稽核實務與資安法落實

數位發展部資通安全署

111年7月

大綱

一、資通安全管理法之資安稽核

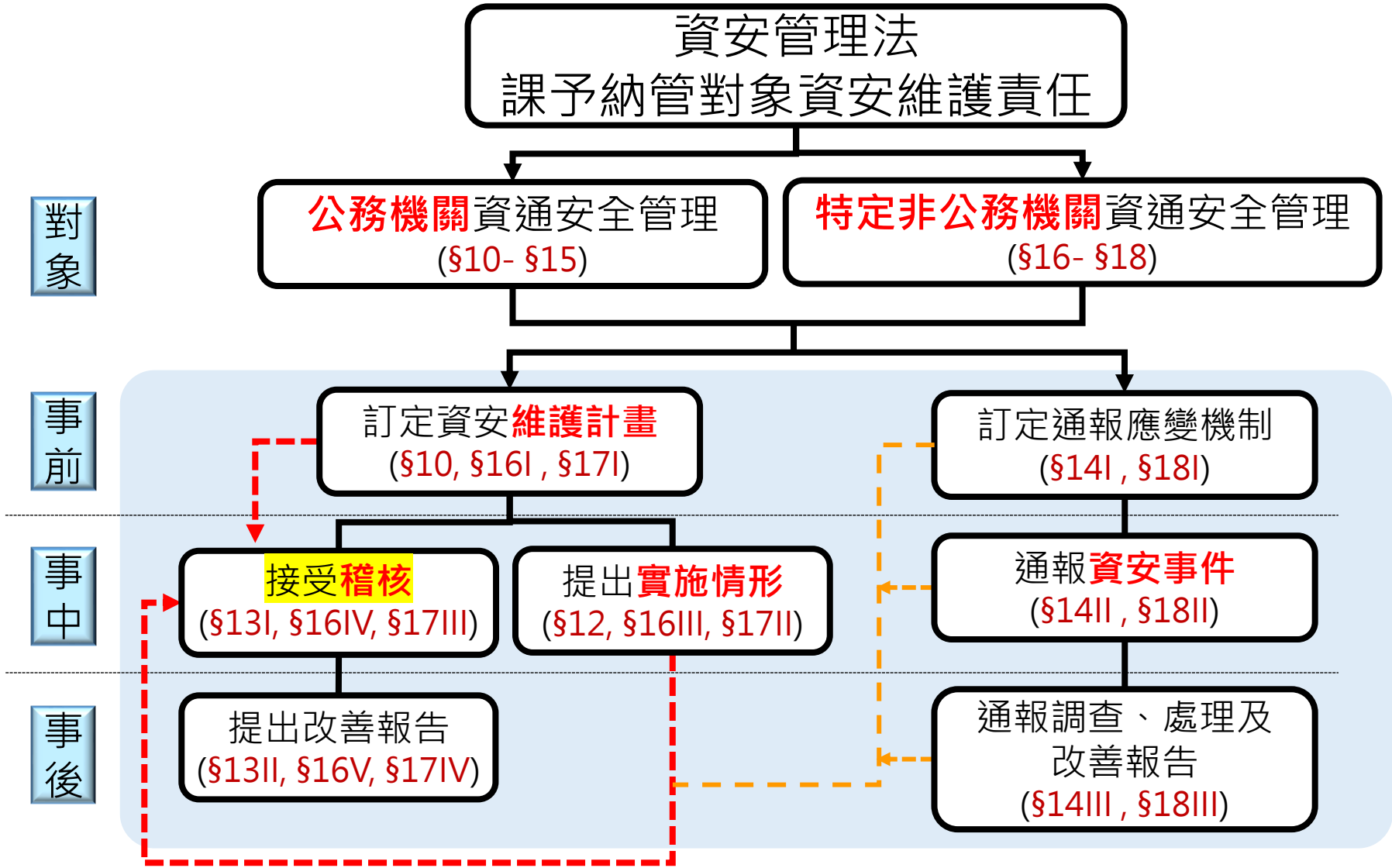
二、主管機關(行政院)資安稽核規劃

三、資安稽核項目及重點

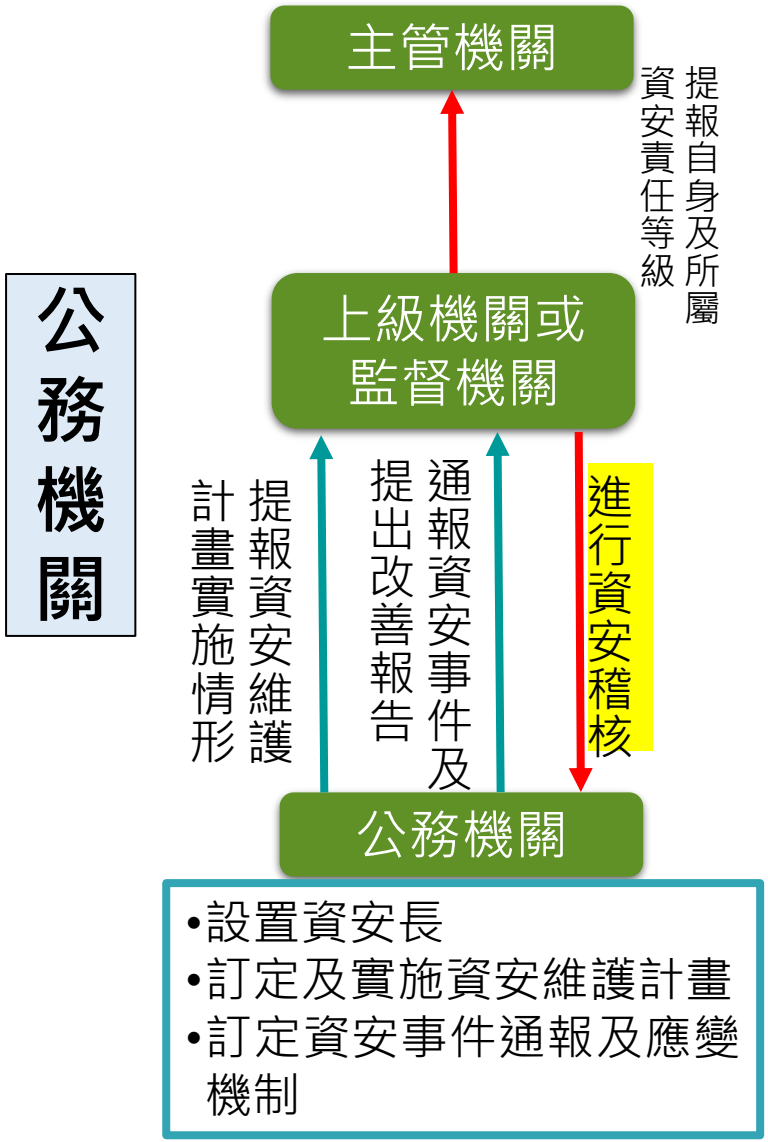
四、後續推動方向

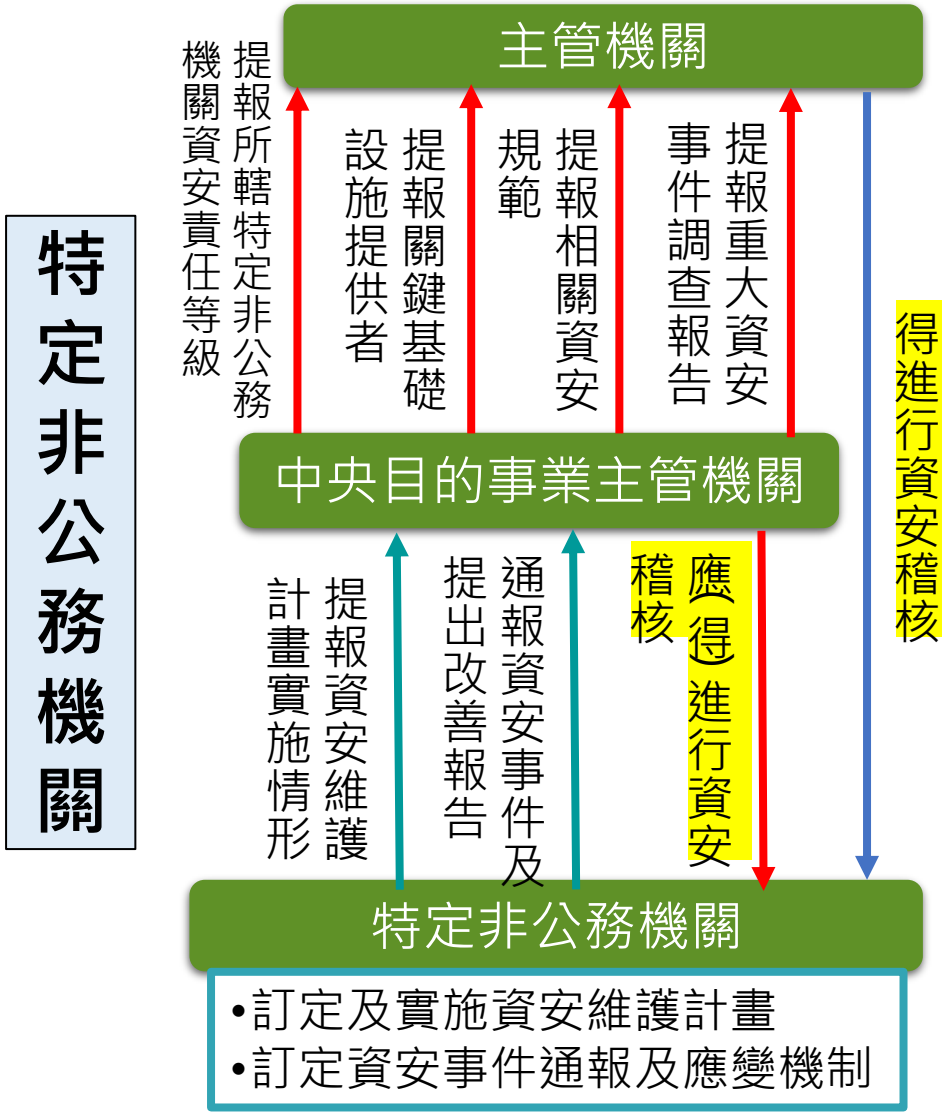
資通安全管理法之資安稽核

資通安全管理法規範架構



角色權責-資安稽核及受稽對象





資通安全管理法-資安稽核

主管機關

- **得**稽核特定非公務機關之**資安維護計畫實施情形(§7)**

公務機關

- **應**稽核所屬或所監督機關之資安維護計畫實施情形(§13)

中央目的事業主管機關

- **應**稽核所管關鍵基礎設施提供者之資安維護計畫實施情形(§16)
- 中央目的事業主管機關**得**稽核所管關鍵基礎設施提供者**以外**之特定非公務機關之資安維護計畫實施情形(§17)

資通安全管理法施行細則

資通安全維護計畫實施情形稽核有缺失或待改善者，應提出改善報告之內容、方式及時間(§3)

資通安全維護計畫及其實施情形之內容應載明事項(§6)

機關資安稽核作業

第一方稽核

機關內稽

第二方稽核

- 上級機關對所屬機關稽核
- 監督機關對行政法人稽核
- 中央目的事業主管機關對特定非公務機關稽核
- 主管機關對特定非公務機關稽核
- 機關對受託者稽核

第三方稽核

ISMS驗證稽核

主管機關(行政院)資安稽核規劃

擬定資安稽核計畫

決定受稽對象

稽核對象(全機關)及頻率
如：每2年完成行政院直屬機關稽核
每年擇部分特定非公務機關稽核

組成稽核小組

稽核領隊、稽核委員
技術檢測人員、**觀察員**、工作人員

制定稽核方式

實地檢測：策略面、管理面、技術面
技術檢測：核心資通系統及使用者電腦

落實追蹤管考

短、中、長期改善措施，**定期追蹤**
如：每季函送稽核結果，填寫改善規劃及進度

資安稽核計畫-稽核範圍及方式

◘稽核範圍

- ➢受稽機關資通安全維護計畫所含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	A級公務機關	B級公務機關	C級公務機關	特定非公務機關
技術檢測(3天)	V	-	-	-
實地稽核(1天)	V	V	V	V

資安稽核計畫-獎勵方式

獎勵分式	行政獎勵	頒發獎座
各稽核分組	第1名	第1名
受獎對象	參與稽核人員	受稽機關
獎勵方式	嘉獎或記功	-

- 獎勵標準：技術檢測及實地稽核皆須達75分(含)以上，未達標準者，依序由後序名次符合條件者遞補
- 個別分組之受稽機關未達獎勵標準時，從缺

資安稽核計畫-實地稽核配分

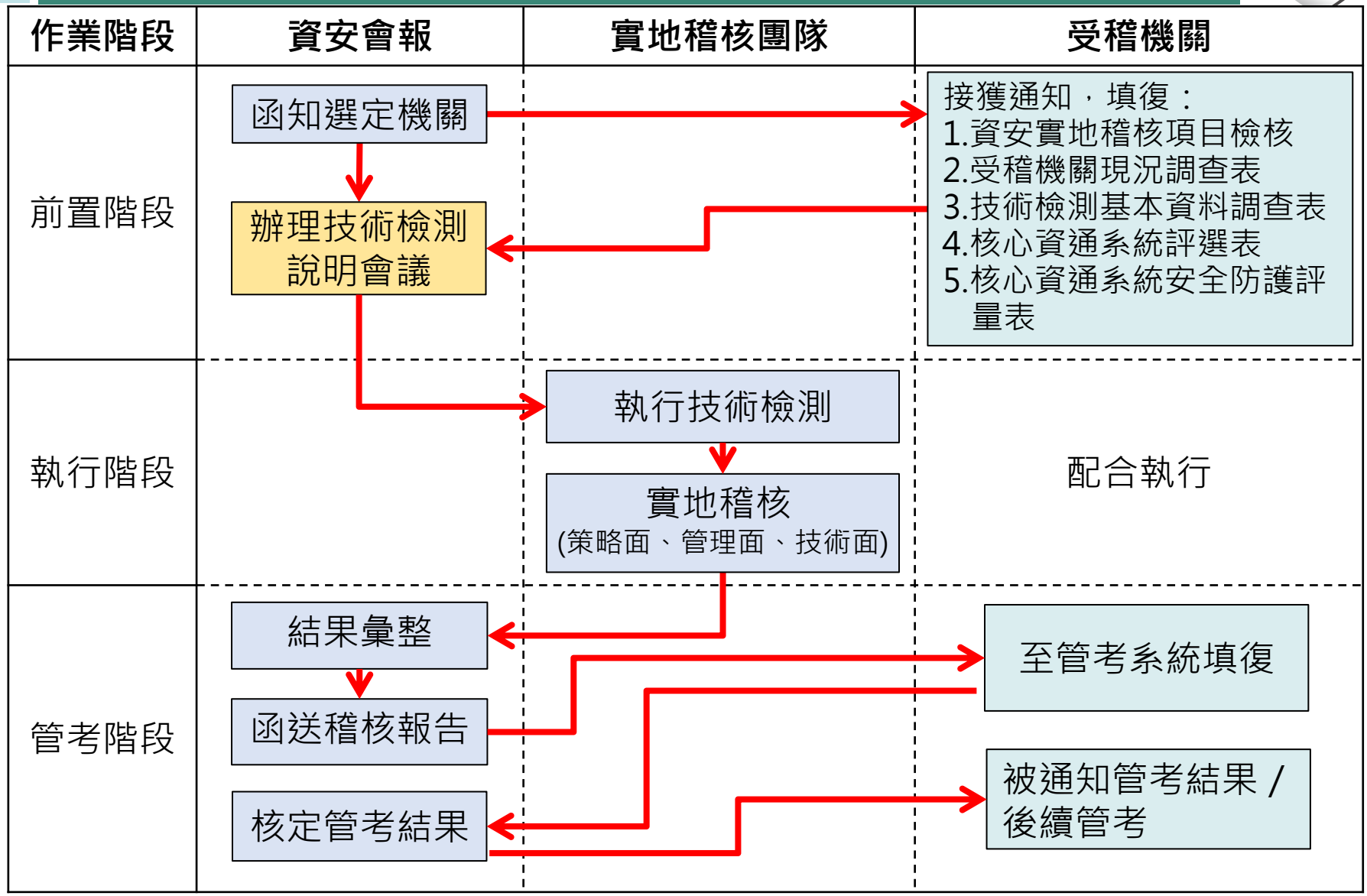
構面	實地稽核項目	配分
策略面	一、核心業務及其重要性	10
	二、資通安全政策及推動組織	10
	三、專責人力及經費配置	10
管理面	四、資通系統盤點及風險評估	10
	五、資通系統或服務委外辦理之管理措施	10
	六、資通安全維護計畫與實施情形之持續精進及績效管理機制	10
技術面	七、資通安全防護及控制措施	20
	八、資通系統發展及維護安全	10
	九、資通安全事件通報應變及情資評估因應	10
合計		100

優(10-9分)、良(8-7分)、佳(6-5分)、可(4分)、待改進(3分(含)以下)

資安稽核計畫-技術檢測配分

項次	技術檢測項目		配分
1	使用者電腦安全檢測(20)	使用者電腦弱點掃描	10
		使用者電腦安全防護檢測	10
2	網路惡意活動檢視(5)	惡意中繼站連線阻擋檢測	5
		APT網路流量檢測	試行不計分
3	核心資通系統安全檢測(25)	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
4	網路架構檢測(10)		10
5	網域主機安全防護檢測(5)		5
6	物聯網設備檢測(10)		10
7	組態設定安全檢測(15)		15
8	資料庫安全檢測(10)		10
合計			100

資安稽核整體作業


作業階段
資安會報
實地稽核團隊
受稽機關
前置階段
函知選定機關
辦理技術檢測說明會議
接獲通知，填復：
1.資安實地稽核項目檢核
2.受稽機關現況調查表
3.技術檢測基本資料調查表
4.核心資通系統評選表
5.核心資通系統安全防護評量表
執行階段
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
核定管考結果
至管考系統填復
被通知管考結果 / 後續管考

資安實地稽核流程

時間	項目	參與人員
啟始會議	•啟始會議 1.**受稽方**代表**OO機關 OO資安長**致詞、介紹出席人員 2.**稽核領隊行政院 OO政委/諮委**致詞、介紹**稽核委員** 3.資安**稽核作業說明**(稽核團隊) 4.**受稽機關資安簡報**(受稽機關)	全體
意見交換	•**稽核團隊稽核前意見交換**	**稽核團隊**
實地稽核	•實地稽核(一)	全體
	•**午餐及彙整實地稽核(一)意見**	稽核團隊
	•實地稽核(二)	全體
意見彙整	•**稽核團隊稽核後意見彙整**	**稽核團隊**
結束會議	•結束會議	全體

資安實地稽核流程

時間	項目	參與人員
9:00~9:30	•啟始會議 1.**受稽方**代表**OO機關 OO資安長**致詞、介紹出席人員 2.**稽核領隊行政院 OO政委/諮委**致詞、介紹**稽核委員** 3.資安**稽核作業說明**(稽核團隊) 4.**受稽機關資安簡報**(受稽機關)	全體
9:30~9:45	•**稽核團隊稽核前意見交換**	**稽核團隊**
9:45~12:30	•實地稽核(一)	全體
12:30~13:30	•**午餐及彙整實地稽核(一)意見**	稽核團隊
13:30~16:30	•實地稽核(二)	全體
16:30~17:00	•**稽核團隊稽核後意見彙整**	**稽核團隊**
17:00~17:30	•結束會議	全體

稽核委員

□委員資格

- 熟悉**資通安全相關法規**(資通安全管理法及子法、CNS 27001或ISO 27001、資安防護訊息之共通規範資料[註1]等)
- 具備**資通安全政策、管理、技術、法律**專業或具**實務經驗**
- **利益衝突之迴避及保密義務**[註2]

□委員訓練

- 機關**自辦訓練**
- 111年**本院稽核員及觀察員訓練課程**(參考)
  - 資通安全管理法概要
  - 資安稽核實務
  - 資安稽核軌跡設計與抽樣檢視技巧
  - 稽核經驗分享
  - 年度稽核重點與配合事項

註1：參考**技服中心網站**\資安防護訊息\共通規範
註2：參考**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**

稽核作業說明

- 稽核範圍(全機關)、法遵重點、實地稽核流程、內容及配分、稽核結束會議、後續辦理事項(追蹤管考)

時間	項目
09:45~12:30 實地稽核(一)	**策略面** **稽核委員：OOO委員、OOO委員** 受稽代表：OOO主任、OOO科長、OOO科長、OOO技正 **管理面** **稽核委員：OOO委員、OOO委員** 受稽代表：OOO技正、OOO技正、OOO技士、OOO小姐 **技術面** **稽核委員：OOO委員、OOO委員、OOO委員** 受稽代表：OOO小姐、OOO聘用研究員、OOO先生、OOO先生、OOO先生、OOO先生 **機房參訪**　**稽核委員提問，請由機關內部人員回答**
12:30~13:30 午餐	
13:30~16:30 實地稽核(二)	

受稽機關資安簡報

一、機關與業務簡介

二、資通安全推動組織

三、ISMS推動情形

四、資訊/資安資源配置

(資訊單位、人力、經費)

五、資訊環境簡介

(網路架構)

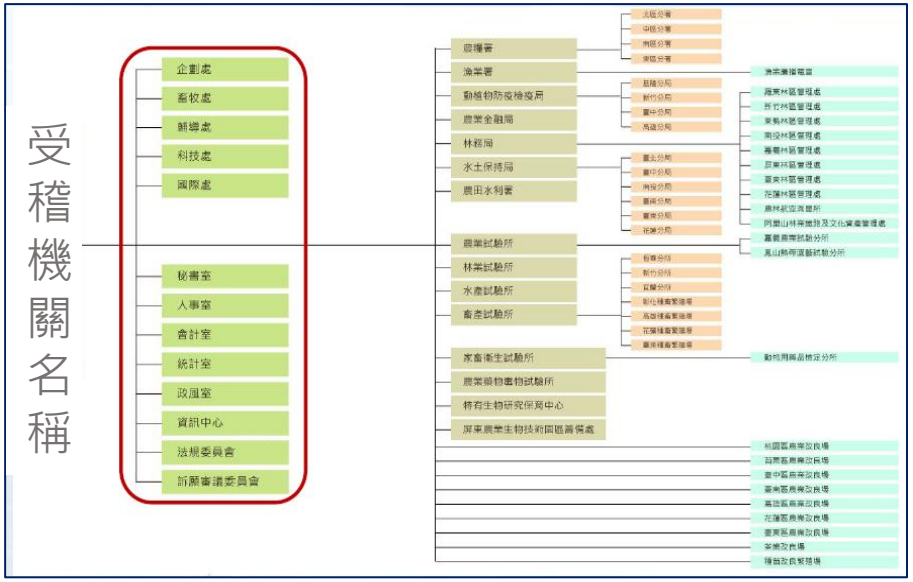
六、資安防護措施

(資通系統、資安法應辦事項)

七、災害復原演練 / 資安事件

八、資通安全維護計畫及實施情形

九、**第二方稽核之規劃與結果**



資安實地稽核流程

時間	項目	參與人員
9:00~9:30	•啟始會議 **1.受稽方**代表**OO機關 OO資安長**致詞、介紹出席人員 **2.稽核領隊行政院 OO政委/諮委**致詞、介紹**稽核委員** 3.資安**稽核作業說明**(稽核團隊) **4.受稽機關資安簡報**(受稽機關)	全體
9:30~9:45	**•稽核團隊稽核前意見交換**	**稽核團隊**
9:45~12:30	•實地稽核(一)	全體
12:30~13:30	**•午餐及彙整實地稽核(一)意見**	稽核團隊
13:30~16:30	•實地稽核(二)	全體
16:30~17:00	**•稽核團隊稽核後意見彙整**	**稽核團隊**
17:00~17:30	•結束會議	全體

稽核前意見交換

綜整提供稽核委員稽核建議

稽核建議-策略面

□核心業務及其重要性

- 資安現況簡報與維護計畫列示計有4個**核心資通系統**，而管考系統列示有25個核心資通系統，建議可再釐清
- 稽核項目檢核表與資安現況簡報列示，**全機關通過ISMS驗證**。另查管考系統列示OO處所管OO網站、ΔΔ處所管ΔΔ資源平臺及□□處所管□□管理系統等4個核心資通系統未包含於ISMS導入範圍，建議可再釐清

□資通安全政策及推動組織

- 已設置資通安全處理小組，推動資通安全相關工作事項。由副主任委員擔任資安長，每年辦理1次**管理審查會議**，必要時，得辦理臨時會議
- 建議可進一步了解會議中討論之**議題**、**決議**事項及**人員出席**情形(如資安維護計畫、資安法遵符合情形、資訊資產風險評鑑等)

稽核建議-管理面

- 資通系統或服務委外辦理之管理措施
  - 已訂定「委外管理指引」，建立委外執行前或委外契約履行時相關資通安全制度之依循標準， 建議可進一步了解是否符合資安法之**相關委外管理要求**(如細則第4條選任及監督受託者時之應注意事項、SSDLC安全需求等)
- 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
  - 已訂定「OO機關所管特定非公務機關資通安全管理作業辦法」，應於每年十月底前擇定關鍵基礎設施提供者，並得擇定其他特定非公務機關，以現場實地稽核之方式，稽核其資通安全維護計畫實施情形
  - 辦理稽核後，應於次年度1月底前彙整第1項稽核結果報告，並提交主管機關備查；查該機關已函報院資安處， 109年由所屬機關(OO局、OO署及OO署)共稽核8個所管特定非公務機關，建議委員可了解其稽核範圍與方式及待改善事項辦理情形追蹤結果是否妥適

稽核建議-技術面

◘資通安全防護及控制措施

- ➢年度**資安檢測結果**與前一次結果比較，是否有重複出現同樣弱點之情形
- ➢**SOC監控範圍**是否涵蓋應辦事項之資安防護項目，併附SOC情資資訊回傳情形

	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
2020年	53	78	131	41	33	65	43	14	75	99	184	132
2021年	224	163	138	152	356	589	433	357	321	299		

◘**個資與機敏資料存取紀錄**是否定期檢視？檢視方式是否妥適？可抽樣檢視是否有非授權存取情形

- ➢電子資料(含防疫個資)之安全管理機制，**防疫期間所蒐集、處理、利用及刪除之個人資料是否依個資法落實妥處並留存佐證紀錄**

資安實地稽核流程

時間	項目	參與人員
9:00~9:30	•啟始會議 1.**受稽方**代表**OO機關 OO資安長**致詞、介紹出席人員 2.**稽核領隊行政院 OO政委/諮委**致詞、介紹**稽核委員** 3.資安**稽核作業說明**(稽核團隊) 4.**受稽機關資安簡報**(受稽機關)	全體
9:30~9:45	•**稽核團隊稽核前意見交換**	**稽核團隊**
9:45~12:30	•實地稽核(一)	全體
12:30~13:30	•**午餐及彙整實地稽核(一)意見**	稽核團隊
13:30~16:30	•實地稽核(二)	全體
16:30~17:00	•**稽核團隊稽核後意見彙整**	**稽核團隊**
17:00~17:30	•結束會議	全體

資安稽核項目及重點

資安維護計畫與稽核項目(1/2)

資通安全維護計畫		資安稽核項目檢核表
一、核心業務及重要性	一、核心業務及重要性 二、非核心業務及說明	(一) 核心業務及其重要性
二、資通安全政策及目標	一、資通安全政策 二、資通安全目標 三、資通安全政策及目標之核定程序 四、資通安全政策及目標之宣導 五、資通安全政策及目標定期檢討程序	(二) 資通安全政策及推動組織
三、資通安全推動組織	一、資通安全長 二、資通安全推動小組	
四、專職(責)人力及經費配置	一、專職(責)人力及資源之配置 二、經費之配置	(三) 專責人力及經費配置
五、資訊及資通系統之盤點	一、資訊及資通系統盤點 二、機關資通安全責任等級分級	(四) 資訊及資通系統盤點及風險評估
六、資通安全風險評估	一、資通安全風險評估 二、核心資通系統及最大可容忍中斷時間	
七、資通安全防護及控制措施	一、資訊及資通系統之管理 二、存取控制與加密機制管理 三、作業與通訊安全管理 四、系統獲取、開發及維護 五、業務持續運作演練 六、執行資通安全健診 七、資通安全防護設備	(七) 資通安全防護及控制措施 (八) 資通系統發展及維護安全

資安維護計畫與稽核項目(2/2)

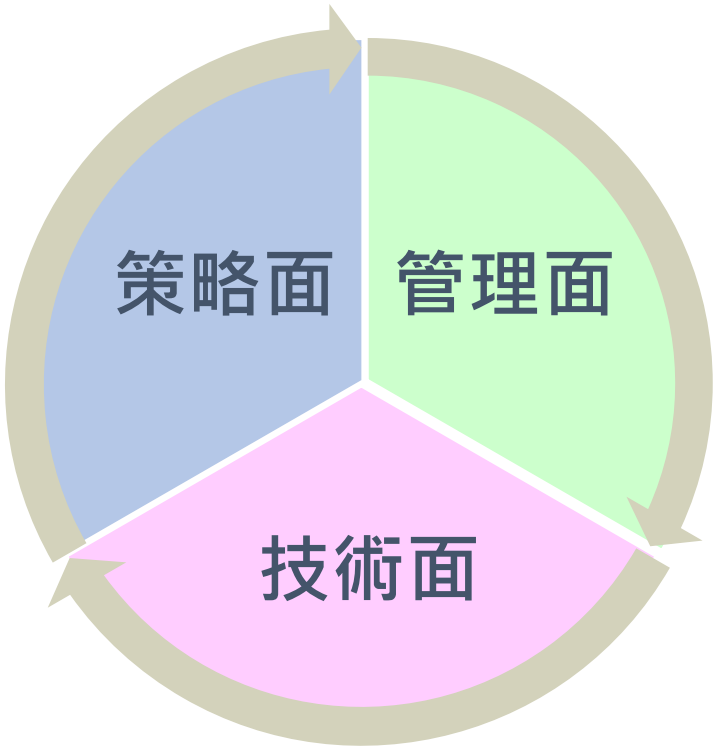
資通安全維護計畫		資安稽核項目檢核表
八、資通安全事件通報、應變及演練相關機制		(九) 資通安全事件通報應變及情資評估因應
九、資通安全情資之評估及因應	一、資通安全情資之分類評估 二、資通安全情資之因應措施	
十、資通系統或服務委外辦理之管理	一、選任受託者應注意事項 二、監督受託者資通安全維護情形應注意事項	(五) 資通系統或服務委外辦理之管理措施
十一、資通安全教育訓練	一、資通安全教育訓練要求 二、資通安全教育訓練辦理方式	(三) 專責人力及經費配置
十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制		(二) 資通安全政策及推動組織
十三、資通安全維護計畫及實施情形之持續精進及績效管理機制	一、資通安全維護計畫之實施 二、資通安全維護計畫實施情形之稽核機制 三、資通安全維護計畫之持續精進及績效管理	(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

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

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

實地稽核項目-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	確認資通**系統盤點及分級**、資訊安全管理系統(ISMS)**範圍**、機關業務持續之**營運衝擊分析**、**備份及備援**機制、**復原測試**、**業務持續運作演練**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**、資安**推動組織**、**資安管理**及運作、**績效評估**量測、**考核**機制及**利害關係人管理**等
3	專責人力及經費配置	確認資安/資訊經費占**經費比率**、**資安人力**配置情形、人員資安作業、**資安認知及訓練**等

實地稽核項目-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**	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
5	**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**	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

實地稽核項目-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**	確認**安全性檢測實施情形**、資通安全健診、資通安全防護實施情形、資通系統及相關設備監控、**使用紀錄管理**、**政府組態基準**實施情形、**電子資料安全管理**機制、**網路規劃及管理**、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、軟體使用安全及**電子郵件安全**等
8	**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，含系統需求、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**	確認**情資分享**機制、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

資安實地稽核流程

時間	項目	參與人員
9:00~9:30	•啟始會議 **1.受稽方**代表**OO機關 OO資安長**致詞、介紹出席人員 **2.稽核領隊行政院 OO政委/諮委**致詞、介紹**稽核委員** 3.資安**稽核作業說明**(稽核團隊) **4.受稽機關資安簡報**(受稽機關)	全體
9:30~9:45	•**稽核團隊稽核前意見交換**	**稽核團隊**
9:45~12:30	•實地稽核(一)	全體
12:30~13:30	•**午餐及彙整實地稽核(一)意見**	稽核團隊
13:30~16:30	•實地稽核(二)	全體
16:30~17:00	•**稽核團隊稽核後意見彙整**	**稽核團隊**
17:00~17:30	•結束會議	全體

稽核發現範例-法遵符合情形

● 法遵符合情形

依據法規條款

策略面

➢已依資通安全責任等級分級辦法應辦事項規定，全機關導入資訊安全管理系統，全部資通系統納入ISMS適用範圍，並通過第三方驗證，**值得肯定**

優規描述

依據法規條款

管理面

➢已依資通安全管理法施行細則第 6 條規定，**確實完成**資通系統盤點，並鑑別其資產價值，且資訊處統一管理所有資通系統及設備，其他單位不能自行委外，落實集中管理

優規描述

技術面

➢已依資通安全責任等級分級辦法應辦事項規定，每年辦理4次網站安全弱點檢測及1次資通安全健診，並建置進階持續性威脅攻擊防禦措施，**優於**資通安全管理法規定

稽核發現範例-待改善事項

● 待改善事項

策略面

➢依資通安全管理法施行細則第7條規定，目前僅將資通系統安全等級高者，列為核心資通系統，**建議**再評估各業務之重要性及必要性，考量增列

法源依據

描述發現事實

要求改善

管理面

➢依「風險評鑑與管理程序書」規定，系統有重大異動時，應執行不定期之風險評鑑，查OO系統本年有重大改版，但未進行風險評鑑，**應**落實執行風險評鑑作業

內規依據

描述發現事實

技術面

➢查OOOO系統之測試站含有正式站之真實資料，**建議**避免使用真實資料進行測試，或將真實資料去識別化

要求改善

未於時限內提供佐證資料

➢依資通安全管理法施行細則第6條規定，雖已訂定資訊資產與個資管理暨盤點程序，**無具體證據顯示**已將網路服務納入資訊資產清單，**應**落實資產盤點

未提供佐證資料

稽核各階段辦理工作摘要

事前準備

- 制定年度稽核計畫(含查檢表等整體規劃)、全體稽核委員擇選、(觀察員遴選)
- 經費估算及分配
- 受稽機關稽核日期編排(以不影響機關重要工作為原則)
- 稽核員及觀察員稽核前訓練

實地稽核前

- 受稽機關稽核前通知
- (現地技術檢測)
- 各場次稽核團隊成員編排
- 行前工作 – 各場次行政作業安排及現場流程協調
- 行前工作 – 各場次受稽機關資料彙整及研析

實地稽核中

- 依當日實地稽核流程進行(時間控制)*
- 稽核結果彙整及提報
- 稽核結果確認並交付受稽機關
- 行政庶務工作

實地稽核後

- 函送稽核結果報告
- 稽核結果登錄系統管考
- 經費核銷
- 稽核結果統計分析
- 年度稽核結束會議

後續推動方向

後續推動

□擴大稽核，確認落實及輔導精進

- ➢資通安全管理法驗證方案：429個
- ➢主管機關全面稽核：府會四院、地方政府

□配套作業

- ➢資通安全管理法修法
- ➢稽核發現代碼：結果彙整分析

機關類型	A級	B級	C級	D級	E級	合計
中央機關	44	113	463	227	111	958
地方政府	0	103	573	4,941	708	6,325
特定非公務機關	46	123	146	88	21	424
全部	90	339	1,182	5,256	840	7,707

統計截止日：111年5月11日

稽核發現代碼

作業規範：依序擇一標註

N	P	L	O01
應辦事項	維護計畫	法條	其他

資通系統：不符項目皆列

C	O02
防護基準	其他

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
1	法遵符合情形	已依資通安全責任等級分級辦法應辦事項規定，全機關導入資訊安全管理系統，**全部資通系統納入ISMS適用範圍，並通過第三方驗證**，值得肯定	資通安全責任等級應辦事項	N10200	(範例)
2	待改善事項	依資通安全管理法施行細則第6條規定，雖已訂定資訊資產與個資管理暨盤點程序，**無具體證據顯示已將網路服務納入資訊資產清單，應落實資產盤點**	資通安全維護計畫實施情形	P6	(範例)
3	建議事項	查○○○○系統之測試站含有正式站之真實資料，**建議避免使用真實資料進行測試，或將真實資料去識別化**	資通系統防護基準	C0504	(範例)

資安是持續精進的風險管理