108年度公務機關資安稽核概況報告

行政院

中華民國 109 年 6 月

目　次

圖 目 次

表 目 次

壹、依據與目的

本院為協助各機關強化資通安全（以下稱資安）防護工作之完整性及有效性，並透過持續改善提升資安防護水準，本院國家資通安全會報於網際防護體系下設「資通安全防護組」，自 90 年起每年選定重要機關辦理資安外部稽核，另資通安全管理法（以下稱資安法）已於 108 年正式施行，明定公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形，本院爰依前述規定辦理 108 年公務機關資安稽核，並依同法第 5 條規定，公布「108 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。

本報告針對受稽機關之資通安全稽核結果提出應改善事項，供其據以持續精進各項資安防護措施，降低資安風險，本院並從中提出共同發現事項，作為持續精進各級公務機關資安防護作為之準據。

貳、108 年度資安稽核作業辦理情形

一、受稽機關

（一）遴選原則

符合以下條件之機關，將優先列為候選名單：

1.當年或近 1 年曾發生重大資安事件（3 級及 4 級）者。

2.當年或近 1 年攻防演練結果仍待改進者。

3.近 4 年稽核結果不佳，仍待持續改善者。

4.資安責任等級列 A 級或 B 級之機關，且近 3 年未曾受稽者。

5.提供跨機關共用（通）性資訊系統服務者。

6.近期完成重大系統建置或改版者。

（二）108 年度受稽機關名單

本院依據上述遴選原則，擇 10 個受稽機關分季進行稽核，受稽機關名單如下表：

表 1　108 年受稽機關名單

項次	受稽機關	資安管理輔導廠商	資安管理驗證廠商	資安管理驗證標準	資安管理驗證範圍
1	法務部	昇達價值管理股份有限公司	BSI 英國標準協會台灣分公司	ISO/IEC 27001:2013	1.法務部資訊處 2.法務部使用者相關安全控制之監督及管理
2	宜蘭縣政府	聯準科技服務有限公司	TUV 漢德技術監督服務亞太有限公司台灣分公司	ISO/IEC 27001:2013 CNS27001:2014	1.計畫處機房 2.公文系統 3.全球資訊網 4.電子郵件系統
3	經濟部	安侯企業管理股份有限公司	SGS 台灣檢驗科技股份有限	ISO/IEC 27001:2013	1.台北資料中心 2.台中資料中心

項次	受稽機關	資安管理輔導廠商	資安管理驗證廠商	資安管理驗證標準	資安管理驗證範圍
		(KPMG)	公司		
4	彰化縣政府	博創資訊科技股份有限公司	BSI 英國標準協會台灣分公司	ISO/IEC 27001:2013	1.全球資訊網 2.公文系統 3.資訊核心系統網路及機房 4.計畫處資訊科個人電腦管理。
5	文化部	漢昕科技股份有限公司	SGS 台灣檢驗科技股份有限公司	ISO/IEC 27001:2013	1.核心資訊系統 2.共構機房
6	內政部	安侯企業管理股份有限公司(KPMG)	BSI 英國標準協會台灣分公司	ISO/IEC 27001:2013	1.資訊中心機房 2.全球資訊網 3.公文電子交換系統 4.憑證管理中心 5.地政資訊核心系統及資訊機房 6.戶役政資訊系統及資訊機房
7	金門縣政府	博創資訊科技股份有限公司	SGS 台灣檢驗科技股份有限公司	ISO/IEC 27001:2013	1. 電腦機房 2. 行政處資管科 3. 政風處
8	行政院主計總處	安侯企業管理股份有限公司(KPMG)	SGS 台灣檢驗科技股份有限公司	ISO/IEC 27001:2013	全機關
9	臺東縣政府	預計 109 年導入	預計 109 年導入	預計 109 年導入	預計 109 年導入

項次	受稽機關	資安管理輔導廠商	資安管理驗證廠商	資安管理驗證標準	資安管理驗證範圍
10	金融監督管理委員會	資誠企管顧問公司	環奧國際驗證有限公司	ISO/IEC 27001:2013 CNS27001:2014	全機關

二、稽核方式

資安稽核分 2 階段進行，第 1 階段為技術檢測，主要係針對受稽機關之核心資通系統及使用者電腦進行弱點檢測，為期 3 個工作日；第 2 階段為實地稽核，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訪視及審查，為期 1 日。

三、稽核日期

108 年度各受稽機關稽核日期如下表：

表 2　108 年各受稽機關稽核日期

編號	受稽機關	技術檢測日期	實地稽核日期
1	法務部	7 月 10 日至 7 月 12 日	7 月 30 日
2	宜蘭縣政府	7 月 24 日至 7 月 26 日	8 月 14 日
3	經濟部	7 月 31 日至 8 月 2 日	8 月 22 日
4	彰化縣政府	8 月 7 日至 8 月 9 日	8 月 26 日
5	文化部	8 月 14 日至 8 月 16 日	9 月 6 日
6	內政部	8 月 27 日至 8 月 30 日、9 月 2 日	9 月 16 日

7	金門縣政府	8 月 21 日至 8 月 23 日	9 月 20 日
8	行政院主計總處	9 月 9 日至 9 月 11 日	9 月 26 日
9	臺東縣政府	9 月 18 日至 9 月 20 日	10 月 7 日
10	金融監督管理委員會	9 月 25 日至 9 月 27 日	10 月 16 日

四、稽核小組組成

本稽核小組由稽核領隊、稽核委員、技術檢測人員、工作人員組成，共同執行資安稽核作業，稽核小組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：由政府機關及產學研等領域之資安專家共同組成，每個受稽機關至少安排 7 位稽核委員，包括策略面 2 位、管理面 2 位及技術面 3 位，稽核委員資格條件如下：

1. 策略面與管理面：具資訊安全管理制度 ISO 27001 LA 證照，並以具資安稽核經驗者為優先。
2. 技術面：具資安技術相關證照，並以具資安稽核經驗者為優先。

（三）技術檢測人員：由本院國家資通安全會報技術服務中心同仁擔任。

五、稽核基準與項目

資安稽核作業係參酌國際資訊安全管理標準 ISO 27001、國際資訊服務技術管理標準 ISO 20000、行政院及所屬各機關資訊安全管理

要點、個人資料保護法及資安法等，據以規劃稽核項目與配分。

（一）稽核項目

1、第 1 階段：技術檢測

技術檢測分為 7 大檢測項目，各檢測項目與配分如下表，本項檢測在檢驗機關安全組態設定及安全性更新之落實度。

表 3　技術檢測項目與分配

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	20
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	

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下表：

表 4　實地稽核項目與配分

構面	稽核項目	配分
策略面	1.導入資訊安全管理系統範圍之適切性	5
	2.機關首長對資安業務之支持度	5
	3.資源投入資安業務情形	5
	4.資安業務運作規劃及落實	15
管理面	5.資產管理及風險管理	8
	6.人力資源管理	6
	7.資訊作業委外安全管理	10
	8.所屬機關監督管理 （上級/監督機關適用）	6
技術面	9.電子資料保護	8
	10.通訊及作業安全	12
	11.資安事件通報及處理	10
	12.資通系統開發及維護安全	10

（二）資安稽核評分

資安稽核評分採計技術檢測與實地稽核 2 項分數，並以加權計算方式計算總分，計算公式為：總分＝技術檢測分數×30%＋實地稽核分數×70%，總分前 3 名且技術檢測與實地稽核個別成績均達 75 分以上之受稽機關為本年度績優機關。

參、 108 年度資安稽核結果

各受稽機關之稽核結果總分平均為 69.3 分，其中技術檢測平均分數為 62.99 分，實地稽核平均分數為 72.01 分。

一、技術檢測

技術檢測分數達 75 分以上者有 2 個機關，表現較佳，其餘 8 個機關整體評分未達 75 分，其中有 6 個機關低於 60 分，顯示部分機關在技術實務管理之落實度仍需加強，整體受稽機關之技術檢測成績分布如圖 1。

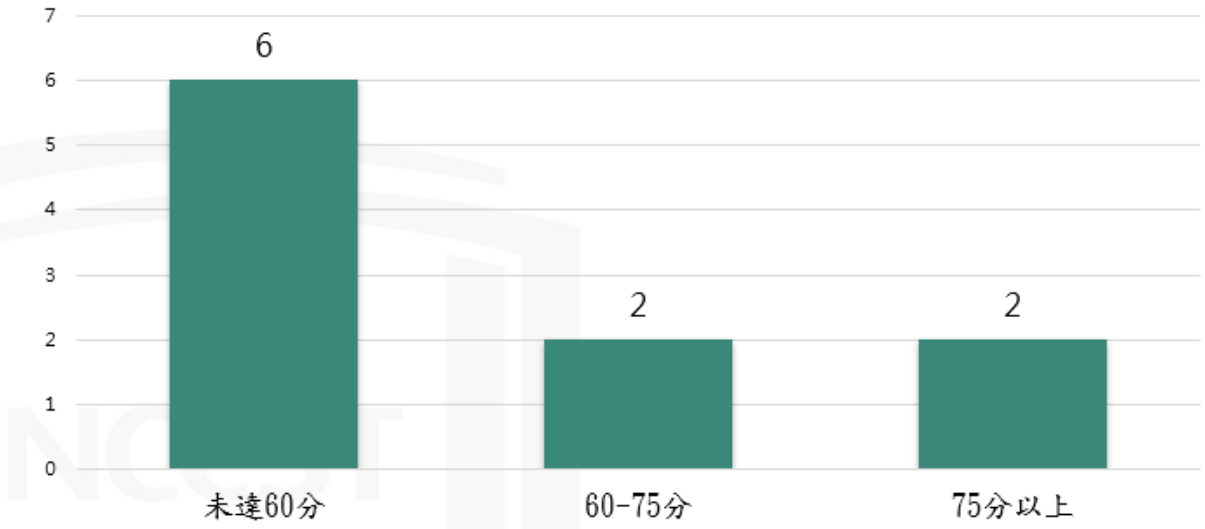


圖 1 技術檢測成績分布

技術檢測個別項目成績，詳如圖 2，其中「惡意中繼站連線阻擋」、「網域主機安全防護」及「組態設定安全」等 3 項表現良好，達 75 分以上水準，然在「網路架構檢測」及「物聯網設備檢測」等 2 個檢測結果顯示仍待改進。

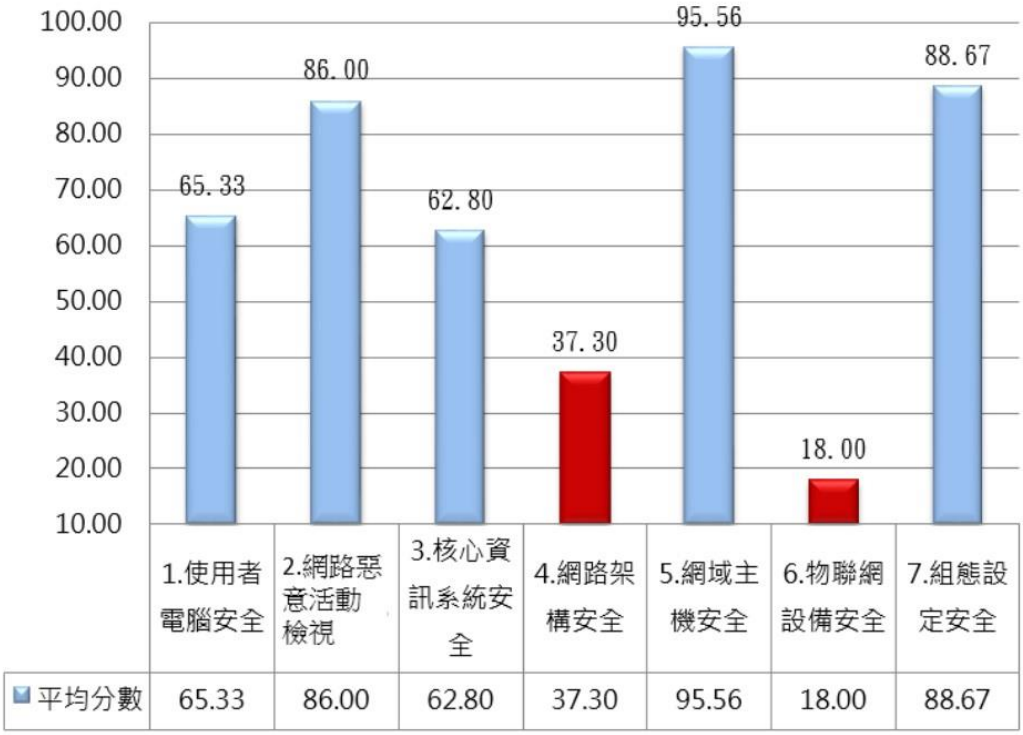


圖 2　技術檢測個別項目成績分布圖

二、實地稽核

實地稽核成績逾 75 分以上者有 3 個機關，7 個機關成績未達 75 分，其中 1 個機關成績低於 60 分，整體受稽機關成績分布如圖 3。

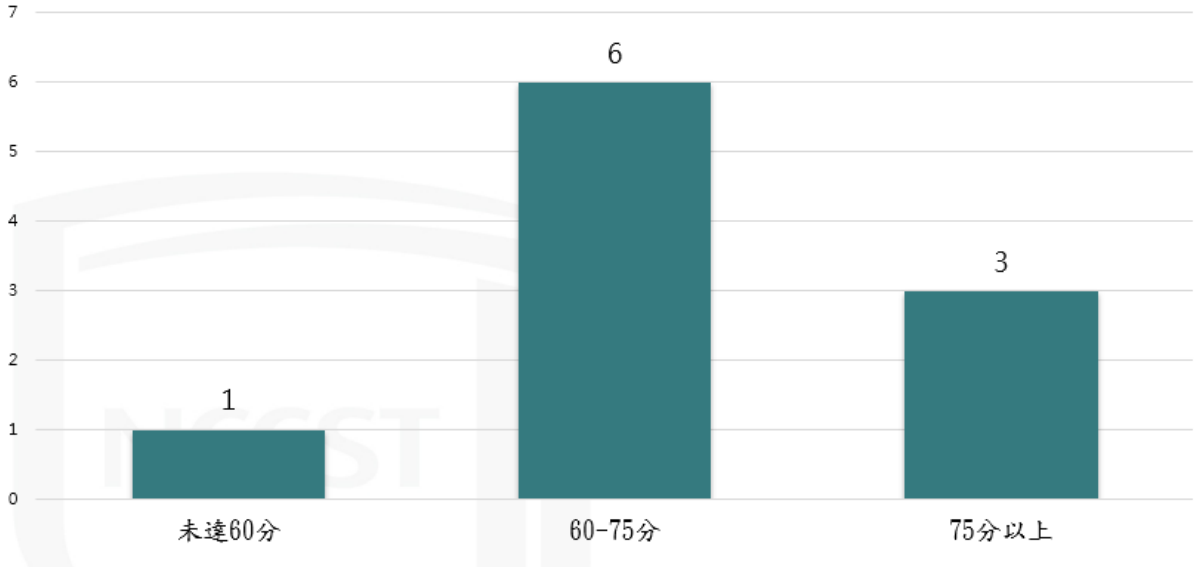


圖 3　實地稽核成績分布

經檢視實地稽核個別項目成績分布（如圖 4），其中「機關首長

對資安業務之支持度」、「資安事件通報及處理」表現良好，達 75 分以上水準，展現機關高層對資安事務推動的決心及支持度，以及對於資安事件通報及處理有具體的規劃及落實，值得肯定，其餘 10 個項目未達 75 分，其中「資安業務運作規劃及落實」及「資通系統開發及維護安全」等 2 項成績較不符預期，仍待改善。

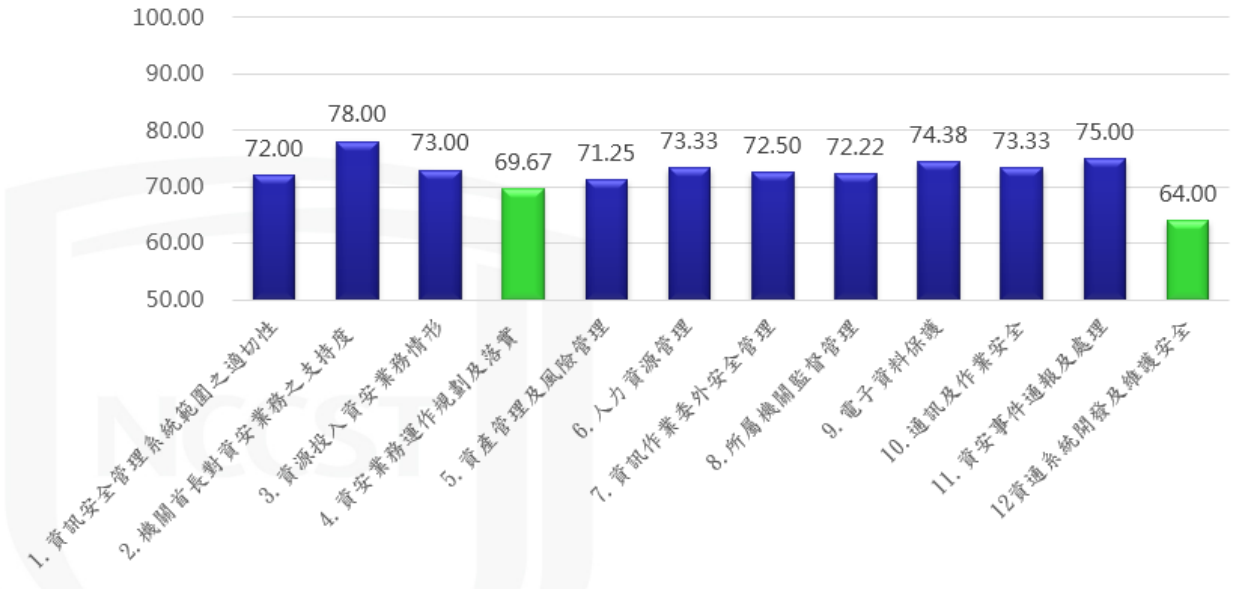
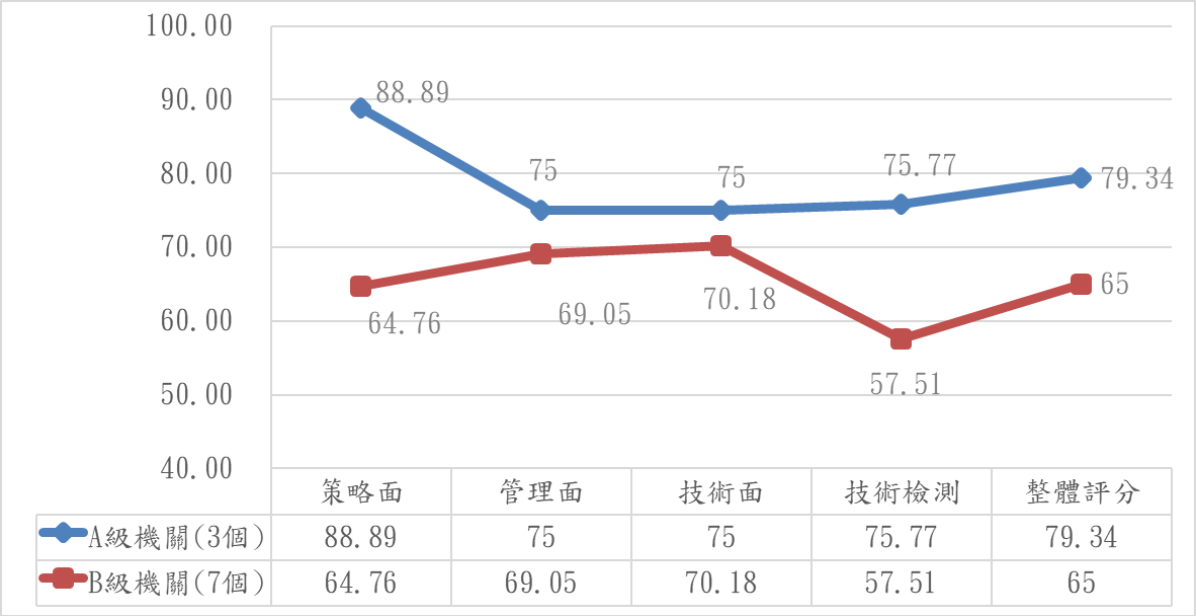


圖 4　實地稽核個別項目成績分布圖

三、 實地稽核構面與技術檢測比較

比較機關於實地稽核各構面（策略面、管理面及技術面）與技術檢測二者之表現情形（詳見圖 5），呈現技術檢測之成績低於實地稽核整體表現，顯示機關雖有管理制度，惟在落實度上仍需加強。



	策略面	管理面	技術面	技術檢測	整體評分
A級機關(3個)	88.89	75	75	75.77	79.34
B級機關(7個)	64.76	69.05	70.18	57.51	65

圖 5　稽核整體表現分布圖

四、資安責任等級級別比較

將公務機關依其資安責任等級分為 A 級、B 級群組進行比較，A 級機關之整體表現明顯優於 B 級機關，顯見 A 級機關對資通安全防護之意識及資源投入較於重視，另外，A 級機關平均分數皆達 75 分以上，普遍表現良好，B 級機關在技術檢測表現尚待加強。各群組成績分布說明如下：

（一） 資安責任等級 A 級機關

本次受稽機關中，資安責任等級列 A 級者計有 3 個，整體平均分數為 79.34 分，其中整體評分 75 分以上有 2 個機關，其餘 1 個機關整體評分 72.74 分，A 級機關表現不俗，成績分布如圖 6。

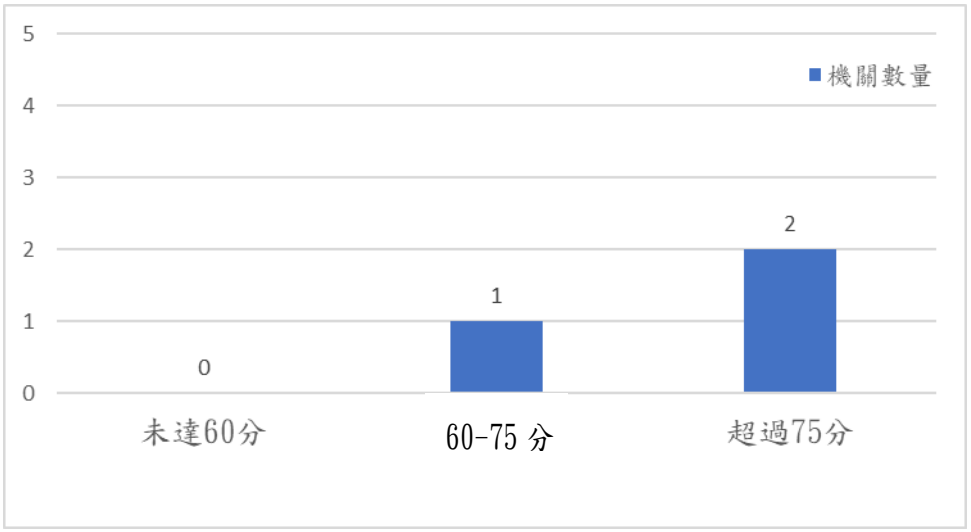


圖 6　A 級機關稽核整體成績

（二）資安責任等級 B 級機關

本次受稽機關中，資安責任等級列 B 級者計有 7 個，整體平均分數為 65 分，其中整體評分 75 分以上有 1 個機關，其餘 6 個機關整體評分未達 75 分，其中有 2 個機關低於 60 分，如圖 7。

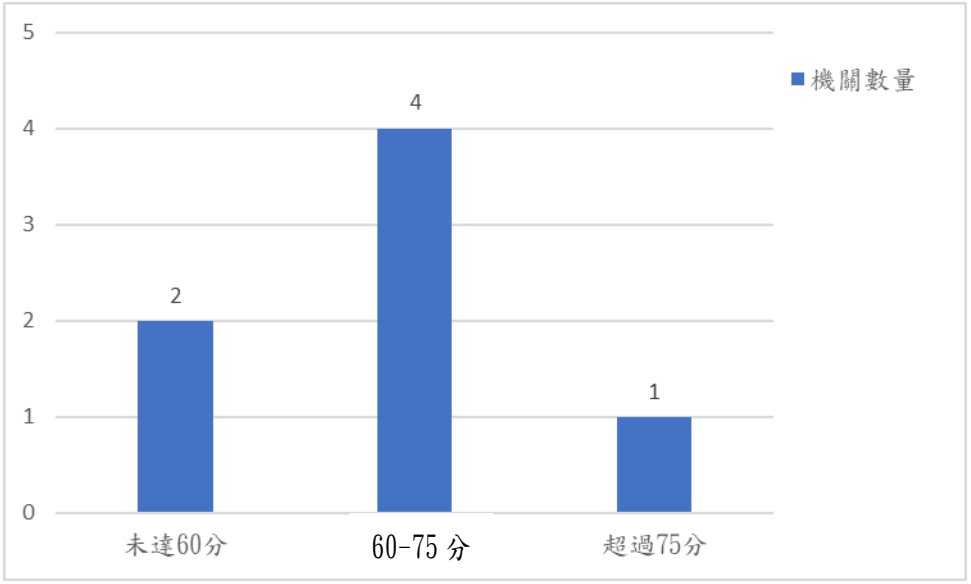


圖 7　B 級機關稽核整體成績

肆、 稽核發現

經綜整 108 年實地稽核結果，說明稽核發現事項如下：

一、法遵符合情形

（一）策略面

1、 大部分機關已依法將全部核心資通系統導入資訊安全管理系統(Information Security Management System, ISMS)並通過驗證，且部分機關 ISMS 驗證範圍已擴及全機關。

2、 部分機關之資安維護計畫，已制定共通性管理程序供所屬機關遵循。

3、 部分機關資安推動組織除加入各有關業務單位主管參與外，並納入所屬機關資安長共同推動。

（二）管理面

1、 部分機關推動資源向上集中整合，統籌管理機關本身及所屬機關整體網路架構。

2、 部分機關已落實強化對委外廠商稽核。

3、 部分機關已規劃及執行對所屬或監督機關稽核作業。

（三）技術面

1、 部分機關就資通系統存取控制均符合最小權限原則。

2、 部分機關已依資通安全情資分享辦法，規劃建立情資分享機制。

3、 機關普遍依資安責任等級分級應辦事項，落實強化網域主機資通安全防護，包括惡意程式防護、防毒軟體、安全性更新等。

二、共同發現事項

以下就實地稽核結果提出共同發現事項。

（一）策略面

1、未有效落實核心業務及核心資通系統之界定。

2、資安維護計畫與內部 ISMS 規範文件不一致，且未納入資安法規要求。

3、資通安全相關法遵及技術知能要求與日俱增，惟受稽機關常因資安人力資源缺乏未配置專職/責人力。

（二）管理面

1、受稽機關人員與委外廠商對於資安相關法規認知仍顯不足。

2、未依資安法等規範事項規劃與落實資訊委外作業。

3、上級機關未依所屬或監督機關之資通安全責任等級，規劃適當之稽核整體計畫（包含明訂受稽機關遴選原則、依機關資安責任等級需求規劃檢核表等），以致影響稽核執行成效。

（三）技術面

1、網路架構安全性仍顯不足，未確實進行網段區隔及存取控管。

2、資通系統安全開發程序未納入資通系統防護需求且未落實。

3、未針對核心資通系統定期進行弱點掃描、系統滲透測試，機關資安健診作業應訂定內部資安作業程序，且應確實改善追蹤。

4、未就政府組態基準(Government Configuration Baseline, GCB)套用之例外管理，提出可行方式及改善時程，並定期追蹤改善情形。

5、未將物聯網設備納入資訊資產盤點範圍，並建立適當防護措施。

三、改善建議

為協助各機關強化資安防護工作，針對本次稽核作業之共同發現事項，已彙整相關改進建議函請各機關據以檢討調整機關現行資安防護作為，相關改善建議如下：

（一）策略面

1、應依據資安法施行細則第 7 條，確實界定機關核心業務及核心資通系統，並依據資通安全責任等級分級辦法完成資通系統分級，及完成相對應之控制措施。

2、因應資安法之施行，各機關應重新檢討機關內部資安規範與資安法之合規性，並配置資源確實執行。

3、機關應依資安法規定，重新檢視目前資安人力配置與運用情形，於機關總員額範圍內，優先調配資安專職人員，並結合資安專業訓練，培養機關所需之資安專職人力。

（二）管理面

1、各機關應配合資安法施行，透過教育訓練、內部會議、張貼公告等方式，落實並宣導資安法之法遵事項。

2、各機關應強化監督及管理委外廠商之權責，加強自身管理能力，並依據資安法規定及參考「政府資訊作業委外安全參考指引」辦理資訊委外管理作業。

3、各機關應依據資安法子法「資通安全責任等級分級辦法」附表十資通系統防護基準「存取控制」構面之各項措施內容重新檢視機關內部各項存取控管措施。

4、公務機關對於所屬或監督機關之第二方稽核作業，建議訂定整體稽核計畫，包含期間、重點領域、稽核方式、基準及項目等，以落實對所屬或監督機關之監督管理。

（三）技術面

1、各機關應針對網路架構建立定期檢視政策，透過網路架構全面性檢視，持續強化網路架構相關安全防護。

2、 各機關應依資通安全責任等級分級辦法附表十資通系統防護基準「系統與服務獲得」構面之各項措施內容重新檢視機關內部在安全系統發展生命週期（SSDLC）之機制，確保軟體系統在開發過程中可以採行相應之安全防護措施。

3、 依資通安全責任等級分級辦法之應辦事項規定，各機關應針對核心資通系統定期進行弱點掃描、系統滲透測試，並且對於全機關進行資安健診作業，並訂定後續改善追蹤機制，以確保機關之資通安全防護。

4、 各機關應確實導入 GCB，除因技術限制、個別資通系統之設計、結構或性質等因素之例外管理，應提出方式及改善時程，並且定期檢視追蹤改善情形。

5、 各機關應將物聯網設備納入資通訊資產盤點範圍，並建立適當防護管理措施，另設備應通過資安檢測規範或標準，以降低資安風險。

伍、 結語

本院為協助各機關強化資安防護工作，於本次資安稽核作業辦竣後，已將稽核共同發現事項及改善建議，函請各機關據以檢討調整並納入資通安全維護計畫，另透過資通安全長會議或全國巡迴說明會加強宣導。目前各機關已依稽核結果完成短期改善建議，部分改善建議屬中長期規劃，各機關將配合採分年、分階段方式調整，本院亦將持續督促各機關改善資安防護作業，並持續追蹤各改善建議之辦理情形。

本次資安稽核發現受稽機關普遍未依規配置專職人員，本院刻正研擬協助各機關補實資安專職人力之措施，並持續推動於公務人員晉用管道增列資通安全職系，另為提升公務人力之資安職能，刻正發展公務人員資安專職人力學習地圖、建立並持續完備資安職能訓練機構制度等。

本院將持續落實資安法規定，對公務機關實施資安稽核，協助機關及早發現風險避免可能危害；另本院仍持續按資安法分層監督管理機制，強化上級機關對所屬機關之第二方稽核能量，協助上級機關對其所屬或監督機關落實資安法遵事項，維護國家整體資通安全發展環境。