107年公務機關資安稽核概況報告

行政院
中華民國108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(以下簡稱資安)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，並依稽核結果，提出受稽機關(構)應改善事項，供其據以持續精進各項防護措施，降低資安風險。

資通安全管理法業於 107 年 6 月 6 日總統令公布，並自 108 年 1 月 1 日起施行，本院爰依資通安全管理法第 5 條第 1 項規定，公布「107 年公務機關資安稽核概況報告」，並送立法院備查。

貳、107 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。

7.未依規定完成資安責任等級相對之應辦事項者。

（二）107 年度受稽機關名單

本院依據上述遴選原則，擇 25 個受稽機關分季進行稽核，受稽機關名單如下表：

表 1　受稽機關名單

場序	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	審計部	自行導入	無	無	無
2	國立臺灣大學醫學院附設醫院	勤業眾信	SGS 台灣檢驗科技股份有限公司	ISO/IEC 27001:2013	全機關
3	臺北市政府警察局	博創資訊科技股份有限公司	艾法諾國際股份有限公司	ISO/IEC 27001:2013	1. 資訊機房及網路基礎建設管理 2. 軟體資產(含套裝

場序	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
					軟體、行動資訊系統、勤務管理系統)、實體資產
4	經濟部中小企業處	宏碁資訊服務股份有限公司	無	無	無
5	國家發展委員會檔案管理局	宏碁雲架構股份有限公司	BSI 英國標準協會台灣分公司	ISO/IEC 27001:2013	全機關
6	桃園市政府教育局	德欣寰宇科技股份有限公司	SGS 台灣檢驗科技股份有限公司	CNS 27001:2013、ISO/IEC 27001:2013	1. 資訊及科技教育科資訊機房管理 2. 教育公務系統入口及網域名稱服務集中管理平台
7	衛生福利部中央健康保險署	自行導入	SGS 台灣檢驗科技股份有限公司	CNS 27001:2014、ISO/IEC 27001:2013	全機關
8	衛生福利部臺北醫院	自行導入	SGS 台灣檢驗科技股份有限公司	ISO/IEC 27001:2013	1. 資訊機房與網路管理 2. 醫療資訊系統及護理資訊系統等
9	新竹市政府	德欣寰宇科技股份有限公司	TUV 漢德技術監督服務亞太有限公司台灣分公司	CNS 27001:2014 ISO/IEC 27001:2013	1. 行政處資訊科資訊機房管理 2. 公文整合資訊系統及民眾申請ｅ好辦系統
10	南投縣政府	漢昕科技股份有限	TUV 漢德技術監督	ISO/IEC	1. 地政處地籍管理科及地政事務所

場序	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
		公司	服務亞太有限公司台灣分公司	27001:2013	資訊機房與網路管理維運 2. 未辦繼承系統、資料庫同步異動系統等
11	衛生福利部疾病管制署	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	全球資訊網資訊系統、慢性傳染病追蹤管理-愛滋及漢生病子系統等 17 個系統
12	經濟部工業局	KPMG 安侯企業管理股份有限公司	BSI 英國標準協會台灣分公司	ISO/IEC 27001:2013	1. 資訊室資訊機房、網路基礎架構及相關委外活動的管理 2. 公文掛文收發櫃台服務作業管理及公文考核作業管理
13	中央研究院	數聯資安股份有限公司	SGS 台灣檢驗科技股份有限公司	ISO/IEC 27001:2013	資訊服務處
14	財政部財政資訊中心	KPMG 安侯企業管理股份有限公司	BSI 英國標準協會台灣分公司	ISO/IEC 27001:2013	全機關
15	高雄市政府警察局	登豐數位科技股份有限公司	無	無	無
16	新北市政府資訊中心	財團法人中華民國國家資訊基本建設	BSI 英國標準協會台灣分公司	ISO/IEC 27001:2013	1. 資訊機房管理 2. 各項資訊處理業務系統

場序	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
		產業發展協進會			
17	花蓮縣政府	久揚科技有限公司	SGS 台灣檢驗科技股份有限公司	ISO/IEC 27001:2013	資訊科資訊機房(含資訊應用系統)
18	臺南市政府(智慧發展中心)	漢昕科技股份有限公司	TUV 漢德技術監督服務亞太有限公司台灣分公司	ISO/IEC 27001:2013	1. 資訊機房 2. 電子公文交換系統、公務入口網、全球資訊網核心系統等
19	高雄市政府交通局	璞方科技管理顧問股份有限公司	SGS 台灣檢驗科技股份有限公司	ISO/IEC 27001:2013	1. 共構機房管理 2. 公車動態資訊系統、停車收費管理系統、交通控制系統及上述系統之網路環境
20	外交部	安碁資訊股份有限公司	BSI 英國標準協會台灣分公司	ISO/IEC 27001:2013	5 個核心系統及公文系統、檔管系統、表單系統、外交服務網、電子郵件系統
21	科技部新竹科學工業園區管理局	宏碁資訊股份有限公司	SGS 台灣檢驗科技股份有限公司	ISO/IEC 27001:2013	1. 資訊機房 2. 園區廠商管理資訊系統
22	國軍退除役官兵輔導委員會	自行導入	SGS 台灣檢驗科技股份有限公司	CNS 27001:2013、ISO/IEC 27001:2013	1. 資訊機房(含資訊應用系統) 2. 統計資訊處及政風處
23	澎湖縣政府	新誼整合科技股份	SGS 台灣檢驗科技	ISO/IEC 27001:2013	1. 第一、第二電腦機房

場序	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
		有限公司	股份有限公司		2. 行政處資訊科、政風處政風預防科
24	國家災害防救科技中心	企盉顧問股份有限公司	SGS 台灣檢驗科技股份有限公司	ISO/IEC 27001:2013	1. 資訊機房管理 2. 災害情資服務平台及全球資訊網
25	行政院農業委員會	資拓宏宇國際股份有限公司	BSI 英國標準協會台灣分公司	ISO/IEC 27001:2013	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，主要係針對受稽核機關之核心資訊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

107 年度各受稽機關稽核日期如下表：

表 2　107 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	審計部	5 月 2 日至 5 月 4 日	5 月 22 日
2	國立臺灣大學醫學院附設醫院	5 月 16 日至 5 月 18 日	6 月 4 日
3	臺北市政府警察局	5 月 21 日至 5 月 23 日	6 月 8 日
4	經濟部中小企業處	5 月 23 日至 5 月 25 日	6 月 14 日

編號	受稽機關	技術檢測日期	實地稽核日期
5	國家發展委員會檔案管理局	5月30日至6月1日	6月20日
6	桃園市政府教育局	6月6日至6月8日	6月28日
7	衛生福利部中央健康保險署	6月11日至6月13日	7月3日
8	衛生福利部臺北醫院	6月20日至6月22日	7月12日
9	中央研究院	7月4日至7月6日	8月6日
10	新竹市政府	7月18日至7月20日	8月16日
11	南投縣政府	8月1日至8月3日	8月29日
12	財政部財政資訊中心	8月8日至8月10日	9月4日
13	經濟部工業局	8月15日至8月17日	9月11日
14	衛生福利部疾病管制署	8月22日至 8月24日	9月17日
15	高雄市政府警察局	8月27日至8月29日	9月21日
16	新北市政府資訊中心	9月5日至9月7日	10月4日
17	花蓮縣政府	9月12日至9月14日	10月12日
18	臺南市政府研究發展考核委員會	9月19日至9月21日	10月18日
19	高雄市政府交通局	9月26日至9月28日	10月24日
20	外交部	10月3日至10月5日	10月30日
21	科技部新竹科學工業園區管理局	10月17日至10月19日	11月16日
22	國軍退除役官兵輔導委員會	10月24日至10月26日	11月22日

編號	受稽機關	技術檢測日期	實地稽核日期
23	澎湖縣政府	10 月 31 日至 11 月 2 日	11 月 30 日
24	國家災害防救科技中心	11 月 5 日至 11 月 7 日	12 月 6 日
25	行政院農業委員會	11 月 7 日至 11 月 9 日	12 月 12 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、個人資料保護法及本院相關資安規定等，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 6 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	配分
1	使用者電腦安全	35
2	中繼站連線阻擋	5
3	核心資訊系統安全	40
4	網路架構安全	10
5	網域主機安全	10
6	物聯網設備安全	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 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(配分)	稽核項目	配分
策略面 (30)	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.資源投入資安業務狀況	5
	4.資安業務運作規劃與落實	15

構面(配分)	稽核項目	配分
管理面 (30)	5.個人資料保護與管理	10
	6.資產管理與風險評鑑	7
	7.人力資源管理	6
	8 資訊委外安全管理	7
技術面 (40)	9.通訊與作業安全	15
	10.資安事件通報與處理	10
	11.資訊系統開發與維護安全	15

（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、107 年度資安稽核結果

各受稽機關之稽核結果總分平均為 67.06 分，其中技術檢測平均分數為 65.81 分，實地稽核平均分數為 67.6 分。

一、技術檢測

技術檢測分數達 75 分以上者有 6 個機關，表現較佳，其餘 19 個機關整體評分未達 75 分，其中有 11 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。

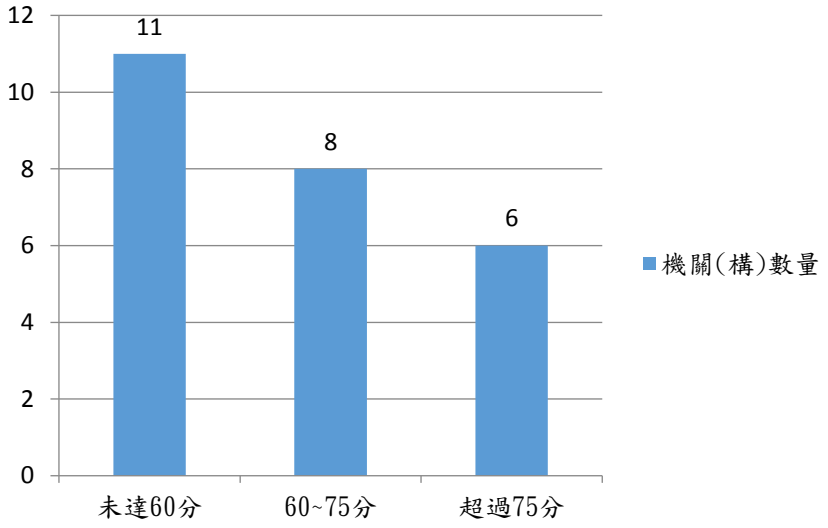


圖 1 技術檢測成績分布

技術檢測個別項目成績如下圖 2，其中「中繼站連線阻擋」及「網域主機安全」等 2 項表現良好，達 75 分以上水準，然在「使用者電腦安全」、「核心資訊系統安全」及「網路架構安全」等 3 個檢測結果顯示仍待改進。

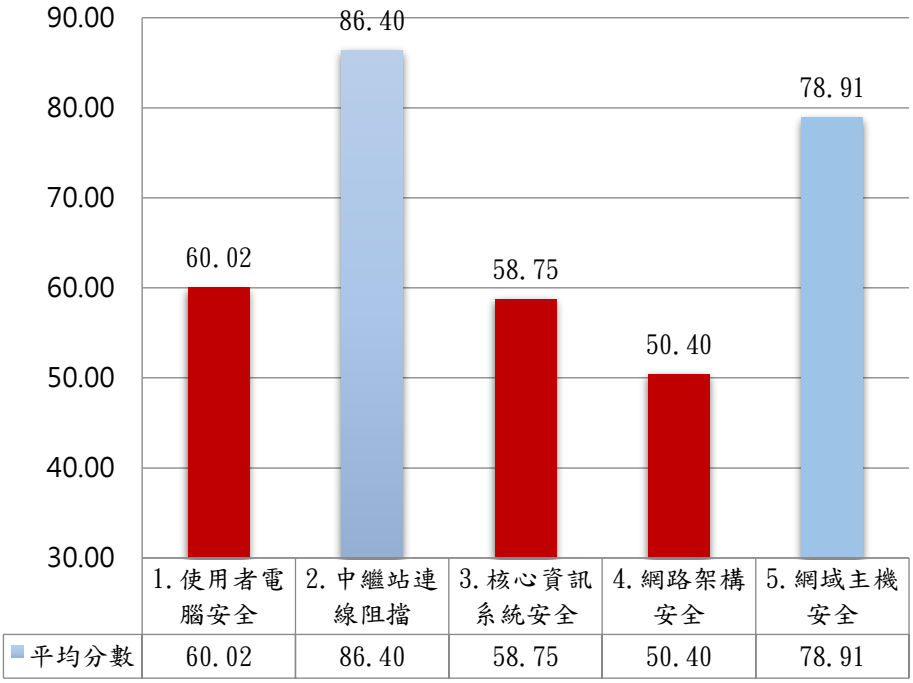


圖 2　技術檢測個別項目成績分布圖

二、實地稽核

實地稽核成績逾 75 分以上者有 8 個機關，17 個機關成績未達 75 分，其中 5 個機關成績低於 60 分，整體受稽機關成績分布如圖 3。

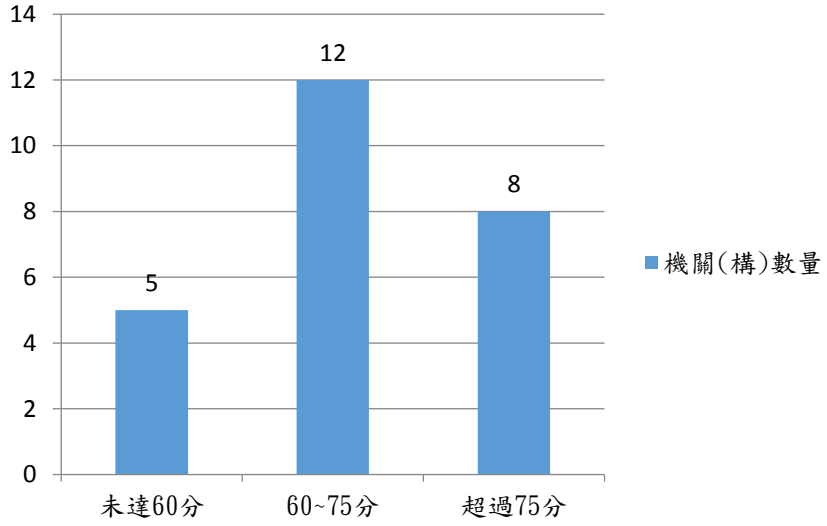


圖 3　實地稽核成績分布

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」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，值得肯定，其餘 10 個項目未達 75 分，其中「個人資料保護與管理」及「資訊委外安全管理」等 2 項成績較不符預期，顯示部分機關對於個人資料保護管理及資訊委外管理仍待改善。

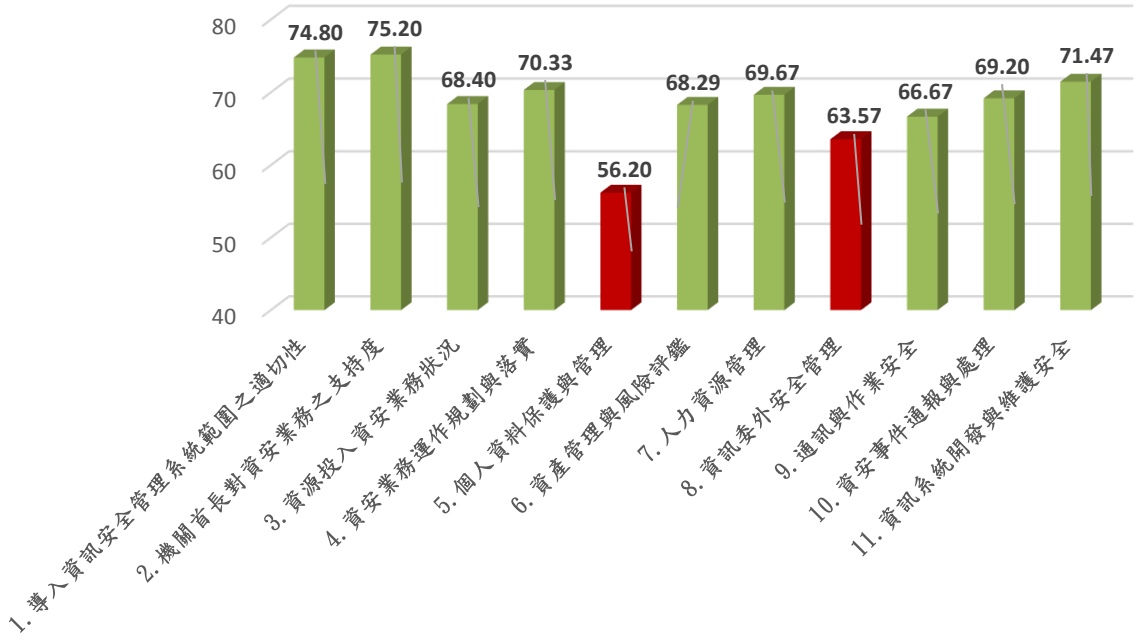
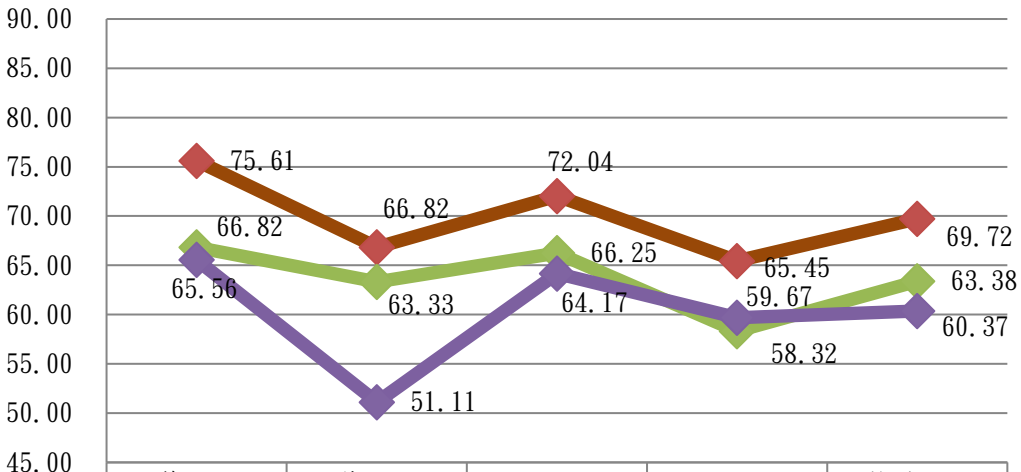


圖 4　實地稽核個別項目成績分布圖

三、 實地稽核構面與技術檢測比較

綜合分析實地稽核各構面(策略面、管理面及技術面)與技術檢測之表現情形，詳見圖 5，分析如下：



	策略面	管理面	技術面	技術檢測	整體評分
A級機關(11個)	75.61	66.82	72.04	65.45	69.72
B級機關(11個)	66.82	63.33	66.25	58.32	63.38
C+/C級機關(3個)	65.56	51.11	64.17	59.67	60.37

圖 5　稽核整體表現分布圖

技術檢測結果可用於反映機關資安實作面之落實度，上圖結果呈現技術檢測之成績低於實地稽核技術面表現，顯示機關雖有管理制度，惟落實度仍需加強。

四、資安責任等級級別比較

將受稽機關依其資安責任等級分為 A 級、B 級及 C+/C 級等 3 個群組進行比較，顯示 A 級機關之整體表現優於其他群組，B 級機關次之，C+/C 級機關表現則仍待改進，顯見 A 級機關對自我安全防護之重要性及意識已有所提升，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 11 個，整體平均分數為 69.72 分，其中整體評分 75 分以上有 3 個機關，其餘 8 個機關整體評分未達 75 分，其中有 2 機關低於 60 分，成績分布如圖 6。

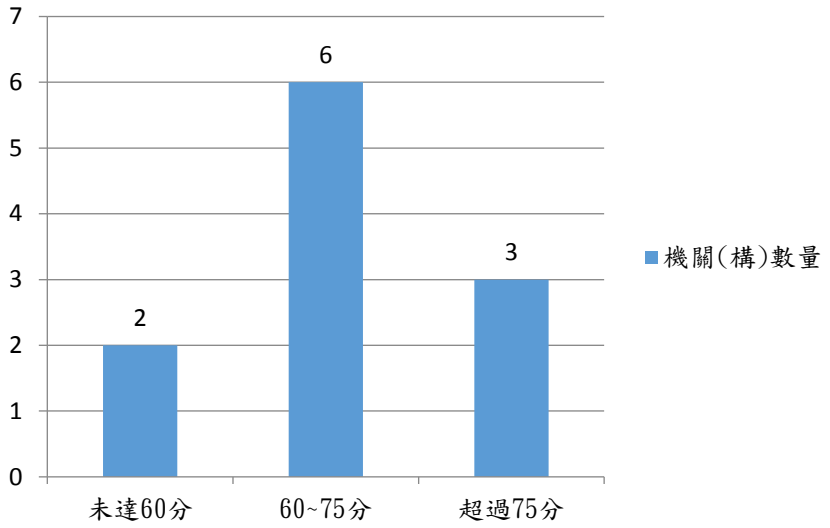


圖 6　A 級機關(構)稽核整體成績

（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 11 個，整體平均分數 63.38 分。其中 75 分以上有 1 個機關，其餘 10 個機關總分未達 75 分，其中有 4 機關低於 60 分，如圖 7。

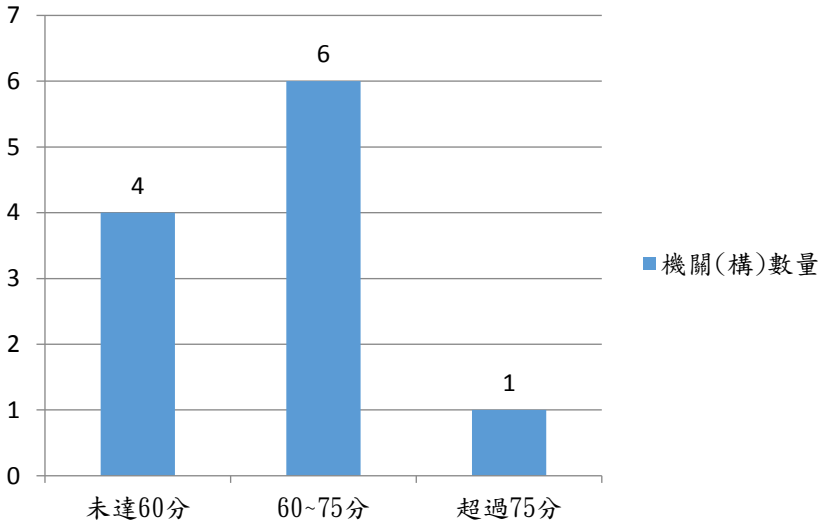


圖 7　B 級機關(構)稽核整體成績

（三） 資安責任等級 C+/C 級機關

本次受稽機關中，資安責任等級列 C+/C 級者計有 3 個，整體平均分數 60.37 分，仍待提升，如圖 8。

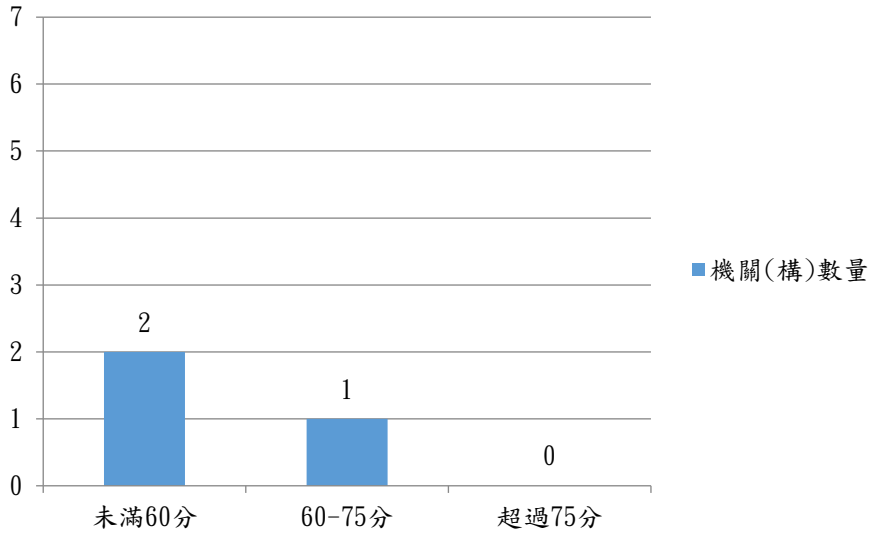


圖 8　C+/C 級機關(構)稽核整體成績

肆、稽核發現

經綜整 107 年實地稽核結果，說明稽核發現事項如下：

一、優點事項

（一）策略面

1、部分機關將一般人員之資安規範遵循情形，納入人事獎懲及單位年終業務績效考評指標，強化全體同仁之日常資安防護認知，有效提升同仁資安意識。

2、多數受稽機關之資安內部稽核作業由政風單位及資訊單位共同執行，以客觀公正之觀點，將資安管理與機關內稽內控制度相互融合，有助提升稽核效率及落實機關自我監督機制。

3、部分機關積極建立資安自主技術能量，避免過度依賴委外廠商及人力。

（二）管理面

1、建置完善數位學習平台，並將資安訓練課程列為機關同仁年度必修課程，課後進行線上測驗及滿意度調查，充分掌握同仁學習情形，並據以精進改善。

2、對重要資訊系統之委外廠商進行實地稽核，落實委外監督管理工作，並將廠商評鑑結果納入後續委外評選之參考。

3、確實辦理汰除設備之儲存資料銷毀作業並留下照片佐證，確保機敏資料難以復原使用。

（三）技術面

1、部分機關之核心資訊系統採多因子認證技術，提高身分鑑別之安全性。

2、部分機關運用工具有效管制未經允許之軟體安裝及行動裝置存取內部網路，並限制可攜式儲存裝置之使用，降低資料外洩及入侵風險。

3、建置資料庫加密及即時異地備份機制，並於正式環境與測試環境使用不同之加密管理機制。

4、辨識機關機敏資料並進行加密保護或去識別化處理，落實資料存取日誌管理及加密金鑰分持管理。

二、共同發現事項

以下針對實地稽核結果提出共同發現事項。

（一）策略面

1、資安推動組織參與之業務單位涵蓋面及參與度不足，致使相關資安政策要求難以宣達全機關。

2、資安推動組織缺乏對追蹤改善事項之審查與管理，致難以確保各項改善事項皆已完成及落實。

3、資通系統鑑別、資產風險評估、業務營運衝擊分析、營運持續計畫演練或驗證範圍等各項作業之間欠缺關聯性。

（二）管理面

1、欠缺完整的個人資料管理制度，包括個人資料盤點、風險評估、隱私衝擊分析及相關管理等。

2、宜加強資安專職人力配置，以符合資通安全管理法規定。

3、缺乏對委外廠商之資安要求及有效監督與管理，包括委外廠商管理程序、契約要求、駐點人員管理、委外稽核等。

4、機關之資訊安全管理系統(ISMS)文件與相關法規規定未有效銜接。

（三）技術面

1、未依使用者權限進行存取權限管理與遠端存取設定。

2、宜落實安全系統發展生命週期防護(SSDLC)，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、資通安全事件通報規範與實際作法未盡一致。

4、使用者電腦仍待落實相關安全管控及安全更新等作業。

5、物聯網設備之盤點及安全管理仍待強化。

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、各機關之資安推動組織，宜由資通安全長召集各單位之主管或副主管組成，共同推動資通安全相關政策，並訂定資安管理績效指標，透過定期召開推動會議，追蹤與檢討相關控制措施的適切性及有效性。

2、資通安全推動小組每年至少應召開 1 次資通安全管理審查會議，相關成員應確實出席且針對資通安全之績效指標及改進事項進行檢討，並適時因應資安威脅趨勢，對主管人員進行資安宣導。

3、機關應落實與檢視資通系統分級作業，釐定機關之核心業務與資通系統，進而進行營運衝擊分析，確實反應資安防護需求，並配予資源進行營運持續演練作業，確保核心資通系統得以因

應各種重大人為及天然災害持續運行。

（二）管理面

1、建議個人資料以作業流程面向進行盤點，詳細識別個資蒐集之法令依據、保存年限及生命週期，並應依「個人資料保護法」及「個人資料保護參考指引」之要求，訂定個資保護管理規範、設立個資保護推動組織，並將個資保護推動情形納入內部稽核範圍，定期檢視資源配置及落實改善情形。

2、機關應重新檢視目前資安人力配置與運用情形，結合資安專業訓練，培養機關所需之資安專職人力。

3、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，並依據資通安全管理法規定及參考「政府資訊作業委外安全參考指引」辦理資訊委外管理作業。

4、因應資通安全管理法之施行，各機關應重新檢討機關內部資安規範與資通安全管理法之合規性，並配置資源確實執行。

（三）技術面

1、落實個人電腦安全管控作業，確保全機關之個人電腦及時完成安全性修補作業並建立檢查機制。

2、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。

資通安全管理法於今(108)年 1 月 1 日正式施行，本院將持續落實資通安全管理法規定，對公務機關及特定非公務機關實施資安稽核，透過稽核發現，協助前述機關持續改善資安防護作業，維護國家資通安全發展環境。