



數位發展部資通安全署
Administration for Cyber Security, MOD

114年資通安全稽核 作業說明

114年 3月





依 據

- ✓ 資通安全管理法第7條第2項、第13條第1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，以持續精進政府整體資安風險



作業期程



數位發展部資通安全署
Administration for Cyber Security, MOD

準備作業

113年12-114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

前置作業

114年2-3月

- 擬定稽核計畫並進行整備
- 確認受稽機關與協調時程
- 確認稽核委員與觀察員名單，並辦理通知作業

實施作業

114年4月-12月

- 辦理稽核委員與觀察員稽核前訓練
- 辦理受稽機關技術檢測及實地稽核

檢討作業

114年12月-115年1月

- 提出稽核結果及共同發現事項
- 建議表揚成績優良及表現良好機關
- 撰擬送交立法院之年度稽核概況報告



稽核團隊



數位發展部資通安全署
Administration for Cyber Security, moda

*以每場次說明

視需求

- 資安署當然委員觀摩2場次，並比照實習階段之觀察員
- 不參與稽核問答過程

至多6人

- 總統府與中央一級機關含所屬機關之公務人員
- 直轄市政府、各縣市政府及所屬一級機關之公務人員



- 辦理現場幕僚或行政作業之人員

1人

- 資安會報副召集人、協同副召集人、其他授權人員
- 數發部正副首長
- 資安署正副首長、主任秘書
- 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

8~10人

- 策略面2人、管理面3人、技術面3人
- 有維運OT者，另配置OT面2人
- 產、官、學、研等資安專家

- 由資安署及資安院具備資安檢測能力及經驗之技術人員擔任

至多12人



- ✓ 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、114年至117年)
- ✓ 資訊安全管理系統國家標準 CNS 27001:2014、CNS 27001:2023
- ✓ 資訊安全管理系統國際標準 ISO 27001:2013、ISO 27001:2022
- ✓ 服務管理系統國際標準 ISO 20000-1:2018
- ✓ 受稽機關之資通安全維護計畫
- ✓ 工控系統或運營科技(OT)相關國際安全標準與主要國家防護文件
- ✓ 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
- ✓ 其他內部控制及資安相關規定

稽核分組原則



數位發展部資通安全署
Administration for Cyber Security, MOD



稽核分組原則



數位發展部資通安全署
Administration for Cyber Security, MOD



資安責任
等級相同



資訊業務
重要性相當



資安法納管
身分相同

公務機關 & 特定非公
務機關



機關業務
屬性相同



維運工控系
統或運營科
技(OT)

稽核方式及配分



數位發展部資通安全署
Administration for Cyber Security, MOD



第1階段

- 原則針對**A級公務機關**實施技術檢測
 - 8大檢測項目
 - 為期**3天**
- 複測前次發現事項之改善情形 
- 文件提供配合情形 
- **EASM**檢測 
(全部受稽機關)



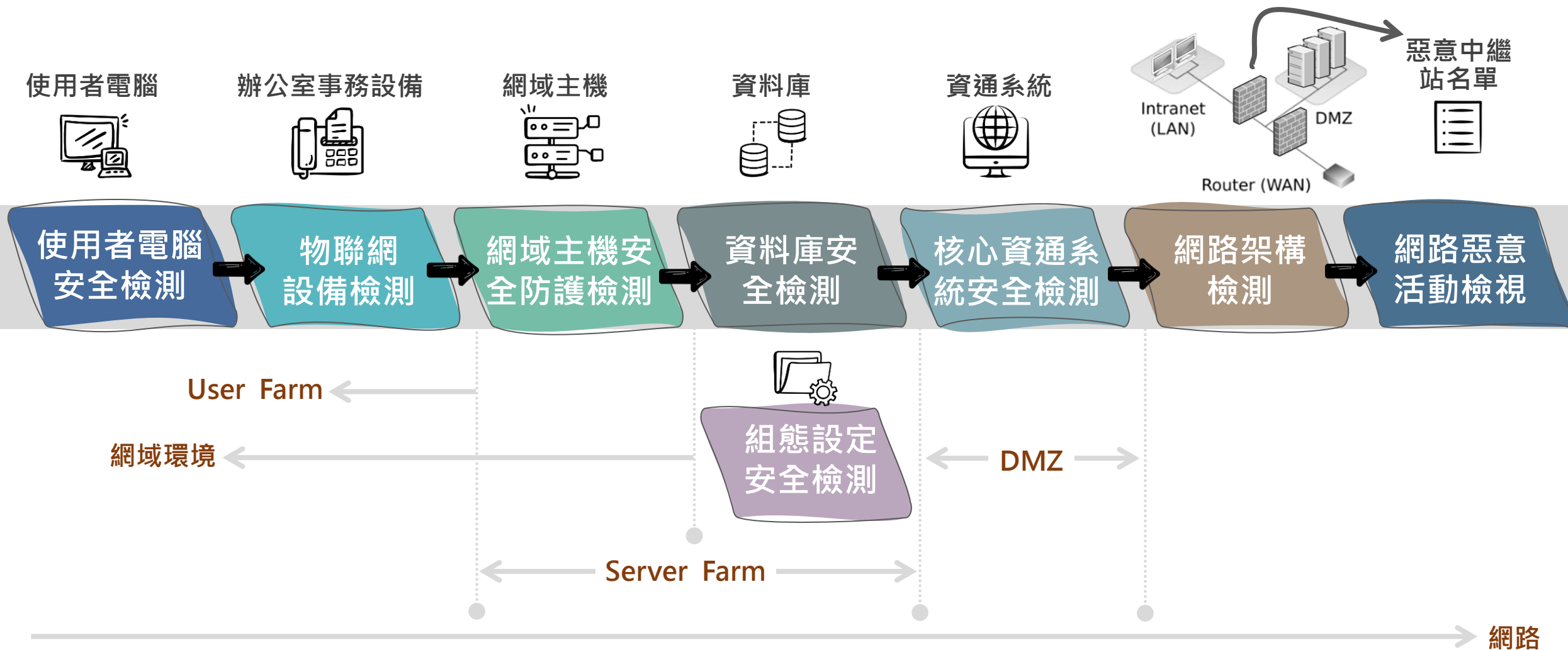
第2階段

- **IT**
3個構面(策略面/管理面/技術面)；共9項稽核項目
- **OT**
2個構面(管理面/技術面)；共10項稽核項目
- 為期**1天**
- 文件提供配合情形 

第1階段-技術檢測框架



數位發展部資通安全署
Administration for Cyber Security, MOD



第1階段-技術檢測項目及配分



數位發展部資通安全署
Administration for Cyber Security, MOD

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

第1階段-技術檢測範圍



數位發展部資通安全署
Administration for Cyber Security, MOD

項次	檢測項目	範圍	執行方式
1	使用者電腦安全檢測	50台使用者電腦	進行全機關網段連接埠掃描，依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
		5台使用者電腦	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安全防護檢測
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，進行身分鑑別、資料安全、系統安全及通訊安全等安全基準檢測
3	網域主機安全防護檢測	1台網域主機	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
4	資料庫安全檢測	1個核心資料庫	抽測10項資料庫安全檢測項目
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及防護基準檢測
6	網路架構檢測	機關網路架構	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

第1階段-技術檢測範圍



數位發展部資通安全署
Administration for Cyber Security, MOD

項次	檢測項目	範圍	執行方式
7	組態設定安全檢測	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	針對已公告之政府組態基準(GCB)項目進行抽測
8	網路惡意活動檢視	全機關	- 依資安院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 - 機關協助提供即時側錄之完整流量，透過資安院自行研發之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
 納入實地稽核參考	複測前次發現事項之改善情形	曾受資安會報技術檢測者	針對前次發現事項進行複測，並將複測結果提供實地稽核參考
 扣分項	文件提供配合情形	須受技術檢測之受稽機關	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
 納入技檢或實地稽核參考	EASM檢測	全部受稽機關	外部攻擊面管理(External Attack Surface Management, EASM)檢測，並將檢測結果提供技術檢測或實地稽核參考

第2階段-實地稽核項目及配分



數位發展部資通安全署
Administration for Cyber Security, MOD

IT稽核

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机制	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

第2階段-實地稽核項目重點



數位發展部資通安全署
Administration for Cyber Security, MOD

IT稽核

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、資安治理成熟度評估等

2

資安政策及推動組織

資安政策及目標、資安推動組織、內稽、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

專責人力及經費配置

資安經費、資訊經費及資安人力等配置情形、人員保密協議、資安教育訓練、資安專業證照及職能訓練證書等

4

資通系統盤點及風險評估

資訊資產盤點及相關管理程序、風險評估、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

5

資通系統或服務委外管理

委外業務安全管理程序、SSDLC安全及防護基準需求、委外廠商及相關人員管理措施、安全性檢測證明或授權證明、受託業務查核等

6

資安持續精進及績效管理

機關資通安全維護計畫、上級機關之監督管理、所屬機關稽核、資安事件審核、資通安全演練之實施等

7

資安防護及控制措施

安全性檢測及資安健診實施情形、GCB/VANS/EDR/資通安全防護措施、網路規劃及管理、電腦機房及重要區域管理等

8

資通系統發展及維護安全

資通系統防護需求、SSDLC各階段資安保護措施、資通系統之變更管制程序等

9

資安事件通報應變及情資

資安情資評估及因應機制、SOC、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、資安演練作業等

第2階段-實地稽核項目及配分



數位發展部資通安全署
Administration for Cyber Security, moda

OT稽核

構面	稽核項目	配分
管理面	一、事件日誌與可歸責性	10
	二、營運持續計畫	10
	三、系統與服務獲得	10
技術面	四、ICS(OT)網路架構	10
	五、存取控制	10
	六、識別與鑑別	10
	七、系統與通訊防護	10
	八、實體與環境防護	10
	九、系統與資訊完整性	10
	十、組態管理	10
合計		100

評分方式

類別	技術檢測	OT	總成績計算方式
1			實地稽核得分 × 100%
2	V		• A級公務機關：技術檢測得分×30% + 實地稽核得分 × 70% • 非A級公務機關：實地稽核得分×100%
3		V	實地稽核得分(資訊系統稽核得分×70% + 工控系統或運營科技(OT)稽核得分×30%) ×100%
4	V	V	• A級公務機關：技術檢測得分×30% + 實地稽核得分(資訊系統稽核得分×70% + 工控系統或運營科技(OT)稽核得分×30%)×70% • 非A級公務機關：實地稽核得分(資訊系統稽核得分×70% + 工控系統或運營科技(OT)稽核得分×30%)×100%

*技術檢測原則針對A級公務機關實施，其他非A級公務機關如經稽核團隊指定為受技術檢測機關，則不計分

*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

*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





績優機關

分數達75分(含)以上，取各分組前1~3名頒發獎座

- ✓ 該分組機關數量 ≥ 9 個
取前3名
- ✓ 該分組機關數量 6~8 個
取前2名
- ✓ 該分組機關數量 < 6 個
取第1名



表現良好機關

未達績優機關，但符合下列情形之一者，函請機關敘獎有功人員：

- ✓ 未列該分組第1名，但分數高於80分
- ✓ 分數未達75分，但列該分組第1名



稽核改善



數發部

每季函送資安稽核報告

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，並至管考系統填報

上級/監督/中央目的 事業主管機關

審查所屬/所監督/所管機關填報內容

追蹤管考



數發部

定期追蹤管考至全部改善完成

受稽機關

持續辦理機關自評為「持續追蹤」項目

上級/監督/中央目的 事業主管機關

審查所屬/所監督/所管機關填報內容

共同性發現



數發部

彙整所有受稽機關之稽核結果，提出資安稽核共同發現事項及建議

受稽機關配合事項



數位發展部資通安全署
Administration for Cyber Security, MOD



受稽機關配合事項



數位發展部資通安全署
Administration for Cyber Security, MOD

期限

依數發部通知函文所訂期限提供

提供文件

全部受稽機關：

- 資通安全實地稽核項目檢核表
- 受稽機關現況調查表
- 機關**最新**之資通安全維護計畫
- 資安推動情形簡報
- 啟始會議簡報

5 項

須受技術檢測者，加填：

- 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护評量表
- 組態設定現況調查表

*擇選3個具資料庫

4 項

有維運OT者，加填：

- OT盤點表
- OT評選表*
- OT資通安全實地稽核項目檢核表

*擇選3個重要性較高

3 項

主辦機關聯絡方式



主辦機關聯絡方式



數位發展部資通安全署
Administration for Cyber Security, moda

實地稽核相關事宜



數位發展部資通安全署

Administration for Cyber Security, moda

游蕙宇、02-2380-8783、hyrain@acs.gov.tw

郭哲維、02-2380-8795、penny@acs.gov.tw

張高禎、02-2380-8781、kaochen@acs.gov.tw

技術檢測相關事宜



數位發展部資通安全署

Administration for Cyber Security, moda

黃 淇、02-2380-8762、huangchi@acs.gov.tw



國家資通安全研究院

National Institute of Cyber Security

陳彥銘、02-6631-6459、yanming@nics.nat.gov.tw



數位發展部資通安全署

Administration for Cyber Security, moda

資安是持續精進的風險管理