

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
as amended by the SEC Office Notification No. Sor Thor. 33/2567 (No. 2)]

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 covering all rules applicable to small-scale business operators on a full-scope basis shall be conducted at least once every three years, in accordance with the cycle specified by the SEC Office.

Operations	Details
	3.1.2 In the case of a low-risk business operator, a full-scope IT audit covering all rules applicable to low-risk business operators shall be conducted at least once every three years, in accordance with the cycle specified by the SEC Office. In the event of a major IT security incident, small-scale business operators and low-risk business operators shall conduct a full-scope IT audit covering all rules applicable to the respective business operators within the same calendar year in which the incident occurred. If, due to necessity, a small-scale or low-risk business operator is unable to conduct the full-scope IT audit within the same calendar year of the major IT security incident, the business operator shall undertake the following actions within four months from the date on which the incident is discovered: (1) Report the circumstances necessitating the inability to conduct a full-scope IT audit within the year in which such circumstances arise, together with the IT audit plan, to the board of directors of the business operator, or the committee assigned by the board of directors in the case of a branch of a foreign commercial bank, and also report such circumstances to the SEC Office; and (2) Conduct a full-scope IT audit. 3.1.3 In the case of a medium-risk business operator, a full-scope IT audit covering all rules applicable to medium-risk business operators shall be conducted at least once a year; 3.1.4 In the case of a high-risk business operator, a full-scope IT audit covering all rules applicable to high-risk business operators 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

Operations	Details
	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 corrective action plan shall be presented without delay to the business operator's board of directors, the business operator's audit committee or, in the case of a branch of a foreign commercial bank, to a committee assigned by the board of directors. 5.2¹ A business operator shall report the audit results and the corrective action plan that have been considered by the business operator's board of directors, the business operator's audit committee or, in the case of a branch of a foreign commercial bank, to a committee assigned by the board of directors, 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 three months from the end of the calendar year in which the audit under Clause 3 was conducted, except in the case of a digital asset business operator that is required to report audit results in accordance with the Notification of the Securities and Exchange Commission No. Kor Thor. 19/2561 Re: Rules, Conditions and Procedures for Undertaking Digital Asset Businesses, dated 3

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
	July 2018. In such case, the digital asset business operator shall comply with the requirements under the Notification. 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.