# 特定非公務機關資通安全維護計畫實施情形稽核辦法-英譯對照

| 特定非公務機關資通安全維護計畫實施情形稽核辦法 | Regulations on Audit of Implementation of Cyber Security Maintenance Plan of Specific Non-Government Agency |
|---|---|
| 第一條　本辦法依資通安全管理法第七條第二項規定訂定之。 | Article 1 These Regulations are stipulated in accordance with Paragraph 2 of Article 7 of the Cyber Security Management Act. |
| 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。 | Article 2 These Regulations stipulate “in writing” document may be an electronic document in accordance with the provisions of the Electronic Signatures Act. |
| 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。<br>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。<br>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。<br>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。 | Article 3 The competent authority shall select and determine the specific non-government agencies (hereinafter referred to as the “audited agency”) for each quarter of the year, and may audit the implementation of their cyber security maintenance plans through onsite audit every year.<br>In selecting and determining the audited agencies under the preceding paragraph, the competent authority shall give comprehensive consideration to the significance and confidential sensitivities of its businesses, the size and nature of their cyber systems, the frequencies and degrees of occurrence of cyber security incidents, the results of cyber offense and defense exercise, the frequencies and results of audits conducted by the competent authority or the central authority in charge of the relevant industry over past years, or other factors relating to cyber security.<br>In conducting the audit under Paragraph 1, the competent authority shall establish the audit program, the content of which shall include the basis and purposes, time period, essential fields of the audit, the manner of formation of the audit team, confidentiality obligation, the method, standards and items of the audit, and assistance issues from the central authority in charge of relevant industry.<br>In determining the essential fields, standards and items of the audit under the preceding paragraph, the competent authority shall take into comprehensive consideration the cyber security policy of our country, domestic and foreign cyber security trends, the contents |

| | |
|---|---|
| | and results of past audit programs, and any other factors relating to the proper allocation of audit resources or audit effectiveness. |
| 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。<br>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。<br>前項申請，除有不可抗力之事由外，以一次為限。 | Article 4　In conducting the audit under Paragraph 1of the preceding article, the competent authority shall deliver the audit program notice in writing to the audited agency one month before the audit.<br>Due to business factor or other justifiable reason, the audited agency may apply to the competent authority for adjustment of the audit date within five days of the receipt of the preceding notice in writing.<br>The preceding application is limited to one time except for the case of force majeure. |
| 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：<br>一、稽核前訪談。<br>二、現場實地稽核。<br>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。<br>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：<br>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。<br>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。 | Article 5　In conducting the audit under Paragraph 1 of Article 3, the competent authority may require the audited agency to give explanations on, to collaborate the implementation of cyber security maintenance plan, or provide relevant documents and supporting information for onsite inspection, and conduct the following issues. The audited agency and its personnel shall cooperate accordingly:<br>1. Pre-audit interview.<br>2. Onsite physical audit.<br>The audited agency cannot give the explanations, collaborate or provide documentation for onsite inspector under the preceding paragraph for justifiable reasons under the law, they shall submit the reasons in writing to the competent authority.<br>Upon receipt the preceding notice in writing, the competent authority shall verify it and then take the following actions, and may suspend all or part of the audit operations:<br>1. If the reasons are considered justifiable, it shall record the accordance and relevant information in the audit report.<br>2. If the reasons are considered groundless, it shall require the audited agency to follow the requirements of Paragraph 1; if the audit operations have been |

| | |
|---|---|
| | suspended, it may select other time periods to continue the audit and deliver the audit program notice in writing to the audited agency ten days before the audit. |
| 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。<br>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。<br>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。<br>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：<br>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。<br>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。<br>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。<br>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。 | Article 6　In conducting the audit under Paragraph 1 of Article 3, the competent authority shall form an audit team composed of three to seven persons respectively for each audited agency, depending on the considerations under Paragraph 2 of the same article.<br>Informing the audit team under the preceding paragraph, the competent authority shall, taking the needs of the audit into consideration, invite representatives of government agencies or experts and scholars who have professional knowledge of cyber security policies or have professional knowledge of technologies, managements, law affairs required for such audit to act as members of such team, of which the number of representatives of the government agency may not be less than one-third of all members.<br>The competent authority shall sign, in writing, with members of audit teams on recusal due to interest conflicts and confidentiality obligations.<br>If the member of audit team under Paragraph 2 has any of the following circumstances, he shall avoid himself from acting as the member of that audit team:<br>1. He, his spouse, his relatives within the third degree, his family member, or the trustee of the property trusts of above-mentioned persons have a property or non-property interest relationship with the audited agency or the responsible person thereof.<br>2. He, his spouse, his relatives within the third degree or his family member has employment, contract, appointment, agency or other similar relationship with the audited agency or the responsible person in the current or the past two years.<br>3. He has served in the current or past two years to be a consultant of the audited agency and his mentoring project is related to the audit program.<br>4. Other circumstance that may be considered that his role |

| | |
|---|---|
| | as a member of the audit team might affect the impartiality of the audit result. |
| 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。<br>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。 | Article 7　The competent authority shall, within one month after the completion of the audit operations on the audited agency as designated for each quarter, deliver the audit reports to the audited agencies for the quarter.<br>The contents of the preceding audit reports shall include the scope of the audit, flaws or items to be improved, the status and reasons for the failures of the audited agency to give explanations, collaborate or provide documentations for on-site inspections under Paragraph 2 of Article 5, and the audit results of the competent authority under Paragraph 3 of the same article, and other necessary contents relating to the audit. |
| 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。<br>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。 | Article 8　If flaws or items to be improved are found in the implementation of the cyber security maintenance plan, the audited agency shall submit improvement report in the manner specified by the competent authority within one month after the competent authority has delivered the audit report, and shall deliver the same to the central authority in charge of the relevant industry. The competent authority and the central government authority in charge of the subject industry may require the audited agency to give explanations or make adjustments when necessary.<br>After the improvement reports are submitted under the preceding paragraph, the audited agency shall submit the implementation status of the improvement reports in the manner and within the timeframe specified by the competent authority, and shall deliver the same to the central authority in charge of the relevant industry. The competent authority may require the audited agency to give explanations or make adjustments when necessary. |
| 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。 | Article 9　In conducting the audit under Paragraph 1 of Article 3, the competent authority may require the central authority in charge of the relevant industry with the audited agency to dispatch personnel for necessary assistance. |

| | |
|---|---|
| 第十條　本辦法之施行日期，由主管機關定之。 | Article 10　The date for enforcement of these Regulations shall be decided by the competent authority. |