Unofficial Translation

Readers should be aware that only the original Thai text has legal force, and that this English translation is strictly for reference.

Appendix 4

[Attached to the SEC Office Notification No. Sor Thor. 38/2565]

Information Technology Audit

A business operator shall comply with the provisions hereunder.

Operations	Details
1. Provision of an auditor	An auditor under 1 shall possess the following characteristics: 1.1 being independent from IT personnel at the following levels: 1.1.1 First Line of Defense: Operations 1.1.2 Second Line of Defense: Risk management and compliance with applicable laws and regulations related to IT operations 1.2 If it is the IT audit from 1st January 2024 onwards, the auditor shall be certified and hold any of the following certificates: 1.2.1 Certified Information Systems Auditor (CISA) 1.2.2 Certified Information Security Manager (CISM) 1.2.3 Certified Information Systems Security Professional (CISSP) 1.2.4 ISO/IEC 27001 Lead Auditor 1.2.5 Other certificates as additionally stipulated on the website of the SEC Office.
2. Audit Planning and Audit Scope Defining	The audit plan and the audit scope shall be reviewed at least once a year and upon any necessary cause requiring such review, to ensure that the scope is aligned with IT risk and the Notification No. Sor Thor. 38/2565.
3. IT Audit under the Established Plan and Scope	3.1 IT audit and reporting of IT audit results should be conducted as follows: 3.1.1 In the case of a small-scale business operator, an IT audit should be conducted at least once a year. In any case, an IT audit that covers all rules applicable to the small-scale business operator shall be completed at least once in every two years.

Operations	Details
	3.1.2 In the case of a low-risk business operator, an IT audit shall be conducted at least once a year. In any case, a full-scope audit covering all applicable rules shall be completed at least once in every two years; 3.1.3 In the case of a medium-risk or high-risk business operator, a full-scope IT audit covering all rules shall be conducted at least once a year; 3.2 Audit information shall be documented and recorded, such as working papers and audit evidence, for a minimum of two years from the date of creation. The documents shall be stored in a way that they will be readily available for inspection upon request by the SEC Office.
4. Provision of a Plan for Corrective Actions Identified in IT Audit and Progress Monitoring	A plan for corrective actions identified in the IT audit under Clause 3 above shall be suitable to the finding's risk level, and the implementation progress of such plan shall be monitored.
5. Preparation of and Reports on Audit Results	5.1 Results of the audit under Clause 3 above and the plan for corrective actions shall be presented to the business operator's board of directors or the business operator's audit committee without delay. 5.2[1] A business operator shall report the audit results and the plan for corrective actions that have been considered by the business operator's board of directors or the business operator's audit committee pursuant to Clause 5.1 above to the SEC Office in the form and procedure as specified on the website of the SEC Office within the following periods, whichever is due first:*

[1] A business operator that is a commercial bank under the law on financial institution business, life insurance company under the law on life insurance or financial institute established under other laws, which has only been granted a license to undertake the following types of securities business, while does not undertake any other types of securities business licenses, shall be exempt from performing the acts under Clause 5.2

1. brokerage, dealing or underwriting of debt securities; or
2. securities borrowing and lending business.

Operations	Details
	5.2.1 30 days from the date of presenting the audit report and the corrective action plan to the board of directors or the audit committee; 5.2.2 90 days from the end date of the report under Clause 3 above having been completed; or 5.2.3 three months from the end of the calendar year of the year in which the audit under Clause 3 above commences in the case that the report on the audit results could not be completed within the year of commencement of the audit. (* Note: For reporting of the audit results for 2023, a business operator shall submit such report within three months from the end of the 2023 calendar year.) 5.3 Audit result report and corrective action plan shall be retained for a minimum of two years from the date of creation, in a way that they are readily available for inspection upon request by the SEC Office.