

SEC public hearing on proposed revisions to the IT Security Standard Rules

The Securities and Exchange Commission (SEC) is seeking public comments on proposed revisions to the Rules on Establishment of Information Technology System (IT Security Standard Rules) to ensure that capital market participants will be able to manage IT security risk and prepare for ever-increasing cybersecurity risk effectively as well as to enhance investor confidence in products and services in the capital market.

The SEC is proposing to revise the rules and related guidelines on the establishment of information technology system, which have been in force since 2016. The proposed changes aim to keep pace with (1) the changing IT usage in business practices, (2) the increasingly sophisticated technical approaches and mechanisms of cyber threats, (3) the revisions to preventive measures for addressing security pitfalls previously causing IT incidents in the capital market, and (4) the updated IT rules and guidelines issued by other regulators in the financial sector. The intended outcome is to accomplish the SEC's strategic priority to build cyber resilience and to ensure that licensed corporations have efficient IT systems and resilience to cyber threats and are able to comply with the governing rules efficiently.

Essentially, the proposed revisions cover the following key domains:

(1) Establish multiple levels of expected security controls and oversight techniques that apply differently to licensed corporations depending on their inherent technology risk, which varies in terms of nature of business, organizational structure, business size and complexity of the utilized technology. In addition, the scope of supervision would expand to cover additional entity types under the SEC regulations;

(2) Define clear roles, responsibilities and involvement of the board of directors, including the governance body, to ensure secure, effective and efficient IT practices and IT usage in businesses. The update would also include requirements related to the information security audits and the qualifications of the auditor who must be a qualified person with independence, objectivity and required competency;

(3) Update the requirements per current standards and guidelines to be in alignment with international standards and other financial IT regulations;

(4) Determine additional requirements and guidelines for IT quality and IT service management such as IT project management and capacity management;

(5) Enhance cybersecurity control measures to strengthen and protect the capital market from cyber threats and recurrence of past incidents as well as to align with the requirements under the Thailand Cybersecurity Act B.E. 2564 (2021), for instance, vulnerability assessment and penetration test;

(6) Strengthen the third-party management section by expanding the scope to include service providers or business partners having a system interconnection or those providers/partners who can access critical data of a business operator or those of its customers.

The consultation paper is available at <https://www.sec.or.th/hearing>. Stakeholders and interested parties are welcome to submit comments and recommendations via the website or email: nakharin@sec.or.th, thanakornb@sec.or.th, or chat@sec.or.th.

The public hearing ends on 25 December 2021.