110年度公務機關資安稽核概況報告

行政院

中華民國 111 年 6 月

目 次

圖 目 次

表 目 次

壹、依據、策進及目的

資通安全管理法(以下稱資安法)於 108 年正式施行，本院依該法第 13 條第 1 項規定，稽核本院所屬或監督機關之資通安全維護計畫實施情形，並依同法第 5 條規定，公布「110 年度公務機關資安稽核概況報告」(以下稱本報告)，並送立法院備查。

本院資安稽核係邀請產官學研領域資安外部專家，協助共同檢視受稽機關法遵落實情形及整體防護作為，協助機關強化資安防護之完整性及有效性；110 年度並持續滾動調修稽核作業程序，除依當前資安情勢彙整稽核重點納入查核項目、事先廣泛蒐集機關資安業務辦況提供稽核委員現地審驗，並依機關資通安全責任等級(以下稱資安等級)適當分組辦理評比，期精進拓展稽核作業之深、廣度、有效性及達成評核公平性。

本報告彙整年度稽核整體辦理結果，研析受稽機關共同發現事項，並提供各級公務機關，俾利政府機關據以自我檢視及策進強化機關整體資安防護，以降低國家整體資安風險。

貳、110 年度資安稽核作業辦理情形

一、 受稽機關

(一) 遴選原則：本院所屬二級及獨立機關受稽核頻率為 2 年 1 次，110 年受稽機關為 109 年未受稽核之本院所屬二級及獨立機關。

(二) 110 年度受稽機關名單

COVID-19 疫情於 110 年提升為第三級警戒，配合防疫政策避免稽核作業人員群聚致升高感染風險，爰本院暫緩實施稽核作業；復於疫情警戒降級後，就原規劃之受稽機關中，優先擇選資安等級 A、B 級機關 11 家辦理稽核，餘資安等級 C 級機關 7 家延期至 111 年辦理。

本院並調查各受稽機關資訊安全管理系統(以下簡稱 ISMS)輔導及驗證廠商，各受稽機關 ISMS 驗證標準主要為 ISO/IEC 27001:2013，其中國軍退除役官兵輔導委員會、行政院主計總處及金融監督管理委員會等 3 個機關同時採用 CNS27001:2014 驗證標準，受稽機關、ISMS 輔導及驗證資訊如表 1：

表 1　110 年受稽機關、ISMS 輔導及驗證列表

項次	受稽機關	ISMS 輔導廠商	ISMS 驗證廠商	ISMS 驗證範圍
1	國軍退除役官兵輔導委員會	自行辦理	台灣檢驗科技股份有限公司(SGS)	非全機關，驗證範圍如下： 1. 統計資訊處 2. 政風處 3. 電腦機房(含資訊系統)
2	經濟部	安侯企業管理股份有限公司(KPMG)	台灣檢驗科技股份有限公司(SGS)	非全機關，驗證範圍如下： 經濟部核心資通系統及資訊中心所有資訊系統之開發、維運及機房管理等相關資通安全管理活動
3	法務部	昇達價值	英國標準協會	非全機關，驗證範圍如下：

項次	受稽機關	ISMS 輔導廠商	ISMS 驗證廠商	ISMS 驗證範圍
		管理股份有限公司	台灣分公司 (BSI)	法務部資訊處提供資訊系統之開發、操作及維護，資料安全管理、網路管理、機房管理與所有的支援性資訊處理活動及法務部本部使用者相關安全控制之監督及管理
4	外交部 (含台灣美國事務委員會)	安碁資訊股份有限公司	英國標準協會台灣分公司 (BSI)	非全機關，驗證範圍如下： 1. 資訊及電務處資安防護及資訊中心、資電處檔案管理組、資電處檔案史料科、資電處資安國際合作科、資電處資訊行政科、國際傳播司網宣小組、公眾外交協調會網路文宣科 2. 公文管理系統、電子表單系統、外交服務網、數位檔案管理系統、中華民國外交部全球資訊網、中華民國政府英文入口網站及資訊機房
5	衛生福利部	勤業眾信聯合會計師事務所 (Deloitte)	英國標準協會台灣分公司 (BSI)	非全機關，驗證範圍如下： 1. 資訊處提供的管理活動，如開發、操作、維護、網路管理及相關支援活動 2. 醫事憑證管理中心所提供之醫事憑證維運，包含系統開發、操作、維護、憑證申請、簽發、發布、廢止和儲存等程序 3. 全國醫療資訊網服務中心(SC)提供該中心資通系統有關的管理活動 4. 醫事司「戰情中心資訊系統(包含緊急醫療管理系統)」及「醫事管理系統」之開發、操作及維護 5. 心理及口腔健康司「精神照護資訊管理系統」、「毒品成

項次	受稽機關	ISMS 輔導廠商	ISMS 驗證廠商	ISMS 驗證範圍
				癮者單一窗口服務系統(含決策系統)」、「醫療機構替代治療作業管理系統」及「藥酒癮戒治個案管理系統」之開發、操作及維護 6. 保護服務司「保護資訊系統（含家庭暴力、性侵害暨兒童少年保護資訊系統、社會安全網-關懷e起來、家庭暴力高危機個案網絡會議作業平、家暴及性侵加害人處遇系統）」及「113保護專線系統」)之開發、操作及維護 7. 長期照顧司「長照失能個案照顧管理流程資訊系統」、「失智照護服務管理系統」、「長照2.0服務費用支付審核系統」及「長照機構暨長照人員相關管理資訊系統」之開發、操作及維護 8. 社會救助及社工司「衛生福利部全國社會福利津貼給付資料比對資訊系統」及「衛生福利部全國社會福利資源整合系統(弱勢e關懷)」之開發、操作及維護 9. 社會保險司「國民年金所得未達一定標準比對及審核管理資訊系統」之開發、操作及維護 10. 護理及健康照護司「空轉後送遠距會診平臺」及「護產人力暨機構管理資訊系統」之開發、操作及維護 11. 綜合規劃司「部長信箱」 12. 醫福會「醫療影像判讀中心系統」之開發、操作及維護

項次	受稽機關	ISMS 輔導廠商	ISMS 驗證廠商	ISMS 驗證範圍
6	文化部	策略數位服務有限公司(SDS)	台灣檢驗科技股份有限公司(SGS)	非全機關，驗證範圍如下： 資通系統防護需求等級為高之資通系統及其相關資料庫、網路、及新莊、永和國光電腦機房
7	內政部	安侯企業管理股份有限公司(KPMG)	英國標準協會台灣分公司(BSI)	非全機關，驗證範圍如下： 1. 資訊中心提供全球資訊網、臺灣行動身分識別(Taiwan FidO)之開發、運作與維護，公文電子交換系統之運作與維護，機房管理及網路基礎設施之支援活動 2. 資訊中心提供本部憑證管理中心之開發、運作與維護，包括機房管理及網路基礎設施之支援活動，但不包括憑證註冊窗口、卡管中心及客服中心等相關作業 3. 地政司地政資訊作業科提供地政資訊核心系統之開發、運作與維護，包括地政資訊網際網路服務作業、全國土地基本資料庫同步異動機制、不動產實價登錄系統、不動產實價交易查詢系統、地籍總歸戶系統，以及機房管理及網路基礎設施之支援活動 4. 資訊中心戶役政資訊科提供戶役政資訊系統之開發、運作與維護，機房管理及網路基礎設施之支援活動 5. 資訊中心和戶政司之實體環境與個人電腦管理 6. 本部內政資料中心東七與文心及防管理及網路基礎設施之支援活動

項次	受稽機關	ISMS 輔導廠商	ISMS 驗證廠商	ISMS 驗證範圍
8	行政院主計總處	安侯企業管理股份有限公司(KPMG)	台灣檢驗科技股份有限公司(SGS)	非全機關，驗證範圍如下： 1. 廣博大樓 2. 行政院區 3. 主計人員訓練中心 4. 中部辦公園區、地方統計推展中心
9	金融監督管理委員會	自行辦理，內稽及個資(資訊資產)盤點作業另有委外案支援辦理。	英國標準協會台灣分公司(BSI)	全機關驗證
10	行政院農業委員會	資拓宏宇國際股份有限公司	英國標準協會台灣分公司(BSI)	全機關驗證
11	科技部	安侯企業管理股份有限公司(KPMG)	台灣檢驗科技股份有限公司(SGS)	非全機關，驗證範圍如下： 科技部資訊處所負責之骨幹網路維運管理、資訊機房（包含台北機房及台中共構機房）之實體環境安全以及所有資通系統之開發、維運與管理。

二、 稽核分組及稽核方式

考量稽核標準，爰將受稽機關依資安等級進行分組並採不同之稽核方式(如表 2)。

表 2　稽核分組及稽核方式

稽核分組		1	2
分組標準		資安等級 A 級	資安等級 B 級
家數		5	6
稽核方式	技術檢測	V	--
	實地稽核	V	V

第 1 分組於實地稽核前先辦理技術檢測，主要係針對受稽機關之核心資通系統、資料庫及使用者電腦等進行弱點檢測，為期 3 個工作日；另第 1、2 分組均辦理實地稽核，由本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。

三、 稽核日期

110 年度各受稽機關實地稽核日期如表 3。

表 3　110 年各受稽機關稽核日期

編號	受稽機關	實地稽核日期
1	國軍退除役官兵輔導委員會	9 月 3 日
2	經濟部	9 月 8 日
3	法務部	9 月 14 日
4	外交部(含台灣美國事務委員會)	9 月 17 日
5	衛生福利部	10 月 7 日
6	文化部	10 月 13 日
7	內政部	10 月 26 日
8	行政院主計總處	11 月 2 日
9	金融監督管理委員會	11 月 4 日
10	行政院農業委員會	11 月 10 日
11	科技部	12 月 10 日

四、 稽核團隊

本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：由本院國家資通安全會報副召集人或協同副召集人擔任。

(二) 稽核委員：

1、 遴選標準

(1) 由本院考量稽核需求，邀請具備資通安全政策、管理、技術、法律或具實務專業之公務機關代表或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三分之一。

(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，應提早通知本院並主動迴避。

2、 分配原則

每個稽核場次以安排 7 位稽核委員為原則，包括策略面 2 位、管理面 2 位及技術面 3 位。

(三) 技術檢測人員：由本院國家資通安全會報技術服務中心專業檢測同仁擔任，每場次技術檢測人員以 9 名為原則。

(四) 觀察員：自總統府與中央一級機關含直屬機關、直轄市政府及所屬一級機關之公務人員遴選，每場次至多 2 名觀察員；惟 110 年本院配合中央防疫政策減少人員群聚，爰觀察員制度暫緩實施。

五、 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(106 年至 109 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 20000：2018 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，各檢測項目與配分如表 4，本項作業重點在檢驗機關資安設定及安全性更新之落實度。

表 4　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	網路惡意活動檢視	惡意中繼站連線阻擋檢測	5
3	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
4	網路架構檢測	網路架構檢測	10
5	網域主機安全防護檢測	網域主機安全防護檢測	5
6	物聯網設備檢測	網路攝影機檢測	10
		門禁設備檢測	
		網路印表機檢測	
		無線網路基地台/無線路由器檢測	
		環控系統檢測	
7	組態設定安全檢測	作業系統組態檢測	15

		瀏覽器組態檢測	
		網通設備組態檢測	
		應用程式組態檢測	
8	資料庫安全檢測	資料庫安全檢測	10

2、 第 2 階段：實地稽核

實地稽核分策略面、管理面及技術面等 3 個構面，共 11 個稽核項目，各構面之稽核項目與配分如表 5。

表 5　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
	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

3、 評分方式

(1) 第 1 分組

整體總成績=技術檢測得分×30%＋實地稽核得分×70%。

(2) 第 2 分組

整體總成績=實地稽核得分×100%。

參、110 年稽核結果

各受稽機關之稽核結果，第 1 分組總分平均為 78.21 分，其中技術檢測平均分數為 80.2 分，實地稽核平均分數為 77.36 分；第 2 分組總分平均為 73.5 分。

一、 技術檢測

第 1 分組受測計 5 個公務機關，技術檢測分數達 75 分以上者有 4 個機關，僅 1 個機關得分為 71 分，主因係該機關網段間未配置適當之存取控制機制、物聯網設備仍使用預設密碼及抽測之使用者電腦瀏覽器未設定安全組態等，受測機關之技術檢測成績分布如圖 1。

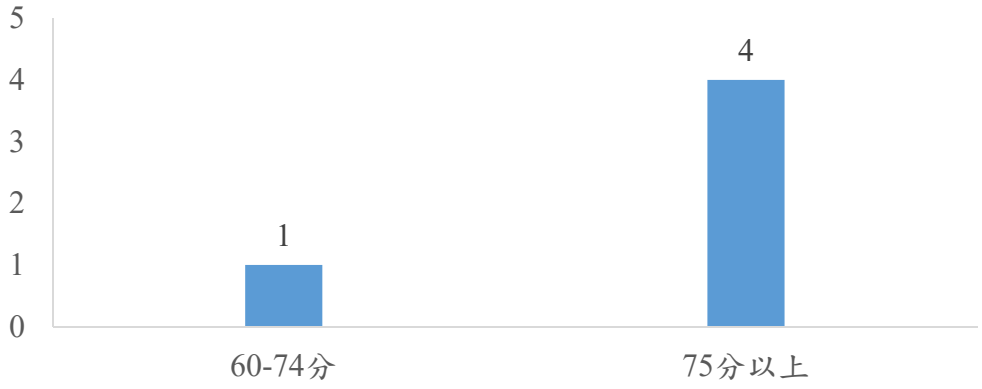

圖 1　技術檢測成績分布

技術檢測個別項目成績，詳見圖 2，其中「網路惡意活動檢視」、「核心資通系統安全檢測」、「網域主機安全防護檢測」、「物聯網設備檢測」及「組態設定安全檢測」等 5 項表現良好，達 75 分以上水準，惟「網路架構檢測」1 項未達 70 分，經統計發現較多機關存在網路設備、網路網段存取控制設計不良、未完整建立實地備援機制及未限制非加密資料傳輸協定等風險弱點。

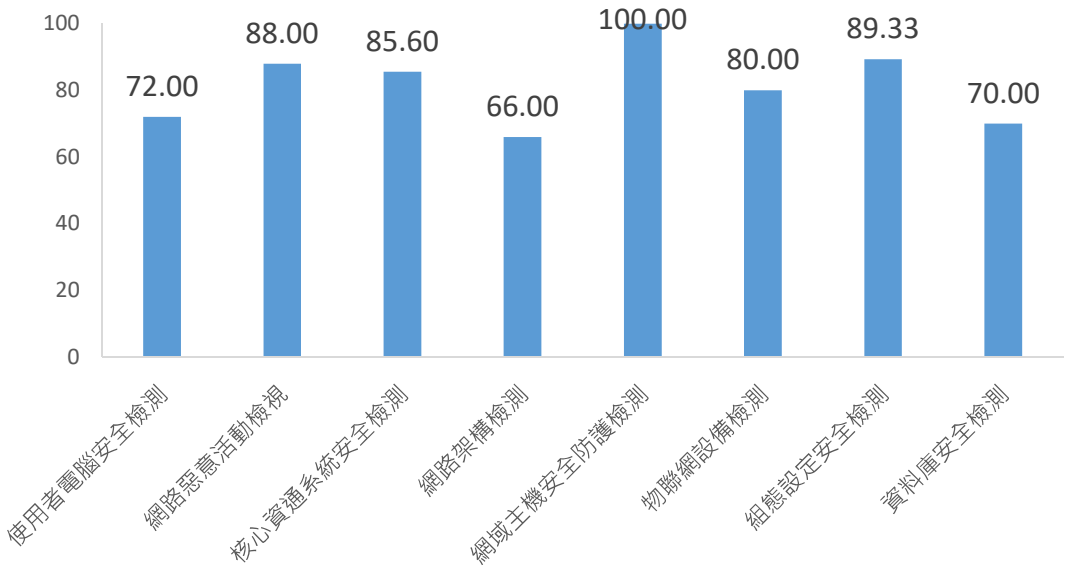

圖 2　技術檢測個別項目成績分布

二、 實地稽核

第 1 分組、第 2 分組實地稽核計 11 個公務機關，稽核結果總分平均為 75.25 分，成績逾 75 分(含)以上者有 7 個機關，4 個機關成績未達 75 分，主要問題點為資通安全維護計畫實施情形填報內容與執行情形有不一致情形(如機關資訊資產盤點未落實等)、委外服務契約未納入資通安全管理法相關法遵要求、系統風險評鑑及處理機制不妥適、資安健診或資安事件發現的風險漏洞及問題未改善追蹤，及未依資安事件通報及應變程序落實執行等，整體受稽機關成績分布，詳見圖 3。

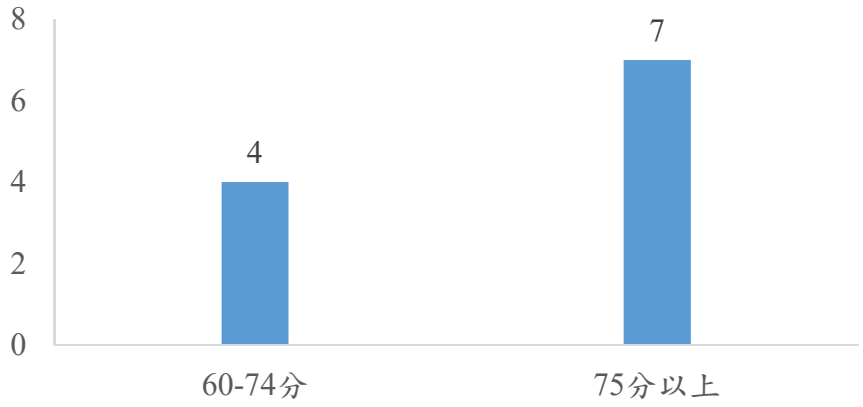

圖 3　實地稽核成績分布

經檢視實地稽核個別項目成績分布，詳見圖 4，其策略面、管理面、技術面在整體表現平均，其中「資通安全防護及控制措施」表現最好；「核心業務及其重要性」成績最低，顯示仍有多數機關未能有效界定並落實盤點核心業務及核心資通系統，有待持續調整改善。

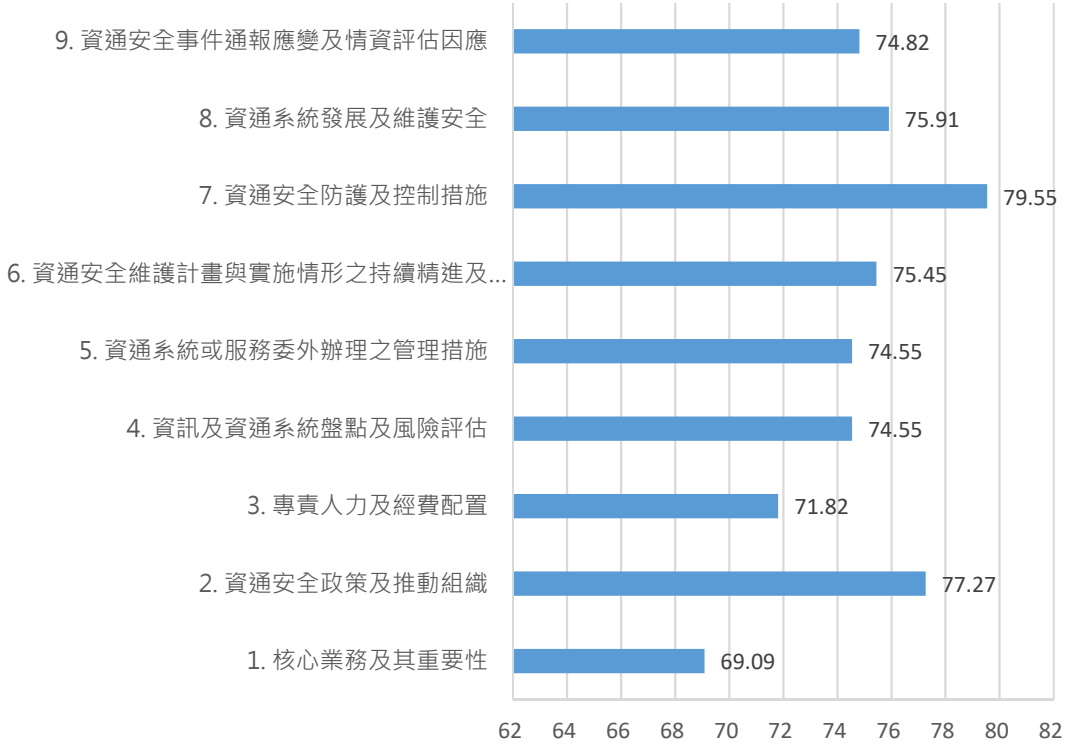

圖 4　實地稽核個別項目成績分布

三、 資安等級 A 級及 B 級實地稽核成績比較

110 年已先將受稽機關依資安等級分組，第 1 分組為資安等級 A 級機關、第 2 分組為資安等級 B 級機關，比較 2 組實地稽核成績結果，顯示第 1 分組整體表現優第 2 分組，可見資安等級 A 級機關對資安防護之落實度及資源投入相對提升，各分組成績分布說明如下：

(一) 第 1 分組

本年第 1 分組受稽機關計有 5 個，實地稽核整體平均分數為 77.36 分，其中整體評分 75 分以上有 4 個機關，僅 1 個機關評分 71 分，成績分布，詳見圖 5。

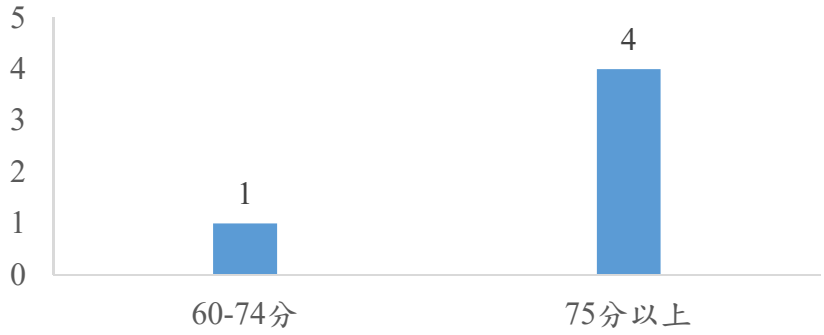

圖 5　第 1 分組實地稽核整體成績

(二) 第 2 分組

本年第 2 分組受稽機關計有 6 個，整體平均分數 73.5 分，其中 75 分以上有 3 個機關，其餘 3 個機關雖未達 75 分惟成績均有 60 分以上，詳見圖 6。

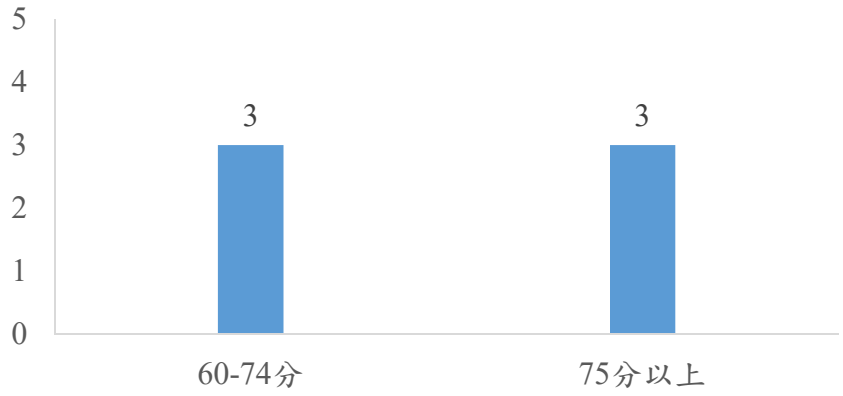

圖 6　第 2 分組實地稽核整體成績

(三) 實地稽核構面成績比較

綜合分析實地稽核各構面(策略面、管理面及技術面)之表現情形，第 1 分組在各構面明顯優於第 2 分組，且第 1 分組各構面平均分數皆達 74 分以上，普遍表現良好，實地稽核各構面成績分布，

詳見圖 7。

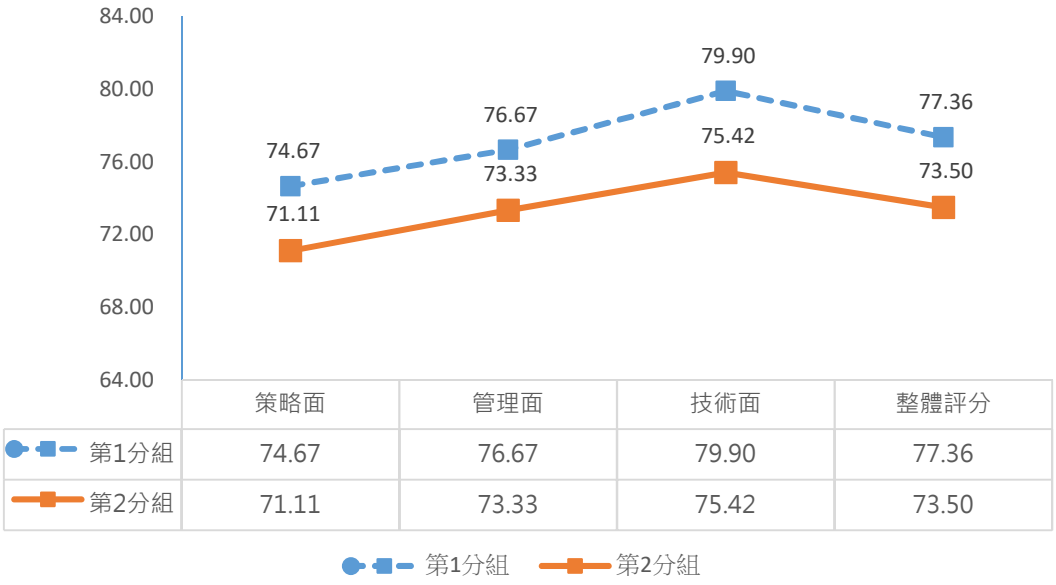

圖 7　分組各面向成績分布

四、 110 年與 109 年實地稽核成績比較

資通安全管理法於 108 年正式施行，各機關施行首年尚在調整機關資安防護相關規範以符合法遵內容，自 109 年起持續建立與法遵要求一致之制度及模式，以 110 年實地稽核結果成績與 109 年進行比較，可以發現機關已持續投入相關資源，逐步落實並達成法遵要求。

(一) 實地稽核構面比較

綜合分析 110 年及 109 年受稽機關實地稽核各構面(策略面、管理面及技術面)之表現情形，110 年受稽機關在各構面明顯優於 109 年，且 110 年受稽機關在各構面平均分數皆達 72 分以上，表現良好，實地稽核各構面 2 年度成績分布，詳見圖 8。

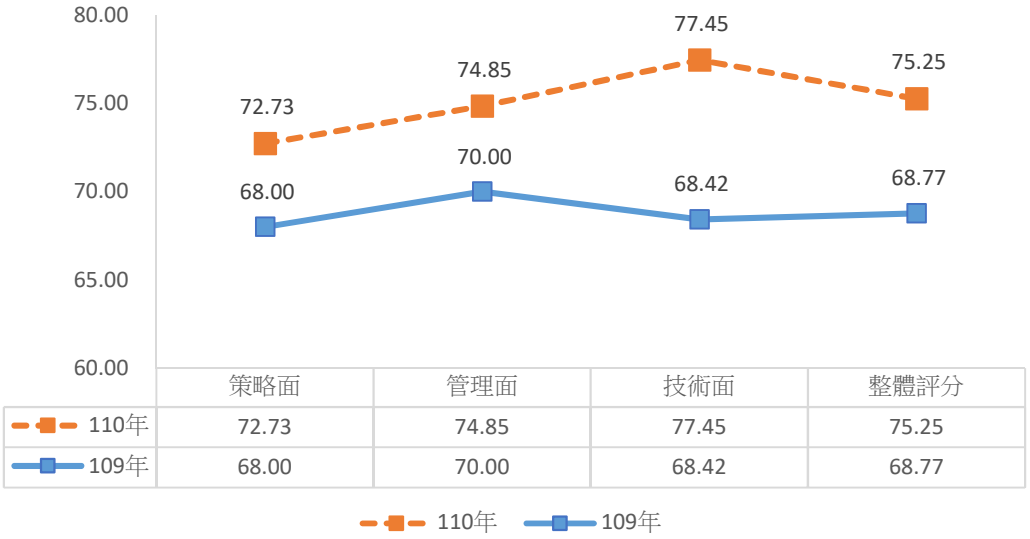

圖 8　110、109 年實地稽核各面向成績分布

(二) 實地稽核項目比較

另分析 110 年及 109 年受稽機關實地稽核個別項目成績分布，110 年受稽機關在所有稽核項目成績均較 109 年為佳，詳見圖 9；其中「資通安全防護及控制措施」進步幅度較大，「資通系統或服務委外辦理之管理措施」進步幅度較小，仍待持續推動強化，詳見圖 10。

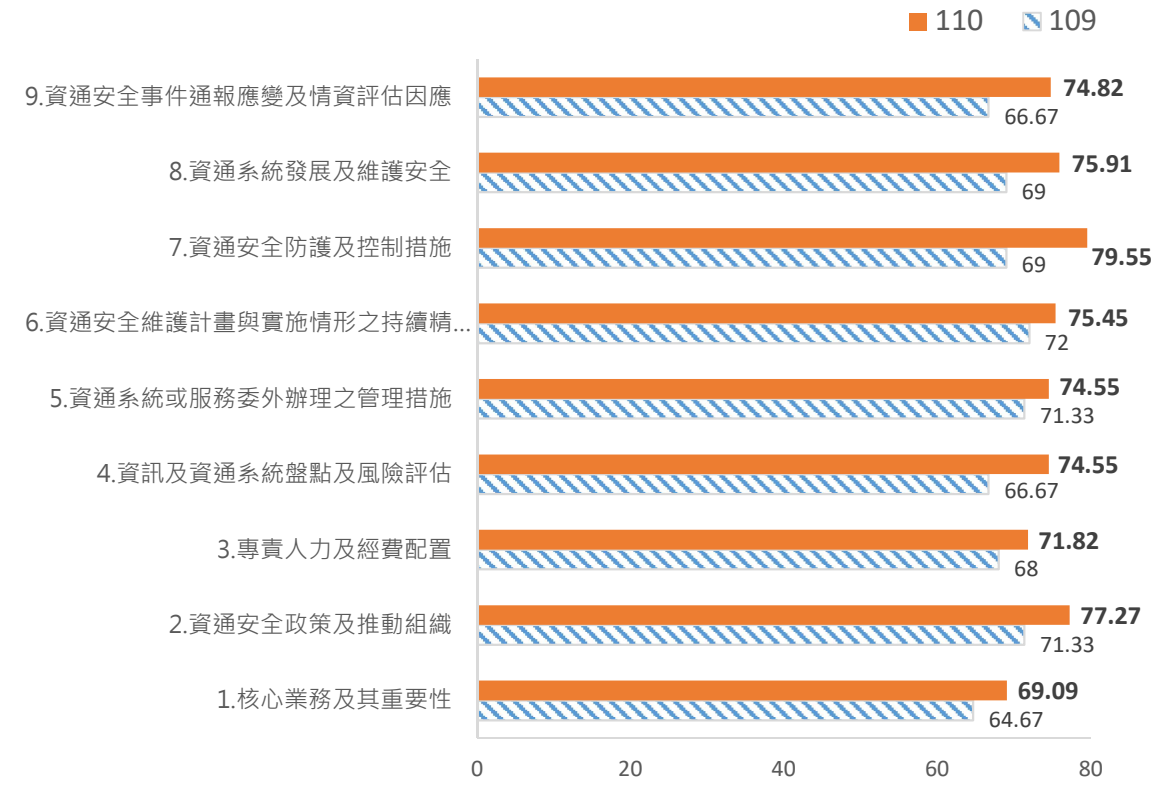

圖 9　110、109 年實地稽核個別項目成績分布

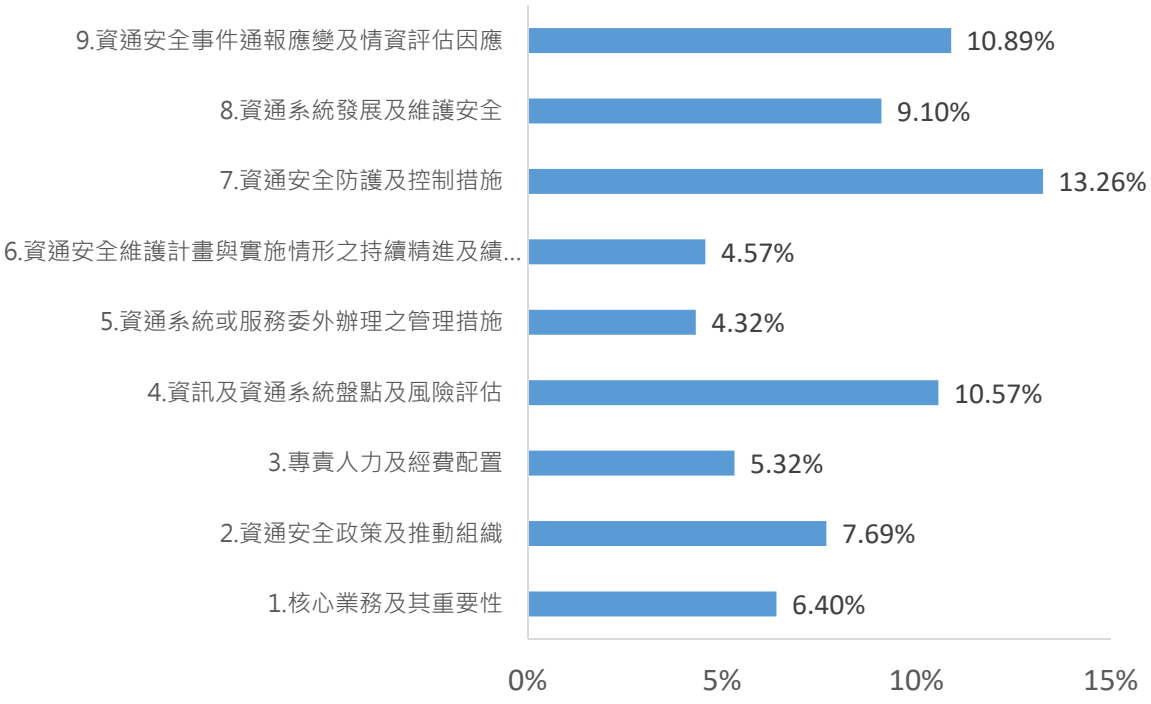

圖 10　110 年較 109 年實地稽核個別項目成績進步比例

肆、 稽核共同發現

綜整 110 年之稽核發現，依法遵符合情形與待改善事項，以策略面、管理面及技術面分別說明。

一、 法遵符合情形

(一) 策略面

1、 已完成核心資通系統 ISMS 導入，並通過公正第三方驗證。

2、 已成立資通安全推動組織，並設置機關資安長職務，負責推動、協調監督與審查資通安全管理相關事務，顯示管理階層對於 ISMS 建立、實作、維持及持續改善之承諾及支持。

3、 已訂定機關人員辦理業務涉及資通安全事項之考核機制及獎懲基準，並適時提供獎勵。

(二) 管理面

1、 針對資通系統委外開發事宜，訂定機關委外作業安全管理規範並要求各單位落實執行。

2、 已訂定內部資通安全稽核計畫，定期辦理實地稽核並針對所發現疏失進行複查。

3、 定期針對所屬或監督公務機關辦理社交工程演練與資安事件通報及應變演練。

(三) 技術面

1、 已定期辦理資通系統網站安全弱點檢測、滲透測試及資通安全健診等作業。

2、 已依法建置資通安全威脅管理、資通安全弱點通報等機制。

3、 已依法訂定資安事件通報作業規範，據以執行資通安全事件通報等作業。

二、 待改善事項

(一) 策略面

1、 未依資安法施行細則第 7 條規定，有效落實核心業務及核心資通系統之界定，部分機關資通安全維護計畫及實施情形填報內容有所差異，且未以客觀與量化衡量指標評估系統防護需求等級。

2、 依資安法施行細則第 6 條規定，雖已成立資通安全組織，負責推動、協調、監督及審查資通安全管理事項，惟召開管審會議時，常有委員係代理出席，難彰顯管理階層之支持及重視。

3、 依資安法施行細則第 6 條規定，部分機關資通安全目標之量測指標仍納入資安事件發生次數，未考量合宜性。

(二) 管理面

1、 未落實資安法施行細則第 4 條規定，資訊服務委外作業未於合約或建議書徵求文件明確規範防護基準需求，如委外廠商選任要求、防護基準納入建議書徵求文件、安全性檢測及通報程序等。

2、 依資安法施行細則第 6 條規定，已辦理資訊資產盤點作業，惟盤點範圍與內容完整性不足。

3、 未落實資安法施行細則第 4 條規定，部分機關辦理委外廠商稽核作業無記錄相關查核證據，且無追蹤管考機制。

4、 依資通安全責任等級分級辦法應辦事項規定，部分機關已規劃執行內部資通安全稽核作業，惟稽核計畫內容不完整。

(三) 技術面

1、 依資通安全責任等級分級辦法應辦事項規定，已進行資通系統安全性檢測、滲透測試及資通安全健診等作業，惟後續修補作業未落實執行，且無訂定相關作業程序進行後續追蹤。

2、 依資通安全責任等級分級辦法防護基準規定，雖已訂定資通系統開發、測試、變更及上線等相關程序，惟其內容未臻完善，且未完整保留資通系統之版本更新過程與紀錄，另系統分析與設計文件未及時更新與納管。

3、 依資通安全責任等級分級辦法防護基準規定，針對資通系統所使用之外部元件或軟體，缺乏明確管理規範。

三、 改善建議

(一) 策略面

1、 應依資安法施行細則第 7 條規定，明確界定應保護之標的且依不同安全等級之資通系統施予安全控制措施，其中相關作業包括界定機關核心業務，盤點各單位之資通系統，包括業務營運之資通系統、輔助系統等；再者以支持核心業務持續運作必要之系統，及資通系統防護需求等級為高者，皆應列為機關之核心資通系統。

2、 依資安法施行細則第 6 條規定，應設置資通安全推動組織，推動資通安全相關政策、落實資通安全事件通報及相關應變處理，建議組織成員親自參與，避免代理出席會議，以顯示管理階層對資安作業之重視與支持。

3、 依資安法施行細則第 6 條規定，應制定資通安全政策、目標，其中資通安全目標宜有量化型與質化型指標，量化型指標應考量合宜性，勿納入資安事件發生次數。

(二) 管理面

1、 依資安法施行細則第 4 條規定，對於委外作業安全應建立相關管理程序，從廠商選擇(技術與能力要求)、服務水平、安全控制措施(包括保密、處理人員之管理)及廠商績效監控(稽核)與報告機制等，皆應明確制訂於管理程序，並落實於與廠商之合約規範中。

2、 依資安法施行細則第 6 條規定，建議機關完整盤點全機關資通系統及資訊，並明確標示核心資通系統及相關資產。

3、 依資安法施行細則第 4 條規定，委託機關應落實定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形；並應注重稽核作業之有效性，如完整記錄查核證據，並訂定機制落實對稽核結果之追蹤管考。

4、 依資通安全責任等級分級辦法應辦事項規定，對於資通安全內部稽核作業，應注意稽核頻率、時程、準則、檢核項目、方式、範圍等是否合適，如範圍是否涵蓋全機關、稽核項目是否完整納入資安法法遵事項，及內部稽核發現事項之改善追蹤情形。

(三) 技術面

1、 依資通安全責任等級分級辦法應辦事項規定，應針對核心資通系統定期進行弱點掃描、系統滲透測試，並追蹤檢測結果

修補情形，以確保機關之安全防護確實。

2、 依資通安全責任等級分級辦法防護基準規定，應完整訂定、儲存與管理系統發展生命週期有關文件。

3、 依資通安全責任等級分級辦法防護基準規定，針對資通系統所使用之外部元件或軟體，應建立系統化管理機制，並納入驗收程序；另針對外部元件或軟體之安全性漏洞通告，應落實評估更新，於資通系統環境中之相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。

伍、 結語

資通安全管理法於 108 年施行，本院依法並透過第二方資通安全稽核作業，協助各機關檢視並落實法遵事項以強化資安防護之完整性及有效性，期達成政府機關整體資訊安全。

資安防護如同防疫，不分中央及地方，本院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並納入資通安全維護計畫，並透過資通安全長會議或全國巡迴說明會加強宣導外，亦規劃辦理政府機關稽核作業相關教育訓練，及將地方政府資安專業人才納入本院稽核團隊之觀察員機制中培訓，期能中央地方相互學習惕勵，提升資安作業聯合防禦，以降低資安威脅可能造成的危害及損失。

資通安全管理法施行迄今已 3 年餘，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，落實對應之各項法遵要求，經本院比較近 2 年受稽機關實地稽核成績，顯示機關持續提升對法遵作業的落實度；本院將檢視機關辦理情形，持續精進資安稽核作業之深、廣度，並彙整分析近年重大資安事件根因及資安威脅情勢，滾動調修稽核項目及稽核重點，深入檢視機關面對資安威脅之因應機制，協助機關找出自身整體防護盲點，以持續精進並有效管理資安風險。