資通安全維護計畫實施情形稽核辦法修正條文

第 一 條　本辦法依資通安全管理法（以下簡稱本法）第八條第四項及第十六條第三項規定訂定之。

第 二 條　公務機關之資通安全維護計畫，應依本法施行細則第九條第一項規定辦理。

公務機關依本法第十四條提出資通安全維護計畫實施情形，應依本法施行細則第九條第二項規定辦理。

第 三 條　公務機關應至主管機關指定之系統平臺，提出資通安全維護計畫實施情形。但有特殊情形者，得經主管機關同意以其他適當方式為之。

第 四 條　本法第十四條規定收受資通安全維護計畫實施情形之公務機關，對其所屬、所監督之公務機關、所轄鄉（鎮、市）公所、直轄市山地原住民區公所及鄉（鎮、市）民代表會、直轄市山地原住民區民代表會之資通安全維護計畫實施情形，應每年訂定稽核計畫，並掌握稽核情形。

第 五 條　主管機關得每年擇定受稽核之公務機關及特定非公務機關，並以實地稽核或其他適當之方式，稽核其資通安全維護計畫實施情形。

公務機關除因不可抗力因素外，應每年擇定其所屬、所監督之公務機關、所轄鄉（鎮、市）公所、直轄市山地原住民區公所及鄉（鎮、市）民代表會、直轄市山地原住民區民代表會，並以實地稽核或其他適當之方式，稽核其資通安全維護計畫實施情形。

第 六 條　主管機關及公務機關（以下合稱稽核機關）擇定受稽核機關時，應綜合考量其業務之重要性與機敏性、資通系統之規模及性質、資通安全事件發生之頻率及程度、資通安全演練之成果、歷年受主管機關、本法第十四條規定收受其資通安全維護計畫實施情形之公務機關、中央目的事業主管機關或其他業務相關機關稽核之頻率及結果或其他與資通安全相關之因素。

本法第八條第五項所定年度計畫，及第四條所定稽核計畫，其內容至少包括下列事項：

一、稽核依據。

二、稽核目的。

三、稽核範圍。

四、作業期程。

五、稽核小組組成方式。

六、保密義務。

七、受稽核機關遴選原則。

八、稽核基準。

九、稽核方式及項目。

稽核機關訂定前項年度計畫或稽核計畫時，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 七 條　稽核機關辦理稽核時，應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，以書面敘明理由向前項稽核之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 八 條　稽核機關辦理稽核時，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、證明資料供稽核小組查閱，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、實地稽核或其他適當之稽核方式。

受稽核機關依法律有正當理由，未能為前項說明、協力或提出資料供稽核小組查閱者，應以書面敘明理由，向前項稽核之機關提出，該機關收受書面後，應進行審核。

第一項稽核機關進行前項審核，認有理由時，應將審核之依據及相關資訊記載於稽核結果報告，並得停止稽核作業之全部或一部；認無理由時，應要求受稽核機關依第一項規定辦理。經停止稽核作業者，第一項稽核機關得擇期續行辦理，並於十日前以書面通知受稽核機關。

第 九 條　稽核機關辦理稽核時，應依第六條第一項所定考量因素，就各受稽核機關分別組成三人以上之稽核小組。

稽核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四分之一。

稽核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，與受稽核機關或其代表人、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，與受稽核機關或其代表人、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 十 條　稽核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、第八條第二項所定受稽核機關未能為說明、協力或

提出資料供稽核小組查閱之情形、理由與同條第三項所定稽核機關審核結果，及其他與稽核相關之必要內容。

第十一條　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，應於稽核機關交付稽核結果報告後一個月內，依本法施行細則第六條第一項規定提出改善報告，送交本法第十四條規定收受其資通安全維護計畫實施情形之公務機關，或其中央目的事業主管機關審查後，由該審查機關送交主管機關。其中屬依第五條第二項辦理之稽核，審查機關應連同稽核結果送交主管機關。

受稽核機關提出改善報告後，應依本法施行細則第六條第二項規定，提出改善報告之執行情形，送交本法第十四條規定收受其資通安全維護計畫實施情形之公務機關或中央目的事業主管機關審查後，由該審查機關送交主管機關。

第一項收受改善報告及前項收受改善報告執行情形之機關認有必要時，得要求該受稽核機關進行說明或調整。

第十二條　主管機關辦理稽核時，得要求本法第十四條、第二十條第三項、第二十一條第二項規定收受資通安全維護計畫實施情形之機關派員或為其他必要之協助。

第十三條　本辦法所定資通安全維護計畫實施情形之稽核、改善報告之提出及其他相關事項，主管機關得委任所屬數位發展部資通安全署辦理之。

第十四條　本辦法自發布日施行。