXIS 網路攝影機	192.168.10.12	AXIS M1033_W	1 樓電梯口	□
	範例 3	網路影像錄影機	192.168.10.20	AXIS 262	1 樓監控室	□
□	1					□
	2					□
	3					□
3.4.無線網路基地台/無線路由器 ※項次不足請自行增加						
□	範例 1	無線區域網路控制器	192.168.0.1	Cisco 2500	資訊處 1 樓辦公室	□
	範例 2	Thin AP	192.168.0.2	Cisco 2602l -x-k9	第 1 會議室	□
	範例 3	Thin AP	192.168.0.3	Cisco 2602l -x-k9	第 2 會議室	□
	範例 4	一般型/SOHO 無線路由器	192.168.0.4	D-link DIR-618	第 3 會議室	□

□	1					□
	2					□
	3					□
3.5.環控系統 ※項次不足請自行增加						
□	範例 1	Advantech 水位計伺服器	192.168.140.55	Advantech WebAccess ver 2.1	資訊處 6 樓機房	■
□	1					□
	2					□
	3					□
3.6.網路儲存裝置(NAS) ※項次不足請自行增加						
□	範例 1	QNAP 威聯通科技 NAS	192.168.140.100	TS-451D2	資訊室 1 樓辦公室	□
	範例 2	Synology 群暉科技 NAS	192.168.140.200	DS418	資訊室 2 樓辦公室	□
□	1					□
	2					□
	3					□
4.網域主機安全防護檢測						
4.1	是否建置網域主機?	□是 □否(請跳至 7.1)				

4.2	網域主機作業系統版本(可複選)	□Windows Server 2003_____台 □Windows Server 2008_____台 □Windows Server 2008 R2_____台 □Windows Server 2012_____台 □Windows Server 2012 R2_____台 □Windows Server 2016_____台 □Windows Server 2019_____台 □Windows Server 2022_____台 □其他：_____
4.3	網域主機防毒軟體病毒碼是否有更新政策?	□是， ■政策文件名稱：_____ ■更新方式： □集中管控、派送(如防毒軟體中控台) □使用者手動更新 □其他：_____ ■更新頻率： □每月 □每兩週 □每週 □每天 □其他：_____ ■最近更新時間：____年___月____日 ■是否有檢視更新紀錄： □是， ➢每隔_____天檢視一次更新紀錄 ➢最近檢視時間：___年___月___日 □否 □否
4.4	網域主機作業系統與微軟應用程式之相關修補程式是否有更新政策?	□是， ■政策文件名稱：_____ ■更新來源： □微軟更新伺服器

		□機關內部 WSUS 伺服器 □其他：_____ ■更新方式： □使用者手動下載與更新 □自動下載，使用者決定是否更新 □自動下載，設定排程安裝更新 □自動下載，自動更新 □其他：_____ ■更新頻率： □每月 □每兩週 □每週 □每天 □其他：_____ ■最近更新時間：___年___月___日 ■是否有檢視更新紀錄： □是， ➢每隔_____天檢視一次更新紀錄 ➢最近檢視時間：___年___月___日 □否 □否
4.5	是否使用 WSUS 派送網域主機安全性更新?	□是， ■派送更新類別(可複選)： □Service Pack □Upgrades □工具 □功能套件 □安全性更新 □更新 □更新彙總套件 □定義更新 □重大更新 □驅動程式 ■目前已選擇更新之產品(可複選)： □Developer Tools, Runtimes, and Redistributables □Office

		□Silverlight □SQL Server □Windows 作業系統 □其他：_____ ■自動核准之更新規則(可複選)： □Service Pack □Upgrades □工具 □功能套件 □安全性更新 □更新 □更新彙總套件 □定義更新 □重大更新 □驅動程式 □否

5.網路架構檢測

5.1.服務主機資訊調查 ※項次不足請自行增加

編號	服務主機類型	無此類型主機	項次	IP	OS 版本
範例 1	網域主機	☑			
範例 2	網域主機	□	1	10.10.10.1	Windows Server 2008 R2
			2	10.10.10.2	Windows Server 2012 R2
			3	10.10.10.3	Windows Server 2012
5.1.1	網域主機	□	1		
			2		
5.1.2	內部 Mail Server	□	1		
			2		
5.1.3	外部 Mail Server	□	1		
			2		
5.1.4	內部 DNS Server	□	1		
			2		
5.1.5	外部 DNS Server	□	1		
			2		

5.1.6	WSUS Server	☐	1		
			2		
5.1.7	防毒伺服器	☐	1		
			2		
5.2.防護主機資訊調查 ※項次不足請自行增加					
編號	防護主機類型	無此類型主機/無部署	項次	設備型號/類型	IP
範例 1	核心資通系統前端是否有 WAF 設備	☑			
範例 2	核心資通系統前端是否有 WAF 設備	☐	1	iMperva X2010	192.168.1.1
			2	iMperva X2010	192.168.1.2
範例 3	惡意中繼站 IP 部署位置	☐	1	防火牆 1	192.168.1.3
			2	防火牆 2	192.168.1.4
5.2.1	核心資通系統前端是否有 WAF 設備	☐	1		
			2		
5.2.2	核心資通系統前端是否有 IPS 設備	☐	1		
			2		
5.2.3	惡意中繼站 IP 部署位置	☐	1		
			2		
5.2.4	惡意中繼	☐	1		

	站 DN 部署位置		2		
5.3.核心網路設備資訊調查　※項次不足請自行增加					
編號	網路設備類型	無此類型設備	項次	設備型號	IP
範例 1	對外線路閘道器	☑			
範例 2	防火牆	☐	1	FG-1000D	10.10.10.1
			2	FG-1000D	10.10.10.2
5.3.1	對外線路閘道器	☐	1		
			2		
5.3.2	防火牆	☐	1		
			2		
5.3.3	核心交換器	☐	1		
			2		
5.4.線路資訊調查　※項次不足請自行增加					
5.4.1	對外線路	(1) ISP 名稱：＿＿＿＿＿＿＿＿＿＿，(如:GSN Internet) 配發 IP：＿＿＿＿＿＿＿＿ (2) ISP 名稱：＿＿＿＿＿＿＿＿＿＿， 配發 IP：＿＿＿＿＿＿＿＿ (3) ISP 名稱：＿＿＿＿＿＿＿＿＿＿， 配發 IP：＿＿＿＿＿＿＿＿ (4) ISP 名稱：＿＿＿＿＿＿＿＿＿＿， 配發 IP：＿＿＿＿＿＿＿＿			

5.4.2	是否與其他機關資料交換	□是， ■機關名稱：_____ ■ISP 名稱：_____ (如:GSN VPN) □否

5.5.網段資訊調查 ※項次不足請自行增加

編號	項目	無此網段	項次	網段 IP
範例 1	是否有網路管理人員網段	☑		
範例 2	是否有網路管理人員網段	□	1	192.168.1.1-20
			2	192.168.2.0/24
5.5.1	是否有網路管理人員網段	□	1	
			2	
5.5.2	是否有系統管理人員網段	□	1	
			2	
5.5.3	是否有資料庫管理人員網段	□	1	
			2	
5.5.4	是否有程式開發人員網段	□	1	
			2	
5.5.5	是否有內部伺服器網段	□	1	
			2	
5.5.6	是否有資料庫網段	□	1	
			2	
5.5.7	是否有系統主機開發、測試網段	□	1	
			2	

5.5.8	是否有虛擬私有網路(VPN)網段	□	1	
			2	
5.5.9	是否有實體隔離網段	□	1	
			2	
5.5.10	是否有網路設備網段	□	1	
			2	
5.5.11	是否有其他未列出網段(請說明網段用途)	□	1	
			2	

5.6.使用者電腦網段配置(User Farm 網段) ※項次不足請自行增加

項次	IP 網段	使用處室	使用者電腦數量	辦公地點	是否加入網域
範例 1	192.168.0.0/24	全機關	150	會本部	■是 □否
範例 2	10.0.1.0/24	綜合規劃處	30	濟南路辦公室	□是 ■否
1					□是 □否
2					□是 □否
3					□是 □否
4					□是 □否
5					□是 □否

6.網路惡意活動檢視

6.1.惡意中繼站連線阻擋檢測

6.1.1	是否可取得技服中心所公布之惡意中繼站名單?	□是， ■技服中心惡意中繼站名單取得方式： □從「國家資通安全通報應變網站」下載 □上級機關提供 □廠商提供

		□其他：_____ ■最近收到名單日期：____年___月___日 □否
6.1.2	是否部署技服中心所公布之惡意中繼站名單?	□是， ■部署週期： □每天 □每週 □每月 □其他：_____ ■最近一次部署日期：____年____月____日 □否
6.1.3	對外連線	■使用者網段 □允許對外連線 □僅能透過 Proxy Server，IP：_____ □不允許對外連線 □其他，連線方式：_____ ■核心資通系統管理者網段 □允許對外連線 □僅能透過 Proxy Server，IP：_____ □不允許對外連線 □其他，連線方式：_____
6.2.APT 網路流量檢測		
6.2.1	對外網路線路是否有作區分?	□統一由單一出口對外連線 □機關區分使用者線路對外連線及其他使用線路對外連線 □補充說明：_____
6.2.2	是否可提供流量側錄連接埠(Mirror Port)，接收涵蓋機關所有內對外與外對內之流量?	□是， ■設備廠牌與型號：_____ □否，請機關於檢測前找出對外流量之主要線路，以利檢測團隊架設檢測設備

附件 4　核心資通系統評選表

範例：系統資訊填寫範例

1.　系統基本資訊	
1.1 核心資通系統名稱	縣政府官網
1.2 系統簡介	提供縣政府同仁使用，功能包含人事業務系統、公文整合資訊系統、差勤子表單、管考系統等項目。
1.3 系統首頁網址	■網址：http://www.test.gov.tw □無
1.4 業務屬性	■行政類　□業務類
1.5 資通系統安全等級	■高　□中　□普
1.6 是否含有個資	□含一般個資與特種個資　□僅有特種個資 ■僅有一般個資　□無個資
1.7 是否曾執行安全檢測 (可複選)	□無　■弱點掃描 ■滲透測試　□源碼掃描
1.8 系統使用對象	■為民服務(提供一般民眾使用) □內部使用(僅供機關內部同仁使用) □其他：_____
1.9 系統是否具備 Load Balance 機制 (若否，請跳至 1.11)	■是 □否
1.10系統由內網連線是否經過 Load Balance 機制	□所有連線強制通過 Load Balance 機制分配 ■僅網頁連線強制通過 Load Balance 機制分配，其餘連線可透過 IP 連線至主機 □所有連線除可通過 Load Balance 機制分配外，亦可透過 IP 連線至主機 □其他：_____
1.11系統使用限制	▪作業系統版本限制：無 ▪作業系統位元限制：■32 位元　□64 位元

	▪瀏覽器版本限制：限用 IE 8 以上版本 ▪需安裝 Client 端程式： ■是 ▪Client 端程式安裝作業系統限制：_____ ▪Client 端程式安裝元件限制：java 8.0.1910.12 □否 ▪其他限制：無
1.12由內部網路連線至核心資通系統是否經過相關安全防護設備	□入侵偵測系統(IDS) □入侵防禦系統(IPS) □網頁應用程式防火牆(WAF) ■防火牆(FW) □其他：_____

2. 系統存取管理	
說明： ▪系統前台登入介面：係指供使用者登入進行系統操作之介面。 ▪系統後台管理登入介面：係指僅供管理人員登入進行系統管理之介面。 ▪若系統無區分前、後台，使用者與管理人員使用相同登入介面時，請將此登入介面視為系統前台登入介面，並填答 2.1~2.7 問項。 ▪外部網路：係指機關使用 IP 範圍外之網路。 ▪內部網路：係指機關使用 IP 範圍內之網路。	
2.1 系統是否有前台登入介面 (若否，請跳至 2.8 作答)	■是　□否
2.2 系統前台登入介面網址	■網址：http://www.test.gov.tw/login □使用 Client 端應用程式登入 □其他：_____
2.3 系統前台登入是否使用單一簽入機制(若否，請跳至 2.5 作答)	■是　□否
2.4 單一簽入系統之管理單位	■自行管理 □主管機關管理，主管機關名稱：_____
2.5 系統前台登入介面連線方式	□僅能透過外部網路連線至系統前台登入介面進

	行操作 ■允許透過內部與外部網路連線至系統前台登入介面進行操作 □僅能透過內部網路連線至系統前台登入介面進行操作
2.6 系統前台登入介面之登入方式	■帳號密碼登入 □軟體憑證登入 □晶片卡登入
2.7 系統前台登入介面允許登入之使用者角色類別(可複選)	■一般使用者　□系統管理員 ■業務承辦使用者　□其他：_____
2.8 系統是否有後台管理登入介面(若否，請跳至 3 作答)	■是　□否
2.9 系統後台管理登入介面網址	■網址：http://www.test.gov.tw/manager/login □使用 Client 端應用程式登入 □其他：_____
2.10系統後台管理登入是否使用單一簽入機制(若否，請跳至 2.12 作答)	■是　□否
2.11單一簽入系統之管理單位	■自行管理 □主管機關管理，主管機關名稱：_____
2.12系統後台管理登入介面連線方式	□僅能透過外部網路連線至系統後台管理登入介面進行操作 □允許透過內部與外部網路連線至系統後台管理登入介面進行操作 ■僅能透過內部網路連線至系統後台管理登入介面進行操作
2.13系統後台管理登入介面登入方式(可複選)	■帳號密碼登入 □軟體憑證登入 □晶片卡登入
2.14系統後台管理登入介面允許登入	□一般使用者　■系統管理員

之使用者角色類別(可複選)	□業務承辦使用者　□其他：＿＿＿＿＿＿

3. 系統主機資訊　**※項次不足請自行增加**

類型 (可複選)	主機名稱	內部 IP	作業系統版本	服務應用程式	主機開啟 Port	實體主機放置位置
■Web Server □AP Server □DB Server □其他	website	10.1.1.1	Windows Server 2012	IIS 8.5	TCP 25 TCP 80	府內機房
□Web Server ■AP Server □DB Server □其他	webap	10.1.1.2	AIX v7.2	Java 1.8	TCP 21 TCP 80 TCP 443	府內機房
□Web Server □AP Server ■DB Server □其他	database	10.1.1.3	Oracle Linux 6.8	Oracle DB 11.2.0.4 SE	TCP 1433	東七機房

4. 資料庫安全管理

4.1.資料庫基本資訊

4.1.1.資料庫名稱(DB Name)	官網資料庫(Official)
4.1.2.資料庫版本	Oracle 11.2.0.4 SE
4.1.3.資料庫類型	■正式資料庫，內部 IP：10.1.1.3 ■備援資料庫，內部 IP：10.1.7.3
4.1.4.資料庫主機作業系統版本	Linux 6.8
4.1.5.資料庫是否含有個資	□僅有特種個資(如：＿＿＿＿＿＿) ■僅有一般個資(如：員工姓名、員編、公務電話、手機、E-Mail、住址) □含一般個資與特種個資(如：＿＿＿＿＿＿) □無個資
4.1.6.資料庫架構簡介	資料庫中包含 Official、WS 及 TS 等 3 個資料庫：

	(1) Official 與 WS 資料庫為縣政府官網資料庫，官網相關資料主要儲存於 Official 資料庫，包含員工姓名、員編、公務電話、手機、E-Mail、住址、內部公開資訊等，官網之系統設定則儲存於 WS 資料庫，可設定是否開啟官網各選單功能。 (2) TS 資料庫則為其它系統(公有場地租借系統)之備援資料庫。	
4.2.資料庫帳號管理		
4.2.1.官方預設帳號	System、Sys	
4.2.2.是否停用或變更官方預設帳號	□是	■否
4.2.3.啟用帳號鎖定次數	■是，於錯誤 5 次後鎖定	□否 (請跳至 4.2.5)
4.2.4.啟用帳號鎖定時間	■是，將鎖定 15 分鐘	□否
4.2.5.啟用「密碼複雜度」原則(可複選)	■是，複雜度原則包含： ■英文 ■數字 ■大小寫 ■特殊符號	□否
4.2.6.啟用「最小密碼長度」原則	■是，密碼長度至少 12 個字元	□否
4.2.7.啟用「密碼最長有效期限」原則	□是，密碼最長有效期為___日	■否
4.3.資料庫資料保護機制		
4.3.1.是否具備資料保護機制(加密)	■是，機制為： □使用資料庫加密 ■資料表欄位內容加密 □其他，請補充說明：_____	□否
4.3.2.是否採用第三方加解密	□是，工具名稱：_____	■否

工具		
4.4 資料庫備份管理機制		
4.4.1.資料庫備份週期	□是，備份週期為： □每天 □每週 ■每月 □其他：_____	□否
4.4.2.資料庫備份執行方式 (可複選)	■完整備份 □差異備份 □增量備份 □其他：_____	
4.4.3.資料庫備份儲存方式 (可複選)	■本地備份 □異地備份，地點說明：_____ □其他：_____	
4.4.4 資料庫備份保護方式	□是，備份保護方式： □備份檔案加密 □硬體加密 ■實體保護(如儲存資料櫃上鎖) □其他：_____	□否
4.4.5.資料庫備份回復測試	■是， ■測試頻率： □每季 □每半年 ■每年 □其他：____ ■最近一次執行日期：110 年 1 月 8 日	□否
4.5.資料庫弱點管理機制		
4.5.1.執行資料庫主機弱點掃描	■是， ■弱點掃描執行頻率： □每週	□否

	□每月 □每季 ■其他：每年 ■最近一次掃描日期：110 年 1 月 4 日 ■執行廠商：中華資安 ■掃描工具：Nessus	
4.5.2.定期修補資料庫主機弱點	■是， ■弱點修補頻率： □每月 □每季 □每半年 ■其他：每年 ■弱點修補門檻： □僅修補高風險弱點 ■修補中風險以上弱點 □修補低風險以上弱點	□否
4.5.3.定期修補資料庫主機安全性更新項目	■是， ■更新方式： □集中管控、派送(如中控台) ■管理者手動更新 □其他： ■更新頻率： ■每月 □每週 □每天 □其他： ■最近更新時間：110 年 2 月 5 日	□否
4.6.資料庫存取與授權		
4.6.1.限制資料庫主機服務埠	■是，僅開啟下列服務埠：20,21,22,25,1521	□否

4.6.2.限制遠端存取的 IP 來源	■是，僅允許下列來源 IP 可存取資料庫： 跳板機 192.168.100.32、192.168.100.33	□否
4.6.3.限制遠端存取的帳號	■是，僅允許下列帳號可遠端存取資料庫： DBA 管理者	□否
4.6.4.禁止管理者帳號透過遠端存取	□是，限制管理者帳號直接透過遠端連線進行操作	■否
4.6.5.資料庫帳號權限最小化原則	■是，依照職務區隔限制資料庫帳號所需權限	□否
4.6.6.資料庫資料傳輸安全機制	■是，資料傳輸安全機制如下： TLS1.0	□否
4.7.資料庫稽核與紀錄		
4.7.1.啟用資料庫帳號變更稽核	■是，針對資料庫的帳號變動(新增、刪除、修改)，留存相關紀錄	□否
4.7.2.啟用資料庫存取稽核	■是，針對資料庫的帳號登出/登入行為，留存相關紀錄	□否
4.7.3.啟用資料庫結構變更稽核	■是，針對資料庫結構新增、刪除、修改等行為，留存相關紀錄	□否
4.7.4.建立稽核紀錄備份週期	□是，備份週期： □每天 □每週 ■每月 □其他：_____	□否
4.7.5.稽核紀錄備份儲存方式	■本機備份 □異地備份 □其他：_____	
4.7.6.設定資料庫主機校時	■是，校時主機 IP 如下：10.132.1.1	□否
4.7.7.定期分析稽核紀錄	■是， ■分析稽核紀錄執行頻率： □每週 ■每月	□否

	□每季 □其他：_____ ■最近一次分析日期:110 年 2 月 5 日 ■分析工具： 稽核紀錄管理系統	

表1　編號 1 系統資訊

1.　系統基本資訊	
1.1 核心資通系統名稱	
1.2 系統簡介	
1.3 系統首頁網址	□網址：_____ □無
1.4 業務屬性	□行政類　□業務類
1.5 資通系統安全等級	□高　□中　□普
1.6 是否含有個資	□含一般個資與特種個資　□僅有特種個資 □僅有一般個資　□無個資
1.7 是否曾執行安全檢測 (可複選)	□無　□弱點掃描 □滲透測試　□源碼掃描
1.8 系統使用對象	□為民服務(提供一般民眾使用) □內部使用(僅供機關內部同仁使用) □其他：_____
1.9 系統是否具備 Load Balance 機制 (若否，請跳至 1.11)	□是 □否
1.10系統由內網連線是否經過 Load Balance 機制	□所有連線強制通過 Load Balance 機制分配 □僅網頁連線強制通過 Load Balance 機制分配，其餘連線可透過 IP 連線至主機 □所有連線除可通過 Load Balance 機制分配外，亦可透過 IP 連線至主機 □其他：_____
1.11系統使用限制	▪作業系統版本限制：_____ ▪作業系統位元限制：□32 位元　□64 位元 ▪瀏覽器版本限制：_____ ▪需安裝 Client 端程式： □是

	▪Client 端程式安裝作業系統限制：_____ ▪Client 端程式安裝元件限制：_____ □否 ▪其他限制：_____
1.12由內部網路連線至核心資通系統是否經過相關安全防護設備	□入侵偵測系統(IDS) □入侵防禦系統(IPS) □網頁應用程式防火牆(WAF) □防火牆(FW) □其他：_____

2. 系統存取管理	
說明： ▪系統前台登入介面：係指供使用者登入進行系統操作之介面。 ▪系統後台管理登入介面：係指僅供管理人員登入進行系統管理之介面。 ▪若系統無區分前、後台，使用者與管理人員使用相同登入介面時，請將此登入介面視為系統前台登入介面，並填答 2.1~2.7 問項。 ▪外部網路：係指機關使用 IP 範圍外之網路。 ▪內部網路：係指機關使用 IP 範圍內之網路。	
2.1 系統是否有前台登入介面(若否，請跳至 2.8 作答)	□是　□否
2.2 系統前台登入介面網址	□網址：_____ □使用 Client 端應用程式登入 □其他：_____
2.3 系統前台登入是否使用單一簽入機制(若否，請跳至 2.5 作答)	□是　□否
2.4 單一簽入系統之管理單位	□自行管理 □主管機關管理，主管機關名稱：_____
2.5 系統前台登入介面連線方式	□僅能透過外部網路連線至系統前台登入介面進行操作 □允許透過內部與外部網路連線至系統前台登入

	介面進行操作 □僅能透過內部網路連線至系統前台登入介面進行操作
2.6 系統前台登入介面之登入方式	□帳號密碼登入 □軟體憑證登入 □晶片卡登入
2.7 系統前台登入介面允許登入之使用者角色類別(可複選)	□一般使用者　□系統管理員 □業務承辦使用者　□其他：_____
2.8 系統是否有後台管理登入介面(若否，請跳至 3 作答)	□是　□否
2.9 系統後台管理登入介面網址	□網址：_____ □使用 Client 端應用程式登入 □其他：_____
2.10系統後台管理登入是否使用單一簽入機制(若否，請跳至 2.12 作答)	□是　□否
2.11單一簽入系統之管理單位	□自行管理 □主管機關管理，主管機關名稱：_____
2.12系統後台管理登入介面連線方式	□僅能透過外部網路連線至系統後台管理登入介面進行操作 □允許透過內部與外部網路連線至系統後台管理登入介面進行操作 □僅能透過內部網路連線至系統後台管理登入介面進行操作
2.13系統後台管理登入介面登入方式(可複選)	□帳號密碼登入 □軟體憑證登入 □晶片卡登入
2.14系統後台管理登入介面允許登入之使用者角色類別(可複選)	□一般使用者　□系統管理員 □業務承辦使用者　□其他：_____

3. 系統主機資訊　**※項次不足請自行增加**

類型	主機名稱	內部 IP	作業系統	服務應用	主機開啟	實體主機

(可複選)			版本	程式	Port	放置位置
□Web Server □AP Server □DB Server □其他						
□Web Server □AP Server □DB Server □其他						
□Web Server □AP Server □DB Server □其他						

4. 資料庫安全管理	
4.1.資料庫基本資訊	
4.1.1.資料庫名稱(DB Name)	
4.1.2.資料庫版本	
4.1.3.資料庫類型	□正式資料庫，內部 IP：_____ □備援資料庫，內部 IP：_____
4.1.4.資料庫主機作業系統版本	
4.1.5.資料庫是否含有個資	□僅有特種個資(如：_____) □僅有一般個資(如：_____) □含一般個資與特種個資(如：_____) □無個資
4.1.6.資料庫架構簡介	
4.2.資料庫帳號管理	
4.2.1.官方預設帳號	

4.2.2.是否停用或變更官方預設帳號	□是	□否
4.2.3.啟用帳號鎖定次數	□是，於錯誤_____次後鎖定	□否 (請跳至 4.2.3)
4.2.4.啟用帳號鎖定時間	□是，將鎖定_____分鐘	□否
4.2.5.啟用「密碼複雜度」原則(可複選)	□是，複雜度原則包含： □英文 □數字 □大小寫 □特殊符號	□否
4.2.6.啟用「最小密碼長度」原則	□是，密碼長度至少_____個字元	□否
4.2.7.啟用「密碼最長有效期限」原則	□是，密碼最長有效期為___日	□否
4.3.資料庫資料保護機制		
4.3.1.是否具備資料保護機制(加密)	□是，機制為： □使用資料庫加密 □資料表欄位內容加密 □其他，請補充說明：_____	□否
4.3.2.是否採用第三方加解密工具	□是，工具名稱：_____	□否
4.4 資料庫備份管理機制		
4.4.1.資料庫備份週期	□是，備份週期為： □每天 □每週 □每月 □其他：_____	□否
4.4.2.資料庫備份執行方式(可複選)	□完整備份 □差異備份 □增量備份	

	□其他：_____	
4.4.3.資料庫備份儲存方式 (可複選)	□本地備份 □異地備份，地點說明：_____ □其他：_____	
4.4.4 資料庫備份保護方式	□是，備份保護方式： □備份檔案加密 □硬體加密 □實體保護(如儲存資料櫃上鎖) □其他：_____	□否
4.4.5.資料庫備份回復測試	□是， ■測試頻率： □每季 □每半年 □每年 □其他：_____ ■最近一次執行日期：___年___月___日	□否
4.5.資料庫弱點管理機制		
4.5.1.執行資料庫主機弱點掃描	□是， ■弱點掃描執行頻率： □每週 □每月 □每季 □其他：_____ ■最近一次掃描日期：___年___月___日 ■執行廠商：_____ ■掃描工具：_____	□否
4.5.2.定期修補資料庫主機弱點	□是， ■弱點修補頻率： □每月	□否

	□每季 □每半年 □其他：_____ ■弱點修補門檻： □僅修補高風險弱點 □修補中風險以上弱點 □修補低風險以上弱點	
4.5.3.定期修補資料庫主機安全性更新項目	□是， ■更新方式： □集中管控、派送(如中控台) □管理者手動更新 □其他：_____ ■更新頻率： □每月 □每週 □每天 □其他：_____ ■最近更新時間：　年　月　日	□否
4.6.資料庫存取與授權		
4.6.1.限制資料庫主機服務埠	□是，僅開啟下列服務埠：_____	□否
4.6.2.限制遠端存取的 IP 來源	□是，僅允許下列來源 IP 可存取資料庫： _____	□否
4.6.3.限制遠端存取的帳號	□是，僅允許下列帳號可遠端存取資料庫： _____	□否
4.6.4.禁止管理者帳號透過遠端存取	□是，限制管理者帳號直接透過遠端連線進行操作	□否
4.6.5.資料庫帳號權限最小化原則	□是，依照職務區隔限制資料庫帳號所需權限	□否
4.6.6.資料庫資料傳輸安全機制	□是，資料傳輸安全機制如下： _____	□否

4.7.資料庫稽核與紀錄		
4.7.1.啟用資料庫帳號變更稽核	□是，針對資料庫的帳號變動(新增、刪除、修改)，留存相關紀錄	□否
4.7.2.啟用資料庫存取稽核	□是，針對資料庫的帳號登出/登入行為，留存相關紀錄	□否
4.7.3.啟用資料庫結構變更稽核	□是，針對資料庫結構新增、刪除、修改等行為，留存相關紀錄	□否
4.7.4.建立稽核紀錄備份週期	□是，備份週期： □每天 □每週 □每月 □其他：_____	□否
4.7.5.稽核紀錄備份儲存方式	□本機備份 □異地備份 □其他：_____	
4.7.6.設定資料庫主機校時	□是，校時主機 IP 如下：_____	□否
4.7.7.定期分析稽核紀錄	□是， ■分析稽核紀錄執行頻率： □每週 □每月 □每季 □其他：_____ ■最近一次分析日期：　年　月　日 ■分析工具：_____	□否

表2　編號 2 系統資訊

1.　系統基本資訊	
1.1 核心資通系統名稱	
1.2 系統簡介	
1.3 系統首頁網址	□網址：_____ □無
1.4 業務屬性	□行政類　□業務類
1.5 資通系統安全等級	□高　□中　□普
1.6 是否含有個資	□含一般個資與特種個資　□僅有特種個資 □僅有一般個資　□無個資
1.7 是否曾執行安全檢測 (可複選)	□無　□弱點掃描 □滲透測試　□源碼掃描
1.8 系統使用對象	□為民服務(提供一般民眾使用) □內部使用(僅供機關內部同仁使用) □其他：_____
1.9 系統是否具備 Load Balance 機制 (若否，請跳至 1.11)	□是 □否
1.10系統由內網連線是否經過 Load Balance 機制	□所有連線強制通過 Load Balance 機制分配 □僅網頁連線強制通過 Load Balance 機制分配，其餘連線可透過 IP 連線至主機 □所有連線除可通過 Load Balance 機制分配外，亦可透過 IP 連線至主機 □其他：_____
1.11系統使用限制	▪作業系統版本限制：_____ ▪作業系統位元限制：□32 位元　□64 位元 ▪瀏覽器版本限制：_____ ▪需安裝 Client 端程式： □是

	▪Client 端程式安裝作業系統限制：_____ ▪Client 端程式安裝元件限制：_____ □否 ▪其他限制：_____
1.12由內部網路連線至核心資通系統是否經過相關安全防護設備	□入侵偵測系統(IDS) □入侵防禦系統(IPS) □網頁應用程式防火牆(WAF) □防火牆(FW) □其他：_____

2. 系統存取管理	
說明： ▪系統前台登入介面：係指供使用者登入進行系統操作之介面。 ▪系統後台管理登入介面：係指僅供管理人員登入進行系統管理之介面。 ▪若系統無區分前、後台，使用者與管理人員使用相同登入介面時，請將此登入介面視為系統前台登入介面，並填答 2.1~2.7 問項。 ▪外部網路：係指機關使用 IP 範圍外之網路。 ▪內部網路：係指機關使用 IP 範圍內之網路。	
2.1 系統是否有前台登入介面 (若否，請跳至 2.8 作答)	□是　　□否
2.2 系統前台登入介面網址	□網址：_____ □使用 Client 端應用程式登入 □其他：_____
2.3 系統前台登入是否使用單一簽入機制(若否，請跳至 2.5 作答)	□是　　□否
2.4 單一簽入系統之管理單位	□自行管理 □主管機關管理，主管機關名稱：_____
2.5 系統前台登入介面連線方式	□僅能透過外部網路連線至系統前台登入介面進行操作 □允許透過內部與外部網路連線至系統前台登入

	介面進行操作 □僅能透過內部網路連線至系統前台登入介面進行操作
2.6 系統前台登入介面之登入方式	□帳號密碼登入 □軟體憑證登入 □晶片卡登入
2.7 系統前台登入介面允許登入之使用者角色類別(可複選)	□一般使用者　□系統管理員 □業務承辦使用者　□其他：_____
2.8 系統是否有後台管理登入介面(若否，請跳至 3 作答)	□是　□否
2.9 系統後台管理登入介面網址	□網址：_____ □使用 Client 端應用程式登入 □其他：_____
2.10系統後台管理登入是否使用單一簽入機制(若否，請跳至 2.12 作答)	□是　□否
2.11單一簽入系統之管理單位	□自行管理 □主管機關管理，主管機關名稱：_____
2.12系統後台管理登入介面連線方式	□僅能透過外部網路連線至系統後台管理登入介面進行操作 □允許透過內部與外部網路連線至系統後台管理登入介面進行操作 □僅能透過內部網路連線至系統後台管理登入介面進行操作
2.13系統後台管理登入介面登入方式(可複選)	□帳號密碼登入 □軟體憑證登入 □晶片卡登入
2.14系統後台管理登入介面允許登入之使用者角色類別(可複選)	□一般使用者　□系統管理員 □業務承辦使用者　□其他：_____

3. 系統主機資訊　**※項次不足請自行增加**

類型	主機名稱	內部 IP	作業系統	服務應用	主機開啟	實體主機

(可複選)			版本	程式	Port	放置位置
□Web Server □AP Server □DB Server □其他						
□Web Server □AP Server □DB Server □其他						
□Web Server □AP Server □DB Server □其他						

4. 資料庫安全管理	
4.1.資料庫基本資訊	
4.1.1.資料庫名稱(DB Name)	
4.1.2.資料庫版本	
4.1.3.資料庫類型	□正式資料庫，內部 IP：_____ □備援資料庫，內部 IP：_____
4.1.4.資料庫主機作業系統版本	
4.1.5.資料庫是否含有個資	□僅有特種個資(如：_____) □僅有一般個資(如：_____) □含一般個資與特種個資(如：_____) □無個資
4.1.6.資料庫架構簡介	
4.2.資料庫帳號管理	
4.2.1.官方預設帳號	

4.2.2.是否停用或變更官方預設帳號	□是	□否
4.2.3.啟用帳號鎖定次數	□是，於錯誤_____次後鎖定	□否 (請跳至 4.2.3)
4.2.4.啟用帳號鎖定時間	□是，將鎖定_____分鐘	□否
4.2.5.啟用「密碼複雜度」原則(可複選)	□是，複雜度原則包含： □英文 □數字 □大小寫 □特殊符號	□否
4.2.6.啟用「最小密碼長度」原則	□是，密碼長度至少_____個字元	□否
4.2.7.啟用「密碼最長有效期限」原則	□是，密碼最長有效期為___日	□否
4.3.資料庫資料保護機制		
4.3.1.是否具備資料保護機制(加密)	□是，機制為： □使用資料庫加密 □資料表欄位內容加密 □其他，請補充說明：_____	□否
4.3.2.是否採用第三方加解密工具	□是，工具名稱：_____	□否
4.4 資料庫備份管理機制		
4.4.1.資料庫備份週期	□是，備份週期為： □每天 □每週 □每月 □其他：_____	□否
4.4.2.資料庫備份執行方式(可複選)	□完整備份 □差異備份 □增量備份	

	□其他：_____	
4.4.3.資料庫備份儲存方式 (可複選)	□本地備份 □異地備份，地點說明：_____ □其他：_____	
4.4.4 資料庫備份保護方式	□是，備份保護方式： □備份檔案加密 □硬體加密 □實體保護(如儲存資料櫃上鎖) □其他：_____	□否
4.4.5.資料庫備份回復測試	□是， ■測試頻率： □每季 □每半年 □每年 □其他：_____ ■最近一次執行日期：___年___月___日	□否
4.5.資料庫弱點管理機制		
4.5.1.執行資料庫主機弱點掃描	□是， ■弱點掃描執行頻率： □每週 □每月 □每季 □其他：_____ ■最近一次掃描日期：___年___月___日 ■執行廠商：_____ ■掃描工具：_____	□否
4.5.2.定期修補資料庫主機弱點	□是， ■弱點修補頻率： □每月	□否

	□每季 □每半年 □其他：_____ ■弱點修補門檻： □僅修補高風險弱點 □修補中風險以上弱點 □修補低風險以上弱點	
4.5.3.定期修補資料庫主機安全性更新項目	□是， ■更新方式： □集中管控、派送(如中控台) □管理者手動更新 □其他：_____ ■更新頻率： □每月 □每週 □每天 □其他：_____ ■最近更新時間：　年　月　日	□否
4.6.資料庫存取與授權		
4.6.1.限制資料庫主機服務埠	□是，僅開啟下列服務埠：_____	□否
4.6.2.限制遠端存取的 IP 來源	□是，僅允許下列來源 IP 可存取資料庫： _____	□否
4.6.3.限制遠端存取的帳號	□是，僅允許下列帳號可遠端存取資料庫： _____	□否
4.6.4.禁止管理者帳號透過遠端存取	□是，限制管理者帳號直接透過遠端連線進行操作	□否
4.6.5.資料庫帳號權限最小化原則	□是，依照職務區隔限制資料庫帳號所需權限	□否
4.6.6.資料庫資料傳輸安全機制	□是，資料傳輸安全機制如下： _____	□否

4.7.資料庫稽核與紀錄		
4.7.1.啟用資料庫帳號變更稽核	□是，針對資料庫的帳號變動(新增、刪除、修改)，留存相關紀錄	□否
4.7.2.啟用資料庫存取稽核	□是，針對資料庫的帳號登出/登入行為，留存相關紀錄	□否
4.7.3.啟用資料庫結構變更稽核	□是，針對資料庫結構新增、刪除、修改等行為，留存相關紀錄	□否
4.7.4.建立稽核紀錄備份週期	□是，備份週期： □每天 □每週 □每月 □其他：_____	□否
4.7.5.稽核紀錄備份儲存方式	□本機備份 □異地備份 □其他：_____	
4.7.6.設定資料庫主機校時	□是，校時主機 IP 如下：_____	□否
4.7.7.定期分析稽核紀錄	□是， ■分析稽核紀錄執行頻率： □每週 □每月 □每季 □其他：_____ ■最近一次分析日期：　年　月　日 ■分析工具：_____	□否

表3　編號 3 系統資訊

1.　系統基本資訊	
1.1 核心資通系統名稱	
1.2 系統簡介	
1.3 系統首頁網址	□網址：_____ □無
1.4 業務屬性	□行政類　□業務類
1.5 資通系統安全等級	□高　□中　□普
1.6 是否含有個資	□含一般個資與特種個資　□僅有特種個資 □僅有一般個資　□無個資
1.7 是否曾執行安全檢測 (可複選)	□無　□弱點掃描 □滲透測試　□源碼掃描
1.8 系統使用對象	□為民服務(提供一般民眾使用) □內部使用(僅供機關內部同仁使用) □其他：_____
1.9 系統是否具備 Load Balance 機制 (若否，請跳至 1.11)	□是 □否
1.10系統由內網連線是否經過 Load Balance 機制	□所有連線強制通過 Load Balance 機制分配 □僅網頁連線強制通過 Load Balance 機制分配，其餘連線可透過 IP 連線至主機 □所有連線除可通過 Load Balance 機制分配外，亦可透過 IP 連線至主機 □其他：_____
1.11系統使用限制	▪作業系統版本限制：_____ ▪作業系統位元限制：□32 位元　□64 位元 ▪瀏覽器版本限制：_____ ▪需安裝 Client 端程式： □是

	▪Client 端程式安裝作業系統限制：_____ ▪Client 端程式安裝元件限制：_____ □否 ▪其他限制：_____
1.12由內部網路連線至核心資通系統是否經過相關安全防護設備	□入侵偵測系統(IDS) □入侵防禦系統(IPS) □網頁應用程式防火牆(WAF) □防火牆(FW) □其他：_____

2. 系統存取管理	
說明： ▪系統前台登入介面：係指供使用者登入進行系統操作之介面。 ▪系統後台管理登入介面：係指僅供管理人員登入進行系統管理之介面。 ▪若系統無區分前、後台，使用者與管理人員使用相同登入介面時，請將此登入介面視為系統前台登入介面，並填答 2.1~2.7 問項。 ▪外部網路：係指機關使用 IP 範圍外之網路。 ▪內部網路：係指機關使用 IP 範圍內之網路。	
2.1 系統是否有前台登入介面 (若否，請跳至 2.8 作答)	□是　　□否
2.2 系統前台登入介面網址	□網址：_____ □使用 Client 端應用程式登入 □其他：_____
2.3 系統前台登入是否使用單一簽入機制(若否，請跳至 2.5 作答)	□是　　□否
2.4 單一簽入系統之管理單位	□自行管理 □主管機關管理，主管機關名稱：_____
2.5 系統前台登入介面連線方式	□僅能透過外部網路連線至系統前台登入介面進行操作 □允許透過內部與外部網路連線至系統前台登入

	介面進行操作 □僅能透過內部網路連線至系統前台登入介面進行操作
2.6 系統前台登入介面之登入方式	□帳號密碼登入 □軟體憑證登入 □晶片卡登入
2.7 系統前台登入介面允許登入之使用者角色類別(可複選)	□一般使用者　□系統管理員 □業務承辦使用者　□其他：_____
2.8 系統是否有後台管理登入介面(若否，請跳至 3 作答)	□是　□否
2.9 系統後台管理登入介面網址	□網址：_____ □使用 Client 端應用程式登入 □其他：_____
2.10系統後台管理登入是否使用單一簽入機制(若否，請跳至 2.12 作答)	□是　□否
2.11單一簽入系統之管理單位	□自行管理 □主管機關管理，主管機關名稱：_____
2.12系統後台管理登入介面連線方式	□僅能透過外部網路連線至系統後台管理登入介面進行操作 □允許透過內部與外部網路連線至系統後台管理登入介面進行操作 □僅能透過內部網路連線至系統後台管理登入介面進行操作
2.13系統後台管理登入介面登入方式(可複選)	□帳號密碼登入 □軟體憑證登入 □晶片卡登入
2.14系統後台管理登入介面允許登入之使用者角色類別(可複選)	□一般使用者　□系統管理員 □業務承辦使用者　□其他：_____

3. 系統主機資訊　**※項次不足請自行增加**

類型	主機名稱	內部 IP	作業系統	服務應用	主機開啟	實體主機

(可複選)			版本	程式	Port	放置位置
□Web Server □AP Server □DB Server □其他						
□Web Server □AP Server □DB Server □其他						
□Web Server □AP Server □DB Server □其他						

4. 資料庫安全管理	
4.1.資料庫基本資訊	
4.1.1.資料庫名稱(DB Name)	
4.1.2.資料庫版本	
4.1.3.資料庫類型	□正式資料庫，內部 IP：_____ □備援資料庫，內部 IP：_____
4.1.4.資料庫主機作業系統版本	
4.1.5.資料庫是否含有個資	□僅有特種個資(如：_____) □僅有一般個資(如：_____) □含一般個資與特種個資(如：_____) □無個資
4.1.6.資料庫架構簡介	
4.2.資料庫帳號管	
4.2.1.官方預設帳號	

4.2.2.是否停用或變更官方預設帳號	□是	□否
4.2.3.啟用帳號鎖定次數	□是，於錯誤_____次後鎖定	□否 (請跳至 4.2.3)
4.2.4.啟用帳號鎖定時間	□是，將鎖定_____分鐘	□否
4.2.5.啟用「密碼複雜度」原則(可複選)	□是，複雜度原則包含： □英文 □數字 □大小寫 □特殊符號	□否
4.2.6.啟用「最小密碼長度」原則	□是，密碼長度至少_____個字元	□否
4.2.7.啟用「密碼最長有效期限」原則	□是，密碼最長有效期為___日	□否
4.3.資料庫資料保護機制		
4.3.1.是否具備資料保護機制(加密)	□是，機制為： □使用資料庫加密 □資料表欄位內容加密 □其他，請補充說明：_____	□否
4.3.2.是否採用第三方加解密工具	□是，工具名稱：_____	□否
4.4 資料庫備份管理機制		
4.4.1.資料庫備份週期	□是，備份週期為： □每天 □每週 □每月 □其他：_____	□否
4.4.2.資料庫備份執行方式(可複選)	□完整備份 □差異備份 □增量備份	

	□其他：_____	
4.4.3.資料庫備份儲存方式 (可複選)	□本地備份 □異地備份，地點說明：_____ □其他：_____	
4.4.4 資料庫備份保護方式	□是，備份保護方式： □備份檔案加密 □硬體加密 □實體保護(如儲存資料櫃上鎖) □其他：_____	□否
4.4.5.資料庫備份回復測試	□是， ■測試頻率： □每季 □每半年 □每年 □其他：_____ ■最近一次執行日期：___年___月___日	□否
4.5.資料庫弱點管理機制		
4.5.1.執行資料庫主機弱點掃描	□是， ■弱點掃描執行頻率： □每週 □每月 □每季 □其他：_____ ■最近一次掃描日期：___年___月___日 ■執行廠商：_____ ■掃描工具：_____	□否
4.5.2.定期修補資料庫主機弱點	□是， ■弱點修補頻率： □每月	□否

	□每季 □每半年 □其他：_____ ■弱點修補門檻： □僅修補高風險弱點 □修補中風險以上弱點 □修補低風險以上弱點	
4.5.3.定期修補資料庫主機安全性更新項目	□是， ■更新方式： □集中管控、派送(如中控台) □管理者手動更新 □其他：_____ ■更新頻率： □每月 □每週 □每天 □其他：_____ ■最近更新時間：　年　月　日	□否
4.6.資料庫存取與授權		
4.6.1.限制資料庫主機服務埠	□是，僅開啟下列服務埠：_____	□否
4.6.2.限制遠端存取的 IP 來源	□是，僅允許下列來源 IP 可存取資料庫： _____	□否
4.6.3.限制遠端存取的帳號	□是，僅允許下列帳號可遠端存取資料庫： _____	□否
4.6.4.禁止管理者帳號透過遠端存取	□是，限制管理者帳號直接透過遠端連線進行操作	□否
4.6.5.資料庫帳號權限最小化原則	□是，依照職務區隔限制資料庫帳號所需權限	□否
4.6.6.資料庫資料傳輸安全機制	□是，資料傳輸安全機制如下： _____	□否

4.7.資料庫稽核與紀錄		
4.7.1.啟用資料庫帳號變更稽核	□是，針對資料庫的帳號變動(新增、刪除、修改)，留存相關紀錄	□否
4.7.2.啟用資料庫存取稽核	□是，針對資料庫的帳號登出/登入行為，留存相關紀錄	□否
4.7.3.啟用資料庫結構變更稽核	□是，針對資料庫結構新增、刪除、修改等行為，留存相關紀錄	□否
4.7.4.建立稽核紀錄備份週期	□是，備份週期： □每天 □每週 □每月 □其他：_____	□否
4.7.5.稽核紀錄備份儲存方式	□本機備份 □異地備份 □其他：_____	
4.7.6.設定資料庫主機校時	□是，校時主機 IP 如下：_____	□否
4.7.7.定期分析稽核紀錄	□是， ■分析稽核紀錄執行頻率： □每週 □每月 □每季 □其他：_____ ■最近一次分析日期：　年　月　日 ■分析工具：_____	□否

附件 5　核心資通系統安全防護評量表

表1　「核心資通系統評選表」編號 1 系統之防護評量表

1.系統環境資訊			
系統名稱		系統等級	□高□中□普
系統性質	□本地端程式□正式網站□測試網站□正式備援網站 □其他：_____		
系統網址	□無 □有，前台網址為:_____ 後台網址為:_____ 其它網址為:_____		
系統主機服務與埠口 註：將依填寫內容檢測埠口開放狀態，請依現況填寫。	系統主機 IP	開放之埠口	目的原因
	(範例)127.0.0.1	80 443	HTTP HTTPS
	主機 1:		
	主機 2:		
	主機 3:		
多重因素認證	身分驗證是否提供多重因素認證： □否 □是，請說明登入方式： (範例：帳號密碼　+　簡訊驗證碼) _____ + _____		
連線核心資通系統進行檢測時，「用戶端」須具備條件(可多選)	□無特定要求 □有(僅支援下列項目，請勾選) 作業系統 □XP □Win 7 □Win 8.x □Win 10 以上 作業系統位元 □32 位元 □64 位元		

	瀏覽器□IE8□IE9□IE10□IE11□Edge□Chrome□FireFox 瀏覽器位元要求□32 位元□64 位元 □作業系統必須加入 AD 網域 必須使用下列元件： □.NET Framework，版本_____ □VC++ Runtime，版本_____ □JRE，版本 _____ □必須使用卡片和讀卡機登入 □必須使用自然人憑證登入 □其他，請說明：_____
2.系統防護評量	
類別	評量項目
普級以上系統適用項目	
識別與鑑別	1. 使用預設密碼登入系統時，應於登入後要求立即變更。
	2. 身分驗證相關資訊不以明文傳輸。
	3. 具備帳戶鎖定機制，帳號登入進行身分驗證失敗達 5 次後，至少 15 分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。 註：請說明登入失敗達_____次，鎖定_____分鐘。如前後台設置不一致請分別提供說明。
	4. 使用密碼進行驗證時，應強制最低密碼複雜度。
	5. 密碼變更時，至少不可以與前 3 次使用過之密碼相同。
	6. 資通系統應遮蔽鑑別過程中之資訊。
系統與服務獲得	7. 發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。

	8. 執行「弱點掃描」安全檢測。 註：請提供檢測報告及修補紀錄。
	9. 於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。
中級以上系統適用項目	
存取控制	10. 採最小權限原則，僅允許使用者(或代表使用者行為之程序)依機關任務及業務功能，完成指派任務所需之授權存取。
識別與鑑別	11. 身分驗證機制應防範自動化程式之登入或密碼更換嘗試。
	12. 密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。
系統與資訊完整性	13. 使用者輸入資料合法性檢查應置放於應用系統伺服器端。
高級系統適用項目	
存取控制	14. 逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。 註：請提供允許閒置時間____分。如前後台設置不一致請分別提供說明。
識別與鑑別	15. 對資通系統之存取採取多重認證技術。
系統與通訊保護	16. 資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。
	17. 使用公開、國際機構驗證且未遭破解之演算法。
	18. 加密金鑰或憑證應定期更換。
系統與服務獲得	19. 執行「源碼掃描」安全檢測。

	註：請提供檢測報告及修補紀錄。
	20. 執行「滲透測試」安全檢測。 註：請提供檢測報告及修補紀錄。
備註 1：資通系統使用單一簽入(SSO)進行權限管控，則亦納入檢測範圍 備註 2：依據「資通安全責任等級分級辦法」第十一條，各機關自行或委外開發之資通系統應依「資通系統防護基準」執行控制措施。若因技術限制、個別資通系統之設計、結構或性質等因素，就特定事項或控制措施之辦理或執行顯有困難者，得經等級提交機關或等級核定機關同意，並報請主管機關備查後，免執行該事項或控制措施；其為主管機關者，經其同意後，免予執行。 若有不適用之項目，請條列於下方欄並詳細說明。	
不適用項目：	

表2　「核心資通系統評選表」編號 2 系統之防護評量表

<table>
<tr><td colspan="4">1.系統環境資訊</td></tr>
<tr><td>系統名稱</td><td></td><td>系統等級</td><td>□高□中□普</td></tr>
<tr><td>系統性質</td><td colspan="3">□本地端程式□正式網站□測試網站□正式備援網站
□其他：_____</td></tr>
<tr><td>系統網址</td><td colspan="3">□無
□有，前台網址為:_____
後台網址為:_____
其它網址為:_____</td></tr>
<tr><td rowspan="5">系統主機服務與埠口
註：將依填寫內容檢測埠口開放狀態，請依現況填寫。</td><td>系統主機 IP</td><td>開放之埠口</td><td>目的原因</td></tr>
<tr><td>(範例)127.0.0.1</td><td>80
443</td><td>HTTP
HTTPS</td></tr>
<tr><td>主機 1:</td><td></td><td></td></tr>
<tr><td>主機 2:</td><td></td><td></td></tr>
<tr><td>主機 3:</td><td></td><td></td></tr>
<tr><td>多重因素認證</td><td colspan="3">身分驗證是否提供多重因素認證：
□否
□是，請說明登入方式：
(範例：帳號密碼 + 簡訊驗證碼)
_____ + _____</td></tr>
<tr><td>連線核心資通系統進行檢測時，「用戶端」須具備條件(可多選)</td><td colspan="3">□無特定要求
□有(僅支援下列項目，請勾選)
作業系統 □XP □Win 7 □Win 8.x □Win 10 以上
作業系統位元 □32 位元 □64 位元
瀏覽器□IE8□IE9□IE10□IE11□Edge□Chrome□FireFox
瀏覽器位元要求□32 位元□64 位元</td></tr>
</table>

	□作業系統必須加入 AD 網域 必須使用下列元件： □.NET Framework，版本_____ □VC++ Runtime，版本_____ □JRE，版本 _____ □必須使用卡片和讀卡機登入 □必須使用自然人憑證登入 □其他，請說明：_____
2.系統防護評量	
類別	評量項目
普級以上系統適用項目	
識別與鑑別	1. 使用預設密碼登入系統時，應於登入後要求立即變更。
	2. 身分驗證相關資訊不以明文傳輸。
	3. 具備帳戶鎖定機制，帳號登入進行身分驗證失敗達 5 次後，至少 15 分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。 註：請說明登入失敗達_____次，鎖定_____分鐘。如前後台設置不一致請分別提供說明。
	4. 使用密碼進行驗證時，應強制最低密碼複雜度。
	5. 密碼變更時，至少不可以與前 3 次使用過之密碼相同。
	6. 資通系統應遮蔽鑑別過程中之資訊。
系統與服務獲得	7. 發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。
	8. 執行「弱點掃描」安全檢測。 註：請提供檢測報告及修補紀錄。

	9. 於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。
中級以上系統適用項目	
存取控制	10. 採最小權限原則，僅允許使用者(或代表使用者行為之程序)依機關任務及業務功能，完成指派任務所需之授權存取。
識別與鑑別	11. 身分驗證機制應防範自動化程式之登入或密碼更換嘗試。
	12. 密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。
系統與資訊完整性	13. 使用者輸入資料合法性檢查應置放於應用系統伺服器端。
高級系統適用項目	
存取控制	14. 逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。 註：請提供允許閒置時間____分。如前後台設置不一致請分別提供說明。
識別與鑑別	15. 對資通系統之存取採取多重認證技術。
系統與通訊保護	16. 資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。
	17. 使用公開、國際機構驗證且未遭破解之演算法。
	18. 加密金鑰或憑證應定期更換。
系統與服務獲得	19. 執行「源碼掃描」安全檢測。 註：請提供檢測報告及修補紀錄
	20. 執行「滲透測試」安全檢測。

	註：請提供檢測報告及修補紀錄

備註 1：資通系統使用單一簽入(SSO)進行權限管控，則亦納入檢測範圍

備註 2：依據「資通安全責任等級分級辦法」第十一條，各機關自行或委外開發之資通系統應依「資通系統防護基準」執行控制措施。若因技術限制、個別資通系統之設計、結構或性質等因素，就特定事項或控制措施之辦理或執行顯有困難者，得經等級提交機關或等級核定機關同意，並報請主管機關備查後，免執行該事項或控制措施；其為主管機關者，經其同意後，免予執行。

若有不適用之項目，請條列於下方欄並詳細說明。

不適用項目：

表3　「核心資通系統評選表」編號 3 系統之防護評量表

1.系統環境資訊			
系統名稱		系統等級	□高□中□普
系統性質	□本地端程式□正式網站□測試網站□正式備援網站 □其他：_____		
系統網址	□無 □有，前台網址為:_____ 後台網址為:_____ 其它網址為:_____		
系統主機服務與埠口 註：將依填寫內容檢測埠口開放狀態，請依現況填寫。	系統主機 IP	開放之埠口	目的原因
	(範例)127.0.0.1	80 443	HTTP HTTPS
	主機 1:		
	主機 2:		
	主機 3:		
多重因素認證	身分驗證是否提供多重因素認證： □否 □是，請說明登入方式： (範例：帳號密碼　+　簡訊驗證碼) _____ + _____		
連線核心資通系統進行檢測時，「用戶端」須具備條件(可多選)	□無特定要求 □有(僅支援下列項目，請勾選) 作業系統 □XP □Win 7 □Win 8.x □Win 10 以上 作業系統位元 □32 位元 □64 位元 瀏覽器□IE8□IE9□IE10□IE11□Edge□Chrome□FireFox 瀏覽器位元要求□32 位元□64 位元		

	□作業系統必須加入 AD 網域 必須使用下列元件： □.NET Framework，版本_____ □VC++ Runtime，版本_____ □JRE，版本 _____ □必須使用卡片和讀卡機登入 □必須使用自然人憑證登入 □其他，請說明：_____
2.系統防護評量	
類別	評量項目
普級以上系統適用項目	
識別與鑑別	1. 使用預設密碼登入系統時，應於登入後要求立即變更。
	2. 身分驗證相關資訊不以明文傳輸。
	3. 具備帳戶鎖定機制，帳號登入進行身分驗證失敗達 5 次後，至少 15 分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。 註：請說明登入失敗達_____次，鎖定_____分鐘。如前後台設置不一致請分別提供說明。
	4. 使用密碼進行驗證時，應強制最低密碼複雜度。
	5. 密碼變更時，至少不可以與前 3 次使用過之密碼相同。
	6. 資通系統應遮蔽鑑別過程中之資訊。
系統與服務獲得	7. 發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。
	8. 執行「弱點掃描」安全檢測。 註：請提供檢測報告及修補紀錄。

	9. 於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。
中級以上系統適用項目	
存取控制	10. 採最小權限原則，僅允許使用者(或代表使用者行為之程序)依機關任務及業務功能，完成指派任務所需之授權存取。
識別與鑑別	11. 身分驗證機制應防範自動化程式之登入或密碼更換嘗試。
	12. 密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。
系統與資訊完整性	13. 使用者輸入資料合法性檢查應置放於應用系統伺服器端。
高級系統適用項目	
存取控制	14. 逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。 註：請提供允許閒置時間____分。如前後台設置不一致請分別提供說明。
識別與鑑別	15. 對資通系統之存取採取多重認證技術。
系統與通訊保護	16. 資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。
	17. 使用公開、國際機構驗證且未遭破解之演算法。
	18. 加密金鑰或憑證應定期更換。
系統與服務獲得	19. 執行「源碼掃描」安全檢測。 註：請提供檢測報告及修補紀錄。
	20. 執行「滲透測試」安全檢測。

	註：請提供檢測報告及修補紀錄。

備註 1：資通系統使用單一簽入(SSO)進行權限管控，則亦納入檢測範圍

備註 2：依據「資通安全責任等級分級辦法」第十一條，各機關自行或委外開發之資通系統應依「資通系統防護基準」執行控制措施。若因技術限制、個別資通系統之設計、結構或性質等因素，就特定事項或控制措施之辦理或執行顯有困難者，得經等級提交機關或等級核定機關同意，並報請主管機關備查後，免執行該事項或控制措施；其為主管機關者，經其同意後，免予執行。

若有不適用之項目，請條列於下方欄並詳細說明。

不適用項目：

附件 6 組態設定現況調查表

1.填表人基本資料			
機關（構）名稱			
填表人姓名			
填表人公務電話		分機	
填表人公務 E-mail			
填表日期	111 年_____月_____日		

1.組態設定安全檢測-作業系統		
項次	GCB 類型	導入情形說明
1.1	Microsoft Windows 7	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度： □測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入 □補充說明：_____ ■導入方式(可複選)： □透過網域主機進行 GPO 派送 □逐台設定 □其他：_____
1.2	Microsoft Windows 8 .1	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度： □測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入

		□補充說明：_____ ■導入方式(可複選)： □透過網域主機進行 GPO 派送 □逐台設定 □其他：_____
1.3	Microsoft Windows 10	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度： □測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入 □補充說明：_____ ■導入方式(可複選)： □透過網域主機進行 GPO 派送 □逐台設定 □其他：_____
1.4	Microsoft Windows Server 2008 R2	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度： □測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入 □補充說明：_____ ■導入方式(可複選)： □透過網域主機進行 GPO 派送 □逐台設定 □其他：_____

1.5	Microsoft Windows Server 2012 R2	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度： □測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入 □補充說明：_____ ■導入方式(可複選)： □透過網域主機進行 GPO 派送 □逐台設定 □其他：_____
1.6	Microsoft Windows Server 2016	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度： □測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入 □補充說明：_____ ■導入方式(可複選)： □透過網域主機進行 GPO 派送 □逐台設定 □其他：_____
1.7	Red Hat Enterprise Linux 8	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度：

		□測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入 □補充說明：_____ ■導入方式(可複選)： □逐台設定 □其他：_____ ■主機數量：_____台 ■主機 IP：_____
2.組態設定安全檢測-瀏覽器		
2.1	Microsoft Internet Explorer 8	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度： □測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入 □補充說明：_____ ■導入方式(可複選)： □透過網域主機進行 GPO 派送 □逐台設定 □其他：_____
2.2	Microsoft Internet Explorer 11	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度： □測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入

		□補充說明：_____ ■導入方式(可複選)： □透過網域主機進行 GPO 派送 □逐台設定 □其他：_____
2.3	Google Chrome	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度： □測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入 □補充說明：_____ ■導入方式(可複選)： □透過網域主機進行 GPO 派送 □逐台設定 □其他：_____
2.4	Mozilla Firefox	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度： □測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入 □補充說明：_____ ■導入方式(可複選)： □透過網域主機進行 GPO 派送 □逐台設定

		□其他：_____
2.5	Microsoft Edge	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度： □測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入 □補充說明：_____ ■導入方式(可複選)： □透過網域主機進行 GPO 派送 □逐台設定 □其他：_____
3.組態設定安全檢測-網通設備		
3.1	Juniper Firewall	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度： □測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入 □補充說明：_____ ■導入方式(可複選)： □逐台設定 □其他：_____ ■設備數量：_____台 ■設備 IP：_____
3.2	Fortinet Fortigate	□無此類設備，無需導入

		□有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度： □測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入 □補充說明：_____ ■導入方式(可複選)： □逐台設定 □其他：_____ ■設備數量：_____台 ■設備 IP：_____
3.3	無線網路	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度： □測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入 □補充說明：_____ ■導入方式(可複選)： □逐台設定 □其他：_____ ■設備數量：_____台 ■設備 IP：_____
3.4	Cisco Firewall	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下：

		■目前導入進度： □測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入 □補充說明：_____ ■導入方式(可複選)： □逐台設定 □其他：_____ ■設備數量：_____台 ■設備 IP：_____
4.組態設定安全檢測-應用程式		
4.1	Exchange Server 2013	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度： □測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入 □補充說明：_____ ■導入方式(可複選)： □逐台設定 □其他：_____ ■主機數量：_____台 ■主機 IP：_____
4.2	Microsoft IIS 8.5	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度：

		□測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入 □補充說明：_____ ■導入方式(可複選)： □逐台設定 □其他：_____ ■主機數量：_____台 ■主機 IP：_____
4.3	Microsoft Word 2016	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度： □測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入 □補充說明：_____ ■導入方式(可複選)： □逐台設定 □其他：_____ _
4.4	Microsoft PowerPoint 2016	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度： □測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入 □補充說明：_____

		■導入方式(可複選)： □逐台設定 □其他：_____ _
4.5	Microsoft Excel 2016	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度： □測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入 □補充說明：_____ ■導入方式(可複選)： □逐台設定 □其他：_____■_
4.6	Microsoft Outlook 2016	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度： □測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入 □補充說明：_____ ■導入方式(可複選)： □逐台設定 □其他：_____
4.7	Apache HTTP Server 2.4	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度：

		□測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入 □補充說明：_____ ■導入方式(可複選)： □逐台設定 □其他：_____ ■主機數量：_____台 ■主機 IP：_____
4.8	SQL Server 2016	□無此類設備，無需導入 □有此類設備，但尚未開始導入 □有此類設備，導入情形如下： ■目前導入進度： □測試中，預定___年___月完成 □部分導入，預定___年___月完成 □已於___年___月完成導入 □補充說明：_____ ■導入方式(可複選)： □逐台設定 □其他：_____ ■主機數量：_____台 ■主機 IP：_____
5.例外管理項目		
5.1	機關組態設定值與 GCB 建議值不同時，需訂定例外管理項目並記錄變更事由及相關配套措施。 機關是否已訂定例外管理項目? □是，	

	■作業系統 ➢Microsoft Windows 7 已訂定____條例外管理項目 ➢Microsoft Windows 8.1 已訂定____條例外管理項目 ➢Microsoft Windows 10 已訂定____條例外管理項目 ➢Microsoft Windows Server 2008 R2 已訂定____條例外管理項目 ➢Microsoft Windows Server 2012 R2 已訂定____條例外管理項目 ➢Microsoft Windows Server 2016 已訂定____條例外管理項目 ➢Red Hat Enterprise Linux 8 已訂定____條例外管理項目 ■瀏覽器 ➢Microsoft Internet Explorer 8 已訂定____條例外管理項目 ➢Microsoft Internet Explorer 11 已訂定____條例外管理項目 ➢Google Chrome 已訂定____條例外管理項目 ➢Mozilla Firefox 已訂定____條例外管理項目 ➢Microsoft Edge 已訂定____條例外管理項目 ■網通設備 ➢Juniper Firewall 已訂定____條例外管理項目 ➢Fortinet Fortigate 已訂定____條例外管理項目 ➢無線網路已訂定____條例外管理項目 ➢Cisco Firewall 已訂定____條例外管理項目 ■應用程式 ➢Exchange Server 2013 已訂定____條例外管理項目 ➢IIS 8.5 已訂定____條例外管理項目 ➢Microsoft Word 2016 已訂定____條例外管理項目 ➢Microsoft PowerPoint 2016 已訂定____條例外管理項目 ➢Microsoft Excel 2016 已訂定____條例外管理項目 ➢Microsoft Outlook 2016 已訂定____條例外管理項目 ➢Apache HTTP Sever 2.4 已訂定____條例外管理項目

	➢SQL Sever 2016 已訂定____條例外管理項目 (例外管理項目請列於 6.2) □否(請跳至 7)

5.2 Windows 7 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	TWGCB-01-001-0002	密碼最長使用期限	90 天以下	180 天	依 ISMS 規範辦理	增加密碼長度並要求需符合密碼複雜度，提升安全性	全機關
1							
2							
3							

5.3 Windows 8.1 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	TWGC B-01-004-0002	密碼最長使用期限	90 天以下	180 天	依 ISMS 規範辦理	增加密碼長度並要求需符合密碼複雜度，提升安全性	全機關
1							
2							
3							

5.4 Windows 10 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	TWGCB-01-005-0002	密碼最長使用期限	90 天以下，但須大於 0 天	180 天	依 ISMS 規範辦理	增加密碼長度並要求需符合密碼複雜度，提升安全性	全機關

1							
2							
3							

5.5 Windows Server 2008 R2 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	TWGC B-01-002-0002	密碼最長使用期限	90 天以下	180 天	依 ISMS 規範辦理	增加密碼長度並要求需符合密碼複雜度，提升安全性	全機關
1							
2							
3							

5.6 Windows Server 2012 R2 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	TWGCB-01-006-0002	密碼最長使用期限	90 天以下，但須大於 0 天	180 天	依 ISMS 規範辦理	增加密碼長度並要求需符合密碼複雜度，提升安全性	全機關
1							
2							
3							

5.7 Windows Server 2016 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	TWGCB-01-007-0002	密碼最長使用期限	90 天以下，但須大於 0 天	180 天	依 ISMS 規範辦理	增加密碼長度並要求需符合密碼複雜度，提升安全性	全機關

1							
2							
3							

5.8 Red Hat Enterprise Linux 8 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	TWGCB-01-008-0227	密碼最長使用期限	90 天以下，但須大於 0	180 天	依 ISMS 規範辦理	增加密碼長度並要求需符合密碼複雜度，提升安全性	全機關
1							
2							
3							

5.9 Internet Explorer 8 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	TWGCB-02-001-0016	即使簽章無效也允許執行或安裝軟體	啟用	停用	導致會計系統線上報表無法列印使用	以受信任網站方式進行限制	會計室
1							
2							
3							

5.10 Internet Explorer 11 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍

範例	TWGCB-02-002-0143	即使簽章無效也允許執行或安裝軟體	停用	啟用	導致會計系統線上報表無法列印使用	以受信任網站方式進行限制	會計室
1							
2							
3							

5.11 Google Chrome 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	TWGCB-02-003-0030	設定擴充功能安裝黑名單	啟用	停用	(機關系統)需使用 Chrome 的多憑證安控模組擴充套件	針對允許使用的擴充功能進行管控	全機關
1							
2							
3							

5.12 Mozilla Firefox 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	TWGCB-02-004-0002	啟用自動下載更新與安裝	true	false	為避免資產盤點問題，不允許自動下載更新與安裝	由資訊室統一進行版本更新派送	全機關
1							
2							

3							

5.13 Microsoft Edge 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	TWGCB-02-005-0011	允許延伸模組	停用	啟用	因業務需使用附加元件，經內部審核流程決議設為啟用	僅允許使用業務所需之延伸模阻	全機關
1							
2							
3							

5.14 Juniper Firewall 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	TWGCB-03-002- 0020	密碼需要最少 4 種不同的字元符號	設置 4 種密碼複雜組合	設置 2 種密碼複雜組合	經內部審核流程決議調整密碼複雜度為小寫英文字母及數字	將密碼長度限制 8 字元調整為 12 字元，以提升安全性	全機關 Juniper Firewall 設備
1							
2							
3							

5.15 Fortinet Fortigate 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	TWGCB-03-003- 0016	密碼最長使用期限	90 天以下	180 天	依 ISMS 規範辦理	增加密碼長度並要求需符合密碼複	全機關 Fortinet

						雜度，提升安全性	Fortigate 設備
1							
2							
3							

5.16 無線網路例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	TWGCB03-001-0 004	變更出廠預設值的密碼內容	12 字元以上	8 個字元以上	依據 ISMS 規定辦理	規範密碼需符合複雜性要求，提升安全性	全機關無線網路設備
1							
2							
3							

5.17 Cisco Firewall 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	TWGCB-03-004- 0005	密碼最長使用期限	90 天	180 天	依 ISMS 規範辦理	增加密碼長度並要求需符合密碼複雜度，提升安全性	全機關 Cisco Firewall 設備
1							
2							
3							

5.18 Exchange Server 2013 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍

範例	TWGCB-04-001- 0026	密碼到期期限	90 天以上	180 天以上	依 ISMS 規範辦理	增加密碼長度並要求需符合密碼複雜度，提升安全性	全機關 Exchange Server 2013 設備
1							
2							
3							

5.19 Microsoft IIS 8.5 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	TWGCB-04-002- 0037	記錄事件目的地	記錄檔和 ETW 事件二者	記錄檔	系統搭配第三方軟體記錄事件	使用第三方軟體紀錄事件並定期檢視	全機關
1							
2							
3							

5.20 Microsoft Word 2016 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	TWGCB04-003-0023	應用程式增益集必須經過信任的發行者簽署	啟用	未設定	因業務需使用自製增益集，經內部審核流程決議設為停用	僅允許使用業務所需之增益集	全機關
1							
2							

3							

5.21 Microsoft PowerPoint 2016 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	TWGCB04-004-0 030	應用程式增益集必須經過信任的發行者簽署	啟用	未設定	因業務需使用自製增益集，經內部審核流程決議設為停用	僅允許使用業務所需之增益集	全機關
1							
2							
3							

5.22 Microsoft Excel 2016 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	TWGCB04-005-0 049	應用程式增益集必須經過信任的發行者簽署	啟用	未設定	因業務需使用自製增益集，經內部審核流程決議設為停用	僅允許使用業務所需之增益集	全機關
1							
2							
3							

5.23 Microsoft Outlook 2016 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	TWGCB04-006-0 088	設定信任的增益集	停用	啟用	因業務需使用增益集，經內部審核流	僅允許使用業務所需之增益集	全機關

					程決議設為啟用		
1							
2							
3							

5.24 Apache HTTP Server 2.4 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	TWGCB-04-007-0042	SSLv3、TLSv1.0 及 TLSv1.1 協定	停用	啟用	因系統使用需求，經內部審核流程決議設為啟用	已規劃於 111 年進行系統升級，以支援 TLSv1.2 協定	全機關
1							
2							
3							

5.25 SQL Server 2016 例外管理清單 ※項次不足請自行增加

項次	TWGCB-ID	原則設定名稱	GCB 建議值	機關設定值	變更事由	配套措施	適用範圍
範例	TWGCB-04-008-0011	預設服務埠	非 1433 埠	1433 埠	因無法於短期時間內完成介接系統調整，將依改善計畫進行調整	透過防火牆規則控管服務埠，預定 111/12 月底完成調整	全機關
1							
2							
3							

6.組態設定安全防護資訊(使用者電腦)

自我檢測方式說明：

1.有加入網域環境

(1) 使用熱鍵「視窗符號+R」開啟「執行」功能，輸入 rsop.msc 開啟「原則結果組」，檢查下列表中組態項目設定值，並確認來源 GPO。

(2) 若透過 rsop.msc 檢查組態項目結果為「尚未定義」且無來源 GPO，請使用熱鍵「視窗符號+R」開啟「執行」功能，輸入 gpedit.msc 開啟「本機群組原則編輯器」，再次確認下列表中組態項目設定值。

2.無加入網域環境，使用單機方式部署 GPO，請使用熱鍵「視窗符號+R」開啟「執行」功能，輸入 gpedit.msc 開啟「本機群組原則編輯器」，確認下列表中組態項目設定值。

項次	類型	項目	設定位置	建議值	機關規定
1	密碼保護	使用可還原的加密來存放密碼	電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則	停用	□啟用 □停用
2		密碼必須符合複雜性需求		啟用	□啟用 □停用
3		密碼最長使用期限		90 天以下	□設為__天 □無規定
4		密碼最短使用期限		1 天	□設為__天 □無規定
5		強制執行密碼歷程記錄		3 以上記憶的密碼	□設為__次 □無規定
6		最小密碼長度		8 個字元以上	□設為__字元 □無規定
7	帳號保護	重設帳戶鎖定計數器的時間間隔	電腦設定\Windows 設定\安全性設定\帳戶原則\帳戶鎖定原則	15 分鐘	□設為___分鐘 □無規定
8		帳戶鎖定期間		15 分鐘	□設為___分鐘 □無規定
9		帳戶鎖定閾值		5 次不正確的登入嘗試	□設為___次 □無規定
10	互動式登入	互動式登入：在密碼到期前提示使用者變更密碼	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項	14 天	□啟用，設為____天 □停用

11		互動式登入：不要求按 CTRL+ALT+DEL 鍵		停用	□尚未定義 □啟用 □停用
12		互動式登入：不要顯示上次登入的使用者名稱		啟用	□啟用 □停用
13	安全設定	網路存取：允許匿名 SID/名稱轉譯	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項	停用	□啟用 □停用
14		網路存取：不允許 SAM 帳戶和共用的匿名列舉		啟用	□啟用 □停用
15		帳戶：Administrator 帳戶狀態		停用	□啟用 □停用
16		帳戶：重新命名系統管理員帳戶		Renamed_Admin	□是，已改為非 Administrator 名稱 □否，仍使用 Administrator 名稱
17		帳戶：Guest 帳戶狀態		停用	□啟用 □停用
18		帳戶：重新命名來賓帳戶名稱		Renamed_Guest	□是，已改為非 Guest 名稱 □否，仍使用 Guest 名稱
19		Microsoft 用戶端：傳送未加密的密碼到其他廠商的 SMB 伺服器		停用	□啟用 □停用

20	自動播放原則	關閉自動播放	電腦設定\系統管理範本\Windows 元件\自動播放原則	啟用：所有磁碟機	□尚未設定 □啟用，並設定為： □光碟機與卸除式媒體磁碟機 □所有磁碟機 □停用
21		AutoRun 的預設行為		啟用/不執行任何 Autorun 命令	□尚未設定 □啟用，並設定為： □不執行任何 AutoRun 命令 □自動執行 AutoRun 命令 □停用
22	記錄檔	安全性\記錄檔大小上限(KB)	電腦設定\系統管理範本\Windows 元件\事件日誌服務\安全性	啟用：81,920 KB	□尚未設定 □啟用，設為_____(KB) □停用
23		安裝程式\記錄檔大小上限(KB)	電腦設定\系統管理範本\Windows 元件\事件日誌服務\安裝程式	啟用：32,768 KB	□尚未設定 □啟用，設為_____(KB) □停用
24		系統\記錄檔大小上限(KB)	電腦設定\系統管理範本\Windows 元件\事件日誌服務\系統	啟用：32,768 KB	□尚未設定 □啟用，設為_____(KB) □停用
25	附件管理員	不要保留檔案附件的區域資訊	使用者設定\系統管理範本\Windows 元件\附件管理員	停用	□尚未設定 □啟用 □停用

26		隱藏移除區域資訊的機制		啟用	□尚未設定 □啟用 □停用
27		開啟附件時通知防毒程式		啟用	□尚未設定 □啟用 □停用
28	螢幕保護	啟用螢幕保護裝置	使用者設定\系統管理範本\控制台\個人化	啟用	□尚未設定 □啟用 □停用
29		以密碼保護螢幕保護裝置		啟用	□尚未設定 □啟用 □停用
30		螢幕保護裝置逾時		啟用：900 秒	□尚未設定 □啟用，設為_____秒 □停用
7.組態設定安全防護資訊(網域主機)					
項次	類型	項目	設定位置	建議值	機關規定
1	密碼保護	使用可還原的加密來存放密碼	電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則	停用	□尚未設定 □啟用 □停用
2		密碼必須符合複雜性需求		啟用	□尚未設定 □啟用 □停用
3		密碼最短使用期限		1 天	□設為___天 □無規定
4		密碼最長使用期限		90(天)以下	□設為___天 □無規定
5		強制執行密碼歷程記錄		3(次)以上記憶的密碼	□設為___次 □無規定
6		最小密碼長度		12 個字元	□設為___字元 □無規定

7	帳戶鎖定原則	重設帳戶鎖定計數器的時間間隔	電腦設定\Windows 設定\安全性設定\帳戶原則\帳戶鎖定原則	15 分鐘	□設為___分鐘 □無規定
8		帳戶鎖定期間		15 分鐘	□設為___分鐘 □無規定
9		帳戶鎖定閾值		5 次不正確的登入嘗試	□設為___次 □無規定
10	使用者權限指派	讓電腦及使用者帳戶受信賴，以進行委派	電腦設定\Windows 設定\安全性設定\本機原則\使用者權限指派	No One	
11		強制從遠端系統進行關閉		Administrators	
12	安全性選項	Microsoft 網路用戶端：傳送未加密的密碼到其他廠商的 SMB 伺服器	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項	停用	□尚未設定 □啟用 □停用
13		Microsoft 網路伺服器：當登入時數到期時，中斷用戶端連線		啟用	□尚未設定 □啟用 □停用
14		互動式登入：網域控制站無法使用時，要快取的先前登入次數		0 次	□設為____次 □尚未設定
15		互動式登入：不要求按 CTRL+ALT+DEL 鍵		停用	□尚未設定 □啟用 □停用
16		互動式登入：不要顯示上次		啟用	□尚未設定 □啟用

		登入的使用者名稱			□停用
17		互動式登入：要求網域控制站驗證以解除鎖定工作站		啟用	□尚未設定 □啟用 □停用
18		修復主控台：允許自動系統管理登入		停用	□尚未設定 □啟用 □停用
19		帳戶：限制使用空白密碼的本機帳戶僅能登入到主控台		啟用	□尚未設定 □啟用 □停用
20		帳戶：重新命名系統管理員帳戶		Renamed_admin	
21		帳戶：Administrator 帳戶狀態		停用	□尚未設定 □啟用 □停用
22		帳戶：Guest 帳戶狀態		停用	□尚未設定 □啟用 □停用
23		裝置：防止使用者安裝印表機驅動程式		啟用	□尚未設定 □啟用 □停用
24		裝置：允許卸除而不須登入		停用	□尚未設定 □啟用 □停用
25		網域成員：停用電腦帳戶密碼變更		停用	□尚未設定 □啟用 □停用
26		網域成員：最長電腦帳戶密碼有效期		30 天	

27		網域成員：安全通道資料加以數位加密或簽章(自動)		啟用	□尚未設定 □啟用 □停用
28		網域成員：要求增強式(Windows 2000 或更新)工作階段金鑰		啟用	□尚未設定 □啟用 □停用
29		網域成員：安全通道資料加以數位加密(可能的話)		啟用	□尚未設定 □啟用 □停用
30		網域控制站：LDAP 伺服器簽章要求		要求簽章	□無 □要求簽章
31		網域控制站：拒絕電腦帳戶密碼變更		停用	□尚未設定 □啟用 □停用
32		網域控制站：允許伺服器操作者排程工作		停用	□尚未設定 □啟用 □停用
33		網路存取：不允許 SAM 帳戶和共用的匿名列舉		啟用	□尚未設定 □啟用 □停用
34		網路存取：讓 Everyone 權限套用到匿名使用者		停用	□尚未設定 □啟用 □停用

35		網路存取：限制匿名存取具名管道和共用		啟用	□尚未設定 □啟用 □停用
36		網路安全性：LAN Manager 驗證等級		只傳送 NTLMv2 回應。拒絕 LM 和 NTLM	□尚未設定 □傳送 LM 和 NTLM 回應 □傳送 LM 和 NTLM-使用 NTLMv2 工作階段安全性 □只傳送 NTLM 回應 □只傳送 NTLMv2 回應 □只傳送 NTLMv2 回應。拒絕 LM □只傳送 NTLMv2 回應。拒絕 LM 和 NTLM
37		網路存取：共用和安全性模式用於本機帳戶		傳統-本機使用者以自身身分驗證	□尚未設定 □傳統-本機使用者以自身身分驗證 □適用於來賓-本機使用者以 Guest 驗證
38		網路安全性：NTLM SSP 為主的(包含		要求 NTLMv2 工作階段安全性	□無 □要求 NTLMv2 工

		安全 RPC)伺服器的最小工作階段安全性		要求 128 位元加密	作階段安全性 □要求 128 位元加密
39		網路安全性：NTLM SSP 為主的(包含安全 RPC)用戶端的最小工作階段安全性		要求 NTLMv2 工作階段安全性 要求 128 位元加密	□無 □要求 NTLMv2 工作階段安全性 □要求 128 位元加密
40		網路安全性：LDAP 用戶端簽章要求		交涉簽章	□無 □交涉簽章 □要求簽章
41		關機：清除虛擬記憶體分頁檔		停用	□尚未設定 □啟用 □停用
42		關機：允許不登入就將系統關機		停用	□尚未設定 □啟用 □停用
43	系統管理範本	關閉自動播放	電腦設定\系統管理範本\Windows 元件\自動播放原則	啟用：所有磁碟機	□尚未設定 □啟用，並設定為： □光碟機與卸除式媒體磁碟機 □所有磁碟機 □停用
44		設定用戶端連線加密層級	• Windows Server 2016、 Windows Server 2012 R2：電腦設定\系統管理範本\Windows	啟用：高等級	□尚未設定 □啟用，並設定為： □用戶端相容

			元件\遠端桌面服務\遠端桌面工作階段主機\安全性 ・Windows Server 2008 R2： 電腦設定\系統管理範本\Windows 元件\終端機服務\終端機伺服器\安全性		□低等級 □高等級 □停用
45	事件記錄服務	安全性\控制記錄檔達到其大小上限時的事件記錄檔行為(Windows Server 2016、Windows Server 2012 R2) 安全性\保留舊事件(Windows Server 2008 R2) *請依作業系統版本回覆	・Windows Server 2016、Windows Server 2012 R2： 電腦設定\系統管理範本\Windows 元件\事件記錄服務\安全性 ・Windows Server 2008 R2： 電腦設定\系統管理範本\Windows 元件\事件日誌服務\安全性	停用	□尚未設定 □啟用 □停用
46		安全性\指定記錄檔大小上限(KB)	・Windows Server 2016、Windows Server 2012 R2： 電腦設定\系統管理範本\Windows	196,608 KB	_____KB

			元件\事件記錄服務\安全性 ・Windows Server 2008 R2： 電腦設定\系統管理範本\Windows 元件\事件日誌服務\安全性		
47		系統\控制記錄檔達到其大小上限時的事件記錄檔行為 (Windows Server 2016、Windows Server 2012 R2) 系統\保留舊事件 (Windows Server 2008 R2) *請依作業系統版本回覆	・Windows Server 2016、Windows Server 2012 R2： 電腦設定\系統管理範本\Windows 元件\事件記錄服務\系統 ・Windows Server 2008 R2： 電腦設定\系統管理範本\Windows 元件\事件日誌服務\系統	停用	□尚未設定 □啟用 □停用
48		系統\指定記錄檔大小上限 (KB)	・Windows Server 2016、Windows Server 2012 R2： 電腦設定\系統管理範本\Windows 元件\事件記錄服務\系統	32,768 KB	_____KB

			• Windows Server 2008 R2： 電腦設定\系統管理範本\Windows 元件\事件日誌服務\系統		
49		應用程式\控制記錄檔達到其大小上限時的事件記錄檔行為 (Windows Server 2016、Windows Server 2012 R2) 應用程式\保留舊事件 (Windows Server 2008 R2) *請依作業系統版本回覆	• Windows Server 2016、Windows Server 2012 R2： 電腦設定\系統管理範本\Windows 元件\事件記錄服務\應用程式 • Windows Server 2008 R2： 電腦設定\系統管理範本\Windows 元件\事件日誌服務\應用程式	停用	□尚未設定 □啟用 □停用
50		應用程式\指定記錄檔大小上限(KB)	• Windows Server 2016、Windows Server 2012 R2： 電腦設定\系統管理範本\Windows 元件\事件記錄服務\應用程式	32,768 KB	_____KB

			• Windows Server 2008 R2： 電腦設定\系統管理範本\Windows 元件\事件日誌服務\應用程式		

附件7 資通安全技術檢測評分表

受稽機關	
技術檢測日期	111 年　月　日~　月　日

項次	技術檢測項目	技術檢測子項	檢測範圍	分數	評分
1	使用者電腦安全檢測	使用者電腦弱點掃描	50 台使用者電腦	10	
		使用者電腦安全防護檢測	5 台使用者電腦	10	
2	物聯網設備檢測	網路印表機檢測	5 台物聯網設備	10	
		門禁設備檢測			
		網路攝影機檢測			
		無線網路基地台/無線路由器檢測			
		環控系統檢測			
		網路儲存裝置(NAS)檢測			
3	網域主機安全防護檢測	網域主機安全防護檢測	1 台網域主機	5	
4	資料庫安全檢測	資料庫安全檢測	1 個核心資料庫	10	
5	核心資通系統安全檢測	核心資通系統內網滲透測試	1 個核心資通系統	20	
		核心資通系統防護基準檢測		5	
6	網路架構檢測	網路架構檢測	機關網路架構	10	
7	組態設定安全檢測	作業系統組態檢測	5 台使用者電腦 1 台網域主機 2 台網通設備 1 台伺服器主機	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	111 年 X 年 X 日中繼站名單	5	
		APT 網路流量檢測	全機關	試行不計分	
			總　分(滿分 100)		

技術檢測結果摘要：

執行人員：_____、_____、_____、_____、_____、

_____、_____、_____、_____

技術檢測項目配分說明

<table>
<tr><th>項次</th><th>檢測項目</th><th>檢測子項</th><th>檢測範圍</th><th>配分</th><th>配分計算方式</th></tr>
<tr><td rowspan="2">1</td><td rowspan="2">使用者電腦安全檢測</td><td>使用者電腦弱點掃描</td><td>50 台使用者電腦</td><td>10</td><td>計算規則：
▪ 每個高風險弱點扣 2 分
▪ 每個中風險弱點扣 1 分
計算公式：
本項得分= 10 – (高風險弱點數) * 2 – (中風險弱點數) * 1
(最低扣至 0 分)</td></tr>
<tr><td>使用者電腦安全防護檢測</td><td>5 台使用者電腦</td><td>10</td><td>計算規則：
<table>
<tr><th>得分</th><th>使用者電腦安全防護
不符合率(Z)</th></tr>
<tr><td>10</td><td>0%</td></tr>
<tr><td>9</td><td>0% < Z≦11%</td></tr>
<tr><td>8</td><td>11% < Z≦22%</td></tr>
<tr><td>7</td><td>22% < Z≦33%</td></tr>
<tr><td>6</td><td>33% < Z≦44%</td></tr>
<tr><td>5</td><td>44% < Z≦55%</td></tr>
<tr><td>4</td><td>55% < Z≦66%</td></tr>
<tr><td>3</td><td>66% < Z≦77%</td></tr>
<tr><td>2</td><td>77% < Z≦88%</td></tr>
<tr><td>1</td><td>88% < Z<100%</td></tr>
<tr><td>0</td><td>100%</td></tr>
</table>
▪ 不符合電腦台數：</td></tr>
</table>

<table>
<tr><th>項次</th><th>檢測項目</th><th>檢測子項</th><th>檢測範圍</th><th>配分</th><th>配分計算方式</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>X=安全性未更新電腦數+具惡意程式電腦數+防毒軟體未更新(或未安裝)電腦數+應用軟體未更新電腦數
▪ 使用者電腦安全防護不符合率：
Z=X/(受測電腦台數*4)*100%
計算公式：
本項得分=使用者電腦安全防護不符合率(Z)對應之得分</td></tr>
<tr><td>2</td><td>物聯網設備檢測</td><td>物聯網設備檢測</td><td>5 台物聯網設備(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))</td><td>10</td><td>計算規則：
<table>
<tr><th>得分</th><th>檢測基準不符合率(X)</th></tr>
<tr><td>10</td><td>0%</td></tr>
<tr><td>9</td><td>0% < X≦11%</td></tr>
<tr><td>8</td><td>11% < X≦22%</td></tr>
<tr><td>7</td><td>22% < X≦33%</td></tr>
<tr><td>6</td><td>33% < X≦44%</td></tr>
<tr><td>5</td><td>44% < X≦55%</td></tr>
<tr><td>4</td><td>55% < X≦66%</td></tr>
<tr><td>3</td><td>66% < X≦77%</td></tr>
<tr><td>2</td><td>77% < X≦88%</td></tr>
<tr><td>1</td><td>88% < X<100%</td></tr>
<tr><td>0</td><td>100%</td></tr>
</table>
▪ 檢測基準不符合率：
X=(不符合檢測基準之項數/檢測項目總數)*100%
計算公式：
本項得分=檢測基準不符合率(X)對應之得分</td></tr>
</table>

<table>
<tr><th>項次</th><th>檢測項目</th><th>檢測子項</th><th>檢測範圍</th><th>配分</th><th>配分計算方式</th></tr>
<tr><td>3</td><td>網域主機安全防護檢測</td><td>網域主機安全防護檢測</td><td>1 台網域主機</td><td>5</td><td>計算規則：
▪ 防毒軟體更新得分= 網域主機防毒軟體已安裝且病毒碼已更新則得 2 分
▪ 安全性更新得分= 網域主機安全性更新皆已安裝則得 2 分
▪ 惡意程式檢測得分=網域主機未發現惡意程式則得 1 分
計算公式：
本項得分=防毒軟體更新得分+安全性更新得分+惡意程式檢測得分</td></tr>
<tr><td>4</td><td>資料庫安全檢測</td><td>資料庫安全檢測</td><td>1 個核心資料庫</td><td>10</td><td>計算規則：
▪ 每個不符合項目扣 1 分
計算公式：
本項得分= 10 – (不符合項數 * 1)</td></tr>
<tr><td rowspan="2">5</td><td rowspan="2">核心資通系統安全檢測</td><td>核心資通系統內網滲透測試</td><td rowspan="2">1 個核心資通系統</td><td>20</td><td>計算規則：
▪ 每個高風險弱點扣 2 分
▪ 每個中風險弱點扣 1 分
計算公式：
本項得分=20 – (高風險弱點數 * 2) – (中風險弱點數 * 1)
(最低扣至 0 分)</td></tr>
<tr><td>核心資通系統防護基準檢測</td><td>5</td><td>計算規則：
<table>
<tr><th>得分</th><th>資通系統防護基準
不符合率(X)</th></tr>
<tr><td>5</td><td>0%</td></tr>
<tr><td>4</td><td>0% < X≦25%</td></tr>
<tr><td>3</td><td>25% < X≦50%</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>項次</th><th>檢測項目</th><th>檢測子項</th><th>檢測範圍</th><th>配分</th><th>配分計算方式</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>
<table>
<tr><td>2</td><td>50% < X≦75%</td></tr>
<tr><td>1</td><td>75% < X< 100%</td></tr>
<tr><td>0</td><td>100%</td></tr>
</table>
▪ 資通系統防護基準不符合率：
X=(系統防護基準不符合項數/系統防護基準檢測總數)*100%
計算公式：
本項得分=資通系統防護基準不符合率(X)對應之得分</td></tr>
<tr><td>6</td><td>網路架構檢測</td><td>網路架構檢測</td><td>機關網路架構</td><td>10</td><td>計算規則：
▪ 每個高風險弱點扣 2 分
▪ 每個中風險弱點扣 1 分
計算公式：
本項得分= 10 – (高風險弱點數 * 2) – (中風險弱點數 * 1)
(最低扣至 0 分)</td></tr>
<tr><td>7</td><td>組態設定安全檢測</td><td>組態設定安全檢測</td><td>5 台使用者電腦、1 台網域主機、2 台網通設備、1 台伺服器主機</td><td>15</td><td>計算規則：
<table>
<tr><th>得分</th><th>組態設定項目不符合率(X)</th></tr>
<tr><td>15</td><td>0%</td></tr>
<tr><td>14</td><td>0% < X≦7%</td></tr>
<tr><td>13</td><td>7% < X≦14%</td></tr>
<tr><td>12</td><td>14% < X≦21%</td></tr>
<tr><td>11</td><td>21% < X≦28%</td></tr>
<tr><td>10</td><td>28% < X≦35%</td></tr>
<tr><td>9</td><td>35% < X≦42%</td></tr>
<tr><td>8</td><td>42% < X≦50%</td></tr>
<tr><td>7</td><td>50% < X≦58%</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>項次</th><th>檢測項目</th><th>檢測子項</th><th>檢測範圍</th><th>配分</th><th>配分計算方式</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>
<table>
<tr><td>6</td><td>58% < X≦65%</td></tr>
<tr><td>5</td><td>65% < X≦72%</td></tr>
<tr><td>4</td><td>72% < X≦79%</td></tr>
<tr><td>3</td><td>79% < X≦86%</td></tr>
<tr><td>2</td><td>86% < X≦93%</td></tr>
<tr><td>1</td><td>93% < X <100%</td></tr>
<tr><td>0</td><td>100%</td></tr>
</table>
▪ X=(組態設定不符合項數/組態設定檢測總數)*100%
計算公式：
本項得分=組態設定項目不符合率(X)對應之得分</td></tr>
<tr><td>8</td><td>網路惡意活動檢視</td><td>惡意中繼站連線阻擋檢測</td><td>中繼站名單</td><td>5</td><td>計算規則：
<table>
<tr><th>得分</th><th>惡意中繼站未阻擋率(Z)</th></tr>
<tr><td>5</td><td>0%</td></tr>
<tr><td>4</td><td>0% < Z≦25%</td></tr>
<tr><td>3</td><td>25% < Z≦50%</td></tr>
<tr><td>2</td><td>50% < Z≦75%</td></tr>
<tr><td>1</td><td>75% < Z < 100%</td></tr>
<tr><td>0</td><td>100%</td></tr>
</table>
▪ 一般使用者網段惡意中繼站未阻擋率：
X= (未阻擋惡意中繼站數/檢測惡意中繼站總數)*100%
▪ 核心資通系統管理者網段惡意中繼站未阻擋率：</td></tr>
</table>

項次	檢測項目	檢測子項	檢測範圍	配分	配分計算方式
					Y= (未阻擋惡意中繼站數/檢測惡意中繼站總數)*100% ▪ 不符合率(Z) =(X+Y)/2， 若無核心資通系統管理者網段，則不計Y，不符合率(Z)=X **計算公式：** 本項得分=惡意中繼站未阻擋率(Z)對應之得分
得 分 總 計 (滿分 100 分)					**計算公式：** 得分總計= (檢測項目總得分/檢測項目總分)*100 ▪ 若為**無網域主機**環境，則不計第 3 項[網域主機安全防護檢測]，得分總計= (檢測項目 1~2 與 4~8 項總得分/ 95) * 100 ▪ 若**無核心資料庫**，則不計第 4 項[資料庫安全檢測]，得分總計= (檢測項目 1~3 與 5~8 項總得分/ 90) * 100 ▪ 若**無網域主機環境與核心資料庫**，則不計第 3 項[網域主機安全防護檢測]與第 4 項[資料庫安全檢測]，得分總計= (檢測項目 1~2 與 5~8 項總得分/ 85) * 100

實地稽核評分表

一、稽核評分　　受稽機關：0000000000　稽核日期：111/00/00

稽核構面	稽核項目	評分
策略面	一、核心業務及其重要性(10分)： 優(10-9分)、良(8-7分)、佳(6-5分)、可(4分)、待改進(3分(含)以下)	
	二、資通安全政策及推動組織(10分)： 優(10-9分)、良(8-7分)、佳(6-5分)、可(4分)、待改進(3分(含)以下)	
	三、專責人力及經費配置(10分)： 優(10-9分)、良(8-7分)、佳(6-5分)、可(4分)、待改進(3分(含)以下)	
管理面	四、資訊及資通系統盤點及風險評估(10分)： 優(10-9分)、良(8-7分)、佳(6-5分)、可(4分)、待改進(3分(含)以下)	
	五、資通系統或服務委外辦理之管理措施(10分)： 優(10-9分)、良(8-7分)、佳(6-5分)、可(4分)、待改進(3分(含)以下)	
	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分)： 優(10-9分)、良(8-7分)、佳(6-5分)、可(4分)、待改進(3分(含)以下)	
技術面	七、資通安全防護及控制措施(20分)： 優(20-17分)、良(16-13分)、佳(12-9分)、可(8分)、待改進(7分(含)以下)	
	八、資通系統發展及維護安全(10分)： 優(10-9分)、良(8-7分)、佳(6-5分)、可(4分)、待改進(3分(含)以下)	
	九、資通安全事件通報應變及情資評估因應(10分)： 優(10-9分)、良(8-7分)、佳(6-5分)、可(4分)、待改進(3分(含)以下)	
得　　分(滿分100分)		

二、稽核發現

項次	內容分類	稽核發現內容	對應稽核分類	稽核項目代碼及驗證項目細項	備註
一	待改善事項	依資通安全責任等級分級辦法資通系統防護基準規定，已針對防護安全等級高之資通系統，委外執行滲透測試安全檢測，部分中風險等級漏洞仍未修復，建議針對資通安全健診與安全性檢測之弱點修補情形，建立內部陳報與管控程序，以強化安全防護作為。	資通系統防護基準	C0701-系統與資訊完整性-漏洞修復	(範例)

項次	內容分類	稽核發現內容	對應稽核分類	稽核項目代碼及驗證項目細項	備註

委員簽名：_____

111年資通安全稽核作業說明

行政院資通安全處

111年4月

大綱

- **依據與目的**
- 稽核計畫
- 作業說明
- 獎勵及改善作業
- 受稽機關配合事項

依據與目的

- **依據**
  - 資通安全管理法(以下簡稱資安法)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
  - 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

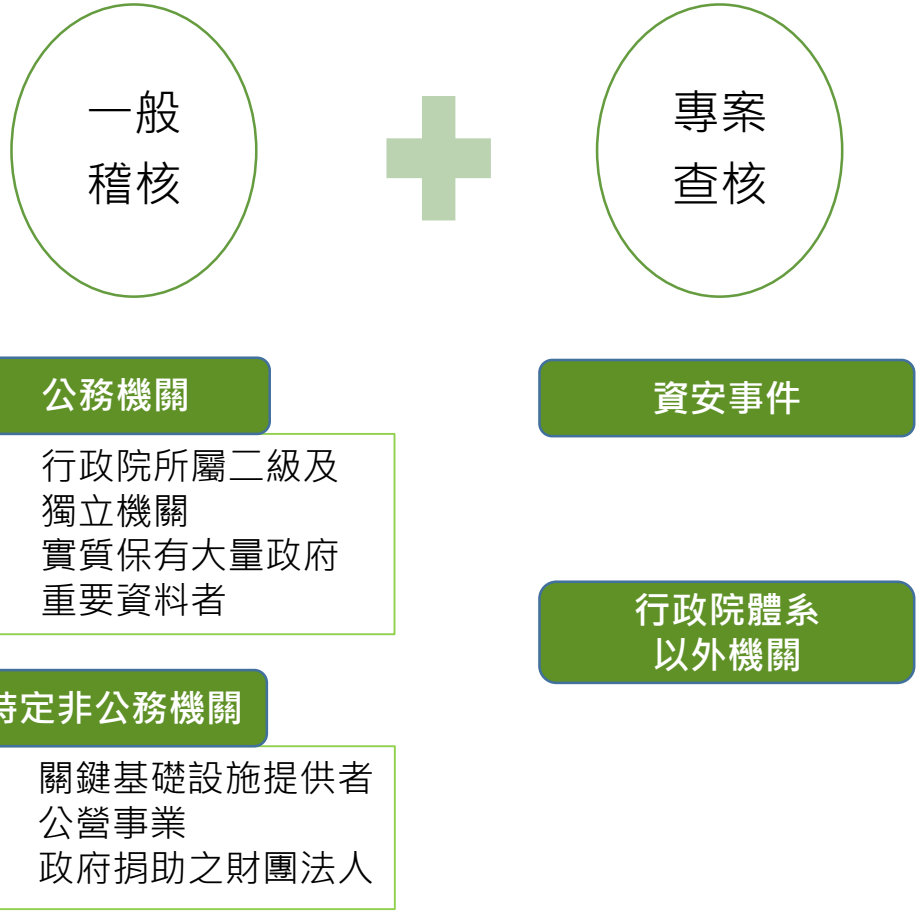
- **目的**
  - 查核公務機關及特定非公務機關辦理資通安全管理法及其子法相關法遵事項之落實情形
  - 經由外部稽核各機關資通安全維護計畫實施情形，改善並強化機關資通安全防護工作之完整性及有效性，以持續精進管理政府整體資安風險

大綱

- 依據與目的
- **稽核計畫**
- 作業說明
- 獎勵及改善作業
- 受稽機關配合事項

稽核計畫 - 稽核說明

項目	說明
法源依據	法律授權
稽核對象	資安法授權本院稽核對象之範圍，其他四院、地方政府以行政協調方式進行
稽核類型	• 一般稽核 • 專案查核
實地稽核項目	依資安法及資通安全維護計畫架構調修



稽核計畫 - 作業階段及時程

階段	作業時程	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 (5-12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
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

1個月前發文受稽機關

稽核計畫 - 稽核團隊

- **領隊**
  - 由行政院國家資通安全會報副召集人或協同副召集人擔任(得由策略面委員代理)
- **實地稽核委員**
  - 依策略、管理及技術3個構面，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專家學者擔任
  - 每個受稽機關原則分配7名委員：策略面2人、管理面2人及技術面3人
- **實地稽核觀察員**
  - 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
- **技術檢測團隊**
  - 由行政院國家資通安全會報技術服務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，每場次技術人員至多10名

稽核計畫 - 受稽機關

- **受稽對象**
- **1.公務機關**
  - 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
  - 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
  - 實質保有大量政府重要資料者
- **2. 特定非公務機關**(關鍵基礎設施提供者、公營事業及政府捐助之財團法人)
  - 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
  - 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
  - 本年或近2年曾發生資安事件者
  - 近3年未曾受稽核或稽核結果建議持續關注協助者
  - 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)

稽核計畫 - 稽核準則

- 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)
- 受稽機關之資通安全維護計畫
- 資訊安全管理系統國家標準 CNS 27001:2014
  (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

稽核計畫 - 稽核範圍、方式與配分

- **稽核範圍**

  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各項資通安全管理政策、程序等

- **稽核方式**

稽核分組	一	二	三	四
共通屬性	1.公務機關 2.資通安全責任等級**A級**	1.公務機關 2.資通安全責任等級**B級**	1.公務機關 2.資通安全責任等級**C級**	特定非公務機關
家數	6	5	6	6
技術檢測(3天)	V	-	-	-
實地稽核(1天)	V	V	V	V

稽核計畫 - 稽核範圍、方式與配分

● 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

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
- 若受稽機關無網域主機、資料庫環境，則技術檢測分數將依比例調整

稽核計畫 - 稽核範圍、方式與配分

- 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

構面	實地稽核項目	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

稽核計畫 - 稽核範圍、方式與配分

- **評分方式**

(一)第一分組

整體總成績=技術檢測得分×30% + 實地稽核得分×70%

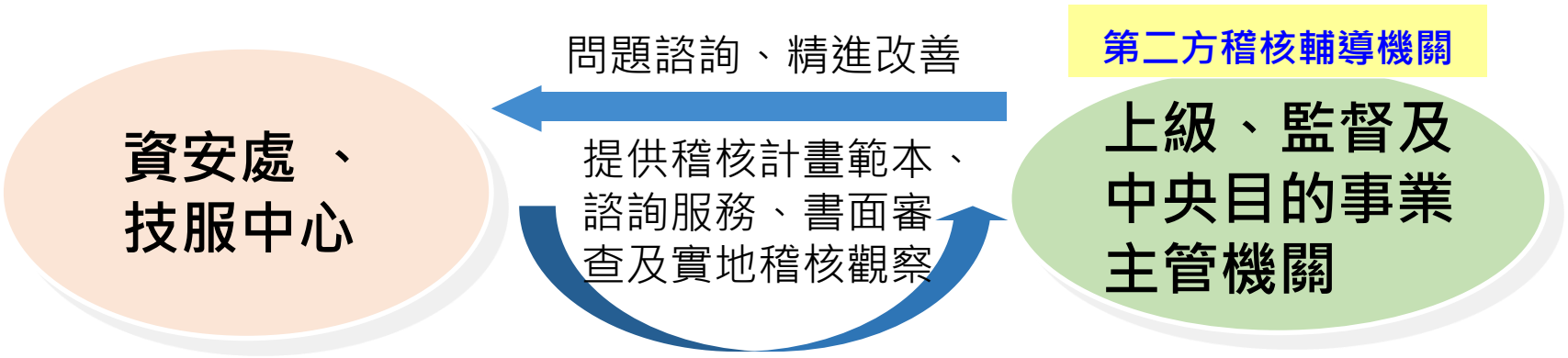
(二)第二、三、四分組

整體總成績=實地稽核得分×100%

工控系統資安稽核試行作業

- 受稽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

第二方稽核輔導作業說明



1.書面審查

- 上級、監督及中央目的事業主管機關所提稽核計畫
- 受稽之所屬、所監督及所管機關之資通安全維護計畫
- 於稽核前提供書面資料審查

2.實地驗證

- 遴聘2位專家進行實地稽核觀察作業
- 對於整體稽核規劃及執行程序提出精進建議

3.作業成效

透過第二方稽核各上級、監督及中央目的事業主管機關對所屬、所監督及所管機關稽核整體流程，檢視法令落實度及稽核成效

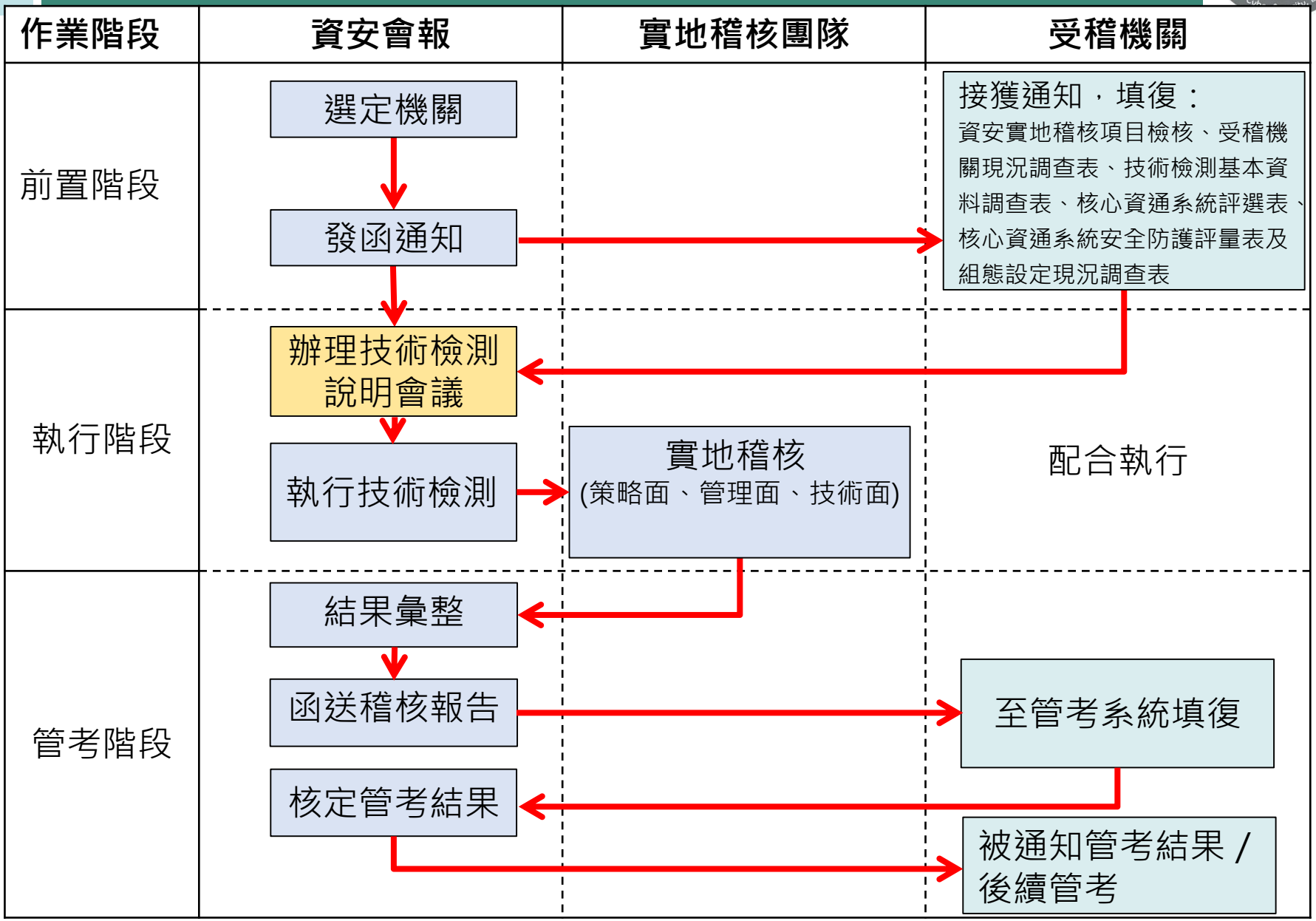
第二方稽核輔導觀察項目與產出

書面審查階段
實地驗證階段

大綱

- 依據與目的
- 稽核計畫
- **作業說明**
- 獎勵及改善作業
- 受稽機關配合事項

作業說明


作業階段
資安會報
實地稽核團隊
受稽機關
前置階段
選定機關
發函通知
接獲通知，填復：
資安實地稽核項目檢核、受稽機關現況調查表、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
執行階段
辦理技術檢測說明會議
執行技術檢測
實地稽核
(策略面、管理面、技術面)
配合執行
管考階段
結果彙整
函送稽核報告
至管考系統填復
核定管考結果
被通知管考結果 / 後續管考

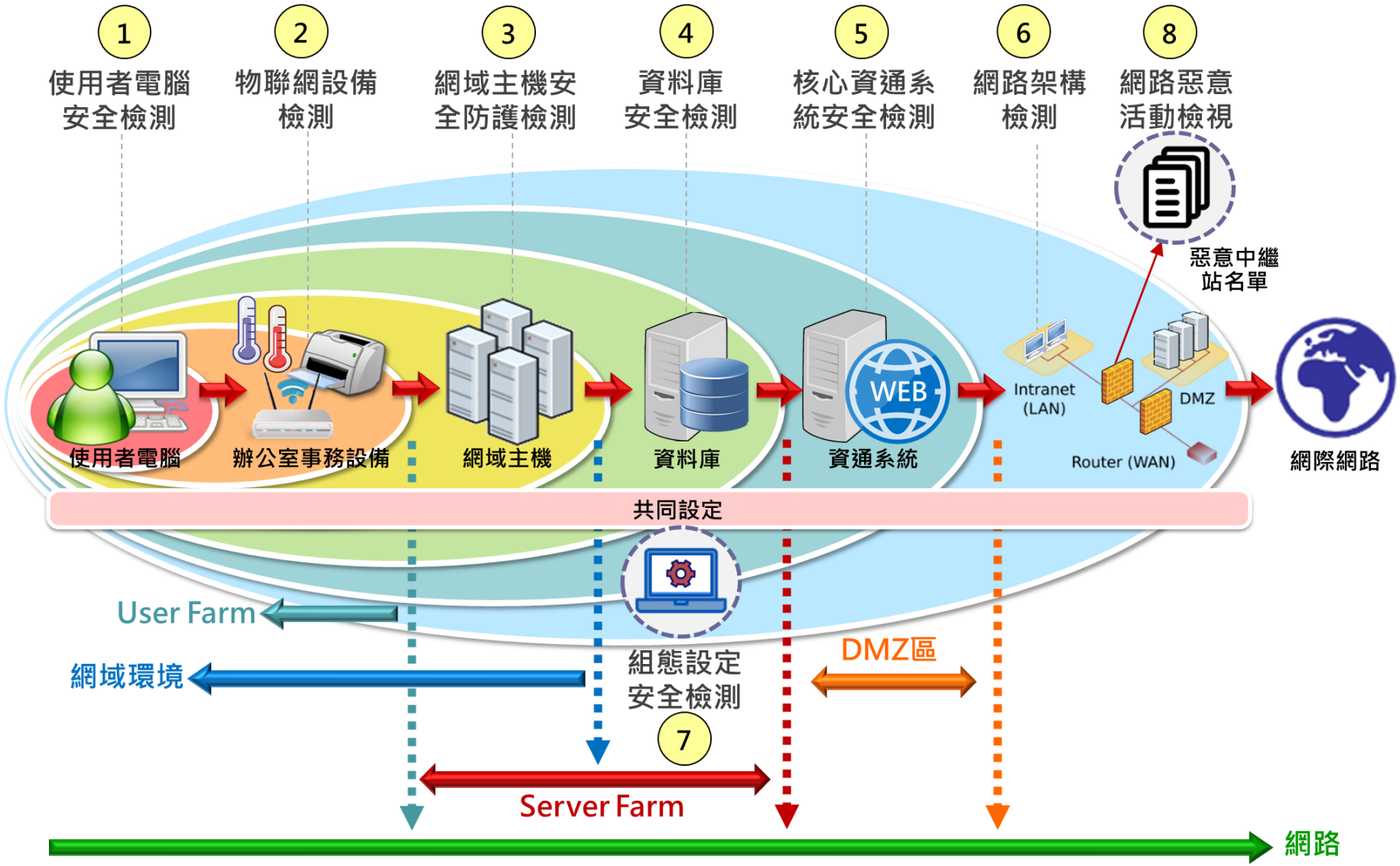
作業說明

- **機關自評**
  - 受稽機關填寫「資通安全實地稽核項目檢核表」、「受稽機關現況調查表」、「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」
  - 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)
- **技術檢測**
  - 於辦理第一分組之實地稽核前，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
- **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，將請其所屬上級/監督/中央目的事業主管機關派員出席
  - 實地稽核項目依據資通安全管理法及其子法相關法遵事項，整併為三大構面、九大稽核項目，詳參附件「資通安全實地稽核項目檢核表」

作業說明 - 技術檢測項目

項次	檢測項目	檢測子項
1	**使用者電腦安全檢測**	使用者電腦弱點掃描
		使用者電腦安全防護檢測
2	**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)等物聯網設備檢測
3	**網域主機安全防護檢測**	防毒軟體檢測
		安全性更新檢測
		惡意程式檢測
4	**資料庫安全檢測**	
5	**核心資通系統安全檢測**	核心資通系統內網滲透測試
		核心資通系統防護基準檢測
6	**網路架構檢測**	
7	**組態設定安全檢測**	作業系統組態檢測
		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
		APT網路流量檢測

作業說明 - 技術檢測框架


1
使用者電腦安全檢測
2
物聯網設備檢測
3
網域主機安全防護檢測
4
資料庫安全檢測
5
核心資通系統安全檢測
6
網路架構檢測
8
網路惡意活動檢視
惡意中繼站名單
使用者電腦
辦公室事務設備
網域主機
資料庫
WEB
資通系統
Intranet (LAN)
DMZ
Router (WAN)
網際網路
共同設定
User Farm
網域環境
組態設定安全檢測
7
DMZ區
Server Farm
網路

作業說明 - 技術檢測項目(1/4)

項次	技術檢測項目	執行範圍	執行方式
1	使用者電腦安全檢測	全機關	• 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
2	物聯網設備檢測	5台物聯網設備	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**
3	網域主機安全防護檢測	1台網域主機	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**

作業說明 - 技術檢測項目(2/4)

項次	技術檢測項目	執行範圍	執行方式
4	資料庫安全檢測	1個資料庫	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
5	核心資通系統安全檢測	1個核心資通系統	• 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** • 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**
6	網路架構檢測	全機關	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

作業說明 - 技術檢測項目(3/4)

項次	技術檢測項目	執行範圍	執行方式
7	組態設定安全檢測	5台使用者電腦	• 針對作業系統(Win7、Win8.1及Win10)**抽測18項政府組態基準設定** • 針對瀏覽器(IE8、IE11、Google Chrome、Mozilla Firefox及Edge)**抽測12項政府組態基準設定** • 針對應用程式(Word 2016、Excel 2016、PowerPoint 2016及Outlook 2016)**抽測12項政府組態基準設定**
		1台網域主機	針對作業系統(Windows Server 2008 R2、Windows Server 2012 R2及Windows Server 2016)**抽測50項政府組態基準設定**
		2台網通設備	抽測**2類**網通設備(Juniper Firewall、Fortinet Fortigate、無線網路及Cisco Firewall)**各10項政府組態基準設定**
		1台伺服器主機	抽測**1類**(Exchange Server 2013、IIS 8.5、Apache HTTP Server 2.4、SQL Server 2016及Red Hat Enterprise Linux 8)**10項政府組態基準設定**

作業說明 - 技術檢測項目(4/4)

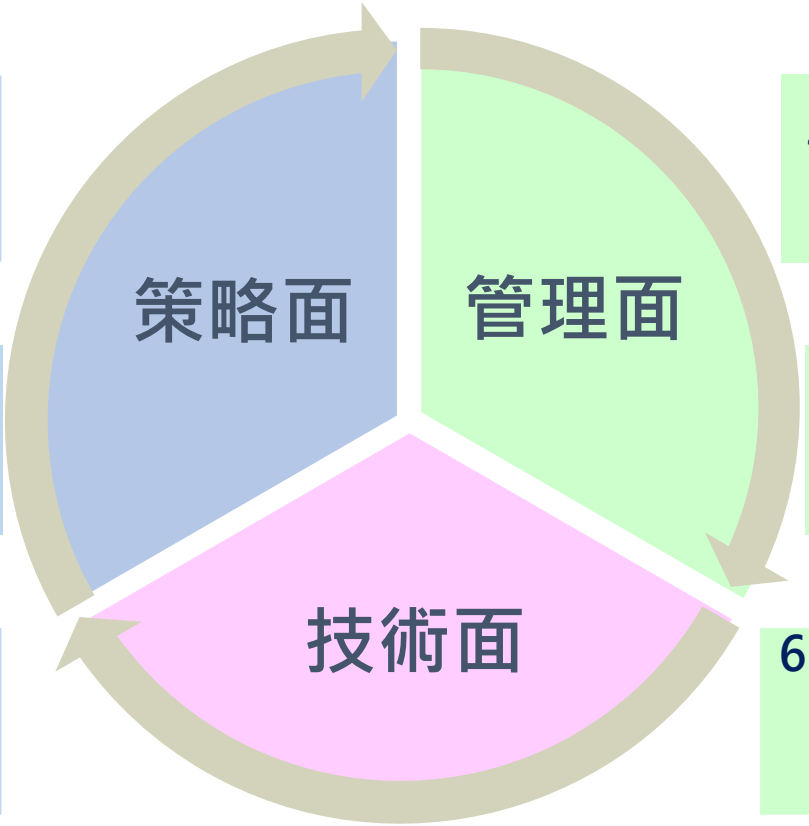
項次	技術檢測項目	執行範圍	執行方式
8	網路惡意活動檢視	全機關	• 依照技服中心每日公布之惡意中繼站名單，分別針對機關**使用者網段及資通系統管理者網段**進行檢測 • 機關協助提供即時側錄之完整流量，透過部署技服中心自行研發之APT流量偵測規則，針對**機關內對外與外對內完整流量**進行APT活動檢測

作業說明 - 實地稽核項目

1.核心業務及其重要性

2.資通安全政策及推動組織

3.專責人力及經費配置



4.資通系統盤點及風險評估

5.資通系統或服務委外辦理之管理措施

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

7.資通安全防護及控制措施

8.資通系統發展及維護安全

9.資通安全事件通報應變及情資評估因應

- 實地稽核項目檢核表，依「資通安全管理法」相關規定之不同，分為公務機關、特定非公務機關2式

作業說明 - 實地稽核項目說明(1/3)

● 策略面

項次	稽核項目	稽核重點說明
1	核心業務及其重要性	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	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	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

作業說明 - 實地稽核項目說明(2/3)

● 管理面

項次	稽核項目	稽核重點說明
4	資通系統盤點及風險評估	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
5	資通系統或服務委外辦理之管理措施	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
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	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

作業說明 - 實地稽核項目說明(3/3)

● 技術面

項次	稽核項目	稽核重點說明
7	資通安全防護及控制措施	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
8	資通系統發展及維護安全	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
9	資通安全事件通報應變及情資評估因應	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

作業說明 - 實地稽核議程

時間	工作項目	參與人員
09:00~09:30	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
09:30~09:45	稽核團隊稽核前意見交換	稽核團隊
09:45~12:30	實地稽核	• 稽核團隊 • 受稽機關
12:30~13:30	午餐(註)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

※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資安長出席

註：午餐委請受稽機關代訂，由稽核團隊支付費用

大綱

- 依據與目的
- 稽核計畫
- 作業說明
- 獎勵及改善作業
- 受稽機關配合事項

獎勵及改善作業 - 獎勵方式

- **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
  - **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

※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

※個別分組之受稽機關未達獎勵標準時，名額從缺

獎勵及改善作業 - 改善作業

- 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
- 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
- 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

大綱

- 依據與目的
- 稽核計畫
- 作業說明
- 獎勵及改善作業
- 受稽機關配合事項

受稽機關配合事項(1/2)

1. 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
2. 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
3. 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

受稽機關配合事項(2/2)

期間/作業	技術檢測	實地稽核
籌備作業	• 指定聯絡窗口 – 協調技術檢測時程 – 參與技術檢測說明會 – 確認組織架構與檢測執行範圍 – 填復技術檢測調查表件 – 確認技術檢測環境配合事項 – 提供交通資訊	• 指定聯絡窗口 – 協調實地稽核日期 – 確認稽核執行範圍 – 填復實地稽核調查表件 – 邀請機關資安長主持會議，並邀請上級/監督/中央目的主管機關代表、政風/會計/業務相關人員參與 – 提供交通資訊(停車指引、換證、接待等)
執行作業	• 安排適宜之會議室-檢測人員約10位 – 啟始會議、結束會議 – 技術檢測作業空間 (會議室) • 會議簡報投影 • 請協助代訂檢測人員中餐便當 • 當日聯繫與協調相關單位/人員配合技術檢測	• 安排適宜之會議室- 稽核團隊約16位(領隊/稽核委員/觀察員/工作人員) – 啟始會議、結束會議 – 策略面、管理面、技術面稽核執行地點(會議室) • 會議簡報投影 • 資安防護辦理情形簡報(約15分鐘) • 整備實地稽核之佐證文件與資料 • 聯繫與協調相關單位/人員接受稽核 • 代訂當日便當 • 稽核報告列印與簽署

主辦機關聯絡方式

- 行政院資安處
  蘇柏菁：02-3356-8144
  pcsu1@ey.gov.tw
  賴妍帆：02-3356-8064
  yeflai@ey.gov.tw

- 技服中心
  陳彥青：02-6631-1893
  chin@nccst.nat.gov.tw
  謝汶廷：02-6631-1883
  wengting@nccst.nat.gov.tw
  鄒宛璉：02-6631-6452 (技術檢測)
  lauratzou@nccst.nat.gov.tw

報告完畢
敬請指教