111 年度公務機關資安稽核概況報告

數位發展部

中華民國 112 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，行政院依該法第 13 條第 1 項規定，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，本部於 111 年 8 月 27 日成立，賡續執行行政院資通安全稽核，並依同法第 5 條規定，公布「111 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。

行政院資安稽核係邀請產官學研領域資安外部專家，協助共同以抽檢方式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，並將法遵事項依屬性，透過 8 大項技術檢測(使用者電腦安全檢測、物聯網設備檢測、網域主機安全防護、資料庫安全、核心資通系統安全、網路架構檢測、組態設定安全檢測及網路惡意活動檢視)，以及策略、管理及技術等 3 項構面進行實地稽核作業，發掘機關可能的資安風險，協助機關強化資安防護之完整性及有效性；111 年度並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，事先廣泛蒐集機關各項資安業務辦況，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 111 年度資安稽核整體辦理結果，研析受稽機關共同發現事項供各機關參考，俾利政府機關據以自我檢視，以持續策進強化機關整體資安防護韌性，以降低國家整體資安風險。

貳、111 年度資安稽核作業辦理情形

一、 受稽機關

(一) 遴選原則：行政院所屬二級及獨立機關受稽核頻率為 2 年 1 次，111 年受稽機關為 109 年受稽核之行政院所屬二級及獨立機關，並將另依 109、110 年稽核結果等整體考量分配調整。

(二) 111 年度受稽機關名單

行政院所屬二級及獨立機關依 111 年資通安全稽核計畫奉准，規劃前揭機關受稽核頻率為 2 年 1 次，爰 111 年受稽核機關原則為 109 年受稽核之行政院所屬二級及獨立機關，另納入原定於 110 年辦理稽核之受稽機關，受 COVID-19 疫情影響延期至 111 年辦理者。

本部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，其中行政院環境保護署係採用 CNS27001:2014 驗證標準，受稽機關、ISMS 輔導及驗證資訊如表 1：

表 1　111 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	客家委員會	安碁資訊股份有限公司	台灣檢驗科技股份有限公司(SGS)	全機關驗證
2	行政院原子能委員會	安侯企業管理股份有限公司	英國標準協會台灣分公司(BSI)	非全機關，驗證範圍如下：核子事故緊急應變工作平台、輻射源進出口簽審通關系統
3	國家運輸安全調查委員會	規劃導入中	規劃導入中	規劃導入中
4	海洋委員	創逸科技服	台灣檢驗科	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
	會	務有限公司	技股份有限公司(SGS)	1. 全球資訊網及資訊機房之安全維運
5	公平交易委員會	漢昕科技股份有限公司	台灣德國北德技術監護顧問股份有限公司(TUV NORD)	非全機關，驗證範圍如下： 1. 主機房及東七機房、結合申報暨聯合行為申請線上填報系統、產業資料整合系統、多層次傳銷管理系統維運與管理。
6	不當黨產處理委員會	規劃導入中	規劃導入中	規劃導入中
7	行政院人事行政總處	資拓宏宇國際股份有限公司	英國標準協會台灣分公司(BSI)	非全機關，驗證範圍如下： 機關資訊處，提供所有業務與資通系統(包含核心系統)的開發，操作及維護，以及機房、網路架構、客戶服務及其他資訊處理活動的管理
8	大陸委員會	關貿網路股份有限公司	英國標準協會台灣分公司(BSI)	非全機關，驗證範圍如下： 1. 由資訊室提供所有資訊系統之系統開發、操作及維運，包含全球資訊網管理系統，網路骨幹、機房及相關支援性資訊處理活動
9	中央銀行	自行導入	台灣檢驗科技股份有限公司(SGS)	非全機關，驗證範圍如下： 全部核心資通系統
10	財政部財政資訊中心	安侯企業管理股份有限公司	英國標準協會台灣分公司(BSI)	全機關，驗證範圍如下： 1.財政資訊中心所有業務活動包含資訊系統開發、維護及操作和相關支援資訊處理流程 2.財政部財政資訊中心支援服務室提供公文系統的開發維護及操作和相關支援資訊處理流程 3.五地區國稅局徵收及資訊

項次	受稽機關	ISMS 輔導廠商	ISMS 驗證廠商	ISMS 驗證範圍
				組所提供的國稅系統服務的維護及操作 4.財政部財政資訊中心支援服務室提供財政部電子公文統合交換中心系統的維護及操作和相關支援資訊處理流程
11	教育部	華電聯網股份有限公司	台灣檢驗科技股份有限公司(SGS)	全機關驗證
12	原住民族委員會	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：核心系統：公文系統、全球資訊網，以及本會資訊機房
13	行政院公共工程委員會	資拓宏宇股份有限公司	英國標準協會台灣分公司(BSI)	非全機關，驗證範圍如下：全部核心資通系統
14	勞動部	安侯企業管理股份有限公司	英國標準協會台灣分公司(BSI)	全機關及勞動資料科學中心
15	僑務委員會	昇達價值管理股份有限公司	台灣德國萊因技術監護顧問股份有限公司(TUV)	非全機關，驗證範圍如下：資訊室提供所有資訊系統之系統開發、操作及軟硬體之維運
16	行政院環境保護署	安碁資訊股份有限公司	台灣檢驗科技股份有限公司(SGS)	非全機關，驗證範圍如下：環境保護許可管理資訊系統及資源回收管理資訊系統之開發:操作與維護，以及網路及機房之管理
17	交通部	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：電子公文交換中心

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	3
分組標準		資安等級 A 級	資安等級 B 級	資安等級 C 級
家數		6	5	6
稽核方式	技術檢測	V	--	--
	實地稽核	V	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、3 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。

三、 稽核日期

111 年度各受稽機關實地稽核日期如表 3。

表 3　111 年各受稽機關稽核日期

編號	受稽機關	實地稽核日期
1	客家委員會	7 月 6 日
2	行政院原子能委員會	7 月 12 日
3	國家運輸安全調查委員會	7 月 18 日
4	海洋委員會	8 月 3 日
5	公平交易委員會	8 月 12 日
6	不當黨產處理委員會	8 月 17 日
7	行政院人事行政總處	8 月 25 日
8	大陸委員會	9 月 6 日
9	中央銀行	9 月 14 日
10	財政部財政資訊中心	9 月 22 日

編號	受稽機關	實地稽核日期
11	教育部	9 月 30 日
12	原住民族委員會	10 月 20 日
13	行政院公共工程委員會	11 月 2 日
14	勞動部	11 月 8 日
15	僑務委員會	11 月 16 日
16	行政院環境保護署	12 月 7 日
17	交通部	12 月 13 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：

由行政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) 由行政院考量稽核需求，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，應提早通知行政院並主動迴避。

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：由原行政院國家資通安全會報技術服務中心專業檢測同仁擔任。

(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。

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(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 20000：2018 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

項次	檢測項目	檢測子項	配分
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	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	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	試行不計分

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 9 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

構面	稽核項目	配分
	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、第 3 分組

整體總成績=實地稽核得分×100%。

參、 111 年稽核結果

各受稽機關之稽核結果，第 1 分組總分平均為 74.76 分，其中技術檢測平均分數為 77.83 分，實地稽核平均分數為 73.44 分；第 2 分組總分平均為 70.70 分；第 3 分組總分平均為 64.33 分。

一、 技術檢測

第 1 分組受測計 6 個公務機關，技術檢測分數達 75 分以上者有 3 個機關，僅 1 個機關得分為 66 分，主因係該機關對主機未配置適當之存取控制機制、主機仍存在高風險弱點，以及防火牆未設定適當規則等，受測機關之技術檢測成績分布如圖 1。

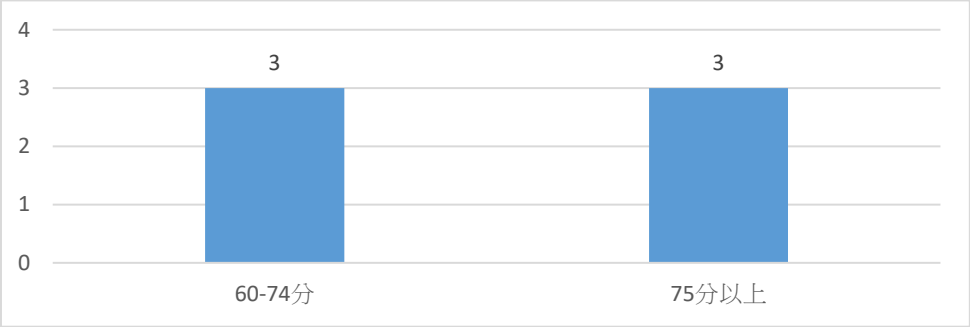

圖 1　技術檢測成績分布

技術檢測個別項目成績(詳見圖 2)，其中「物聯網設備檢測」、「網域主機安全防護檢測」、「資料庫安全檢測」、「組態設定安全檢測」及「網路惡意活動檢視」等 5 項表現較佳，達 75 分以上水準，惟在「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。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、及未限制非加密資料傳輸協定等風險弱點。

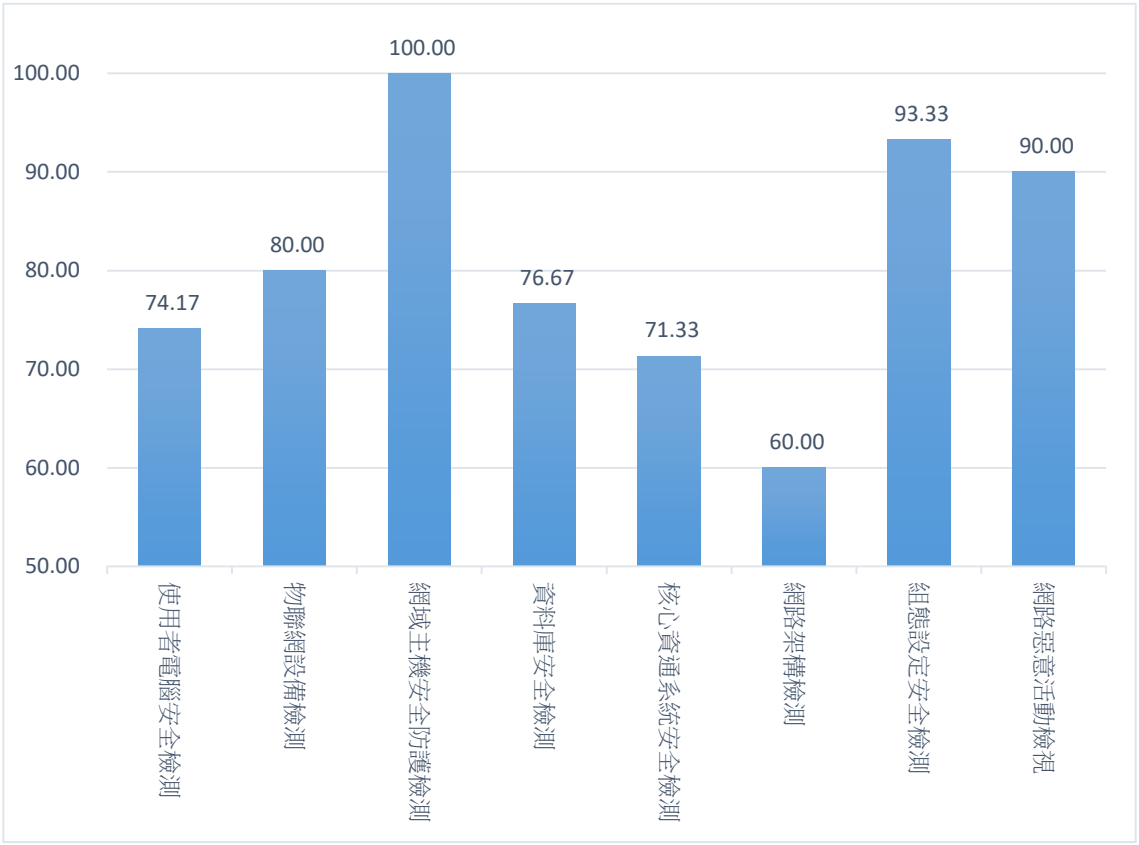

圖 2　技術檢測個別項目成績分布

二、 實地稽核

第 1 分組、第 2 分組及第 3 分組實地稽核計 17 個公務機關，稽核結果總分平均為 69.89 分，成績達 75 分(含)以上者有 5 個機關，12 個機關成績未達 75 分，主要問題點為未落實資訊資產盤點、委外服務契約未納入資通安全管理法相關法遵要求或未落實執行、系統風險評鑑及處理機制不妥適、未就資安健診或資安事件發現的風險漏洞及問題有改善追蹤機制，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。

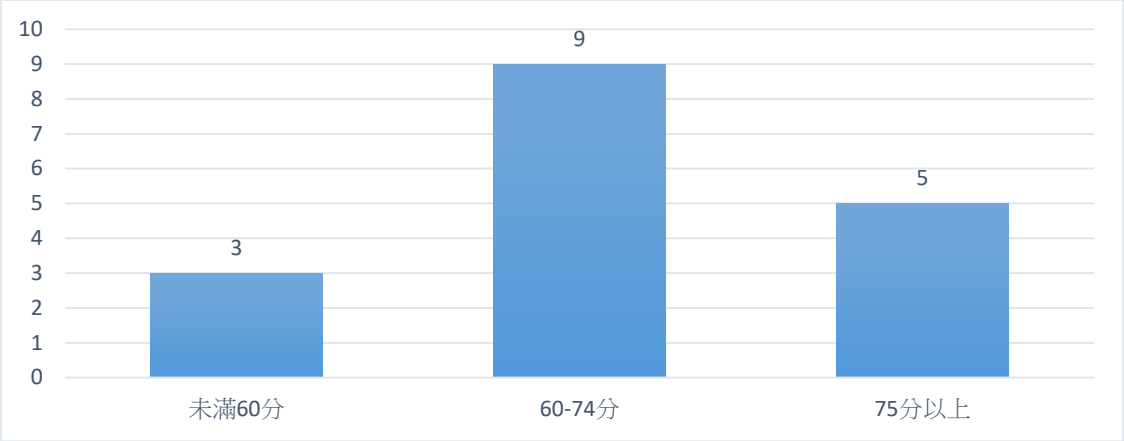

圖 3　實地稽核成績分布

經檢視實地稽核個別項目成績分布，詳見圖 4，其策略面、管理面、技術面在整體表現平均，其中「資通安全政策及推動組織」表現最好；「資訊及資通系統盤點及風險評估」成績最低，顯示仍有多數機關在界定並落實盤點核心業務及核心資通系統，尚待持續調整改善。

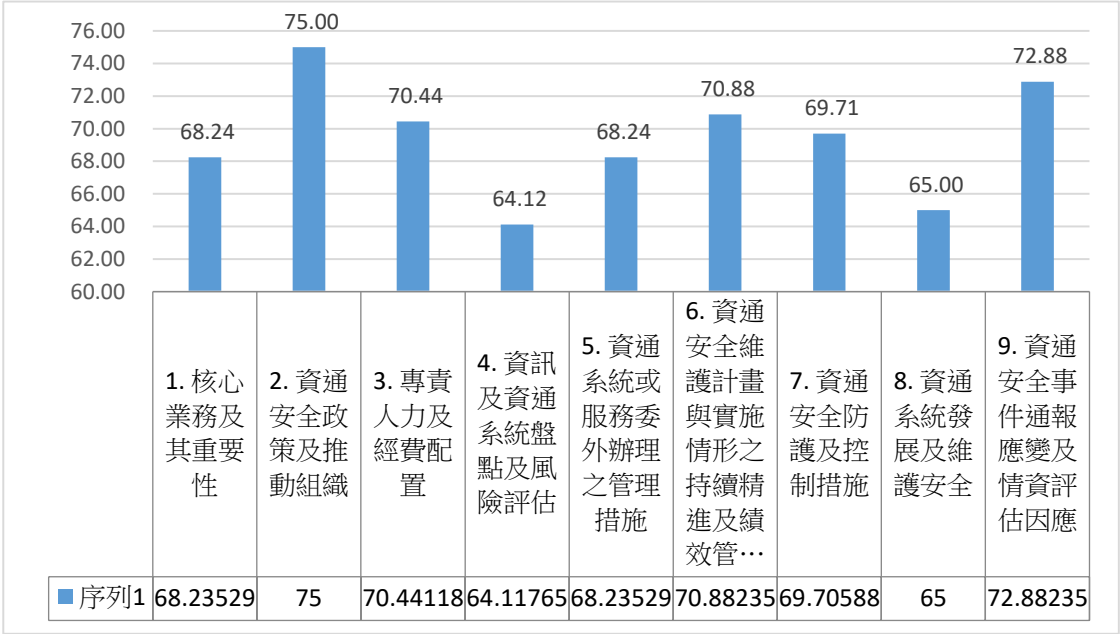

圖 4　實地稽核個別項目成績分布

三、 資安等級 A 級、B 級及 C 級實地稽核成績比較

111 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，第 3 分組為資安等級 C 級機

關。比較 3 組實地稽核成績結果，顯示第 1 分組整體表現優於第 2 分組及第 3 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 6 個，實地稽核整體平均分數為 74.75 分，其中整體評分 75 分以上有 3 個機關，其餘 3 個機關雖未達 75 分，但成績均有 60 分以上，成績分布，詳見圖 5。

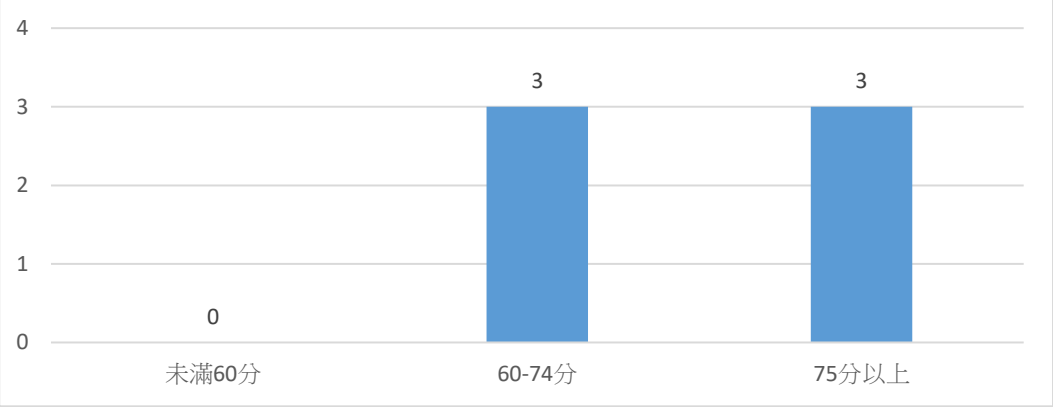

圖 5　第 1 分組實地稽核成績分布

(二) 第 2 分組

本年第 2 分組受稽機關計有 5 個，整體平均分數 70.70 分，其中 75 分以上有 1 個機關，其餘 4 個機關雖未達 75 分，但成績均有 60 分以上，詳見圖 6。

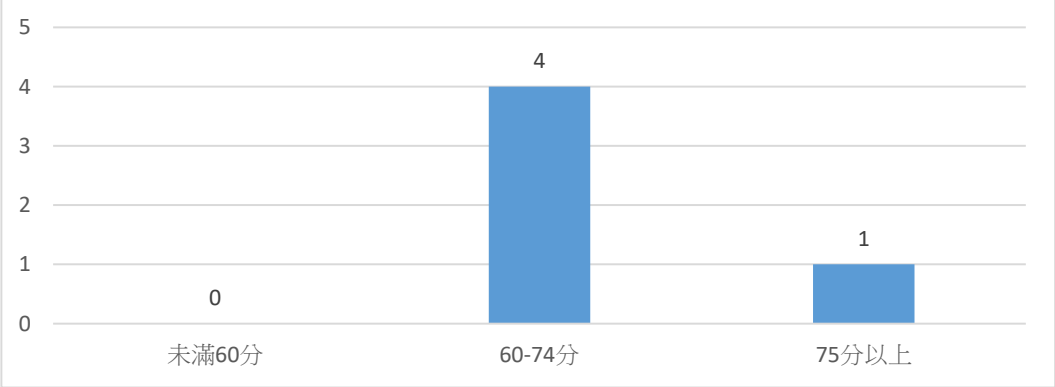

圖 6　第 2 分組實地稽核成績分布

(三) 第 3 分組

本年第 3 分組受稽機關計有 6 個，整體平均分數 64.33 分，其中 75 分以上有 1 個機關，其餘 5 個機關未達 75 分(2 個未滿 60 分)詳見圖 7。

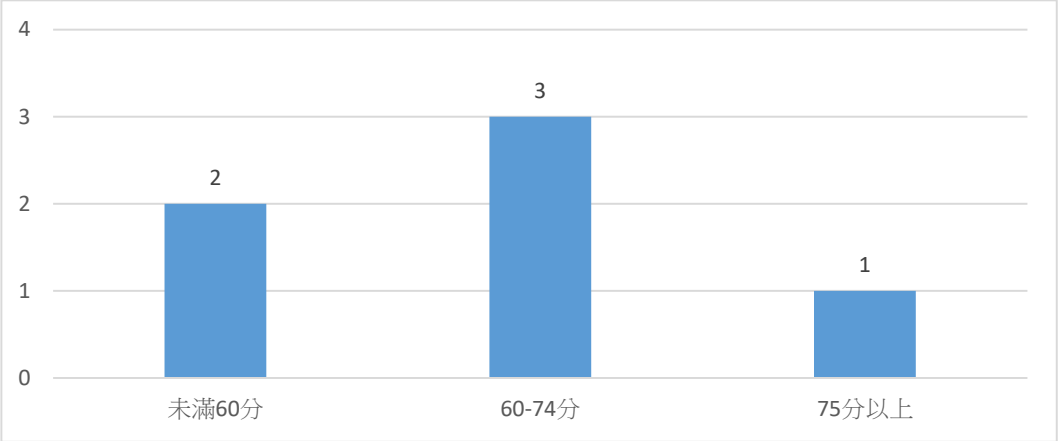

圖 7　第 3 分組實地稽核成績分布

(四) 實地稽核構面成績比較

綜合分析實地稽核策略面、管理面及技術面等構面之表現情形，第 1 分組在各構面明顯優於第 2 分組及第 3 分組，且第 1 分組各構面平均分數皆達 72 分以上，普遍表現良好，實地稽核各構面成績分布，詳見圖 8。

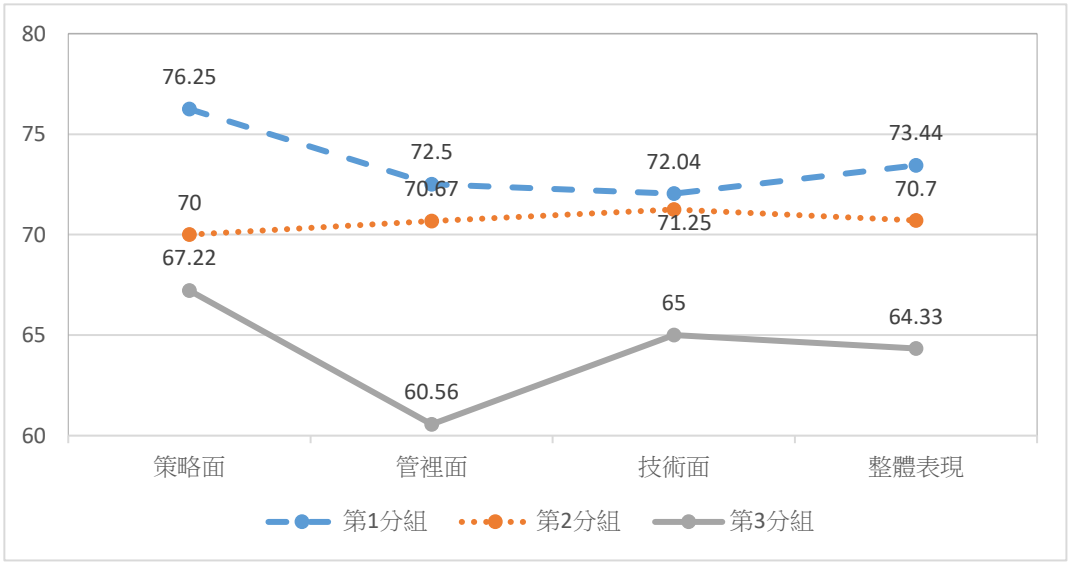

圖 8　分組各面向成績分布

肆、 稽核共同發現

綜整 111 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、 完成核心資通系統導入 ISMS，並通過公正第三方驗證。

2、 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、 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、 訂定內部資通安全稽核計畫，定期辦理實地稽核並複查所發現疏失。

2、 就資通系統委外開發，訂定機關委外作業安全管理規範，並要求各單位落實執行。

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、 依法導入政府組態基準，及建置資通安全威脅管理、資通安全弱點通報、端點偵測及應變等機制。

2、 定期辦理資通安全健診及安全性檢測等作業。

3、 訂定資通安全事件通報應變相關規範，據以執行資通安全事件通報及應處等作業。

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。

2、 部分機關所訂資通安全目標，未有一致性之客觀衡量指標，或與機關實際作業所訂目標不一致、將資安事件發生次數納入量化行目標等。

3、 核心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)設定不當，且備份資料回復測試頻率過久

4、 業務持續運作演練範圍，演練情境多為災害復原演練且僅以資訊單位為主，建議以業務執行為導向、參考資安威脅趨勢設計複合式演練情境，並擴大演練範圍至相關業務單位。

(二) 管理面

1、 部分機關辦理資訊委外作業未訂定安全管理措施、監督內容及受託者應辦理之安全維護事項，建議書徵求文件亦未明確規範防護基準需求及資通安全防護水準。

2、 部分機關辦理委外廠商稽核作業未訂定委外廠商稽核計畫相關管理規範，且未明確訂定廠商稽核之挑選原則及家數。

3、 已辦理資訊資產盤點作業，惟盤點範圍與內容完整性不足，建議盤點範圍應包含全機關。

(三) 技術面

1、 部分機關資安事件通報及應變程序，未訂定資安事件相關證據資料保護規範、事件調查復原與後續矯正改善追蹤機制，應建立相關程序儘速改善。

2、 已進行資通系統安全性檢測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。

3、 部分機關允許以遠端方式維護資通系統。

三、 改善建議

(一) 策略面

1、 依資通安全管理法(以下簡稱資安法)施行細則第 7 條規定，核心業務範圍至少應包含下列 4 類，各機關應依核心業務盤點對應之資通系統，並將支持核心業務持續運作之必要系統列為核心資通系統。

(1) 公務機關應至少為依組織法規足認該業務為核心權責所在，以及提供關鍵基礎設施所需要之業務。

(2) 公營事業及財團法人應至少為其主要服務或功能。

(3) 關鍵基礎設施提供者應至少為提供關鍵基礎設施所需要之業務。

(4) 各機關符合其資通安全責任等級第 4 條第 1 至 5 款或第 5 條第 1 至 5 款所涉及之業務，例如涉及民眾個人資料或服務、跨公務機關之共通性資通系統或服務等。

2、 依資通安全管理法施行細則第 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，量化型指標並應考量合宜性，可依機關之資通安全責任等級對應資通安全責任等級分級辦法附表一至八之應辦事項、資通系統分級結果所對應之防護需求，審酌機關業務屬性、系統特性及資料持有情形等，訂定較客觀及量化之衡量指標，據以一致性評估機關資通系統之防護需求，並勿納入資安事件發生次數，以免影響資安事件通報意願。

3、 核心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)之評估，應考量實際業務需求，與業務單位共同評估，並適度安排備份資料回復測試週期且落實執行。

4、 依資通安全責任等級分級辦法應辦事項規定，應以業務持續運作為導向，辦理業務持續運作演練，演練情境除參考資安威脅趨勢設計外，並應適時納入複合式情境；演練對象並應涵蓋資訊單位及業務單位。

(二) 管理面

1、 依資通安管理法施行細則第 4 條及資通系統籌獲各階段資安強化措施規定，應對委外作業安全建立相關管理程序，從選商(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)及績效之管控、對廠商之稽核等監督管理機制，皆應明制於機關管理程序，並納入與廠商之契約規範中落實執行。

2、 依資通安管理法施行細則第 4 條規定，委託機關應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。並應完整記錄查核證據，訂定改善追蹤管考機制並納入與廠商之契約規範，

透過落實執行，以維稽核之有效性。

3、 依資通安全管理法施行細則第 6 條規定，應完整盤點資通系統及資訊，明確標示核心資通系統及相關資產，盤點範圍為全機關，不應侷限於資訊單位維管者或經費來源。盤點後應進行資產價值鑑別及風險評估，對於老舊軟、硬體、已停止之服務，或已移轉他機關之資產，應即規劃更新及落實資產異動管理程序。

(三) 技術面

1、 依資通安全管理法第 14 條規定，應訂定通報及應變機制，內容除知悉資通安全事件後之通報及應變，應包含資安事件相關跡證保護、事件調查復原與後續矯正改善追蹤機制，並應定期演練。

2、 依資通安全責任等級分級辦法應辦事項規定，至少核心資通系統應定期進行安全性檢測(弱點掃描、滲透測試)及資通安全健診，檢測結果應即處置，並應有追蹤檢測機制確認修補之有效性，以確實降低機關之資安風險。

3、 依行政院資通安全處 110 年 3 月 2 日院臺護字第 1100165761 號函規定，各機關對於遠端維護資通系統，除應採「原則禁止、例外允許」，並應強化相關管理作為，至少辦理以下防護措施：

(1) 如開放委外廠商遠端存取，應要求委外廠商依資通安全管理法施行細則第 4 條，辦理受託業務相關程序及環境，具備完善之資通安全管理措施。

(2) 資通安全責任等級分級辦法附表十「存取控制」構面下「遠端存取」相關規定。

(3) 遠端存取開放原則應以短天期為限，並建立異常行為管理機制。

(4) 遠端存取開放期滿，應即確實關閉網路連線，並更換遠端存取通道(如 VPN 等)登入密碼等。

伍、 結語

資通安全管理法於 108 年施行，迄今已 4 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，本部協助行政院辦理第二方資通安全稽核作業，檢視各機關落實法遵事項及資安防護強化之完整性及有效性，期達成政府機關整體資訊安全。

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。

資安防護不分中央及地方，本部除將地方政府資安專業人才納入行政院資安會報資安稽核團隊之觀察員機制中培訓，亦規劃辦理政府機關稽核作業相關教育訓練，及將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。

本部將彙整分析資安整體威脅情勢，滾動調修稽核項目及稽核重點，持續精進資安稽核作業之深、廣度，協助機關找出自身整體防護盲點，檢視機關面對資安威脅之因應機制，以持續精進並有效管理資安風險。