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

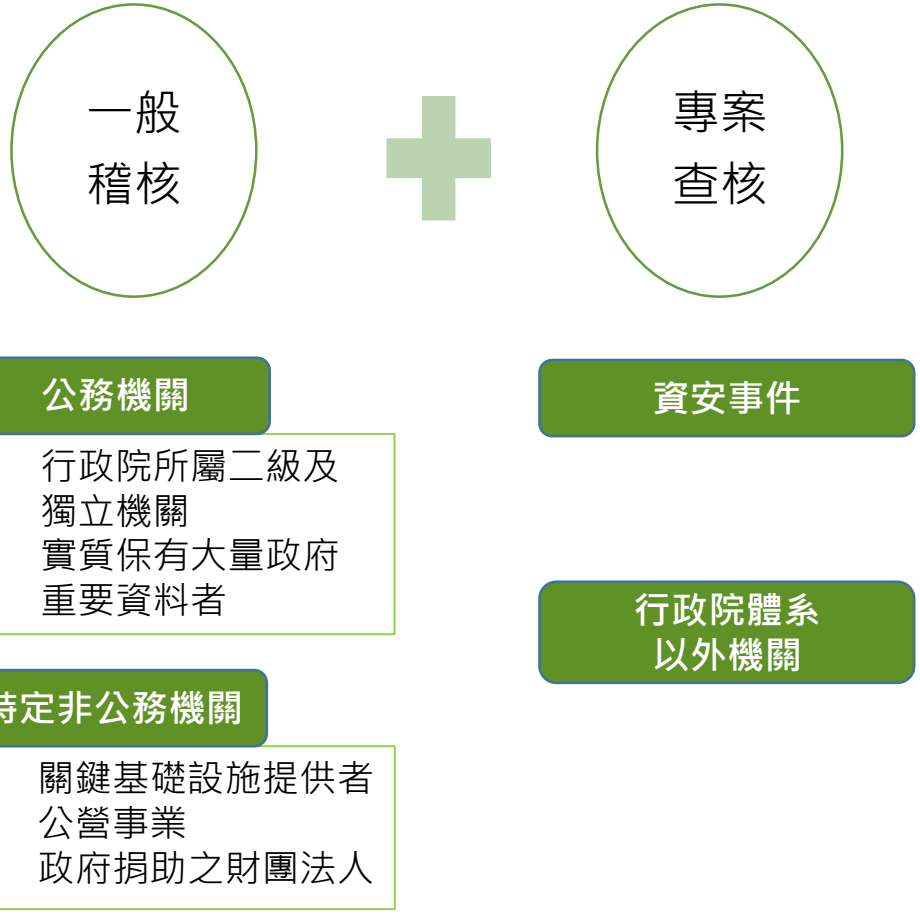
- **目的**
  - 查核公務機關及特定非公務機關辦理資通安全管理法及其子法相關法遵事項之落實情形
  - 經由外部稽核各機關資通安全維護計畫實施情形，改善並強化機關資通安全防護工作之完整性及有效性，以持續精進管理政府整體資安風險

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%

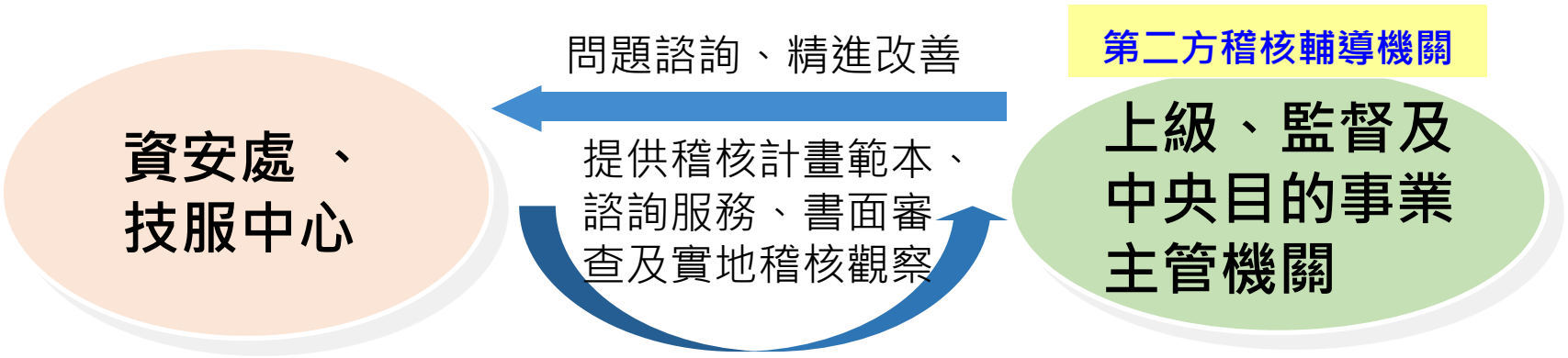
(二)第二、三、四分組

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

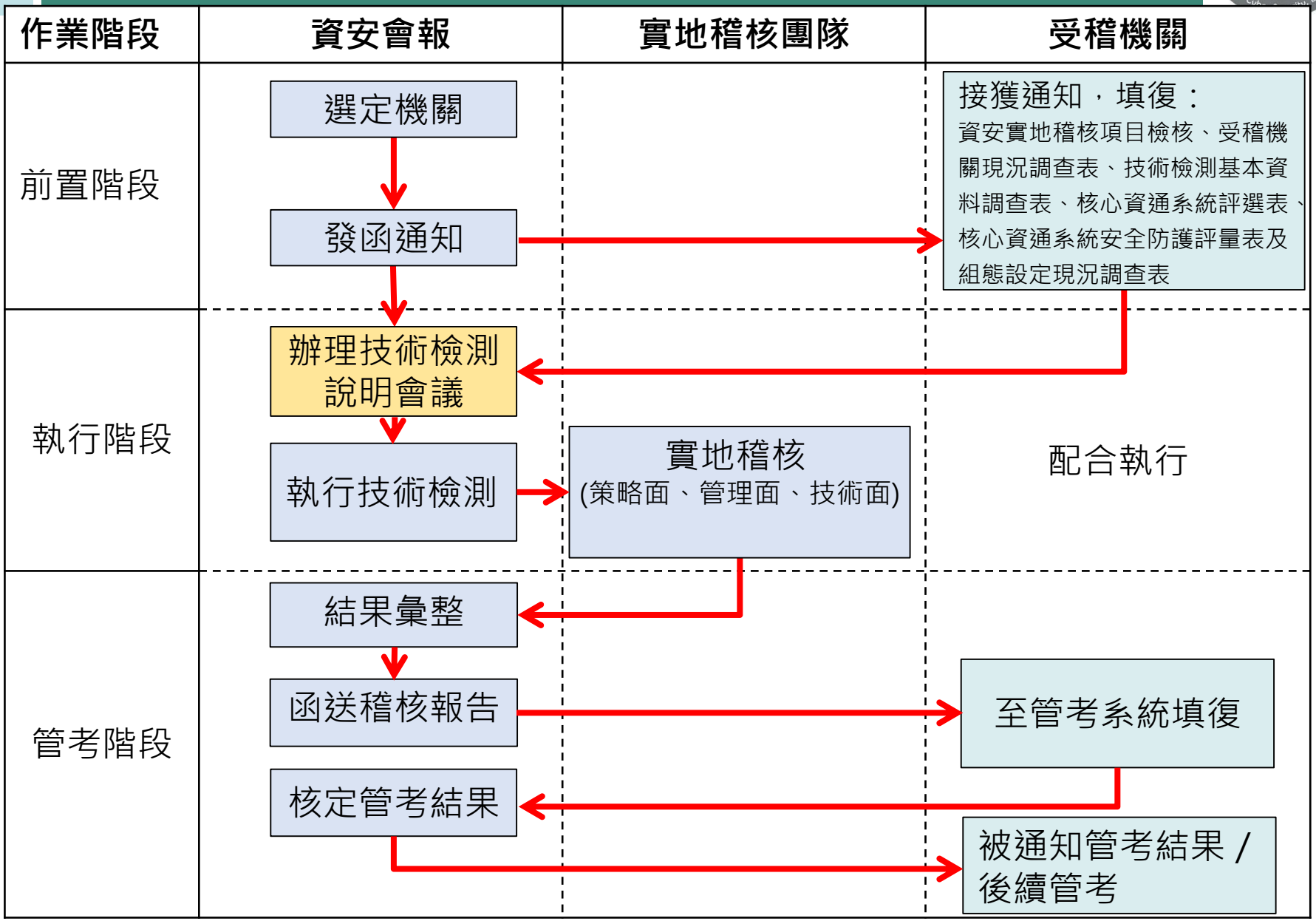
第二方稽核輔導觀察項目與產出

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

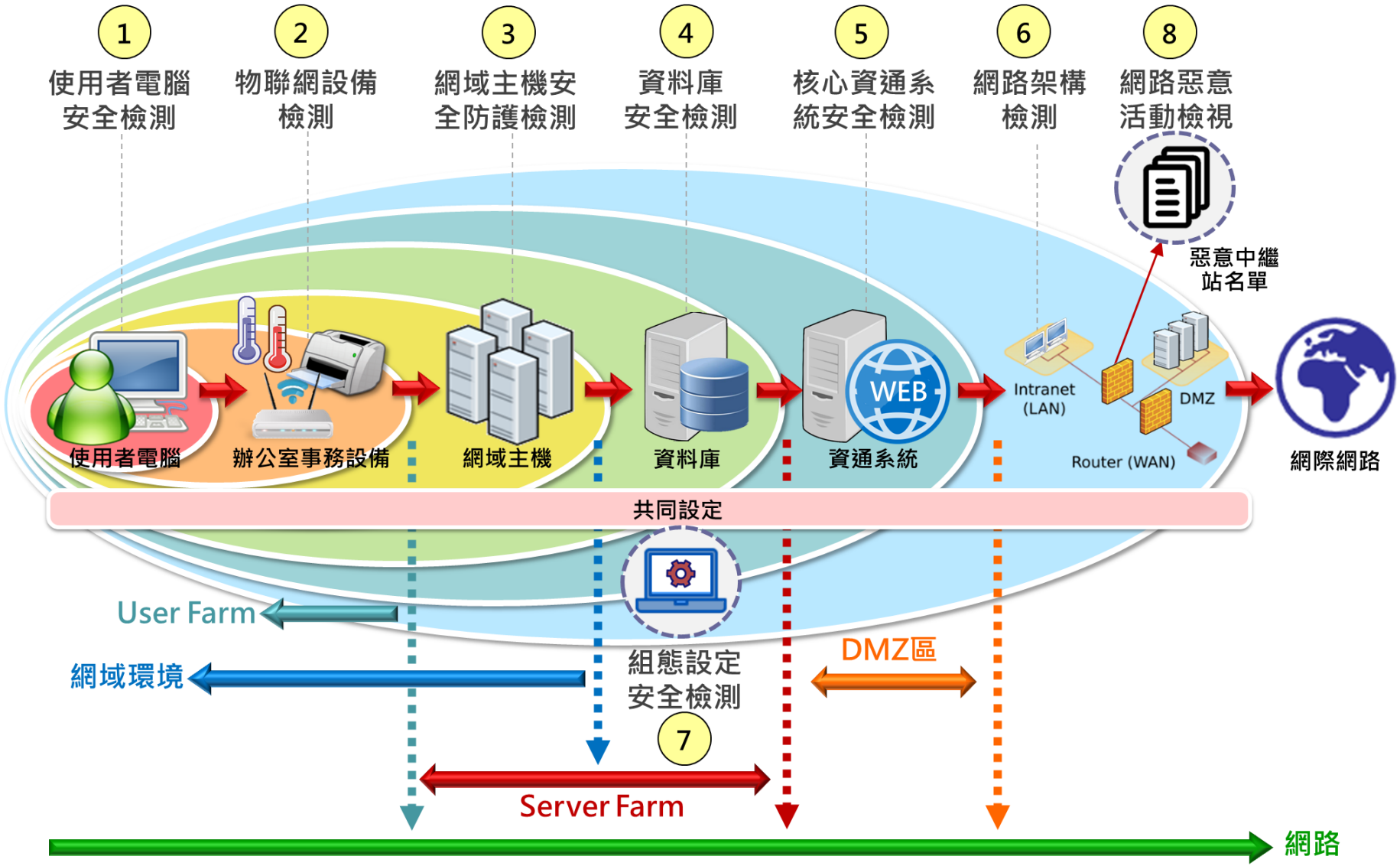
作業說明

- **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)

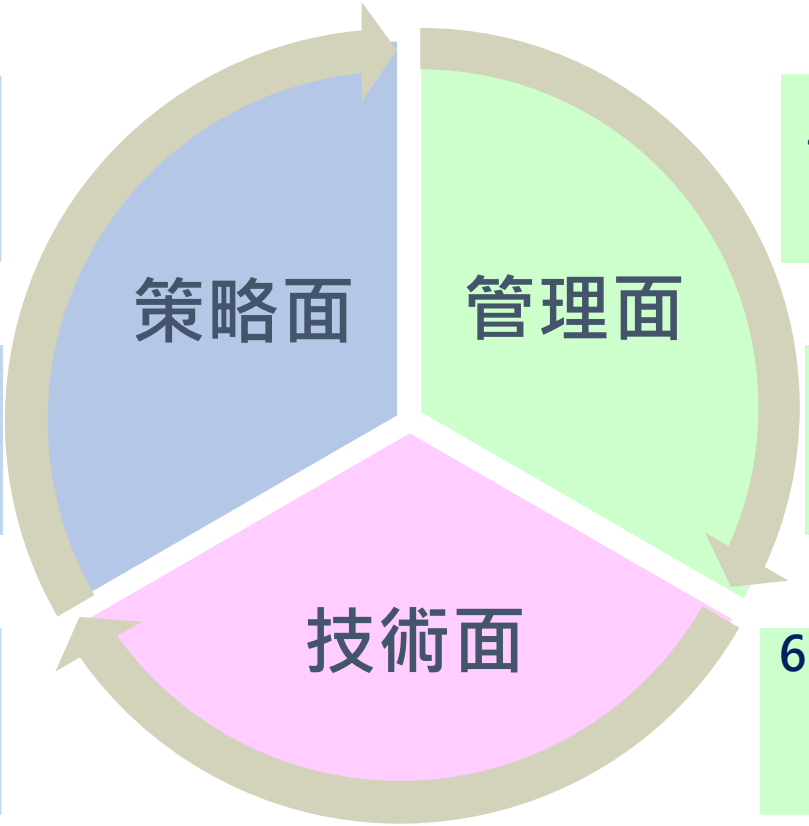
項次	技術檢測項目	執行範圍	執行方式
8	網路惡意活動檢視	全機關	• 依照技服中心每日公布之惡意中繼站名單，分別針對機關**使用者網段及資通系統管理者網段**進行檢測 • 機關協助提供即時側錄之完整流量，透過部署技服中心自行研發之APT流量偵測規則，針對**機關內對外與外對內完整流量**進行APT活動檢測

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