

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，為強化主管機關對於特定非公務機關之監督與管理，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，提升其資通安全防护能量，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。為訂定稽核之頻率、內容與方法及其他相關事項，爰擬具「特定非公務機關資通安全維護計畫實施情形稽核辦法」草案，其要點如下：

- 一、本辦法之授權依據。(草案第一條)
- 二、本辦法之書面得以電子文件為之。(草案第二條)
- 三、受稽核機關之擇選及其考量因素、稽核計畫之內容應載明事項。(草案第三條)
- 四、稽核之通知及期程調整規定。(草案第四條)
- 五、受稽核機關之配合事項。(草案第五條)
- 六、稽核小組之組成及利益迴避與保密義務之規定。(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、改善報告之提出方式及時程。(草案第八條)
- 九、受稽核機關之中央目的事業主管機關協助稽核作業之義務。(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，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>主管機關為辦理前項稽核，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>主管機關決定第一項受稽核機關時，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、程度與潛在風險、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之稽核頻率、結果或其他與資通安全相關之因素。</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及方式。</p> <p>二、第二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>三、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，爰於第三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>四、為有效利用稽核資源，提升稽核成效，爰於第四項明定主管機關於訂定稽核計畫，決定受稽核機關時，應綜合考量之因素，以決定最適之受稽核機關名單。</p>
<p>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通知受稽核機關。</p> <p>受稽核機關如因業務因素或其他正當理由，得於收受前項通知五日內，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，受稽核機關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，通知受稽核機關。</p> <p>二、若受稽核機關因業務等因素，難以配合稽核者，得於收受前項通知五日內，以書面敘明理由向主管機關申請調整稽核日期，並原則以一次</p>

	<p>為限，爰為第二項及第三項之規定。</p>
<p>第五條 主管機關辦理第三條第一項之稽核，得要求受稽核機關之人員為資通安全維護計畫實施情形相關之說明、配合措施或現場提供相關之文件或證明資料，並執行下列事項：</p> <p>一、稽核前訪談。</p> <p>二、現場實地稽核。</p> <p>受稽核機關如依法律有正當理由，不能為前項說明、配合措施或提供資料時，應以書面敘明理由，向主管機關提出。</p>	<p>一、第一項明定主管機關辦理第三條第一項之稽核時，受稽核機關之配合義務內容，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，而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，應依第三條第四項擇定受稽核機關時之考量因素，就各受稽核機關，分別組成三至七人之稽核小組。</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與保密義務。</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、本人、其配偶、三親等內親屬或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間曾有僱傭、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曾任職之機關(構)或單位，曾為受稽核機關進行與受稽核項目相關之顧問</p>	<p>一、為使主管機關得妥適辦理對各不同場次之特定非公務機關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組成稽核小組。</p> <p>二、考量稽核小組所需具備之知能，爰於第二項明定主管機關組成稽核小組時，所邀請之公務機關代表或專家學者應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，以協助主管機關進行稽核及提供專業意見。且為確保稽核結果之公平性，爰明定公務機關代表於稽核小組之人數占比應至少為三分之一。</p> <p>三、為保障受稽核機關之權益，爰於第三項規明定稽核小組之利益衝突迴避與保密義務，且主管機關應與其等進行書面約定。</p> <p>四、為確保稽核結果之客觀性，以及避免爭議，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之情形。</p>

<p>輔導。</p> <p>四、有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疑義者。</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，應包含稽核之範圍、缺失或待改善事項、第五條第二項受稽核機關無法為必要說明、配合措施或提供資料之情形與理由，及其他相關之必要內容。</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，依指定之方式，向主管機關提出改善報告，並送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。如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>一、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，爰明定受稽核機關經發現其資通安全維護計畫實施有缺失或待改善之情形，應提出改善報告之程序，並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。</p> <p>二、為使受稽核機關提出改善報告之內容更為明確，爰於本法施行細則第三條明定該改善報告應包含之內容等相關事項。</p>
<p>第九條 主管機關辦理第三條第一項之稽核時，得指定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，以利稽核之成效，並有助中央目的事業主管機關知悉受稽核機關之資通安全維護情形。</p>
<p>第十條 本辦法之施行日期，由主管機關定之。</p>	<p>明定本辦法之施行日期，由主管機關定之。</p>