109年度公務機關資安稽核概況報告

行政院

中華民國 110 年 6 月

目　次

圖 目 次

表 目 次

壹、 依據與目的

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，透過持續改善提升資安防護水準，本院國家資通安全會報(以下稱資安會報)自 90 年起每年選定重要機關辦理資安外部稽核。資通安全管理法（以下稱資安法）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 109 年公務機關資安稽核，並依同法第 5 條規定，公布「109 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安稽核結果提出應改善事項，協助其據以持續改善及精進各項資安防護措施，降低資安風險，本院並由稽核結果中彙整發布共同發現之待改善事項，提供各級公務機關據以檢討策進資安防護作為。

貳、 109 年度資安稽核作業辦理情形

一、 受稽機關

(一) 遴選原則：自本院所屬二級機關中遴選，各機關受稽核頻率為 2 年 1 次。

(二) 109 年度受稽機關名單

本院依據上述遴選原則，擇 15 個受稽機關分季辦理稽核作業，並調查各受稽機關資安管理輔導及驗證廠商，除確認受稽機關已依資通安全責任等級分級辦法應辦事項，導入及通過公正第三方驗證，及提供本院對照廠商輔導、驗證之有效性參考，同時也避免本院遴選之稽核委員與受稽機關發生利益衝突迴避關係，受稽機關及資安管理輔導、驗證資訊如下表：

表 1　109 年受稽機關及資安管理輔導、驗證列表

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	是否為全機關
1	僑務委員會	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 CNS27001:2014	1.資訊室 2.僑務委員會資訊系統及資訊機房	否
2	原住民族委員會	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 CNS27001:2014	1.核心資訊系統 2.原住民族委員會資訊機房	否
3	財政部	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	文書檔管系統	否

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	是否為全機關
4	國家發展委員會	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 CNS27001:2014	1. 行政院政府計畫管理資訊網 2. 公文管理系統 3. 全球資訊網、我的E政府、個人化資料自主運用平臺之開發 4. 寶慶及濟南辦公區機房 5. 行政院及所屬委員會雲端資料中心	否
5	大陸委員會	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	資訊室提供之系統開發、維運及網路維運與管理、資訊服務委外管理、機房實體環境安全控管與相關支援活動管理。	否
6	教育部	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	ISO/IEC 27001:2013	1. 畢業生流向追蹤系統 2. 大專教師資格審查	否

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	是否為全機關
					系統 3.技專校院校務資料庫系統網站 4.大專校院學生基本資料庫系統網站 5.五專展翅計畫網站 6.閩南語語言能力認證考試網站 7.直轄市及各縣市短期補習班資訊管理系統 8.教育部高級中等以下學校及幼兒園教師資格檢定考試系統 9.全國教育實習資訊平臺 10.中小學師資資料庫 11.高級中等	

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	是否為全機關
					以下學校及幼兒園教師證書核發服務系統 12.全國教師在職進修資訊網 13.教育部特殊教育通報網 14.教育部全球資訊網 15.行政資訊入口網 16.公文電子交換系統 17.教育部網頁式電子郵件系統暨垃圾郵件防制系統 18.各教育場域不適任人員通報及查詢系統 19.資訊機房活動和相關網路	

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	是否為全機關
7	勞動部	數聯資安股份有限公司	BSI 英國標準協會台灣分公司	ISO/IEC 27001:2013 CNS27001:2014	全機關	是
8	行政院人事行政總處	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 CNS27001:2014	人事資訊處提供之資料系統的開發、操作及維護，以及相關的機房和網路架構支援活動的安全管理	否
9	行政院環境保護署	安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	提供全球資訊網之開發與維護，以及網路及機房之管理。	否
10	國立故宮博物院	財團法人中華民國國家資訊基本建設產業發展協進會	BSI 英國標準協會台灣分公司	ISO/IEC 27001:2013	1. 故宮精品網路商城系統 2. 數位典藏知識庫整合型系統	否
11	中央選舉委員會	安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. 中央選舉委員會綜合規劃處 2. 選務作業管理系統及全球資訊網 3. 網路安全管理	否

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	是否為全機關
12	國家通訊傳播委員會	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	全機關	是
13	中央銀行	無	SGS 台灣檢驗科技股份有限公司	ISO/IEC 27001:2013	全部核心資訊系統 之管理、維護及運作	否
14	行政院公共工程委員會	中華電信股份有限公司數據通信分公司	BSI 英國標準協會台灣分公司	ISO/IEC 27001:2013	政府電子採購網	否
15	交通部	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	技師與工程技術顧問公司管理資訊系統	否

二、 稽核方式

採實地稽核 1 日方式進行，由本院國家資通安全會報遴選稽核委員組成稽核小組，先期審查受稽機關填復之調查表件，再至機關實地訪談及審視各稽核項目佐證文件。

三、 稽核日期

109 年度各受稽機關稽核日期如下表：

表 2　109 年各受稽機關稽核日期

編號	受稽機關	實地稽核日期
1	僑務委員會	6 月 11 日
2	原住民族委員會	6 月 23 日
3	財政部	7 月 2 日
4	國家發展委員會	7 月 8 日
5	大陸委員會	7 月 31 日
6	教育部	8 月 20 日
7	勞動部	8 月 25 日
8	行政院人事行政總處	9 月 10 日
9	行政院環境保護署	9 月 16 日
10	國立故宮博物院	9 月 29 日
11	中央選舉委員會	10 月 7 日
12	中央銀行	10 月 27 日
13	行政院公共工程委員會	11 月 4 日
14	國家通訊傳播委員會	11 月 23 日
15	交通部	11 月 30 日

四、 稽核團隊

由稽核領隊及稽核委員組成，共同執行受稽機關實地稽核；另為培訓政府機關稽核種子人員，由稽核委員輔導觀察員參與實地稽核作

業，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，得由策略面委員代理。

（二）稽核委員：由政府機關及產學研等領域資安專家共同組成，每個稽核場次安排 7 位稽核委員，包括策略面 2 位、管理面 2 位及技術面 3 位。

（三）觀察員：自本院及其所屬二級機關、直轄市政府及各縣市政府之公務人員遴選，每場次至多 2 名觀察員。

五、 稽核基準、稽核範圍與項目

資安稽核係依據資安法與其子法、參酌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含之全機關與核心資通系統之各項資安管理政策、程序等。

（二）項目及評分方式

實地稽核分策略面、管理面及技術面等 3 構面，各構面之稽核項目及配分說明，詳見表 3，總分合計 100 分。

表 3　各構面稽核項目配分

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 分		

參、 109 年度資安稽核結果

實地稽核 15 個公務機關稽核結果總分平均為 68.8 分。

一、 實地稽核成績分布

本次受稽機關中，成績 75 分以上者有 3 個機關，其餘 12 個機關成績未達 75 分，其中有 3 個機關低於 60 分，整體受稽機關成績分布，詳見圖 1。

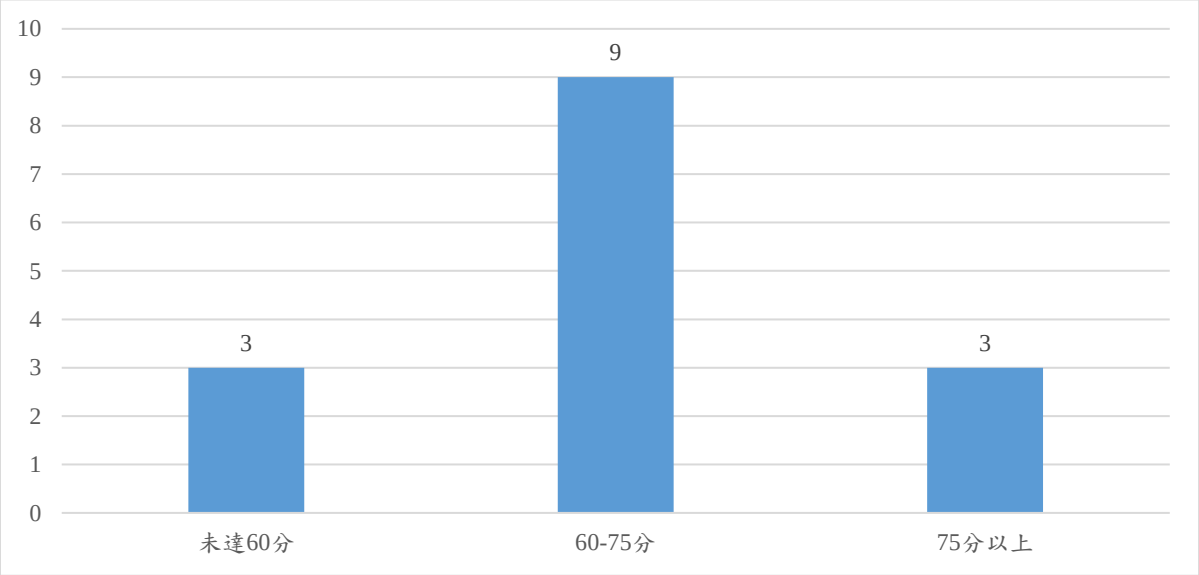

圖 1　公務機關實地稽核成績分布

實地稽核個別項目成績分布詳見圖 2，其中成績較高為「資通安全維護計畫與實施情形之持續精進與績效管理機制」、「資通安全政策及推動組織」及「資通系統或服務委外辦理之管理措施」，自資安法施行，賦予公務機關強化資通安全、降低資安風險之責任與義務，稽核發現公務機關已重視機關資安防護，由資安長帶領推動組織制定、推動及檢討資通安全維護計畫，並有良好的績效管理制度；另對機關委外業務或廠商尚能符合法遵要求並落實管控。另「核心業務及其重要性」、「資訊及資通系統盤點及風險評估」及「資通安全事件通報應變及情資評估因應」成績較低，顯示受稽機關對機關核心資通系統分級、機關內資通系統盤點完整性及風險評估處理、資安事件通報應變程序仍未落實及妥善處置。

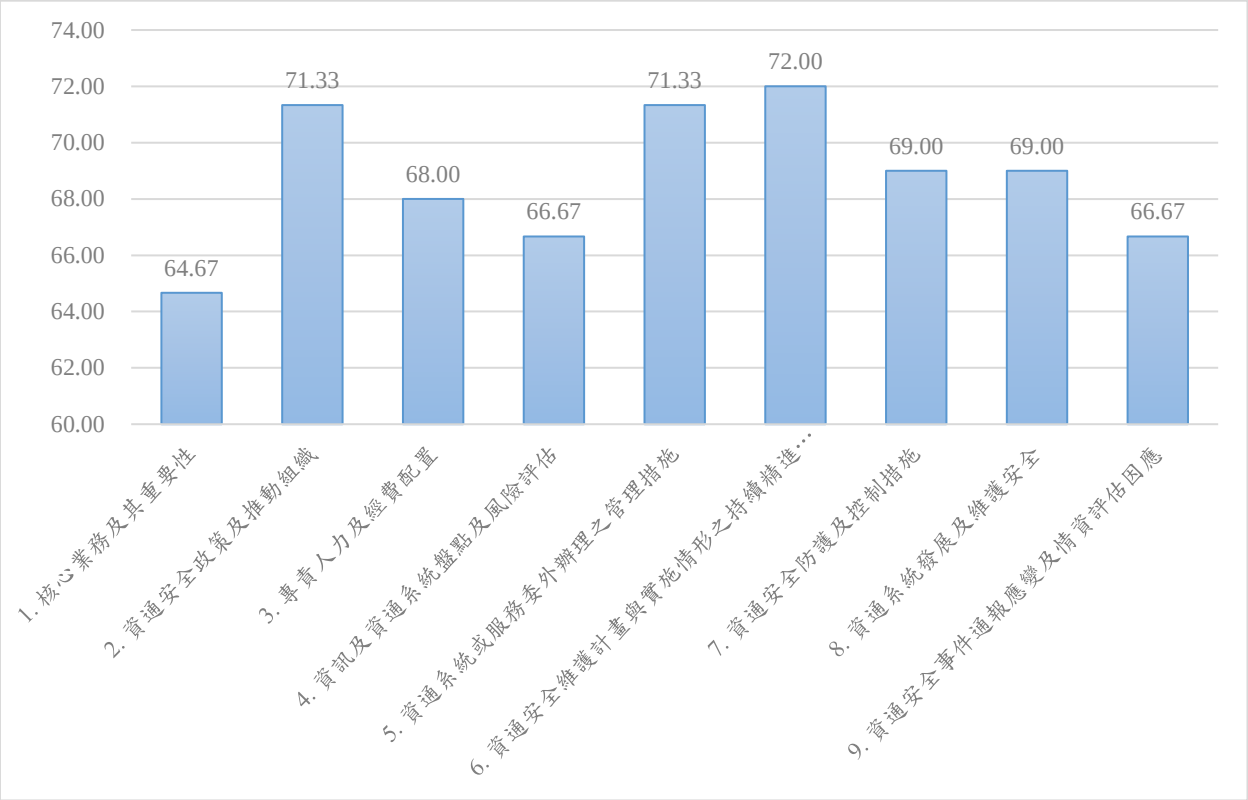

圖 2　公務機關實地稽核個別項目成績分布圖

二、 實地稽核各構面比較

實地稽核各構面(策略面、管理面及技術面)整體表現平均，詳見圖3，顯示受稽機關就稽核法遵內容並無偏重某一構面，各構面均能平衡發展，另綜合分析 A 級公務機關在各構面明顯優於 B、C 級公務機關，且 A 級機關各構面平均分數皆達 73 分以上，普遍表現良好。

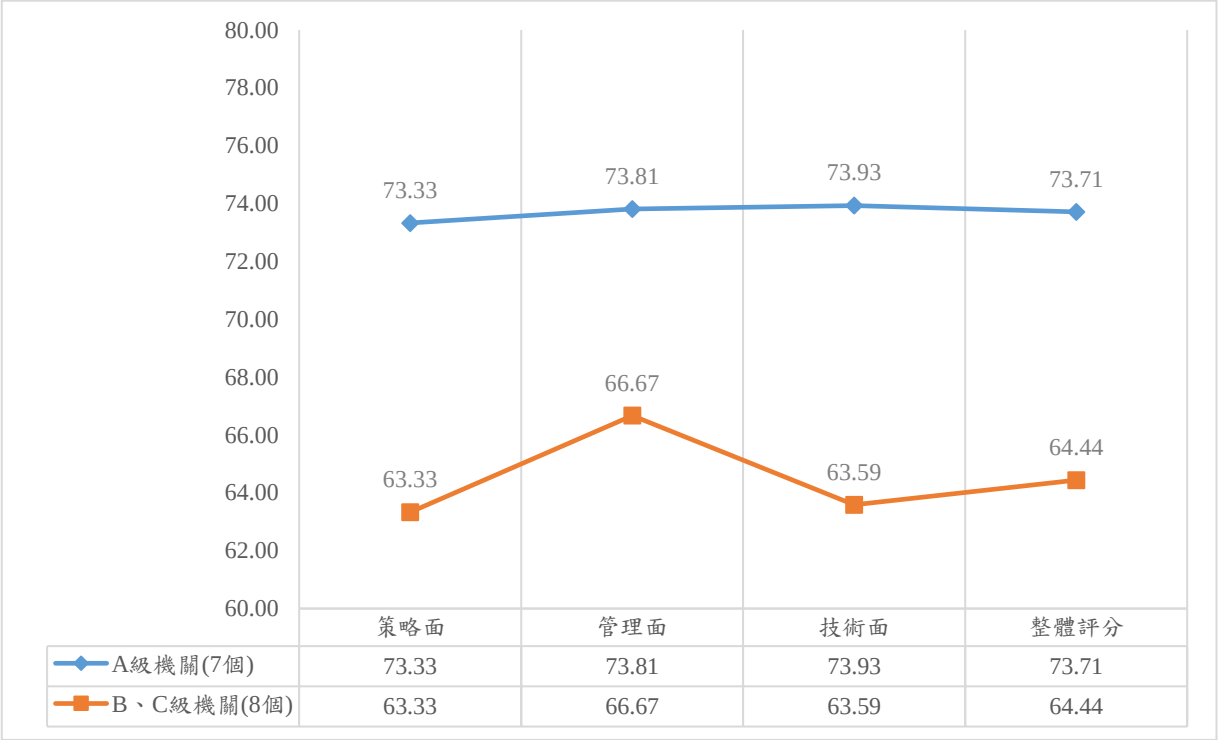

圖 3　實地稽核成績分布

三、 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 級與 B、C 級群組進行比較，顯示 A 級機關之整體表現優 B、C 級機關，A 級機關係為權責業務及所保有資料相對重要之政府機關，法遵要求應辦事項相對嚴格，稽核結果顯示受稽之 A 級機關對資安防護相對重視，此是良好現象，惟 B、C 級機關尚待加強，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 級公務機關者計有 7 個，整體平均分數為 73.7 分，其中整體評分 75 分以上有 2 個機關，其餘 5 個機關整體評分 71.4 分，成績分布，詳見圖 4。

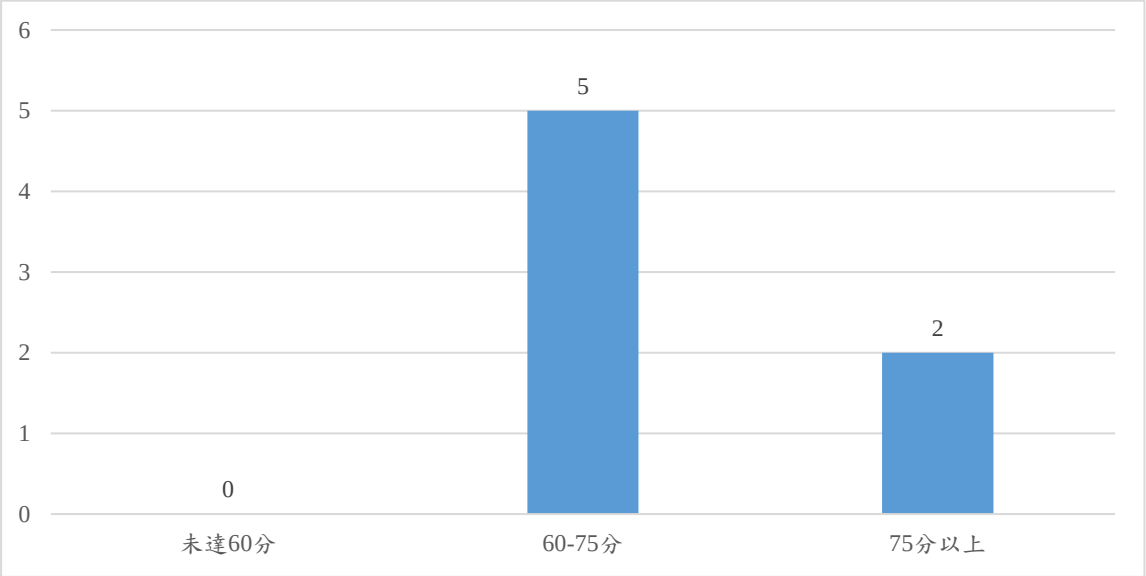

圖 4　A 級公務機關稽核整體成績

（二） 資安責任等級 B、C 級公務機關

本次受稽機關中，資安責任等級列 B、C 級者計有 8 個，整體平均分數 64.4 分，其中 75 分以上有 1 個機關，其餘 7 個機關總分未達 75 分，其中有 3 個機關低於 60 分，詳見圖 5

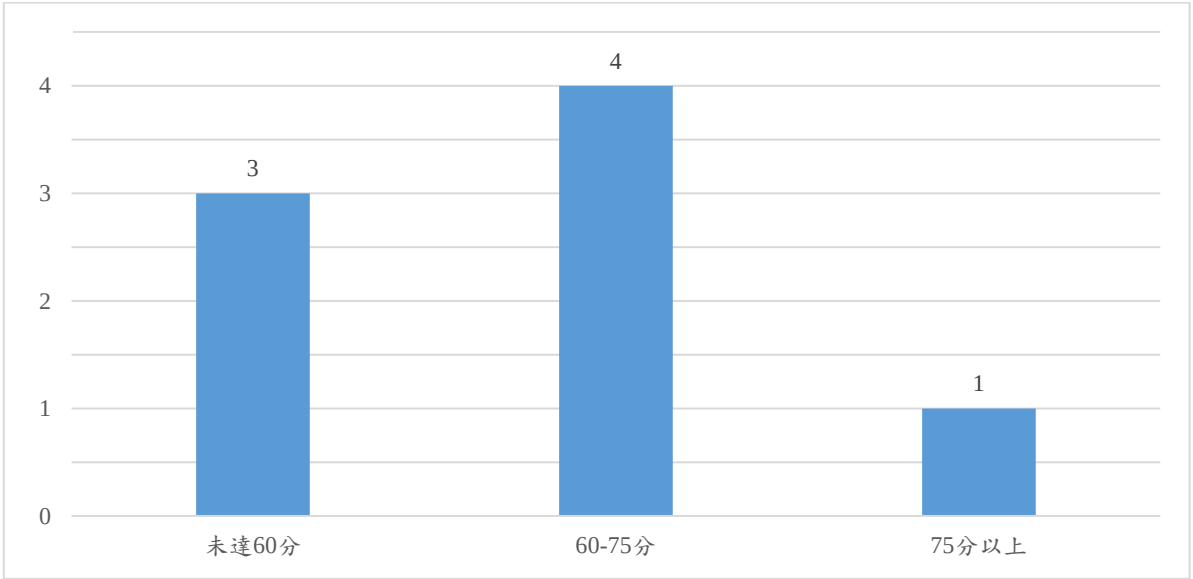

圖 5　B、C 級公務機關稽核整體成績

肆、 稽核發現

綜整 109 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、 符合資通安全責任等級分級辦法應辦事項規定，已完成核心資通系統 ISMS 導入，並通過公正第三方驗證。

2、 符合資安法施行細則第 6 條規定，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。

3、 符合資通安全責任等級分級辦法應辦事項規定，已辦理一般使用者及主管接受 3 小時以上之資通安全通識教育訓練。

（二） 管理面

1、 符合資安法施行細則第 6 條規定，已訂定風險管理程序文件，建立風險評估準則、衝擊準則及風險接受準則，並執行資通安全風險評估作業。

2、 符合資安法施行細則第 4 條規定，針對委外客製化資通系統，於系統驗收前要求委外廠商提供資通安全檢測證明，另部分資通系統由委託者自行或委託第三方進行安全性檢測。

3、 符合資安法施行細則第 6 條規定，已依法訂定資通安全維護計畫，且每年向上級提出實施情形。

（三） 技術面

1、 符合資通安全責任等級分級辦法應辦事項規定，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、 部分機關優於資通安全責任等級分級辦法資通系統防護基準規

定，針對所有委外資通系統源碼進行掃描安全檢測。

3、符合資通安全事件通報及應變辦法第 9 條規定，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

以下就實地稽核結果提出共同發現待改善事項。

（一） 策略面

1、未依資安法施行細則第 6 條及第 7 條規定，有效落實核心業務與核心資通系統之界定，且部分機關之資通安全維護計畫與實施情形之填報內容有所差異。

2、未依資通安全事件通報及應變辦法第 9 條規定，完整建立機關內、外部利害關係人清單，並定期檢討其適宜性。

3、未依資通安全責任等級分級辦法應辦事項規定，資通安全相關法遵、資安威脅趨勢及技術知能要求與日俱增，惟部分機關受限資安人力資源，未配置資安專職/責人力。

（二） 管理面

1、依資安法施行細則第 6 條規定，已辦理資訊資產盤點並建立資產清冊，惟盤點範圍與內容完整性不足。

2、未依資安法施行細則第 4 條規定，規劃與落實資訊委外作業(如委外廠商選任要求、防護基準納入 RFP、安全檢測、通報程序等)。

3、依資通安全責任等級分級辦法應辦事項規定，已規劃並執行資通安全內部稽核作業，惟部分機關稽核對象未涵蓋全機關，且稽核項目未完整納入資安法應辦事項。

（三） 技術面

1、依資通安全責任等級分級辦法應辦事項規定，部分機關網路架構安全性仍顯不足，如網段區隔與存取控管未確實。

2、依資通安全責任等級分級辦法應辦事項規定，已進行網站安全性檢測、滲透測試及資通安全健診等作業，惟未訂定相關作業程序進行後續追蹤。

3、未依資通安全責任等級分級辦法資通系統防護基準規定，將資通系統安全開發程序納入資通系統防護需求。

4、依資通安全事件通報及應變辦法第 8 條規定，已辦理資安事件通報與應變演練，惟未納入事件通報環節，另建議將新興資安議題或事件納入演練情境。

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如下：

（一） 策略面

1、機關應依資安法施行細則第 6 條及第 7 條規定，明確界定應保護之標的，且依不同防護需求等級之資通系統施予防護控制措施，相關作業包含界定機關核心業務，盤點各單位之資通系統，並包括業務營運之資通系統、輔助系統等。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並達成法規要求之防護作業。

2、依資通安全事件通報及應變辦法第 9 條規定，應完善資通安全事件通報窗口及聯繫方式資訊，包含機關內部、外部利害關係人(如上級／監督機關、所屬／所管機關、合作機關、IT 服務供應商及民間等)。

3、機關應依資通安全責任等級分級辦法應辦事項規定，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，優先調配資安專責人員，並結合資安專業訓練、證照及職能訓練證書，培養

機關所需之資安專業人力。

（二） 管理面

1、 依資安法施行細則第6條規定,機關應落實盤點資訊及資通系統,並標示核心資通系統及相關資產。

2、 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，皆應於管理程序明確制訂，並落實於與廠商之合約規範。

3、 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、範圍等是否妥適，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，及有效管考內部稽核發現事項之改善情形。

（三） 技術面

1、 依資通安全責任等級分級辦法應辦事項規定，機關網路架構應清楚界定並規劃不同需求屬性之區域，且依業務屬性設定內部人員可存取網段，並定期檢視網路架構安全及存取授權。

2、 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，機關資安健診作業應訂定內部資安作業程序，包括何人實施、實施標的(涵蓋範圍)、何時實施、如何實施(工具、方法等)、及實施結果之改善(改善機制、改善時程)，以確保機關之安全防護。

3、 應依資通安全責任等級分級辦法資通系統防護基準之「系統與服務獲得」構面，重新檢視系統發展生命週期(SSDLC)於需求、設計、開發、測試、部署與維運等階段之各項安全要求，並落實資

通系統防護需求等級對應之防護基準。

4、 依資通安全事件通報及應變辦法規定，應訂定資安事件通報/應變作業規範，公務機關每年應辦理 1 次之資安事件通報及應變演練。

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。

資安稽核之目的在確保機關落實資安法法遵事項，並透過外部檢視方式發掘機關資安盲點，以強化機關資安防護，從而降低資安風險及危害；而各受稽機關評比分數、排序及獎勵機制，為本院對各機關落實並精進資安防護作為之激勵誘因，並使本院能經相對比較後確實掌握各所屬機關資安防護狀況之良窳，俾作為後續辦理資安強化輔導擇選對象之參考。

本院持續蒐整研析國、內外重大資安威脅情勢，將對應之資安防護措施納入稽核重點項目，於資安稽核實地檢視機關對本院資安政策落實情形；另依資安法分層監督管理原則，本院藉由第二方稽核輔導機制，強化上級機關對其所屬或監督機關第二方稽核能量，以維護國家整體資通安全發展環境。