113 年度公務機關資安稽核概況報告

數位發展部

中華民國 114 年 4 月

目 次

圖 目 次

表 目 次

壹、 依據及目的

資通安全管理法（以下稱資安法）於 108 年正式施行，行政院依資安法第 13 條第 1 項規定，應稽核行政院所屬或監督機關之資通安全維護計畫實施情形，嗣數位發展部（以下稱本部）自 111 年 8 月 27 日成立，賡續辦理行政院國家資通安全會報資通安全稽核（以下稱行政院資安稽核），協助各機關強化資安防護工作之完整性及有效性，及依同法第 5 條規定，公布「113 年度公務機關資安稽核概況報告」，並送立法院備查。

113 年度行政院資安稽核將資安法法遵事項依屬性，區分策略、管理及技術等 3 項構面進行實地稽核作業，邀請產官學研領域資安外部專家，協同檢視各機關資通安全維護計畫所包括全機關資通系統之各項資通安全管理政策、程序等法遵事項落實情形，並對資通安全責任等級（以下稱資安責任等級）A 級公務機關於實地稽核前實施技術檢測；及對有維運工控系統或運營科技（OT）之受稽機關，額外辦理工控系統或運營科技（OT）實地稽核。113 年度依當前資安威脅情勢，持續滾動調修稽核作業程序及稽核重點，以提升稽核作業之深度及廣度，期經由外部資安稽核，持續改善強化各機關資通安全防護工作之完整性及有效性。

本報告統計 113 年度公務機關資安稽核整體辦理結果，彙整稽核發現之法遵符合情形及待改善事項，摘錄較具重要性可提供各級公務機關共同借鏡之事項，並提出對應之改善建議，以供各級政府機關參考，俾利據以進行檢視，以持續強化機關人員資安意識及提升營運韌性，降低國家整體資安風險。

貳、113 年度資安稽核作業辦理情形

一、 稽核重點

依當前國際資安發展、資安威脅趨勢及我國資安業務推動現況，持續滾動調修稽核作業程序及稽核重點，113 年資安稽核重點為資通系統使用外部元件之盤點更新、危害國家資通安全產品之禁用管控、資安治理成熟度評估及因應、資安事件通報應處及人員認知與訓練符合情形等項目，期敦促加強落實相關因應對策，持續強化公務機關整體資安防護。

二、 受稽機關遴選原則

依 113 年資通安全稽核計畫奉准規劃，113 年受稽核機關原則為 111 年受稽核之行政院所屬二級及獨立機關，並依過去稽核頻率、稽核結果及政策推動情形等綜整考量分配調整。

三、 稽核分組及稽核方式

考量稽核實務，爰將受稽機關依資安責任等級等條件進行分類並分別適用不同之稽核項目及評分方式如表 1。

表 1　稽核類別及評分方式

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

受稽核公務機關之資安責任等級如為 A 級，於實地稽核前先行辦理技術檢測，主要對受稽機關之核心資通系統、網域主機、資料庫、使用者電腦、網路架構及物聯網設備等進行安全檢測，為期 3 個工作日，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，則不納入計分；實地稽核作業由行政院國家資通安全會報組成稽核小組，至受稽機關進行實地查核，為期 1 個工作日。

四、 受稽機關及稽核日期

113 年度各受稽核公務機關實地稽核日期如表 2。

表 2　113 年各受稽機關稽核日期

編號	受稽機關	實地稽核日期
1	中央銀行	4 月 18 日
2	內政部警政署刑事警察局	7 月 18 日
3	勞動部勞工保險局	8 月 8 日
4	內政部	8 月 12 日
5	財政部關務署	8 月 15 日
6	國家發展委員會檔案管理局	8 月 19 日
7	教育部	8 月 26 日
8	財政部財政資訊中心	9 月 2 日
9	行政院人事行政總處	9 月 9 日
10	衛生福利部中央健康保險署	9 月 12 日
11	法務部調查局	9 月 19 日
12	行政院主計總處	9 月 23 日
13	衛生福利部疾病管制署	10 月 7 日
14	交通部公路局	10 月 17 日
15	教育部國民及學前教育署	10 月 24 日
16	內政部移民署	11 月 8 日

五、 稽核團隊

稽核團隊主要由稽核領隊、稽核委員、技術檢測人員組成，共同執行資安稽核作業；另為培訓政府機關稽核種子人員，設置觀察員，並由稽核委員輔導觀察員參與實地稽核，稽核團隊人員組成與其資格如下，本部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。

(一)稽核領隊：

由行政院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，或由行政院國家資通安全會報幕僚單位：本部之正副首長及資通安全署（以下簡稱資安署）之正副首長、主任秘書擔任稽核領隊，並得由策略面委員代理。

(二)稽核委員：

1、 遴選標準

(1) 由本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少於全體成員人數之四分之一。

(2) 稽核委員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，應通知資安署並主動迴避擔任該場次稽核委員。

(3) 稽核委員如於 113 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次稽核之稽核委員。

2、 分配原則

每個稽核場次以安排 8 位稽核委員為原則，包括策略面 2 名、管理面 3 名及技術面 3 名。如受稽機關有維運工控系統或運營科技（OT），則額外配置 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。

(三)技術檢測人員：

由國家資通安全研究院及本部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檢測人員擔任，每場技術檢測人員至多 12 名。

(四)觀察員：

自總統府與中央一級機關含直屬機關、直轄市政府與各縣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。

(五)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 3 至 6 名。

(六)觀摩人員：

觀摩現場實地稽核作業，不參與稽核問答過程，人數視實際需求而定。

六、 稽核基準、範圍與項目

依據資安法及其子法、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、CNS 27001:2023 或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、資通安全維護計畫、其他內部控制及資安相關規定，及受稽機關之資通安全維護計畫等，據以規劃稽核項目。

(一)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安管理政策、程序等。

(二)稽核項目

1、 第 1 階段：技術檢測

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 3。

表 3　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、 第 2 階段：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 個構面共 9 個稽核項目，各構面之稽核項目與配分如表 4。

表 4　資訊系統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

構面	稽核項目	配分
	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

參、113 年稽核結果

113 年受稽公務機關計有 16 個，依稽核階段分以技術檢測、實地稽核及稽核結果說明如下。

一、 技術檢測

技術檢測 8 個檢測項目之平均分數經標準化後，檢視個別項目得分情形，各項目得分整體較去（112）年度呈現向上趨勢，其中「網域主機安全防護檢測」、「資料庫安全檢測」、「核心資通系統安全檢測」及「網路架構檢測」等 4 個項目得分有明顯進步，各項目得分情形詳見圖 1。

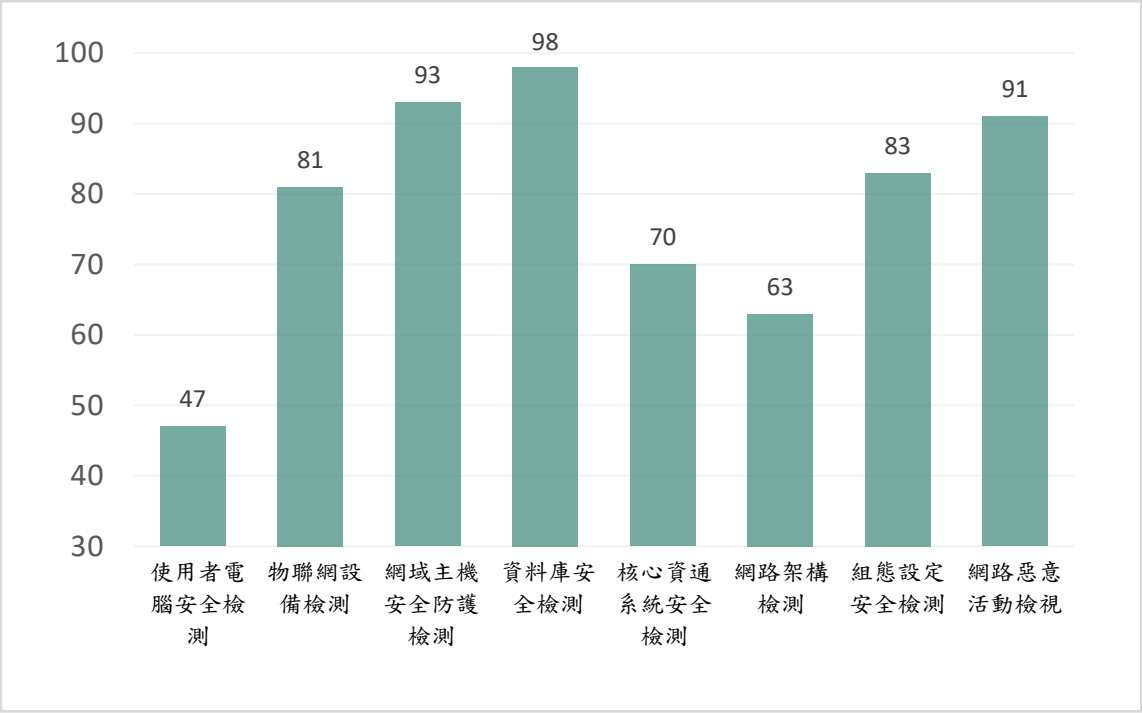

圖 1　技術檢測各項目得分情形

二、 實地稽核

實地稽核 9 個項目之平均得分經標準化後，檢視個別項目得分情形，其中「資安人力及經費配置」得分最高，「資安防護與控制措施」次高，個別項目平均得分情形相較去（112）年度除「核心業務及其

重要性」及「資安政策及推動組織」持平，其餘項目得分均較去年度進步，整體呈現均衡向上趨勢，各項目得分詳見圖 2。

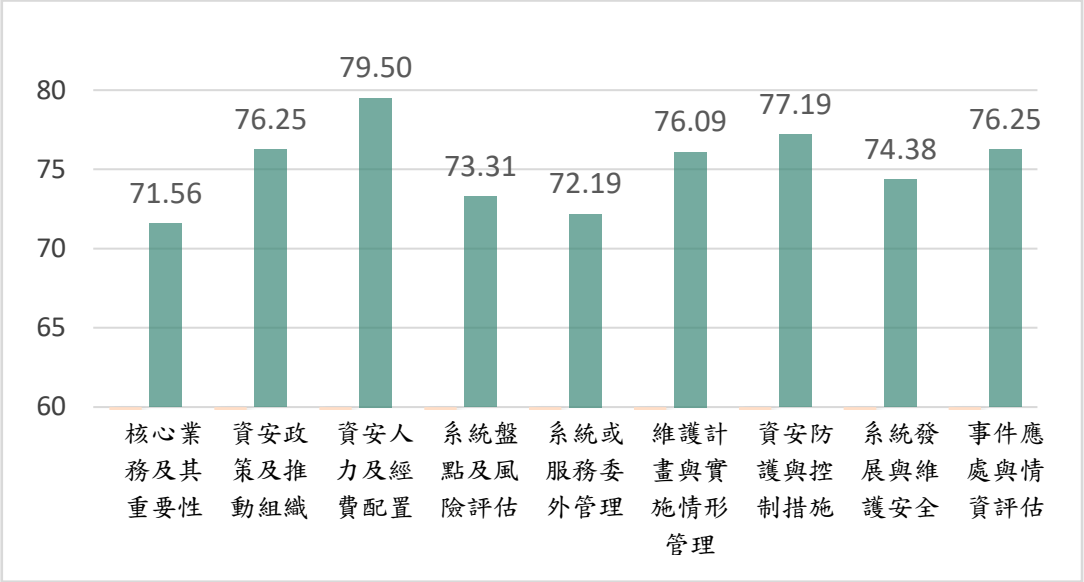

圖 2　實地稽核各項目得分情形

三、 稽核總成績

113 年受稽公務機關平均總成績為 74.69 分，稽核各階段項目平均得分，詳見圖 3。

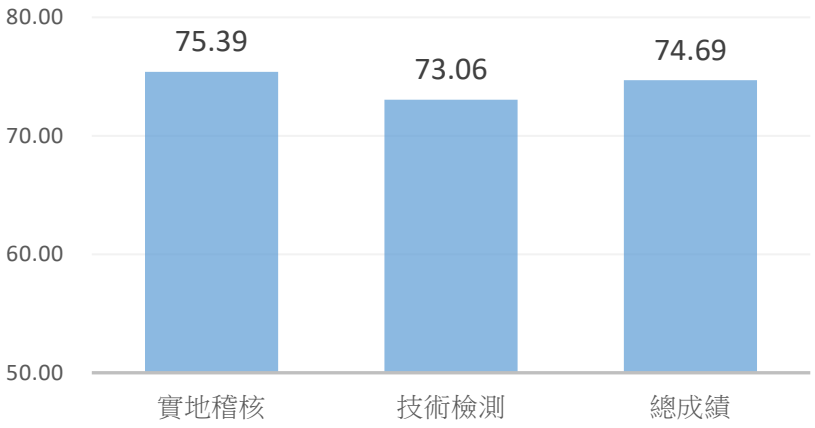

圖 3　各階段項目平均得分成績

另依受稽核機關是否保有重要資料庫分別進行得分成績比較，在實地稽核得分兩者差異不大；技術檢測部分，保有重要資料庫機關之得分表現優於未保有重要資料庫機關，此結果顯示保有重要資料庫機關具備較高的資安風險意識，資通安全防護落實情形相對較佳。平均得分及成績，詳見圖 4。

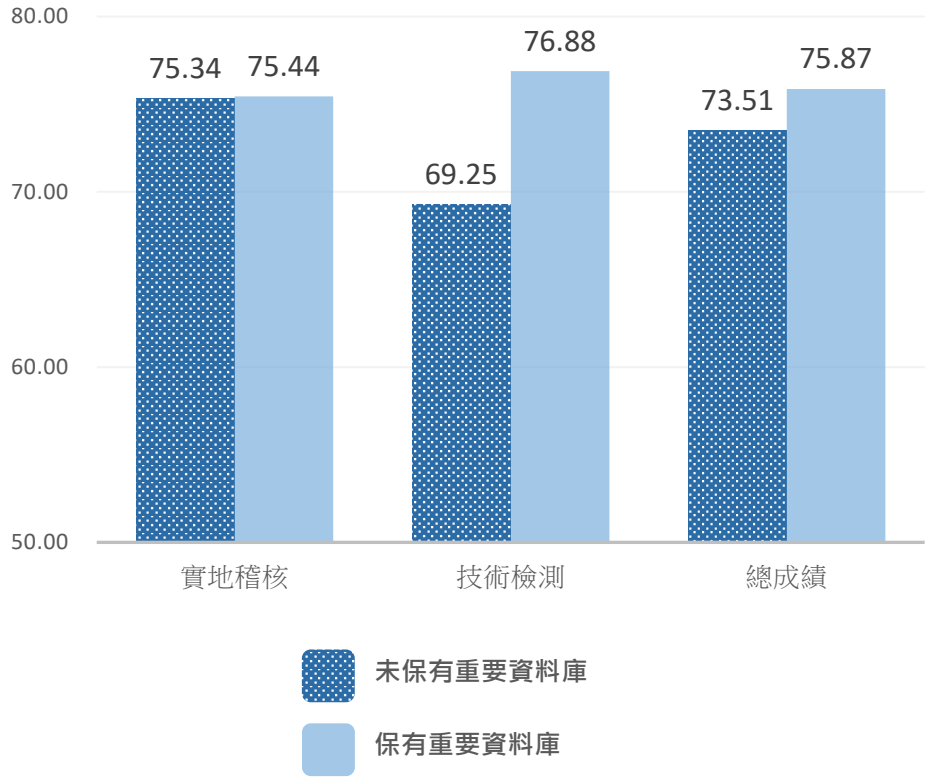

圖 4　是否保有重要資料庫之平均得分成績比較

本次受稽公務機關其中 6 個機關在 108 年資安法施行後曾受行政院資安稽核、10 個機關為首次受行政院資安稽核，分別統計各階段稽核結果，曾受行政院資安稽核機關在實地稽核、技術檢測及整體表現均優於首次受稽核機關。此結果顯示經由行政院資安稽核機制檢視機關各項資安工作及防護措施落實情況，及將稽核結果確實納入機關 PDCA 管理循環流程，對提升機關資安防護工作之完整性、有效性均呈現正面效益。平均得分及成績，詳見圖 5。

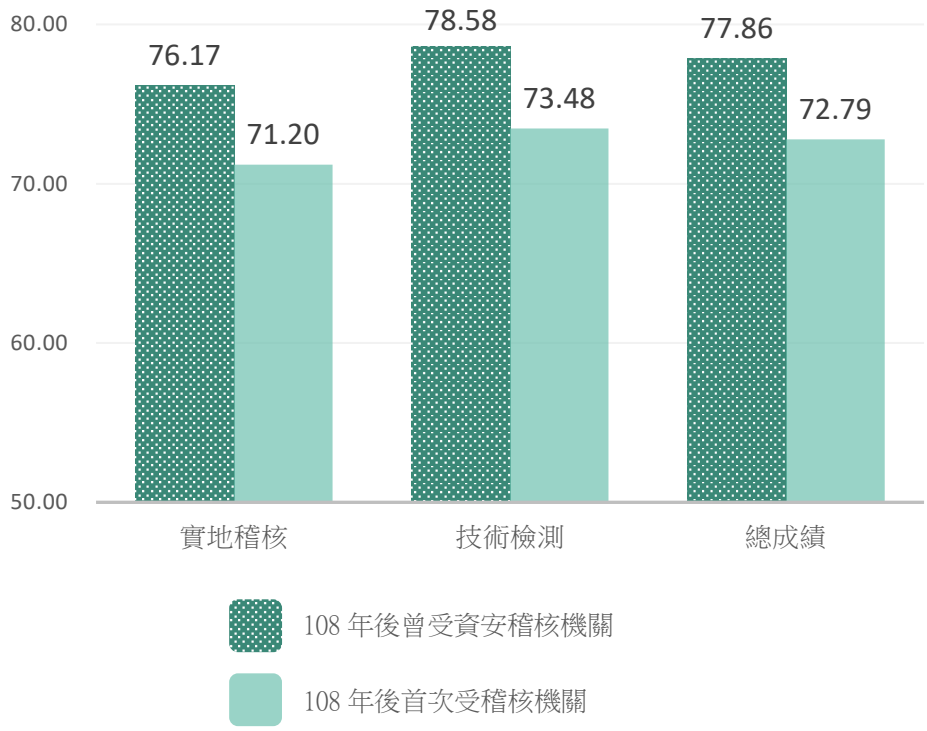

圖 5　是否曾受稽核之平均得分成績比較

肆、稽核共同發現

經綜整 113 年之稽核發現，就法遵符合情形及待改善事項，彙整較具重要性可提供各級公務機關借鏡之事項，分別就策略面、管理面及技術面分別說明如下。

一、法遵符合情形

(一)策略面

1、依規定配置足額之資通安全專職人員外，並另增加專職辦理資安業務之人力，且增加之人員均持有資安專業證照及職能證書。

2、由資安長親自主持資通安全管理審查會議，並要求組織成員親自出席，審議資安相關之重要事項，顯示管理階層對機關資通安全政策之支持與重視。

3、成立專責單位將資訊及資安業務及資源向上集中整合，並統籌辦理系統安全性檢測工作。

(二)管理面

1、以實地稽核方式，確認機關全部核心資通系統及部分非核心資通系統之委外廠商受託業務執行情形，並留存稽核管考紀錄，落實委外監督管理工作。

2、依規定將全部核心系統導入 ISMS 及通過第三方驗證，並逐步擴大導入及驗證範圍至其他資通系統，部分機關已完成全機關導入並通過驗證。

3、依規定訂定資安事件通報相關作業規範及進行演練，並針對各級資安事件設計數十種模擬真實狀況演練情境。

(三)技術面

1、除依法令規定按系統防護需求分級辦理相關控制措施，另依機關實務需求就高風險項目加強執行安全性檢測。

2、辦理資安紅隊演練，以強化精進機關資安防護及應變能力。

3、機關運用工具嚴格管制內部跨網段資料交換，並紀錄資料交換行為且定期進行檢視。

二、待改善事項

(一)策略面

1、部分機關業務持續運作演練未切合實際，且未妥適規劃備份資料之復原程序。

2、部分機關資通安全政策及目標未臻妥適，或目標、指標設定過低。

3、部分機關持續精進及績效管理機制未確實執行。

(二)管理面

1、部分機關未落實監督及管理委外廠商工作。

2、部分機關未完整盤點資通系統及資訊資產、未妥適界定核心系統及系統分級。

3、部分機關之內部稽核辦理範圍、頻率及稽核項目規劃未臻妥適。

(三)技術面

1、部分機關未完成全部高風險弱點之修補，或完成修補前未加強管控或採行緩解措施。

2、部分機關資安事件通報作業仍有未符規定情形。

3、部分機關資安防護控制措施之執行未完備。

三、 改善建議

(一)策略面

1、依資通安全責任等級分級辦法應辦事項及防護基準規定，核心資通系統應辦理持續運作演練，及辦理系統備份備援作業。機關應對整體資訊服務進行營運衝擊分析（BIA），明確訂定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），並訂定備份資料之復原程序及定期執行回復測試，

以確保備份資料之有效性。另建議評估納入複合式及資安新興議題演練情境，以切合實際。

2、依資通安全管理法施行細則第 6 條規定，機關資通安全維護計畫應訂定資通安全政策及目標，目標宜有量化型及質化型指標，且應考量合宜性（例如不應納入資安事件發生次數）並有一致性的量測頻率及衡量基準，定期依實際執行及指標達成情形，檢討調修資通安全維護計畫。

3、依資通安全管理法第 10 條、第 12 條、資通安全管理法施行細則第 6 條及資通安全責任等級分級辦法應辦事項規定，機關應訂定且每年滾動式調修資安維護計畫，並確實辦理內部資通安全稽核及稽核發現之後續改善作業追蹤管考，以落實 PDCA 管理循環流程及持續精進及績效管理目標。

(二)管理面

1、依資通安全管理法第 9 條、資通安全管理法施行細則第 4 條、第 6 條及資通安全責任等級分級辦法應辦事項規定，對資通系統或服務之委外，應依資通系統分級將 SSDLC 安全及防護基準需求納入招標文件，並落實辦理 ISMS 程序書、維護計畫等委外管理要求，且定期以稽核或其他適當方式，確認受託業務執行情形。另對危害國家資通安全產品應依相關規定落實管制，並確實要求委外廠商禁止使用。

2、依資通安全管理法施行細則第 6 條規定，應落實盤點完整掌握全機關之資通系統及相關資產。盤點範圍應涵蓋全機關，包含業務單位、輔助單位，納入 OT、IoT、連網及未連網設備，並落實資產異動管理程序，及依規定進行後續資安風險評估及資通系統分級等作業。

3、依資通安全管理法施行細則第 6 條及資通安全責任等級分級辦法應辦事項規定，機關應實施內部資安稽核，稽核範圍應

涵蓋全機關，非僅限資訊單位，並建議擬定整體稽核計畫，規劃各單位之稽核頻率、稽核委員組成及稽核發現之後續追蹤管考機制。

(三)技術面

1、依資通安全責任等級分級辦法應辦事項及資通系統防護基準規定，應定期辦理安全性檢測、導入弱點通報機制及定期進行軟體元件漏洞修復與更新，倘發現軟體或元件具有安全漏洞，或經安全性檢測所檢出之系統漏洞，應依機關風險評估及處理原則，設法修復並定期追蹤修復進度，並配合定期之安全性檢測確認複測。發現高風險以上之弱點，應即時完成修補，於完成修補前應規劃緩解措施及管理作為。

2、依資通安全管理法第 14 條、資通安全事件通報及應變辦法第 9 條規定，應訂定資通安全事件通報作業規範並進行相關演練，於發生資安事件時方能確實依相關作業流程規範，執行等級判定等作業，並依時限完成通報。

3、依資通安全責任等級分級辦法應辦事項及資通系統防護基準規定，並得參考國家資通安全研究院訂定之參考文件，如資通系統防護基準驗證實務規範、安全控制措施參考指引等，持續落實技術面各應辦事項及控制措施。並建議加強確認遠端連線原則禁止例外允許、高權限帳號控管、無線 AP 管理檢查機制、SOC 導入範圍及監控管理資料之提交、防火牆規則定期檢視、資訊機房消防區隔及監視設備等事項。

伍、結語

資安法於 108 年施行，迄今已 6 年餘，本部於 111 年成立後賡續辦理行政院國家資通安全會報層級資通安全稽核作業，檢視各機關資通安全維護計畫實施情形及相關資安防護強化措施之完整性及有效性，協助政府機關持續依循法遵，逐步調整機關內部資安政策、管理制度及防護基準，提升各項法遵要求落實程度。此外，為強化國家整體資通安全法制，刻正推動資安法修法工作，期持續健全各級機關資安防護，強化國家整體資通訊安全及韌性。

本部除定期將年度稽核共同發現事項及改善建議，函請全國各機關作為持續精進資安防護作為之準據，並透過資通安全長會議或全國巡迴說明會加強宣導；以本部資安署資通安全作業管考系統，管考受稽機關改善情形，列管至全部改善完成為止，同時視個案狀況進行相關輔導作業，俾受稽機關落實並強化資安防護工作。

資安政策之推動及各項防護措施之落實，有賴中央及地方各級機關之合作，本部除將各直轄市、縣市政府行政機關資安專業人才，納入行政院資安稽核團隊之稽核員培訓，亦辦理政府機關資安知能及資安稽核相關教育訓練，以促進政府各級機關資安同仁進行經驗交流及學習分享。此外，逐步擴大納入民間產學研資安專業人才，遴選聘任資安稽核委員，提升整體資安稽核量能。並將持續分析資安整體威脅情勢，滾動調整稽核項目與重點，持續精進資安稽核作業，協助機關發掘形成問題的根本原因並提出對應解決方案，以防範潛在之資安風險，持續改善提升各機關資安防護水準。