112 年度公務機關資安稽核概況報告

數位發展部

中華民國 113 年 7 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，為檢視機關辦理資安法及其子法相關法遵事項之落實情形，上級機關應稽核所屬公務機關之資安維護計畫實施情形與整體防護作為。

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，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，且依同法第 5 條規定，公布「112 年度公務機關資安稽核概況報告」，並送立法院備查。

112 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 8 大項技術檢測；112 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，並將工業控制系統項目正式納入稽核計分，依資通安全責任等級分級辦法應辦事項規定及該領域適用之工業控制系統資安防護基準進行稽核，並依機關資安責任等級適當分組辦理評比，期拓展稽核作業之深、廣度及有效性，並達成評核公平性。

本報告彙整 112 年度資安稽核整體辦理結果，研析受稽機關共同發現事項，並提供改善建議供各機關參考，俾利政府機關據以自我檢視，以持續策進強化機關資安意識及整體資安防護韌性，以降低國家整體資安風險。

貳、112 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，112 年資安稽核重點為危害國家資通安全產品使用管控、第二方稽核執行情形、警戒專案網站韌性強化措施及電子防疫個資管理等項目，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韌性。

二、 受稽機關遴選原則

依 112 年資通安全稽核計畫奉准規劃，112 年受稽核機關原則為 2 年內未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進行分組並分別適用不同之稽核方式如表 1。

表 1　稽核分組及稽核方式

稽核分組			第 1 分組	第 2 分組	第 3 分組	第 4 分組
資安責任等級			A	B	A	B
稽核方式	技術檢測		●	–	●	–
	實地稽核	無工業控制系統	●	●	–	–
		有工業控制系統	–	–	●	●

第 1、3 分組於實地稽核前先辦理技術檢測，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；另第 1 至 4 分組均辦理實地稽核，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

112 年度各受稽機關實地稽核日期如表 2，各受稽機關 ISMS 驗證資訊詳如附錄。

表 2　112 年各受稽機關稽核日期

編號	受稽機關	實地稽核日期
1	衛生福利部臺中醫院	6 月 13 日
2	國立故宮博物院	6 月 15 日
3	交通部民用航空局飛航服務總臺	7 月 3 日
4	中央選舉委員會	7 月 10 日
5	文化部	7 月 12 日
6	衛生福利部	7 月 17 日
7	衛生福利部桃園醫院	7 月 27 日
8	國家發展委員會	7 月 31 日
9	交通部中央氣象局氣象資訊中心	8 月 21 日
10	國家通訊傳播委員會	8 月 25 日
11	國軍退除役官兵輔導委員會	8 月 28 日
12	內政部警政署	8 月 30 日
13	高雄榮民總醫院	9 月 7 日
14	內政部消防署	9 月 13 日
15	臺中榮民總醫院	9 月 25 日
16	外交部	9 月 27 日
17	外交部領事事務局	10 月 4 日
18	國立成功大學醫學院附設醫院	10 月 11 日
19	臺北榮民總醫院	10 月 25 日
20	海洋委員會海巡署	10 月 30 日
21	國立臺灣大學醫學院附設醫院	11 月 2 日
22	國家教育研究院教育制度及政策研究中心	11 月 6 日
23	法務部	11 月 9 日
24	衛生福利部臺南醫院	11 月 16 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：

(一)稽核領隊：

由行政院國家資通安全會報副召集人、協同副召集人或經其授權之人員擔任，得由協同領隊或策略面委員代理。

(二)協同領隊：

每個受稽機關配置至多 1 人，由行政院國家資通安全會報幕僚單位(本部)之正副首長、主任秘書或國家資通安全研究院(以下稱資安院)之院長擔任。

(三)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 項各款之迴避參與該次稽核情形，應通知本部並主動迴避擔任該場次之稽核委員。

(3) 稽核委員如於 112 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，亦應通知本部及迴避擔任該次稽核之稽核小組成員。

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業控

制系統，則額外配置 2 名工業控制系統稽核委員進行工業控制系統實地稽核作業。

(四)技術檢測人員：

由本部資安院及資通安全署(以下稱資安署)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。

(五)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。

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 或國際資訊安全管理標準 ISO 27001:2013、國際資訊技術服務管理標準 ISO 20000-1：2018 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，重點在檢驗機關資安設定及安全性更新之落實度，各檢測項目與配分如表 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
	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

構面	稽核項目	配分
	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

工業控制系統實地稽核分管理面及技術面2個構面10個稽核項目，稽核項目與配分如表5。

表 5　工業控制系統各構面稽核項目及配分

構面	稽核項目	配分
管理面	一、稽核與可歸責性	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

3、 計分方式

(1) 第1分組

整體總成績=技術檢測得分x30%＋實地稽核得分x70%。

(2) 第2分組

整體總成績=實地稽核得分x100%。

(3) 第3分組

整體總成績=技術檢測得分x30%＋實地稽核得分(資訊系統稽核得分x70%+工業控制系統稽核得分x30%)x70%

(4) 第4分組

整體總成績=實地稽核得分(資訊系統稽核得分x70%+工業控制系統稽核得分x30%)x100%

參、112 年稽核結果

各受稽機關之稽核結果，第 1 分組總分平均為 70.26 分，其中技術檢測平均分數為 65.72 分，實地稽核平均分數為 72.2 分；第 2 分組總分平均為 69.83 分；第 3 分組總分平均為 63.71 分，其中技術檢測平均分數為 53.66 分，工業控制系統平均分數為 51.1 分，實地稽核平均分數為 75.26 分；第 4 分組總分平均為 59.70 分，其中工業控制系統平均分數為 54.33 分，實地稽核平均分數為 62 分。

一、 技術檢測

112 年計 15 個公務機關受測，技術檢測分數達 75 分以上者有 2 個機關，其餘 13 個機關未達 75 分之主因係機關使用者電腦未落實執行安全性更新，物聯網設備未落實執行重大 CVE 漏洞軟/韌體更新修補，資料保護機制不完備，以及未使用加密方式儲存與傳輸機敏資料等，受測機關之技術檢測成績分布如圖 1。

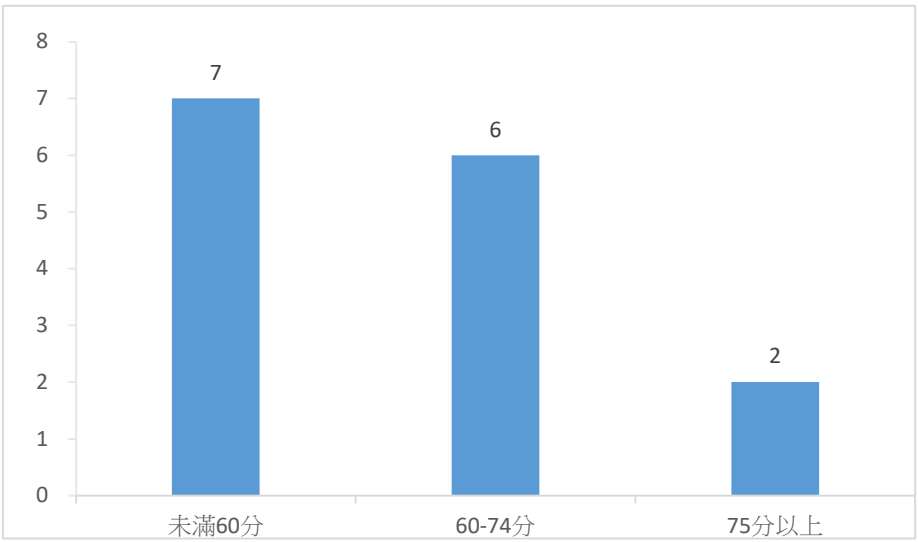

圖 1　技術檢測成績分布

技術檢測個別項目成績，詳見圖 2，其中「網域主機安全防護檢測」、「組態設定安全檢測」及「網路惡意活動檢視」等 3 項表現較佳，達 75 分以上水準。在「使用者電腦安全檢測」、「核心資通系統安全檢

測」及「網路架構檢測」等 3 個檢測結果顯示仍待改進。經統計發現較多機關存在使用者電腦開啟之 SSL 服務存在安全性不足的加密演算法弱點、系統存在注入攻擊弱點(Injection Attack)及網路設備管理介面未限制存取來源位址等風險弱點。

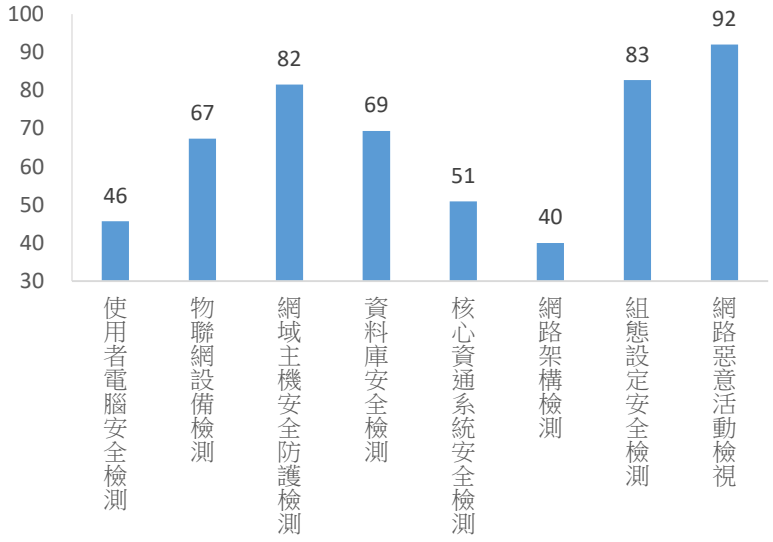

圖 2　技術檢測個別項目成績分布

二、 實地稽核

實地稽核計 24 個公務機關分為 4 組，總分平均為 70.97 分。成績達 75 分(含)以上者有 7 個機關，17 個機關成績未達 75 分，主要問題點為資通系統及資訊盤點完整性不足、第三方驗證範圍未適時調整或有部分核心系統未納入驗證範圍、委外管理仍待加強致供應商配合度不足、內部稽核機制待改善，以及未落實執行資安事件通報及應變程序等，整體受稽機關成績分布，詳見圖 3。

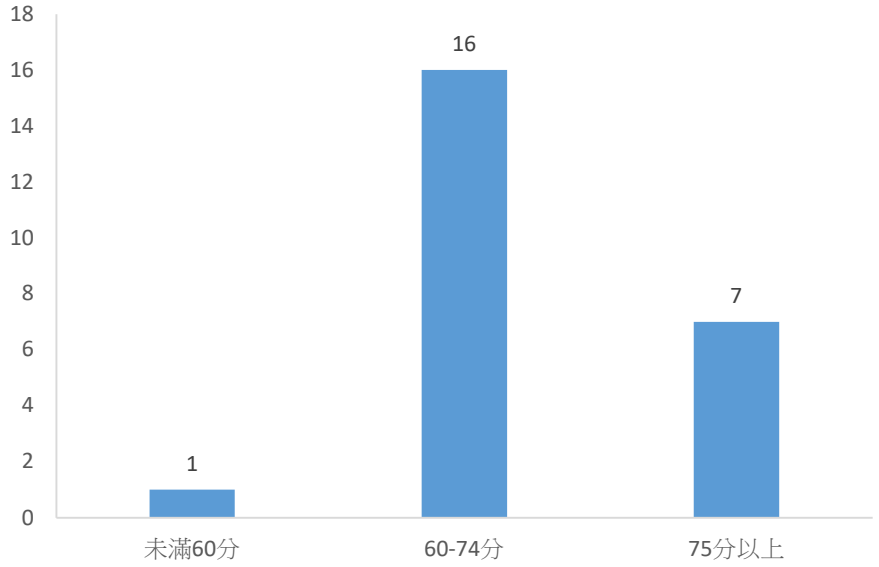

圖 3　實地稽核成績分布

經檢視實地稽核個別項目成績分布，詳見圖 4，其中「資通安全政策及推動組織」表現最好；「資通安全事件通報應變及情資評估因應」成績最低，顯示仍有多數機關在資安事件通報及情資的應處效率可再持續精進改善。

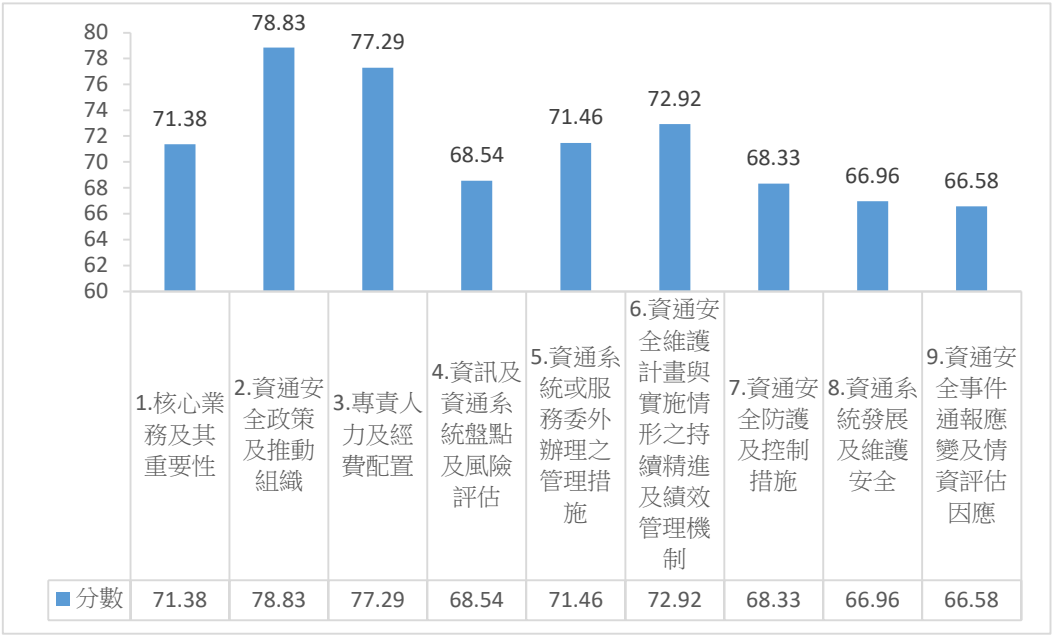

圖 4　實地稽核個別項目成績分布

經檢視工業控制系統稽核個別項目成績分布，詳見圖 5，其中「實體與環境防護」表現最好；「事件日誌與可歸責性」成績最低，顯示仍有多數機關在日誌保存時間、備份及定期查看與審核部分尚待持續調整改善。

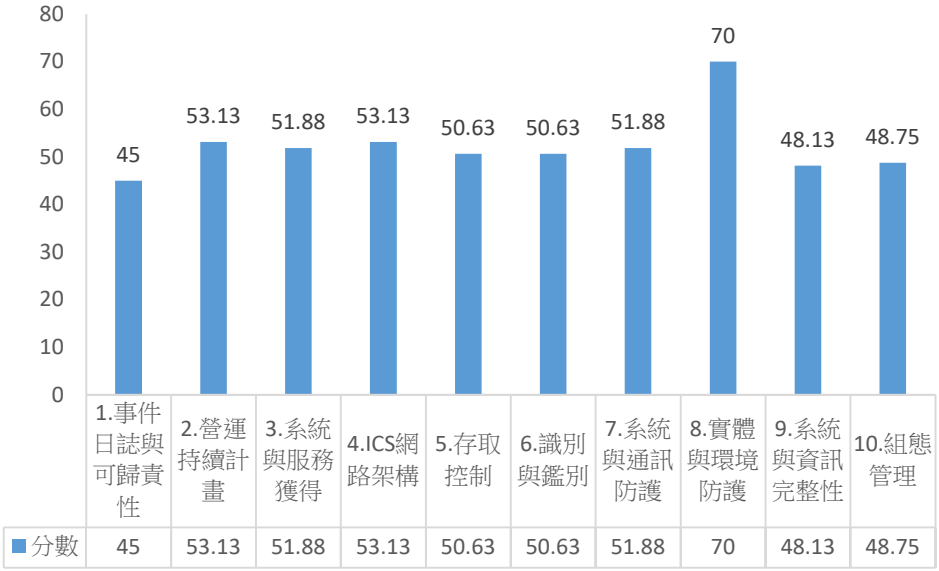

圖 5　工業控制系統實地稽核個別項目成績分布

三、 各分組稽核成績比較

112 年受稽機關分為 4 組，稽核分組及稽核方式詳如本報告表 1。

(一)第 1 分組

資安責任等級 A 級且無工業控制系統之機關計 10 個，實地稽核平均分數 72.2 分，其中 75 分以上有 4 個機關，其餘 6 個機關未達 75 分，成績分布，詳見圖 6。

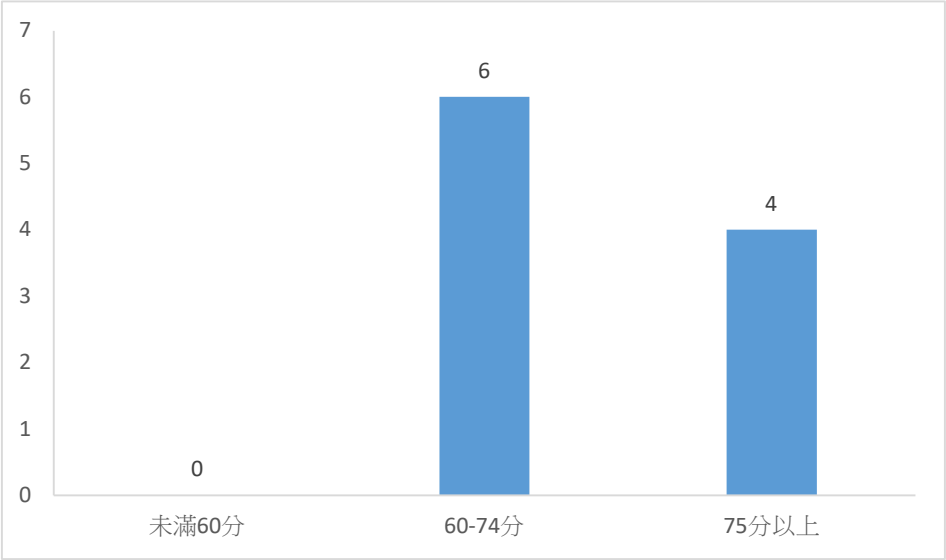

圖 6　第 1 分組實地稽核成績分布

(二)第 2 分組

資安責任等級 B 級且無工業控制系統之機關計 6 個，實地稽核平均分數為 69.83 分，其中 75 分以上有 1 個機關，其餘 5 個機關未達 75 分，成績分布，詳見圖 7。

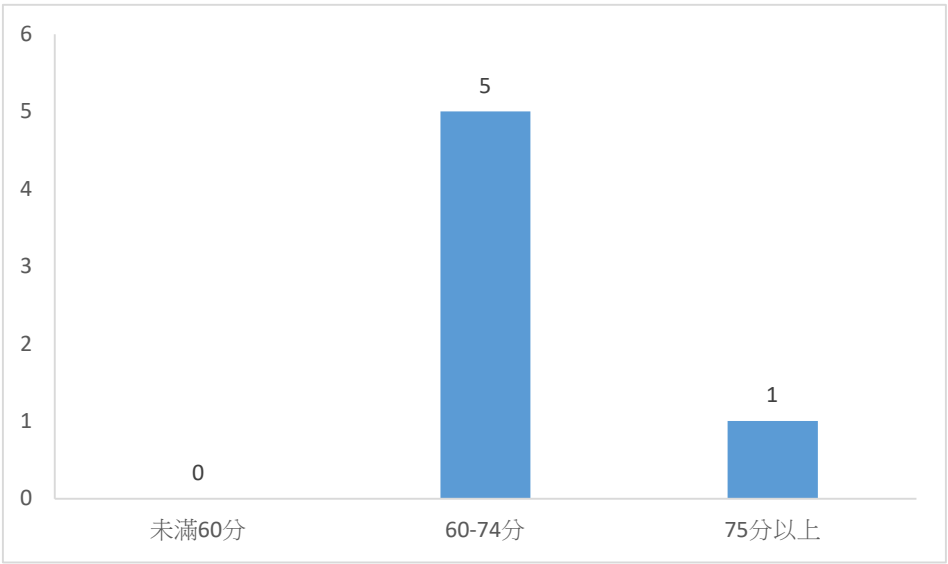

圖 7　第 2 分組實地稽核成績分布

(三)第 3 分組

資安責任等級 A 級且有工業控制系統之機關計 5 個，實地稽核平均分數 75.26 分，其中 75 分以上機關有 2 個，3 個機關未達 75 分，成績分布，詳見圖 8。

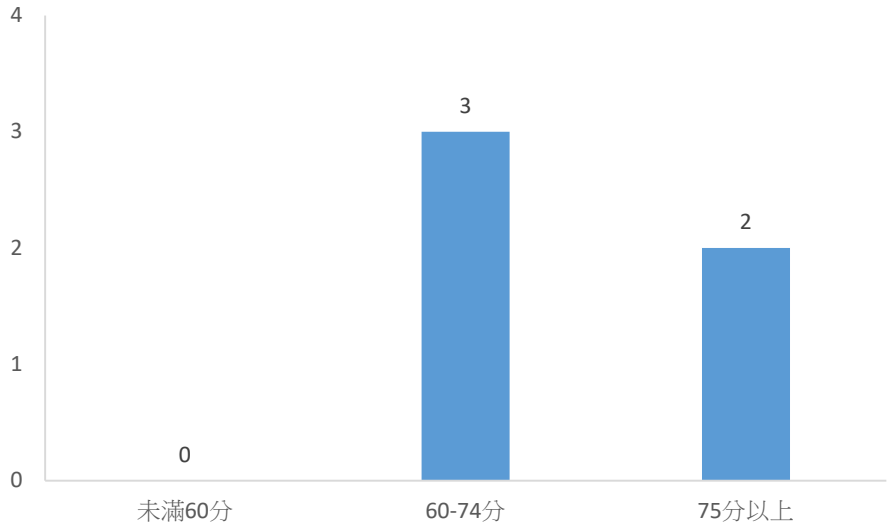

圖 8　第 3 分組實地稽核成績分布

(四)第 4 分組

資安責任等級 B 級且有工業控制系統之機關計 3 個，實地稽核平均分數為 62 分， 3 個機關未達 75 分(1 個機關未滿 60 分)，成績分布，詳見圖 9。

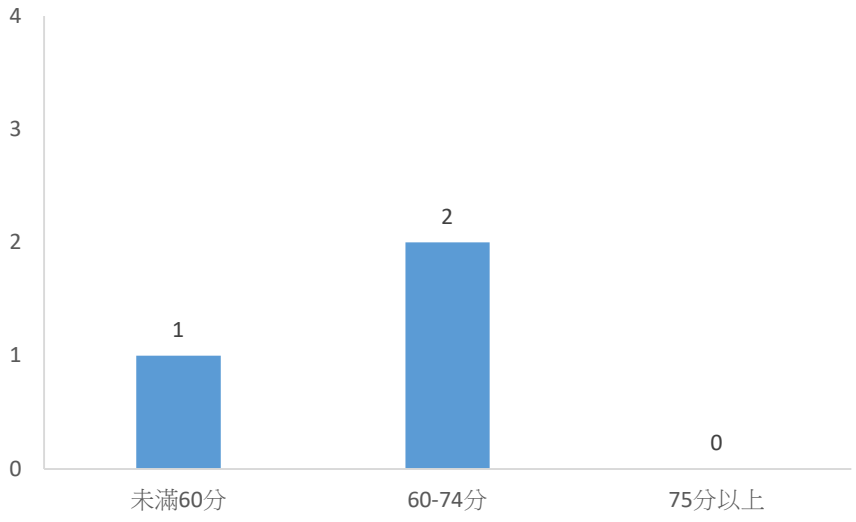

圖 9　第 4 分組實地稽核成績分布

肆、 稽核共同發現

綜整 112 年之稽核發現，依法遵符合情形與待改善事項，以策略面、管理面、技術面及工業控制系統分別說明。

一、 法遵符合情形

(一)策略面

1、 配置足額資通安全專責/專職人員，且各別人員均持有資通安全專業證照及職能訓練證書各 1 張以上，並維持其有效性。

2、 定期辦理全部核心資通系統業務持續運作演練，且參與人員涵蓋全機關，包含相關作業人員、業務單位及資訊單位。

3、 機關指派資安長負責推動及監督機關內資通安全相關事務，由資安長親自主持資通安全管理審查會議，顯示管理階層對資通安全政策之支持與重視。

(二)管理面

1、 機關辦理之資通系統及資訊資產盤點，包含已終止支援服務(End of Support)之伺服器、作業系統及非資訊部門採購之電腦設備等，並落實進行資產價值鑑別與風險評估。

2、 定期辦理社交工程演練，並依據演練成果辦理教育訓練，提升機關人員資安意識。

3、 就資通系統委外開發或維運，在選任及監督等各階段皆納入對委外廠商之資安要求。

(三)技術面

1、 定期辦理資通安全健診及安全性檢測作業。

2、 依資通安全責任等級辦法資通系統防護基準，執行對應之控制措施。

3、 導入端點偵測機制，及進階持續性威脅攻擊防禦機制。

(四)工業控制系統

1、 建立安全防護網路架構，區隔工控網路邊界。

二、 待改善事項

(一)策略面

1、 未建立完整利害關係人清單及聯繫通報機制，致未能確保資通安全政策目標之完整性。

2、 營運持續計畫之系統備份與系統備援措施未完善，未能驗證備份媒體之可靠性及資訊之完整性。

3、 資通安全維護計畫與實施情形未有持續精進及績效管理機制，或未就績效指標之量測頻率與次數訂定標準。

(二)管理面

1、 部分機關辦理內部稽核範圍及內容不足，僅針對資訊單位執行內部稽核，亦有稽核自身所管業務及未有追蹤改善機制情形。

2、 部分機關辦理資通系統及資訊資產盤點範圍及內容完整性不足，僅為資訊單位且對資產分類不一致。

3、 部分機關辦理風險評估及處理範圍不足，未納入全機關資通系統與資訊資產，且未訂有一致性的評估及處置標準，未能有效反映核心資通系統之重要性。

(三)技術面

1、 部分機關資安事件通報及應變程序，未納入演練相關規定或未留存相關紀錄。

2、 部分機關未能確認資通系統相關漏洞修復之有效性，且未能針對安全漏洞通告有評估、處理、測試等機制。

3、 部分機關日誌保存政策與資通安全責任等級分級辦法資通系統防護基準規定不完全符合，日誌未至少留存 6 個月，且未建立日誌審查及保存檢核機制。

(四)工業控制系統

1、 部分機關未將工業控制系統納入資通系統及資訊資產盤點範圍，未執行對應之控制措施。

2、 部分機關在工業控制系統未訂有帳號新增、刪除、盤點及審核等管理機制，亦無遠端存取管控機制。

3、 部分機關工業控制系統未有日誌留存紀錄或留存範圍不足。

三、 改善建議

(一)策略面

1、 依資通安全管理法施行細則第 6 條規定，機關制訂之資通安全政策目標，應涵蓋利害關係人之資通安全目標。機關之利害關係人應至少包含機關內部、上級/監督機關、所屬/所管機關、合作機關、資通訊服務供應商、民眾等，並於機關發生資通安全事件時，通知相關之利害關係人。

2、 資通系統之最大可容忍中斷時間(MTPD)、系統復原時間目標(RTO)與資料復原時間點(RPO)，應依實際業務需求與業務單位共同評估，並據以訂定合適之備份政策，並依資通系統防護等級分級結果實施對應之備份媒體存放及測試措施，系統防護需求等級中級以上之資通系統，並應建立系統備援機制。

3、 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所訂定各項量化型及質化型資通安全指標，應有一致性的量測頻率及衡量基準，且定期檢討指標達成及資安維護計畫執行情形，並據以調修資通安全維護計畫。

(二)管理面

1、 依資通安全責任等級分級辦法應辦事項規定，機關內部稽核之範圍應為全機關，不應侷限於資訊單位，且不應以各內部單位輪流受稽方式辦理。對於內部稽核之發現，亦應有改善情形追蹤及持續精進等管理機制。

2、 依資通安全管理法施行細則第 6 條規定，機關資通系統及資訊資產盤點範圍應為全機關，並定義一致之資訊資產分類，不應侷限於資訊單位、經費來源或有連網設備，並應包含各單位營運之系統及相關設備、有線及無線網路設備。

3、 依資通安全管理法施行細則第 6 條規定，機關風險評估及處理範圍應為全部資通系統與資訊資產，不侷限於核心資通系統，並應以機密性、可用性、完整性及法遵性等面向，制定有一致的資產價值鑑別、風險評估及處置準則。

(三)技術面

1、依資通安全管理法第14條規定，機關應訂定資通安全事件通報及應處機制，並應依資通安全事件通報及應變辦法第 9 條及第10條規定，至少包含影響範圍之判定、損害控管、鑑識調查、證據保全、內部通報程序、通知其他受影響之機關等之權責等，以及前開各項程序之演練。

2、依資通安全責任等級分級辦法應辦事項規定，至少核心系統應定期進行安全性檢測及資通安全健診，並應即處置並有追蹤驗測機制確認修補或替代措施之有效性；針對已被公開之資通安全漏洞，應即評估影響範圍並即時修補，倘即時修補有窒礙難行之處，應執行其他替代措施，並應測試修補及替代措施之有效性。

3、依資通安全責任等級分級辦法資通系統防護基準及各機關資通安全事件通報及應變處理作業程序規定，各機關於日常維運資通系統時，應依自身資安責任等級，至少保存最近 6 個月之日誌紀錄(log)，保存範圍除全部核心資通系統外，建議納入各項資通及防護設備及網域名稱系統(DNS)，保存項目至少包含作業系統日誌(OS Event log)、網站日誌(Web log)、應用程式日誌(AP log)及登入日誌(Logon log)，且應

透過日誌審查機制，確保日誌範圍之正確性及可用性。

(四)工業控制系統

1、 依資通安全管理法施行細則第 6 條規定，機關資通系統與資訊資產盤點為全機關，不侷限於IT類，應包含工控系統(ICS)或運營科技(OT)類系統及對應設備。

2、 依資通安全責任等級分級辦法第 11 條規定，自行或委外開發之資通系統，包含工控系統(ICS)或運營科技(OT)類系統，均應依資通系統分級結果，依同辦法附表十所定資通系統防護基準執行控制措施，例如帳號管理、最小權限等。機關於針對工控系統(ICS)或運營科技(OT)類系統於執行附表十各項資安防護措施有窒礙難行且無替代措施時，應適時提報中央目的事業主管機關，俾其評估自訂該領域防護基準之可行性。

3、 依資通安全責任等級分級辦法資通系統防護基準規定，機關制訂之日誌管理政策，至少包含記錄時間週期、至少 6 個月之留存政策、管理或特權帳號執行紀錄及定期審查機制，且範圍應包含 IT、工控系統(ICS)及運營科技(OT)，及工控系統(ICS)或運營科技(OT)網路邊界之存取及傳輸紀錄。工控系統(ICS)及運營科技(OT)系統之日誌，並應包含特權帳號執行紀錄(如帳號異動等)、特定行為(如更改密碼、登入失敗等)，以及狀態值回傳紀錄。

伍、結語

資安法於 108 年施行，迄今已 5 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，協助政府機關持續熟悉法遵內容，逐步調修機關內部資安政策、管理制度及防護基準，提升各項法遵要求落實程度，期健全政府機關整體資安防護之韌性。

本部除將年度稽核共同發現事項及改善建議，函請全國各機關據以檢討調整資通安全維護計畫，並透過資通安全長會議或全國巡迴說明會加強宣導；亦定期透過本部資安署資通安全作業管考系統，追蹤受稽機關後續改善情形，適時給予輔導，俾協助受稽機關強化資安防護工作，持續精進資安防護水準。

資安防護不分中央及地方，本部除將地方行政機關資安專業人才納入行政院國家資通安全會報資安稽核團隊之觀察員機制中培訓，亦辦理政府機關資安知能及資安稽核相關教育訓練，期促進中央地方相互學習惕勵，本部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之深、廣度，協助機關發掘潛在之資安風險，以強化我國資安防護韌性。

附錄

112 年受稽機關、ISMS 驗證範圍列表

項次	受稽機關	ISMS 驗證範圍
1	衛生福利部臺中醫院	非全機關，驗證範圍如下：資訊中心提供辦公區域、電腦機房及核心資通系統
2	國立故宮博物院	非全機關，驗證範圍如下：核心資通系統
3	交通部民用航空局飛航服務總臺	非全機關，驗證範圍如下：核心資通系統
4	中央選舉委員會	非全機關，驗證範圍如下：核心資通系統、資訊安全管理活動及網路安全管理
5	文化部	非全機關，驗證範圍如下：核心資通系統及相關資料庫，網路服務及電腦機房
6	衛生福利部	非全機關，驗證範圍如下：核心資通系統、網路服務及其開發、操作、維護、網路管理及相關支援活動
7	衛生福利部桃園醫院	非全機關，驗證範圍如下：核心資通系統及資訊機房
8	國家發展委員會	非全機關，驗證範圍如下：核心資通系統、資訊安全管理活動及資訊機房
9	交通部中央氣象局氣象資訊中心	非全機關，驗證範圍如下：資通訊服務資訊安全管理，包含網路管理，機房維運，資通系統開發及維運
10	國家通訊傳播委員會	全機關驗證
11	國軍退除役官兵輔導委員會	非全機關，驗證範圍如下：政風處、統計資訊處(含機房)及核心業務資通訊系統
12	內政部警政署	非全機關，驗證範圍如下：核心資通系統及網路服務管理
13	高雄榮民總醫院	非全機關，驗證範圍如下：核心資通系統、資訊室及電腦機房
14	內政部消防署	非全機關，驗證範圍如下：核心資通系統及相關機房
15	臺中榮民總醫院	非全機關，驗證範圍如下：核心資通系統、資訊室及電腦機房
16	外交部	非全機關，驗證範圍如下：核心資通訊系統
17	外交部領事事務局	非全機關，驗證範圍如下：核心資通訊系統、官方網站、機房及資訊小組

項次	受稽機關	ISMS 驗證範圍
18	國立成功大學醫學院附設醫院	非全機關，驗證範圍如下：核心資通訊系統、資訊室之維護與管理
19	臺北榮民總醫院	非全機關，驗證範圍如下：資訊室、電腦機房、網路與核心資通系統
20	海洋委員會海巡署	非全機關，驗證範圍如下：通電資訊組之資通訊安全管理，核心資通訊系統及資訊機房
21	國立臺灣大學醫學院附設醫院	非全機關，驗證範圍如下：核心資通系統及網路服務管理
22	國家教育研究院教育制度及政策研究中心	非全機關，驗證範圍如下：辦公區域環境、資訊機房及資料庫系統(服務)運作與維護之安全管理
23	法務部	非全機關，驗證範圍如下：核心資通訊系統及網路服務管理
24	衛生福利部臺南醫院	非全機關，驗證範圍如下：資訊機房、核心資通訊系統