

特定非公務機關資通安全維護計畫實施情形稽核 辦法草案總說明

「資通安全管理法」(以下簡稱本法)業於一百零七年六月六日制定公布。依本法第七條第二項規定，主管機關得稽核特定非公務機關之資通安全維護計畫實施情形；其稽核之頻率、內容與方法及其他相關事項之辦法，由主管機關定之。為強化主管機關對於特定非公務機關之監督及管理，並協助特定非公務機關發現其資通安全維護之缺漏，以適時進行修正，提升其資通安全防護能量，爰依前開規定擬具「特定非公務機關資通安全維護計畫實施情形稽核辦法」(以下簡稱本辦法)草案，其要點如下：

- 一、本辦法之授權依據。(草案第一條)
- 二、本辦法之書面，依電子簽章法之規定，得以電子文件為之。(草案第二條)
- 三、主管機關應每年擇定當年度受稽核之特定非公務機關辦理稽核，擇定受稽核機關之考量因素，及稽核計畫之內容。(草案第三條)
- 四、主管機關辦理稽核之通知及日期調整。(草案第四條)
- 五、受稽核機關就主管機關之稽核應配合之事項。(草案第五條)
- 六、稽核小組之組成與利益迴避及保密義務。(草案第六條)
- 七、稽核結果報告之內容及交付時程。(草案第七條)
- 八、受稽核機關改善報告及其執行情形之提出方式及時程。(草案第八條)
- 九、主管機關得要求受稽核機關之中央目的事業主管機關協助辦理稽核。
(草案第九條)
- 十、本辦法之施行日期。(草案第十條)

特定非公務機關資通安全維護計畫實施情形 稽核辦法草案

條文	說明
<p>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。</p>	<p>明定本辦法訂定之依據。</p>
<p>第二條 本辦法所稱書面，依電子簽章法之規定，得以電子文件為之。</p>	<p>明定本辦法所定書面，得以電子文件為之。</p>
<p>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），並以現場實地查核之方式，稽核其資通安全維護計畫實施情形。</p> <p>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。</p> <p>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。</p> <p>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。</p>	<p>一、第一項明定主管機關稽核特定非公務機關資通安全維護計畫實施情形之頻率。</p> <p>二、為有效利用稽核資源，提升稽核成效，爰於第二項明定主管機關擇定受稽核機關時應綜合考量之因素，以決定最適之受稽核機關名單。</p> <p>三、第三項明定主管機關為辦理第一項之稽核，應訂定稽核計畫及其內容應包括之事項。</p> <p>四、為使稽核作業能切合我國資通安全政策之規劃內容，並適時反映國內外資通安全相關趨勢，強化稽核資源分配與成效，爰於第四項明定主管機關於訂定稽核計畫，決定稽核之重點領域與基準及其項目時，應綜合考量之因素。</p>
<p>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以前以書面通知受稽核機關。</p> <p>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。</p> <p>前項申請，除有不可抗力之事由外，以一次為限。</p>	<p>一、為避免主管機關辦理稽核影響受稽核機關之日常業務，並使受稽核機關有充裕時間預為準備，以增進稽核效能，爰於第一項明定主管機關應於實際辦理稽核之一個月前，以書面通知受稽核機關。</p> <p>二、考量受稽核機關可能有因業務因素或其他正當理由，難以依主管機關所定日期配合稽核之情形，爰於第二項及第三項明定於此情形，受稽核機關得於收受第一項通知後</p>

	<p>五日內，以書面敘明理由向主管機關申請調整稽核日期，其申請除有不可抗力之事由外，以一次為限。</p>
<p>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或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：</p> <p>一、稽核前訪談。</p> <p>二、現場實地稽核。</p> <p>受稽核機關依法律有正當理由，不能為前項說明、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。</p>	<p>一、本法第七條第二項明定主管機關得稽核特定非公務機關之資通安全維護計畫實施情形，並授權主管機關就稽核之頻率、內容與方法及其他相關事項之辦法，依其立法說明，係為監督特定非公務機關實施資通安全維護計畫之情形。從上開法律規定及立法理由整體觀察，足認受稽核之特定非公務機關有配合主管機關辦理稽核之義務，主管機關並應就稽核之內容、方法等相關事項訂定規範，以利實務執行，爰於第一項明定主管機關辦理第三條第一項之稽核時得要求受稽核機關配合之事項，以利主管機關藉由稽核確認受稽核機關遵循本法之情形。</p> <p>二、受稽核機關如依法律有正當理由，不能為第一項之說明、配合措施或提供資料，例如提供資料將侵害第三人之正當權利，此時受稽核機關應以書面敘明其理由，向主管機關提出，俾利主管機關依第七條第二項規定記載於稽核結果報告或其他相關紀錄，爰為第二項規定。</p>
<p>第六條 主管機關為辦理第三條第一項之稽核，應依第三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。</p> <p>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。</p> <p>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。</p> <p>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：</p>	<p>一、為使主管機關對不同之特定非公務機關均得妥適辦理其資通安全維護計畫實施情形之稽核，爰於第一項明定主管機關應考量相關因素，就各受稽核機關分別組成稽核小組。</p> <p>二、考量稽核小組成員需具備之知能，於第二項明定主管機關組成稽核小組時應邀請之人員，以協助主管機關進行稽核及提供專業意見。另為確保稽核結果之公平性，明定公務機關代表不得少於稽核小組全體成員人數之三分之一。</p> <p>三、為保障受稽核機關之權益，爰於第三項明定主管機關應以書面與稽</p>

<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>	<p>核小組成員約定利益衝突之迴避及保密義務。</p> <p>四、為確保稽核結果之客觀性及避免爭議，爰於第四項明定第二項之公務機關代表或專家學者應主動迴避擔任稽核小組成員之情形。</p>
<p>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。</p> <p>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、第五條第二項受稽核機關無法為說明、協力或提出資料供現場查閱之情形與理由，及其他與稽核相關之必要內容。</p>	<p>一、第一項明定主管機關應於每季所定受稽核機關之稽核作業均辦理完成後之一個月內，將稽核結果報告交付該季受稽核機關。</p> <p>二、第二項明定稽核結果報告應記載之內容。</p>
<p>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之一個月內，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。</p> <p>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；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。</p>	<p>依本法第七條第三項規定，特定非公務機關受主管機關稽核，經發現其資通安全維護計畫實施有缺失或待改善者，應向主管機關提出改善報告，並送中央目的事業主管機關。為利執行，爰於第一項明定受稽核機關應提出改善報告之期限及程序，並於第二項明定應提出改善報告之執行情形，俾利主管機關及中央目的事業主管機關進行後續之監督。有關改善報告應包括之內容，則係於本法施行細則第三條規範之。</p>
<p>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。</p>	<p>明定主管機關辦理第三條第一項之稽核時，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，以利順利執行稽核，並使中央目的事業主管機關亦得知悉受稽核機關之資通安全維護實施情形。</p>

第十條 本辦法之施行日期，由主管機關定之。	明定本辦法之施行日期，由主管機關定之。
-----------------------	---------------------