特定非公務機關資通安全維護計畫實施情形稽核辦法

第一條　本辦法依資通安全管理法（以下簡稱本法）第七條第二項規定訂定之。

第二條　本辦法所定書面，依電子簽章法之規定，得以電子文件為之。

第三條　主管機關應每年擇定當年度各季受稽核之特定非公務機關（以下簡稱受稽核機關），並以現場實地稽核之方式，稽核其資通安全維護計畫實施情形。

主管機關擇定前項受稽核機關時，應綜合考量其業務之重要性與機敏性、資通系統之規模與性質、資通安全事件發生之頻率與程度、資通安全演練之成果、歷年受主管機關或中央目的事業主管機關稽核之頻率與結果或其他與資通安全相關之因素。

主管機關為辦理第一項稽核，應訂定稽核計畫，其內容包括稽核之依據與目的、期間、重點領域、稽核小組組成方式、保密義務、稽核方式、基準與項目及中央目的事業主管機關協助事項。

主管機關決定前項稽核之重點領域與基準及項目時，應綜合考量我國資通安全政策、國內外資通安全趨勢、過往稽核計畫之內容與稽核結果，及其他與稽核資源之適當分配或稽核成效相關之因素。

第四條　主管機關辦理前條第一項之稽核，應將稽核計畫於一個月前以書面通知受稽核機關。

受稽核機關如因業務因素或有其他正當理由，得於收受前項通知後五日內，以書面敘明理由向主管機關申請調整稽核日期。

前項申請，除有不可抗力之事由外，以一次為限。

第五條　主管機關辦理第三條第一項之稽核，得要求受稽核機關為資通安全維護計畫實施情形之說明、協力或提出相關之文件、證明資料供現場查閱，並執行下列事項，受稽核機關及其所屬人員應予配合：

一、稽核前訪談。

二、現場實地稽核。

受稽核機關依法律有正當理由，未能為前項說明、協力或提出資料供現場查閱者，應以書面敘明理由，向主管機關提出。

主管機關收受前項書面後，應進行審核，依下列規定辦理，並得停止稽核作業之全部或一部：

一、認有理由者，應將審核之依據及相關資訊記載於稽核結果報告。

二、認無理由者，應要求受稽核機關依第一項規定辦理；已停止稽核作業者，得擇期續行辦理，並於十日前以書面通知受稽核機關。

第六條　主管機關辦理第三條第一項之稽核，應依同條第二項所定考量因素，就各受稽核機關分別組成三人至七人之稽核小組。

主管機關組成前項稽核小組時，應考量稽核之需求，邀請具備資通安全政策或該次稽核所需之技術、管理、法律或實務專業知識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得少於全體成員人數之三分之一。

主管機關應以書面與稽核小組成員約定利益衝突之迴避及保密義務。

第二項之公務機關代表或專家學者，有下列情形之一者，應主動迴避擔任該次稽核之稽核小組成員：

一、本人、其配偶、三親等內親屬、家屬或上開人員

財產信託之受託人，與受稽核機關或其負責人間有財產上或非財產上之利害關係。

二、本人、其配偶、三親等內親屬或家屬，與受稽核機關或其負責人間，目前或過去二年內有僱傭、承攬、委任、代理或其他類似之關係。

三、本人目前或過去二年內任職之機關（構）或單位，曾為受稽核機關之顧問，其輔導項目與受稽核項目相關。

四、其他情形足認擔任稽核小組成員，將對稽核結果之公正性造成影響。

第七條　主管機關應於每季所定受稽核機關之稽核作業完成後一個月內，將稽核結果報告交付該季受稽核機關。

前項稽核結果報告之內容，應包括稽核之範圍、缺失或待改善事項、第五條第二項所定受稽核機關未能為說明、協力或提出資料供現場查閱之情形、理由與同條第三項所定主管機關審核結果，及其他與稽核相關之必要內容。

第八條　受稽核機關經發現其資通安全維護計畫實施情形有缺失或待改善者，應於主管機關交付稽核結果報告後一個月內，依主管機關指定之方式提出改善報告，並送交中央目的事業主管機關；主管機關及中央目的事業主管機關認有必要時，得要求該受稽核機關進行說明或調整。

前項受稽核機關提出改善報告後，應依主管機關指定之方式及時間，提出改善報告之執行情形，並送交中央目的事業主管機關；主管機關認有必要時，得要求該受稽核機關進行說明或調整。

第九條　主管機關辦理第三條第一項之稽核，得要求受稽核機關之中央目的事業主管機關派員為必要協助。

第十條　本辦法之施行日期，由主管機關定之。