115 年資通安全稽核計畫(核定本)

115 年 3 月

壹、依據

資通安全管理法(114 年修正施行)第 8 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、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資通系統之各項資通安全管理政策、程序等。

肆、作業期程

本(115)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	期程	重點工作
一	準備作業(114 年 12 月-115 年 1 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(2-3 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

項次	期程	重點工作
三	實施作業 (4 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 (三)試辦受稽機關自動化工具檢測及 AI 輔助場外稽核
四	檢討作業 (115 年 12 月-116 年 1 月)	(一)提出稽核結果及共同發現事項 (二)建議表揚成績優良及表現良好機關 (三)撰擬送交立法院之年度稽核概況報告

伍、稽核方式

本年度資通安全稽核將採取 2 類稽核作業，類型 1 為傳統稽核，包含**實地稽核及技術檢測**方式辦理，類型 2 將試辦導入 AI 輔助場外稽核及自動化檢測，檢視機關資通安全管理制度與實際資通安全防護情形。

一、類型 1：

(一)實地稽核：組成稽核小組，由稽核委員分策略、管理、技術及工控面至現地進行檢視及訪談，以發覺潛在之資安風險。

(二)技術檢測：以人工檢測為主，使用者電腦、物聯網設備、核心系統等多面向檢測角度切入，以主動發現機關潛在弱點及協助機關改善為主要辦理重點。

二、類型 2(試辦不計分)：

(一)AI 輔助場外稽核：由受稽機關提供自評資料及佐證文件，透過本署稽核資料分析平臺 AI 分析後，由資安署及稽核委員複審，確認機關資安法落實情形。

(二)自動化工具檢測：使用自動化工具發掘潛在系統弱點與網域帳號權限異常狀況，提供風險評估結果與改善對策。

陸、稽核小組

一、實地稽核小組組成原則如下：

(一)領隊：國家資通安全會報副召集人、協同副召集人、其他經其授權之人員，或由資安法主管機關數位發展部(以下簡稱數發部)之

正副首長、資安專責機關資通安全署(以下簡稱資安署)之正副首長、主任秘書擔任，並得由國家安全會議國家資通安全辦公室主任、資安署各組組長或策略面委員代理。

(二)稽核委員：

1、每個受稽機關原則配置 4-8 名委員進行資安實地稽核作業，分配為策略面 1-2 名、管理面 1-3 名及技術面 2-3 名。

2、如受稽機關有維運工控系統或運營科技(OT)，則另外配置 1-2 名工控(OT)稽核委員進行工控系統或運營科技(OT)實地稽核作業。

3、由數發部考量稽核實際需求，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得少於全體成員人數之四分之一，且各場次策略面委員由政府機關委員或資安稽核領域具有相當專業經驗之委員擔任，倘委員無法配合出席稽核場次或其他情形者，得由資安署彈性調整。

4、委員遴選原則參考國家標準 CNS 27006 及國際標準 ISO/IEC 17021-1 規範之精神。

5、如有涉及資通安全維護計畫實施情形稽核辦法第 9 條第 4 項各款之情形，稽核委員應通知資安署，並主動迴避擔任該場次稽核委員。

6、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，亦應通知資安署及迴避擔任該場次稽核委員。

7、資安署委員得視專業能力及稽核需求支援或擔任其他構面之委員。

(三)觀察員：自總統府與中央一級機關含所屬機關、直轄市政府與各縣市政府及所屬機關之公務人員遴選，每場次至多 4 名。

(四)工作人員：辦理現場幕僚或行政作業之人員，負責啟始會議、委員意見交換、結束會議簡報及其他行政庶務作業，人數視實際需求配置，每場次 1-4 名。

(五)觀摩人員：觀摩現場實地稽核作業，人數視實際需求而定。

二、技術檢測小組：由國家資通安全研究院(以下簡稱資安院)及資安署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，每場次技術人員原則 12 名。

三、AI 輔助場外稽核小組：由資安署具備資安稽核能力並熟稔資通安全管理法人員針對 AI 分析內容進行初步確認，再由稽核委員進行複審，每場原則配置資安署人員 1 名及稽核委員 1 名。

四、自動化檢測小組：由國家資通安全研究院(以下簡稱資安院)及資安署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，每場次技術人員原則 3 名。

五、各類小組成員對於所知悉或持有之相關機敏資訊或文件，應善盡保管及保密之責，並應簽署保密切結書。

六、各類稽核小組組成及員額配置，詳見表 2。數發部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調整。

表 2 稽核小組組成及員額配置

項目	稽核小組組成	人員配置	總計
實地稽核 (有維運工控系統或運營科技(OT)者，須另外進行工控系統或運營科技(OT)稽核)	領隊	1 名	1 名
	稽核委員 • 策略面 • 管理面 • 技術面 • (工控系統或運營科技(OT))	 • 1-2 名 • 1-3 名 • 2-3 名 • (1-2 名)	4-8 名 (5-10 名)
	觀察員	至多 4 名	至多 4 名
	工作人員	1-4 名	1-4 名
	觀摩人員	視需求	視需求
技術檢測	資安院及資安署檢測人員	原則 12 名	原則 12 名
AI 輔助場外稽核	資安署人員	1 名	1 名
	稽核委員	1 名	1 名

自動化工具檢測	資安院及資安署檢測人員	原則 3 名	原則 3 名

柒、受稽機關遴選原則

依 114 年 12 月 1 日修正施行之資通安全管理法，主管機關得定期或不定期稽核公務機關及特定非公務機關之資通安全維護計畫實施情形。

一、實地稽核及技術檢測：

(一)未曾受行政院國家資通安全會報（修法後為國家資通安全會報）稽核者。

(二)資安治理成熟度達 3 級以上者。

(三)符合下列遴選原則之一者：

1、實質保有大量政府重要資料或個人資料者。

2、提供或維運共用(通)性資通系統服務者。

3、屬公務機關，且業務涉及關鍵基礎設施事項。

4、屬關鍵基礎設施提供者，其資通系統失效或受影響將產生嚴重影響者。

二、AI 輔助場外稽核及自動化工具檢測（試辦不計分）：

(一)曾受行政院國家資通安全會報（修法後為國家資通安全會報）稽核者。

(二)距前次稽核時間較長者。

(三)符合下列遴選原則之一者：

1、實質保有大量政府重要資料或個人資料者。

2、提供或維運共用(通)性資通系統服務者。

3、屬公務機關，且業務涉及關鍵基礎設施事項。

捌、稽核基準

本計畫為稽核 114 年度資通安全維護計畫實施情形，稽核基準係依據資通安全管理法(108 年施行)及其子法(110 年施行)、國家資通安全發展方案(114 年至 117 年)、資訊安全管理系統國家標準 CNS 27001:2023 或資訊安全管理系統國際標準 ISO 27001:2022、資通安全維護計畫、其他內部控制及資安相關規定。

工控系統或運營科技(OT)，相關稽核基準係依據資通安全責任等級分級辦法附表十資通系統防護基準或中央目的事業主管機關依資通安全

責任等級分級辦法第 11 條自行擬訂之防護基準等。

玖、稽核項目及配分

一、類型 1：

(一)整體考量受稽機關屬性及為有效運用稽核能量，將類似性質機關進行分組，同分組計分方式須一致，符合下列任一條件者得為同一分組，分組原則如下：

1、資訊業務重要性相當者。

2、資通安全管理法納管身分相同者。

3、維運工控系統或運營科技(OT)者。

(二)資安稽核除對辦公場域外，並得延伸至重要系統所在之外部專案辦公室或機房，得擴展為多場域稽核模式，另可依實際需要動態調整稽核天數，不以 1 日為限。

1、資訊系統及工控系統或運營科技(OT)實地稽核

資訊系統實地稽核分策略面、管理面及技術面等 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(資通安全實地稽核項目檢核表，請參閱附件 1-1、1-2)，各構面之稽核項目及配分說明如表 3，總分合計 100 分。

表 3 各構面稽核項目及配分

構面	稽核項目	配分
策略面	1、核心業務及其重要性	10
	2、資通安全政策及推動組織	10
	3、專責人力及經費配置	10
管理面	4、資訊及資通系統盤點及風險評估	10
	5、資通系統或服務委外辦理之管理措施	10
	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	10
技術面	7、資通安全防護及控制措施	20
	8、資通系統發展及維護安全	10
	9、資通安全事件通報應變及情資評估因應	10
合計		100

針對有維運工控系統或運營科技(OT)，且具關鍵基礎設施

提供者身分之受稽機關，就擇定之核心系統(OT)等，依據 10 大稽核項目(分管理面及技術面等 2 個構面)、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，另外辦理工控系統或運營科技(OT)實地稽核，各構面之稽核項目及配分說明如表 4，總分合計 100 分。

表 4 各構面稽核項目及配分

構面	稽核項目	配分
管理面	1、事件日誌與可歸責性	10
	2、營運持續計畫	10
	3、系統與服務獲得	10
技術面	4、ICS(OT)網路架構	10
	5、存取控制	10
	6、識別與鑑別	10
	7、系統與通訊防護	10
	8、實體與環境防護	10
	9、系統與資訊完整性	10
	10、組態管理	10
合計		100

2、技術檢測(由稽核小組指定)

(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。

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	10
		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	5
合計			100

(2)如受稽機關無檢測項目之檢測標的，則不進行該項檢測項目，技術檢測計分方式依分數比例調整(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÷85×100)。

3、評分方式

實地稽核及技術檢測評分方式如表 6。

表 6 實地稽核及技術檢測評分方式

類別	實地稽核		技術檢測	總成績計算方式
	IT	OT		
1	V			IT 實地稽核得分 × 100%
2	V		V	技術檢測得分×30%＋IT 實地稽核得分 × 70%
3	V	V		實地稽核得分(IT 得分×70%＋OT 稽核得分×30%) ×100%

4	V	V	V	技術檢測得分×30%＋實地稽核得分 (IT 得分×70%＋OT 得分× 30%)×70%

備註：

1. 實地稽核所需文件如逾期提供或未於實地稽核前完成配合事項者，扣 1 分。
2. 技術檢測所需調查表逾期提供、內容正確性與完整性不足或未於檢測前完成配合事項，足以影響檢測作業執行者，扣 1 分。

二、類型 2：

(一)本年度為試辦 AI 輔助場外稽核及自動化檢測，不另計分及分組。

(二)AI 輔助場外稽核原則以機關提供自評及相關佐證資料進行審查，無須實際到場；自動化工具檢測則將請機關進行檢測軟體派送，復由檢測團隊實地至實地收整資料，不以 1 日為限。

1、AI 輔助場外稽核：

AI 輔助場外稽核分策略面、管理面 2 個構面，各構面之稽核項目如表 7。

表 7 AI 輔助場外稽核項目

構面	稽核項目
策略面	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
管理面	4、資訊及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

2、自動化工具檢測：

自動化工具檢測分為 5 大檢測項目，各檢測項目之執行內容說明如表 8。

表 8 自動化工具檢測項目

項次	檢測項目
1	使用者電腦及主機安全檢測
2	物聯網設備檢測

3	核心資通系統安全檢測
4	組態設定安全檢測
5	AD 帳號權限曝險檢測

壹拾、作業說明

一、機關自評

(一)類型 1：

1、實地稽核：

(1)受稽機關填復「資通安全實地稽核項目檢核表」(公務機關詳附件 1-1、特定非公務機關詳附件 1-2)、「受稽機關現況調查表」(附件 2)，併附機關最新之「資通安全維護計畫」，並請提供紀錄文件等佐證資料電子檔。

(2)有維運工控系統或運營科技(OT)，且具關鍵基礎設施提供者身分之受稽機關，應於事前辦理相關整備工作，盤點工控系統或運營科技(OT)，另填復「工控系統或運營科技(OT)盤點表」(附件 3)、「工控系統或運營科技(OT)評選表」(附件 4，自行擇選 3 個重要性較高之工控系統或運營科技(OT))及「工控系統或運營科技(OT)資通安全實地稽核項目檢核表」(附件 5)，並請提供紀錄文件等佐證資料電子檔。

2、技術檢測：受測機關填復「技術檢測基本資料調查表」(附件 6)、「核心資通系統評選表」(附件 7，自行擇選 3 個具資料庫之核心資通系統，核心資通系統不足 3 個者，以具資料庫之資通系統補足之)、「核心資通系統安全防護評量表」(附件 8)及「組態設定現況調查表」(附件 9)。

(二)類型 2(試辦不計分)：

1、AI 輔助場外稽核：受稽機關填復「AI 輔助場外稽核項目檢核表」(附件 10)、受稽機關現況調查表(附件 2)，併附機關最新之「資通安全維護計畫」、前一年度「資通安全維護計畫實施情形」、「ISMS 文件」及其他佐證資料。

2、自動化工具檢測：受測機關填復「技術檢測基本資料調查表」(附件 6)、「核心資通系統評選表」(附件 7，自行擇選 3 個具

提供網頁服務之核心資通系統，核心資通系統不足 3 個者，以具提供網頁服務之資通系統補足之)、「核心資通系統安全防護評量表」(附件 8)及「組態設定現況調查表」(附件 9)。

二、實地稽核

由領隊帶領稽核小組至受稽機關進行實地稽核，如受稽機關為特定非公務機關，為協助中央目的事業主管掌握所管機關資安管理情形，請受稽機關邀請中央目的事業主管機關派員出席(實地稽核時程規劃如表 9)，並協調中央目的事業主管機關出席人員接待及餐飲等事宜。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 3 個構面、9 個稽核項目，重點說明如下(實地稽核評分表及工控系統或運營科技(OT)實地稽核評分表，請分別參閱附件 11、附件 12)：

(一)策略面

1、核心業務及其重要性：資通系統分級、資訊安全管理系統(ISMS)範圍、營運衝擊分析、業務持續運作計畫、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：資安政策及目標、資安推動組織、內部稽核及後續追蹤、所屬人員對於資通安全維護之考核或獎懲機制、利害關係人管理等。

3、專責人力配置：資安人力配置情形、資安教育訓練、資安專業證照及職能訓練證書等。

(二)管理面

1、資訊及資通系統盤點及風險評估：資訊資產盤點及相關管理程序、風險評鑑、風險處理程序、是否禁止使用大陸廠牌資通訊產品等。

2、資通系統或服務委外辦理之管理措施：委外業務安全管理程序、委外廠商及相關人員管理措施、安全性檢測證明、第三方元件授權證明、受託業務查核等。

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：機關資通安全維護計畫訂定、修正及實施情形、上級/監督/中央目的事業主管機關之監督管理、對於所屬/所監督/所管機關之稽核作業、資安事件審核、資通安全演練之實施等。

(三)技術面

1、資通安全防護及控制措施：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/資通安全防護措施實施情形、電子資料安全管理機制、網路規劃及管理、電腦機房及重要區域管理、行動裝置安全、軟體使用安全及電子郵件安全等。

2、資通系統發展及維護安全：資通系統防護需求、SSDLC 各階段(包括系統需求、設計、開發、測試、部署維運階段)資安保護措施、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：資通安全情資評估及因應機制、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、資安事件通報應變作業規範及落實情形、資安事件改善措施、資通安全演練作業實施情形等。

(四)針對受稽機關配合情形進行評分，如有實地稽核所需文件逾期提供或未於實地稽核前完成配合事項等情形，將予以扣分。

表 9 實地稽核時程

時間	工作項目	參與人員
9:00~9:30	啟始會議 • 受稽機關代表致詞、介紹出席人員(5 分鐘) • 稽核小組領隊致詞、介紹稽核小組(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)	• 稽核小組 • 受稽機關 • 上級/監督/中央目的事業主管機關
9:30~09:45	稽核小組稽核前意見交換	稽核小組
9:45~12:30	實地稽核	• 稽核小組 • 受稽機關
12:30~13:30	午餐及彙整稽核發現	• 稽核小組
13:30~15:30	實地稽核	• 稽核小組 • 受稽機關
15:30~17:00	稽核小組意見彙整	• 稽核小組

17:00~17:30	結束會議 • 稽核結果報告 • 意見交流	• 稽核小組 • 受稽機關 • 上級/監督/中央目的事業主管機關

備註：

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。
2. 稽核啟始/結束會議之受稽機關代表建議由資安長出席，以掌握機關之資安管理及追蹤改善情形。
3. 中央目的事業主管機關出席人員之餐飲及交通安排等事宜請受稽機關自行處理。

三、技術檢測說明

本年擇選部分機關於辦理實地稽核前先進行 3 天之技術檢測，檢視受稽機關之資通安全防護情形，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(技術檢測評分表請參閱附件 13)：

(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

針對全機關之網路印表機、門禁系統、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)等物聯網設備執行弱點掃描。

(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、依照資安院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，透過部署資安院自行研發之 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。

(九)針對須受技術檢測之受稽機關配合情形進行評分，如有檢測所需調查表逾期提供、內容正確性與完整性不足或未於檢測前完成配合事項等情形，足以影響檢測作業執行，將予以扣分。

四、AI 輔助場外稽核（試辦不計分）：

(一)依數發部通知期限內填復「AI 輔助場外稽核項目檢核表」（附件 10）辦理情形及佐證文件欄位，並提供相關佐證文件。

(二)如須補充資料或修正內容，以 1 次為限，並請受稽機關配合於期限內完成(逾期未補充則視為不符合)。

(三)數發部將於 AI 輔助場外稽核作業結束後，提供稽核報告予受稽機

關，並據以改善，後續由受稽機關自行追蹤管考。

五、自動化工具檢測（試辦不計分）：

本年擇選部分機關試辦自動化工具檢測，以可自動化執行之檢測工具為主，檢視受稽機關之資通安全防護情形，重點說明如下：

(1) 依數發部通知期限內填復「技術檢測基本資料調查表」(附件6)、「核心資通系統評選表」(附件7，自行擇選3個具提供網頁服務之核心資通系統，核心資通系統不足3個者，以具提供網頁服務之資通系統補足之)、「核心資通系統安全防護評量表」(附件8)及「組態設定現況調查表」(附件9)。

(2) 使用者電腦及主機安全檢測：

1. 數發部將於檢測首日起 3 週前提供檢測工具，請受稽機關配合於期限內針對使用者電腦完成派送、執行、蒐整及提供檢測工具執行結果。
2. 數發部將於檢測首日攜帶檢測設備至受稽機關，針對使用者電腦與核心資通系統主機執行弱點掃描。

(3) 物聯網設備檢測：數發部將於檢測首日攜帶檢測設備至受稽機關，針對網路印表機、門禁系統、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)等物聯網設備執行弱點掃描。

(4) 核心資通系統安全檢測：數發部將於檢測首日攜帶檢測設備至受稽機關，針對受稽機關核心資通系統使用自動化工具進行網頁弱點掃描。

(5) 組態設定安全檢測：針對已公告之政府組態基準(GCB)項目以自動化工具進行檢測。數發部將於檢測首日起3週前提供檢測工具，請受稽機關配合於期限內針對使用者電腦完成派送、執行、蒐整及提供檢測工具執行結果。

(6) AD帳號權限曝險檢測：數發部將於檢測首日攜帶檢測工具，透過受稽機關已加入網域之使用者電腦進行AD帳號權限曝險檢測。無AD網域者不進行此項檢測。

(7) 數發部將於檢測首日至受稽機關執行檢測，請受稽機關於檢測前完成檢測環境整備。檢測首日會將檢測設備存置於受稽機關持續進行檢測，請受稽機關安排適當環境並於檢測期間保管檢測設備。

(8) 數發部將於檢測首日後 7 個工作日內至受稽機關回收檢測設備並帶回檢測結果。

(9) 數發部將於檢測作業結束後，提供檢測報告予受稽機關，並據以改善，後續由受稽機關自行追蹤管考。

壹拾壹、獎勵

一、為鼓勵對於資安防護表現優良之受稽機關，將依相關整體成績表現擇取類型 1 之績優及表現良好機關予以獎勵。

二、績優機關

依各分組機關數量擇取各分組成績第 1、前 2 或前 3 名之受稽機關評為績優機關；如該分組之機關數量小於 6 個，取第 1 名為績優機關；如該分組之機關數量 6 至 8 個，取前 2 名為績優機關；如該分組之機關數量大於等於 9 個，取前 3 名為績優機關。數發部將函請績優機關，針對有功人員予以敘獎，並於國家資通安全會報委員會議或相關會議中頒發績優獎座。

績優機關資格條件：

(一)公務機關之分組，其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；其他績優機關之實地稽核成績，須達 75 分(含)以上

(二)各稽核分組之受稽機關稽核成績均未達 75 分(含)時，名額從缺。

三、稽核表現良好機關

為鼓勵機關精進資安防護作業，針對未達績優機關，但符合下列情形之一者，為表現良好機關，數發部將函請表現良好機關，針對有功人員予以敘獎。

(一)未列該分組第 1 名，惟分數高於 80 分者。

(二)分數達 70 分(含)以上，且列該分組第 1 名者。

壹拾貳、改善作業

一、類型 1：數發部將於每季稽核作業結束後，函送資安稽核報告予受稽機關，同時副知其上級/監督/中央目的事業主管機關，並請受稽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等相關內容，於期限內至指定平臺填報，由上級/監督/中央目的事業主管機關審查，後由數發部核定結果；後續資安署將以電子郵件通知受稽

機關定期填報，管考至全部改善完成。

二、類型 2：數發部將於稽核作業結束後，函送資安稽核報告予受稽機關，同時副知其上級/監督/中央目的事業主管機關，請受稽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，並自行管考。

三、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 28 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 29、30 及 31 條所述之情形，中央目的事業主管機關應依法辦理之。

四、本年資安稽核作業結束後，數發部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。

壹拾參、機關配合事項

一、數發部稽核通知原則：類型 1 於每季稽核前 1 個月、類型 2 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，請受稽機關於數發部通知函文所訂期限內，依「壹拾、作業說明 一、機關自評」填復相關文件；如有臨時狀況將由數發部與受稽機關聯繫後辦理。

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，稽核作業說明文件將併同稽核計畫一併提供。各上級/監督/中央目的事業主管機關於收到今年稽核計畫後，請轉知所屬/所監督/所管機關相關資安稽核事宜，並可參考本計畫內容，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，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、有關受稽機關應填復之文件及配合事項如表 10、表 11。

表 10 類型 1 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(提交)文件	文件回復日期
受稽機關	第 1 梯次 4-6 月 第 2 梯 7-9 月 第 3 梯 10-12 月	稽核前 1 個月函文通知	發通知函文前	**全部受稽機關**： 1. 資通安全實地稽核項目檢核表(附件 1-1、1-2)，並請提供紀錄文件等佐證資料電子檔 2. 受稽機關現況調查表(附件 2) 3. 資通安全維護計畫(機關自訂之最新版本) 4. 資安推動情形簡報 5. 啟始會議簡報 **須技術檢測之機關加填**： 1. 技術檢測基本資料調查表(附件 6) 2. 核心資通系統評選表(附件 7) 3. 核心資通系統安全防護評量表(附件 8) 4. 組態設定現況調查表(附件 9) **有維運工控系統或運營科技(OT)之受稽機關加填**： 1. 工控系統或運營科技	依通知函文所訂期限

對象	稽核期間	通知日期及方式	協調稽核日期	填寫(提交)文件	文件回復日期
				(OT)盤點表(附件 3) 2. 工控系統或運營科技(OT)評選表(附件 4) 3. 工控系統或運營科技(OT)資通安全實地稽核項目檢核表(附件 5)，並請提供紀錄文件等佐證資料電子檔	

表 11 類型 2 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(提交)文件	文件回復日期
受稽機關	7-12 月	稽核前 1 個月函文通知	發通知函文前	**全部受稽機關**： 1. AI 輔助場外稽核項目檢核表(附件 10) 2. 受稽機關現況調查表(附件 2) 3. 資通安全維護計畫(機關自訂之最新版本) 4. 前一年度資通安全維護計畫實施情形 5. ISMS 文件及相關佐證資料 **須自動化工具檢測之機關加填**： 1. 技術檢測基本資料調查表(附件 6) 2. 核心資通系統評選表(附件 7) 3. 核心資通系統安全防護評量表(附件 8) 4. 組態設定現況調查表(附件 9)	依通知函文所訂期限

壹拾肆、附件

附件 1-1　資通安全實地稽核項目檢核表(公務機關)

附件 1-2　資通安全實地稽核項目檢核表(特定非公務機關)

附件 2　受稽機關現況調查表

附件 3　工控系統或運營科技(OT)盤點表

附件 4　工控系統或運營科技(OT)評選表

附件 5　工控系統或運營科技(OT)資通安全實地稽核項目檢核表
附件 6　技術檢測基本資料調查表
附件 7　核心資通系統評選表
附件 8　核心資通系統安全防護評量表
附件 9　組態設定現況調查表
附件 10 AI 輔助場外稽核項目檢核表
附件 11 實地稽核評分表
附件 12 工控系統或運營科技(OT)實地稽核評分表
附件 13 技術檢測評分表