Content

Title：	Regulations Governing Cyber Security Management for Specific Non-Government Agencies Supervised by Ministry of Finance Ch
Date：	2026.08.27
Legislative：	1.Promulgated by the Ministry of Finance on March 26, 2019, under Decree No.1081001059A. 2.Amended by the Ministry of Finance on August 27, 2026, under Decree No. 1150003104A.
Content：	Chapter One General Principles Article 1 These Regulations are enacted pursuant to the provisions of Article 22 of the Cyber Security Management Act (hereinafter referred to as the Act). Chapter Two Necessary Matters for the Implementation of the Cyber Security Maintenance Plan Article 2 The cyber security maintenance plan of the specific non-government agency regulated by the Ministry of Finance (hereinafter referred to as the Ministry) shall be conducted pursuant to the provisions of Paragraph 1, Article 9 of the Enforcement Rules of the Act. Specific non-government agencies shall, in accordance with the provisions of Paragraph 2, Article 21 of the Act, submit reports on the implementation status of their cyber security maintenance plans. Such reporting shall be conducted pursuant to the provisions of Paragraph 2, Article 9 of the Enforcement Rules of the Act. Article 3 Specific non-government agencies shall submit their annual cyber security maintenance plan for the succeeding year before the end of December each year via official document. Article 4 Specific non-government agencies shall submit reports on the implementation of their cyber security maintenance plan for the preceding year before the end of February each year via official document. Chapter Three Audit of the Implementation of Cyber Security Maintenance Plan Article 5 The Ministry shall, before the end of November each year, select specific non-government agencies for audit; onsite audits shall be conducted on the implementation of their cyber security maintenance plans.

To conduct the audit specified in the preceding paragraph, the Ministry shall establish an audit plan including, but not limited to, the following matters: the basis and purpose of the audit, the audit period, the composition method of the audit team, confidentiality obligations, the audit method, and the benchmarks and items.
When determining the benchmarks and items of the audit plan specified in the preceding paragraph, the Ministry shall comprehensively consider factors including, but not limited to, the nation's cyber security policy, domestic and international cyber security trends, past audit effectiveness, and audit resources.
When selecting specific non-government agencies to be audited (hereinafter referred to as the auditee) in accordance with the provisions of Paragraph 1, the level of cyber security responsibility, the frequency and extent of the occurrence of cyber security incidents, the results of cyber security exercises, the frequency and results of previous audits by the Ministry or other competent authorities, and other cyber security related factors shall be comprehensively considered by the Ministry.

Article 6
The Ministry, in conducting the audit under Paragraph 1 of the preceding Article, shall notify the auditee in writing of the audit plan one month prior to the audit.
Should the auditee be unable to cooperate with the audit at the specified time due to business factors or other reasonable causes, it may apply in writing to the Ministry to change the date of the audit within five days of receiving the notification.
The application to change the audit date specified in the preceding paragraph is limited to one time only, except in cases of force majeure.

Article 7
When conducting an audit, the Ministry may require the auditee to cooperate by providing relevant explanations or documents, or supporting evidence for onsite inspection. The audit execution shall include the following items:
1. Initial audit interviews;
2. Onsite audits.
If the auditee has any reasonable causes according to law and is unable to provide explanations, cooperation, or documentation, it shall state the reasons in writing and submit them to the Ministry.
Upon receiving the written documents mentioned above, the Ministry shall conduct an examination of the documents and in accordance with the following provisions may cancel all or part of the audit operations:
1. If the reasons are deemed sufficient, the basis of the audit and relevant information shall be recorded in the audit report.
2. If the reasons are deemed insufficient, the auditee shall be required to handle the matter in accordance with the provisions of the first paragraph.
If audit operations were suspended, they may be resumed at a selected time, and the auditee shall be notified in writing ten days prior to the resumed audit.

Article 8

To conduct the audit specified in Paragraph 1 of Article 5, the Ministry shall, in accordance with the considerations specified in Paragraph 4 of the same Article and the actual auditing requirements, form a respective audit team for each auditee.
The audit team shall consist of three to twelve members. These members shall be representatives of government agencies or experts and scholars who possess the technical, management, legal, or practical expertise required for the cyber security policy or the audit. Representatives of government agencies shall account for no less than one-third of the total number of members.
Any member of the audit team shall voluntarily recuse themselves from the audit in any of the following circumstances:
1. They, their spouse, their relatives within the third degree of kinship, their family members, or the trustee of any property trust of the aforementioned persons have a pecuniary or non-pecuniary interest in the auditee or its responsible person.
2. They, their spouse, their relatives within the third degree of kinship, or their family members currently have, or have had within the past two years, a relationship of employment, contracting, mandate, agency, or other similar relationship with the auditee or its responsible person.
3. The agency, organization, or unit where they are currently employed or were employed within the past two years has served as a consultant to the auditee on the matters related to the audited items.
4. Other circumstances sufficient to indicate that their serving as a member of the audit team will affect the impartiality of the audit results.
The Ministry shall reach a written agreement with the members of the audit team regarding recusal due to conflicts of interest and confidentiality obligations.

Article 9
Within one month after the completion of the audit, the Ministry shall deliver the audit report to the auditee.
The audit report referred to in the preceding paragraph shall include the scope of the audit, deficiencies or items requiring improvement, the circumstances and reasons under Paragraph 2, Article 7 where the auditee was unable to explain, cooperate, or provide information, and other relevant matters.
The Ministry shall collate the audit reports for the current year by the end of January of the following year and submit them to the competent authority for reference.

Article 10
Where deficiencies or areas for improvement are identified in the implementation of an auditee's cyber security maintenance plan, the auditee shall submit an improvement report to the Ministry within one month of receiving the report. The status of its implementation shall be submitted in writing in accordance with Article 6 of the Enforcement Rules of the Act. If deemed necessary, the Ministry may require the auditee to provide explanations, make adjustments, or undergo necessary re-verification.

Chapter Four Supplementary Provisions

Article 11
The written documents set out in these Regulations may be in digitized form in accordance with the provisions of the Electronic Signatures Act.

Article 12
These Regulations shall take effect as of the date of promulgation.

Data Source：Ministry of Finance, R.O.C. Laws and Regulations Retrieving System