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 2

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

Information Technology Governance

Scope of operation

Low-risk business operators, medium-risk business operators or high-risk business operators shall comply with the provisions specified hereunder.

Operation related to IT Governance

Part 1: Roles and responsibilities of the Board of Directors

A business operator shall ensure that IT risk governance will be supervised by its board of directors to ensure that the IT risk is aligned with risk appetite, taking into consideration the enterprise risk management (if any). The business operator shall at least address the following matters:

1.1 Establishment of an IT governance framework and oversight of IT plans, ensuring the IT plans will conform with business plans and be sufficiently appropriate for accommodating future IT changes and business operation changes;

1.2 allocation of appropriate and sufficient IT resources and IT personnel for business operation;

1.3 stipulation of written policies related to IT risk supervision, which shall at least cover the policies prescribed in Clause 2.2 of Part 2;

1.4 establishment of processes and procedures for IT risk management and IT security to be in line with policies in Clause 1.3, including ensuring appropriate implementation thereof;

1.5 creation of knowledge and awareness of IT risk for directors and personnel continuously and effectively; and

1.6 monitoring, reviewing, and reporting on the conformance of the policies in Clause 1.3 to the board of directors at least once a year. In case of the occurrence of any incident or change that may significantly affect the conformance of such policies, the board of directors shall be informed without delay.

Part 2: Organizational IT Risk Governance

2.1 A business operator shall establish an IT governance framework that shall at least contain the following features:

2.1.1 enabling independent checks and balances; and

2.1.2 being in line with the three Lines of Defense (3LoDs) concept, under which IT-related duties are clearly segregated as follows:

1st Line of Defense: Operations

2nd Line of Defense: Risk management and compliance with applicable laws and regulations; and

3rd Line of Defense: Audit

2.2 A business operator shall establish policies on IT risk supervision in writing which shall be approved by its board of directors or the committee assigned by the board of directors, as follows:

Policies	Control factors
2.2.1 IT risk management policy	(1) Roles and responsibilities of related persons in IT risk management; (2) Establishment of IT risk management process to ensure the risk will be in line with the organization's risk appetite.
2.2.2 IT security policy	(1) Organization of IT security; (2) Personnel and third-party management; (3) IT asset management; (4) Data security; (5) Access control; (6) Cryptographic control; (7) Physical and environmental security (8) IT operations security; (9) Communication system security; (10) IT project management, system acquisition, development and maintenance; (11) IT incident management;

Policies	Control factors
	(12) IT contingency plan.

2.3 A business operator shall operate according to the policies in Clause 2.2, as follows:

2.3.1 Communication of policies under Clause 2.2 to related persons[1] for acknowledgement in accordance with their roles, responsibilities, and data access rights in an easily accessible manner to enable such related persons to understand and comply with the policies properly;

2.3.2 Establishment of operational processes and procedures in compliance with the policies under Clause 2.2;

2.3.3 In the event of changes in the policies under Clause 2.2, such changes shall be communicated to all related persons and the operational processes and procedures shall be revised to be in line with such changes.

2.4 A business operator shall review or revise the policies under Clause 2.2 at least once a year and without delay upon occurrence of any incident that may significantly affect the governance and management of IT risk.

[1] "Related persons" means personnel, directors, including third-parties.